PTO/AIA/15 (07-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office. U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	47583.5US02
First Inventor	Paul Timothy Miller
Title	CRYPTOGRAPHIC SECURITY ......
Express Mail Label No.	Electronically filed

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: **Commissioner for Patents**
P.O. Box 1450
Alexandria VA 22313-1450

1. ☑ **Fee Transmittal Form.**
(PTO/SB/17 or equivalent)

2. ☑ **Applicant claims small entity status.**
See 37 CFR 1.27.

3. ☑ **Specification.** [*Total Pages* 60]
Both the claims and abstract must start on a new page
(For information on the preferred arrangement, see MPEP § 608.01(a))

4. ☑ **Drawing(s).** *(35 U.S.C. 113)* [*Total Sheets* 11]

5. **Inventor's Oath or Declaration.** [*Total Sheets* 2]
(including substitute statements under 37 CFR 1.64 and assignments serving as an oath or declaration under 37 CFR 1.63(e))
a. □ Newly executed (original or copy)
b. ☑ A copy from a prior application (37 CFR 1.63(d))

6. ☑ **Application Data Sheet.** **See Note below.*
See 37 CFR 1.76 (PTO/AIA/14 or equivalent)

7. □ **CD-ROM or CD-R.**
in duplicate, large table or Computer Program *(Appendix)*
□ Landscape Table on CD

8. **Nucleotide and/or Amino Acid Sequence Submission.**
(if applicable, items a. – c. are required)
a. □ Computer Readable Form (CRF)
b. □ Specification Sequence Listing on:
i. □ CD-ROM or CD-R (2 copies); or
ii. □ Paper
c. □ Statements verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. □ **Assignment Papers.**
(cover sheet & document(s))
Name of Assignee____________________
____

10. □ **37 CFR 3.73(c) Statement.** □ **Power of Attorney.**
(when there is an assignee)

11. □ **English Translation Document.**
(if applicable)

12. □ **Information Disclosure Statement.**
(PTO/SB/08 or PTO-1449)
□ Copies of citations attached

13. □ **Preliminary Amendment.**

14. □ **Return Receipt Postcard.**
(MPEP § 503) (Should be specifically itemized)

15. □ **Certified Copy of Priority Document(s).**
(if foreign priority is claimed)

16. □ **Nonpublication Request.**
Under 35 U.S.C. 122(b)(2)(B)(i). Applicant must attach form PTO/SB/35 or equivalent.

17. □ **Other:**____________________
____

***Note:** (1) Benefit claims under 37 CFR 1.78 and foreign priority claims under 1.55 **must** be included in an Application Data Sheet (ADS).
(2) For applications filed under 35 U.S.C. 111, the application must contain an ADS specifying the applicant if the applicant is an assignee, person to whom the inventor is under an obligation to assign, or person who otherwise shows sufficient proprietary interest in the matter. See 37 CFR 1.46(b).

18. CORRESPONDENCE ADDRESS

☑ The address associated with Customer Number: 27683 **OR** □ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone		Email	

Signature		Date	3-18-16
Name (Print/Type)	David Bowls	Registration No. (Attorney/Agent)	39,915

This collection of information is required by 37 CFR 1.53(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	47583.5US02
	Application Number	

Title of Invention	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2:

□ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove
Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Paul	Timothy	Miller	

Residence Information (Select One) ● US Residency ○ Non US Residency ○ Active US Military Service

City	Irvine	**State/Province**	CA	**Country of Residence**	US

Mailing Address of Inventor:

Address 1	10 Wandering Rill		
Address 2			
City	Irvine	**State/Province**	CA
Postal Code	92603	**Country** i	US

Inventor 2 Remove
Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	George	Allen	Tuvell	

Residence Information (Select One) ● US Residency ○ Non US Residency ○ Active US Military Service

City	Thompson's Station	**State/Province**	TN	**Country of Residence**	US

Mailing Address of Inventor:

Address 1	2617 Clayton Arnold Road		
Address 2			
City	Thompson's Station	**State/Province**	TN
Postal Code	37179	**Country** i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

**Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).**

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	47583.5US02
	Application Number	
Title of Invention	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE	

□ **An Address is being provided for the correspondence Information of this application.**		
Customer Number	27683	
Email Address	ipdocketing@haynesboone.com	Add Email Remove Email

Application Information:

Title of the Invention	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE		
Attorney Docket Number	47583.5US02	**Small Entity Status Claimed** □	
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	11	**Suggested Figure for Publication (if any)**	

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

□ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

□ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	● Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	27683		

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	47583.5US02
	Application Number	
Title of Invention	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE	

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Continuation of	14/458123	2014-08-12

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14/458123	Continuation of	13/366197	2012-02-03	8817984	2014-08-26

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13/366197	Claims benefit of provisional	61/462474	2011-02-03

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

			Remove
Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	47583.5US02
	Application Number	

Title of Invention	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	47583.5US02
	Application Number	

Title of Invention	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

□ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

□ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	47583.5US02
	Application Number	
Title of Invention	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

● Assignee ○ Legal Representative under 35 U.S.C. 117 ○ Joint Inventor

○ Person to whom the inventor is obligated to assign. ○ Person who shows sufficient proprietary interest

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

Organization Name	mSignia, Inc.		
Mailing Address Information For Applicant:			
Address 1	10 Wandering Rill		
Address 2			
City	Irvine	**State/Province**	CA
Country	US	Postal Code	92603
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button.

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	47583.5US02
	Application Number	

Title of Invention	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

If the Assignee or Non-Applicant Assignee is an Organization check here. □

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature				Date (YYYY-MM-DD)	2016-03-18
First Name	David	Last Name	Bowls	Registration Number	39915

Additional Signature may be generated within this form by selecting the Add button.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	47583.5US02
	Application Number	
Title of Invention	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE

Paul Timothy Miller, George Allen Tuvell

CROSS REFERENCE TO RELATED APPLICATIONS

This application is a continuation of co-pending U.S. Patent Application No. 14/458,123 filed August 12, 2014, which is a continuation of and claims benefit of priority to U.S. Patent Application No. 13/366,197 filed February 3, 2012, now U.S. Patent No. 8,817,984, issued August 26, 2014, which claims the benefit of U.S. Provisional Patent Application No. 61/462,474 filed February 3, 2011, all of which are incorporated by reference.

BACKGROUND

Technical Field

The present disclosure generally relates to dynamic key cryptography used, for example, for authentication between a client electronic device and a service provider, encryption of data communications, and digital signatures and, more particularly, to cryptography using dynamic keys derived from dynamically changing key material.

Related Art

Use of computers for connecting to a network (such as the Internet) and communicating with a variety of services risks the privacy of many types of information belonging to a user including, for example, the user's relationships (e.g., social connections), business secrets, banking details, payment options, and health records. The use of cryptography is common to authenticate identities, protect data, and digitally sign the summary (i.e. digest) of an action.

Cryptography generally uses an algorithm (e.g., Advanced Encryption Standard (AES), Rivest Shamir Adelman (RSA)) to combine cryptographic keys (which may be symmetric, public, or private, for example) with plain text to form cipher text. Cryptography keys are typically random numbers without any special meaning. The process of distributing cryptographic keys and storing them on a client computer (referred to as "key management") is difficult to perform securely and is often the point-of-attack for breaking the security of a cryptographic system. The key represents a single sequence of data and thus a single point-of-failure for the cryptographic system. Since the key normally must be present at the client computer, finding the key and then copying it to another computer can allow an imposter entity to masquerade as a valid entity.

Secure elements (e.g., smartcards) can securely store the cryptographic key and, in some instances, generate the key in a secure environment. Access to the key was typically controlled by requiring the user to enter a personal identification number (PIN); this ensured that the user had to provide a secret before the secure element would allow use of the key. Such access to a key is commonly known as two-factor authentication, and the two factors are generally referred to as: "Something You Know" and "Something You Have". A third factor, "Something You Are", can include, for example, biometric information. The factors themselves are related in use but entirely separate in material. Possession of the physical secure element ("Something You Have") may be via validation of cryptographic functions using the random number cryptographic key provisioned to a particular secure element whose use may be protected by a secret PIN ("Something You Know"). There is no implicit binding between the key and the user.

The use of certificates in cryptography enabled the binding of a distinguished name (e.g., a unique user) with a cryptographic key. Yet, still the cryptographic key is a random number, and when the key is validated, the cryptographic system attributes the user in the certificate to the usage of the key; the key matter itself has no relation to the user.

On the Internet, ensuring a real-world identity for the user is critical for protecting data and privacy. Mobile users especially are at risk because they often do not use anti-virus applications and many of the service providers use applications (apps) optimized for simplicity, not security. This leaves much of the private data meaningful to both a user's identity and a service's value inadequately protected. Since online service providers (OSP) incur much of the risk, safety has become their responsibility.

The standard method for identifying a user to an online service is by entering a username and password. The username is a known service index and, as such, can be stored on the computer for convenience. The password is a user secret verifiable by the OSP; it should not be stored at the computer, where it can be compromised. However, because a quality password has many characters which should be a mix of upper, lower, punctuation and special characters, the password is often difficult and time-consuming to type. This is especially true on a mobile computer using touch keypads that have various 'levels' of keypads for characters beyond simple alpha-numeric. Thus, many mobile apps store the password on the computer. Because mobile operating systems require mobile apps to be signed in order to run, the apps themselves cannot be altered after installation. So, any data stored by the mobile app is separate from the mobile app and often can be vulnerable to attack. Furthermore, because the app cannot change, if encryption was used to protect the cached password, there could only be one encryption key for all instances of the application. This commonality made harvesting and cracking stored passwords on a mobile computer relatively simple, even if the passwords were encrypted, since they all used the same key for decryption.

Computer and computer identification has been attempted by calculating a hash of the minutia found on a computer to uniquely identify the computer, often referred to as a computer fingerprint. Computer fingerprints typically are used, among other things, to 'lock' software to a particular computer fingerprint and identify computers used in online actions to profile the history and potential risk of particular actions. A typical computer identifier is computed and remains static; to ensure reliability the computer fingerprint typically uses computer minutiae (e.g., serial numbers) that normally do not change. Thus, current computer fingerprints typically use a relatively small set of static minutia which may be prone to spoofing. Some approaches to improving computer identification have sought to increase the number of minutiae used in identifying the computer through the analysis of time (both in clock and network latency) and bits of information left on the computer (i.e. 'cookies'). However, as more minutiae are included in the computation, the probability that changes occurred naturally to the minutia can result in a new computer fingerprint. This falsely identifies a computer as 'different' when it is actually the same computer (often referred to as 'false negatives'). These changes to the minutia on a unique computer occur naturally during normal use and can invalidate the computer fingerprint process or inconvenience the user or service by forcing a re-initialization of the computer fingerprint.

SUMMARY

According to one or more embodiments of the present invention, methods and systems for dynamic key cryptography use a wide range of minutiae as key material including computer hardware, firmware, software, user secrets, and user biometrics rather than store a random number as a cryptographic key on the computer. Methods and systems for using dynamic key cryptography, according to one or more embodiments, can be used for authenticating users to services, ciphering data for protection, and digitally signing message digests. In one embodiment, dynamic key cryptography anticipates changes to computers caused by industry updates to hardware, firmware, and software of computers.

In one embodiment, a method of dynamic key cryptography includes: selecting a subset from a set of minutia types; for a particular device, sending a challenge to the device, in which: the challenge includes information from which the device can collect actual values of minutia corresponding to the selected subset of minutia types in order to form a cryptographic key, the cryptographic key is never transmitted from the device across any communication channel, and the cryptographic key is used to encrypt an actual response to the challenge; pre-processing a set of responses to the challenge based on tracking updates of minutia from which the selected subset of minutia types is selected, in which: the set of pre-processed responses covers a range of all actual responses possible to be received from the particular device if the combination of the particular device with collected actual values of minutia is valid; comparing the actual response from the particular device to the set of pre-processed responses; and validating the combination of the particular device with the collected actual values if the actual response is included in the set of pre-processed responses for the particular device.

In another embodiment, a method includes: selecting at least one type of minutia from a plurality of minutia types; forming a challenge that conveys the selection of minutia types; computing a plurality of pre-processed responses possible to receive from a valid device, in which: each pre-processed response is computed using a key, each key is computed using values that are possible for the selection of minutia types; sending the challenge to the device; receiving an actual response to the challenge from the device, in which: the actual response is computed using an actual key, the actual key is computed using: a deduction of the selection of minutia types from the challenge and actual values of the selection of minutia types; comparing the actual response to the pre-processed responses for a match; and based on whether or not a match was found, validating the combination of the device with the actual values of the selection of minutia types.

In still another embodiment, a system includes a server configured to communicate with a device, in which the server selects at least one type of minutia from a plurality of minutia types; the server forms a challenge that conveys the selection of minutia types; the server computes a plurality of pre-processed responses possible to receive from a valid device, in which: each pre-processed response is computed using a key, each key is computed using values that are possible for the selection of minutia types; the server sends the challenge to the device; the server receives an actual response to the challenge from the device, in which: the actual response is computed using an actual key; the actual key is computed using: a deduction of the selection of minutia types from the challenge and actual values of the selection of minutia types; the server compares the actual response to the pre-processed responses for a match; and based on whether or not a match was found, the server validates the combination of the device with the actual values of the selection of minutia types.

In yet another embodiment, a computer program product includes a non-transitory computer readable medium having computer readable and executable code for instructing a processor to perform a method, the method including: selecting at least one type of minutia from a plurality of minutia types; forming a challenge that conveys the selection of minutia types; computing a plurality of pre-processed responses possible to receive from a valid device, in which: each pre-processed response is computed using a key and each key is computed using values that are possible for the selection of minutia types; sending the challenge to the device; receiving an actual response to the challenge from the device, in which: the actual response is computed using an actual key, the actual key is computed using: a deduction of the selection of minutia types from the challenge and actual values of the selection of minutia types; comparing the actual response to the pre-processed responses for a match; and based on whether or not a match was found, validating the combination of the device with the actual values of the selection of minutia types.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a system diagram illustrating communication and security between a client, a client device and a service provider facilitated by a dynamic key cryptography provider in accordance with one or more embodiments;

Figure 2, comprising Figure 2A and Figure 2B, is a system diagram illustrating a challenge, response and validation process performed by the system of Figure 1 in accordance with an embodiment;

Figure 3 is a system diagram illustrating a service provider application (app) delivery system in accordance with an embodiment;

Figure 4 is a system process flow diagram illustrating a system for registration of computer system and user minutiae and services in accordance with an embodiment;

Figure 5 is a system diagram illustrating a system to catalogue and model industry minutia and user heuristics to create and update anticipated minutia databases in accordance with an embodiment;

Figure 6, comprising Figure 6A and Figure 6B, is a system process flow diagram illustrating a system for validation scoring, confidence rating and step-up authentication processing in accordance with an embodiment;

Figure 7 is a system process flow diagram for an authentication and digital signature system capable of incorporating three identity factors in accordance with an embodiment;

Figure 8 is a system process flow diagram illustrating a system for application processing for local and update data security functions in accordance with an embodiment; and

Figure 9 is a system diagram illustrating computer identity provider lifecycle functionality and services to service providers in accordance with an embodiment.

DETAILED DESCRIPTION

In accordance with embodiments of the present invention, methods and systems of dynamic key cryptography using dynamically changing keys composed of or derived from dynamically changing key material provide cryptographic services such as authentication, data protection, and digital signature by uniquely identifying a user's computer or other electronic device based on (1) the electronic device itself, e.g., a mobile phone or personal computing device, and using a very wide range of hardware, firmware, and software minutia found on the computer; (2) secrets a user of the computer knows; and (3) biometric information the computer might collect from the user. Dynamic key cryptography in accordance with one or more embodiments enables secured actions for users of electronic computers and, more particularly, provides authentication between a client electronic computer and a service provider, encryption of data electronically stored or sent on a communication channel, and digital signature for electronic digests of actions performed by the user on an electronic computer.

The dynamic key cryptography system according to one embodiment anticipates changes to the minutia caused by updates and natural usage of the computer and practically eliminates false negatives that block valid users from a network service. Dynamic key cryptography may provide a safe, reliable method to users of network services for authenticating the user to network services that protects both the user and the network services, protects the integrity and privacy of data, and provides for digitally signing the digest of an action performed by the user on the electronic computer.

One or more embodiments may provide features such as: 1) simple user experience – no difficult passwords to remember or type, the user device or computer is invisibly authenticated and the user can be asked to enter a second identity factor such as a secret PIN or biometric (e.g., voiceprint) into the computer only if required by the service and protected services can be automatically reconnected to a new device or computer when it is registered by the user; 2) unprecedented security – using a wider range of hardware, firmware, software, secret and biometric minutia to deliver a very accurate device or computer and user identity that is more difficult to spoof, especially as some computer identifier values are not static but are expected to change; 3) reliability – anticipating changes to the user device or computer delivers a tolerant, yet secure authentication with fewer false negatives that anger users and clog customer support services; and 4) service and data separation – delivered as an integrated part of a mobile application (app), a “foundation” (e.g., dynamic key cryptographic service) helps protect the app, encrypt service data stored on the user device or computer, digitally sign actions and allows the service to react without affecting other services, e.g., should data need to be wiped, only the app's data is affected, not the user's other information such as the user’s pictures or messages.

One or more embodiments may enable a more convenient method for connecting the user and service. For example, instead of subscribers typing in cumbersome passwords (or worse yet, storing them unencrypted on the computer), the dynamic key cryptographic (dynamic key crypto) service and related client software can compute and manage the unique properties of the user device or computer. The resultant identified computer can be used in place of passwords to simplify the customer connection experience. Since the computer itself is uniquely identified, it represents a safer method of identifying customers (e.g., users or subscribers). By forming cryptographic keys which use minutia found on the computer, the computer itself (as defined by its minutia) is validated, not a static key stored or intended to be stored only on the computer. The discovery and copying of a single value (the secret key) is significantly easier than the discovery and copying of a very large range of computer minutia values. In addition, the writing of a single key in a computer's memory effectively counterfeits the uniqueness of a computer identified by a single, static stored value. To counterfeit a dynamic key crypto-identified computer, it would be necessary to intercept various methods to learn the minutiae values of the computer. Several direct and related methods may exist for learning the value of a particular computer minutia; to effectively counterfeit the computer, it may be that all methods for accessing all computer minutia values would need to be intercepted and the fraudulent response returned. Furthermore, since the dynamic key crypto system expects certain computer minutia values to change, a successfully counterfeited computer would also need to ensure the fraudulent computer minutia values change in an expected manner. Should a user's online activities require an even higher level of trust, the platform (e.g., dynamic key crypto service and related client software) can force the user to enter the user's standard PIN into the computer to ensure a valid user is the person using the computer.

Several technologies exist for processing security and assurance claims using static values. These include passwords themselves and static 'seed keys' for functions like one-time-password and challenge-respond security mechanisms. Even public key cryptography is based off a static key pair (public and private). One or more embodiments of the dynamic key crypto system may use a very large numeric representation (e.g., 100,000's of bits) of computer and user minutia (e.g., any piece of information that can be definitively associated with the computer and its user, including information from the general categories of what the user or computing device has, what the user knows, and what the user is) to form cryptographic keys that support a range of security functions in a verifiable manner (a cornerstone of security). In one or more embodiments methods based on the predictable dynamic nature of the minutia may allow for verification of the minutia (as if they were a single static value) but not all of the minutia is required to be static; most values of the minutia can (and are expected to) change and evolve over time and the change of the minutia values themselves increases the perceived randomness of the resultant dynamic crypto keys. The validation of dynamic key cryptography based on changing minutia uses a complex confidence scoring which isolates and evaluates the minutiae that have changed and uses confidence weightings against the predictability of such changes. Changing minutia when used as dynamic key material for dynamic key cryptography adds complexity to the cryptographic system which can improve security as a one-time copy of the minutia values or resultant key will likely fail later in time as the minutia values are expected to change.

Layering static minutia (e.g., hardware minutia, user secrets, some user biometrics), slow-changing minutia (e.g., firmware minutia, some user biometrics), and predictably changing minutia (e.g., software minutia) can create a very large set of key material (or keyspace) which can be processed as subsets of minutia. These subsets of minutia function as static keys over a particular time interval and provide increased security while being fault-tolerant to normal and natural anomalies. Examples of categories of minutia include various hardware, firmware, software, user secrets, and user biometric values. For example, hardware minutia may include the make and model of the computing device (e.g., smart phone or pad), an international mobile equipment identification (IMEI) number of the computing device, or a circuit manufacturer's ID number which may be readable from a circuit chip element of the computing device. Similarly, examples of firmware and software minutia may include which firmware and software codes are installed on the computing device and characteristics such as what particular version or release date of firmware or software are installed on the computing device. Other minutia may include such information as geo-location from GPS (global positioning system) capability of the computing device. In some embodiments, minutia may also include secrets a user of the computing device knows (e.g., a PIN number or password) or biometric information the computing device might collect from the user (e.g., a fingerprint, voiceprint, or retinal scan). In this manner, dynamic key cryptography can utilize minutia values from the three identity factors (“have”, “know”, and “are”) to form a dynamic key so that dynamic key crypto purposes such as authentication, data protection, and digital signature can benefit from the three identity factors simultaneously.

Dynamic key cryptography key matter is a significant improvement over static cryptographic keys of simply random numbers (as nearly all prior art cryptography uses). Dynamic key crypto keys are permutations of a very large collection of minutia values, many of which change over time; the result is a seemingly random number comprised of independently meaningful minutia values.

To achieve fault tolerance over a possibly changing set of minutia, anticipated changes to minutia and multiple subsets of minutia that provide back-up to any single subset can be used. By using mass produced electronic devices (e.g., mobile units and computers) which contain both a vast array of minutia and predictable evolution paths of minutia, a dynamic encryption system of methods based on evolving minutia can be maintained for the benefit of nearly any security function. In addition, since the range of minutia is so large, certain cryptographic functions can be performed several times using different subsets of minutia. In this manner, should one subset of minutia change, cryptographic checks using other minutia subsets and the anticipated changes to the minutia can improve fault tolerance and detection of spoofed minutia values.

Assertions regarding a computer’s uniqueness, confidence in the computer’s uniqueness, and service-orientated directives (e.g., provision, lock-hold, erase, transfer, blacklist) are formulated, controlled, and directed by the dynamic key crypto service. For example, computer dynamic key crypto libraries (installed on various user devices) gather the computer minutia values (e.g., from various user devices) and act on the computer (selected one of the various user devices) in response to dynamic key crypto service directives. The heuristics for the predictive and constantly changing minutia values are performed in the dynamic key crypto service using data forwarded by the dynamic key crypto libraries (from the various user devices) in addition to data gleaned from industry sources. Industry data includes cataloguing publically available data (such as over-the-air upgrades – including operating system (OS), firmware, and applications – and network updates) over the range of possible computers. While nearly infinitely larger than the changes that can occur to a single computer (lending security via a broader search space) the industry data is still finite and, therefore, useful in predictive heuristics regarding computers in use.

Various embodiments may provide systems and methods for secure dynamic key cryptography services including:

1) Registering online service providers (OSP) with the dynamic key crypto service to create custom (for each OSP) computer dynamic key crypto libraries that conduct security functions but are resistant to successful attacks by other services and prohibit collaborating online service providers from profiling users.

2) Collecting and registering the minutia values with the dynamic key crypto system, tying the minutiae to an online service provider account identifier.

3) Gathering industry information regarding updates to computer hardware, firmware and software to create a catalogue of industry minutia values which may possibly appear on registered computers when they are updated. The catalogued industry minutia values are indexed and the possible minutia and current minutia are combined and permutations intelligently stored to anticipate future minutia possibilities.

4) Identification based on a hash from a subset of minutia taken from a very wide range of minutia found or collected by the computer including hardware, firmware, software, user secrets, and user biometrics. The authentication can be performed as an intelligent challenge and response which indexes minutiae and, when compared to possible responses from anticipated minutiae, can ascertain minutia changes without having to actually exchange the minutiae between the computer and dynamic key crypto services.

5) Scoring the confidence of a valid response based on the minutia used, the anticipated and expected changes to the minutia used including non-computer factors such as user PIN entry, geo-location, and biometrics. Different minutia can be intelligently chosen for the challenge to achieve a response that yields a higher confidence score, increased computer uniqueness, multiple identity factors, and particular minutia isolation.

6) Protecting the application and data running on a computer by using the minutia in cryptographic functions such as encrypted memory, local identification, and heartbeat to prohibit application self-destruction. Some cryptographic functions are computed using more than one subset of minutia to allow back-up functionality should minutia used in the

cryptographic function change. The high number of meaningful minutia enables a more complex interaction between the user, the computer, and the software computing the identifier. The increased "chatter", a mix of meaningful and decoy reads of minutia, obscure which minutia is meaningful, and thereby increases the difficulty of spoofing minutia values and intercepting calls intended to counterfeit the original computer.

7) Digitally signing a digest of an action performed by the user on the computer by ciphering the message digest with a key formed by minutia values which can include the three factors of identity ("have", "know", and "are", e.g., respectively, computer or device, user secret, user biometric information).

8) Notifying a wide range of online service providers should a computer status change. This enables a single event to trigger responses from a wide range of registered online service providers so that security and service continuity are maintained.

9) Forcing a user to enter a service PIN, computer PIN or biometric on a registered computer to include user minutia in the dynamic key cryptography function and ensure that a valid user is controlling an identified computer.

Some embodiments of systems and methods allow the calculation of one or more minutia value subsets to be based on a very wide possible range of minutia from various categories including hardware, firmware, software, user secrets, and user biometrics. One embodiment models predictive and anticipated changes that occur naturally and during the use of a computer or device. The larger considered ranges of minutia found on a computer or collected by a computer and the modeled dynamic nature of some minutiae enable a more robust and secure authentication system which is less prone to spoofing.

One embodiment uses a computer identity provider service to collect computer minutia information from the industry and uses this data to anticipate possible changes and permutations to minutiae on registered computers. By anticipating changes in minutiae found on the hardware, firmware, and software elements of a computer, embodiments are more fault-tolerant to natural changes in the computer. In this manner, embodiments can anticipate changes to minutiae and, through a challenge and response exchange between a computer and dynamic key crypto service, synchronize changes to minutiae without actually exchanging the minutiae between the computer and dynamic key crypto service.

Since nearly all security functions such as authentication, encryption, and digital signature are based on static keys and identifiers, embodiments of the present systems and methods also allow for the in-system back up of some cryptographic functions and secure transmission, synchronization, and updating of dynamically changing minutiae between the computer and the dynamic key crypto service. The dynamic key crypto service and computer enable the dynamically changing minutiae to be used in or used in place of traditionally static security functions including authentication, encryption, digital rights management, and data protection.

Figure 1 illustrates a system 100 in which a service user 20 may communicate through a network 16 (e.g., the Internet, local area networks (wired and wireless), and personal networks (e.g., P2P, Bluetooth, near field communications (NFC)) using a computer 18 (e.g., a mobile phone, computer system, smart phones, laptops, tablets, sensors, payment terminals, and meters or any other communication capable electronic computer). The computer 18 (also referred to as “electronic device”, “user device”, or simply “device”) may operate by executing an operating system (OS) that may enable execution on computer 18 of a dynamic key crypto library 56 and a service provider app 44. Service provider app 44 may be provided by one or more of a number of various OSPs and may provide features specific to a particular service provider 14 that provides the service provider app 44 to the service user 20 and user computer 18. As shown in Figure 1, service provider app 44 may interface with dynamic key crypto library 56, and both service provider app 44 and dynamic key crypto library 56 may interface with computer 18 and its operating system. Service user 20 may communicate with service provider 14 over the network 16 using computer 18, for example, using service provider app 44. A service user 20 may be a person that can have several different types of computer 18 and may be a user of any number of service provider systems 14. Likewise, a computer 18 may be used by more than one service user 20, for example, family members sharing a smartphone or pad.

A dynamic key crypto provider 10 may provide various services and functions related to minutiae found on the computer 18 or minutiae collected by the computer 18 from the service user 20. The dynamic key crypto provider 10 may be a web service capable of securely manipulating and analyzing large amounts of data such as performing calculations, data modeling, permutation processing, interpolation, internet searches and complex database functions. The dynamic key crypto provider 10 may be cloud-based so it can have sufficient computational speed and power to off-load intensive computational efforts from a sometimes resource-constrained computer 18. The dynamic key crypto provider 10 may provide a secured processing environment for the processing in some embodiments including managing an enormous data-intensive query engine for complex data pattern matching, modeling and processing of complex and numerous permutations. As shown in Figure 1, dynamic key crypto library 56 may communicate with dynamic key crypto provider 10 and may also communicate with the service provider 14 through Network 16. Dynamic key crypto provider 10 also may communicate with online service providers via network 16 and may communicate with the particular service provider 14 that provides the service provider app 44 to the service user 20 and user computer 18. Service provider 14 may have a customer-vendor relationship, for example, with dynamic key crypto provider 10 in which service provider 14 is a customer receiving services from dynamic key crypto provider 10. There can be any number of service provider systems 14 connected to the dynamic key crypto provider 10. The service provider 14 may be an industry typical website usually requiring a username and password. Examples of a service provider 14 include but are not limited to social networking websites, corporate IT services, and online banking, healthcare, and travel services.

Figure 2 shows an illustrative example for providing and using dynamic key cryptography to ensure a valid service user 20 is using an authenticated computer 18 in a system such as system 200 shown in Figure 2. As described in more detail below, system 200 may collect and catalog a number of minutiae values of computer 18 and service user 20 that may be useful for identifying the computer 18 and service user 20 in the sense that computer minutia 64 and secrets and biometric minutia 26 can be used by the dynamic key crypto provider 10 to form dynamic keys unique to each and every distinct computer 18 and service user 20. In other words, each distinct computer 18 may have a method for using unique computer minutia 64 and secrets and biometric minutia 26 in system 200 that corresponds to that distinct computer 18 and service user 20, and each uniquely identified computer 18 corresponds to one and only one distinct computer 18 and each uniquely identified service user 20 may correspond to one and only one distinct service user 20. The unique identification of a computer 18 may be processed by system 100, for example, by a service provider 14 or by the dynamic key crypto provider 10, and there be no meaningful single identifier or identity key itself stored on the computer 18. System 200 shown in Figure 2, illustrates an example of identifying and authenticating a specific computer 18 and service user 20 via challenge, response and validation sequences performed by dynamic key crypto provider 10. Each distinct computer 18 and service user 20 may be recognized, for example, by specific computer minutia 64, specific secrets and biometric minutia 26, combinations of computer minutia 64, combinations of specific secrets and biometric minutia 26 or combinations of both specific computer minutia 64 and combinations of specific secrets and biometric minutia 26 found on the computer 18 or collected by the computer 18 from the service user 20 as cataloged by the dynamic key crypto provider 10.

Collection of minutia can include methods such as fuzzing and hashing that obfuscate the actual values of minutiae that represents personal identifiable information before the minutiae values are sent from the computer 18 to the dynamic key crypto provider 10 such that the anonymity of a service user 20 is maintained. For example, phone numbers can be hashed so that the actual phone number is not known. In another example, the geo-location home of a service user 20 can be fuzzed by truncating the GPS coordinates so that the value processed by the dynamic key crypto library 56 represents, for example, a multiple mile radius, not multiple feet. In this manner, it would be difficult to determine the exact address a computer 18 resides nearly every night that could be interpolated to be the home of the service user 20. The fuzzy geo-location can be beneficial because the location of the computer 18 can be tracked without invading the privacy of the service user 20 because, to the dynamic key crypto provider, the service user 20 can be anonymous. If a service provider that knows the true identity of a service user 20 were to also know the geo-location of the device, the privacy of the service user 20 could be abused. Thus, a separation of device and user knowledge can exist so that the device (i.e. computer 18) of an anonymous service user 20 can be tracked 24×7 and service providers (who do know the identity of service user 20) can ask for geo-location information from dynamic key crypto provider 10 only when they require it so as to gain benefit of geolocation without a privacy invasion of the service user 20.

As shown in Figure 2 at step 2001, in one example, computer minutia 64 can represent a set of 390 distinct minutiae values that may be chosen for collecting and cataloging from the computer 18. In the particular example, there are 40 categories or types of the minutia that are hardware minutia; 70 categories or types of the minutia are firmware minutia; and 280 categories or types of the minutia are software minutia. Hardware minutia may include such items as the device manufacturer, model number, serial number, and international mobile equipment identification (IMEI) number, for example. Firmware minutiae may include, for example, the name of the firmware vendor, version number, revision number, revision date, communication and telephony services, location and GPS data, and operating system. Software minutia, similarly for example, may include application name, supplier identification, software release number, memory reads, software cataloguing, clock and other counters, and date. Hardware minutia values typically cannot change without changing a physical component of the computer 18. Firmware minutia can be updated but usually their update is controlled by someone other than the service user 20. Software minutia changes dynamically via various individual instantiations of service user 20 and includes elements that may require predictable, constant change in normal situations (i.e., frequently called contact phone numbers).

It is important to note that software minutiae values can often reflect customizations performed by the service user 20. In this manner, software minutiae values can accurately identify computer 18 devices that are otherwise extremely similar in hardware and firmware. When the computer 18 is manufactured, devices are very similar, hence the need for serial numbers, but, under security considerations, these hardware minutia identifiers are few in number and can be easily spoofed. Significant customization affecting software minutiae values is typically done within days, even hours, of ownership of a computer 18 by the service user 20. Thus the software minutiae values diverge significantly at device personalization and the addressable space continues to expand throughout the use of the computer 18 by the service user 20. Therefore, the uniqueness of a computer 18 increases with time after manufacturing, this is often referred to as entropy, or the natural tendency towards chaos, and, thus, software minutiae are valuable in the security of dynamic key cryptography functions. To illustrate the potential range represented by the values of minutia if, for example, there were 300 minutia values each averaging four bytes in length, by interleaving and mixing the minutia values to form dynamic crypto keys, the keys could represent a space defined by as 2 raised to the 9600th power (cryptographic keys of 2 raised to the 1024 power are considered secure by the industry).

Nearly any data can be introduced into the system 200 by the definition and addition of minutia classes. For example, PIN, password, service history and other service user 20 secrets can be entered and processed as if they were a class of minutia. For example, a minutia index might refer to memory location where the minutia value could be read and processed. If the minutia index for the PIN is sent to the device, instead of, for example, reading a memory location, a PIN screen can be displayed on the computer 18, the service user 20 can enter their PIN (or other secret value) and the information entered can be processed as the minutia value in the method here described by system 200. A similar process can be performed for biometric values, for example, facial geometry, voice patterns, fingerprinting. In another example, the service provider app 44 might be analyzed and the software structure itself provide minutiae values that can be challenged and validated to ensure the run-time integrity of the calling application service provider app 44. Thus by adding minutia classes, any information can be processed to get the benefits of system 200 (e.g., secure input for crypto key material, fuzzy validation matching, inferred minutia value learning, confidence rating).

Step 2003 shows an example of specific values of the minutia 70 database for a specific computer 18. The minutiae can be obtained via the dynamic key crypto library 56. Various instances of the dynamic key crypto library can exist on a single computer 18 and can be related to one or more instances and providers of a service provider app 44. In this example, the first hardware minutia (H1) may be the IMEI number of computer 18, and for the specific computer 18 of the example, the IMEI number may be encoded as "1234". The computer 18 may have specific values for the 40 different hardware minutia, H1 to H40; specific values for 70 different firmware minutia, F1 to F70; 280 specific values for different software minutia, S1 to S280, 2 specific values for service user 20 secrets, ?1 and ?2; and 5 specific values for service user 20 biometric minutia, B1 to B5, from which it may be possible to accurately and uniquely identify the specific computer 18 and associated service user 20 for computer 18. The actual minutia used and their index ordering as H1 to H40, F1 to F70, S1 to S280, ?1 to ?2, and B1 to B5 provide a particular cataloging scheme or a cataloging of minutia DB 70 for the specific example illustrated in Figure 2. The combination of specific hardware, firmware, software, secret and biometric values found on the computer 18 and collected from the service user 20 at a particular time or within some pre-defined time frame may be referred to as the "current device image" as indicated at step 2003.

For a particular computer 18 and a particular scheme (e.g., H1 to H40, F1 to F70, S1 to S280, ?1 to ?2, and B1 to B5 of Figure 2) a number of possibilities for specific values of the minutia can actually occur on the computer 18, be known by the service user 20 or represent the biometrics of service user 20. For example, as indicated at step 2005, the specific minutia value for index F1 may be either of F1A, F1B, or possibly others, referred to as the anticipated minutia DB 98. All other computer minutia values remaining the same, a change at the F1 index from a value of F1A to F1B, for example, represents one permutation of computer minutia possible for a specific type of computer 18 (e.g., for computers running the Android operating system). It can be seen that if five different values were possible at index F1, then 5 permutations that change only F1 may be possible for each different combination of the remaining computer minutia. Although all 5 values of F1 may not be possible for every combination, the number of permutations is generally multiplicative so that an estimate of the number of possible permutations can be made by multiplying together the number of possible values at each index, for all the indexes H1 to H40, F1 to F70, S1 to S280, ?1 to ?2, and B1 to B5. For the example shown in Figure 2, it can be seen that even with only 2 or 3 values of possibility for each index, the number of permutations, or different possible combinations of minutia, for all types of computer 18 can easily be practically infinite. Thus, even for large numbers of computer 18 that appear otherwise identical, within the millions of different possible combinations of minutia DB 70 and the related practically infinite range of minutia values in the anticipated minutia DB 98, each single computer 18 can be uniquely identified by matching its unique computer minutia 64 and secrets and biometric minutia 26 collected by computer 18. As an example, when a service user 20 receives a newly manufactured mobile device (i.e. computer 18), typically part of the out-of-the-box initialization routine is to customize the computer 18 with service user 20 specific information such as, for example, contacts, email and network connections. The customizations these additions represent (i.e. minutia) can immediately differentiate two examples of computer 18 that were manufactured one immediately after the other. As the service user 20 uses their computer 18, the usage continues to affect and differentiate the minutiae that can be collected from the computer 18 (e.g., frequently called phone numbers). By maintaining a database of all industry updates related to the collective industry of instances of computer 18 – e.g., by collecting and cataloging all industry updates to hardware, firmware, and software minutia –dynamic key crypto provider 10, for example, may be able to know what all the possibilities are for the computer minutia 64 of a given computer 18 so that system 200 may be able to recognize a computer 18 in spite of changes not reflected or known by the current minutia DB 70. In fact system 200 may improve the accuracy and fault tolerance of its recognition of devices (i.e. computer 18, computer minutia 64, service user 20 and secrets and biometric minutia 26) by exploiting knowledge of changes (i.e. anticipated minutia DB 98) to the current device image (i.e. minutia DB 78).

When using combinations of computer minutia 64 for identifying a specific computer 18, system 200 may use intelligent minutia selection 114 to select a combination of minutia from the total set of minutia (i.e. computer minutia 64 and secrets and biometric minutia 26). In the specific method 2010 example illustrated in Figure 2, the combination of minutia chosen is one hardware minutia, Hx, one firmware minutia, Fy, and one software minutia Sz. Such a combination may be referred to as a "triplet". Although a triplet Hx-Fy-Sz may include one hardware, one firmware, and one software minutia as in the example illustrated in Figure 2, a triplet could also include, for example, two hardware minutiae and one software minutia, e.g., Hx-Hy-Sz. Also, for example, more or less than three minutiae could be used at a time, e.g., a "quadruplet" such as Hx-Fy-Sz-Bb. Any combination of minutia from the total set of minutia DB 70 may be used. Smaller subsets of minutia values constrain the scope of change within the minutia values so the results can be rapidly validated. Longer subsets of minutia values increase the potential change (and therefore security) and can be useful in infrequent, but high security crypto actions like digital signature.

The particular values for x, y, and z are not specified for this example so that Hx could be any one of the 40 hardware minutia H1-H40 shown in step 2003, e.g., IMEI number. Similarly, Fy could be any one of the 70 firmware minutia, and Sz could be any one of the 280 software minutia shown, for example, in step 2003. A hardware minutia of a particular computer 18 generally will not change without changing the entire computer 18 (and identity) itself, so whatever hardware minutia, Hx, is used, it may not be expected to change for the particular computer 18 being challenged, as indicated by "(no changes)" next to H1-H40 in step 2005, so that the number of possibilities for each individual Hx is limited to one. In the particular example illustrated in method 2030 of Figure 2, the firmware minutia, Fy, is assumed to have nine different acceptable values for illustration, and the software minutia, Sz, is assumed to have twenty different acceptable values for illustration. Method 2030 can vary the fault tolerance of the invention by varying the allowable range of acceptable minutia values with respect to the range of possible minutia values for each minutia value.

Although it may be the case that certain combinations of hardware, firmware, and software values may be incompatible (e.g., a particular software update might require a particular firmware update) the example of Figure 2 assumes that all updates are independent so that the total number of permutations of acceptable device characteristic values for the particular computer 18 being challenged is the product of the number of acceptable possibilities for each component, Hx, Fy, Sz, of the triplet Hx-Fy-Sz, or 1*9*20 = 180, as indicated at step 2007. The number of acceptable permutations for a selected combination of minutia, then, can be smaller than the number of possible permutations for the same triplet and significantly smaller than the total number of permutations for all minutiae, as shown by this example, e.g., 180 out of potentially millions of possible minutia values and 180 out of the potentially infinite number of permutations as indicated at step 2005.

Selection of the particular combination of minutia (e.g., Hx, Fy, Sz for the example of Figure 2) to be used for challenging a particular device may vary, not only from computer 18 to computer 18 and service provider 14 to service provider 14, but, for example, each time the same computer 18 is challenged on behalf of the same service provider 14. The intelligent minutia selection 114 may employ a number of considerations in selecting the combination of minutia to be used for a particular challenge of a particular computer 18 and service user 20. As shown step 2010, intelligent selection of the combination of minutia (e.g., Hx, Fy, Sz for the example) may be based on need for uniqueness, predictability and scope of possible changes. For example, selection of minutia may use expectations for changes to the current minutia DB 70 database based on knowledge of the current computer minutia 64, current secrets and biometric minutia 26 and knowledge of all minutia value updates that can occur (i.e. anticipated minutia DB). Knowledge of all minutia value updates that can occur, whether or not the updates actually have occurred, can be gained from the previously mentioned collecting and cataloging industry-wide of all computer minutia updates and the heuristically determined trends caused by the use of computer 18 by a particular service user 20 . Also, for example, if uniqueness and predictability are of concern, minutiae may be chosen for which the values are known and are not expected to change. If scope of possible changes is of concern, minutiae with a reduced capacity for change or a tighter tolerance of acceptable change may be selected. Combinations of minutiae can be selected to isolate a particular minutia by combining it with static minutiae. Likewise, a static minutia can be grouped with minutia that changes rapidly to form a set that changes in some manner to protect static minutia members. Minutia sets can be selected to address specific purposes such as geo-location or user secrets. Minutia sets can combine minutia from the various identity factors of something you have, something you know and something you are. Minutia values can be selected to periodically 'refresh' validations of specific minutiae.

The intelligent minutia selection 114 process can select minutiae from the different minutia sources of hardware, firmware, software, user secrets and user biometrics. The intelligent minutia selection 114 process chooses the minutia nearly randomly to widely and unpredictably sample various computer minutia 64 and secrets and biometric minutia 26 such that deducing a pattern for minutia sampling is difficult to infer. However, there may be certain minutia pairings and groupings that readily show and determine changes to computer minutia 64. In such cases, a 'selected' (versus 'random') subset of minutiae may be selected by the intelligent minutia selection 114 process.

After the intelligent minutia selection 114 process determines the minutiae to be used, the formulate challenge 116 process looks up the minutia index for that minutia from the SP info and IDs 32 database; this allows the minutia index for one service provider 14 to be different from another service provider 14. The indexes are then combined with a random number using an algorithm defined for each service provider (as described in Figure 3, specifically the SP info and IDs 32 database); again to provide differentiation and security between service provider 14 instances. The challenge result from the formulate challenge 116 process can then be processed at step 2020 and given to the send challenge and await response 118 process. Since the challenge contains nearly random information which serves as the actual challenge value, the transmission of the challenge need not be done via an encrypted tunnel but it can be sent securely by send challenge and await response 118 if desired.

As shown at step 2020, the formulate challenge 116 process can compute a cryptographic key based on the selected combination of minutia (e.g., Hx-Fy-Sz for the illustrated example). For example, each of x, y, and z may be a table index value (e.g., an integer) to the corresponding hardware (H), Firmware (F) and Software (S) information in a database of the particular service provider 14. The specific x, y and z table ordering and properties for a particular service provider 14 is found both in the dynamic key crypto library 56 created specifically for the service provider 14 and in a database of information specific to the service provider 14 maintained by the dynamic key crypto provider 10. The key may be computed as shown at step 2020, for example, by applying a mathematical or cryptographic function "Fn" to the combination of minutia values Hx+Fy+Sz. Thus, the cryptographic key may cryptographically encode information from the selected combination of minutia, e.g., triplet Hx-Fy-Sz. The same minutiae references, for example the x, y and z table indexes, can be computed by applying a mathematical or cryptographic function "Fn", which may be the same or a different function from that used earlier, to form a challenge value combining the indexes with other information such a random number, as used in the example. Thus, the challenge cryptographically encodes enough information for the computer 18 being challenged to determine which minutia should be used in computing its actual response. It is important to note, however, that even though the computer 18 may use the minutiae Hx-Fy-Sz and its own actual values for those minutiae in computing its response, no information as to what are the actual values of the minutiae is included in the challenge or response nor is directly gleanable from the response.

At step 2030, the dynamic key crypto provider 10 computes all responses that are acceptable for the computer 10 to make. The acceptable response computations can be based on the allowable range of possible changes to the defined subset of minutiae selected for the challenge. These computations can be performed beforehand (e.g., independently – whether prior, concurrently, or after – receiving the actual response from the computer 18) and stored in valid responses DB 130 for comparison to the actual response from computer 18. The challenge may be sent by dynamic key crypto provider 10 or by the service provider 14 to the particular computer 18 being challenged. The range of possible changes may be processed because of the constant and continuous collecting and cataloging of industry updates for the total set of minutia from which the particular combination of minutia (e.g., Hx, Fy, Sz for the example of Figure 2) to be used for challenging the particular device is selected. Because every allowable response to a challenge is therefore known (e.g., computed at step 2030) before the challenge is sent to the computer 18, the actual response that will be received from the computer 18 to the challenge may be among the range of pre-processed acceptable responses (and therefore among the acceptable changes) computed by the dynamic key crypto provider 10 that is challenging the computer 18. As illustrated at step 2030, in this particular example having no possible changes for hardware (e.g., one possible value), nine possible changes or values for firmware and twenty possible changes for software, there are 180 allowable responses for the computer 18 to return to the challenge. Each of the 180 allowable responses may be calculated by the dynamic key crypto provider 10 in a similar manner that the computer 18 will compute its actual response in response process 112, as illustrated in step 2040.

At step 2040, the particular computer 18 being challenged may receive the challenge and unpack the challenge to determine which minutia it should collect and use the values of to form its response to the challenge. Having unpacked the challenge using information and algorithms stored in the dynamic key crypto library 56, the response process 112 can use the computer 18 to fetch the values of the selected computer minutia 64 or collect the values of selected service and biometrics minutia 26 and build a key that may be identical to the key computed by the dynamic key crypto provider 10 at step 2020. The particular computer 18 being challenged may form a response to the challenge by applying a mathematical or cryptographic function "Fn", which should be the same as that used at step 2020 or step 2030, to the key + challenge as shown in Figure 2. The computer 18 being challenged may then communicate the response to return it directly to the dynamic key crypto provider 10 or indirectly via the service provider 14. Again, since the challenge and response exchange may contain a random number element, it can change every time, even if the same minutiae were selected. As such, it does not need to be securely transmitted between computer 18 and dynamic key crypto provider 10 over network 16, but it can be if desired. The dynamic key crypto provider 10 sends the computer 18 response to the validate response from computer 120 process for processing in step 2050.

As illustrated at step 2050, the validate response from computer 120 process can therefore be determined by simply comparing the actual response received from the computer 18 to the allowable responses that are pre-processed by the dynamic key crypto provider 10 to determine if there is a match. Decrypting or decoding of a response is not necessary so the validation can occur very quickly. On a match between the actual response and one of the pre-processed responses, the validate response from computer 120 process may then know what the particular actual minutia values from computer 18 are for the combination selected (e.g., triplet Hx-Fy-Sz) by knowing which possible response has matched the actual response even though neither response contains any direct or decipherable information about the actual minutia values. If a match is found, the subset of minutiae used in the challenge may be regarded as being known or authenticated. For example, as seen at step 2007, if the actual response matches the 172nd possible response "Resp172" or permutation, then the actual device values must match those of Hx, the first possibility for Fy (e.g., Fy0), and the twentieth possibility for Sz (e.g., Sz19) even though "Resp172" itself contains no direct information regarding the actual minutia values being challenged.

The validate response from computer 120 process can use logical groupings of minutia values to increase the confidence of a matched response. Groupings of related minutia may be gleaned, for example, from the anticipated minutia DB 98 or discovered heuristically. For example, if a set of minutiae is only changed via an industry update and all minutiae within the set change to unique values in unison with the particular update, then should a particular minutia value or values within the set of update related minutia not share the expected values of other minutiae with regard to a single update set, then the validate response from computer 120 could deduce the response related to the minutiae values within the update logical grouping may be in error or fraudulent. As an example, should a fraudulent entity alter the computer 18 to return falsified information when the minutia value is collected by the response process 112 via the operating system on computer 18, the actual minutia value would not be returned. In this manner, a fraudulent entity could make one computer 18 look like another computer 18 or make one service user 20 appear as another service user 20. The validate response from computer 120 can use logical groupings of minutiae and, for example, employ multiple methods for collecting what should be the same value (i.e. a smartphone's phone number can be learned through several methods) (1) Often, multiple methods exist for reading a particular value such as phone number. The various methods can be used and the returned minutia value compared for consistency. (2) Often groups of minutia values are related such that a change in one should create changes elsewhere (for example time and time zone.) In the validate response from computer 120 process, the minutia values related to one another can be verified to ensure changes are found to be consistent throughout the related 'group' of minutia values.

Even if an exact match is not found, the allowable ranges from the set of possible minutiae may be expanded or additional challenges using other, possibly related, minutiae may be sent to the device in an effort to validate the device. If necessary, changes in the computer minutia 64 of a computer 18 can be sent from the computer 18 to the dynamic key crypto provider 10 using the registration subsystem 400 described in Figure 4.

If the response is not an expected response, then a validation failure process as described in Figure 6B can alert the service provider 14 that the validation has failed.

At step 2060, on a match between the actual response and one of the pre-processed responses, the update computer minutia 128 process may then know what the particular actual minutia values from computer 18 are for the combination selected (e.g., triplet Hx-Fy-Sz) by knowing which possible response has matched the actual response even though neither response contains any direct or decipherable information about the actual minutia values. The values from the valid responses DB 130 used in the response calculation can then be used to update the values stored in the minutia DB 70 database.

Figure 3 illustrates a service provider application (app) delivery system 300 in accordance with an embodiment. Figure 3 shows a system for delivering a service provider app 44 to a computer 18 such that the service provider app 44 has included within it a dynamic key crypto library 56 which is unique to the service provider 14 and performs computer security functions on the computer 18.

The service provider app 44 may be similar to a typical industry application except that service provider app 44 makes application programmer interface (API) calls to a dynamic key crypto library 56 that was compiled as a library with the application source code 42 to form the final executable form of the service provider app 44. The service provider app 44 can be shared with the dynamic key crypto provider 10 for analysis to generate minutia values that can validate the integrity of service provider app 44 when service provider app 44 is running on a computer 18. Service provider app 44 may contain or wish to store data that the service provider 14 requires to secure and make private.

Within the dynamic key crypto provider 10 there may be a service provider registration 30 process for registering service provider systems 14 to use system 300. The service provider registration 30 process records and generates data specific to the service provider 14 and stores that data in the SP info and IDs 32 database. Such data can include preferences like PIN utilization (i.e. force a system PIN, use a service PIN, etc.) and minimum scores to allow connection. The SP info and IDs 32 database may be, for example, a list of customers and partners for whom a custom dynamic key crypto library 56 has been created. The SP info and IDs database 32 may include key material used to identify and encrypt data of the service provider 14 throughout the system 300 and a table for indexing minutia. Such SP info and IDs 32 database may uniquely identify the service provider 14 and ensure that features and elements of system 300 used by the service provider 14 are secure and separate from other service provider systems 14 that might use the system 300. This provides service separation of data and identifiers such that multiple, independent service provider systems 14 cannot collude, compare data and infer what might be considered private data or tendencies of a service user 20.

The SP info and IDs 32 data unique to a service provider 14 may be used in a custom library creation 34 process to make a dynamic key crypto library 56 which contains data elements of the SP info and IDs 32 database. In addition to data unique to the service provider 14, the custom library creation 34 process can create code custom to a particular service provider 14. Such custom code can include different encryption algorithms (e.g., AES, RSA, Elliptical curve), different hashing algorithms (e.g., secure hash algorithm (SHA-1), message digest (MDM)), unique system encryption keys, unique look up table routines and orderings, different hashing methods for combining minutia values into dynamic crypto keys (e.g., interleaved bit transformations, reverse-ordering, bit inverse, bit shifting), and minutia definitions and classes uniquely available to a particular service provider 14. All of the customizations when compiled form a dynamic key crypto library 56 unique to the service provider 14 such that a breach of a dynamic key crypto library 56 for one service provider 14 may not affect the dynamic key crypto library 56 of another service provider 14. In addition, even if the exact same minutia values are used to form a dynamic crypto key on the exact same computer 18, the resultant dynamic crypto key for one service provider 14 may be different than the resultant dynamic crypto key for another service provider 14; thus the responses for different instances of service provider 14 would be different even if the exact same challenge was sent.

Because of the different SP info and IDs 32 databases used in the formation of the dynamic key crypto libraries 56, two instances of service provider 14 (e.g., two different online service providers), for example, may be prevented from being able to compare information gleaned from the computer 18 and conclude their individual service provider apps 44 are residing on the same computer 18. This prohibits the profiling of a service user 20 based on multiple instances of service provider 14 connected to their computer 18.

Likewise, because of the unique computational possibilities introduced in the custom library creation 34 that formed the dynamic key crypto library 56, a successful attack against the privacy and security included within a particular dynamic key crypto library 56, may not be successful against a dynamic key crypto library 56 related to another service provider 14.

The dynamic key crypto library 56 is responsible for, among other activities:

1) reading computer minutia 64 found on the computer 18 and facilitating entry by service user 20 of secrets and biometric minutia 26 into computer 18 that can validate that an appropriate service user 20 is using an identified computer 18;

2) communicating computer minutia information across the network 16;

3) responding to dynamic key crypto provider 10 challenges to establish a computer's unique identity, protect data, and perform digital signatures using computer minutia 64 found on the computer 18 and secrets and biometric minutia 26 input by service user 20 into computer 18;

4) processing requests from the dynamic key crypto provider 10 to possibly hold, transfer, or a delete service provider app 44 and itself (dynamic key crypto library 56); and

5) randomizing or obfuscating dynamic key crypto library 56 activity through various mechanisms that make it difficult to intercept sensitive actions.

The dynamic key crypto library 56 created uniquely for the service provider 14 may be sent to the service provider 14 securely over a network 16 in the send custom library to service 38 process using any of several methods. The dynamic key crypto library 56 may include program logic designed to perform security functions both directed by and on behalf of the service provider app 44 by interacting with the computer 18. With newer forms of computer 18 (e.g., smartphones and tablets), a dynamic key crypto library 56 that functions as part of the service provider app 44 when it is running is a more reliable method then independently running applications to access the required services for computer 18. Furthermore, the larger combined code size of the dynamic key crypto library 56 and the service provider app 44 can impose a more tedious and difficult effort to isolate the security functions in an effort to defeat the security.

The service provider 14 may perform an industry typical build application 40 process by combining the dynamic key crypto library 56 with application source code 42 of the service provider 14 to create a service provider app 44. The service provider app 44 can be distributed any number of ways including directly over a network 16 and through a third party software distributor 22 either over the network 16 or directly to the service user 20 for loading on the computer 18 via the distribute application 46 process. The third party software distribution system 22 may be an optional system or systems for distributing software from the service provider 14 to computer 18. Apple's AppStore® is an example of such a software distribution system.

Figure 4 illustrates a system 400 for registration of computer and user minutiae in accordance with an embodiment. Figure 4 shows a system for registering a computer 18 with a dynamic key crypto provider 10 and a service provider 14 over a network 16.

The computer 18 may have on it a service provider app 44. When the service provider app 44 is installed, the dynamic key crypto library 56 within the service provider app 44 may run tests to proof the install 76. Proof the install 76 can be part of the dynamic key crypto library 56 and can use a shared secret supplied by service provider 14 through a user authentication 50 process. In this case the service user 20 might answer previously defined questions, recognize historical service usage, and recognize past instances of computer 18 used by service user 20 or other identity proofing methods.

Additionally, the proof the install 76 process can look for other instances of service provider app 44 from other service provider systems 14 and report any found instances back to the dynamic key crypto provider 10 for additional assurances on the history of the computer 18.

After the user authentication 50 is performed, the service provider 14 may send to the dynamic key crypto provider 10 an account identifier that the service provider 14 uses to identify the service user 20. The register computer 68 process binds the account identifier with the computer minutia database (DB) 70 to link the service user 20 to a particular computer 18.

The dynamic key crypto library 56 can sample a wide range of computer minutia 64 and secrets and biometric minutia 26 using the fetch key minutia 58 process including minutiae from the computer 18 (hardware, firmware, and software) and minutiae from the service user 20 (secrets and biometrics). Secrets and biometric minutia 26 may be collected from the service user 20 by the computer 18 or via other conveyance methods. Not all possible minutia values are required to be read at installation; some may be read at a later time.

A process to select minutia for service keys 60 uses some or all of the computer minutia 64 to create encryption and identifier keys that can be used by the dynamic key crypto library 56 and other parts of the systems 100, 200, 300, 400, 500, 600, 700, 800, and 900 for things like encrypted service data 196 stored locally on the computer 18. These selections may be predefined in a dynamic key crypto library 56 or stored in a service key minutia selections 66 database that is managed and secured by the dynamic key crypto library 56. The service key minutia selections 66 database may reside within a secure element on the computer 18 and can be used for offline processing. The minutia selected by the select minutia for service keys 60 process may be used by the dynamic key crypto library 56 to dynamically build the service keys required by the dynamic key crypto library 56; the keys that result from reading the computer minutia 64 are not stored within the dynamic key crypto library 56 or system 400; they may be computed as they are needed by consulting the service key minutia selections 66 database and using the fetch key minutia 58 process to obtain the resulting computer minutia 64 or secrets and biometric minutia 26. Thus if a service provider app 44 was copied from one computer 18 to another computer 18, when the service keys were built from computer minutia 64, the resulting service key would not be able, for example, to properly decrypt data stored locally on the computer 18.

Some of the computer minutia 64 and secrets and biometric minutia 26 are sent to the dynamic key crypto provider 10 via the transmit minutia to dynamic key crypto provider (DKCP) 62 process. A relatively small amount of computer minutia 64 and secrets and biometric minutia 26 can be sent to the dynamic key crypto provider 10 so the dynamic key crypto provider 10 can look for existing matches to the computer minutia 64 in its minutia DB 70 database. If the dynamic key crypto provider 10 finds matching minutia 64, then the dynamic key crypto provider 10 can send challenge, response, and validation exchanges described in Figure 2 to verify a wider set of computer minutia 64. If a wider sampling of computer minutia 64 are properly verified by the dynamic key crypto provider 10, then it can possibly deduce that this is another service provider app 44 being added to a computer 18. If the dynamic key crypto provider 10 does not finding matching computer minutia 64 in its minutia DB 70 database, then a subset of computer minutia 64 and secrets and biometric minutia 26 can use the process "transmit minutia to DKCP 62" such that the computer 18 can be properly and uniquely identified and the remainder of computer minutia 64 and secrets and biometric minutia 26 can be learned by the dynamic key crypto provider 10 using the update computer minutia 128 process described in Figure 2. In this manner, it may be possible to transfer some of the minutia via challenge, response, and validation as described in Figure 2, and not all of the minutia may need to be transferred via the transmit minutia to DKCP 62 process, which can use several secure transmission methods that may vary by service provider 14 through the customization of the dynamic key crypto library 56.

By performing a transmit minutia to DKCP 62 process, various values of computer minutia 64 and secrets and biometric minutia 26 may be sent along with their minutia descriptor to the dynamic key crypto provider 10 which may perform a register computer 68 process. The register computer 68 process may record the computer minutia 64 and secrets and biometric minutia 26 into a minutia DB 70 along with a reference to the service provider 14 account identifier for the service user 20. The minutia DB 70 can store the type (or category) of minutia, its value and the service identifier for later processing.

The dynamic key crypto provider 10 is able to store the computer minutia 64 and secrets and biometric minutia 26 which have been randomized by the unique dynamic key crypto library 56. The dynamic key crypto provider 10 is also able to decrypt service provider (SP) minutia 74 using SP info and IDs 32 data to learn the actual computer minutia

64. Many of these actual minutia values are known only by the dynamic key crypto provider 10 and may be used later for services to multiple service provider systems 14.

Some of the actual computer minutia 64 and secrets and biometric minutia 26 may be sent to the service provider 14 via a send computer profile to SP 72 process. To protect a service user 20 from being profiled by various instances of service provider 14 that might collude and interpolate minutia values, the descriptive names of the minutia values can be abstracted so their actual meaning is unknown (e.g., counter-1, counter-2, entertainment-1). In addition, where possible, the values of the minutia can be hashed to hide the actual minutia value. The service provider 14 can store computer info 52 into SP computer info DB 54 or store data in the service and user data 24 database (or both). The SP computer info DB 54 information can be useful to the service provider 14 for understanding the types and minutia of computer systems 18 running their service provider app 44 software. Such information might include OS type and version, computer make and model, for example. The service and user data 24 database might contain secrets such as PINs and passwords meaningful to the service provider 14.

Figure 5 illustrates a system 500 that may be used to catalogue and model industry minutia to create and update anticipated minutia databases in accordance with an embodiment. Figure 5 shows a system 500 for creating an industry update catalogue DB 96 from a wide range of industry sources and using that information to form an anticipated minutia DB 98.

The dynamic key crypto provider 10 routinely performs industry minutia cataloguing 86 processes for ultimately amassing an industry update catalogue DB 96. This database is for managing a vast but finite collection of industry minutia. Large scale searches, interpolation, multi-upgrade permutation modeling and probability calculations are performed against the data found in the industry update catalogue DB 96.

The industry minutia cataloguing 86 process uses computer industry research 90 to heuristically and empirically perform a minutia update collection 88 process. The minutia update collection 88 process scours a network 16 (for example, the Internet) seeking out information from software manufacturers 80, computer hardware manufacturers 82 and firmware manufacturers 84. Software manufacturers 80 may include, among other entities, software manufacturers, online software storefronts, support services for software, and some operating systems. Computer hardware manufacturers 82 may include, among other entities, manufacturers of PCs, laptops, tablets, smart phones, purpose-built computers, and other hardware often capable of connecting to a network 16. Firmware manufacturers 84 may include, among other entities, software related to hardware (commonly called drivers), some operating system software, software for configuring and controlling access to a network 16 such as a mobile operator network, or public and private cloud networks.

The minutia update collection 88 process collects such information as the computer industry research 90 process may deem beneficial to system 500. The collected data is then given to a data modeling, heuristics and permutations 92 process for analysis with regard, for example, to computer or user device identification. The data modeling, heuristics and permutations 92 process considers historical minutia trends and data mining 94 as well as the current minutia DB 70, the current anticipated minutia DB 98 and the event log 12 which may log actions and exchanges performed by the dynamic key crypto provider 10 for auditing and heuristic analysis at later times. The industry updates themselves can be grouped and related such that one minutia update in the industry update catalogue DB 96 can trigger expected changes in other related minutia values. For example, if an operating system industry update is shown to change fifteen minutia values and the minutia values are not affected by service user 20 usage (including, e.g., build number, build name, subsystem versions, system sizes), then these minutia values can be grouped and inferred or validated collectively in the data modeling, heuristics and permutations 92 process.

Other related minutia values may change as a result of service user 20 usages. This is related but different to service user 20 behavior patterns; minutia values in minutia DB 70 (such as minutia values related to the computer 18) establish the behavior of the minutiae (such as computer 18) and, therefore, behavioral algorithms can be applied to the minutia DB 70 values. For example, if the computer 18 repeatedly connects to a secured wireless LAN (such as one provided by an employer) when the computer 18 is in its ‘work’ environment during business hours, this could imply a third-party trust of the computer 18 (via, e.g., MAC address validation, WEP key authentication) by the secured wireless LAN; failure to connect under ‘normal’ working conditions could signal a change such as a lost device or new job. As another example, if values in the minutia DB 70 show that an address book has consistently added addresses over a time period reaching hundreds of names and suddenly the address name count goes to eighty, that could signal ownership by a new service user 20.

From data collected and modeled, the data modeling, heuristics and permutations 92 process records possible minutia values in the anticipated minutia DB 98. The data stored in the anticipated minutia DB 98 is pre-calculated combinations of industry update catalogue DB 96 and minutia DB 70 which are managed and ordered according to probability within the database so that rapid derivative comparisons can be verified and scored against a confidence scale.

For example, when computer industry research 90 discovers a pending operating system release, the minutia update collection 88 process can gather a copy of the newly released operating system from, again for example, the appropriate firmware manufacturers 84. The new operating system is processed by the data modeling, heuristics and permutations 92 function and the resultant minutia stored in the anticipated minutia DB 98 for later use by system 500.

As another example of anticipated minutia, for minutia that represents system counters, the counter information collected from the minutia DB 70 can be increased an allowable range as determined by the data modeling, heuristics and permutations 92 process. All counter values within the allowable range would then be stored in the anticipated minutia DB 98.

In most cases, the data modeling, heuristics and permutations 92 process and the historical minutia trends and data mining 94 process calculate a probability and confidence scoring related to the values stored in the anticipated minutia DB 98. These probability and confidence scoring values are a determinative factor in the confidence scoring system for computer authentication.

Figure 6 illustrates a system 600 for scoring, confidence rating and step-up processing in accordance with an embodiment. Figure 6 shows a system 600 for computing a minutia validation scoring 140, comparing the scoring against a threshold defined by the service provider 14 and taking additional actions to process SP step-up request 150 in an effort to increase the scoring over the desired threshold.

The dynamic key crypto provider 10 contains a subsystem for the minutia validation scoring 140. The minutia validation scoring 140 subsystem receives a response validated using the subsystem 200 defined in Figure 2. The compute score 144 process computes a heuristic and probabilistic scoring of the minutia and minutia values used in the validated response using data from the valid responses DB 130, the SP info and IDs 32 data, the event log 12 and the anticipated minutia DB 98. Information in the valid responses 130 database includes both information representative of the current state of computer minutia on the computer 18 and anticipated minutia from industry sources and service user 20 norms, both of which are described in previous figures and in Figure 9 with regard to the service provider app 44 subsystem 900.

For example, the scoring for hardware minutiae might be typically higher than the scoring for software minutiae. Firmware minutia values that change as expected may also have a higher confidence scoring. Likewise, software minutiae (such as date) that change as expected may positively affect the overall scoring of the response.

Some minutiae value changes, while possibly anticipated, may negatively affect the overall scoring of the response. For example, if a counter value takes an unusually large jump, it will negatively affect scoring. Also, if firmware minutiae values do not reflect routine updating as per industry norms, the scoring may be negatively affected. In addition, if a computer reset is detected that resets a wide range of minutia back to a known factory default, the resulting score may be lower.

Some minutiae themselves score differently. For example, certain software minutiae may be more predictable and useful than others. So, when a more favored minutia or minutiae are used, the resultant scoring may be higher when compared to validation done with less desirable minutiae.

Because of the vast number of minutiae to be validated, another scoring input can be the time since a particular minutia value was last validated in a challenge and response exchange with the computer 18.

Information outside the scope of a single computer 18 may also impact the scoring. If several instances of a computer 18 are registered to a single service user 20 within a particular service provider 14 as shown in the minutia DB 70, the high number of registered computer 18 may negatively impact the scoring, especially if several computer 18 computers are considered to be equivalent (for example, three smart phones instead of one smart phone, one tablet and one laptop).

After compute score 144 is performed, the resulting score is compared against the initial threshold defined by the service provider 14 and typically sent up during the initial connection to the service provider 14. If the computed score >= threshold 142 then the send score to SP 148 process is used to return the score to the service provider 14 for further consideration.

If the score >= threshold 142 is not true, then the process SP step-up request 150 is performed. Note the similar process SP step-up request 150 process can be performed if the initial threshold or subsequent thresholds are not met, as defined by the service provider 14.

The process SP step-up request 150 performs a compare valid responses and threshold 152 to determine if a possible response and corresponding score are equal to or above the threshold using information from the valid responses 130 database. The process may be governed by a user impact heuristics 154 process which determines the best response and step-up manner in which to increase the score.

If any score >= threshold 156 is true, then specific minutiae as defined in the use selected minutia elements 168 may be used to formulate challenge 116 and system 600 will continue using the system 200 shown in Figure 2. In this manner, the service users 20 may not be inconvenienced by having to take an action.

If current score + 2nd >= threshold 158 is true, then the use three identity factors 170 process may request the dynamic key crypto provider 10 to direct the dynamic key crypto library 56 to collect service user 20 secrets or biometric minutia using computer 18.

If new score + 2nd >= threshold 160 then both the new, selected minutia challenge and the use three identity factors 170 processes may be triggered.

If there is no way for a new, selected minutia challenge to achieve a score equal to or higher than the threshold requested by service provider 14, then the send validation failure to SP 162 process is performed.

When the service provider 14 receives a scoring from the Minutia validation scoring 140 from the dynamic key crypto provider 10, it first determines if a step failure 172 occurred. If this is the case, the dynamic key crypto provider 10 is unable to match the threshold desired by the service provider 14. The service provider 14 must then determine how to respond in the validation failure process 180 which, for example, can include denying the service request or conducting an out-of-band identity proofing of the service user 20 that might trigger a new computer 18 registration as shown in Figure 4.

If the score from the dynamic key crypto provider 10 is not a step-up failure as determined in step failure 172, then the SP risk process 174 compares the score against its own risk tables for the service action requested by the service user 20. If the score >= threshold 142 then the allow user action 182 may be performed; the confidence in the computer 18 and optional service user 20 may be sufficient for the service provider 14 to allow the requested action.

If the score >= threshold 142 fails, then the request step-up authentication from dynamic key crypto 178 process requests the dynamic key crypto provider 10 to perform a process SP step-up request 150 in an effort to get a scoring above the desired threshold.

Figure 7 illustrates an authentication system 700 in accordance with an embodiment. Figure 7 shows a system 700 for dynamic key cryptography authentication possibly using minutiae from the three identity factors (have, know and are) found on computer 18 or collected from a service user 20.

When a PIN or password entry is required, for example, as a second identity factor to computer 18 identification, the dynamic key crypto provider 10 may perform a use service PIN 250 decision to determine whether a service PIN native to the computer 18 is used or a PIN specific to the service provider 14 is used according to data stored in the SP info and IDs 32 database. The service provider 14 can mandate the use of a service PIN or mandate or allow that the native computer 18 PIN (or password) be used.

The dynamic key crypto provider 10 can request a service user 10 PIN entry by the challenge process described in Figure 2. In such case, the unpack challenge 108 process can enable the fetch key minutia 58 process to determine a PIN minutia request in the challenge and query use service PIN 250 to determine true or false.

The dynamic key crypto provider 10 can request either the computer 18 (if such functionality exists) to display system PIN 256 or the dynamic key crypto library 56 running on the computer 18 to perform the display service PIN 254 entry processes.

If the service provider 14 allows a PIN native to the computer 18 and the computer 18 is capable of a process to display system PIN 256, then a computer 18 process similar to (or possibly the same as) the display system PIN 256 process is called by the computer 18.

If a use service PIN 250 is yes or a computer 18 is not capable of being remotely directed to display system PIN 256, then the dynamic key crypto library 56 performs the display service PIN 254 entry process.

If use service PIN 250 is not required, then the dynamic key crypto library 56 determines if system PIN in use 252 is yes. If system PIN in use 252 is yes, then the computer 18 native PIN (or password) screen is displayed via the display system PIN 256 process as if, for example, the computer 18 'timed out' and the service user 20 was prompted to re-enter their PIN.

If use service PIN 250 is yes or a system PIN in use 252 is no, then the dynamic key crypto library 56 performs the display service PIN 254 process and a custom PIN entry screen is shown. The valid PIN can be a pre-determined number between the service provider 14 and the service user 20 or can be set during the computer system registration system in Figure 4 as part of the proof the install 76 process or some other registration process.

Regardless of the PIN screen displayed, the service user 20 enters a PIN into the computer 18 using the secrets and biometric minutia 26 information the service user 20 possesses. When the system PIN in use 252 is true the validation of the PIN is performed by the computer 18 itself. When a correct PIN is entered, the dynamic key crypto library 56 can perform a get time since last successful PIN event 260 process and return the new time since a valid last PIN entry to the dynamic key crypto provider 10. In this manner, a service user 20 may not have to enter multiple PINs or the same PIN multiple times to show they are in possession of the device; the system PIN acts a universal PIN for all protected service provider apps 44 running on the computer 18. When use service PIN 250 is true, the dynamic key crypto library 56 uses the PIN value entered by the service user 20 into the computer 18 to calculate actual response 106 which is then returned to the dynamic key crypto provider 10 for validation as described in Figure 2.

If a valid PIN entry is not performed, the dynamic key crypto library 56 may time-out and return the failure to the dynamic key crypto provider 10.

In another example, the fetch key minutia 58 process may result in a process biometric request 262. In such case, the get biometric minutia 264 process will interact with the computer 18 to collect the secret and biometric minutia 26 data from service user 20 via entry into computer 18. The biometric minutia values can then be used to calculate actual response 106 which is then returned to the dynamic key crypto provider for validation as described in Figure 2.

In still another example, the fetch key minutia 58 process may determine a digital signature 258 is requested and perform a digital signature via a substitute message hash for random number 242 process. In this manner, the hash or digest of an action (such as a transaction receipt or other summary) can be signed by the minutia returned by the fetch key minutia 58 process using the calculate actual response 106 process. The fetch key minutia 58 process may fetch any number of minutia values covering any or all of the three factors of identity (“have”, “know”, and “are”, e.g., respectively, the computer 18, the secrets service user 20 knows or represents or biometric minutia (from secrets and biometric minutia 26)).

As an illustrative example, to form a digital signature, the contents of a message can be hashed so that changes to the message contents form a different hash and any changes to the message become evident. The hash can then be ‘signed’ (encrypted) using a dynamic crypto key that contains minutiae that represent the computer 18 on which the signature occurred including relatively stable minutia (e.g., hardware minutia), geo-location minutia, and fast changing minutia (e.g., date, counters) that establish the computer 18 on which the signature was performed, where the signature was performed and multiple minutia values that collectively could validate when the signature occurred. In addition, the minutia used to form the signing dynamic crypto key could include secrets (e.g., PIN) that only a service user 20 should know and biometric minutia (e.g., facial geometry) that only a service user 20 could produce to establish who digitally signed the digest. In this manner, the dynamic crypto key can bind the instrument, place, time and person to a particular message. Thus, a very wide range of minutia can be used in the dynamic signature key (not a single triplet, but potentially dozens or even hundreds of minutia values). Furthermore, the behavioral trajectory of the computer 18 could be considered before and after the signature to lend credibility to the digital signature performed.

Figure 8 illustrates a system 800 for application processing for data protection security functions in accordance with an embodiment. Figure 8 shows a system 800 for processing interaction between the service provider app 44 and the dynamic key crypto library 56 to improve the security of both while running on a computer 18.

On the computer 18, the service provider app 44 may have been installed which contains a dynamic key crypto library 56 which may be unique to the service provider 14. The dynamic key crypto library 56 can process responses from the dynamic key crypto provider 10 to establish a heartbeat and chatter 194, possibly triggering a delete service from computer 236 self-destruction when there is no heartbeat 210 and randomize or obfuscating dynamic key crypto library 56 activity through heartbeat and chatter 194 system calls to make it difficult to intercept sensitive actions.

The dynamic key crypto library 56 performs some of its activities in direct response to either calls by the service provider app 44 or the dynamic key crypto provider 10. For the randomization, obfuscation and sampling of the computer minutia 64, the dynamic key crypto library 56 can perform tasks while the service provider app 44 is idle, waiting for response from either the service user 20 or other external drivers; often this is referred to as waiting in the event loop.

The service provider app 44 can encrypt and decrypt data 190 to securely and privately store service provider 14 and service user 20 data on the computer 18 in encrypted service data 196. The encrypt and decrypt data 190 process can use the service key minutia selections 66 database to determine which minutia the fetch key minutia 58 process should fetch from the computer minutia 64 found on the computer 18 or the fetch key minutia 58 can receive instructions from the dynamic key crypto provider 10.

In this manner, the encrypt and decrypt data 190 process may not actually store the keys used in encrypting and decrypting data; the keys are computed as required from the computer minutia 64. Thus, when the encrypted service provider 14 data and service user 20 data is stored in the encrypted service data 196 database, it cannot be decrypted unless the same computer minutia 64 are present on the computer 18. Copying the service provider app 44 or encrypted service data 196 (or both) will not enable the decryption of the encrypted service data 196.

Encrypted data to be processed by encrypt and decrypt data 190 can be transmitted securely from the service provider 14 over a network 16 to the computer 18, input into computer 18 by service user 20 or generated locally on the computer 18 by the service provider app 44 or dynamic key crypto library 56. In the case where the encrypted service data 196 is added or changed by the service provider app 44 or dynamic key crypto library

56, the service provider 14 can be updated with the encrypted service data 196 over a secure communication between the computer 18 and the service provider 14 using the network 16. The encrypt and decrypt data 190 process is intended to function on data at rest on the computer 18, not data typically in transit over a network 16. However, the same key creation processes based on computer minutia 64 found on the computer 18 can be used for many types of data protection.

The dynamic key crypto library 56 can also enable a local computer check 192 which uses the encrypt and decrypt data 190 to randomly validate computer minutia 64. In this manner, random data can be encrypted and, at a later time, decrypted to verify the computer minutia 64 are still valid, and thus the service provider app 44 is running on the intended computer 18. Similar verifications can be made by the dynamic key crypto provider 10 using challenge, response, and validation system 200 described in Figure 2.

Since the computer minutia 64 may contain minutia that change with normal use and time, the encrypt and decrypt data 190 may fail after those changes. For fault tolerance of the system, the encrypt and decrypt data 190 can process the data using multiple subsets from the large range of possible computer minutia 64. In this manner, the encrypt and decrypt data 190 can compute several different copies of encrypted data based off a very wide range of computer minutia 64. The number of different instances of encryptions based off a single plain text source can be controlled by the dynamic key crypto library 56 which is customizable for each service provider 14.

When encrypting plain text data, the encrypt and decrypt data 190 process uses the fetch key minutia 58 process the required number of times as controlled by the dynamic key crypto library 56. Each time a fetch key minutia 58 is performed, the corresponding minutia indexes are read from the service key minutia selections 66 and the resultant computer minutia 64 is read. The service key minutia selections 66 can be, for example, stored locally on computer 18, stored in a secure element on computer 18, or stored in the dynamic key crypto provider 10 data and be directed using the challenge, response, and validation system 200 described in Figure 2. Each return of fetch key minutia 58 contains a set of minutia values hashed and used by the encrypt and decrypt data 190 process to encrypt the plain text data and stores the encrypted result in the encrypted service data 196. Thus, multiple encryptions of the same plain text may be stored in encrypted service data 196 database.

When attempting to decrypt data in encrypt and decrypt data 190 process, the fetch key minutia 58 process follows the same logic in determining the service key minutia selections 66 and then fetching the related minutia from the computer minutia 64. When the fetch key minutia 58 returns the minutia values to the encrypt and decrypt data 190, the encrypt and decrypt data 190 retrieves the encrypted values from the encrypted service data 196 and uses a hash of the minutia values to decrypt the information.

If the decryption performed by the encrypt and decrypt data 190 does not properly decrypt the plain text – determined by some means of checksum, know plain text tests or other means in the valid decryption 202 determination – then the number of retries exhausted 206 is compared. If more encrypted instances of the plain text exist, then the next set of fetch key minutia 58 is performed which uses the service key minutia selections 66 to index another subset of minutia values which are then retrieved from the computer minutia 64 information.

This loop of fetch key minutia 58, valid decryption 202 and retries exhausted 206 is performed until a valid decryption of the data occurs or no more retries remain. If retries exhausted 206 returns true before a valid decryption of the data occurs, then the system faults and triggers a re-registration of the computer 18 as shown in Figure 4 or the original minutia values used when the encryption was done can be returned by the dynamic key crypto provider 10 to the dynamic key crypto library 56.

If a valid decryption 202 was found, then the encrypt and decrypt data 190 can perform a synch minutia with DKCP 201 on any minutia that failed to properly decrypt the plain text. When a synch minutia with DKCP 201 is performed, the changed minutia selections are indexed from the service key minutia selections 66, the changed minutia is read from the computer minutia 64 and given to the dynamic key crypto library 56 for secure transmission over the network 16 to the dynamic key crypto provider 10 which stores the updated minutia values in the minutia DB 70.

The synch minutia with DKCP 201 process can also perform an update library storage 208 function which calls on the encrypt and decrypt data 190 process to recalculate the failed decryptions using the new minutia found in the computer minutia 64.

When the dynamic key crypto library 56 connects to the dynamic key crypto provider 10 to update computer minutia of the computer 18, the dynamic key crypto provider 10 performs an authentication just as if the computer 18 was connecting to a service provider 14.

The dynamic key crypto library 56 can also have a heartbeat and chatter 194 process that, for example, may: 1) perform random activity on the computer 18; 2) function as a heartbeat between the dynamic key crypto library 56 and the dynamic key crypto provider 10; and 3) obscure and obfuscate meaningful actions.

The heartbeat and chatter 194 process can periodically perform a response process 112 using a challenge sent by the dynamic key crypto provider 10. Recall that the dynamic key crypto provider 10 can send a number of challenges to the dynamic key crypto library 56 for later processing. In this manner (described in Figure 2) minutia values can be inferred and updated between the computer 18 and the dynamic key crypto provider 10.

This or a similar process can also serve as a heartbeat between the computer 18 and the dynamic key crypto provider 10. If the heartbeat and chatter 194 process does not perform a valid challenge and response cycle within a timeframe defined by service provider 14 and stored within their customized version of the dynamic key crypto library 56, as shown in the no heartbeat 210 decision, then the heartbeat and chatter 194 process can call the delete service from computer 236 process described in Figure 8.

The heartbeat and chatter 194 process may also periodically fetch random minutia 204 reads of the computer minutia 64 to utilize a wide search space for any malicious parties listening to systems calls made on the computer 18. The heartbeat and chatter 194 may also randomly call the local computer check 192 process.

The heartbeat and chatter 194 may perform all of these functions to improve security and obfuscate critical actions. The heartbeat and chatter 194 may be most often called during the event loop of a service provider app 44 so as not to impact performance. The heartbeat and chatter 194 process may also be intelligent so as not to overly use battery power, network bandwidth, or other system resources.

Figure 9 illustrates computer identity provider lifecycle functionality and services to service providers in accordance with an embodiment. Figure 9 shows a system 900 for managing the lifecycle of a service provider 14 and a computer 18 including deleting and transferring services from one computer 18 to a new computer 220 and notifying service provider systems 14 of a new computer 220.

The transfer service 226 process can be triggered by several events such as: 1) a new computer 220 being detected as a possible replacement to the computer 18; 2) a service user 20 requesting a service transfer to the service provider 14; 3) a reaction to either trigger 1 or trigger 2, causing other service providers 230 to proactively transfer their service provider app 44.

When a new computer 220 performs the registration system 400 shown in Figure 4, if the dynamic key crypto provider 10 discovers that the account identifier supplied by the service provider 14 is already in use by a similar computer 18 (for example, a second smart phone) then a transfer service 238 message can be added as part of the registration process. If required, the service user 20 agrees to transfer service from their old computer 18, then the dynamic key crypto provider 10 can perform the transfer service 226 process.

When the service user 20 notifies the service provider 14 that their computer 18 is no longer valid due to loss, theft, replacement, or some other event, then the service provider 14 can request the dynamic key crypto provider 10 to perform a hold, delete, transfer service 232.

When a transfer service 226 process is performed, the dynamic key crypto provider 10 can perform a notify other service providers 228 process that notifies the other service providers 230 who have an account identifier registered to that particular computer 18. Upon notification, the dynamic key crypto provider 10 can share a SP confidence scoring 240 based off information in the SP info and IDs 32 database on the initiating service provider 14 to gauge the validity of the action. The other service providers 230 can, at their discretion, direct the dynamic key crypto provider 10 to perform a hold service 222, a transfer service 226, a delete service 224, or even take no action.

The notify other service providers 228 process stores only the minimal amount of service provider 14 information – such as pointer to the service provider 14 and an account identifier for the service user 20 – to link a computer 18 to a service provider 14; personal identifiable information of the service user 20 may not be stored or logged by the dynamic key crypto provider 10.

For a hold service 222, the dynamic key crypto provider 10 can update the minutia DB 70 such that it may send a send validation failure to SP 162 for the held computer 18 which will cause a validation failure process 180 to occur and, ultimately, may prompt contact of the service user 20 by the service provider 14 customer care effort.

For a delete service 224, the dynamic key crypto provider 10 can instruct the dynamic key crypto library 56 running on the target computer 18 to completely erase the encrypted service data 196 and the service key minutia selections 66 if present, sending a confirmation erase send receipt and encrypted data 234 when the data stores are erased. After the send receipt and encrypted data 234 is sent, the dynamic key crypto library 56 can self-destruct by deleting the service provider app 44 if desired.

For a transfer service 226, the delete service 224 is called to affect the old computer 18. The service provider app delivery system 300 shown in Figure 3 is then performed. Afterward, the computer system registration system 400 in Figure 4 may then be performed to completely transfer the service from the old computer 18 to the new computer 220. The reloading of service and user data 24 may also be performed as described in Figure 8 with the data being encrypted to computer minutia 64 found on the new computer 220.

Both the delete service 224 and the transfer service 226 cause the minutia DB 70 to reflect the decommissioning of the old computer 18. The old computer 18 minutia data is not deleted from the minutia DB 70 so it can be recognized for other service providers 230 or if the computer 18 performs a new registration either maliciously or through other events such as giving or selling the computer 18 to another service user 20.

Various alternative embodiments are possible. For example, in one alternative embodiment, the dynamic key crypto provider 10 may be a multi-tier distribution model that supports tiered ecosystems of service provider systems 14. In this manner, the dynamic key crypto provider 10 presiding over an eco-system can resolve the minutia within the minutia DB 70 to determine that separate instances of a service provider 14 are referencing the same computer 18. This allows the dynamic key crypto provider 10 to perform the computer identity provider lifecycle functionality shown in Figure 9 on their own ecosystem. Only the top tier dynamic key crypto provider 10 can resolve the absolute minutia value from a computer 18. Certain data will need to be exported from the sub-tier dynamic key crypto provider 10 to the master dynamic key crypto provider 10 to facilitate the lifecycle functionality shown in Figure 9.

In various embodiments, parts of the dynamic key crypto provider 10 can be designed to run onsite for a particular service provider 14 to allow data ownership. Certain data will need to be exported from the onsite dynamic key crypto provider 10 to the master dynamic key crypto provider 10 to facilitate the lifecycle functionality shown in Figure 9.

Also, for example, the dynamic key crypto library 56 does not need to be included in a service provider app 44 in all cases. Some instances of a service provider 14 may not require additional application code at the computer 18 or may use a web browser as their service portal. In this case, the dynamic key crypto library 56 will still exist on the computer 18 but may be a stand-alone, callable routine or a shared resource for the computer 18. If the dynamic key crypto library 56 is a shared resource, certain application processing functions as shown in Figure 8 may be compartmentalized within the dynamic key crypto library 56 to achieve the same, for example, service provider 14 and encrypted service data 196 separation.

In another example, the service provider 14 may also have the ability to make system calls directly to the dynamic key crypto library 56 rather than through an interface of the service provider app 44.

In another example, service provider app 44 may not communicate directly with dynamic key crypto library 56, but communication performed via exchanges between service provider 14 and dynamic key crypto provider 10 who independently communicate with service provider app 44 and dynamic key crypto library 56, respectively.

In another example, challenges could be stored on the computer 18 to facilitate faster launch of the service provider app 44 and offline processing.

In another example, anomalies in computer 18 minutiae might also be used to detect computer malware or other abnormal processing considerations.

In another example, the challenge, response and validation described in system 200 could be originate from the computer 18 and be useful for service provider 14 authentication and protected data exchange; this enables mutual authentication and benefits for the system.

In another example, the dynamic key crypto system can facilitate digital rights management for content where the content can only be decrypted on a specific computer 18 by using computer minutiae 64 specifically from computer 18 and content can be only decrypted for viewing by a specific user when they enter secrets and biometric minutia 26.

In another example, the anticipated minutia DB 98 can be expanded to model biometric minutia from secrets and biometric minutia 26 to address maturity and aging of service user 20 for biometric minutiae such as, for example, voice and facial recognition.

In another example, some forms of a computer 18 that can connect to a network 16 may not be designed for service user 20 interaction, for example machine-to-machine systems. Embodiments may still be extremely useful in this case – for what else is there to identify than the computer 18 – but the secrets and biometric minutia functionality may not apply.

In various embodiments, the encrypt and decrypt data 190 process generally functions on service and user data 198 stored on the computer 18 locally in the encrypted service data 196 database. In another alternative embodiment, however, the same encryption key processing could be used to secure service and user data 198 as it is transferred over a network 16. In a similar manner, the minutia DB 70 maintained by the dynamic key crypto provider 10 may be used to decrypt the service and user data 198 when received from the computer 18.

Implementations of various embodiments may include computers connecting to the Internet or other networks and computers connecting to a network including but not limited to traditional PCs non-traditional PCs (i.e. smart phones, smart tablets); purpose-built network computers (i.e. smart meters, network equipment, appliances); and computers without a user interface (i.e. machine-to-machine functionality). Various embodiments may include identifying computers which connect to a network; identifying computers which connect to each other with or without concurrent connection to a wide-area network; authenticating computer connections to an online service; authenticating users to an online service; and encrypting information stored on a computer

In implementation of the various embodiments, embodiments of the invention may comprise a personal computing device, such as a personal computer, laptop, PDA, cellular phone or other personal computing or communication devices. The payment provider system may comprise a network computing computer, such as a server or a plurality of servers, computers, or processors, combined to define a computer system or network to provide the payment services provided by a payment provider system.

In this regard, a computer system may include a bus or other communication mechanism for communicating information, which interconnects subsystems and components, such as processing component (e.g., processor, micro-controller, digital signal processor (DSP), etc.), system memory component (e.g., RAM), static storage component (e.g., ROM), disk drive component (e.g., magnetic or optical), network interface component (e.g., modem or Ethernet card), display component (e.g., CRT or LCD), input component (e.g., keyboard or keypad), and/or cursor control component (e.g., mouse or trackball). In one embodiment, disk drive component may comprise a database having one or more disk drive components.

The computer system may perform specific operations by processor and executing one or more sequences of one or more instructions contained in a system memory component. Such instructions may be read into the system memory component from another computer readable medium, such as static storage component or disk drive component. In other embodiments, hard-wired circuitry may be used in place of or in combination with software instructions to implement the embodiments.

Logic may be encoded in a computer readable and executable medium, which may refer to any medium that participates in providing instructions to the processor for execution. Such a medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media. In one embodiment, the computer readable medium is non-transitory. In various implementations, non-volatile media includes optical or magnetic disks, such as disk drive component, volatile media includes dynamic memory, such as system memory component, and transmission media includes coaxial cables, copper wire, and fiber optics, including wires that comprise bus. In one example, transmission media may take the form of acoustic or light waves, such as those generated during radio wave and infrared data communications.

Some common forms of computer readable and executable media include, for example, floppy disk, flexible disk, hard disk, magnetic tape, any other magnetic medium, CD-ROM, any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, RAM, ROM, E2PROM, FLASH-EPROM, any other memory chip or cartridge, carrier wave, or any other medium from which a computer is adapted.

In various embodiments, execution of instruction sequences for practicing the invention may be performed by a computer system. In various other embodiments, a plurality of computer systems coupled by communication link (e.g., LAN, WLAN, PTSN, or various other wired or wireless networks) may perform instruction sequences to practice the invention in coordination with one another.

Computer system may transmit and receive messages, data, information and instructions, including one or more programs (i.e., application code) through communication link and communication interface. Received program code may be executed by processor as received and/or stored in disk drive component or some other non-volatile storage component for execution.

Where applicable, various embodiments provided by the present disclosure may be implemented using hardware, software, or combinations of hardware and software. Also, where applicable, the various hardware components and/or software components set forth herein may be combined into composite components comprising software, hardware, and/or both without departing from the spirit of the present disclosure. Where applicable, the various hardware components and/or software components set forth herein may be separated into sub-components comprising software, hardware, or both without departing from the scope of the present disclosure. In addition, where applicable, it is contemplated that software components may be implemented as hardware components and vice-versa – for example, a virtual implementation or a logical hardware implementation.

Software, in accordance with the present disclosure, such as program code and/or data, may be stored on one or more computer readable and executable mediums. It is also contemplated that software identified herein may be implemented using one or more general purpose or specific purpose computers and/or computer systems, networked and/or otherwise. Where applicable, the ordering of various steps described herein may be changed, combined into composite steps, and/or separated into sub-steps to provide features described herein.

The foregoing disclosure is not intended to limit the present invention to the precise forms or particular fields of use disclosed. It is contemplated that various alternate embodiments or modifications to the present invention, whether explicitly described or implied herein, are possible in light of the disclosure. Having thus described various example embodiments of the disclosure, persons of ordinary skill in the art will recognize that changes may be made in form and detail without departing from the scope of the invention. Thus, the invention is limited only by the claims.

CLAIMS

What is claimed is:

1. A method of recognition of a device, the method comprising:

selecting, from a plurality of minutia sources of dynamically changing minutia, the sources comprising one or more of hardware sources of the device, firmware sources of the device, software sources of the device, geo-location data from the device, calling app data from the device, user secrets input to the device, or biometric information collected by the device, a combination of the minutia sources from which a corresponding combination of actual minutia values reflecting user-specific personalization associated with the device are collected from the device;

sending a challenge to the device, wherein the challenge includes information about the combination of the minutia sources such that the information enables the device to collect the corresponding combination of actual minutia values reflecting user-specific personalization associated with the device and from which the device can compute an actual response to the challenge based on the collected actual minutia values;

pre-processing a set of responses to the challenge such that:

the set of pre-processed responses covers a range of all actual responses possible to be received from the device when the corresponding combination of actual minutia values reflecting user-specific personalization associated with the device is valid for the device;

the set of pre-processed responses are processed based on information from known updates of the plurality of minutia sources of dynamically changing minutia such that the set of pre-processed responses anticipates changes on the device to the collected actual minutia values from which the device computes the actual response to the challenge; and

the set of pre-processed responses differentiates the device from other devices based on user personalization of the device due to the actual response depending on the collected actual minutia values reflecting user-specific personalization associated with the device;

comparing the actual response from the device to the set of pre-processed responses; and

recognizing the device based on a match of the actual response to one of the set of pre-processed responses for the device.

2. The method of claim 1, wherein recognizing the device further comprises identifying the device.

3. The method of claim 1, wherein recognizing the device further comprises authenticating a user.

4. The method of claim 1, wherein the selecting further comprises:

varying the selection of the combination of sources among the one or more of the hardware sources of the device, firmware sources of the device, software sources of the device, geo-location data from the device, calling app data from the device, user secrets input to the device, or biometric information collected by the device.

5. The method of claim 1, wherein the selecting further comprises:

varying the selection of the combination of sources from one challenge to the next of a plurality of challenges sent to the device.

6. The method of claim 1, wherein the actual minutia values reflecting user-specific personalization associated with the device comprise values from software sources of the device, geo-location data from the device, calling app data from the device, user secrets input to the device, or biometric information collected by the device that change dynamically via various individual instantiations of the user, including elements requiring predictable, constant change in normal situations, such elements comprising: frequently called phone numbers, contacts, email, or network connection data stored on the device.

7. The method of claim 1, wherein the selecting further comprises:

selecting the combination of minutia sources according to a logical grouping for which a particular minutia value or values within the set of update related minutia share a set of expected values of other minutiae with regard to a single update set;

determining from the one of the pre-processed responses that matches the actual response whether the actual response is valid based on determining the collected actual minutia values from the one of the pre-processed responses that matches the actual response and comparing the collected actual minutia values to the set of expected values with regard to the single update set.

8. The method of claim 1, further comprising:

detecting a change on the device of one or more of the collected actual minutia values based on the processing of the set of pre-processed responses and using the one of the pre-processed responses that matches the actual response.

9. The method of claim 1, further comprising:

determining the collected actual minutia values from the one of the pre-processed responses that matches the actual response, based on the processing of the set of pre-processed responses, without the collected actual minutia values having been transmitted on any communication channel, and without the actual response carrying decryptable information about the collected actual minutia values.

10. The method of claim 1, wherein:

the set of pre-processed responses are processed based on information from tracking known updates of the plurality of minutia sources of dynamically changing minutia such that changes to the collected actual minutia values, determined from the one of the pre-processed responses that matches the actual response, provide synchronization of the changes to the collected actual minutia values on the device without actually exchanging the collected actual minutia values between the device and a database.

11. A system comprising:

a non-transitory memory;

one or more hardware processors in communication with the non-transitory memory, configured to communicate with a device, and configured to read instructions from the non-transitory memory to cause the system to perform operations comprising:

selecting, from a plurality of minutia sources of dynamically changing minutia, the sources comprising one or more of hardware sources of the device, firmware sources of the device, software sources of the device, geo-location data from the device, calling app data from the device, user secrets input to the device, or biometric information collected by the device, a combination of the minutia sources from which a corresponding combination of actual minutia values reflecting user-specific personalization associated with the device are collected from the device;

sending a challenge to the device, wherein the challenge includes information about the combination of the minutia sources such that the information enables the device to collect the corresponding combination of actual minutia values reflecting user-specific personalization associated with the device and from which the device can compute an actual response to the challenge based on the collected actual minutia values;

pre-processing a set of responses to the challenge such that:

the set of pre-processed responses covers a range of all actual responses possible to be received from the device when the corresponding combination of actual minutia values reflecting user-specific personalization associated with the device is valid for the device;

the set of pre-processed responses are processed based on information from known updates of the plurality of minutia sources of dynamically changing minutia such that the set of pre-processed responses anticipates changes on the device to the collected actual minutia values from which the device computes the actual response to the challenge; and

the set of pre-processed responses differentiates the device from other devices based on user personalization of the device due to the actual response depending on the collected actual minutia values reflecting user-specific personalization associated with the device;

comparing the actual response from the device to the set of pre-processed responses; and

recognizing the device based on a match of the actual response to one of the set of pre-processed responses for the device.

12. The system of claim 11, wherein recognizing the device further comprises identifying the device.

13. The system of claim 11, wherein recognizing the device further comprises authenticating a user.

14. The system of claim 11, wherein the selecting further comprises:

varying the selection of the combination of sources among the one or more of the hardware sources of the device, firmware sources of the device, software sources of the device, geo-location data from the device, calling app data from the device, user secrets input to the device, or biometric information collected by the device.

15. The system of claim 11, wherein the selecting further comprises:

varying the selection of the combination of sources from one challenge to the next of a plurality of challenges sent to the device.

16. The system of claim 11, wherein the actual minutia values reflecting user-specific personalization associated with the device comprise values from software sources of the device, geo-location data from the device, calling app data from the device, user secrets input to the device, or biometric information collected by the device that change dynamically via various individual instantiations of the user, including elements requiring predictable, constant change in normal situations, such elements comprising: frequently called phone numbers, contacts, email, or network connection data stored on the device.

17. The system of claim 11, wherein the selecting further comprises:

selecting the combination of minutia sources according to a logical grouping for which a particular minutia value or values within the set of update related minutia share a set of expected values of other minutiae with regard to a single update set;

determining from the one of the pre-processed responses that matches the actual response whether the actual response is valid based on determining the collected actual minutia values from the one of the pre-processed responses that matches the actual response and comparing the collected actual minutia values to the set of expected values with regard to the single update set.

18. The system of claim 11, further comprising an operation of:

detecting a change on the device of one or more of the collected actual minutia values based on the processing of the set of pre-processed responses and using the one of the pre-processed responses that matches the actual response.

19. The system of claim 11, further comprising an operation of:

determining the collected actual minutia values from the one of the pre-processed responses that matches the actual response, based on the processing of the set of pre-processed responses, without the collected actual minutia values having been transmitted on any communication channel, and without the actual response carrying decryptable information about the collected actual minutia values.

20. The system of claim 11, wherein:

the set of pre-processed responses are processed based on information from tracking known updates of the plurality of minutia sources of dynamically changing minutia such that changes to the collected actual minutia values, determined from the one of the pre-processed responses that matches the actual response, provide synchronization of the changes to the collected actual minutia values on the device without actually exchanging the collected actual minutia values between the device and a database.

21. A non-transitory machine-readable medium having stored thereon machine-readable instructions executable to cause a system to perform operations comprising:

selecting, from a plurality of minutia sources of dynamically changing minutia, the sources comprising one or more of hardware sources of the device, firmware sources of the device, software sources of the device, geo-location data from the device, calling app data from the device, user secrets input to the device, or biometric information collected by the device, a combination of the minutia sources from which a corresponding combination of actual minutia values reflecting user-specific personalization associated with the device are collected from the device;

sending a challenge to the device, wherein the challenge includes information about the combination of the minutia sources such that the information enables the device to collect the corresponding combination of actual minutia values reflecting user-specific personalization associated with the device and from which the device can compute an actual response to the challenge based on the collected actual minutia values;

pre-processing a set of responses to the challenge such that:

the set of pre-processed responses covers a range of all actual responses possible to be received from the device when the corresponding combination of actual minutia values reflecting user-specific personalization associated with the device is valid for the device;

the set of pre-processed responses are processed based on information from known updates of the plurality of minutia sources of dynamically changing minutia such that the set of pre-processed responses anticipates changes on the device to the collected actual minutia values from which the device computes the actual response to the challenge; and the set of pre-processed responses differentiates the device from other devices based on user personalization of the device due to the actual response depending on the collected actual minutia values reflecting user-specific personalization associated with the device;

comparing the actual response from the device to the set of pre-processed responses; and

recognizing the device based on a match of the actual response to one of the set of pre-processed responses for the device.

ABSTRACT

Dynamic key cryptography validates mobile device users to cloud services by uniquely identifying the user's electronic device using a very wide range of hardware, firmware, and software minutiae, user secrets, and user biometric values found in or collected by the device. Processes for uniquely identifying and validating the device include: selecting a subset of minutia from a plurality of minutia types; computing a challenge from which the user device can form a response based on the selected combination of minutia; computing a set of pre-processed responses that covers a range of all actual responses possible to be received from the device if the combination of the particular device with the device's collected actual values of minutia is valid; receiving an actual response to the challenge from the device; determining whether the actual response matches any of the pre-processed responses; and providing validation, enabling authentication, data protection, and digital signatures.

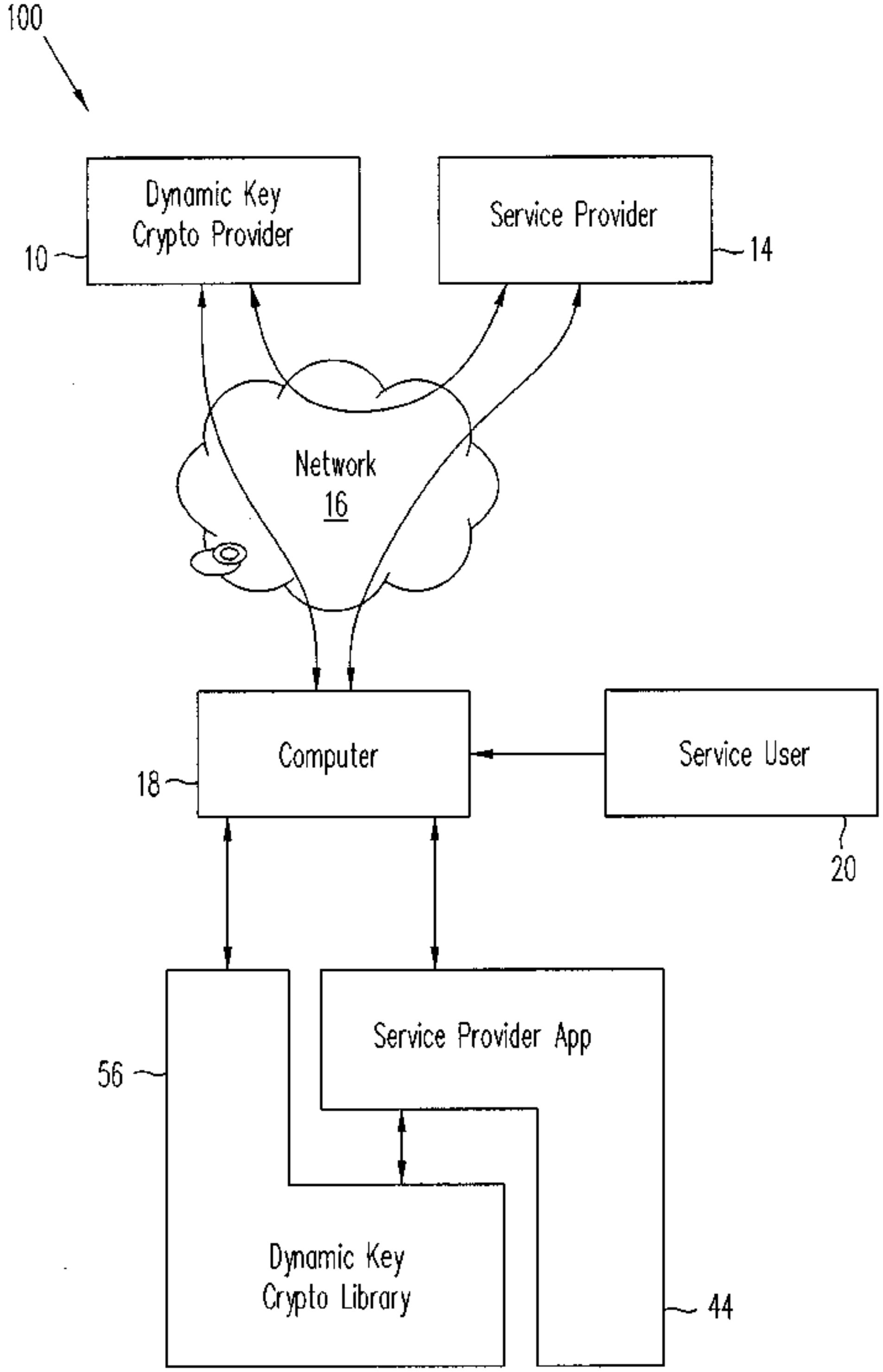

100
Dynamic Key Crypto Provider
10
Service Provider
14
Network
16
Computer
18
Service User
20
56
Service Provider App
Dynamic Key Crypto Library
44

FIG. 1

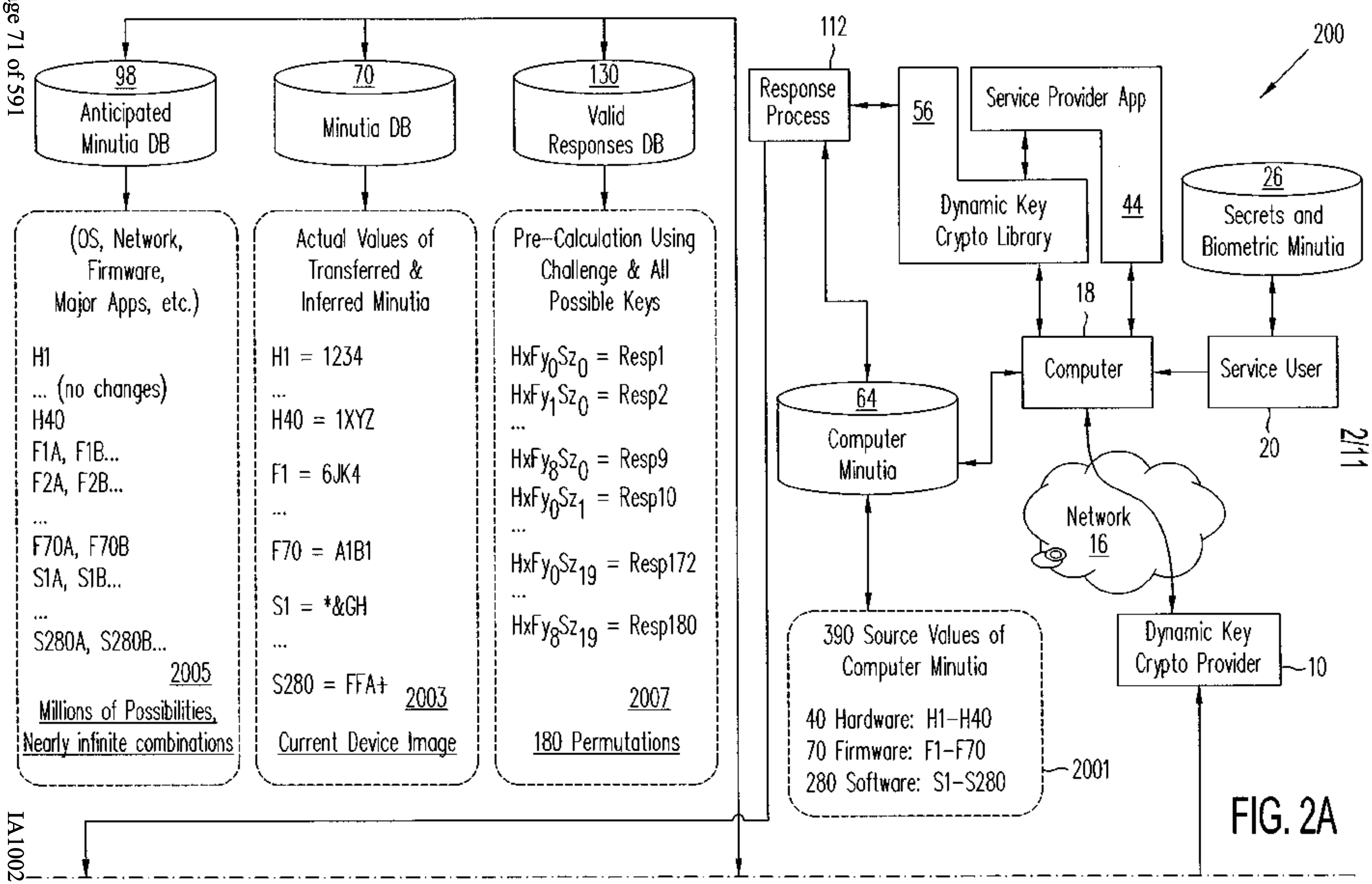

200
98
Anticipated Minutia DB
70
Minutia DB
130
Valid Responses DB
(OS, Network, Firmware, Major Apps, etc.)
H1
... (no changes)
H40
F1A, F1B...
F2A, F2B...
...
F70A, F70B
S1A, S1B...
...
S280A, S280B...
2005
Millions of Possibilities,
Nearly infinite combinations
Actual Values of Transferred & Inferred Minutia
H1 = 1234
...
H40 = 1XYZ
F1 = 6JK4
...
F70 = A1B1
S1 = *&GH
...
S280 = FFA+
2003
Current Device Image
Pre–Calculation Using Challenge & All Possible Keys
$HxFy_0Sz_0$ = Resp1
$HxFy_1Sz_0$ = Resp2
...
$HxFy_8Sz_0$ = Resp9
$HxFy_0Sz_1$ = Resp10
...
$HxFy_0Sz_{19}$ = Resp172
...
$HxFy_8Sz_{19}$ = Resp180
2007
180 Permutations
112
Response Process
56
Dynamic Key Crypto Library
Service Provider App
44
26
Secrets and Biometric Minutia
18
Computer
Service User
20
64
Computer Minutia
Network
16
Dynamic Key Crypto Provider
10
390 Source Values of Computer Minutia
40 Hardware: H1–H40
70 Firmware: F1–F70
280 Software: S1–S280
2001

FIG. 2A

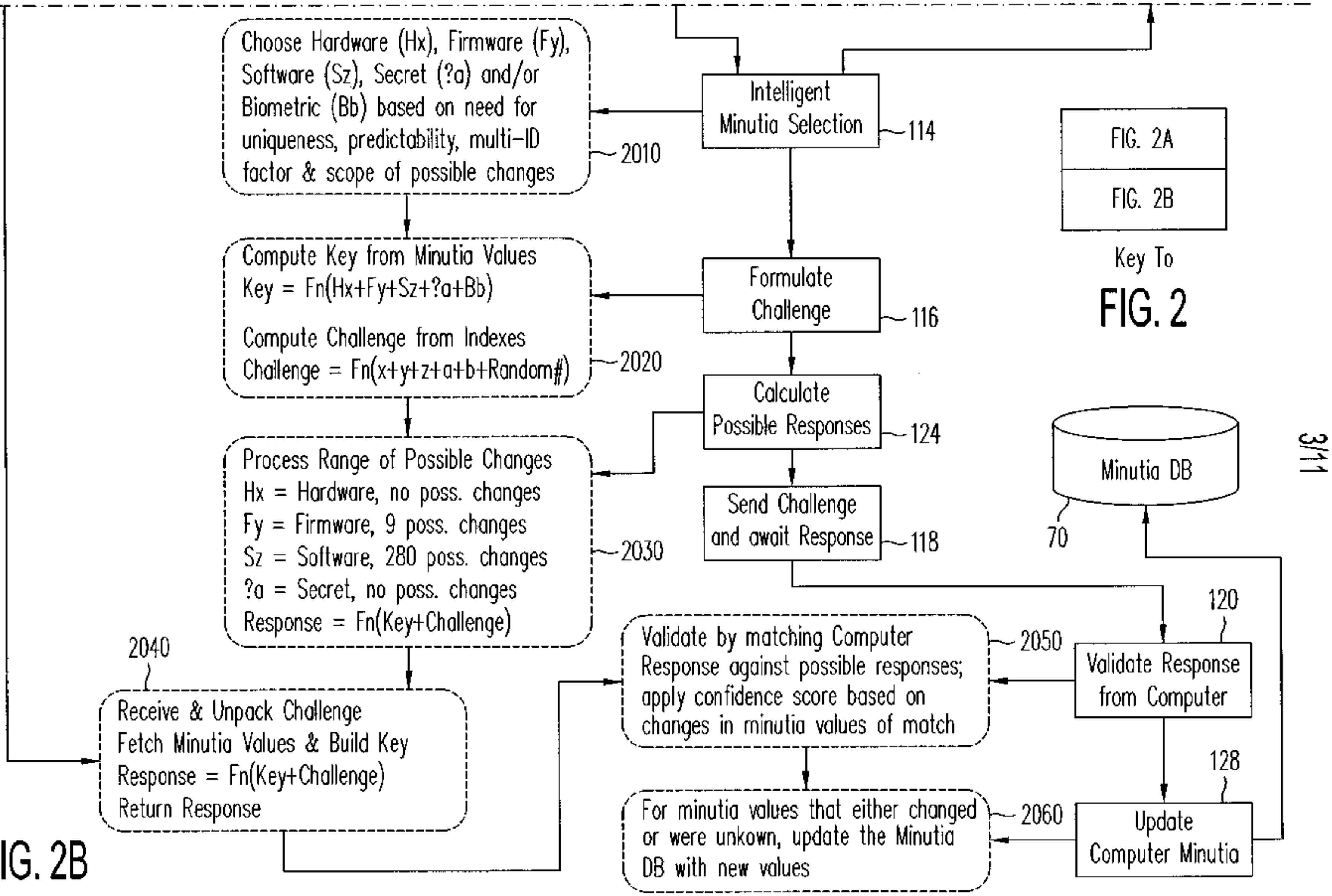


FIG. 2A
FIG. 2B
Intelligent Minutia Selection
114
Choose Hardware (Hx), Firmware (Fy), Software (Sz), Secret (?a) and/or Biometric (Bb) based on need for uniqueness, predictability, multi-ID factor & scope of possible changes
2010
Formulate Challenge
116
Compute Key from Minutia Values
Key = Fn(Hx+Fy+Sz+?a+Bb)
Compute Challenge from Indexes
Challenge = Fn(x+y+z+a+b+Random#)
2020
Calculate Possible Responses
124
Process Range of Possible Changes
Hx = Hardware, no poss. changes
Fy = Firmware, 9 poss. changes
Sz = Software, 280 poss. changes
?a = Secret, no poss. changes
Response = Fn(Key+Challenge)
2030
Send Challenge and await Response
118
Minutia DB
70
2040
Receive & Unpack Challenge
Fetch Minutia Values & Build Key
Response = Fn(Key+Challenge)
Return Response
Validate by matching Computer Response against possible responses; apply confidence score based on changes in minutia values of match
2050
120
Validate Response from Computer
128
For minutia values that either changed or were unkown, update the Minutia DB with new values
2060
Update Computer Minutia

Key To
FIG. 2

FIG. 2B

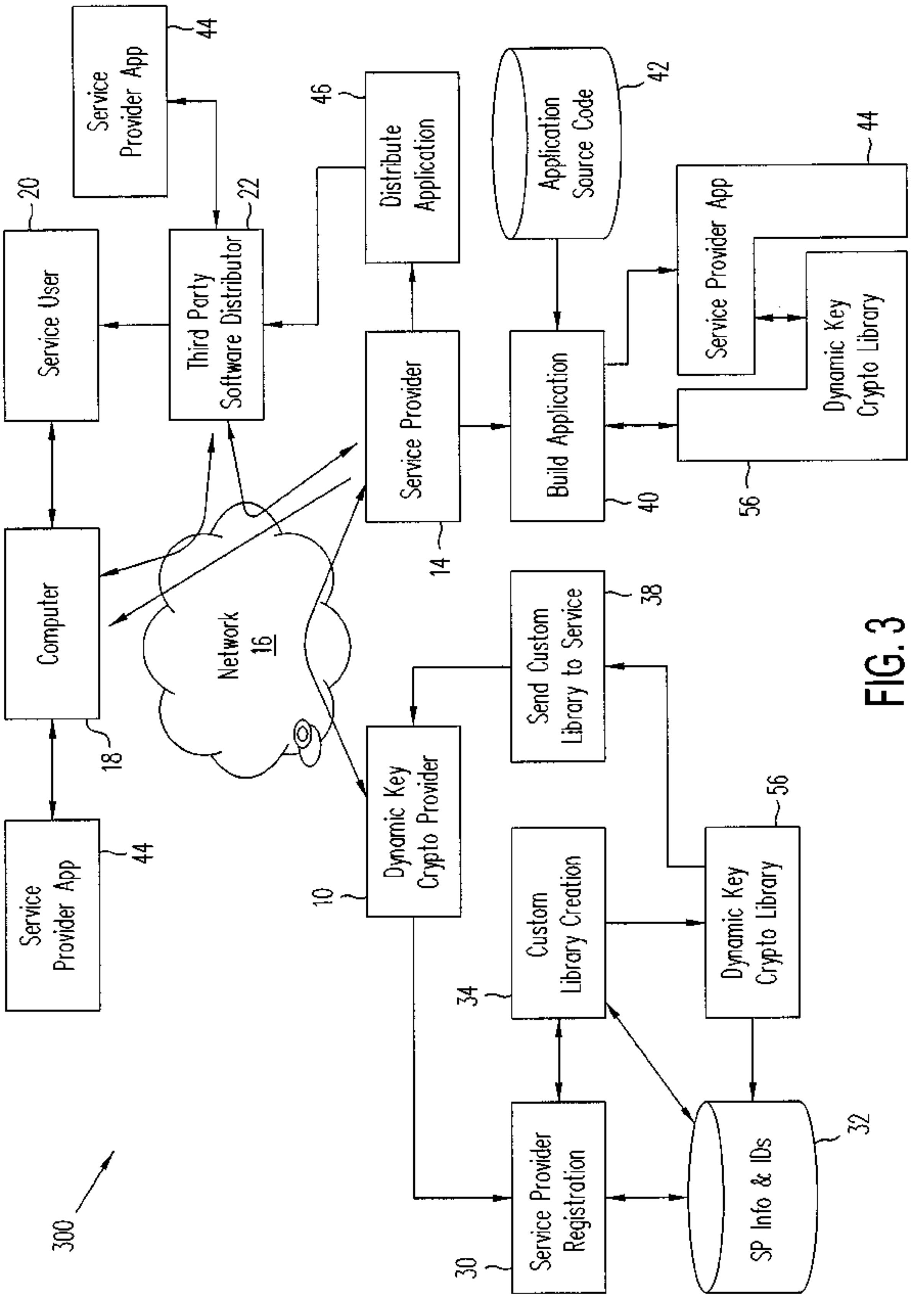

300
Service Provider App
44
Computer
18
Service User
20
Third Party Software Distributor
22
Service Provider App
44
Network
16
Service Provider
14
Distribute Application
46
Dynamic Key Crypto Provider
10
Build Application
40
Application Source Code
42
Service Provider App
44
Dynamic Key Crypto Library
56
Send Custom Library to Service
38
Custom Library Creation
34
Dynamic Key Crypto Library
56
Service Provider Registration
30
SP Info & IDs
32

FIG. 3

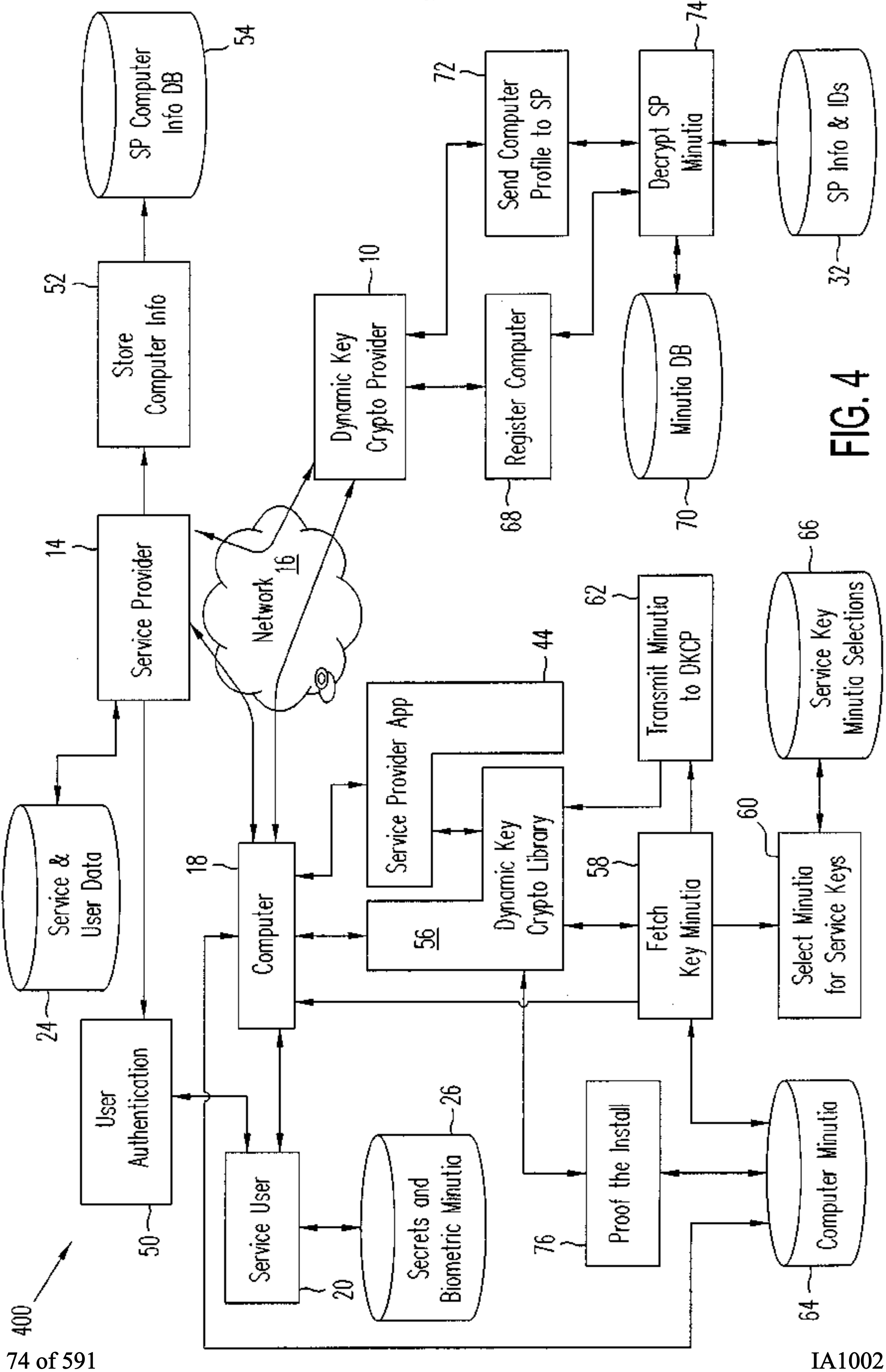

400
Service Provider
14
SP Computer Info DB
54
Store Computer Info
52
Network 16
Dynamic Key Crypto Provider
10
Register Computer
68
Send Computer Profile to SP
72
Decrypt SP Minutia
74
Minutia DB
70
SP Info & IDs
32
Service & User Data
24
User Authentication
50
Computer
18
Service Provider App
44
Dynamic Key Crypto Library
56
Transmit Minutia to DKCP
62
Fetch Key Minutia
58
Select Minutia for Service Keys
60
Service Key Minutia Selections
66
Service User
20
Secrets and Biometric Minutia
26
Proof the Install
76
Computer Minutia
64

FIG. 4

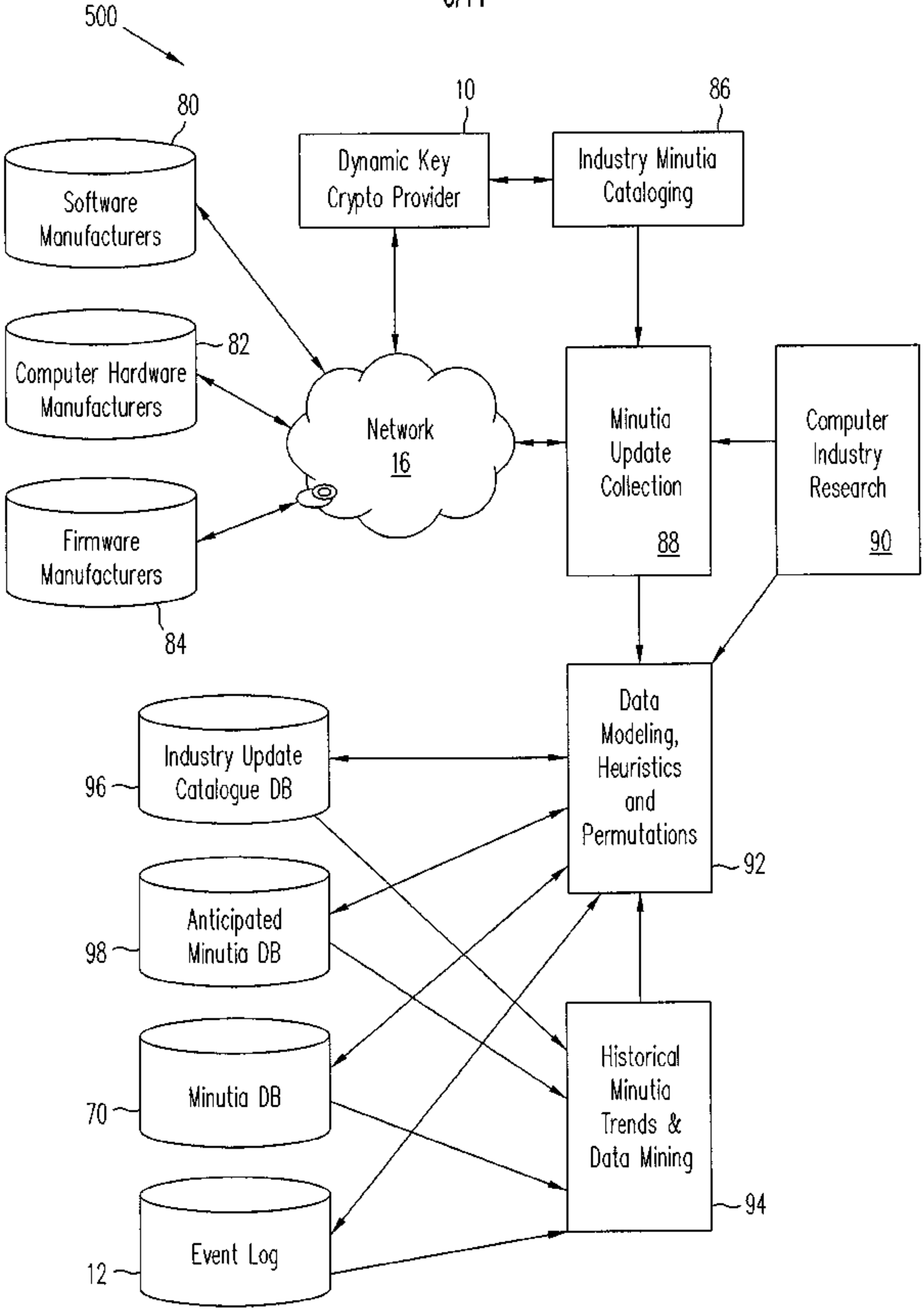

500
80
Software Manufacturers
82
Computer Hardware Manufacturers
Firmware Manufacturers
84
10
Dynamic Key Crypto Provider
86
Industry Minutia Cataloging
Network 16
Minutia Update Collection 88
Computer Industry Research 90
Data Modeling, Heuristics and Permutations
92
96
Industry Update Catalogue DB
98
Anticipated Minutia DB
70
Minutia DB
12
Event Log
Historical Minutia Trends & Data Mining
94

FIG. 5

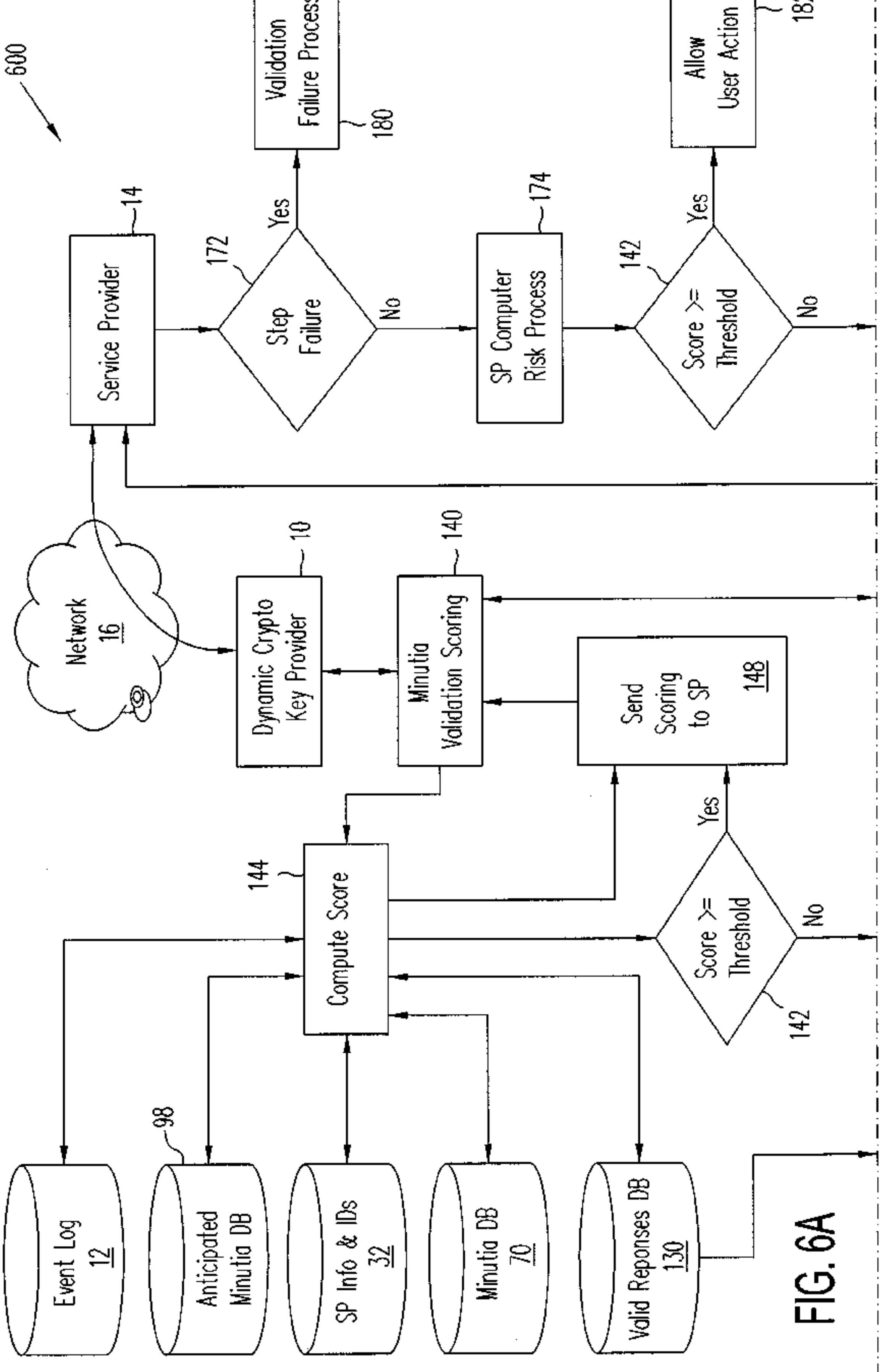

600
Service Provider
14
Step Failure
172
Yes
No
Validation Failure Process
180
SP Computer Risk Process
174
Score >= Threshold
142
Yes
No
Allow User Action
182
Network
16
Dynamic Crypto Key Provider
10
Minutia Validation Scoring
140
Send Scoring to SP
148
Yes
Compute Score
144
Score >= Threshold
No
142
Event Log
12
Anticipated Minutia DB
98
SP Info & IDs
32
Minutia DB
70
Valid Reponses DB
130

FIG. 6A

8/11

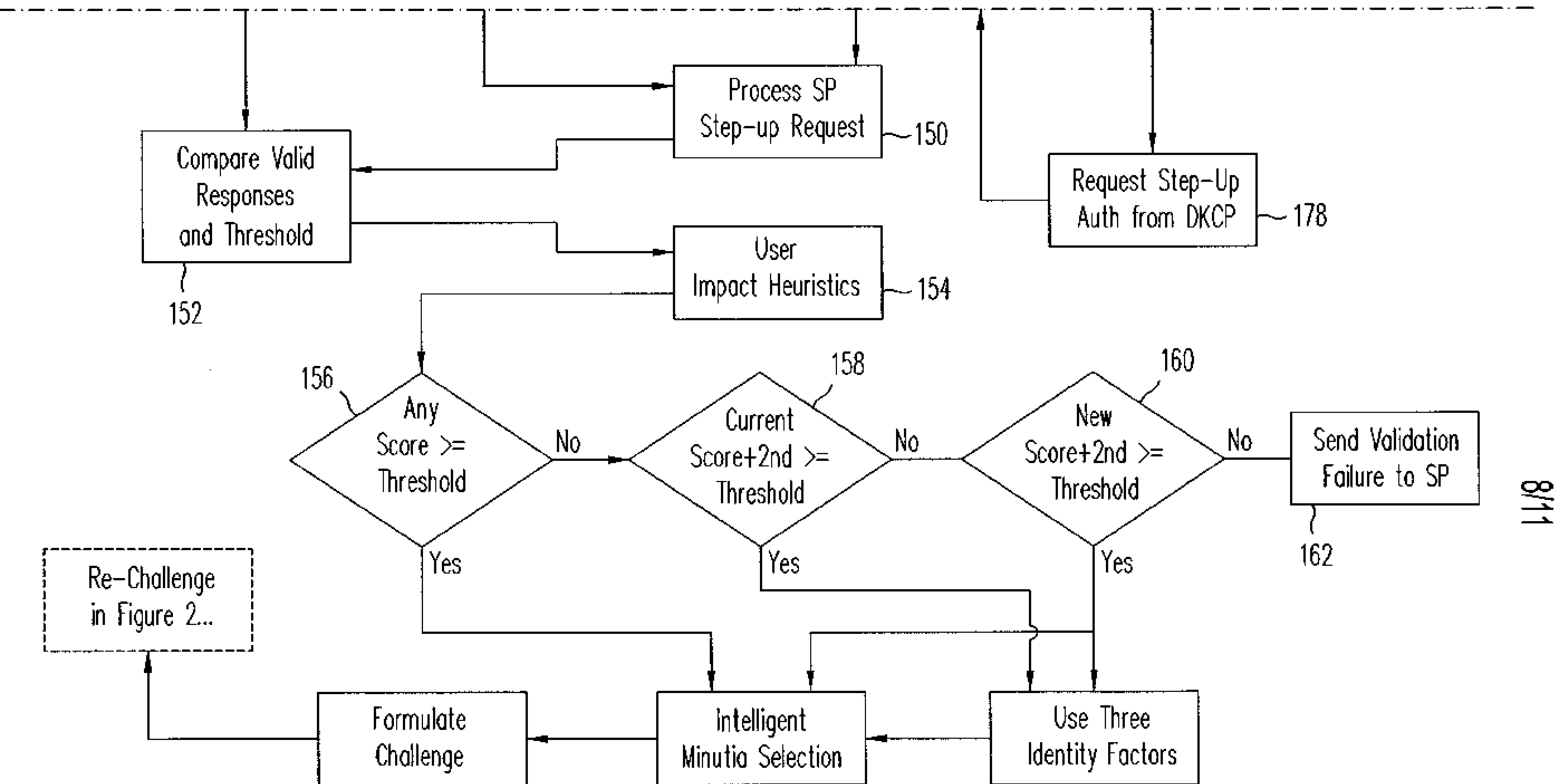
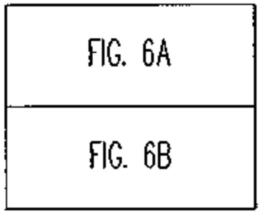

Compare Valid Responses and Threshold
152
Process SP Step-up Request
150
User Impact Heuristics
154
Request Step-Up Auth from DKCP
178
156
Any Score >= Threshold
No
Yes
158
Current Score+2nd >= Threshold
No
Yes
160
New Score+2nd >= Threshold
No
Yes
Send Validation Failure to SP
162
Re-Challenge in Figure 2...
Formulate Challenge
116
Intelligent Minutia Selection
114
Use Three Identity Factors
170

FIG. 6B



Key to FIG. 6

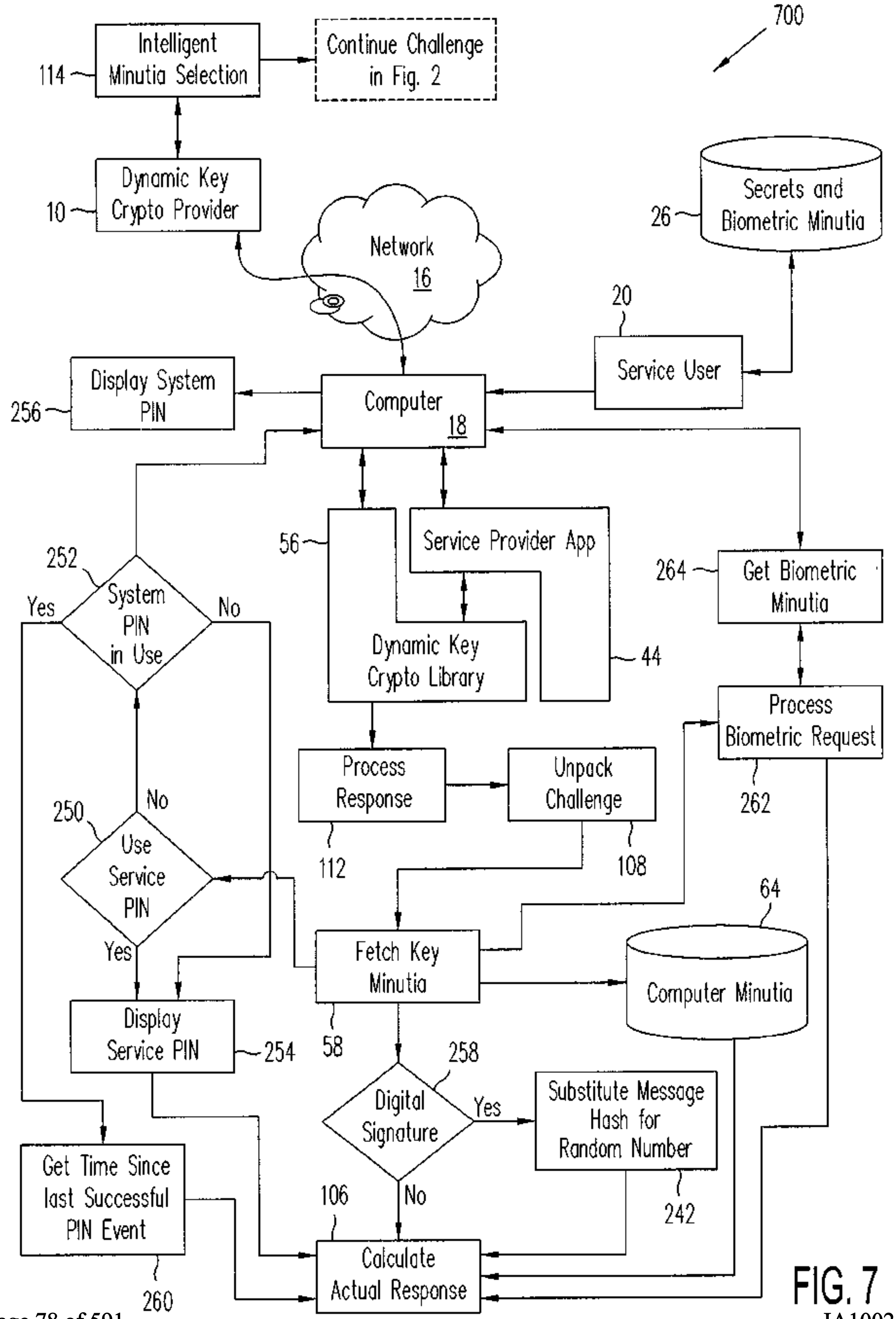

700
114
Intelligent Minutia Selection
Continue Challenge in Fig. 2
10
Dynamic Key Crypto Provider
Network 16
26
Secrets and Biometric Minutia
20
Service User
256
Display System PIN
Computer 18
56
Service Provider App
Dynamic Key Crypto Library
44
264
Get Biometric Minutia
252
System PIN in Use
Yes
No
Process Biometric Request
262
Process Response
112
Unpack Challenge
108
250
Use Service PIN
No
Yes
Fetch Key Minutia
58
64
Computer Minutia
Display Service PIN
254
258
Digital Signature
Yes
No
Substitute Message Hash for Random Number
242
Get Time Since last Successful PIN Event
260
106
Calculate Actual Response

FIG. 7

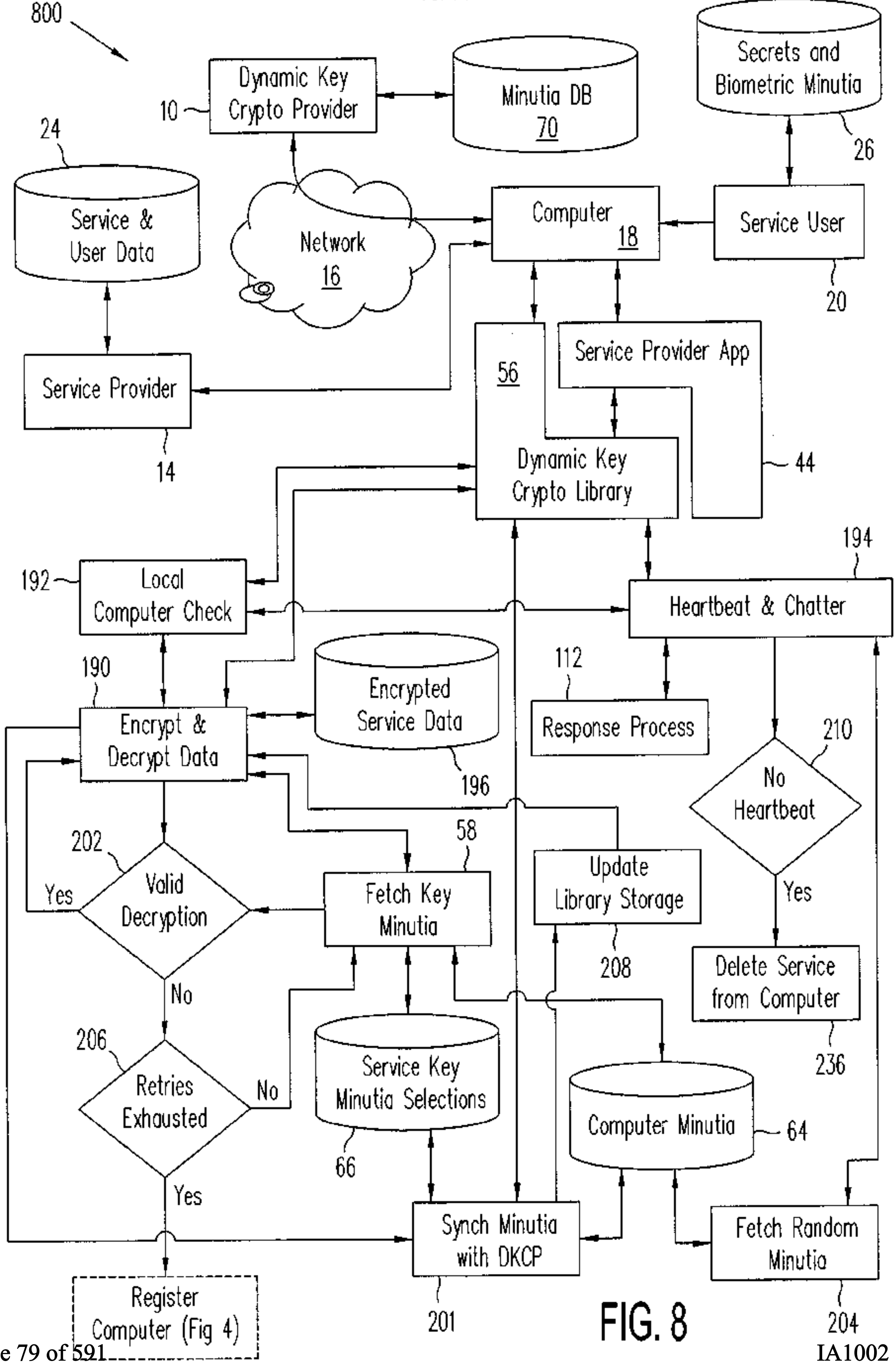

800
Dynamic Key Crypto Provider
10
Minutia DB 70
Secrets and Biometric Minutia
26
24
Service & User Data
Network 16
Computer 18
Service User
20
Service Provider
14
56
Service Provider App
Dynamic Key Crypto Library
44
194
192
Local Computer Check
Heartbeat & Chatter
190
Encrypt & Decrypt Data
Encrypted Service Data
196
112
Response Process
210
No Heartbeat
Yes
Delete Service from Computer
236
202
Yes
Valid Decryption
No
58
Fetch Key Minutia
Update Library Storage
208
206
Retries Exhausted
No
Service Key Minutia Selections
66
Computer Minutia
64
Yes
Synch Minutia with DKCP
201
Fetch Random Minutia
204
Register Computer (Fig 4)

FIG. 8

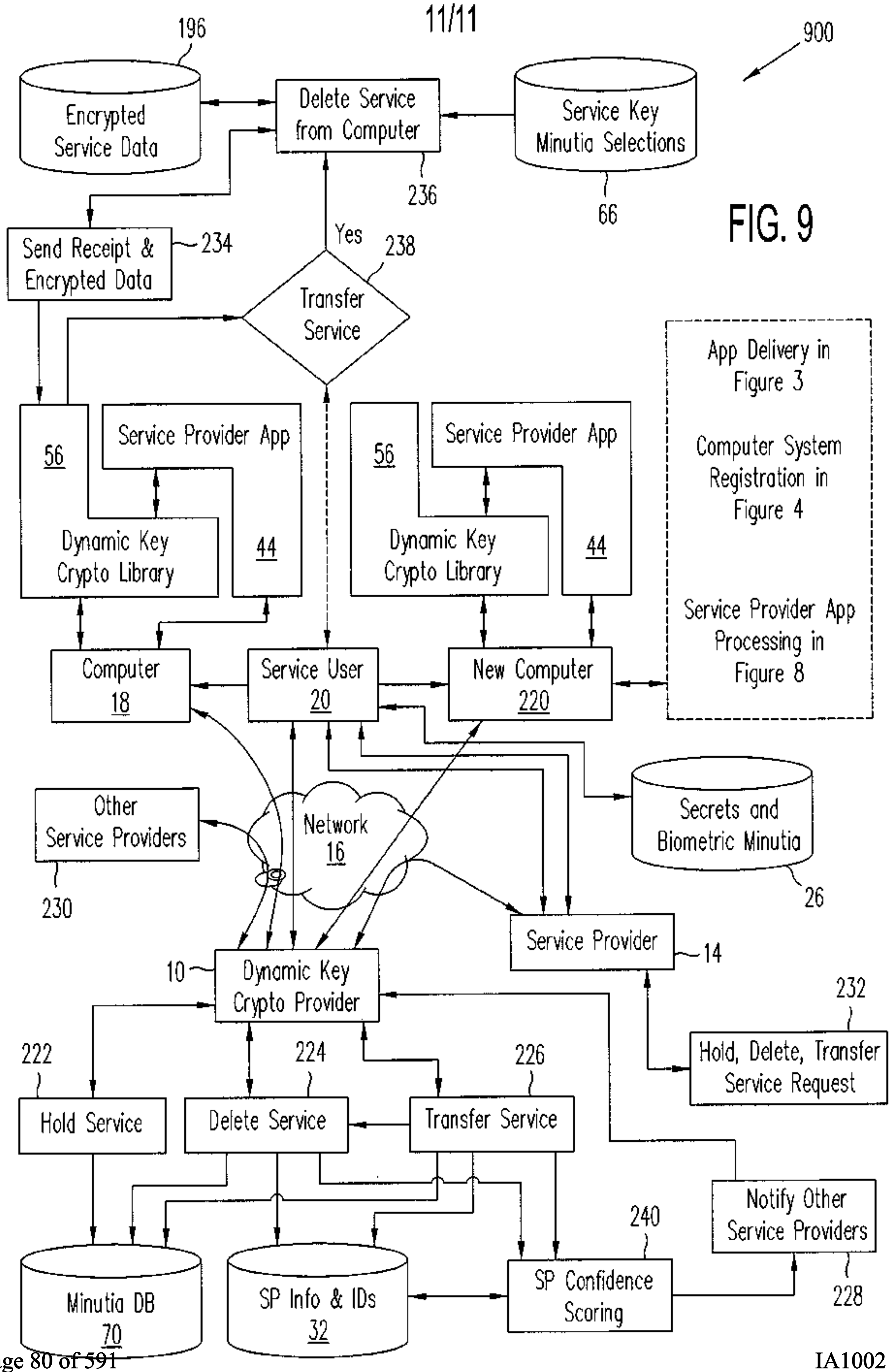

196
Encrypted Service Data
Delete Service from Computer
236
Service Key Minutia Selections
66
900
Send Receipt & Encrypted Data
234
Yes
238
Transfer Service
App Delivery in Figure 3
Computer System Registration in Figure 4
Service Provider App Processing in Figure 8
56
Service Provider App
Dynamic Key Crypto Library
44
56
Service Provider App
Dynamic Key Crypto Library
44
Computer 18
Service User 20
New Computer 220
Other Service Providers
230
Network 16
Secrets and Biometric Minutia
26
Service Provider
14
10
Dynamic Key Crypto Provider
232
Hold, Delete, Transfer Service Request
222
224
226
Hold Service
Delete Service
Transfer Service
240
Notify Other Service Providers
228
Minutia DB 70
SP Info & IDs 32
SP Confidence Scoring

FIG. 9

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE

As the below named inventor, I hereby declare that:

This declaration is directed to:

☒ The attached application, or

□ United States application or PCT international application number ____________________

filed on ____________________.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Paul Timothy Miller Date (Optional) : ____________________

Signature: ____________________

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE

As the below named inventor, I hereby declare that:

This declaration is directed to:
☒ The attached application, or
☐ United States application or PCT international application number ______________________
filed on ______________________.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: George Allen Tuvell Date (Optional) : Aug 11, 2014

Signature:

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul Timothy Miller
Filer:	David B. Bowls/Maria Castillo
Attorney Docket Number:	47583.5US02

Filed as Small Entity

Filing Fees for **Track I Prioritized Examination - Nonprovisional Application under 35 USC 111(a)**

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	70	70
Utility Search Fee	2111	1	300	300
Utility Examination Fee	2311	1	360	360
Request for Prioritized Examination	2817	1	2000	2000
Pages:				
Claims:				
Claims in excess of 20	2202	1	40	40
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Publ. Fee- Early, Voluntary, or Normal	1504	1	0	0
PROCESSING FEE, EXCEPT PROV. APPLS.	2830	1	70	70
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**2840**

Electronic Acknowledgement Receipt

EFS ID:	25247861
Application Number:	15075066
International Application Number:	
Confirmation Number:	1166
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul Timothy Miller
Customer Number:	27683
Filer:	David B. Bowls/Maria Castillo
Filer Authorized By:	David B. Bowls
Attorney Docket Number:	47583.5US02
Receipt Date:	18-MAR-2016
Filing Date:	
Time Stamp:	21:41:02
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$2840
RAM confirmation Number	7265
Deposit Account	081394
Authorized User	BOWLS, DAVID B.

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 CFR 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 CFR 1.19 (Document supply fees)

Charge any Additional Fees required under 37 CFR 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

<table>
<tr><th>Document Number</th><th>Document Description</th><th>File Name</th><th>File Size(Bytes)/ Message Digest</th><th>Multi Part /.zip</th><th>Pages (if appl.)</th></tr>
<tr><td rowspan="2">1</td><td rowspan="2">TrackOne Request</td><td rowspan="2">47583_5US02_TrackOneRequest.pdf</td><td>490326</td><td rowspan="2">no</td><td rowspan="2">1</td></tr>
<tr><td>135d50958c3c95a73e3586a08cb1325f09d2a128</td></tr>
<tr><td colspan="6"><b>Warnings:</b></td></tr>
<tr><td colspan="6"><b>Information:</b></td></tr>
<tr><td rowspan="2">2</td><td rowspan="2"></td><td rowspan="2">47583_5US02_Transmittals.pdf</td><td>3456229</td><td rowspan="2">yes</td><td rowspan="2">9</td></tr>
<tr><td>ad0e2c697943d6042aaec992997f5972d1fb33c9</td></tr>
<tr><td rowspan="4"></td><td colspan="5"><b>Multipart Description/PDF files in .zip description</b></td></tr>
<tr><td colspan="3"><b>Document Description</b></td><td><b>Start</b></td><td><b>End</b></td></tr>
<tr><td colspan="3">Transmittal of New Application</td><td>1</td><td>1</td></tr>
<tr><td colspan="3">Application Data Sheet</td><td>2</td><td>9</td></tr>
<tr><td colspan="6"><b>Warnings:</b></td></tr>
<tr><td colspan="6"><b>Information:</b></td></tr>
<tr><td rowspan="2">3</td><td rowspan="2"></td><td rowspan="2">47583_5US02_Specification.pdf</td><td>21008323</td><td rowspan="2">yes</td><td rowspan="2">60</td></tr>
<tr><td>080135f14e37c18a50772be40cbe11832547a26e</td></tr>
<tr><td rowspan="5"></td><td colspan="5"><b>Multipart Description/PDF files in .zip description</b></td></tr>
<tr><td colspan="3"><b>Document Description</b></td><td><b>Start</b></td><td><b>End</b></td></tr>
<tr><td colspan="3">Specification</td><td>1</td><td>49</td></tr>
<tr><td colspan="3">Claims</td><td>50</td><td>59</td></tr>
<tr><td colspan="3">Abstract</td><td>60</td><td>60</td></tr>
<tr><td colspan="6"><b>Warnings:</b></td></tr>
<tr><td colspan="6"><b>Information:</b></td></tr>
<tr><td rowspan="2">4</td><td rowspan="2">Drawings-only black and white line drawings</td><td rowspan="2">47583_5US02_Drawings.pdf</td><td>2559040</td><td rowspan="2">no</td><td rowspan="2">11</td></tr>
<tr><td>92106ce6ffa6c2f5a5625c6834cab5822fcff027</td></tr>
<tr><td colspan="6"><b>Warnings:</b></td></tr>
<tr><td colspan="6"><b>Information:</b></td></tr>
</table>

5	Oath or Declaration filed	47583_5US02_Declarations.pdf	891895 996e801dc5c524c066decb1eca33f780290 41b5c	no	2
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	42272 a086d38422b281dbe2bf03ff04cdadbdaf6b 3dab	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	28448085		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc Code: TRACK1.REQ
Document Description: TrackOne Request

47583.5US02 PTO/AIA/424 (04-14)

CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION UNDER 37 CFR 1.102(e) (Page 1 of 1)

First Named Inventor:	Paul Timothy Miller	Nonprovisional Application Number (if known):	
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i)(1) and the prioritized examination fee set forth in 37 CFR 1.17(c) have been filed with the request. The publication fee requirement is met because that fee, set forth in 37 CFR 1.18(d), is currently $0. The basic filing fee, search fee, and examination fee are filed with the request or have been already been paid. I understand that any required excess claims fees or application size fee must be paid for the application.

2. I understand that the application may not contain, or be amended to contain, more than four independent claims, more than thirty total claims, or any multiple dependent claims, and that any request for an extension of time will cause an outstanding Track I request to be dismissed.

3. The applicable box is checked below:

I. ☑ Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)

i. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.

---OR---

(b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.

ii. An executed inventor's oath or declaration under 37 CFR 1.63 or 37 CFR 1.64 for each inventor, **or** the application data sheet meeting the conditions specified in 37 CFR 1.53(f)(3)(i) is filed with the application.

II. □ Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)

i. A request for continued examination has been filed with, or prior to, this form.
ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature	Date 03-18-2016
Name (Print/Typed) David Bowls	Practitioner Registration Number 39,915

*__Note__: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required.**

☑ *Total of 1 forms are submitted.

U. S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(use as many sheets as necessary)

Complete if Known	
Application Number	15/075,066
Filing Date	March 18, 2016
Applicant(s)	mSignia, Inc.
Art Unit	2431
Examiner Name	Not Yet Assigned
Attorney Docket Number	47583.5US02

SHEET	1	OF	1

U. S. PATENT DOCUMENTS

Examiner's Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
		2007/0240218	10-11-2007	Tuvell et al.
		2007/0240219	10-11-2007	Tuvell et al.
		2007/0240220	10-11-2007	Tuvell et al.
		2007/0240221	10-11-2007	Tuvell et al.
		2007/0240222	10-11-2007	Tuvell et al.
		2008/0086773	04-10-2008	Tuvell et al.
		2008/0086776	04-10-2008	Tuvell et al.
		2008/0196104	08-14-2008	Tuvell et al.
		2011/0082768	04-07-2011	Eisen, Ori
		2011/0293094	12-01-2011	Os et al.
		2011/0296170	12-01-2011	Chen, Hu-Mu
		7,373,669	05-13-2008	Eisen, Ori
		2007/0124801	05-31-2007	Thomas et al.
		2007/0214151	09-13-2007	Thomas et al.
		2008/0244744	10-02-2008	Thomas et al.
		2011/0113388	05-12-2011	Eisen et al.
		7,908,662	03-15-2011	Richardson, Ric B.
		2009/0138975	05-28-2009	Richardon, Ric B.
		2010/0229224	09-09-2010	Etchegoyen, Craig S.
		7,333,871	02-19-2008	Schwarm, Alexander T.
		8,312,157	11-13-2012	Jakobsson et al.
		2013/0340052	12-19-2013	Jakobsson, Bjorn Markus
		7,937,467 B2	05-03-2011	Barber, Timothy P.
		7,330,871 B2	02-12-2008	Barber, Timothy P.
		6,041,133	03-21-2000	Califano et al.
		6,185,316	02-06-2001	Buffam, William J.
		2006/0031676	02-09-2006	Vantalon et al.
		2006/0104484	05-18-2006	Bolle et al.
		2007/0174206	07-26-2007	Colella, Brian
		2008/0175449	07-24-2008	Fang et al.
		2008/0235515	09-25-2008	Yedidia et al.
		2009/0310779	12-17-2009	Lam et al.
		2010/0027834	02-04-2010	Spitzig et al.
		2012/0201381	08-09-2012	Miller et al.
		8,375,221	02-12-2013	Thom et al.

FOREIGN PATENT DOCUMENTS

Examiner's Initials	Cite No.	Foreign Patent Document (Country Code – Number – Kind)	Publication Date MM-DD-YYYY	Patentee or Applicant of Cited Document	Translation Y/N
		WO 2010/035202	04-01-2010	KONIN-KLIJKE PHILIPS ELECTRONICS N.V.	Y
		WO 2013/154936	10-17-2013	BRIVAS LLC	Y
		WO 2013/138714	09-19-2013	ACUITY SYSTEMS, INC.	Y

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 September 2013 (19.09.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/138714 A1

(51) International Patent Classification:
H04L 9/32 (2006.01) *H04W 12/06* (2009.01)

(21) International Application Number:
PCT/US2013/032040

(22) International Filing Date:
15 March 2013 (15.03.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/612,023	16 March 2012 (16.03.2012)	US
61/708,607	1 October 2012 (01.10.2012)	US
61/737,557	14 December 2012 (14.12.2012)	US

(71) Applicant: **ACUITY SYSTEMS, INC.** [US/US]; 23629 Mill Valley, Santa Clarita, California 91355 (US).

(72) Inventors: **SPENCER, Herbert, W., III**; c/o ACUITY SYSTEMS, INC., 23629 Mill Valley, Santa Clarita, California 91355 (US). **CANFIELD, Christopher, M.**; c/o ACUITY SYSTEMS, INC., 23629 Mill Valley, Santa Clarita, California 91355 (US). **HUTSON, Harlan**; c/o ACUITY SYSTEMS, INC., 23629 Mill Valley, Santa Clarita, California 91355 (US). **CONROY, Vince**; c/o ACUITY SYSTEMS, INC., 23629 Mill Valley, Santa Clarita, California 91355 (US). **HICKERSON, Steven, A.**; c/o ACUITY SYSTEMS, INC., 23629 Mill Valley, Santa Clarita, California 91355 (US).

(74) Agents: **SHELDON, Jeffrey, G.** et al.; Sheldon Mak & Anderson PC, 100 Corson Street, Third Floor, Pasadena, California 91103-3842 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[Continued on next page]

(54) Title: AUTHENTICATION SYSTEM

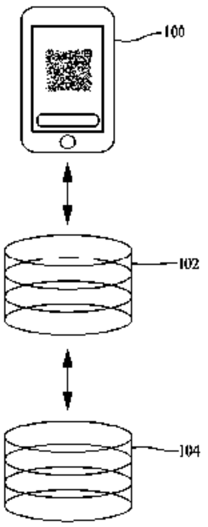


Fig. 1

(57) Abstract: A system for creating a combined electronic identification that obtains user information (202) about a user of a hardware device (100), authenticates the user from the user information (202), obtains a hardware profile (208) of the device (100), the hardware profile 208 comprising user generated data stored on the device (100) and links the user information (202) and the hardware profile (208) as a combined electronic identification. The hardware device (100) can be comprised of a main processor, memory, a touchscreen interface, and a wireless communication module, such as a mobile phone, computer, or tablet computer.

WO 2013/138714 A1

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

AUTHENTICATION SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of United States Provisional Patent Application Numbers 61/612,023 filed March 16, 2012, 61/708,607 filed October 1, 2012, and 61/737,577 filed December 14, 2012, the contents of which are incorporated herein by reference in their entirety.

BACKGROUND

[0002] Identity fraud is the leading type of credit card fraud in the US. Over 9 million adults are victims each year, which results in $100 million in merchant losses. Despite the increased digital power at our disposal, the state of the current security systems available for the prevention of identity fraud is still inadequate.

[0003] A problem associated with current security systems is that they lack the ability to truly discern an identity of an individual at the fundamental level.

[0004] Accordingly, there is a need for a better security system that is able to truly discern an identity of an individual in order to prevent identity fraud.

SUMMARY

[0005] The present invention is directed to methods and systems that satisfy this need. An exemplary method comprises obtaining user information about a user of a hardware device, authenticating the user from the user information, obtaining a hardware profile of the device, the hardware profile comprising user generated data stored on the device, and linking the user information and the hardware profile as a combined electronic identification. The hardware device can comprise a processor, memory, a touchscreen interface, and a wireless communication module, and can be a device such as a mobile phone, computer, or tablet computer.

[0006] Preferably, linking comprises concatenating the user information and the hardware profile.

[0007] The invention is also directed to a method for creating a combined electronic identification associated with a hardware device comprising the steps of inputting user information about a user on the device, sending the user information from the device to a server, receiving authentication from the server, and sending a hardware profile from the device to the server to create a combined electronic identification, the hardware profile comprising user generated data stored on the device.

[0008] In one version the hardware profile comprises information on the hardware device selected from the group consisting of (a) contact information, (b) mobile network code, (c) information about music, (d) pixel colors from a background screen, (e) installed applications, (f) arrangement of the applications, (g) frequency of use of applications, (h) location of the user, (i) Bluetooth device pairings, (j) carrier name, (k) mobile country code, (l) phone number, (m) photos, (n) device name, (o) MAC address, (p) device type, and combinations of one or more thereof.

[0009] In one version the user is authenticated from user information, the user information comprising information about the user selected from the group consisting of the user's (a) name, (b) social security number, (c) national identification number, (d) passport number, (e) IP address, (f) vehicle registration number, (g) vehicle license plate number, (h) driver's license number, (i) appearance, (j) fingerprint, (k) handwriting, (l) credit card information, (m) bank account information, (n) digital identity, (o) date of birth, (p) birthplace, (q) past and current residence, (r) age, (s) gender, (t) marital status, (u) race, (v) names of schools attended, (w) workplace, (x) salary, (y) job position, (z) biometric data, and combinations of one or more thereof.

[0010] In another version, the user provides answers to knowledge based questions that only the user would know all the answers to. The probability to which the user is identified can also be determined.

[0011] In one version the user information comprises biometric data of the user, such as fingerprint, retina, and voice data.

[0012] In another version of the invention at least one of the user information and the hardware profile are salted and hashed prior to linking to create a combined electronic identification. Alternatively, both the user information and the hardware profile are salted and hashed prior to linking. Preferably, salting is done by a three to seven digit random number generator, and hashing is done by SHA-2.

[0013] Preferably, the hardware profile and user information are salted and hashed before transfer to any external device. The salting and hashing can be by individual items or in groups of items.

[0014] A system for performing for creating a combined electronic identification associated with a hardware device comprising a processor, memory, an input interface, and a transmitter, the processor being programmed to process through the input interface the user information, transmit through the transmitter the user information to a first server, receive through the transmitter authentication from a second server, transmit through the transmitter the hardware profile to the first server to create a combined electronic identification.

[0015] In one embodiment, the first and second server are the same server.

[0016] In one version the hash information and hardware are truncated to reduce the amount of information transmitted to a server. The truncation can be performed in such a way that sufficient information is retained to differentiate one user from another user.

[0017] The present invention is also directed to a method of allowing a transaction by a user utilizing a stored electronic identification, the stored electronic identification comprising a first stored hardware profile and stored user information, the method comprising the steps of receiving user information and a hardware profile of hardware associated with the user, both hardware profiles comprising user generated data stored on the device, comparing the received user information and the received hardware profile against the stored electronic profile, wherein the received hardware profile and the stored hardware profile are different by at least 0.02%, and allowing the transaction to proceed only if the received hardware profile and the stored hardware profile match by at least 60% and the received user information and the stored user information match by at least 30%.

[0018] The present invention is also directed to a method for a user to perform a transaction with an electronic communication device comprising the steps of salting and hashing a hardware profile of the electronic communication device with user information stored on the device, the hardware profile comprising user generated data stored on the device, sending the salted and hashed hardware profile and the user information to a server, and receiving instructions from the server regarding whether or not to proceed with the transaction.

[0019] Alternatively, the method further comprises the step of entering a security pin to verify the user.

[0020] The present invention is also directed to a method for a user to perform a transaction utilizing a first electronic communication device comprising the steps of connecting with a transaction receiver, receiving from the transaction receiver electronic data for a second electronic communication device different from the first electronic communication device, the second electronic communication device having a user associated therewith and a hardware profile associated therewith, the hardware profile comprising user generated data stored on the device, sending with the second electronic communication device at least part of the received electronic data, user information of the user, and the hardware profile to an authentication server, and if the authentication server authenticates the sent user information, the hardware profile, and the sent electronic data, performing the transaction with the first electronic communication device. Preferably, the first electronic communication device is a desktop computer and the second electronic device is a smartphone.

[0021] Alternatively, the method can comprise the additional step of authenticating with the authentication server.

[0022] In one version the first electronic communication device comprises a visual display, wherein the visual display is read with the second electronic communication device.

[0023] In another version the second electronic communication device comprises a visual display, wherein the visual display is read with the first electronic communication device.

[0024] Preferably, the visual display is a Quick Response (QR) code.

[0025] The present invention is also directed to a system for creating a combined electronic identification associated with a hardware device comprising a processor, memory, and a connection for receiving information executable by the processor. The processor being programmed to receive through the connection the user information, authenticate the user from the user information, receive through the connection the hardware profile, store in memory the received user information and the received hardware profile, and link the user information and the hardware profile together as a combined electronic identification.

[0026] The present invention is also directed to a system for allowing a transaction by a user comprising a processor, memory, and a connection for receiving information for processing by the processor. The memory stores the stored user information and the stored hardware profile. The processor is programmed to receive through the connection the received user information and the received hardware profile, compare the received user information and the received hardware profile against the stored hardware profile wherein the received hardware profile and the stored hardware profile are different by at least 0.02%, and execute the transaction if the received hardware profile and the stored hardware profile match by at least 60% and the received user information and the stored user information match by at least 30%.

[0027] The present invention is also directed to a method of performing a transaction for a user using a first electronic communication device to perform the transaction comprising the steps of receiving information from the first electronic communication device, transmitting electronic data to the user, receiving from a second electronic communication device of the user at least part of the transmitted electronic data, user information associated with the second electronic communication device, and a hardware profile of the second communication device, the hardware profile comprising user generated data stored on the device, determining if the received electronic data, user information and hardware profile are authentic, and if authentic, permitting the user to perform the transaction with the first electronic communication device.

[0028] The present invention is also directed to a system for performing a transaction for a user using a first electronic communication device to perform the transaction comprising a processor, memory, and a connection for receiving information executable by the processor. The memory stores electronic data. The processor is programmed to receive through the connection information from the first electronic communication device, transmit through the connection the stored electronic data to the user, receive through the connection from the second electronic communication device at least part of the transmitted electronic data, user information associated with the second communication device, and hardware profile of the second communication device, and determine if the received electronic data, user information and hardware profile are authentic, and if authentic, permitting the user to perform the transaction with the first electronic communication device.

[0029] In one version of the invention, the received electronic data, user information and hardware profile are authentic, and the processor is programmed to send through the connection to the first electronic communication device a response regarding whether or not to perform the transaction.

DRAWINGS

[0030] These and other features, aspects and advantages of the present invention will become better understood with regard to the following description, appended claims, and accompanying figures where:

[0031] FIG. 1 shows a diagram of a system for creating a combined electronic identification and for allowing a transaction by a user to proceed;

[0032] FIG. 2A shows a flow diagram that illustrates the process of creating a combined electronic identification from both the user side and the server side;

[0033] FIG. 2B shows a flow diagram that illustrates the process of creating a combined electronic identification from both the user side and the server side;

[0034] FIG. 3A shows a flow diagram that illustrates the process of allowing a transaction by a user to proceed from both the user side and the server side;

[0035] FIG. 3B shows a flow diagram that illustrates the process of allowing a transaction by a user to proceed from both the user side and the server side;

[0036] FIG. 4A shows a diagram of a system and method for performing a transaction with a computer and a smartphone from both the user side and the server side;

[0037] FIG. 4B shows a version of the invention for performing a transaction with a computer and a smartphone from both the user side and the server side; and

[0038] FIG. 4C shows a version of the invention for performing a transaction with a computer and a smartphone from both the user side and the server side.

DESCRIPTION

[0039] Methods and systems that implement the embodiments of the various features of the invention will now be described with reference to the drawings. The drawings and the associated descriptions are provided to illustrate embodiments of the invention and not to limit the scope of the invention. Reference in the specification to "one embodiment", "an embodiment", or "one version" is intended to indicate that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least an embodiment of the invention. The appearances of the phrase "in one embodiment", "an embodiment", or "one version" in various places in the specification are not necessarily all referring to the same embodiment.

[0040] Throughout the drawings, reference numbers are re-used to indicate correspondence between referenced elements. In addition, the first digit of each reference number indicates the figure where the element first appears.

[0041] As used in this disclosure, except where the context requires otherwise, the term "comprise" and variations of the term, such as "comprising", "comprises", and "comprised" are not intended to exclude other additives, components, integers or steps.

[0042] In the following description, specific details are given to provide a thorough understanding of the embodiments. However, it will be understood by one of ordinary skill in the art that the embodiments may be practiced without these specific details. Well-known circuits, structures and techniques may not be shown in detail in order not to obscure the embodiments. For example, circuits may be shown in block diagrams in order not to obscure the embodiments in unnecessary detail.

[0043] Also, it is noted that the embodiments may be described as a process that is depicted as a flowchart, a flow diagram, a structure diagram, or a block diagram. Although a flowchart may describe the operations as a sequential process, many of the operations can be performed in parallel or concurrently. In addition, the order of the operations may be rearranged. A process is terminated when its operations are completed. A process may correspond to a method, a function, a procedure, a subroutine, a subprogram, etc. When a process corresponds to a function, its termination corresponds to a return of the function to the calling function or the main function.

[0044] Moreover, storage may represent one or more devices for storing data, including read-only memory (ROM), random access memory (RAM), magnetic disk storage mediums, optical storage mediums, flash memory devices and/or other machine readable mediums for storing information. The term "machine readable medium" includes, but is not limited to portable or fixed storage devices, optical storage devices, wireless channels and various other mediums capable of storing, containing or carrying instruction(s) and/or data.

[0045] Furthermore, embodiments may be implemented by hardware, software, firmware, middleware, microcode, or a combination thereof. When implemented in software, firmware, middleware or microcode, the program code or code segments to perform the necessary tasks may be stored in a machine-readable medium such as a storage medium or other storage(s). One or more than one processor may perform the necessary tasks in series, concurrently or in parallel. A code segment may represent a procedure, a function, a subprogram, a program, a routine, a subroutine, a module, a software package, a class, or a combination of instructions, data structures, or program statements. A code segment may be coupled to another code segment or a hardware circuit by passing and/or receiving information, data, arguments, parameters, or memory contents. Information, arguments, parameters, data, etc. may be passed, forwarded, or transmitted through a suitable means including memory sharing, message passing, token passing, network transmission, etc.

[0046] In the following description, certain terminology is used to describe certain features of one or more embodiments of the invention.

[0047] "Transaction" means a communicative action or activity involving two parties or things that reciprocally affect or influence each other.

[0048] "Hardware profile" means data that is generated by a user with regard to a hardware device and at least some data specifically associated with and created by the user. As examples, it can be information relating to installed applications, portions of the user's contacts, applications added by the user, music added by the user, and the like.

[0049] Fig. 1 shows an embodiment of the present invention, depicting a system for creating a combined electronic identification and for allowing a transaction by a user to proceed, comprising a hardware device 100, an authentication server 102, and an evaluation server 104. The hardware device 100 is preferably any device configured with a touchscreen that has the ability to engage in secure wireless communications with various communication networks, such as cellular, satellite and the various forms of Internet connectivity. In one embodiment, the hardware device 100 is capable of capturing biometric input including, but not limited to, fingerprint, facial recognition, voice verification, and vein verification.

[0050] In another embodiment, the hardware device 100 comprises a processor, memory, an input interface, and a transmitter, the processor being programmed to process through the input interface the user information, transmit through the transmitter the user information to a first server, receive through the transmitter authentication from a second server, and transmit through the transmitter the hardware profile to the first server to create a combined electronic identification. In one version of the invention, the hardware device 100 is a mobile phone, computer, or tablet computer. The input interface is preferably a touchscreen interface, and the transmitter is preferably a wireless communication module. Alternatively, the first and second server are the same server.

[0051] In one embodiment, the authentication server 102 comprises a processor, memory, an input interface, and a connection for receiving information executable by the processor, the processor being programmed to receive through the connection user information, authenticate the user from the user information, receive through the connection a hardware profile, store in memory the received user information and the received hardware profile, and link the user information and the hardware profile together as a combined electronic identification.

[0052] Preferably the authentication server 102 is an infrastructure as a service (IaaS) provider that includes at least two 64-bit high-CPU medium Amazon Elastic Compute Cloud (EC2) server instances to be used for active Mongo database hosts, which are connected to a load balancer, which is in turn connected to the client. Preferably, the authentication server 102 also includes 16 Elastic Block Store (EBS) volumes to be used in two redundant array of independent disks (RAID) 10 arrays to support active Mongo database servers, and one 64-bit micro instance to be used for Mongo Arbiter role.

[0053] Preferably, the evaluation server 104 can be associated with any third party authentication authority such as a credit information agency, such as, but not limited to, Experian.

[0054] Referring now to Figs. 2A and 2B, an embodiment of the present invention depicts a method of creating a combined electronic identification associated with a hardware device 100. A user first installs an application onto the hardware device and executes the application 200. The application is a program that is downloaded and installed onto the hardware device 100, and is used to create the combined electronic identification. The application obtains user information about the user of the device 202 by prompting the user to input user information 204 about the user on the device, including but not limited to, the user's e-mail address, password, name, address, home number, and mobile phone number. The e-mail address is checked with an authentication server to determine whether there is a conflicting e-mail that was previously registered 206.

[0055] In another version of the invention, the user information comprises information about the user selected from the group consisting of the user's (a) name, (b) the user's social security number, (c) national identification number, (d) passport number, (e) IP address, (f) vehicle registration number, (g) vehicle license plate number, (h) driver's license number, (i) appearance, (j) fingerprint, (k) handwriting, (l) credit card information, (m) bank account information, (n) digital identity, (o) date of birth, (p) birthplace, (q) past and current residence, (r) age, (s) gender, (t) marital status, (u) race, (v) names of schools attended, (w) workplace, (x) salary, (y) job position, (z) additional biometric data, and combinations of one or more thereof. All of this information, except for the password, can be automatically gathered by the application if it is already stored in the hardware device 100.

[0056] The user's name includes, but is not limited to, first, last, middle, and any nicknames, and portions thereof. The user's social security number and IP address include all or part of the number and combinations thereof. The user's national identification number, passport number, vehicle registration number, vehicle license plate number, and driver's license number include letters and symbols, in addition to numbers, and portions thereof. Biometric data includes, but is not limited to, fingerprint, handwriting, retina, appearance, and voice data. Credit card information includes all or part of the number, expiration date, issuing bank, type (e.g. Visa, MasterCard, Discover, or American Express) and combinations thereof. The user's digital identity includes characteristics and data attributes, such as a username and password for various online accounts (e.g. banking, social media, weblogs, e-mail, etc), online search activities (e.g. electronic transactions), medical history, purchasing history, purchasing behavior. A digital identity can also be linked to an e-mail address, URL, and domain name.

[0057] The hardware device stores the user information and obtains a hardware profile 208 of the hardware device 210, the hardware profile 208 comprising user generated data stored on the device 100. The hardware profile 208 includes, but is not limited to information on the hardware device selected from the group consisting of (a) contact information, (b) mobile network code, (c) information about music, (d) pixel colors from a background screen, (e) installed applications, (f) arrangement of the applications, (g) frequency of use of applications, (h) location of the user, (i) Bluetooth device pairings, (j) carrier name, (k) mobile country code, (l) phone number, (m) photos, (n) device name, (o) MAC address, (p) device type, and combinations of one or more thereof. The hardware profile 208 can also include portions of any of the above such as just a portion of the titles of some of the music on the device 100.

[0058] Contact information includes, but is not limited to, telephone numbers (home, work, and mobile), e-mail addresses (personal and work), addresses (home and work), and names (first, last, middle, and nickname) of contacts stored on the hardware device 100. Information about music includes, but is not limited to, song names, artist names, playlist names, songs in playlists, and duration of songs and playlists. Information about applications includes, but is not limited to, application names, size of applications, and version of applications. Information about photos includes, but is not limited to, photo names, photo locations, and photo sizes. Information about device type includes, but is not limited to, iPhone, iPad, Droid smartphone, and all other types of smartphones and tablet computers.

[0059] The hardware device 100 then sends the user information along with the hardware profile from the device to an authentication server 212 to create a combined electronic identification, the hardware profile 208 comprising user generated data stored on the device 100. In one version of the invention, the authentication server stores the user information and hardware profile and passes only portions of the received user information and none of the hardware information to an evaluation server 214. In order to authenticate the user from the user information, the evaluation server evaluates the information, and responds with an identity score based on the evaluation of the user provided information 216. The hardware device receives the authentication from the server. In the case the evaluation server is associated with Experian, a Precise ID (PID) score is received. In one case the identity score is a numerical representation (from 0 to 1000) of the likelihood the user is a fraud. The closer the identity score is to 1000, the less likely the user is a fraud. Preferably, the matter proceeds only if the identity score is over 660.

[0060] The authentication server stores the identity score 218 and uses it to create a confidence score 220, which is also stored on the authentication server. The confidence score is calculated using the identity score and the user information 220. The confidence score is a numerical representation of the likelihood the user is a fraud. If the confidence score is within accepted tolerances 222, the user information and the hardware profile are linked together to create the combined electronic identification that is stored on the hardware device and authentication server 224. The accepted tolerances are set according to the requirements of the transactions. For example, for lower value transactions the probability that it is an authenticated user may be set at 80%. For higher value transactions the probability that it is an authenticated user may be set at 99.999999%. Preferably, linking is done by concatenating the user information 202 and the hardware profile 208. The user is then notified of the authentication and creation of the combined electronic identification 226.

[0061] In one version of the invention at least one of the user information 202 and the hardware profile 208 are salted and hashed prior to linking. Alternatively, both the user information 202 and hardware profile 208 are salted and hashed prior to linking. Preferably, salting is done by a three to seven digit random number generator, and hashing is done by Secure Hash Algorithm-2 (SHA-2). The hash can be four digits of a 64 bit string. Preferably, the hardware profile 208 and user information 202 are salted and hashed before transfer to any external device. The salting and hashing can be by individual items or in groups of items.

[0062] In one version the hash is truncated to reduce the amount of information transmitted to a server. The truncation can be performed in such a way that sufficient information is retained to differentiate one user from another user.

[0063] In one version of the invention, if the confidence score is not within the accepted tolerances, a request is sent by the hardware device to the authentication server that further authentication is needed, and the authentication server receives the request 228. The authentication server then sends the request to the evaluation server, the evaluation server receives the request 230, and the evaluation server sends knowledge based questions (KBQ) to the authentication server 230, which sends the KBQ's to the hardware device 232. The knowledge questions are commonly used by credit agencies to verify a user's identity, and are commonly known in the art, e.g., "What was the color of your first car?" Preferably, the knowledge questions are sent in extensible markup language (XML) format. The user is presented with the knowledge questions, the user provides answers to the knowledge questions, and the answers are sent back to the evaluation server via the authentication server 234, 236. The evaluation server evaluates the answers and sends an updated identity score to the authentication server 238, which is then sent to the device 240. An updated confidence score is calculated using the updated identity score and the user information. If the updated confidence score is within accepted tolerances 242, the user information and the hardware profile are linked to create the combined electronic identification, which is stored on the hardware device 244, and the user is notified of the result 246. The accepted tolerances are set according to the requirements of the transactions. For example, for lower value transactions the probability that it is an authenticated user may be set at 80%. For higher value transactions the probability that it is an authenticated user may be set at 99.999999%. If the confidence score is not within accepted tolerances, the updated confidence score, user information, and hardware profile are deleted 248 and the user is notified that the authentication was denied 250.

[0064] Preferably, the confidence score determines the types of transactions that are available to the user, which includes consideration of the method by which the user was authenticated to create the combined electronic identification. For example, whether the user needed to answer KBQ's.

[0065] In one version of the invention, once the combined electronic identification is created, no personal identifying factors are retained or only a selected set is retained on the hardware device, such as the user's name and address.

[0066] Alternatively, instead of using an evaluation server 104, the user's identity can be verified by authenticating the user information against a private database or directory, including but not limited to, Lightweight Directory Access Protocol (LDAP) or Active Directory, as commonly known in the art. In another version of the invention, the user's identity can be verified by sending a one-time password to the user via voice call, SMS message, or e-mail, which is commonly known in the art.

[0067] Preferably, the above-described method is accomplished by executing the following algorithm:

[0068] I. User information

[0069] 1) Concatenate provided e-mail (SHA-2) and MAC address (SHA-2) and store. Include the salt: (SHA-2/123e-mailAddressSHA-2/321MACaddress). Salt is the extra digits appended to e-mail and MAC (123,321).

[0070] II. Generate confidence score

[0071] 1) User Activity

[0072] a) Did user perform an activity that enhances the confidence that they are the actual user of the device, such as selecting information already stored on the hardware device or whether the user is at a normal location consistent with their activities.

[0073] i) If yes, set variable DPID to 90%

[0074] ii) If no, set variable DPID to 70%

[0075] 2) Receive KBQ identity score from evaluation server.

[0076] a) If KBQ identity score is over 66, allow creation of combined electronic identification.

[0077] b) If KBQ identity score is below 66, deny creation of combined electronic identification.

[0078] 3) Calculate confidence score. Confidence score is stored on authentication server, never passed to hardware device.

[0079] a) Confidence Score = (PID from Experian * DPID) * (0.01*KBQ identity score)

[0080] b) Example: (630*0.9)*(0.01*73) = 413, where for purposes of this example 630 is a generic PID that is representative of the type of score that can be provided.

[0081] III. Hardware profile

[0082] 1) Initial and Subsequent State Characteristics

[0083] a) Device Characteristics

[0084] i) MAC address

[0085] ii) Device type – iPhone, iPad, etc. (*model)

[0086] iii) Device name (*name)

[0087] iv) Carrier name (*carrierName)

[0088] v) Mobile Country Code (*mcc)

[0089] vi) Mobile Network Code (*mnc)

[0090] b) Device Personality

[0091] i) Contacts using full name.

[0092] ii) Songs using full song names.

[0093] iii) Application names.

[0094] iv) Bluetooth device parings. (go over testing methods with Charles)

[0095] v) Photo names (as stored on device) (future development)

[0096] vi) Photo locations (future development)

[0097] 2) TraitWareID (TWID-Initial State) – Items sent to MongoDB

[0098] With the following items, create salted hashes with dynamic salt on the device and send to the server. In addition, store the salt independently on the device. Use a random five digit number for the salt.

[0099] a) Initial Database of Contacts (Full Name)

[00100] b) Initial Database of Song Titles (Use full titles)

[00101] c) Initial Database of Apps (App name)

[00102] d) Bluetooth Device Pairings

[00103] e) Device type – iPhone, iPad, etc. (*model)

[00104] f) Device name (*name)

[00105] g) Carrier name (*carrierName)

[00106] h) Mobile Country Code (*mcc)

[00107] i) Mobile Network Code (*mnc)

[00108] Referring now to Figs. 3A and 3B, an embodiment of the present invention, depicting a method of allowing a transaction by a user utilizing a stored electronic identification, the stored electronic identification comprising a first stored hardware profile and stored user information, the method comprising the steps of receiving user information and a hardware profile of hardware associated with the user, both hardware profiles comprising user generated data stored on the device, comparing the received user information and the received hardware profile against the stored electronic profile, wherein the received hardware profile and the stored hardware profile are different by at least 0.02%, and allowing the transaction to proceed only if the received hardware profile and the stored hardware profile match by at least 60% and the received user information and the stored user information match by at least 30% is shown.

[00109] In another version of the invention, an authentication server 102 comprises a processor, memory, and a connection for receiving information for processing by the processor, the memory storing a stored user information and a stored hardware profile, the processor being programmed to receive through the connection the received user information and the received hardware profile, compare the received user information and the received hardware profile against the stored hardware profile wherein the received hardware profile and the stored hardware profile are different by at least 0.02%, and execute the transaction if the received hardware profile and the stored hardware profile match by at least 60% and the received user information and the stored user information match by at least 30%.

[00110] First the user opens the application after being authenticated and having a combined electronic identification created by the steps described above 300. The user is then presented with an option to either delete the combined electronic identification 302-312, or to initiate a transaction 316. In the figure, the transaction depicted is an ATM withdrawal. In other embodiments, the transaction can be any type of transaction, including, but not limited to, financial transactions, accessing a file, logging into a website, opening a door to a business or house, starting a car, and being alerted to a washing machine reaching the end of its cycle.

[00111] If the user chooses to initiate a transaction, the hardware device's current hardware profile and user information are used to create a new combined electronic identification on the hardware device, and the new combined electronic identification is sent to an authentication server 318. The authentication server then compares the new combined electronic identification that was sent from the hardware device with a stored previously created combined electronic identification on the authentication server 320. If they do not match 322, the transaction does not proceed 324. If they match within a set tolerance, the current hardware profile and transaction details are sent to an authentication server 326. In one embodiment, the set tolerance is between 0.02% and 76%.

[00112] The authentication server then compares the received current hardware profile to a previously stored hardware profile 328. This is accomplished by calculating the percentage difference of the previously stored hardware profile with the received current hardware profile. If the percentage difference is not within a set tolerance 330, the transaction does not proceed 332. In one embodiment, the set tolerance for the hardware profile is between 0.02% and 76%. If the current hardware profile matches the previously stored hardware profile within the set tolerance, the transaction is allowed to proceed 334. Alternatively, the combined electronic identifications and the hardware profiles are sent together for evaluation by the authentication server at the same time. Preferably the percentage difference between the current user information and a previously stored user information is also between 0.02% and 76%.

[00113] Preferably the transaction is allowed to proceed only if the current hardware profile and the previously stored hardware profile are different by at least a factor which is a function of the time since the last transaction. For example, a transaction may not be allowed to proceed unless there is a 0.02% change in the hardware profile, which would represent a change in one of the user's characteristics after a week.

[00114] In one version of the invention, the transaction is not allowed to proceed if the received hardware profile and the stored hardware profile are identical, which could indicate a copied profile.

[00115] A new confidence score is generated by using the previously created combined electronic identification, the new combined electronic identification, the confidence score calculated based on the percent difference between the previously stored and current hardware profiles, and the previously calculated confidence score 335. The new confidence score is a numerical representation between 0 and 1 of the probability that the user is a fraud.

[00116] In one version multiple user hardware profiles are obtained for user information data and the percent differences between user hardware profiles are computed. The differences are used to create statistical distributions which can be used to create statistical probabilities by which a user data or information differs from another user and which can be used to determine that a device to which a user has been assigned is statistically different from another user. This information can be used to determine that a particular device belongs to a particular user.

[00117] In one version of the invention, the percent differences between user hardware profiles are computed using the Levenshtein Distance equation, which defines the distance between two strings a, b is given by $\operatorname{lev}_{a,b}(|a|, |b|)$ where:

$$\operatorname{lev}_{a,b}(i,j) = \begin{cases} \max(i,j) & , \min(i,j) = 0 \\ \min \begin{cases} \operatorname{lev}_{a,b}(i-1,j) + 1 \\ \operatorname{lev}_{a,b}(i,j-1) + 1 \\ \operatorname{lev}_{a,b}(i-1,j-1) + [a_i \neq b_j] \end{cases} & , \text{ else} \end{cases}$$

[00118] The new confidence score is checked to determine if it is within a set tolerance 336. Preferably, the set tolerance is 99.999999%, so that the transaction proceeds only if the new confidence score is over 99.999999%. If it is not, then additional steps need to be taken to increase the new confidence score, such as prompting the user for a password or biometric authentication 338-350. If the confidence score is unable to be increased, the transaction is not allowed to proceed 352, 354.

[00119] If the new confidence score is within the set tolerance, the new combined electronic identification replaces the stored combined electronic identification on the authentication server and the transaction is allowed to be completed 356-360.

[00120] In another version of the invention, the transaction is allowed to proceed only if the received hardware profile and the stored hardware profile match by at least 40%. Alternatively, the transaction is allowed to proceed only if the received hardware profile and the stored hardware profile match by at least 50%. In another version the transaction is allowed to proceed only if the received hardware profile and the stored hardware profile are different by at least 1%.

[00121] It has been found that, though there will be changes in the user information and the hardware profile, individuals are sufficiently unique that a particular user can still be identified by the user information and the hardware profile to a high probability. The data shows that even if the received hardware profile and the stored hardware profile differ by 44%, there is still only a 1 in 360 billion chance that it is not the same device. If the data were to change by 60% there would be still be a 99.99% chance that the device is the same. Even a 76% difference corresponds to a 1 in 3 probability. In regards to the current invention, using the user information and the hardware profile results in differentiation of an individual device to greater than 1 in 500 million.

[00122] Figs. 4A through 4F depict systems and methods for a user to perform a transaction with an electronic communication device 400, 402 comprising the steps of salting and hashing a hardware profile 208 of the electronic communication device 400, 402 with user information 204 stored on the device, the hardware profile comprising user generated data stored on the device, sending the salted and hashed hardware profile 208 and user information 204 to a server 404, and receiving instructions from the server 404 regarding whether or not to proceed with the transaction.

[00123] Preferably, salting is done by a three to seven digit random number generator, and hashing is done by SHA-2.

[00124] Preferably, the steps further comprise entering a security pin to verify the user. The security pin can be any arrangement of numerical digits that is well-known in the art.

[00125] In one version of the invention, a method for a user to perform a transaction utilizing a first electronic communication device 400 comprises the steps of connecting with a transaction receiver, receiving from the transaction receiver electronic data for a second electronic communication device 402 different from the first electronic communication device 400, the second electronic communication device 402 having a user associated therewith and a hardware profile 208 associated therewith, the hardware profile 208 comprising user generated data stored on the second electronic communication device 402, sending with the second electronic communication device 402 at least part of the received electronic data, user information 204 of the user, and the hardware profile 208 to an authentication server 404, and if the authentication server 404 authenticates the sent user information 206, the hardware profile 208, and the sent electronic data, performing the transaction with the first electronic communication device 400. Preferably, the method includes the step of authenticating with the authentication server 404. Preferably, the transaction receiver is a secure website that uses the methods described above in Figs. 3A and 3B for authenticating a combined electronic identification for accessing the secure website.

[00126] In one version the first electronic communication device 400 comprises a visual display, wherein the visual display is read with the second electronic communication device 402.

[00127] In another version the second electronic communication device 402 comprises a visual display, wherein the visual display is read with the first electronic communication device 400.

[00128] Preferably, the visual display is a Quick Response (QR) code.

[00129] In one embodiment, a method of performing a transaction for a user using a first electronic communication device 400 to perform the transaction comprises the steps of receiving information from the first electronic communication device 400, transmitting electronic data to the user, receiving from a second electronic communication device 402 of the user at least part of the transmitted electronic data, user information 204 associated with the second electronic communication device 402, and a hardware profile 208 of the second electronic communication device 402, the hardware profile comprising user generated data stored on the second electronic communication device 402, and determining if the received electronic data, user information 204 and hardware profile 208 are authentic, and if authentic, permitting the user to perform the transaction with the first electronic communication device 400.

[00130] In one version of the invention, the method comprises the additional step of permitting the user to perform the transaction.

[00131] In one version of the invention, if the received electronic data, user information 204 and hardware profile 208 are authentic, the method comprises the additional step of performing the transaction for the user.

[00132] In another embodiment, a system for performing a transaction for a user using a first electronic communication device 400 to perform the transaction comprises a processor, memory, and a connection for receiving information executable by the processor, the memory storing electronic data, the processor being programmed to receive through the connection information from the first electronic communication device 400, transmit through the connection the stored electronic data to the user, receive through the connection from the second electronic communication device 402 at least part of the transmitted electronic data, user information 204 associated with the second communication device 402, and hardware profile 208 of the second communication device 402, and determine if the received electronic data, user information 204 and hardware profile 208 are authentic, and if authentic, permitting the user to perform the transaction with the first electronic communication device 400.

[00133] In one version of the invention, if the received electronic data, user information 204 and hardware profile 208 are authentic, the processor is programmed to send through the connection to the first electronic communication device 400 a response regarding whether or not to perform the transaction.

[00134] Fig. 4A depicts a system of performing a transaction with a first electronic communication device 400 and a second electronic communication device 402. Preferably, the first electronic communication device 400 is a desktop computer and the second electronic communication device 402 is a smartphone. The desktop computer can be a public computer, a workplace computer, or any computer not used by the user in relation to creating or authenticating a combined electronic identification. The smartphone has previously been used to create a combined electronic identification according to the methods described above in Figs. 2A and 2B, and has a combined electronic identification associated with it. The first electronic communication device 400 and the second electronic communication device 402 each comprise a processor, memory, and a connection for receiving and transmitting information executable by the processor. The system further comprises an authentication server 404 and a webserver 406.

[00135] Fig. 4D describes a method of performing a transaction with a first electronic communication device 400 and a second electronic communication device 402. A user first navigates to a secure website which uses the methods described above in Figs. 3A and 3B for authenticating a combined electronic identification for accessing the secure website 408. The user is presented with a visual display on the desktop computer, the visual display containing information about the website and the computer requesting access 410. Preferably, the visual display is a Quick Response (QR) code. In another version of the invention, the user receives a wireless signal instead of a visual display. The wireless signal can be of any type known in the art, including, but not limited to, near field communication (NFC) and Bluetooth. The information presented in the visual display or wireless signal may consist of, but is not limited to, the website URL, a geographic location, the IP address of the computer, a time stamp, and a date stamp.

[00136] The user scans the visual display with a program stored on the smartphone 412. Most smartphones come equipped with a program that uses a camera 403 on the smartphone to scan visual displays or other objects. The smartphone transmits the encoded information in the visual display along with the combined electronic identification to an authentication server 414. In the version where a wireless signal is used, the smartphone transmits the encoded information in the wireless signal along with the combined electronic identification to the authentication server.

[00137] The authentication server receives the encoded information and the combined electronic identification and analyzes the received encoded information and combined electronic identification to determine if the user has the necessary rights to access the secure website using the authentication method described above in Figs. 3A and 3B 416. Preferably, the authentication process uses information such as a previously created combined electronic identity and a confidence score, which are stored on the authentication server or on the webserver.

[00138] The authentication server sends a response to a webserver 418 which then grants or denies access to the secure website 420. The response is displayed to the user on the desktop computer either allowing or denying the user access to the secure website.

[00139] In one version of the invention involving high security access, the user will have to use a biometric whose characteristics were previously stored on the smartphone, authentication server, or webserver to either access the smartphone or access the program used to read the QR code.

[00140] Figs. 4B and 4E show another version of the invention, where a user scans a visual display generated by a secure website on a first electronic communication device with a second electronic communication device 422-426, and the second electronic communication device determines if the second electronic communication device has the appropriate credentials to access the secured website 428. The visual display contains encoded information about the website and the computer requesting access. Preferably, the first electronic communication device 400 is a desktop computer and the second electronic communication device 402 is a smartphone. The desktop computer can be a public computer, a workplace computer, or any computer not used by the user in relation to creating or authenticating a combined electronic identification. Preferably the desktop computer has a webcam 401 that is programmed to recognize QR codes. The smartphone has previously been used to create a combined electronic identification according to the methods described above in Figs. 2A and 2B, and has a combined electronic identification associated with it.

[00141] If the smartphone has the appropriate credentials, the smartphone generates a visual display 430 which is scanned by the desktop computer to grant access to the secure website 432. The authentication process is the same as that described above for Figs. 3A and 3B. Preferably, the visual display is a QR code. In another version of the invention, the user receives a wireless signal instead of a visual display. The wireless signal can be of any type known in the art, including, but not limited to, NFC and Bluetooth. The encoded information may contain, but is not limited to, login credentials, a geographic location, a confidence score, a time stamp, and a date stamp.

[00142] In one version of the invention involving high security access, the user will have to use a biometric whose characteristics were previously stored on the smartphone, an authentication server, or a webserver to either access the smartphone or access the program used to read the QR code.

[00143] Figs. 4C and 4F show another version of the invention, where a user's smartphone, which has been previously authenticated according to the method described above in Figs. 1-3, creates a QR code, or sends a wireless signal using NFC or Bluetooth, which contains encoded information about the user 434. The encoded information presented in the QR or wireless signal, includes, but is not limited to, a name, a geographic location, a time stamp, and a date stamp. The encoded information is for one-time use.

[00144] When the QR or other encoded information is created on the device, the device also sends the encoded information to an authentication server along with a combined electronic identification associated with the smartphone 436. The authentication server analyzes the combined electronic identification and matches the encoded information to an account of the user in order to authenticate the user. When a desktop computer scans the QR code or receives the wireless signal created by smartphone 438, the desktop computer sends the encoded message to a webserver 440. The desktop computer can be a public computer, a workplace computer, or any computer not used by the user in relation to creating or authenticating a combined electronic identification. Preferably the desktop computer has a webcam that is programmed to recognize QR codes.

[00145] The webserver queries the authentication server regarding whether the user is authenticated based on the encoded information and the combined electronic identification 442. The authentication server responds to the webserver to either grant or deny access to a secure website 444. The webserver then grants or denies access to the secure website 446.

[00146] In one version of the invention involving high security access, the user will have to use a biometric whose characteristics were previously stored on the smartphone, authentication server, or webserver to either access the smartphone or access the program used to read the QR code.

[00147] Although the present invention has been discussed in considerable detail with reference to certain preferred embodiments, other embodiments are possible. For example, the visual display can be a bar code. Therefore, the scope of the appended claims should not be limited to the description of preferred embodiments contained in this disclosure.

[00148] All the features disclosed in this specification (including any accompanying claims, abstract, and drawings) can be replaced by alternative features serving the same, equivalent or similar purpose, unless each feature disclosed is one example only of a generic series of equivalent or similar features.

What is claimed is:

1. A method for creating a combined electronic identification associated with a hardware device comprising the steps of:

a) obtaining user information about a user of the device;

b) authenticating the user from the user information;

c) obtaining a hardware profile of the device, the hardware profile comprising user generated data stored on the device; and

d) linking the user information and the hardware profile as a combined electronic identification.

2. A method for creating a combined electronic identification associated with a hardware device comprising the steps of:

a) inputting user information about a user on the device;

b) sending the user information from the device to a server;

c) receiving authentication from the server; and

d) sending a hardware profile from the device to the server to create a combined electronic identification, the hardware profile comprising user generated data stored on the device.

3. The invention of claim 1 or 2 wherein the hardware profile comprises information on the hardware device selected from the group consisting of (a) contact information, (b) mobile network code, (c) information about music, (d) pixel colors from a background screen, (e) installed applications, (f) arrangement of the applications, (g) frequency of use of applications, (h) location of the user, (i) Bluetooth device pairings, (j) carrier name, (k) mobile country code, (l) phone number, (m) photos, (n) device name, (o) MAC address, (p) device type, and combinations of one or more thereof.

4. The invention of claim 1 or 2 wherein the user information comprises information about the user selected from the group consisting of the user's (a) name, (b) the user's social security number, (c) national identification number, (d) passport number, (e) IP address, (f) vehicle registration number, (g) vehicle license plate number, (h) driver's license number, (i) appearance, (j) fingerprint, (k) handwriting, (l) credit card information, (m) bank account

information, (n) digital identity, (o) date of birth, (p) birthplace, (q) past and current residence, (r) age, (s) gender, (t) marital status, (u) race, (v) names of schools attended, (w) workplace, (x) salary, (y) job position, (z) additional biometric data, and combinations of one or more thereof.

5. The invention of claim 1 or 2 wherein at least one of the user information and the hardware profile are salted and hashed prior to linking.

6. The invention of claim 5 wherein both the user information and the hardware profile are salted and hashed prior to linking.

7. The invention of claim 6 wherein salting is done by a three to seven digit random number generator, and hashing is done by SHA-2.

8. The method of claim 1 wherein the step of linking comprises concatenating the user information and the hardware profile.

9. A system for performing the method of claim 1 comprising a processor, memory, and a connection for receiving information executable by the processor, the processor being programmed to:

a) receive through the connection the user information;

b) authenticate the user from the user information;

c) receive through the connection the hardware profile;

d) store in memory the received user information and the received hardware profile; and

e) link the user information and the hardware profile together as a combined electronic identification.

10. A system for performing the method of claim 2 comprising a processor, memory, an input interface, and a transmitter, the processor being programmed to:

a) process through the input interface the user information;

b) transmit through the transmitter the user information to a first server;

c) receive through the transmitter authentication from a second server; and

d) transmit through the transmitter the hardware profile to the first server to create a combined electronic identification.

11. The system of claim 10 wherein the first and second servers are the same server.

12. A method of allowing a transaction by a user utilizing a stored electronic identification, the stored electronic identification comprising a first stored hardware profile and stored user information, the method comprising the steps of:

a) receiving user information and a hardware profile of hardware associated with the user, both hardware profiles comprising user generated data stored on the device;

b) comparing the received user information and the received hardware profile against the stored electronic profile, wherein the received hardware profile and the stored hardware profile are different by at least 0.02%; and

c) allowing the transaction to proceed only if the received hardware profile and the stored hardware profile match by at least 60% and the received user information and the stored user information match by at least 30%.

13. The method of claim 12 wherein the transaction proceeds only if the received hardware profile and the stored hardware profile match by at least 40%.

14. The method of claim 12 wherein the transaction proceeds only if the received hardware profile and the stored hardware profile match by at least 50%.

15. The method of claim 12 wherein the received hardware profile and the stored hardware profile are different by at least 1%.

16. The method of claim 15 wherein the transaction proceeds only if the received hardware profile and the stored hardware profile match by at least 40%.

17. The method of claim 15 wherein the transaction proceeds only if the received hardware profile and the stored hardware profile match by at least 50%.

18. A system for performing the method of claim 12 comprising a processor, memory, and a connection for receiving information for processing by the processor, the memory storing the stored user information and the stored hardware profile, the processor being programmed to:

a) receive through the connection the received user information and the received hardware profile;

b) compare the received user information and the received hardware profile against the stored hardware profile wherein the received hardware profile and the stored hardware profile are different by at least 0.02%; and

c) execute the transaction if the received hardware profile and the stored hardware profile match by at least 60% and the received user information and the stored user information match by at least 30%.

19. A method for a user to perform a transaction with an electronic communication device comprising the steps of:

a) salting and hashing a hardware profile of the electronic communication device with user information stored on the device, the hardware profile comprising user generated data stored on the device;

b) sending the salted and hashed hardware profile and the user information to a server; and

c) receiving instructions from the server regarding whether or not to proceed with the transaction.

20. The method of claim 19 wherein salting is done by a three to seven digit random number generator, and hashing is done by SHA-2.

21. The method of claim 19 further comprising the step of entering a security pin to verify the user.

22. A method for a user to perform a transaction utilizing a first electronic communication device comprising the steps of:

a) connecting with a transaction receiver;

b) receiving from the transaction receiver electronic data for a second electronic communication device different from the first electronic communication device, the second electronic communication device having a user associated therewith and a hardware profile associated therewith, the hardware profile comprising user generated data stored on the second electronic communication device;

c) sending with the second electronic communication device at least part of the received electronic data, user information of the user, and the hardware profile to an authentication server; and

d) if the authentication server authenticates the sent user information, the hardware profile, and the sent electronic data, performing the transaction with the first electronic communication device.

23. The method of claim 22 wherein the step of authenticating with the authentication server is performed before step d).

24. The method of claim 22 wherein the first electronic communication device comprises a visual display, and step (b) further comprises reading the visual display with the second electronic communication device.

25. The method of claim 22 wherein the second electronic communication device comprises a visual display, and step (b) further comprises the step of reading the visual display with the first electronic communication device.

26. The method of claim 24 or 25 wherein the visual display is a Quick Response (QR) code.

27. A method of performing a transaction for a user using a first electronic communication device to perform the transaction comprising the steps of:

a) receiving information from the first electronic communication device;

b) transmitting electronic data to the user;

c) receiving from a second electronic communication device of the user at least part of the transmitted electronic data, user information associated with the second electronic communication device, and a hardware profile of the second electronic communication device, the hardware profile comprising user generated data stored on the second electronic communication device; and

d) determining if the received electronic data, user information and hardware profile are authentic, and if authentic, permitting the user to perform the transaction with the first electronic communication device.

28. The method of claim 27 wherein the user is permitted to perform the transaction.

29. The method of claim 27 wherein the received electronic data, user information and hardware profile are authentic, the method comprising the additional step of performing the transaction for the user.

30. A system for performing the method of claim 27 comprising a processor, memory, and a connection for receiving information executable by the processor, the memory storing electronic data, the processor being programmed to:

a) receive through the connection information from the first electronic communication device;

b) transmit through the connection the stored electronic data to the user;

c) receive through the connection from the second electronic communication device at least part of the transmitted electronic data, user information associated with the second communication device, and hardware profile of the second electronic communication device; and

d) determine if the received electronic data, user information and hardware profile are authentic, and if authentic, permitting the user to perform the transaction with the first electronic communication device.

31. The system of claim 30 wherein the received electronic data, user information and hardware profile are authentic, the processor being programmed to:

e) send through the connection to the first electronic communication device a response regarding whether or not to perform the transaction.

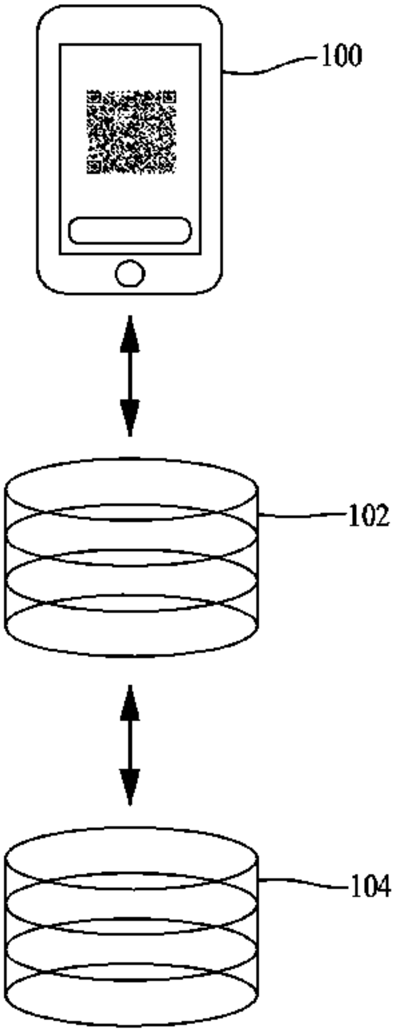


FIG. 1

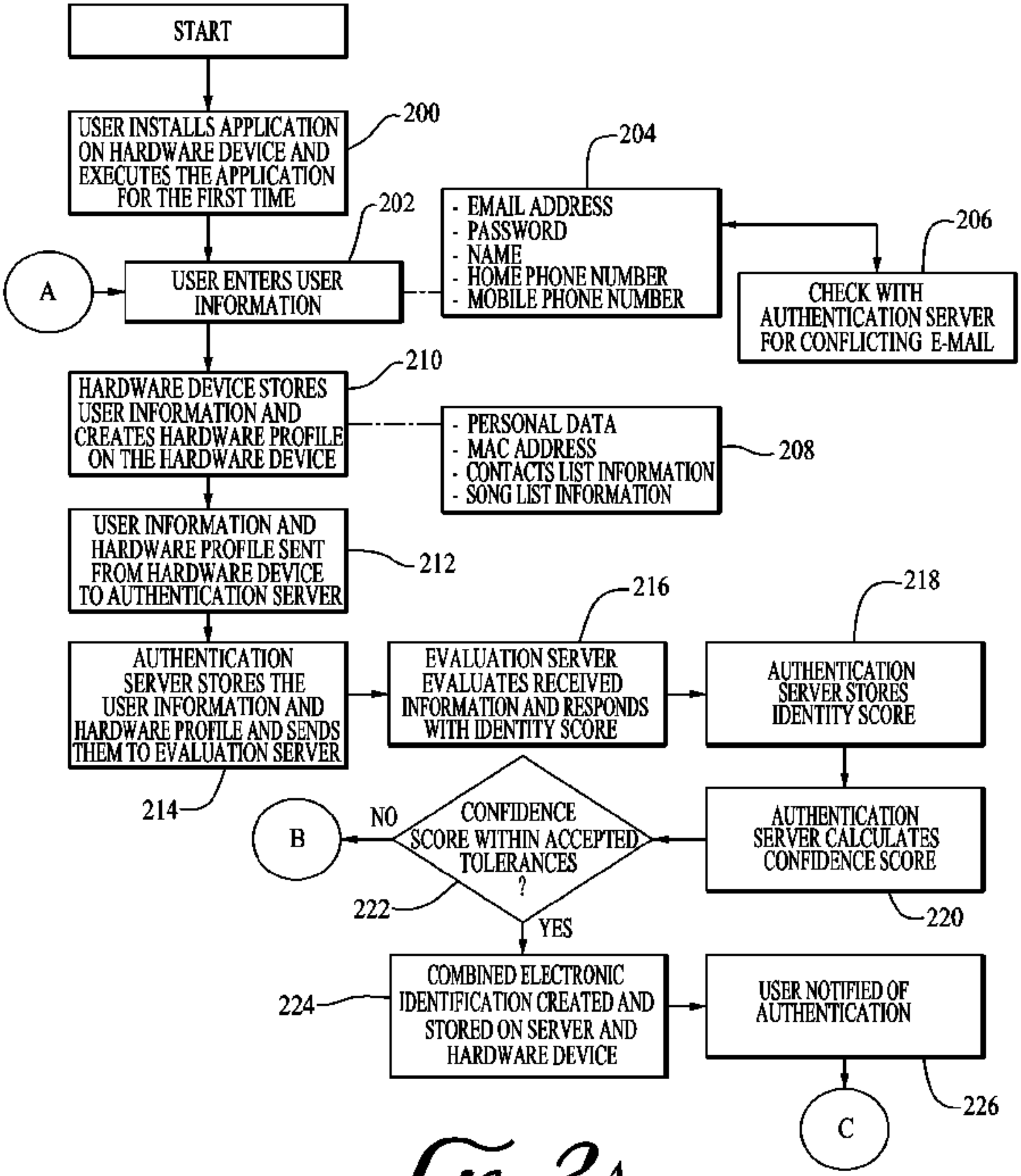

START
USER INSTALLS APPLICATION ON HARDWARE DEVICE AND EXECUTES THE APPLICATION FOR THE FIRST TIME
200
204
202
- EMAIL ADDRESS
- PASSWORD
- NAME
- HOME PHONE NUMBER
- MOBILE PHONE NUMBER
206
A
USER ENTERS USER INFORMATION
CHECK WITH AUTHENTICATION SERVER FOR CONFLICTING E-MAIL
210
HARDWARE DEVICE STORES USER INFORMATION AND CREATES HARDWARE PROFILE ON THE HARDWARE DEVICE
- PERSONAL DATA
- MAC ADDRESS
- CONTACTS LIST INFORMATION
- SONG LIST INFORMATION
208
USER INFORMATION AND HARDWARE PROFILE SENT FROM HARDWARE DEVICE TO AUTHENTICATION SERVER
212
216
218
AUTHENTICATION SERVER STORES THE USER INFORMATION AND HARDWARE PROFILE AND SENDS THEM TO EVALUATION SERVER
EVALUATION SERVER EVALUATES RECEIVED INFORMATION AND RESPONDS WITH IDENTITY SCORE
AUTHENTICATION SERVER STORES IDENTITY SCORE
214
NO
B
CONFIDENCE SCORE WITHIN ACCEPTED TOLERANCES ?
AUTHENTICATION SERVER CALCULATES CONFIDENCE SCORE
222
YES
220
224
COMBINED ELECTRONIC IDENTIFICATION CREATED AND STORED ON SERVER AND HARDWARE DEVICE
USER NOTIFIED OF AUTHENTICATION
226
C

FIG. 2A

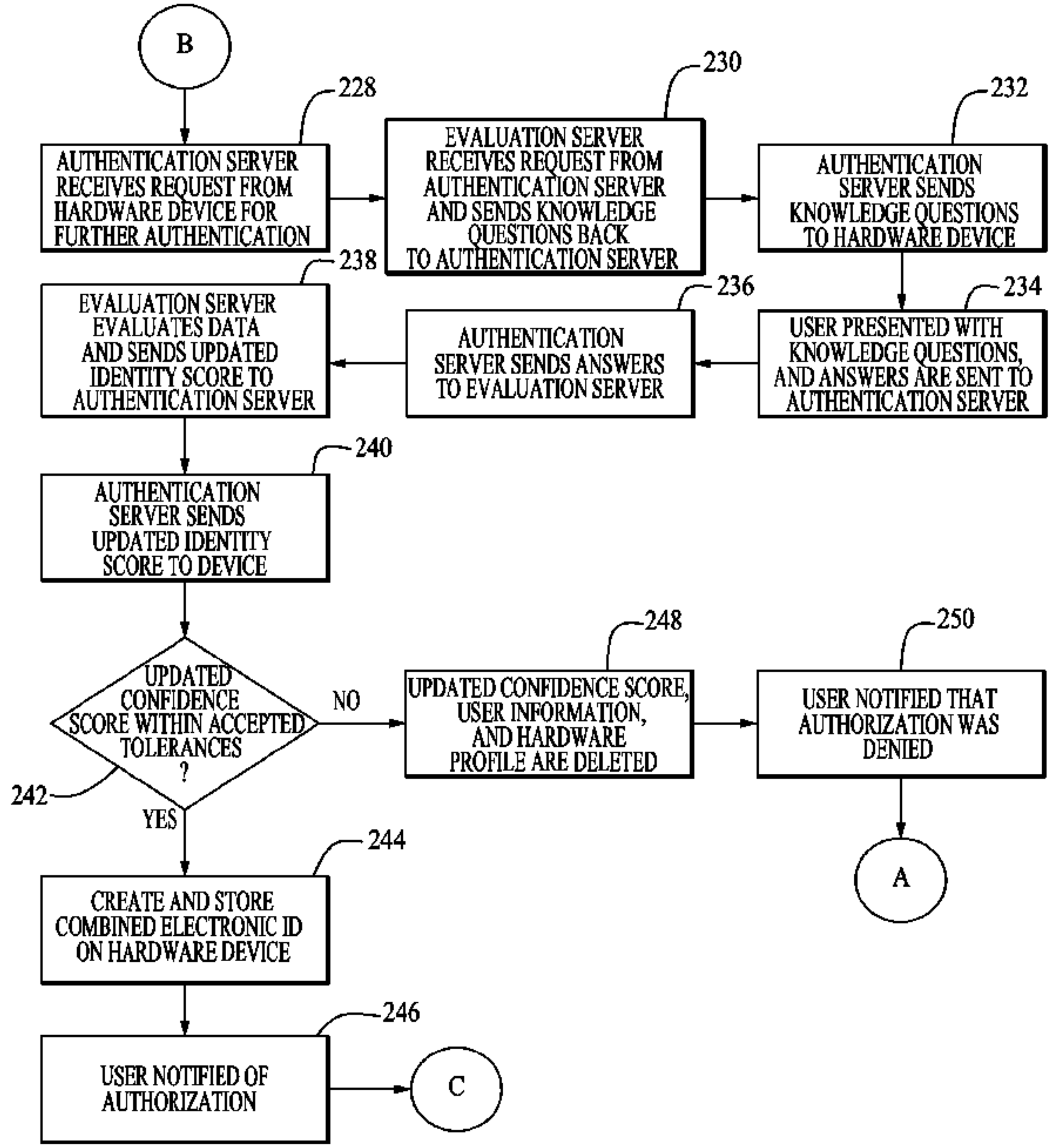

B
228
AUTHENTICATION SERVER RECEIVES REQUEST FROM HARDWARE DEVICE FOR FURTHER AUTHENTICATION
230
EVALUATION SERVER RECEIVES REQUEST FROM AUTHENTICATION SERVER AND SENDS KNOWLEDGE QUESTIONS BACK TO AUTHENTICATION SERVER
232
AUTHENTICATION SERVER SENDS KNOWLEDGE QUESTIONS TO HARDWARE DEVICE
234
USER PRESENTED WITH KNOWLEDGE QUESTIONS, AND ANSWERS ARE SENT TO AUTHENTICATION SERVER
236
AUTHENTICATION SERVER SENDS ANSWERS TO EVALUATION SERVER
238
EVALUATION SERVER EVALUATES DATA AND SENDS UPDATED IDENTITY SCORE TO AUTHENTICATION SERVER
240
AUTHENTICATION SERVER SENDS UPDATED IDENTITY SCORE TO DEVICE
242
UPDATED CONFIDENCE SCORE WITHIN ACCEPTED TOLERANCES ?
NO
248
UPDATED CONFIDENCE SCORE, USER INFORMATION, AND HARDWARE PROFILE ARE DELETED
250
USER NOTIFIED THAT AUTHORIZATION WAS DENIED
A
YES
244
CREATE AND STORE COMBINED ELECTRONIC ID ON HARDWARE DEVICE
246
USER NOTIFIED OF AUTHORIZATION
C

FIG. 2B

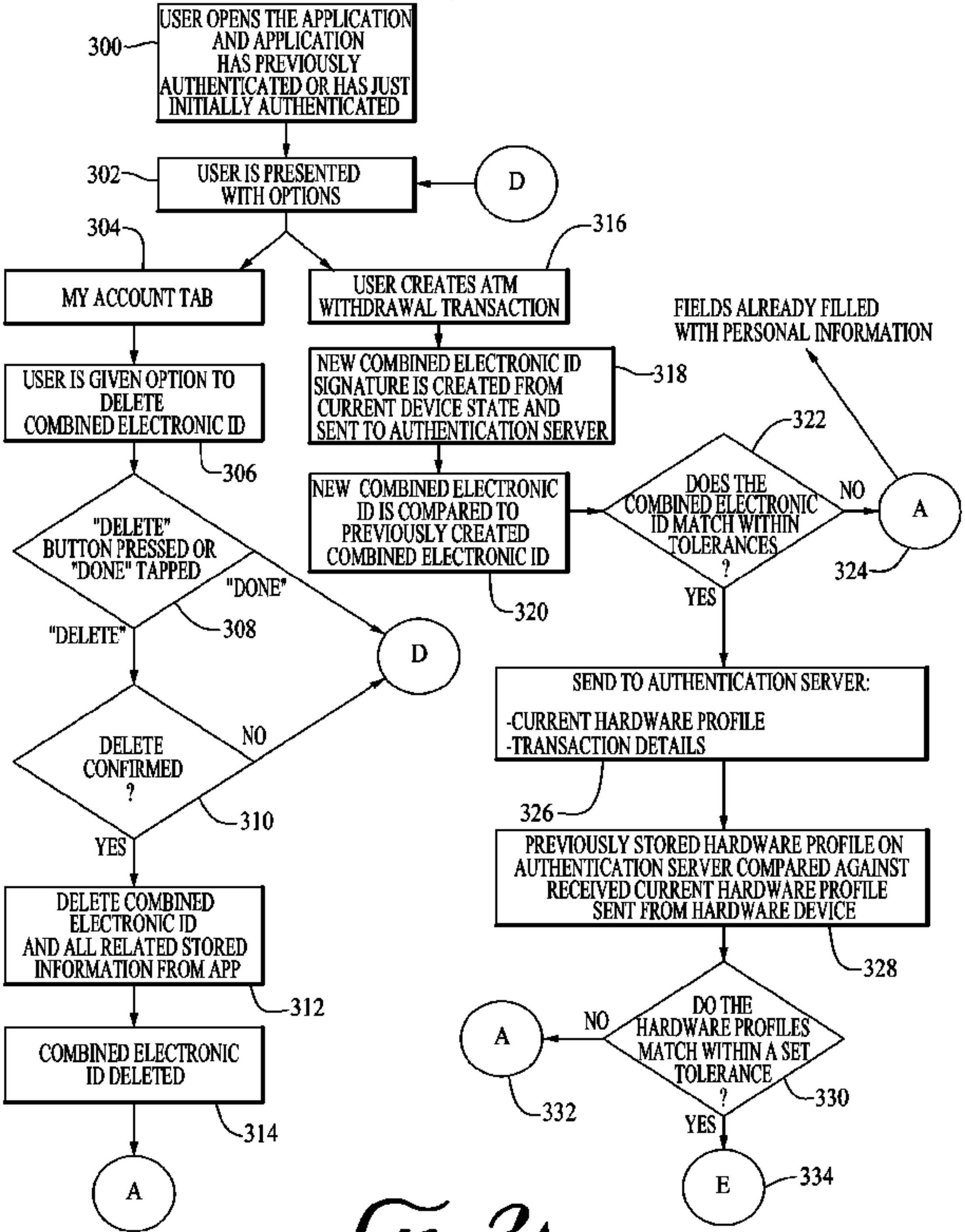

300
USER OPENS THE APPLICATION AND APPLICATION HAS PREVIOUSLY AUTHENTICATED OR HAS JUST INITIALLY AUTHENTICATED
302
USER IS PRESENTED WITH OPTIONS
D
304
MY ACCOUNT TAB
316
USER CREATES ATM WITHDRAWAL TRANSACTION
USER IS GIVEN OPTION TO DELETE COMBINED ELECTRONIC ID
306
NEW COMBINED ELECTRONIC ID SIGNATURE IS CREATED FROM CURRENT DEVICE STATE AND SENT TO AUTHENTICATION SERVER
318
FIELDS ALREADY FILLED WITH PERSONAL INFORMATION
322
"DELETE" BUTTON PRESSED OR "DONE" TAPPED
"DONE"
"DELETE"
308
D
NEW COMBINED ELECTRONIC ID IS COMPARED TO PREVIOUSLY CREATED COMBINED ELECTRONIC ID
320
DOES THE COMBINED ELECTRONIC ID MATCH WITHIN TOLERANCES ?
NO
A
324
YES
DELETE CONFIRMED ?
NO
310
YES
SEND TO AUTHENTICATION SERVER:
-CURRENT HARDWARE PROFILE
-TRANSACTION DETAILS
326
PREVIOUSLY STORED HARDWARE PROFILE ON AUTHENTICATION SERVER COMPARED AGAINST RECEIVED CURRENT HARDWARE PROFILE SENT FROM HARDWARE DEVICE
328
DELETE COMBINED ELECTRONIC ID AND ALL RELATED STORED INFORMATION FROM APP
312
COMBINED ELECTRONIC ID DELETED
314
A
A
NO
DO THE HARDWARE PROFILES MATCH WITHIN A SET TOLERANCE ?
330
332
YES
E
334

FIG. 3A

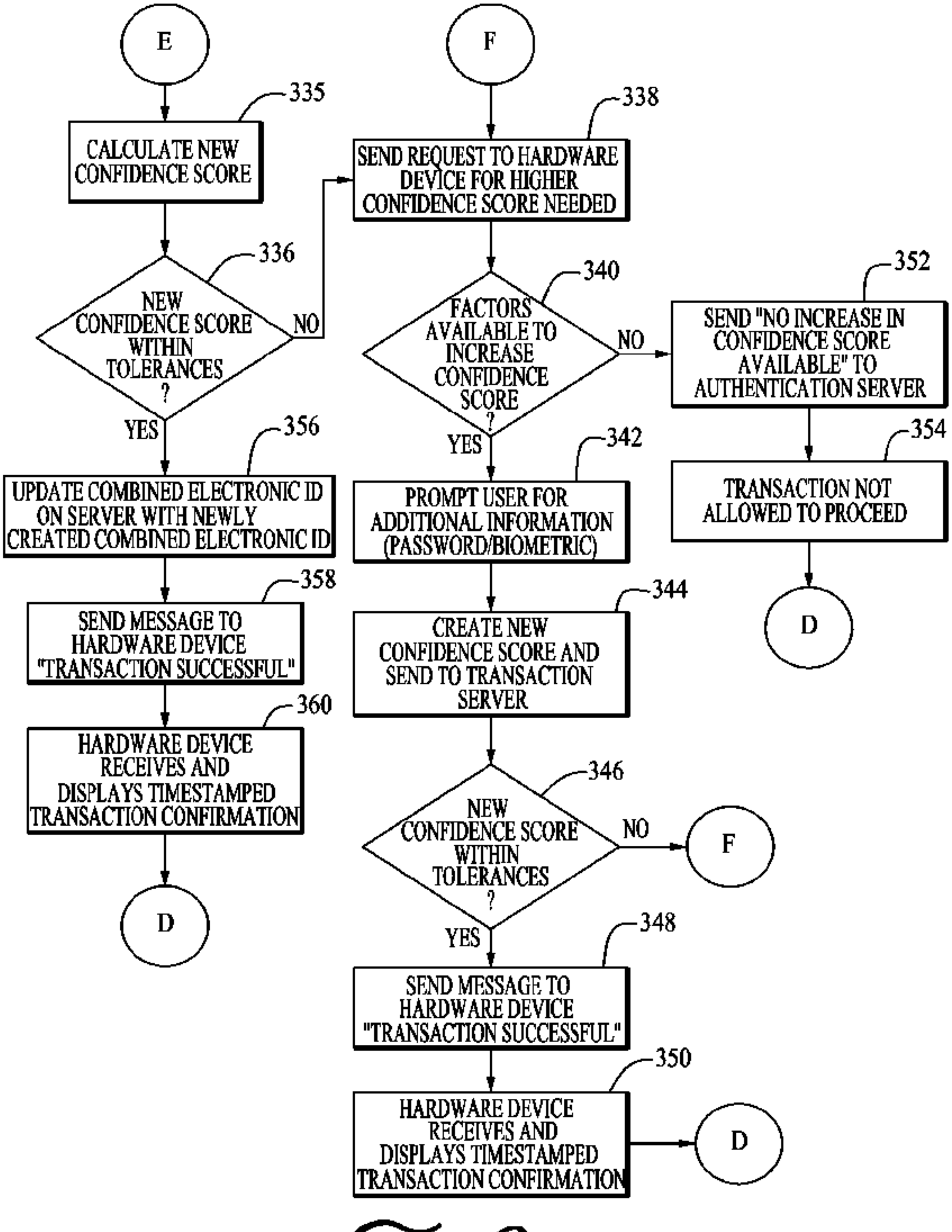

E
F
335
CALCULATE NEW CONFIDENCE SCORE
336
NEW CONFIDENCE SCORE WITHIN TOLERANCES ?
NO
YES
338
SEND REQUEST TO HARDWARE DEVICE FOR HIGHER CONFIDENCE SCORE NEEDED
340
FACTORS AVAILABLE TO INCREASE CONFIDENCE SCORE ?
NO
YES
352
SEND "NO INCREASE IN CONFIDENCE SCORE AVAILABLE" TO AUTHENTICATION SERVER
354
TRANSACTION NOT ALLOWED TO PROCEED
D
356
UPDATE COMBINED ELECTRONIC ID ON SERVER WITH NEWLY CREATED COMBINED ELECTRONIC ID
358
SEND MESSAGE TO HARDWARE DEVICE "TRANSACTION SUCCESSFUL"
360
HARDWARE DEVICE RECEIVES AND DISPLAYS TIMESTAMPED TRANSACTION CONFIRMATION
D
342
PROMPT USER FOR ADDITIONAL INFORMATION (PASSWORD/BIOMETRIC)
344
CREATE NEW CONFIDENCE SCORE AND SEND TO TRANSACTION SERVER
346
NEW CONFIDENCE SCORE WITHIN TOLERANCES ?
NO
F
YES
348
SEND MESSAGE TO HARDWARE DEVICE "TRANSACTION SUCCESSFUL"
350
HARDWARE DEVICE RECEIVES AND DISPLAYS TIMESTAMPED TRANSACTION CONFIRMATION
D

FIG. 3B

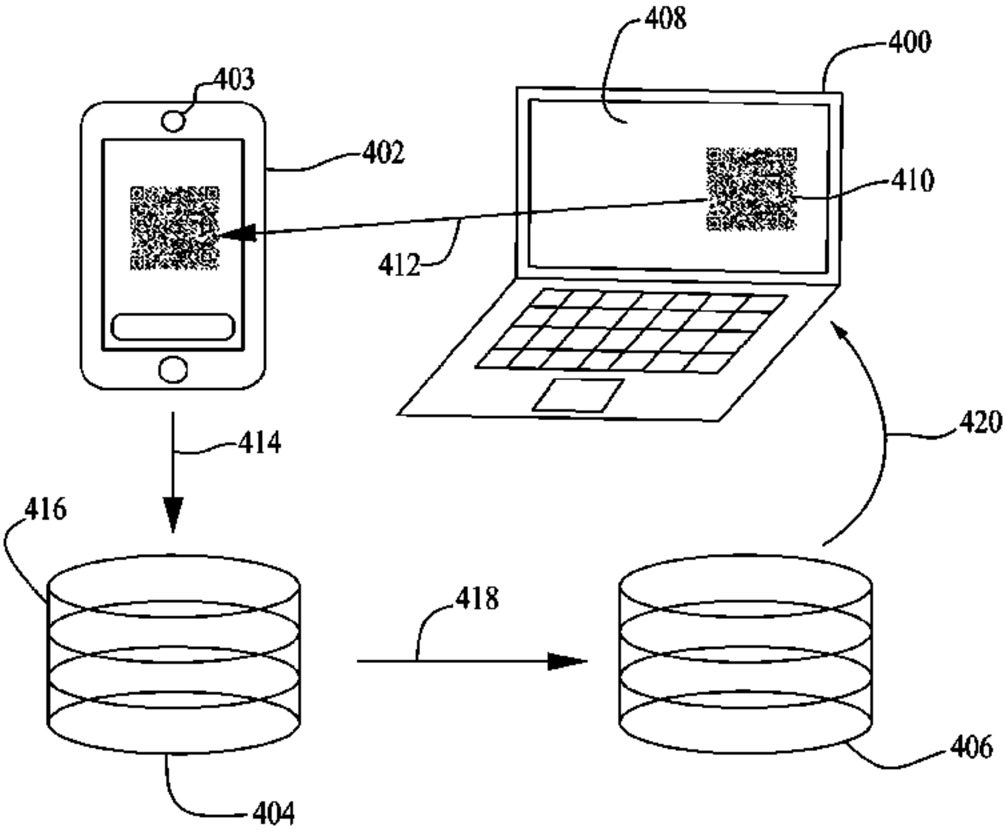


FIG. 4A

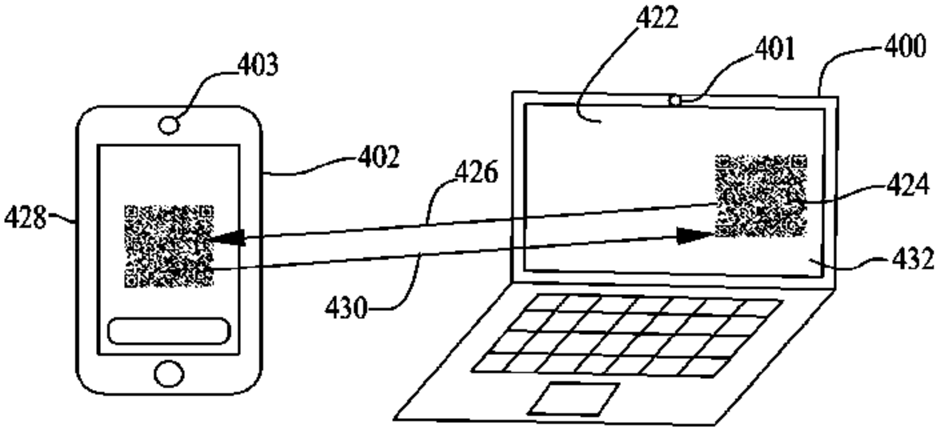


FIG. 4B

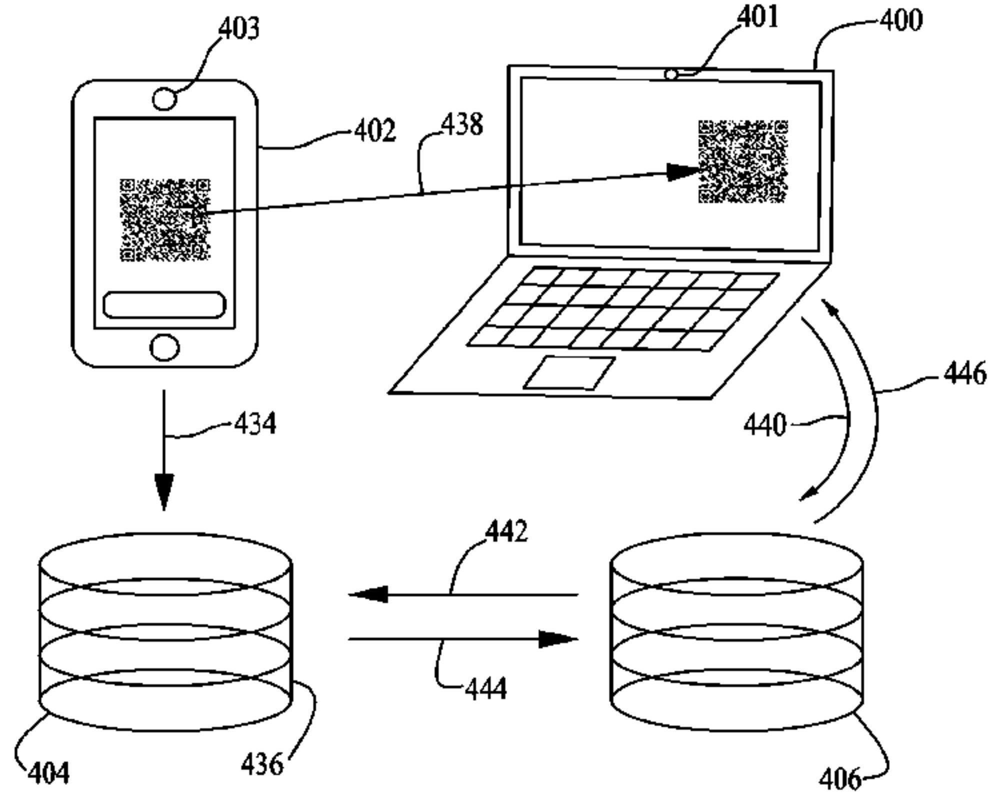


Fig. 4C

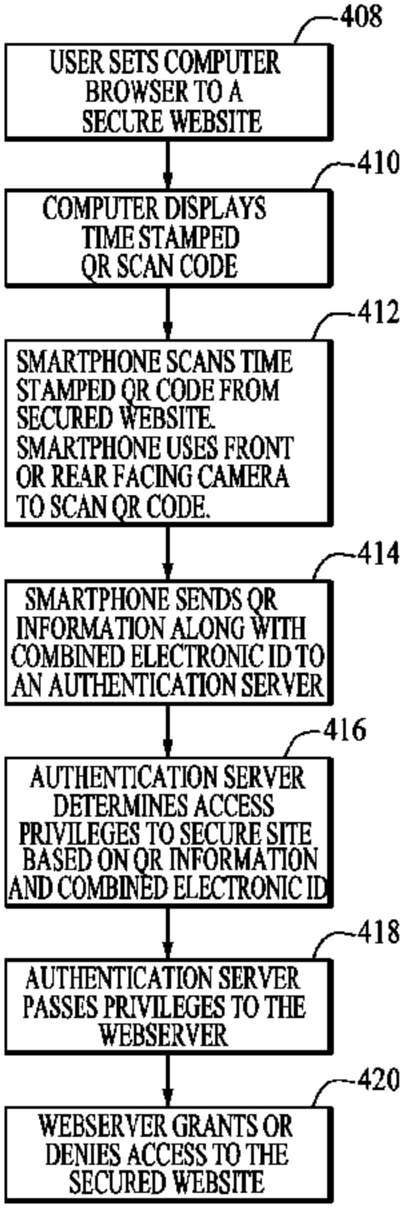

408
USER SETS COMPUTER BROWSER TO A SECURE WEBSITE
410
COMPUTER DISPLAYS TIME STAMPED QR SCAN CODE
412
SMARTPHONE SCANS TIME STAMPED QR CODE FROM SECURED WEBSITE. SMARTPHONE USES FRONT OR REAR FACING CAMERA TO SCAN QR CODE.
414
SMARTPHONE SENDS QR INFORMATION ALONG WITH COMBINED ELECTRONIC ID TO AN AUTHENTICATION SERVER
416
AUTHENTICATION SERVER DETERMINES ACCESS PRIVILEGES TO SECURE SITE BASED ON QR INFORMATION AND COMBINED ELECTRONIC ID
418
AUTHENTICATION SERVER PASSES PRIVILEGES TO THE WEBSERVER
420
WEBSERVER GRANTS OR DENIES ACCESS TO THE SECURED WEBSITE

FIG. 4D

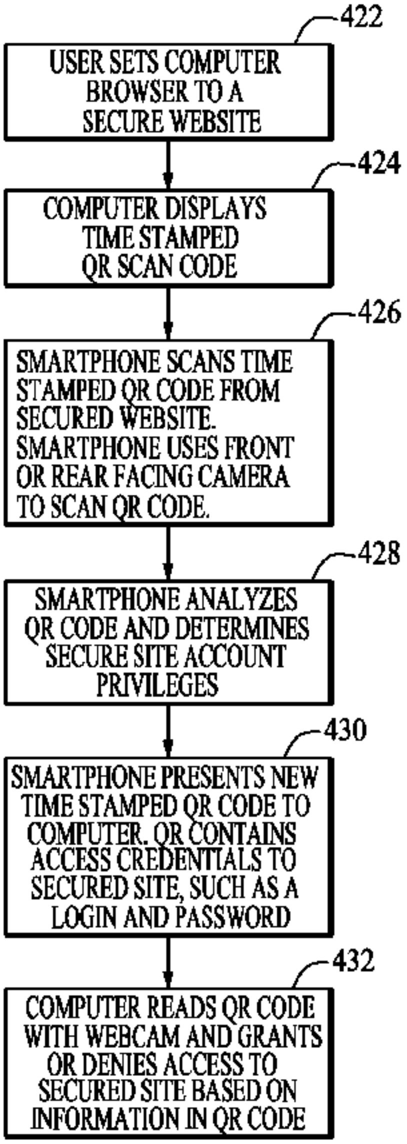

422
USER SETS COMPUTER BROWSER TO A SECURE WEBSITE
424
COMPUTER DISPLAYS TIME STAMPED QR SCAN CODE
426
SMARTPHONE SCANS TIME STAMPED QR CODE FROM SECURED WEBSITE. SMARTPHONE USES FRONT OR REAR FACING CAMERA TO SCAN QR CODE.
428
SMARTPHONE ANALYZES QR CODE AND DETERMINES SECURE SITE ACCOUNT PRIVILEGES
430
SMARTPHONE PRESENTS NEW TIME STAMPED QR CODE TO COMPUTER. QR CONTAINS ACCESS CREDENTIALS TO SECURED SITE, SUCH AS A LOGIN AND PASSWORD
432
COMPUTER READS QR CODE WITH WEBCAM AND GRANTS OR DENIES ACCESS TO SECURED SITE BASED ON INFORMATION IN QR CODE

FIG. 4E

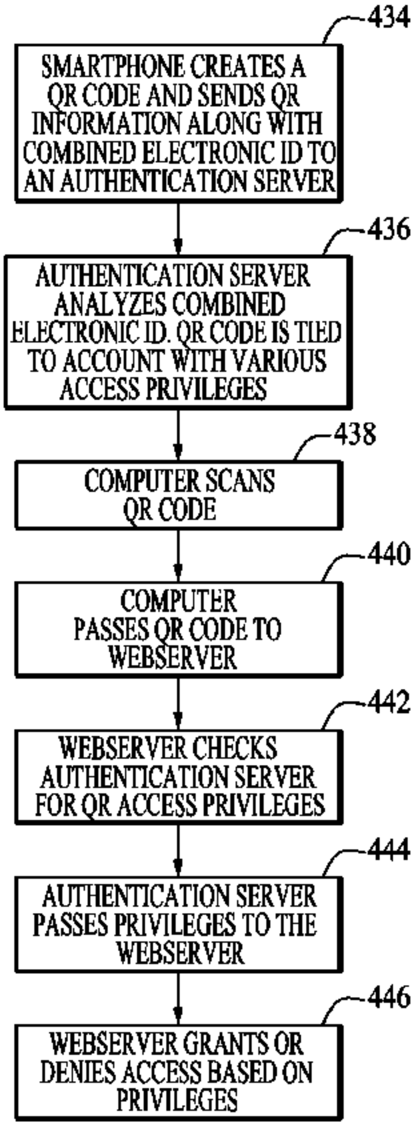

434
SMARTPHONE CREATES A QR CODE AND SENDS QR INFORMATION ALONG WITH COMBINED ELECTRONIC ID TO AN AUTHENTICATION SERVER
436
AUTHENTICATION SERVER ANALYZES COMBINED ELECTRONIC ID. QR CODE IS TIED TO ACCOUNT WITH VARIOUS ACCESS PRIVILEGES
438
COMPUTER SCANS QR CODE
440
COMPUTER PASSES QR CODE TO WEBSERVER
442
WEBSERVER CHECKS AUTHENTICATION SERVER FOR QR ACCESS PRIVILEGES
444
AUTHENTICATION SERVER PASSES PRIVILEGES TO THE WEBSERVER
446
WEBSERVER GRANTS OR DENIES ACCESS BASED ON PRIVILEGES

FIG. 4F

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/032040

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i, H04W 12/06(2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L 9/32; H04W 12/06; G06Q 99/00; H04K 1/00; G06Q 30/00; G06F 21/00; H04M 1/56

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: user information, hardware profile, link, electronic identification

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2008-0127431 A2 (VERIENT. INC.) 23 October 2008 See paras. 21, 24-26, 28-33, 35-38, 41, 43-44, 46; claim 1; and figs. 1-4.	1-4.8-12,18
A		5-7,13-17,19-31
A	US 2006-0212407 A1 (DENNIS BOWER LYON) 21 September 2006 See paras. 59-61, 80, 83, 85-86, 90, 96, 111, 126, 131, 183; claim 1; and figs. 1-2.	1-31
A	US 2006-0173781 A1 (IRAH H. DONNER) 03 August 2006 See paras. 48, 52, 56, 89, 111, 113, 141, 151, 163, 166, 179, 190-191, 306-314; claim 1; and fig. 21.	1-31
A	US 2011-0176667 A1 (SAURABH KUMAR) 21 July 2011 See paras. 4-5, 47-67; claim 1; and figs. 3-4.	1-31
A	US 2010-0332396 A1 (CRAIG STEPHEN ETCHEGOYEN) 30 December 2010 See paras. 6-21, 37-57; claim 1; and fig. 2.	1-31

□ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 21 June 2013 (21.06.2013)	Date of mailing of the international search report **24 June 2013 (24.06.2013)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer KANG, Hee Gok Telephone No. 82-42-481-8264

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2013/032040

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2008-127431 A2	23.10.2008	EP 2095221 A2	02.09.2009
		EP 2095221 A4	18.08.2010
		US 2008-0120195 A1	22.05.2008
		US 2008-0120229 A1	22.05.2008
		US 2008-0120507 A1	22.05.2008
		US 2008-0120717 A1	22.05.2008
		US 2009-0228370 A1	10.09.2009
		US 7548890 B2	16.06.2009
		US 7620600 B2	17.11.2009
		WO 2008-095011 A2	07.08.2008
		WO 2008-127431 A3	08.01.2009
		WO 2009-067477 A1	28.05.2009
US 2006-0212407 A1	21.09.2006	US 2009-0138953 A1	28.05.2009
		WO 2006-101684 A2	28.09.2006
		WO 2006-101684 A3	06.12.2007
US 2006-0173781 A1	03.08.2006	US 7031945 B1	18.04.2006
		US 7162454 B1	09.01.2007
		US 7203665 B2	10.04.2007
		US 7216109 B1	08.05.2007
		US 7280975 B1	09.10.2007
		US 7343350 B1	11.03.2008
		US 7379891 B1	27.05.2008
		US 7386517 B1	10.06.2008
		US 7415424 B1	19.08.2008
		US 7529713 B1	05.05.2009
		US 7562028 B1	14.07.2009
		US 7562051 B1	14.07.2009
		US 7565328 B1	21.07.2009
		US 7577575 B1	18.08.2009
		US 7577619 B1	18.08.2009
		US 7577620 B1	18.08.2009
		US 7617159 B1	10.11.2009
US 2011-0176667 A1	21.07.2011	US 2013-070919 A1	21.03.2013
		US 8358759 B2	22.01.2013
US 2010-0332396 A1	30.12.2010	EP 2273413 A2	12.01.2011
		EP 2273413 A3	30.11.2011

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 October 2013 (17.10.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/154936 A1

(51) International Patent Classification: *G06F 21/00* (2013.01)

(21) International Application Number: PCT/US2013/035450

(22) International Filing Date: 5 April 2013 (05.04.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/621,728 9 April 2012 (09.04.2012) US
13/829,180 14 March 2013 (14.03.2013) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US 13/829,180 (CON)
Filed on 14 March 2013 (14.03.2013)

(71) Applicant: BRIVAS LLC [US/US]; 7400 Indian Hill Road, Cincinnati, OH 45243 (US).

(72) Inventors: PARRY, Beau, Robertson; 7400 Indian Hill Road, Cincinnati, OH 45243 (US). BODDETI, Yasodekshna; 5850 Hobart Street, Floor 2, Pittsburgh, PA 15217 (US).

(74) Agents: HAUGH, Lucas, V. et al.; Ulmer & Berne LLP, 600 Vine Street, Suite 2800, Cincinnati, OH 45202 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

— *with international search report (Art. 21(3))*

[Continued on next page]

(54) Title: SYSTEMS, METHODS AND APPARATUS FOR MULTIVARIATE AUTHENTICATION

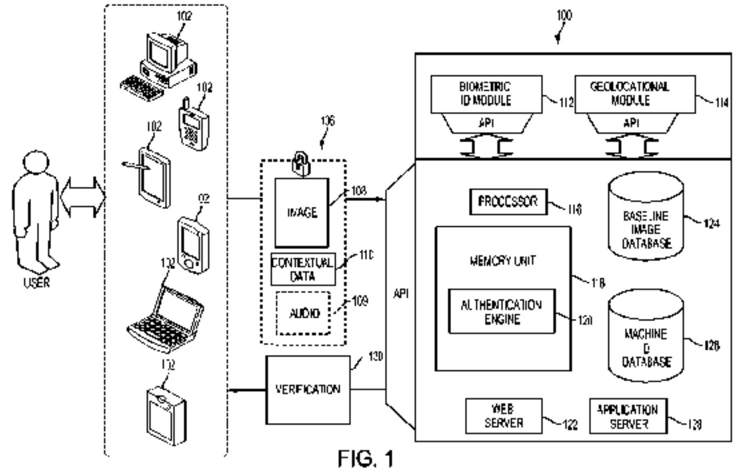


FIG. 1

(57) Abstract: Systems, methods, and apparatus are disclosed for user authentication using a plurality of authentication variables, such as biometrics and contextual data. Example contextual data includes the geographical location of the user, a gesture of the user, and the machine identification of the individual's user device.

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

SYSTEMS, METHODS AND APPARATUS FOR MULTIVARIATE AUTHENTICATION

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims the benefit of U.S. patent application Serial No. 13/829,180, filed on March 14, 2013, entitled " SYSTEMS AND METHODS FOR MULTIVARIATE AUTHENTICATION," which claims the benefit of U.S. provisional patent application Serial No. 61/621,728, filed on April 9, 2012, entitled " SYSTEMS AND METHODS FOR MULTIVARIATE AUTHENTICATION," the disclosures of which are hereby incorporated by reference herein in their entirety.

BACKGROUND

[0002] User authentication has become increasingly of interest as Internet and network-based computer usage have become more prevalent and capabilities of these media have grown. The significance of user authentication has also increased as businesses, government departments, medical organizations and individuals have become increasingly reliant on computer networks and on the security of proprietary information transmitted across networks to users of computing devices.

SUMMARY

[0003] In one embodiment, a computer-based method of authenticating is provided. The method including receiving a request for authentication of a user. The request for authentication including a biometric feature of the user collected by a user device and contextual data from the user device. The method also including comparing the biometric feature of the user to baseline biometric feature of the user, comparing the contextual data to an expected contextual data value, and determining whether to authenticate the user based on the comparison of the biometric feature of the user to the baseline biometric feature of the user and the comparison of the contextual data to the expected contextual data value.

[0004] A computer-based method of the preceding embodiment, where the contextual data is a machine identification (ID) of the user device.

[0005] A computer-based method of one or more of the preceding embodiments, where the contextual data is data collected from a sensor of the user device.

[0006] A computer-based method of one or more of the preceding embodiments, where the sensor is any of an accelerometer, a gyroscope, and a magnetometer.

[0007] A computer-based method of one or more of the preceding embodiments, including receiving an image of the user, the image including the biometric feature, where a baseline image includes the baseline biometric feature.

[0008] A computer-based method of one or more of the preceding embodiments, including comparing a first gesture made by the user in the image of the user to a second gesture in the baseline image.

[0009] A computer-based method of one or more of the preceding embodiments, including comparing a location of the first gesture in the image to a location of the second gesture in the baseline image.

[0010] A computer-based method of one or more of the preceding embodiments, including comparing a location of a first camera flash location in the image to a location of a second camera flash location in the baseline image.

[0011] A computer-based method of one or more of the preceding embodiments where the contextual data is a geographical location of the user device.

[0012] A computer-based method of one or more of the preceding embodiments, including transmitting to the user device a color key, where the biometric feature of the user collected by a user device includes a color signature of the user.

[0013] A computer-based method of one or more of the preceding embodiments, including comparing the color signature of the user to a stored color signature of the user.

[0014] A computer-based method of one or more of the preceding embodiments, where the user device is a first user device and the biometric feature is included in a first image, where the request for authentication includes the first image of the user collected by the first user device and a second image including the biometric feature of the user collected by a second user device.

[0015] A computer-based method of one or more of the preceding embodiments, including comparing the first image of the user to a first baseline image and the second image of the user to a second baseline image.

[0016] A computer-based method of one or more of the preceding embodiments, where the image is collected during a rotary scan of the user.

[0017] In one embodiment, a computer-based authentication system is provided. The system including a baseline image database, a contextual data database, and an authentication computing system. The authentication system is configured to receive a request for authentication of a user from a user device. The request for authentication including an image of the user and contextual data. The authentication system is also configured to compare the image of the user to a baseline image of the user stored in the baseline image database, compare the contextual data to an expected contextual data value stored in the contextual data database, and determine whether to authenticate the user based on the comparison of the biometric feature of the user to the baseline image of the user and the comparison of the contextual data to the expected contextual data value.

[0018] A computer-based authentication system of the preceding embodiment, where the contextual data indicates a geographical location of the user device.

[0019] A computer-based authentication system of one or more of the preceding embodiments, where the contextual data is acceleration data collected from an accelerometer.

[0020] A computer-based authentication system of one or more of the preceding embodiments, where the baseline image includes a first hand gesture, and where the authentication system configured to compare a second hand gesture made by the user in the image of the user to the first gesture made by the user in the baseline image.

[0021] A computer-based authentication system of one or more of the preceding embodiments, where the authentication system is configured to compare a location of the first gesture in the image to a location of the second gesture in the baseline image.

[0022] In one embodiment, a non-transitory computer readable medium having instructions stored thereon is provided. When the instructions are executed by a processor, they cause the processor to receive a request for authentication of a user. The request for authentication includes an image of the user collected by a user device and contextual data from the user device. When the instructions are executed by a processor, they also cause the processor to compare the image of the user to a baseline image of the user, compare the contextual data to an expected contextual data value and determine whether to authenticate the user based on the comparison of the biometric feature of the user to the baseline image of the user and the comparison of the contextual data to the expected contextual data value.

[0023] A non-transitory computer readable medium of the preceding embodiment, where the contextual data is a geographical location of the user device.

[0024] A non-transitory computer readable medium of one or more of the preceding embodiments, where the contextual data is gathered by a sensor of the user device.

[0025] A non-transitory computer readable medium of one or more of the preceding embodiments, where the instructions cause the processor to compare a first gesture made by the user in the image of the user to a second gesture in the baseline image.

[0026] A non-transitory computer readable medium of one or more of the preceding embodiments, where the instructions cause the processor to compare a location of the first gesture in the image to a location of the second gesture in the baseline image.

[0027] In one embodiment a non-transitory computer readable medium having instructions stored thereon is provided. When the instructions are executed by a processor, they cause the processor to receive from a first user device via a network communication a network packet including an electronic data file and recipient biometrics and receive from a second user device via network communication biometric data obtained from a user of the second user device. When the biometric data obtained from the use of the second user device matches the recipient biometrics, the electronic data file is permitted to be accessed on the second user device.

[0028] A non-transitory computer readable medium of the preceding embodiment, where the recipient biometrics is a facial image of a recipient.

[0029] A non-transitory computer readable medium of one or more of the preceding embodiments, where the biometric data obtained from the user of the second user device is an image of a face of the user of the second user device.

[0030] A non-transitory computer readable medium of one or more of the preceding embodiments, where the electronic data file is encrypted based on biometrics of the second user and contextual data associated with the second user.

[0031] A non-transitory computer readable medium of one or more of the preceding embodiments, where the recipient biometrics includes biometrics from each of a plurality of recipients, and where the biometric data obtained from a user of the second user device includes biometric data obtained from each of a plurality of users of the second user device.

[0032] A non-transitory computer readable medium of one or more of the preceding embodiments, where the instructions cause the processor to permit the electronic data file to be accessed on the second user device when the biometric data obtained from each of a plurality of users of the second user device matches corresponding recipient biometrics received from the first user device.

[0033] A non-transitory computer readable medium of one or more of the preceding embodiments, where the plurality of recipients includes *N* recipients, where *N* is an integer, and where the plurality of users of the second user includes *k* recipients.

[0034] A non-transitory computer readable medium of one or more of the preceding embodiments, where $k<N$.

[0035] In one embodiment a method of electronically sharing data is provided. The method includes identifying an electronic file, providing biometrics associated with a recipient, providing contextual data associated with a recipient, causing the electronic file to be encrypted based on the provided biometrics and the provided contextual data and causing the transmission of the encrypted with another embodiment.

[0036] A method of electronically sharing data of the preceding embodiment, where providing the biometrics associated with a recipient includes selecting a digital image of the recipient's face.

[0037] A method of electronically sharing data of one or more of the preceding embodiments, where providing contextual data associated with the recipient includes identifying a geographic location of the recipient.

[0038] A method of electronically sharing data of one or more of the preceding embodiments, where providing biometrics includes providing biometrics from each of a plurality of recipients.

[0039] A method of electronically sharing data of one or more of the preceding embodiments, where the plurality of recipients includes *N* recipients, where *N* is an integer.

BRIEF DESCRIPTION OF THE DRAWINGS

[0040] The present disclosure will be more readily understood from a detailed description of some example embodiments taken in conjunction with the following figures:

[0041] FIG. 1 illustrates an example authentication computing system that receives and process identity-based information for use authorization.

[0042] FIGS. 2A-2L schematically illustrate various forms of information that may be sent to an authentication computing system via an image in accordance with various non-limiting embodiments.

[0043] FIG. 3 illustrates a user device capturing an image of a user in accordance with one non-limiting embodiment.

[0044] FIGS. 4A-4D illustrate various image analysis techniques in accordance with non-limiting embodiments.

[0045] FIGS. 5A-5D show example images provided to an authentication computing system.

[0046] FIG. 6 shows a user authentication process in accordance with one non-limiting embodiment.

[0047] FIGS. 7A-7B depict example moving image scans.

[0048] FIG. 7C illustrate an example process flow associated with a moving image scan.

[0049] FIG. 8A illustrates an example moving image scan.

[0050] FIG. 8B illustrates an example process flow associated with a moving image scan utilizing multi-colored strobing.

[0051] FIGS. 9-10 illustrate example authentication processes utilizing multi-image acquisition processes.

[0052] FIG. 11 illustrates an authentication computing system that comprises a local authentication computing system and a remote authentication computing system.

[0053] FIG. 12 illustrates an example data transferring technique utilizing an authentication computing system.

[0054] FIG. 13 illustrates an authentication process for a computing device using a color signature in accordance with one non-limiting embodiment.

[0055] FIG. 14 illustrates an authentication process for an authentication computing system using a color signature in accordance with one non-limiting embodiment.

[0056] FIG. 15 illustrates an authentication process for a computing device in accordance with one non-limiting embodiment.

[0057] FIG. 16 illustrates an authentication process of an authentication computing system in accordance with one non-limiting embodiment.

[0058] FIG. 17 illustrates an authentication process in accordance with one non-limiting embodiment.

[0059] FIG. 18A illustrates an example message flow diagram for a registration process.

[0060] FIG. 18B illustrates an example message flow diagram for an authentication process.

[0061] FIG. 19A illustrates an example simplified block diagram for a user registration process.

[0062] FIG. 19B illustrates an example simplified block diagram for a user authentication process.

[0063] FIG. 20A illustrates an example process for registering a user with an authentication computing system.

[0064] FIG. 20B illustrates an example process for authenticating a registered user of an authentication computing system.

[0065] FIG. 21 illustrates an example block diagram of a communication system.

[0066] FIG. 22 illustrates a system flow diagram for photo cloaking utilizing biometric key generation.

[0067] FIG. 23 illustrates an example biometric encryption system flow diagram.

DETAILED DESCRIPTION

[0068] Various non-limiting embodiments of the present disclosure will now be described to provide an overall understanding of the principles of the structure, function, and use of the authentication systems and processes disclosed herein. One or more examples of these non-limiting embodiments are illustrated in the accompanying drawings. Those of ordinary skill in the art will understand that systems and methods specifically described herein and illustrated in the accompanying drawings are non-limiting embodiments. The features illustrated or described in connection with one non-limiting embodiment may be combined with the features of other non-limiting embodiments. Such modifications and variations are intended to be included within the scope of the present disclosure.

[0069] The presently disclosed embodiments are generally directed to user identification and authorization. Such systems and methods may be implemented in a wide variety of contexts. In one example embodiment, the presently disclosed systems and methods allow the identity of a user of a computing device to be authenticated. The user may be authenticated though a multivariate platform, as described in more detail below. In some embodiments, the authentication process may process an image supplied by the computing device to the authentication computing system. The process may utilize a biometric attribute of the user along with one or more additional authentication variables in order to confirm an identity of the user. The image may, for example, include a user gesture, a flash burst, or other authentication variable. The gesture, the relative location of the gesture, and/or the relative location of the flash may be compared to a baseline image as part of the authentication process. In some implementations, contextual data associated with the image may be processed as part of the authentication process. Such contextual data (sometimes referred to as “metadata”) may include, without limitation, a machine ID, device data, or geographical/locational information. As described in more detail below, contextual data may also include data obtained from sensors onboard a user computer device. Example sensors include accelerometers, magnetometers, proximity sensors, and the like. Such sensors may provide contextual data such as movement data and user device orientation data, for example.

[0070] In some example embodiments, a computing device may display a particular color on its graphical display screen during an authentication process. The particular color may have been provided to the computing device by an authentication system. The image subsequently provided to the authentication computing system by the computer device may include an image of the user with the particular color reflected off of facial features of a user to form a color signature. Along with biometrical facial features of the user, the particular color present in the image and the color signature may be analyzed by an authentication computing system to provide user authentication.

[0071] In some example embodiments, at least some of the communication between a computing device and an authentication computing system is encrypted using any suitable encryption technique. In one example embodiment, chaos-based image encryption may be used, although this disclosure is not so limited. Additional details regarding chaos-based image encryption may be found in "Chaos-Based Image Encryption" by Yaobin Mao and Guaron Chen (available at http://www.open-image.org/725publication/journal/CBIE.pdf), which is incorporated herein by reference. In one example embodiment, images provided to the authentication computing system by a computing device are encrypted though a pixel-rotation technique, a codec watermarking technique, and/or other encrypting technique.

[0072] Generally, the presently disclosed systems and methods may authenticate a user before giving the user access to a mobile computer device, access to an application on a computer device, access to a building or other structure, access to a web portal, access to any other type of computing device, access to data, or access to any other secured virtual or physical destination. The authentication can be based on a combination of biometric analysis and contextual data analysis, with the contextual data based on a user device of the user seeking authentication. Therefore, the presently disclosed systems and methods generally bind man and machine to effectuate the authentication paradigms described in more detail below.

[0073] Reference throughout the specification to "various embodiments," "some embodiments," "one embodiment," "some example embodiments," "one example embodiment," or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment. Thus, appearances of the phrases "in various embodiments," "in some embodiments," "in one embodiment," "some example embodiments," "one example embodiment, or "in an embodiment" in places throughout the specification are not necessarily all referring to the same embodiment. Furthermore, the particular features, structures or characteristics may be combined in any suitable manner in one or more embodiments.

[0074] Referring now to FIG. 1, one example embodiment of the present disclosure may comprise an authentication computing system 100 that receives and processes identity-based information to execute user authorization. The authentication computing system 100 may be provided using any suitable processor-based device or system, such as a personal computer, laptop, server, mainframe, or a collection (e.g., network) of multiple computers, for example. The authentication computing system 100 may include one or more processors 116 and one or more computer memory units 118. For convenience, only one processor 116 and only one memory unit 118 are shown in FIG. 1. The processor 116 may execute software instructions stored on the memory unit 118. The processor 116 may be implemented as an integrated circuit (IC) having one or multiple cores. The memory unit 118 may include volatile and/or non-volatile memory units. Volatile memory units may include random access memory (RAM), for example. Non-volatile memory units may include read only memory (ROM), for example, as well as mechanical non-volatile memory systems, such as, for example, a hard disk drive, an optical disk drive, etc. The RAM and/or ROM memory units may be implemented as discrete memory ICs, for example.

[0075] The memory unit 118 may store executable software and data for authentication engine 120. When the processor 116 of the authentication computing system 100 executes the software of the authentication engine 120, the processor 116 may be caused to perform the various operations of the authentication computing system 100, such as send information to remote computer devices, process information received from remote computer devices, and provide authentication information to the remote computer devices, as discussed in more detail below. Data used by the authentication engine 120 may be from various sources, such as a baseline image database 124, which may be an electronic computer database, for example. The data stored in the baseline image database 124 may be stored in a non-volatile computer memory, such as a hard disk drive, a read only memory (e.g., a ROM IC), or other types of non-volatile memory. Also, the data of the database 124 may be stored on a remote electronic computer system, for example. Machine ID database 126, which may be an electronic computer database, for example, may also provide used by the authentication engine 120. The data stored in the machine ID database 126 may be stored in a non-volatile computer memory, such as a hard disk drive, a read only memory (e.g., a ROM IC), or other types of non-volatile memory. Also, the data of the Machine ID database 126 may be stored on a remote electronic computer system, for example. In some embodiments, the Machine ID database comprises mobile equipment identification (MEID) numbers, Electronic Serial Numbers (ESN), and/or other suitable identifying indicia that may be used to identify electronic devices. While machine ID database 126 is illustrated as storing expected contextual data related to an identifier of a user device, it is to be appreciated that other embodiments may utilize other databases configured to store other forms of expected contextual data (expected movement data, expected geolocational data, expected magnetic data, and so forth) that may be compared to contextual data received from a user device during an authentication process.

[0076] The authentication computing system 100 may be in communication with user devices 102 via an electronic communications network (not shown). The communications network may include a number of computer and/or data networks, including the Internet, LANs, WANs, GPRS networks, etc., and may comprise wired and/or wireless communication links. In some example embodiments, an authentication system API is used to pass information between the user devices 102 and the authentication computing system 100. The user devices 102 that communicate with the authentication computing system 100 may be any type of client device suitable for communication over the network, such as a personal computer, a laptop computer, or a netbook computer, for example. In some example embodiments, a user may communicate with the network via a user device 102 that is a combination handheld computer and mobile telephone, sometimes referred to as a smart phone. It can be appreciated that while certain embodiments may be described with users communication via a smart phone or laptop by way of example, the communication may be implemented using other types of user equipment (UE) or wireless computing devices such as a mobile telephone, personal digital assistant (PDA), combination mobile telephone/PDA, handheld device, mobile unit, subscriber station, game device, messaging device, media player, pager, or other suitable mobile communications devices. Further, in some example embodiments, the user device may be fixed to a building, vehicle, or other physical structure.

[0077] Some of the user devices 102 also may support wireless wide area network (WWAN) data communications services including Internet access. Examples of WWAN data communications services may include Evolution-Data Optimized or Evolution-Data only (EV-DO), Evolution For Data and Voice (EV-DV), CDMA/1xRTT, GSM with General Packet Radio Service systems (GSM/GPRS), Enhanced Data Rates for Global Evolution (EDGE), High Speed Downlink Packet Access (HSDPA), High Speed Uplink Packet Access (HSUPA), and others. The user device 102 may provide wireless local area network (WLAN) data communications functionality in accordance with the Institute of Electrical and Electronics Engineers (IEEE) 802.xx series of protocols, such as the IEEE 802.11a/b/g/n series of standard protocols and variants (also referred to as "Wi-Fi"), the IEEE 802.16 series of standard protocols and variants (also referred to as "WiMAX"), the IEEE 802.20 series of standard protocols and variants, and others.

[0078] In some example embodiments, the user device 102 also may be arranged to perform data communications functionality in accordance with shorter range wireless networks, such as a wireless personal area network (PAN) offering Bluetooth® data communications services in accordance with the Bluetooth®. Special Interest Group (SIG) series of protocols, specifications, profiles, and so forth. Other examples of shorter range wireless networks may employ infrared (IR) techniques or near-field communication techniques and protocols, such as electromagnetic induction (EMI) techniques including passive or active radio-frequency identification (RFID) protocols and devices.

[0079] The user device 102 may comprise various radio elements, including a radio processor, one or more transceivers, amplifiers, filters, switches, and so forth to provide voice and/or data communication functionality. It may be appreciated that the user device 102 may operate in accordance with different types of wireless network systems utilize different radio elements to implement different communication techniques. The user device 102 also may comprise various input/output (I/O) interfaces for supporting different types of connections such as a serial connection port, an IR port, a Bluetooth® interface, a network interface, a Wi-Fi interface, a WiMax interface, a cellular network interface, a wireless network interface card (WNIC), a transceiver, and so forth. The user device 102 may comprise one or more internal and/or external antennas to support operation in multiple frequency bands or sub-bands such as the 2.4 GHz range of the ISM frequency band for Wi-Fi and Bluetooth® communications, one or more of the 850 MHz, 900 MHZ, 1800 MHz, and 1900 MHz frequency bands for GSM, CDMA, TDMA, NAMPS, cellular, and/or PCS communications, the 2100 MHz frequency band for CDMA2000/EV-DO and/or WCDMA/JMTS communications, the 1575 MHz frequency band for Global Positioning System (GPS) operations, and others.

[0080] The user device 102 may provide a variety of applications for allowing a user to accomplish one or more specific tasks using the authentication computing system 100. Applications may include, without limitation, a web browser application (e.g., INTERNET EXPLORER, MOZILLA, FIREFOX, SAFARI, OPERA, NETSCAPE NAVIGATOR) telephone application (e.g., cellular, VoIP, PTT), networking application, messaging application (e.g., e-mail, IM, SMS, MMS, BLACKBERRY Messenger), contacts application, calendar application and so forth. The user device 102 may comprise various software programs such as system programs and applications to provide computing capabilities in accordance with the described embodiments. System programs may include, without limitation, an operating system (OS), device drivers, programming tools, utility programs, software libraries, application programming interfaces (APIs), and so forth. Exemplary operating systems may include, for example, a PALM OS, MICROSOFT OS, APPLE OS, UNIX OS, LINUX OS, SYMBIAN OS, EMBEDIX OS, Binary Run-time Environment for Wireless (BREW) OS, JavaOS, a Wireless Application Protocol (WAP) OS, and others.

[0081] In general, an application may provide a user interface to communicate information between the authentication computing system 100 and the user via user devices 102. The user devices 102 may include various components for interacting with the application such as a display for presenting the user interface and a keypad for inputting data and/or commands. The user devices 102 may include other components for use with one or more applications such as a stylus, a touch-sensitive screen, keys (e.g., input keys, preset and programmable hot keys), buttons (e.g., action buttons, a multidirectional navigation button, preset and programmable shortcut buttons), switches, a microphone, speakers, an audio headset, a camera, and so forth. Through the interface, the users may interact with the authentication computing system 100.

[0082] The applications may include or be implemented as executable computer program instructions stored on computer-readable storage media such as volatile or non-volatile memory capable of being retrieved and executed by a processor to provide operations for the user devices 102. The memory may also store various databases and/or other types of data structures (e.g., arrays, files, tables, records) for storing data for use by the processor and/or other elements of the user devices 102.

[0083] As shown in FIG. 1, the authentication computing system 100 may include several computer servers and databases. For example, the authentication computing system 100 may include one or more web servers 122 and application servers 128. For convenience, only one web server 122 and one application server 128 are shown in FIG. 1, although it should be recognized that this disclosure is not so limited. The web server 122 may provide a graphical web user interface through which users of the system may interact with the authentication computing system 100. The web server 122 may accept requests, such as HTTP requests, from clients (such as web browsers on the device 102), and serve the clients responses, such as HTTP responses, along with optional data content, such as web pages (e.g., HTML documents) and linked objects (such as images, etc.).

[0084] The application server 128 may provide a user interface for users who do not communicate with the authentication computing system 100 using a web browser. Such users may have special software installed on their user devices 102 that allows them to communicate with the application server 128 via the network. Such software may be downloaded, for example, from the authentication computing system 100, or other software application provider, over the network to such user devices 102. The software may also be installed on such user devices 102 by other means known in the art, such as CD-ROM, etc.

[0085] The servers 122, 128 may comprise processors (e.g., CPUs), memory units (e.g., RAM, ROM), non-volatile storage systems (e.g., hard disk drive systems), etc. The servers 122, 128 may utilize operating systems, such as Solaris, Linux, or Windows Server operating systems, for example.

[0086] Although FIG. 1 depicts a limited number of elements for purposes of illustration, it can be appreciated that the authentication computing system 100 may include more or less elements as well as other types of elements in accordance with the described embodiments. Elements of the authentication system 100 may include physical or logical entities for communicating information implemented as hardware components (e.g., computing devices, processors, logic devices), executable computer program instructions (e.g., firmware, software) to be executed by various hardware components, or combination thereof, as desired for a given set of design parameters or performance constraints.

[0087] In addition to the end user devices 102, the authentication computing system 100 may be in communication with other entities, such as a biometric ID module 112. In some example embodiments, biometric ID functionality may be supplied from one or more third party biometric services providers. One example provider of biometric services is available at http://www.face.com and accessible via an application programming interface (API). Other services may be provided by other third party providers, such as geolocational services, which may be provide by a geolocational module 114 through an API. An example geolocational service is the W3C Geolocation API provided by the World Wide Web Consortium (W3C). In some embodiments, biometric ID and/or geolocational services may be provided by the authentication computing system 100 without the aid of outside service providers. For example, biometric information of users of the system may be stored by the authentication computing system.

[0088] During an authentication event, the authentication computing system 100 may receive and process an encrypted network packet 106 from the user device 102. The encrypted network packet 106 may be encrypted using chaos-based image encryption, for example. The network packet 106 may include an image 108 and may also include contextual data 110. The image 108 may include, for example, an image of the user for biometric analysis. The image 108 may also include additional image data that may be analyzed and processed by the authentication computing system 100. For example, the additional image data may include, without limitation, a source of light at a particular location in the image relative to the user, a particular gesture by the user, a particular facial expression by the user, a particular color reflected off a portion of the user, and so forth. The contextual data 110 may include, without limitation, a machine ID, locational information, device global positioning system (GPS) information, radio-frequency identification (RFID) information, near-field communication (NFC) information, MAC address information, and so forth. For user devices 102 supporting a position determination capability, examples of position determination capability may include one or more position determination techniques such as Global Positioning System (GPS) techniques, Assisted GPS (AGPS) techniques, hybrid techniques involving GPS or AGPS in conjunction with Cell Global Identity (CGI), Enhanced Forward Link Trilateration (EFLT), Advanced Forward Link Trilateration (AFTL), Time Difference of Arrival (TDOA, Angle of Arrival (AOA), Enhanced Observed Time Difference (EOTD), or Observed Time Difference of Arrival (OTDOA), and/or any other position determination techniques in accordance with the described embodiments. The image 108 and any other information associated with the image may be purged by the user device 102 subsequent to the transmission of the image 108 to the authentication computing system 100.

[0089] The encrypted network packet 106 may be sent to the authentication computing system 100 in response to a user's interaction with the user device 102. For example, a user may be seeking to log into a restricted website, access a restricted website, access a restricted file, access a restricted building, or access a restricted computing device. Upon receipt of the encrypted network packet 106 (which may be comprised of a plurality of individual network packets) the authentication computing system 100 may decrypt the information in order to process the image 108 and any associated contextual data 110. If a third party biometric ID module 112 is used, information may be provided to the service provider through an API. For example, the biometric ID module 112 may analyze facial features of the user to ascertain identity. The additional image data in the image 108 (such as relative flash placement, for example) may be compared to a baseline image stored in the baseline image database 124. In some example embodiments, additional comparisons or analysis may be performed on the contextual data 110, the image 108, or other information contained in the encrypted network packet 106.

[0090] In some embodiments, the encrypted network packet 106 may include an audio file 109 which includes a voice of the user, in addition to the contextual data 110. The audio file 109 may be included, for example, in the place of the image 108 when an image of the user cannot be obtained. The audio file 109 may be processed by the authentication computing system 100 to compare the audio file 109 to a known voice signature of the user. The audio file 109 may be collected by the user device 102 and transmitted to the authentication computing system 100 when it is deemed, for example, that an onboard camera of the user device 102 is not functioning. In other embodiments, both the image 108 and the audio file 109 are required by the authentication computing system 100 for authentication.

[0091] Once the user has been authenticated, verification 130 indicating that the user has been property authenticated may be provided to the user device 102 by the authentication computing system 100. The verification 130 may be in any suitable form. For example, the verification 130 may indicate to an application running on the user device 102 that the user is an authorized user. Subsequent to receiving the verification, the user device 102 may allow the user to log into a restricted website, access a restricted website, access a restricted file, access a restricted building, or access a restricted computing device, for example.

[0092] FIGS. 2A-2L schematically illustrate various forms of information that may be sent to the authentication computing system 100 via an image in order to authenticate a particular user. As is to be appreciated, the illustrated images are merely examples of illustrative embodiments and are not intended to be limiting.

[0093] Referring first to FIG. 2A, in one example embodiment, an image 200 comprises a biometric feature and a flash location. The biometric feature may be, for example, a facial feature, a hand feature, a retinal feature, a biological sinusoidal rhythm, and so forth. The flash location, as described in more detail below, may be the relative position of a point of light relative to the biometric feature. Referring next to FIG. 2B, in one example embodiment, an image 210 comprises a biometric feature and a gesture. The gesture may be, for example, a hand gesture, a multi-hand gesture, a facial expression, an arm position, and so forth. Referring next to FIG. 2C, in one example embodiment, an image 212 comprises a biometric feature, a gesture, and a flash location. Referring next to FIG. 2D, in one example embodiment, an image 214 comprises a biometric feature, a gesture location, and a flash location.

[0094] Referring to FIG. 2E, in one example embodiment, an image 216 comprises a biometric feature and a color feature. As described in more detail below, in some example embodiments, prior to capturing the image, the computer device may output a particular color on its graphical display such that can reflect off a biometric feature of the user as a color signature. The reflected color, along with the biometric features, may be analyzed by the authentication computing system 100 to confirm identity. Referring next to FIG. 2F, in one example embodiment, an image 218 comprises a biometric feature, a flash location, and a color feature. Referring next to FIG. 2G, in one example embodiment, an image 220 comprises a biometric feature, a color feature, and a gesture.

[0095] Referring to FIG. 2H, in one example embodiment, an image 224 comprises a biometric feature and a gesture. Machine ID may also be associated with the image 224 and provided to the authentication computing system 100. The machine ID may be contextual data, which may include any type of additional data, such as locational information, GPS information, RFID information, NFC information, MAC address information, device data, and so forth. The machine ID provided as contextual data may be compared to machine ID stored by the authentication computing system 100. For example, the authentication computing system 100 may compare the locational information provided with the image 224 to an expected location stored by the system. If the image 224 was not captured at a geographical location near the expected location, authentication will not be successful.

[0096] Referring to FIG. 2I, in one example embodiment, an image 226 comprises a biometric feature and a flash angle. The flash angle may be, for example, an angle of incidence of the flash. A non-limiting example of flash angle determination is described in more detail with regard to FIG. 4D. Referring now to FIG. 2J, an image 228 comprise a biometric feature and a user device angle. The value of the user device angle may be measured by an accelerometer on-board the user device, for example.

[0097] Referring now to FIG. 2K, an image 230 comprises a biometric feature and locational information. The locational information may be gathered by an on-board GPS, for example. In one embodiment, the location information can include longitude, latitude, and altitude. The image 230 may also comprise flash angle information.

[0098] Referring next to FIG. 2L, an image 232 may comprise a biometric feature, flash/shutter synchronicity information, and a gesture location. With regard to flash/shutter synchronicity, the authentication computing system 100 may communicate with the user device 102 during the image capture process to control the relative timing of the flash and the shutter. For example, the authentication computing system 100 may cause a slight flash delay or shutter delay to give the captured image a particular flash signature. A change in the flash delay or shutter delay may result in a different flash signature. The flash signature in the image may be analyzed by the authentication computing system 100 as an authentication variable.

[0099] It is noted that the informational components of the various images illustrated in FIGS. 2A-2L are merely for illustrative purposes. In fact, images provided to the authentication computing system 100 may include any number of authentication variables and/or any combination of authentication variables. The number or combination of authentication variables transmitted with the image may depend, at least in part, on a desired level of security. In some embodiments, the number authentication variables used and/or the priority of the authentication variables may be based on the available resources at the time of authentication. As described in more detail below, example resources that may be considered included, without limitation, battery supply, data transmission rates, network signal strength, and so forth.

[00100] In some embodiments, the authentication computing system may require user authentication based on contextual operational information, such as the geographical location of the user device or the period of time since a previous successful authentication, for example. By way of example, a user of a user device may power down a user device during a plane flight. Upon arriving at the destination, the user device will be powered up. The distance between the particular geographic location of the user device upon power down and the particular geographic location of the user device upon power up can be assessed. If the distance is beyond a predetermined distance threshold, the user device may require user authentication before providing user access.

[00101] Furthermore, in some embodiments, the user device may include a plurality of data collection devices that each requires different levels of operational resources. For example, a smart phone may have two on-board cameras, a high-resolution camera and a low-resolution camera. Images captured using the low-resolution camera requires less data and, therefore, such camera may be useful during times of low data transmission rates. In such instances, the biometric data collected from the user may include periocular data, for example. If the user device is operating on a network connection having high data transmission rates, the high-resolution camera may be used. In any event, the systems and methods described herein may alter or shift the type of authentication variables considered, and the techniques for gathering such variables, based on operational or environmental factors existing at the time of the authentication request. The systems and methods described herein may use additional techniques or processes to compensate for operational conditions. For example, during low light conditions, a particular color may be displayed on a screen of the user device, such that the screen can be held proximate to the user to illuminate the user's face with that particular hue. The particular color may change over time (such as in a strobed fashion), with the shutter coordinated with the pulses of light. As such, as an additional layer of security, an image with a particular color reflected off of the user's face can be compared with an expected color.

[00102] FIG. 3 illustrates a user device 304 capturing an image of a user in accordance with the presently disclosed systems and methods. The user is positioned in front of a reflective surface 310, such as a mirror or reflective window, for example. Prior to capturing the image, a light source 306 (such as a flash on a smart phone) is activated. The user may then position the light source reflection 308 at a pre-defined position relative the user reflection 302. The pre-defined position may be based on a desired angle of incidence, a desired distance from the user, or other desired relative location. While not shown, in some embodiments, the user may additionally make a gesture for reflection by the reflective surface 310. Once in the proper position, a camera 312 associated with the user device 304 may capture an image of the reflective surface 310. The image, similar to image 108 in FIG. 1, for example, may be provided to an authentication computing system local to the user device 304 or to a remote authentication computing system via a networked connection. In some example embodiments, the reflective surface 310 may include a communication element 316. The communication element 316 may utilize, for example, a BLUETOOTH® communication protocol or a near-field communication protocol. The communication element 316 may provide addition data (such as contextual data) that may be transmitted along with the image to the authentication computing system.

[00103] Various forms of assistance may be provided to the user by the authentication computing system 100 during the image capture process illustrated in FIG. 3. In one embodiment, for example, a visual cue is provided to the user on the screen of the user device 304. The visual cue may provide an indication of the relative proper placement of the user device 304 in the image for a particular image capture session. The visual cue may be, without limitation, a solid dot on the screen, a flashing dot on the screen, a grid on the screen, graphical bars or lines on the screen, or any other suitable visual cue.

[00104] The particular location of the visual cue on the screen may be provided to the user device 304 by signaling from the authentication computing system 100. In various embodiments, the particular location of the visual cue may change for each image capture process (similar to a rolling code, for example). As the user positions themselves in front of the reflective surface 310, they may also position the user device 304 in the proper relative placement as noted by the visual cue. The user may also provide any additional authentication variables (such as a gesture, gesture location, user device angle, and so forth). Once the user device 304 is in the proper position the user device 304 may automatically capture the image without additional input from the user. For example, in one operational example, the screen of the user device 304 may have a visual indication flashing in the upper left quadrant of the screen. Once the user device 304 detects, through image analysis, that the user device 304 is positioned in the upper left quadrant of the image, an image may be automatically captured and transmitted to the authentication computing system 100. While in some embodiments, the user device 304 may automatically capture an image, in other embodiments the user may initiate the image capture by pressing a button (physical or virtual) on the user device 304.

[00105] It is noted that an audio cue may alternatively or additionally serve as a form of assistance. For example, when the user has positioned in the user device 304 in the proper relative position, an audible alert may be provided by the user device 304. As is to be appreciated, other forms of assistance may be used, such as haptic feedback, for example.

[00106] The various image components of the image received from the user device 304 by an authentication computing system may be analyzed using any number of analytical techniques. FIG. 4A shows an analysis technique that divides the image 400 into a grid sixteen square segments. In one embodiment, the grid is keyed to a chin 404 of the user. As illustrated, the reflected light source 406 in the image 400 is located in segment 8. As part of the authentication, the authentication computing system analyzing the image 400 could use a two part process. First, the identity of the user could be determined by a biometric analysis of the user image 402. Second, the relative placement of the reflected light source 406 in the image could be used as an authentication variable. For example, a comparison could be made to a baseline image stored in a database in order to confirm the reflected light source 406 is in the proper segment. In some embodiments, the proper segment may change over time. In such embodiments, a user of the system would know in which segment to place the reflected light source 406 based on a time of day, day of the week, or based on where the user was physically located, for example.

[00107] FIG. 4B shows an analysis technique that uses distances between various features of the image 420 to confirm identity and provide authorization. The illustrated embodiment shows a shoulder width distance 422, a chin to shoulder vertical distance 424, and a reflected light source to chin distance 426 as variables. In some example embodiments, a relative angle of the reflected light source may be calculated or measured and compared to a baseline angle.

[00108] FIG. 4C shows an analysis technique that divides the image 440 into a plurality of pie shaped segments. While the illustrated embodiment shows six pie segments, this disclosure is not so limited. For example, the image 440 may be divided up into 12 pie shaped segments to emulate the face of an analog clock. The pie shaped segments may converge on the nose 442 of the user image 402, or may converge on another location (such as a gesture). As shown, the user is placing the reflected light source 406 in segment "B." Similar to the embodiment illustrated in FIG. 4A, the segment in FIG. 4C providing proper authorization may change over time. With a rolling segment approach, the overall security offered by the system may be increased.

[00109] FIG. 4D shows an analysis technique for determining an angle of incidence (shown as "θ") of the light source 306. The angle θ may be compared to a stored angular value as part of the authentication process. In FIG. 4D a top view of the user device 304 capturing a user image 402 and reflected light source 406 is provided. In the illustrated embodiment, angle θ is function of a distance 450 (the distance between the reflected light source 406 and a center of the user image 402) and the distance 458 (the distance between the user/light source 306 and the reflective surface 310). The distance 450 may be orthogonal to distance 458. It is noted that while the light source 306 and the user are illustrated as being co-planar with the reflected surface 310, this disclosure is not so limited. In other words, in some implementations, the user may position the light source 306 either closer to the reflective surface 310 or further way from the reflected surface 310 relative to the user.

[00110] The distance 458 may be determined by the authentication computing system 100 based on an analysis of one or more facial dimensions (or ratios of dimensions) of the user image 402. For example, a head width dimension 452, an eye width dimension 456, and/or a nose-to-ear dimension 454 may be determined by any suitable image processing technique. In one embodiment, the user image 402 may be vectorized by the authentication computing system 100 as part of the image analysis processing. Once the dimension(s) (and/or ratios) are determined, they can be compared to known biometric data stored by the authentication computing system 100 in order to extrapolate the distance 458. The distance 450 can also be determined, for example, by image analysis of the image received by the authentication computing system 100.

[00111] Once distances 450 and 458 are determined, in one embodiment, the angle θ may be calculated based on Equations 1 and 2:

$$Tan\,\theta = \frac{Distance\ 450}{Distance\ 458} \quad \text{EQ. 1}$$

$$\theta = ArcTan\frac{Distance\ 450}{Distance\ 458} \quad \text{EQ. 2}$$

[00112] Once angle θ has been determined, it can then be compared to an angular value stored by the authentication computing system 100 as an authentication variable.

[00113] By way of example, an angular value of 30° may be stored by the authentication computing system 100. If the determined angle θ is in the range of 27° to 33°, for example, the flash angle may be deemed authenticated. It is to be appreciated that the acceptable range of angles may vary. In some embodiments, for example, the determined angle may be authenticated if it is within +/- 25% of the stored angular value, while other embodiments may only permit authentication if the determined angle is within +/- 1% of the stored angular value.

[00114] In some embodiments, real-time image analysis of the image feed from the camera 312 may be used during the image capture process. For example, the image feed may be analyzed to determine one or more facial dimensions (or ratios of dimensions) of the user image 402, such as the head width dimension 452 and the

eye width dimension 456. When the dimensions are at a predetermined value (which may indicate the user is at a proper distance 458 from the reflective surface 310) the image may be automatically captured. As is to be appreciated, visual and/or audio cues can be provided to the user to assist with proper placement. Similar to above, the distance 450 may be determined by image analysis of the image received by the authentication computing system 100. Angle θ may then be determined using Equations 1 and 2, for example.

[00115] FIGS. 5A-5D show example images provided to an authentication computing system. Image 500 in FIG. 5A shows a user 504 holding a light source 506 at one position and a gesture 502 at another position. Images 500, 520, 540, and 560 illustrate the user 504, the light source 506, and the gesture 502 at other relative positions. As it to be appreciated, the features 504, the relative placement of the light source 506, the gesture 502, and the relative placement of the gesture relative to the user 504 and/or the light source 506 may be analyzed in accordance with the systems and methods described herein. It is noted that FIG. 5D illustrates that the image 560 may also include contextual data for processing by the authentication computing system. The contextual data may include device information, geographical location data, or other information which may be compared to expected contextual data stored by the system.

[00116] In some example embodiments, in addition or alternatively to the various authentication techniques described above, various authentication systems may perform a color signature analysis on the incoming image as part of the authentication process. FIG. 6 shows a user authentication process in accordance with one non-limiting embodiment. As shown at an event 610, a user is interacting with a computer device 612. The computing device 612 may be similar to user device 102 (FIG. 1) and may include a camera 614 and a graphical display 616. The computer device 612 may send a request 692 to an authentication module 600 through a communications network 690. The request 692 may be dispatched by an application running on the computing device 612. The request may include any information needed by the authentication module 600. The request may include, for example, a device ID or a user ID. Upon receipt of the request 692, the authentication computing system 600 may transmit a color key 694. The color key

694 may be stored in a color database 602. In various embodiments, the color key 694 may be in the form of a hex code or a decimal code, as shown in Table 1.

HTML name	Hex code	Decimal code
	R G B	**R G B**
IndianRed	CD 5C 5C	205 92 92
LightCoral	F0 80 80	240 128 128
Salmon	FA 80 72	250 128 114
DarkSalmon	E9 96 7A	233 150 122
LightSalmon	FF A0 7A	255 160 122
Red	FF 00 00	255 0 0
Crimson	DC 14 3C	220 20 60
FireBrick	B2 22 22	178 34 34
DarkRed	8B 00 00	139 0 0
Pink	FF C0 CB	255 192 203
LightPink	FF B6 C1	255 182 193
HotPink	FF 69 B4	255 105 180
DeepPink	FF 14 93	255 20 147
MediumVioletRed	C7 15 85	199 21 133
PaleVioletRed	DB 70 93	219 112 147
LightSalmon	FF A0 7A	255 160 122
Coral	FF 7F 50	255 127 80
Tomato	FF 63 47	255 99 71
OrangeRed	FF 45 00	255 69 0
DarkOrange	FF 8C 00	255 140 0
Orange	FF A5 00	255 165 0
Gold	FF D7 00	255 215 0
Yellow	FF FF 00	255 255 0
LightYellow	FF FF E0	255 255 224
LemonChiffon	FF FA CD	255 250 205
LightGoldenrodYellow	FA FA D2	250 250 210
PapayaWhip	FF EF D5	255 239 213
Moccasin	FF E4 B5	255 228 181
PeachPuff	FF DA B9	255 218 185
PaleGoldenrod	EE E8 AA	238 232 170
Khaki	F0 E6 8C	240 230 140
DarkKhaki	BD B7 6B	189 183 107
Lavender	E6 E6 FA	230 230 250
Thistle	D8 BF D8	216 191 216
Plum	DD A0 DD	221 160 221
Violet	EE 82 EE	238 130 238
Orchid	DA 70 D6	218 112 214
Fuchsia	FF 00 FF	255 0 255

Magenta	FF 00 FF	255 0 255
MediumOrchid	BA 55 D3	186 85 211
MediumPurple	93 70 DB	147 112 219
BlueViolet	8A 2B E2	138 43 226
DarkViolet	94 00 D3	148 0 211
DarkOrchid	99 32 CC	153 50 204
DarkMagenta	8B 00 8B	139 0 139
Purple	80 00 80	128 0 128
Indigo	4B 00 82	75 0 130
DarkSlateBlue	48 3D 8B	72 61 139
SlateBlue	6A 5A CD	106 90 205
MediumSlateBlue	7B 68 EE	123 104 238
GreenYellow	AD FF 2F	173 255 47
Chartreuse	7F FF 00	127 255 0
LawnGreen	7C FC 00	124 252 0
Lime	00 FF 00	0 255 0
LimeGreen	32 CD 32	50 205 50
PaleGreen	98 FB 98	152 251 152
LightGreen	90 EE 90	144 238 144
MediumSpringGreen	00 FA 9A	0 250 154
SpringGreen	00 FF 7F	0 255 127
MediumSeaGreen	3C B3 71	60 179 113
SeaGreen	2E 8B 57	46 139 87
ForestGreen	22 8B 22	34 139 34
Green	00 80 00	0 128 0
DarkGreen	00 64 00	0 100 0
YellowGreen	9A CD 32	154 205 50
OliveDrab	6B 8E 23	107 142 35
Olive	80 80 00	128 128 0
DarkOliveGreen	55 6B 2F	85 107 47
MediumAquamarine	66 CD AA	102 205 170
DarkSeaGreen	8F BC 8F	143 188 143
LightSeaGreen	20 B2 AA	32 178 170
DarkCyan	00 8B 8B	0 139 139
Teal	00 80 80	0 128 128
Aqua	00 FF FF	0 255 255
Cyan	00 FF FF	0 255 255
LightCyan	E0 FF FF	224 255 255
PaleTurquoise	AF EE EE	175 238 238
Aquamarine	7F FF D4	127 255 212
Turquoise	40 E0 D0	64 224 208
MediumTurquoise	48 D1 CC	72 209 204
DarkTurquoise	00 CE D1	0 206 209
CadetBlue	5F 9E A0	95 158 160
SteelBlue	46 82 B4	70 130 180

LightSteelBlue	B0 C4 DE	176 196 222
PowderBlue	B0 E0 E6	176 224 230
LightBlue	AD D8 E6	173 216 230
SkyBlue	87 CE EB	135 206 235
LightSkyBlue	87 CE FA	135 206 250
DeepSkyBlue	00 BF FF	0 191 255
DodgerBlue	1E 90 FF	30 144 255
CornflowerBlue	64 95 ED	100 149 237
RoyalBlue	41 69 E1	65 105 225
Blue	00 00 FF	0 0 255
MediumBlue	00 00 CD	0 0 205
DarkBlue	00 00 8B	0 0 139
Navy	00 00 80	0 0 128
MidnightBlue	19 19 70	25 25 112
Cornsilk	FF F8 DC	255 248 220
BlanchedAlmond	FF EB CD	255 235 205
Bisque	FF E4 C4	255 228 196
NavajoWhite	FF DE AD	255 222 173
Wheat	F5 DE B3	245 222 179
BurlyWood	DE B8 87	222 184 135
Tan	D2 B4 8C	210 180 140
RosyBrown	BC 8F 8F	188 143 143
SandyBrown	F4 A4 60	244 164 96
Goldenrod	DA A5 20	218 165 32
DarkGoldenrod	B8 86 0B	184 134 11
Peru	CD 85 3F	205 133 63
Chocolate	D2 69 1E	210 105 30
SaddleBrown	8B 45 13	139 69 19
Sienna	A0 52 2D	160 82 45
Brown	A5 2A 2A	165 42 42
Maroon	80 00 00	128 0 0
White	FF FF FF	255 255 255
Snow	FF FA FA	255 250 250
Honeydew	F0 FF F0	240 255 240
MintCream	F5 FF FA	245 255 250
Azure	F0 FF FF	240 255 255
AliceBlue	F0 F8 FF	240 248 255
GhostWhite	F8 F8 FF	248 248 255
WhiteSmoke	F5 F5 F5	245 245 245
Seashell	FF F5 EE	255 245 238
Beige	F5 F5 DC	245 245 220
OldLace	FD F5 E6	253 245 230
FloralWhite	FF FA F0	255 250 240
Ivory	FF FF F0	255 255 240
AntiqueWhite	FA EB D7	250 235 215

Linen	FA F0 E6	250 240 230
LavenderBlush	FF F0 F5	255 240 245
MistyRose	FF E4 E1	255 228 225
Gainsboro	DC DC DC	220 220 220
LightGrey	D3 D3 D3	211 211 211
Silver	C0 C0 C0	192 192 192
DarkGray	A9 A9 A9	169 169 169
Gray	80 80 80	128 128 128
DimGray	69 69 69	105 105 105
LightSlateGray	77 88 99	119 136 153
SlateGray	70 80 90	112 128 144
DarkSlateGray	2F 4F 4F	47 79 79
Black	00 00 00	0 0 0

TABLE 1: COLOR CHART

[00117] At event 630, the computing device 612 may output the color on the graphical display 616. The user can then position themselves proximate the graphical display 616 so that the color 618 is reflected off the user's feature as a color signature 620. In some embodiments, the user positions themselves within about 12 inches of the graphical display 616. The computer device 612 may then capture an image 622 of the user with accompanying color signature 620 using the camera 614. As is to be appreciated, while not illustrated in FIG. 6, the user may also make a gesture that could be captured by the camera 614. Furthermore, the graphical display 616 may be caused to sequentially display a plurality of different colors, such as to provide a color-keyed strobe affect, as described herein.

[00118] At event 650, the image 622 is sent to the authentication computing system 600, as illustrated by image upload 696. The image 622 may be encrypted using any suitable encryption scheme. Upon receipt, the authentication computing system 600 may perform various analytic processes on the image. For example, the authentication computing system 600 may perform a color analysis on the color signature 620 to confirm the proper color is present in the image and that it is properly reflected off the user. Furthermore, biometric analysis techniques may also be performed to the image received to confirm the identity of the user. Biometric information may be stored in a biometric database 604. As is to be appreciated, a gesture present in the image could also be analyzed by the authentication computing system as part of the authentication process. As is to be appreciated, the authentication computing system 600 may comprise a variety of databases 606 relevant to the authentication process. For example, in some embodiments, one or more databases 606 may store gesture-related information. Database 606 may also store various device specific variables, such as machine IDs. Database 606 (or other associated databases) may also various authentication variables, such as flash angle variables, user device angle variables, shutter/flash synchronicity variables, and so forth.

[00119] At event 670, an authentication confirmation 698 is sent to the computing device 612. Upon receipt of the authentication confirmation, an application, or other gatekeeper on the computing device, could allow the user access to the desired destination.

[00120] In some embodiments, a moving image scan may be utilized for authentication purposes. The moving image scan (sometimes referred to herein as a rotary scan) can generate image data that is recorded as a video file or can generate image data that is a series of still images. The image data may be obtained as a user moves a user device in a particular path in space proximate to the user's body. The particular path may be chosen so that image data regarding a user's body is collected from many different angles so that it may be analyzed as part of the authentication process. In one embodiment, the particular path is generally arc-shaped and circumnavigates at least a portion of a user's head or upper torso. In some embodiments, instead of moving the user device, the user may move in a predetermined path while the camera on the user device remains relatively still. For example, the user may slowly sweep or swivel their head side to side as image data is collected by a relatively stationary camera. The camera (such as a camera on a user device), may be held in the hand of a user or positioned on a stationary object, for example.

[00121] In addition to image data, additional contextual data may be collected during the moving image scan and provided to the authentication computing system as part of authentication processes utilizing "man and machine" binding. The contextual data may be collected by sensors that are onboard the user device, such as gyroscopes, accelerometers, and electromagnetic field meters, for example. This contextual data may be used by the authentication computing system to determine whether parameters associated with the predetermined path are within a particular range. For example, for proper authentication, a user may need to move the user device at a speed of about 2 ft/sec in a counter-clockwise direction, while the user device held at about a 45 degree angle. Information that may be used to determine if these requirements are satisfied may be provided as contextual data that is sent with image data to the authentication computing system. Furthermore, measurements related to electromagnetic fields may be included with the contextual data and be used to confirm that the user started and ended the path at the proper positions.

[00122] FIG. 7A depicts an example moving image scan in accordance with one non-limiting embodiment. A user device 702 includes an onboard camera 708 that may collect video and/or still images. As part of an authentication process the user 704 sweeps the user device 702 in a path 706 while the camera 708 collects image data. While the path 706 is shown as an arc, a variety of paths may be used, such as saw-tooth paths, v-shaped paths, linear paths, and so forth. FIG. 7B depicts an example moving image scan where the user 704 sweeps their head side to side in a path 706 while the camera 708 collects the image data. In other embodiments, the user may be required to nod their head up and down, move their head in a circular pattern, or otherwise execute a particular head and/or body movement. In any event, during or subsequent to the sweep, images 710 may be provided to an authentication computing system, such as the authentication computing system 100 shown in FIG. 1. The images 710 may include contextual data 712, which may include speed data, orientation data, machine ID, GPS data, and so forth. The images 710 and the contextual data 712 may be transmitted to the authentication computing system in an encrypted network packet, similar to the encrypted network packet 106 shown in FIG. 1. The authentication computing system can analyze the images 710 and the contextual data 712 to determine if the user 704 should be authenticated. For example, the images 710 may be compared to images in a baseline image database 124 (FIG. 1).

[00123] FIG. 7C depicts an example process flow 740 associated with a moving image scan. At 742, a camera is activated on a user device, such as a mobile computing device. At 744, sensor data from the mobile computing device is gathered. While a wide variety of sensor data can be gathered from the mobile computing device, example sensors 764 include, without limitation, a gyroscope 766, an accelerometer 768, a magnetometer 770, a camera 772, a GPS 774, among others. As described herein, in some embodiments the particular sensor data that is utilized by the process flow 740 may be based, at least in part, on the availability of resources, such as network bandwidth and battery power, for example. In any event, at 746 a face is moved in front of the camera, such as by sweeping the camera in front of the face (similar to the moving image scan described in FIG. 7A, for example). During the moving image scan, at time periods "Ts", the mobile computing device can find the face in the image and detect various fiducial points, as shown at 748. Time period Ts can be any suitable period of time, such as 0.03125 seconds (i.e., 32 frames/second), 0.1 seconds, 0.5 seconds, and so forth. As is to be appreciated, as the interval Ts is shortened, the needed bandwidth may increase. Example fiducuial points include eye locations, nose location, ear locations, facial measurements, and the like. At 750, camera movement is detected, by way of the sensor data gathered by the mobile computing device. Camera movement may be detected at intervals Ts. By way of the determined camera movement, it is can determined if the camera was moved by the user in the expected path. At 760, liveness of the user is detected. In one embodiment, liveness is confirmed based on changes of the face in the image matching the angular movements as detected by the sensors. Basing the determination off of angular movements can mitigate attempted spoofing by using a 2-dimensional image of a user. At 762, it is determined whether to authenticate user. Such determination may be made, for example, after a sufficient number of intervals Ts have elapsed, such as 5 intervals, 10 intervals, 20 intervals, 100 intervals, or 160 intervals, for example.

[00124] FIG. 8A depicts another example of an authentication process utilizing a moving image scan. The illustrated authentication process includes the use of a color signature, which is described above with regard to FIG. 6. A user device 802 includes a graphical display 816 and an onboard camera 808 that may collect video and/or still images. As part of an authentication process, the graphical display 816 projects a particular color 818, which may be reflected off the facial features of the user 804 as a color signature 820, as described above. The user 804 sweeps the user device 802 in a path 806 while the camera 808 collects image data, which includes the color signature 820. During or subsequent to the sweep, images 810 may be provided to an authentication computing system, such as the authentication computing system 100 shown in FIG. 1. The images 810 may include contextual data 812, as described above with regard to contextual data 712. The authentication computing system may analyze the images 810 and the contextual data 812 to determine if the user 804 should be authenticatedd.

[00125] FIG. 8B illustrates an example process flow 840 associated with a moving image scan utilizing multi-colored strobing. At 842, a scan is started. The scan may be generally similar to the moving image scan described with regard to FIG. 8A. At 844, an ambient light condition is sensed. Such condition may be sensed using an ambient light sensor onboard the user device 802 (FIG. 8A). If there is adequate ambient lighting to collect biometric data, the process can continued to execute authentication under normal light conditions, as shown at 860. If a low light condition exists (i.e., under a threshold lux level), the authentication process may utilize a multi-colored strobe technique to gather biometric data from the user. At 848, a multi-color strobe is activated by successively displaying different colors on a display of the user device 801. In one embodiment, one of seven colors is blinked twice on the screen. The color may be displayed on the display for a particular time period, such as Ts, described above. The periodic color strobe and the periodic collection of the image data may be coordinated so that image data is collected at times when the display is illuminated with a particular color. At 850, the camera is moved relative to a face. At 852, the camera is rotated with respect to the face such that images of the face at a plurality of different angular vantages can be collected. At 854, an image is received 854. As the color changes after Ts, additional images can be collected at 854. At 856, the illumination on the face with respect to both the angular position (as determined by sensor data) and the color data is determined. At 858, authentication is determined using biometric data, illumination data, and any other contextual data, such as geolocational information, machine ID, and so forth.

[00126] The data collected from the image scan using the strobing colors may not be sufficient to satisfy an authentication threshold. In some embodiments, a communication feedback loop between the authentication computing system and the user may be used to obtain the user's observations during the scan. For example, if the facial recognition data is not sufficient to authenticate the user, the authentication computing system can send an electronic communication to the user device. The electronic communication can be in any suitable format, such as a SMS text message, an email message, an "in-application" message, a messenger message, and so forth. The electronic communication can ask the user to identify the color or colors they saw on the screen during the attempted authentication. The user can reply with the color using any suitable messaging technique, such as a reply SMS message, for example. If the user's observation of the color data matches the color that was, in fact, blinked on the screed on the user device, the authentication computing system can use that observation to qualify the user. Accordingly, using this techniques, there generally two observers in the authentication process. The authentication computing system observes the illumination data reflected off the skin of a user by way of the image gathering process and the user observes the color that is displayed on the display of the user device.

[00127] In some embodiments, the authentication may include acquisition of images from a plurality of devices in either a sequential or concurrent image collection process. For example, for proper authentication, a handheld mobile device may need to collect a first image of a user and a laptop computer (or other computing device), collects a second image of the user. In other embodiments, a different collection of computing devices may be used to collect the images, such as a mobile device and a wall-mounted unit, for example. FIG. 9 illustrates an authentication process utilizing a multi-image acquisition process in accordance with one non-limiting embodiment. A user is positioned proximate to a first user device (shown as a smart phone) having a camera 904. The user is also positioned proximate to a second user device 906 (shown as a laptop) having a camera 908. While two user devices are illustrated in FIG. 9, some embodiments may utilize three more or more user devices. In any event, the first user device 902 collects first image 910 and the second user device collects second image 914. The first image 910 and the second image 914 may be collected at generally the same time or they may be collected sequentially. Each image 910, 914 may include associated contextual data 912, 916. The images 910, 914 may be provided to the authentication computing system 100 for processing. As shown, verification 130 may be provided to the first user device 902 if the authentication computing system 100 to indicate a successful authentication of the user. It is noted that while the verification 130 is shown being delivered to the first user device 902, the verification 130 may additionally or alternatively be delivered to the second user device 906.

[00128] FIG. 10 illustrates an authentication process utilizes multi-image acquisition process in accordance with another one non-limiting embodiment. The authentication process is generally similar to the process shown in FIG. 9. In FIG. 10, however, user movement 920 is required as part of the authentication process. Such movement may be used to aid in thwarting spoofing techniques. In some embodiments, the particular movement required of the user may be identified during the authentication process. For example, the first image 910 may be collected with the user at a first position. The user may then be instructed by one of the first and second user devices 904, 906 to perform a certain movement, such as raise an arm. The second image 914 may then be collected and analyzed by the authentication computing system 100 to confirm the user successfully completed the requested movement.

[00129] Various systems and methods described herein may generally provide resource aware mobile computing. Examples of resources that can be considered include, without limitation, network bandwidth, batter power, application settings, and the like. Based on the particular availability of the resources at the time of authentication, the system may change the type of biometric data collected and transmitted, the type of contextual data collected and transmitted, or change other authentication parameters. During periods of relatively high resource availability, the system can use authentication techniques that utilize large amount of resources, such as bandwidth, battery power, and the like. During periods of relatively low resource availability, the system can use authentication techniques that do not necessarily utilize large amount of resources. In some embodiments, authentication procedures, or at least some of the authentication procedures, may be performed local to the computing device by a local authentication computing system. The amount or portion of the authentication process performed local to the computing device compared to the amount or portion of the authentication process performed remotely (such as by authentication computing system 100), may be based on available resources, including environmental and/or operational factors. Example factors may include, without limitation, power source strength, available data transmission rates, available image processing ability, type of network connections available (i.e., cellular vs. WiFi), and so forth. Thus, resource-aware decision making may be used to determine which part of the authentication process is performed locally and which part of the authentication process is performed remotely. In some embodiments, the system attempts to perform the entire authentication process local to the user device. Such approach may be aimed to conserve bandwidth and/or to minimize communications over a network. If the user cannot be properly authenticated, communications with a remote authentication computing system may be utilized in an attempt to complete the authentication request. In some embodiments, if the battery supply of the client device is beneath a certain threshold, a majority of the authentication process is offloaded to the remote authentication computing system. Moreover, the number of authentication variables considered, or the types of authentication variables considered during the authentication process may be dependent on the environmental and/or operational factors. For example, during periods of high data connectivity and/or high-battery strength, the authentication computing system may require the user device to supply a relatively high number of authentication variables and/or resource intensive variables. During periods of low data connectivity and/or low battery strength, the authentication computing system may determine that a subset of authentication variables are suitable for authentication based on the operational conditions and request a limited number of authentication variables from the user device. In some embodiments, when the user device resumes high data connectivity and/or high battery strength, the authentication computing system may require the user to re-authenticate using additional authentication variables.

[00130] FIG. 11 illustrates an authentication computing system that comprises a local authentication computing system 1101 and a remote authentication computing system 1100. In the illustrated embodiment the remote authentication computing system 1100 comprises the elements of the authentication computing system 100 described above with regard to FIG. 1. The local authentication computing system 1101 is executed on a user device 102. The local authentication computing system 1100 may include a variety of modules or components for authenticating a user of the user device 102. For example, the local authentication computing system 1100 may comprise one or more processors 1116 and one or more computer memory units 1118. For convenience, only one processor 1116 and only one memory unit 1118 are shown in FIG. 11. In some embodiments, for example, the user device 102 includes a graphics processing unit (GPU). The processor 1116 may execute software instructions stored on the memory unit 1118. The processor 1116 may be implemented as an integrated circuit (IC) having one or multiple cores. The memory unit 1118 may include volatile and/or non-volatile memory units. Volatile memory units may include random access memory (RAM), for example. Non-volatile memory units may include read only memory (ROM), for example, as well as mechanical non-volatile memory systems, such as, for example, a hard disk drive, an optical disk drive, etc. The RAM and/or ROM memory units may be implemented as discrete memory ICs, for example.

[00131] The memory unit 1118 may store executable software and data for authentication engine 1120. When the processor 1116 of the local authentication computing system 1101 executes the software of the authentication engine 1120, the processor 1116 may be caused to perform the various operations of the local authentication computing system 1101, such as send information to remote computer devices, process information received from remote computer devices, and provide verification information regarding user authentication to applications executing on the user device 102. Data used by the authentication engine 1120 may be from various sources, either local or remote, such as a baseline image database 1124 and/or baseline image database 124. The data stored in the baseline image database 1124 may be stored in a non-volatile computer memory, such as a hard disk drive, a read only memory (e.g., a ROM IC), or other types of non-volatile memory.

[00132] The user device 102 in the illustrated embodiment also comprises various components, such as a camera 1130, a microphone 1132, an input device 1134, a display screen 1136, a speaker 1138, and a power supply 1140. As is to be readily appreciated, other types of user device may have different components as those illustrated in FIG. 11. In any event, the user may interact with various components during an authentication process. Depending on the available resources, the authentication engine 1120 may determine whether to perform some or all of the authentication process, or to offload some of all of the authentication process to the remote authentication computing system 1100. For example, if the available power in the power supply 1140 is relatively low, the user device 1101 may offload much of the authentication processing to the remote authentication computing system 1100. In another example, if the data connection to the remote authentication computing system 1100 is unstable, of low quality, or non-existent, the user device 1101 may perform much of the authentication processing using the local authentication computing system 1101.

[00133] FIG. 12 illustrates an example data transferring technique utilizing an authentication computing system. In the illustrated embodiment, the authentication computer system 100 illustrated in FIG. 1 is utilized. A first user (illustrated at User 1) determines which file 1212 to transmit using a user device 1210. The file 1212 may be any suitable type of electronic data file, such as a document file, an image file, a video file, or any other type of computer storable data. The first user may send an encrypted packet 1204 through a communications network 1202, such as a public network (i.e., the Internet), to the authentication computing system 100. The encrypted packet 1204 may include the file 1212 and recipient biometrics 1208. In one embodiment, the recipient biometrics 1208 includes an image of the recipient. In other embodiments, the recipient biometrics 1208 includes a recipient fingerprint, a recipient retina scan, or other recipient biometric identifier. In the illustrated embodiment, the second user (illustrated as User 2) is the intended recipient of the file 1212. Prior to being given access to the file 1212, the second user provides the user 2 biometrics 1214 to the authentication computing system 100. Such user 2 biometrics 1214 may include, for example, an image of the second user obtained using a camera (not shown) of the user device 1220. When the user 2 biometrics 1214 are deemed to match the recipient biometrics 1208, or at least satisfy a confidence threshold, that were originally provided by the first user, an encrypted packet 1216 may be delivered to the user device 1220 of the second user. The encrypted packet 1216 may include the file 1212.

[00134] While FIG. 12 illustrates a one-to-one file sharing scenario, other sharing scenarios may be facilitated by the authentication computing system 100, such as a one-to-many file sharing scenario. In such scenarios, user 1 may provide recipient biometrics 1208 for each of a plurality of recipients, such as a group of *N* recipients. When the file 1212 is encrypted, as described above, biometrics from of all of the plurality of recipients may be used. Subsequently, when a user seeks access to the encrypted file 1212, the authentication computing system 100 may determine if the biometrics of the user seeking access to the file matches any one of the recipient biometrics 1208 provided by user 1. The authentication computing system 100 may also utilized contextual data received from the user seeking access to the file, as described herein.

[00135] In yet another embodiment one-to-many sharing scenario, such as for high security type implementations, a certain number of recipients must concurrently access the encrypted file 1212 at the same time, or at least nearly at the same time, in order for the collective group to gain access to the encrypted file. Such techniques may seek to ensure that certain files are accessed only in presence of other people. By way of example, user 1 may identify the biometrics of *N* recipients that may access the file 1212, where *N*>1. User 1 may also identify a threshold number *k*, where *k*=1...N. Here, *k* is the number of recipients that must each provide individual biometrics before the file is decrypted so that the file may be accessed by the group of k recipients. The value for *k* can be any suitable number, and may vary based on implementation, the desired level of security, or any other factors. In some embodiment, *k* is set by the authentication computing system 100based on the number *N* of recipients such that *k* is a majority of *N*, for example. In some embodiments, *k* is 20% of *N*, rounded to the nearest integer, and so forth. Furthermore, in addition to having the requisite number of recipients providing biometrics, the authentication computing system 100 may also process contextual data associated with each recipient for an additional layer of security.

[00136] FIG. 13 illustrates an authentication process 1300 for a computing device using a color signature in accordance with one non-limiting embodiment. At block 1302, an application is executed. The application may be executed on a user device 102 (FIG. 1), for example. At block 1304, the application sends a call requesting a color key. The call may include various identification data. At block 1306, the color key is received. The color key may be in the form of a hex color code. At block 1308, the color is displayed on the display screen of the user device. At block 1310, a camera is activated. The camera may be integral or may be a standalone camera (such as a web cam, for example). At block 1312, an image is captured. The image may be of the face of the user with the color reflecting off the face as a color signature. At block 1314, the image may be cryptographically sent to an authentication computing system. At block 1316, an authentication confirmation is received when the face and the color signature is authenticated.

[00137] FIG. 14 illustrates an authentication process 1400 for an authentication computing system using a color signature in accordance with one non-limiting embodiment. At block 1402, a color key is requested from a mobile device. In some example embodiments, the request may be received from other types of devices, such as building access devices or desktop computers, for example. At block 1404, a particular color key is sent to the mobile device. At block 1406, an image is received from the mobile device. At block 1408, the biometric components of the image are analyzed. In some example embodiments, this analysis is performed by a third party biometric analytics service. At block 1410, color analysis is performed on a color signature of the image. In particular, the color signature can be analyzed to confirm it matches the signature for a particular user and that it is the same color as the color key originally sent to the mobile device. At block 1412, an authentication confirmation is sent to the mobile device when the face and the color signature is authenticated.

[00138] FIG. 15 illustrates an authentication process 1500 for a computing device in accordance with one non-limiting embodiment. At block 1502, an application is executed. At block 1504, a flash on the computing device is activated. At block 1506, the camera is activated. At block 1508, an image is captured by the camera. At block 1510, the image is sent to an authentication computing system. The image may be encrypted prior to transmission. In some embodiments, the computing device purges the image subsequent to the transmission so that there is no local copy of the image stored on the device. At block 1512, when the face and flash location have been authenticated by the authentication computing system, an authentication confirmation is received.

[00139] FIG. 16 illustrates an authentication process 1600 of an authentication computing system in accordance with one non-limiting embodiment. At block 1602, a baseline image is received from a mobile device. The baseline image may be stored in a baseline image database. The baseline image may contain various features, such as a gesture by a user and a relative location of a source of light. At block 1604, an image is received from the mobile device for the purposes of authentication. At block 1606, biometric analysis may be performed on the user's features (such as facial features, hand features, fingerprint features, or retinal features, for example). At block 1608, the location of the flash in the received image is compared to the location of the flash in the baseline image. In some embodiments, the baseline image must be updated (changed) periodically. In any event, at block 1610, when the face and flash location are authenticated, an authentication confirmation is sent to the mobile device. As discussed herein, additional layers of authentication may also be performed, such as analysis of locational data or device data, for example.

[00140] FIG. 17 illustrates a user's authentication process 1700 in accordance with one non-limiting embodiment. At block 1702, a user holds a mobile device with its flash activated. At block 1704, the user faces a reflective surface. At block 1706, the user makes a gesture and positions the gesture relative to their body, the mobile device, or other object. At block 1708, the user positions the active flash in a particular position. At block 1710, a photograph of the reflective surface is taken by a camera of the mobile device. At block 1712, the photograph is uploaded for authentication. As is to be appreciated, any number of authentication variables may be provided with the uploaded image at block 1712. For example, uploaded authentication variables may include, without limitation, the mobile device angle, the shutter/flash synchronicity information, location information and so forth.

[00141] FIG. 18A illustrates an example message flow diagram 1800 for a registration process in accordance with one embodiment. The message flow diagram 1800 generally depicts messages utilized by a user device 1802 and an authentication computing system 1806, some of which may be sent through a communications network 1804, during user registration. The user device 1802 comprises a biometric collection tool 1808 and a contextual data collection tool 1810.

The biometric collection tool 1808 may be, for example, a digital camera, a retina scanner, a fingerprint scanner or any other suitable device. The contextual data collection tool 1810 may include software and/or hardware components for acquiring data, such as geolocational data, user device movement data, machine identification data, and so forth. The biometric collection tool 1808 and a contextual data collection tool 1810 may respectively provide, via messages 1822 and 1824, data to the processor 1812. The messages 1822 and 1824 may generally provide various types of data unique to the user and the user device 1802. The processor 1812 may perform pre-transmission processing of the data, such as crop an image collected by the biometric collection tool 1808, convert an image to grey scale, convert a file type of the image (i.e., convert to .BMP), create array of images, normalize the data to a particular format, encrypt the data, and so forth.

[00142] Subsequent to any pre-transmission processing, the processor 1812 may cause a message 1826 to be sent through the communications network 1804 to the authentication computing system 1806. The message 1826 may be received by a listener 1814. The listener 1814 may be “listening,” for example, to messages transmitted using HTTP or HTTPS protocols for an authentication request or a registration request. Here, the message 1826 is an authentication request so the listener 1814 provides a message 1828 which includes registration data to a processor 1816. The processor 1816 may process the information received and then provide a message 1830 to a user database 1818, a message 1832 to a biometric database 1820, and a message 1834 to a contextual database 1822. The message 1830 may identify provide user identification data (such as social security number, patient ID number, account number, etc.), the message 1832 may include, for example, image data, and the message 1834 may include, for example, geolocational data and/or machine identification data. Generally, the messages 1830, 1832, and 1834 register a user of the user device 1802 with the authentication computing system 1806. The database 1818, 1820, and 1822 may be implemented using any suitable type of database hardware or software. For example, in some embodiments, cloud-based storage systems are utilized.

[00143] FIG. 18B depicts an example message flow diagram 1840 for an authentication process in accordance with one embodiment. The message flow diagram 1840 generally depicts messages utilized by the user device 1802 and the authentication computing system 1806, some of which may be sent through the communications network 1804, during user authentication. As part of the authentication process, the biometric collection tool 1808 and the contextual data collection tool 1810 may respectively provide, via messages 1850 and 1852, data to the processor 1812. The messages 1850 and 1852 may generally provide various types of data unique to the user and the user device 1802. Similar to the processing described in FIG. 18A, the processor 1812 may perform pre-transmission processing of the data. It is noted that the contextual data delivered using message 1852 may vary. For example, the type of user device 1802 (including the type of on-board sensors) or the operational conditions (such data transmission rates, for example), may at least partially determine which type of contextual data may be transmitted to authentication purposes.

[00144] Subsequent to any pre-transmission processing, the processor 1812 may cause a message 1854 to be sent through the communications network 1804 to the authentication computing system 1806. The message 1854 may be received by a listener 1814, as described above. Here, the message 1854 is a registration request so the listener 1814 provides a message 1856, which includes authentication data, to the processor 1816. The processor 1816 may execute an authentication process utilizing various database calls. A message 1858 to the user database 1818 may seek confirmation of a user's personal data included in the message 1854, such as SSN, patient number, user name, account number, and so forth. A message 1860 may indicate whether a positive match was found.

[00145] A message 1862 to the biometric database 1818 may seek confirmation of a user's biometric data included in the message 1854, such as facial data, fingerprint data, and so forth. In some embodiments, the biometric data is a streamed collection of facial images. A message 1864 may indicate whether a positive match was found. As is to be appreciated, a positive match of the biometric data may be based on a threshold confidence level or other metric. A message 1866 to the contextual database 1822 may seek authentication of various types of additional data received from the user device 1802, such as geolocational data and/or machine identification data. A message 1868 indicates if a positive match for contextual data was found. In some embodiments, the confidence level threshold for biometric data, along with the confidence level thresholds for other types of contextual data that are analyzed may be selectively increased or decreased to adjust the overall usability of function of the authentication system.

[00146] Upon receiving and processing the information from the various databases, the processor 1816 may provide an authentication request response message 1870 to the listener 1814. In turn, the listener 1814 may transmit a message 1872 through the network 1804 to the user device 1802 indicating a positive or negative authentication.

[00147] Authentication processes in accordance with the present systems and methods may be triggered using any suitable techniques. For example, when a user seeks to access a protection computing device, application, electronic document, and so forth, the authentication process may be triggered. In some embodiments, a transponder (such as an RFID device) may be positioned proximate to a restricted access device, such as a lockable door. Upon a user approaching the restricted access device, the transponder may trigger an authentication process to activate on a user device of the user. The user device may gather and provide information, such as biometric data and contextual data, to an authentication computing system associated with door. When authentication is successfully performed, an unlock command may be transmitted to the restricted access device.

[00148] FIG. 19A illustrates an example simplified block diagram for a user registration process. In some embodiments, the authentication computing system 1900 is implemented as a DLL access server. The authentication computing system 1900 may be positioned behind a firewall 1904, which may generally serve protect enterprise data stored by the authentication computing system, for example. A user device 1916 may be in communication with the authentication computing system 1900 through a communications network 1904. The user device 1916 may be provided using any suitable processor-based device or system, such as a personal computer, laptop, server, mainframe, or a collection (e.g., network) of multiple computers, for example. The user device 1916 may include one or more processors 1918 and one or more computer memory units 1920. For convenience, only one processor 1918 and only one memory unit 1920 are shown in FIG. 19A. The processor 1918 may execute software instructions stored on the memory unit 1924, such as a web browsing application 1924. The processor 1918 may be implemented as an integrated circuit (IC) having one or multiple cores. The memory unit 1920 may include volatile and/or non-volatile memory units. Volatile memory units may include random access memory (RAM), for example. Non-volatile memory units may include read only memory (ROM), for example, as well as mechanical non-volatile memory systems, such as, for example, a hard disk drive, an optical disk drive, etc. The RAM and/or ROM memory units may be implemented as discrete memory ICs, for example.

[00149] The memory unit 1920 may store executable software and data. When the processor 1918 of the user device 1916 executes the software, the processor 1918 may be caused to perform the various operations used for registration and authentication of a use of the user device 1916, such as send information to the authentication computing system 1900 and process information received from the authentication computing system 1900.

[00150] The user device 1916 may comprise a wide variety of components, some example of which are illustrated in FIG. 19A. For example, the user device 1916 may comprise a biometric collection unit 1922 for collecting biometric information from a user of the user device 1916. In certain embodiments, the biometric collection unit 1922 is a digital camera. The user device 1916 may also include, without limitation, an accelerometer 1926, a magnetometer 1928, or any other type of sensor 1930, device, or component (such as an ambient light sensor, gyroscopic sensor, microphone, proximity sensor, and so forth) that may be used for collecting data or information that may be provided to the authentication computing system 1900 during a registration or authentication process.

[00151] During a registration process, the user device 1916 may transmit a communication 1906 to the authentication computing system 1900. The communication 1906, or at least components of the communication, may be encrypted. In the illustrated embodiment, the communication 1906 comprises base image data 1908 and contextual data 1910. The base image data 1908 may be, for example, a series of streamed images of a user. The contextual data 1910 may comprise information gathered from one or more sensors, such as magnetometer

1928, information regarding the user device 1916, such as a machine ID or ESN, for example. Upon processing by the authentication computing system 1900, an output 1912 may be provided to the user device 1916. The output 1912 may include, for example, an indication 1914 that registration is complete.

[00152] Subsequent to registration with the authentication computing system, a use may seek an authorization request. FIG. 19B illustrates an example simplified block diagram for a user authentication process. In the illustrated embodiment, an authorization request 1950 comprises image data 1952 and contextual data 1954. The image data 1952 may be, for example, streamed image data of a user's face. The contextual data 1954 may include, for example, machine ID or ESN information, acceleration or movement data, magnetic field data, and so forth. In any event, based on the image data 1952 and the contextual data 1954, the authentication computing system 1900 may determine whether the user of the user device 1916 is an authenticated user. An output 1956 may be transmitted to the user device 1916 to convey the results of the authentication request, which may include an indication of authentication 1958 or an indication of non-authentication 1960.

[00153] FIG. 20A illustrates an example process for registering a user with an authentication computing system. At 2000, a camera on a user device is activated. The user device may be a component of, for example, a mobile computing device, a laptop computer, a desktop computer, a table computer, a wall-mounted device, and so forth. At 2002, the liveness of a user is detected using any suitable technique or combination of suitable techniques. The particular technique or techniques used may vary on operational conditions, such as ambient lighting conditions, available data transfer rates, battery life, and so forth. A rotary facial scan 2004 may be employed in suitable conditions, such as high ambient lighting conditions. Image collection during a color keyed strobe 2006 may be used, such as during low ambient conditions. During a color keyed strobe, a screen on a user device may be sequentially changed colors, which images of the user's face positioned close to the screen sequentially collected. Other techniques 2008 may be used to detect liveness, such as instructing a user to make certain movements, say certain words, and so forth. At 2010, a plurality of facial images are collected by the camera. In some embodiments, each facial image is a non-compressed file that is 100 pixels by

100 pixels, although other formats may be used. At 2012, an array of the images is streamed to an authentication computing system. In some embodiments, five facial images are combined into a 100 pixel by 500 pixel array. At 2014, contextual data is streamed. As provided herein, the contextual data may include, for example, machine identification data, geolocational data, movement data, and so forth. At 2016, upon satisfaction of the registration requirements, the user is registered with the authentication computing system.

[00154] FIG. 20B illustrates an example process for authenticating a registered user of an authentication computing system. At 2050, a camera on a user device is activated. As described above with regard to FIG. 20A, the user device may be a component of, for example, a mobile computing device, a laptop computer, a desktop computer, a table computer, a wall-mounted device, and so forth. At 2052, the liveness of the user seeking authentication is detected. Example techniques for detecting liveness during the authentication process include a rotary scan 2054, a color keyed strobe 2056, or other technique 2058, such as requiring certain movements or audio responses by a user. At 2060, one or more facial images are gathered and at 2062, the one or more facial images are streamed to an authentication computing system. At 2064, contextual data associated with the user device is streamed to the authentication computing system. At 2066, the user is authenticated based on processing of the facial images and the contextual data.

[00155] In some embodiments, an authentication computing system in accordance with the systems and methods described herein may be used by a certain relying parties, such as using an OpenID-type authentication. FIG. 21 illustrates an example communication block diagram. A protected application 2106 may be accessible via a use device 2108. The protected application 2106 may be, without limitation, a website, a local application, a remote application, and so forth. A user operating the user device may either be a registered user of the OpenID platform 2104 or need to become a registered user in order to access the protected application 2106. As illustrated, during a “new user” registration process credentials may be logged with an authentication computing system 2100. In some embodiments, the credentials include both a user ID and biometric data, such as an image. Once the user is registered with the OpenID platform 2104, the user’s credentials may be provided to the authentication computing system 2100 (which may include biometric data) so that a user may be authenticated. It is noted that communications between the protected application 2106 and the authentication computing system 2100 may be facilitated through one or more application programming interfaces 2102. Accordingly, in some embodiments, the authentication computing system 2100 may generally function as a third party, biometric authentication tool for a variety of websites, applications, and the like.

[00156] FIG. 22 illustrates a system flow diagram 2200 for photo cloaking utilizing biometric key generation. In the illustrated embodiment, secret image/text 2204A may be any type of data that a use wishes to transmit in an encrypted format. The system flow also utilizes a cover image 2202A. At 2206, encryption is performed such that the secret image/text 2204A is hidden within the cover image 2202A utilizing a biometric/contextual data encryption technique. An example biometric/contextual data encryption technique is described in more detail below with regard to FIG. 23. A stego object 2208 is created that generally comprises the cover image 2202A with the secret image/text 2204A embedded in it. The stego object 2208 can then be transmitted through a communications network 2210, which can include, for example, a public network. At 2212, the stego object 2208 can be decrypted using the biometric/contextual data key 2210. As a result, a cover image 2204B and secret text 2204B are extracted from the stego object 2208, with the cover image 2204B and secret text 2204B being similar, or identical to, the cover image 2202A and the secret image/text 2204A.

[00157] FIG. 23 illustrates an example biometric encryption system flow diagram 2300. The system flow diagram generally includes three aspects, namely an input-side 2302, a network 2304, and a target-side 2306. A variety of operational environments can utilize the system flow diagram 2300, such as a first user operating a first smart phone on the input-side 2302 and communicating with a second user operating a second smart phone on the target-side 2306. The first and second user may be, for example, chatting using a real-time chatting application utilizing communications over the network 2304. Using the systems and methods described herein, the first user can share a document, image, or other type of data file utilizing the described encryption process. The data file may be shared in generally real-time using the network 2304. In the illustrated embodiment, the document desired to be shared is shown as a sensitive document 2308A. The sensitive document 2308A may be any type of data capable of being transmitted over a network. Prior to transmitting the sensitive document 2308A, it may be encrypted using an encryption key 2310. Generally, the encryption key 2310 enables the sensitive document 2308A to be securely shared over a public network and requiring the target recipient to provide biometric and contextual data to access the sensitive document 2308A. In the illustrated embodiment, a plurality of variants are provided at the input-side 2302 to form the encryption key 2310, including a target user location 2312, target biometrics 2314, and a time duration of validity 2316. The target user location 2312 provided may vary based on implementation. In some cases, a city or address of the target is provided. In some cases, latitude and longitude coordinates are provided. Other implementations may use other techniques for identifying a geographic location of a target. The target biometrics 2314 can include, for example, an image of the target user stored within a target biometrics database 2318. The target biometrics database 2318 can be local to the input side 2302, or hosted by a third party, such as a social networking website, or example. In some embodiments, the target biometrics 2314 is an image selected from a digital photo album stored on a user device. In some embodiments, target biometrics 2314 may include the biometrics for *N* recipients, as described above with regard to FIG. 12. In any event, the encryption key 2310 may then be created based on the biometric data of the target along with various forms of contextual information. Once the encryption key 2310 key is generated, an encrypted document 2320 may then be transmitted via the network 2304 to a user device of the target. In order to retrieve the sensitive document, target biometrics are retrieved 2322 (i.e., using a camera associated with a user device of the target), target location is retrieved 2324 (i.e, based on GPS data), and a time of access 2326 is determined (i.e, based on network time). When the target satisfies the confidence thresholds associated with all of the various variables, the document is decrypted at 2328 and a copy of the sensitive document 2308B may be provided to the target. As is to be readily appreciated, the authentication process at the target-side 2306 can include any of various authentication techniques described herein, such as color strobing, livness detection, moving image scans, and so forth. Furthermore, when biometric encryption system flow diagram 2300 is used with one-to-many file sharing scenarios, similar to those described above, the document may be decrypted at 2328 only after a sufficient number of recipients, such as *k* recipients, provide their biometrics to an authentication engine.

[00158] In general, it will be apparent to one of ordinary skill in the art that at least some of the embodiments described herein may be implemented in many different embodiments of software, firmware, and/or hardware. The software and firmware code may be executed by a processor or any other similar computing device. The software code or specialized control hardware that may be used to implement embodiments is not limiting. For example, embodiments described herein may be implemented in computer software using any suitable computer software language type, using, for example, conventional or object-oriented techniques. Such software may be stored on any type of suitable computer-readable medium or media, such as, for example, a magnetic or optical storage medium. The operation and behavior of the embodiments may be described without specific reference to specific software code or specialized hardware components. The absence of such specific references is feasible, because it is clearly understood that artisans of ordinary skill would be able to design software and control hardware to implement the embodiments based on the present description with no more than reasonable effort and without undue experimentation.

[00159] Moreover, the processes associated with the present embodiments may be executed by programmable equipment, such as computers or computer systems and/or processors. Software that may cause programmable equipment to execute processes may be stored in any storage device, such as, for example, a computer system (nonvolatile) memory, an optical disk, magnetic tape, or magnetic disk. Furthermore, at least some of the processes may be programmed when the computer system is manufactured or stored on various types of computer-readable media.

[00160] It can also be appreciated that certain process aspects described herein may be performed using instructions stored on a computer-readable medium or media that direct a computer system to perform the process steps. A computer-readable medium may include, for example, memory devices such as diskettes, compact discs (CDs), digital versatile discs (DVDs), optical disk drives, or hard disk drives. A computer-readable medium may also include memory storage that is physical, virtual, permanent, temporary, semipermanent, and/or semitemporary.

[00161] A “computer,” “computer system,” “host,” “server,” or “processor” may be, for example and without limitation, a processor, microcomputer, minicomputer, server, mainframe, laptop, personal data assistant (PDA), wireless e-mail device, cellular phone, pager, processor, fax machine, scanner, or any other programmable device configured to transmit and/or receive data over a network. Computer systems and computer-based devices disclosed herein may include memory for storing certain software modules used in obtaining, processing, and communicating information. It can be appreciated that such memory may be internal or external with respect to operation of the disclosed embodiments. The memory may also include any means for storing software, including a hard disk, an optical disk, floppy disk, ROM (read only memory), RAM (random access memory), PROM (programmable ROM), EEPROM (electrically erasable PROM) and/or other computer-readable media.

[00162] In various embodiments disclosed herein, a single component may be replaced by multiple components and multiple components may be replaced by a single component to perform a given function or functions. Except where such substitution would not be operative, such substitution is within the intended scope of the embodiments. Any servers described herein, for example, may be replaced by a “server farm” or other grouping of networked servers (such as server blades) that are located and configured for cooperative functions. It can be appreciated that a server farm may serve to distribute workload between/among individual components of the farm and may expedite computing processes by harnessing the collective and cooperative power of multiple servers. Such server farms may employ load-balancing software that accomplishes tasks such as, for example, tracking demand for processing power from different machines, prioritizing and scheduling tasks based on network demand and/or providing backup contingency in the event of component failure or reduction in operability.

[00163] The computer systems may comprise one or more processors in communication with memory (e.g., RAM or ROM) via one or more data buses. The data buses may carry electrical signals between the processor(s) and the memory.

The processor and the memory may comprise electrical circuits that conduct electrical current. Charge states of various components of the circuits, such as solid state transistors of the processor(s) and/or memory circuit(s), may change during operation of the circuits.

[00164] While various embodiments have been described herein, it should be apparent that various modifications, alterations, and adaptations to those embodiments may occur to persons skilled in the art with attainment of at least some of the advantages. The disclosed embodiments are therefore intended to include all such modifications, alterations, and adaptations without departing from the scope of the embodiments as set forth herein.

What is claimed:

1. A computer-based method of authenticating, the method comprising:

receiving a request for authentication of a user, wherein the request for authentication comprises a biometric feature of the user collected by a user device and contextual data from the user device;

comparing the biometric feature of the user to baseline biometric feature of the user;

comparing the contextual data to an expected contextual data value; and

determining whether to authenticate the user based on the comparison of the biometric feature of the user to the baseline biometric feature of the user and the comparison of the contextual data to the expected contextual data value.

2. The computer-based method of authenticating of claim 1, wherein the contextual data is a machine identification (ID) of the user device.

3. The computer-based method of authenticating of claim 1, wherein the contextual data is data collected from a sensor of the user device.

4. The computer-based method of authenticating of claim 3, wherein the sensor is any of an accelerometer, a gyroscope, and a magnetometer.

5. The computer-based method of authenticating of claim 1, comprising:

receiving an image of the user, the image comprising the biometric feature, wherein a baseline image includes the baseline biometric feature.

6. The computer-based method of authenticating of claim 5, comprising:

comparing a first gesture made by the user in the image of the user to a second gesture in the baseline image.

7. The computer-based method of authenticating of claim 6, comprising:

comparing a location of the first gesture in the image to a location of the second gesture in the baseline image.

8. The computer-based method of authenticating of claim 5, comparing a location of a first camera flash location in the image to a location of a second camera flash location in the baseline image..

9. The computer-based method of authenticating of claim 1, wherein the contextual data is a geographical location of the user device.

10. The computer-based method of authenticating of claim 1, comprising:

transmitting to the user device a color key, wherein the biometric feature of the user collected by a user device comprises a color signature of the user.

11. The computer-based method of authenticating of claim 10, comprising comparing the color signature of the user to a stored color signature of the user.

12. The computer-based method of authenticating of claim 1, wherein the user device is a first user device and the biometric feature is included in a first image, wherein the request for authentication comprises the first image of the user collected by the first user device and a second image including the biometric feature of the user collected by a second user device.

13. The computer-based method of authenticating of claim 12, comprising: comparing the first image of the user to a first baseline image and the second image of the user to a second baseline image.

14. The computer-based method of authenticating of claim 1, wherein the image is collected during a rotary scan of the user.

15. A computer-based authentication system, comprising:

a baseline image database;

a contextual data database;

an authentication computing system, the authentication system configured to:

receive a request for authentication of a user from a user device, wherein the request for authentication comprises

an image of the user; and

contextual data;

compare the image of the user to a baseline image of the user stored in the baseline image database;

compare the contextual data to an expected contextual data value stored in the contextual data database; and

determine whether to authenticate the user based on the comparison of the biometric feature of the user to the baseline image of the user and the comparison of the contextual data to the expected contextual data value.

16. The computer-based authentication system of claim 15, wherein the contextual data indicates a geographical location of the user device.

17. The computer-based authentication system of claim 15, wherein the contextual data is acceleration data collected from an accelerometer.

18. The computer-based authentication system of claim 15, wherein the baseline image comprises a first hand gesture, and wherein the authentication system configured to compare a second hand gesture made by the user in the image of the user to the first gesture made by the user in the baseline image.

19. The computer-based authentication system of claim 18, wherein the authentication system is configured to compare a location of the first gesture in the image to a location of the second gesture in the baseline image.

20. A non-transitory computer readable medium having instructions stored thereon which when executed by a processor cause the processor to:

receive a request for authentication of a user, wherein the request for authentication comprises

an image of the user collected by a user device; and contextual data from the user device;

compare the image of the user to a baseline image of the user;

compare the contextual data to an expected contextual data value; and

determine whether to authenticate the user based on the comparison of the biometric feature of the user to the baseline image of the user and the comparison of the contextual data to the expected contextual data value.

21. The non-transitory computer readable medium of claim 20, wherein the contextual data is a geographical location of the user device.

22. The non-transitory computer readable medium of claim 20, wherein the contextual data is gathered by a sensor of the user device.

23. The non-transitory computer readable medium of claim 20, wherein the instructions cause the processor to compare a first gesture made by the user in the image of the user to a second gesture in the baseline image.

24. The non-transitory computer readable medium of claim 23, wherein the instructions cause the processor to compare a location of the first gesture in the image to a location of the second gesture in the baseline image.

25. A non-transitory computer readable medium having instructions stored thereon which when executed by a processor cause the processor to:

receive from a first user device via a network communication a network packet comprising an electronic data file and recipient biometrics;

receive from a second user device via network communication biometric data obtained from a user of the second user device; and

when the biometric data obtained from the user of the second user device matches the recipient biometrics, permit the electronic data file to be accessed on the second user device.

26. The non-transitory computer readable medium of claim 25, wherein the recipient biometrics is a facial image of a recipient.

27. The non-transitory computer readable medium of claim 26, wherein the biometric data obtained from the user of the second user device is an image of a face of the user of the second user device.

28. The non-transitory computer readable medium of claim 25, wherein the electronic data file is encrypted based on biometrics of the second user and contextual data associated with the second user.

29. The non-transitory computer readable medium of claim 25, wherein the recipient biometrics comprises biometrics from each of a plurality of recipients, and wherein the biometric data obtained from a user of the second user device comprises biometric data obtained from each of a plurality of users of the second user device.

30. The non-transitory computer readable medium of claim 25, wherein the instructions cause the processor to permit the electronic data file to be accessed on the second user device when the biometric data obtained from each of a plurality of users of the second user device matches corresponding recipient biometrics received from the first user device.

31. The non-transitory computer readable medium of claim 25, wherein the plurality of recipients comprises *N* recipients, where *N* is an integer, and wherein the plurality of users of the second user comprises *k* recipients.

32. The non-transitory computer readable medium of claim 25, wherein $k<N$.

33. A method of electronically sharing data, comprising:

identifying an electronic file;

providing biometrics associated with a recipient;

providing contextual data associated with a recipient;

causing the electronic file to be encrypted based on the provided biometrics and the provided contextual data; and causing the transmission of the encrypted electronic file to the recipient over an electronic communications network.

34. The method of electronically sharing data of claim 33, wherein providing the biometrics associated with a recipient comprises selecting a digital image of the recipient's face.

35. The method of electronically sharing data of claim 33, wherein providing contextual data associated with the recipient comprises identifying a geographic location of the recipient.

36. The method of electronically sharing data of claim 33, wherein providing biometrics comprises providing biometrics from each of a plurality of recipients.

37. The method of electronically sharing data of claim 33, wherein the plurality of recipients comprises *N* recipients, where *N* is an integer.

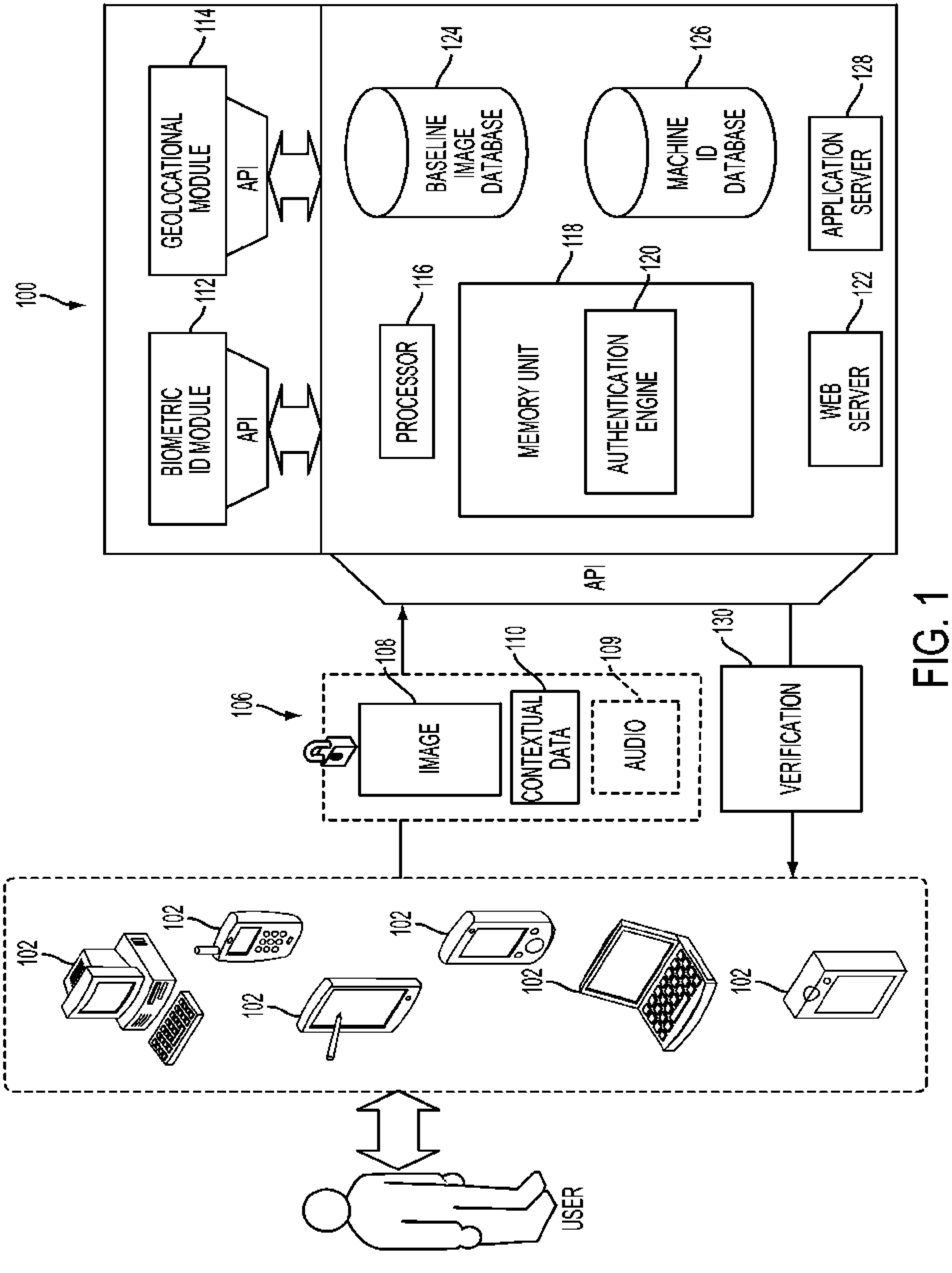

100
BIOMETRIC ID MODULE
API
112
GEOLOCATIONAL MODULE
API
114
PROCESSOR
116
MEMORY UNIT
118
AUTHENTICATION ENGINE
120
WEB SERVER
122
BASELINE IMAGE DATABASE
124
MACHINE ID DATABASE
126
APPLICATION SERVER
128
API
106
IMAGE
108
AUDIO
109
CONTEXTUAL DATA
110
VERIFICATION
130
102
102
102
102
102
102
USER

FIG. 1

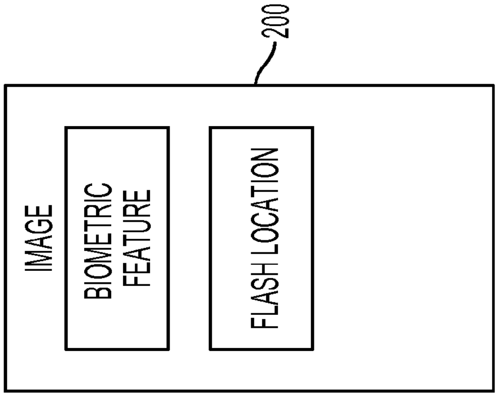


FIG. 2A

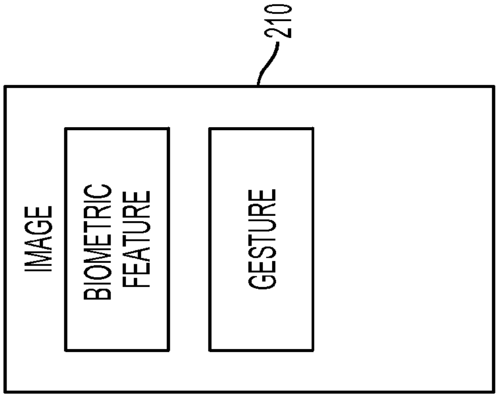


FIG. 2B

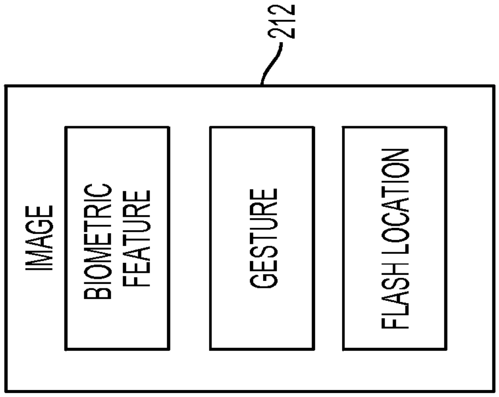


FIG. 2C

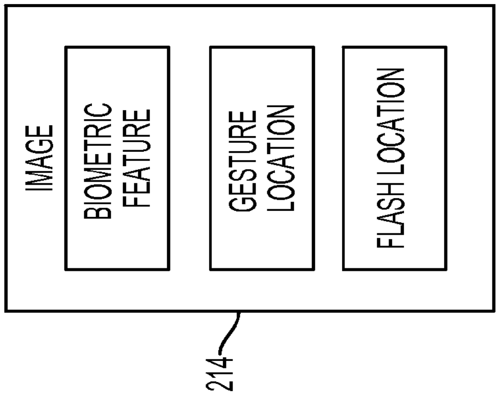


FIG. 2D

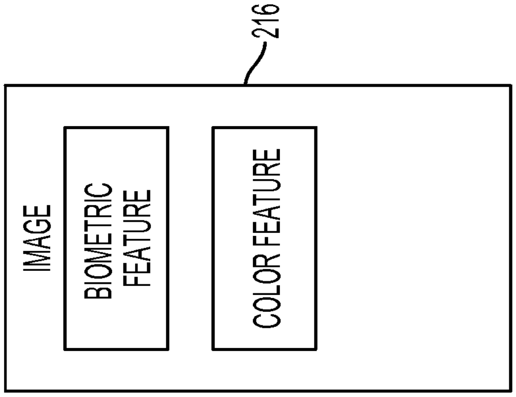


FIG. 2E

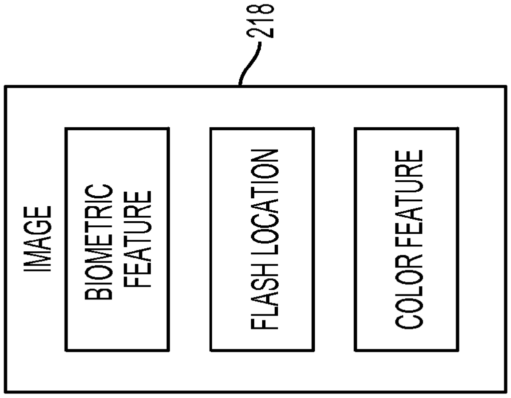


FIG. 2F

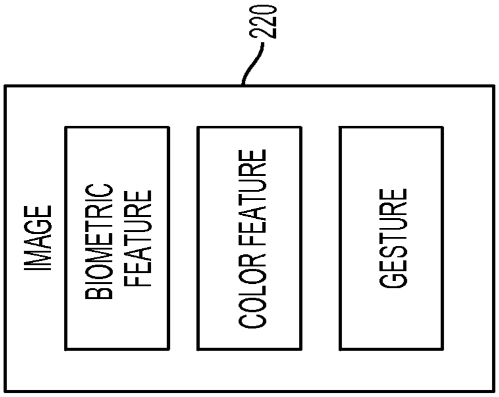


FIG. 2G

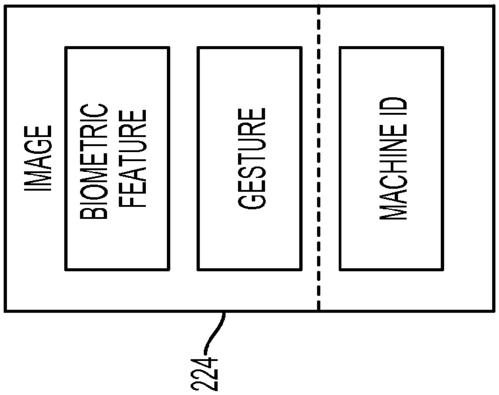


FIG. 2H

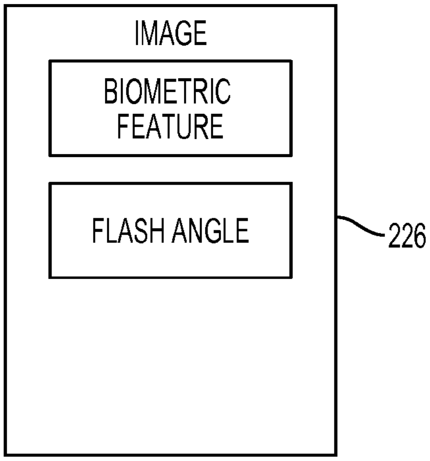


FIG. 2I

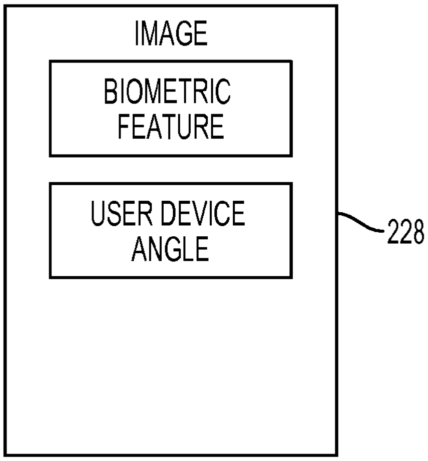


FIG. 2J

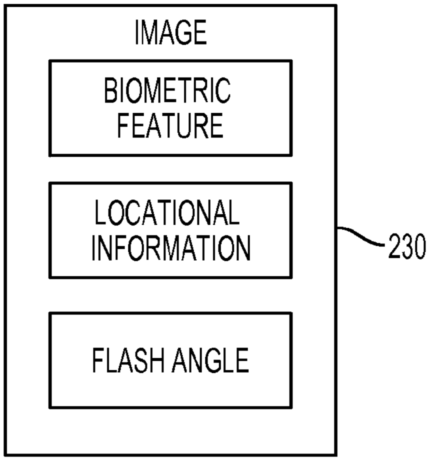


FIG. 2K

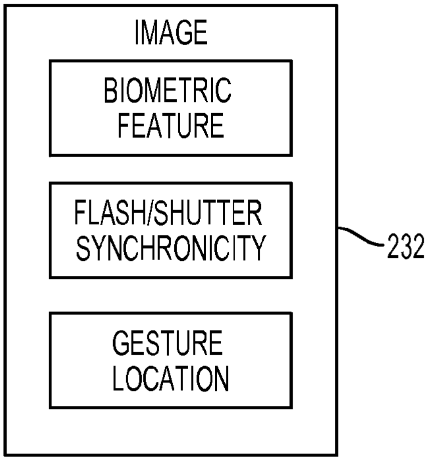


FIG. 2L

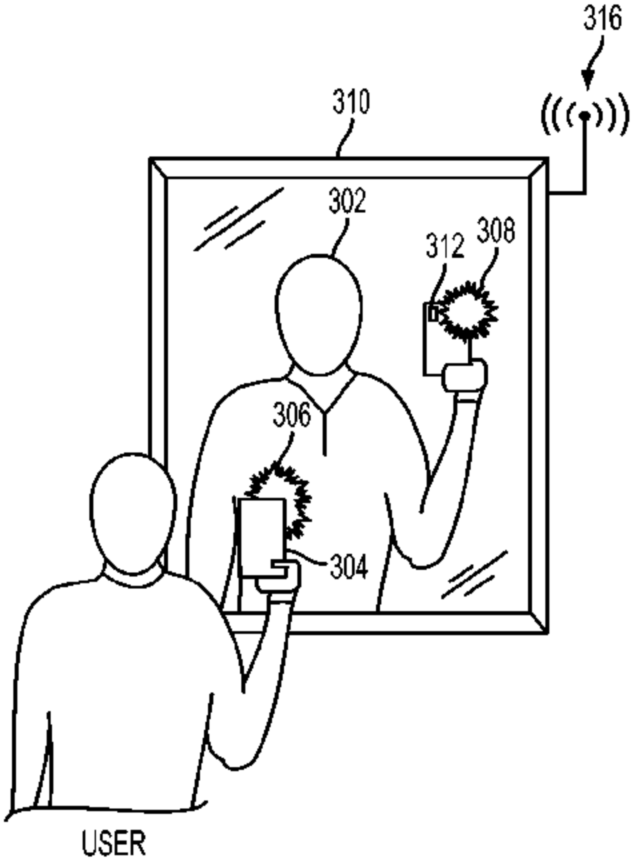


FIG. 3

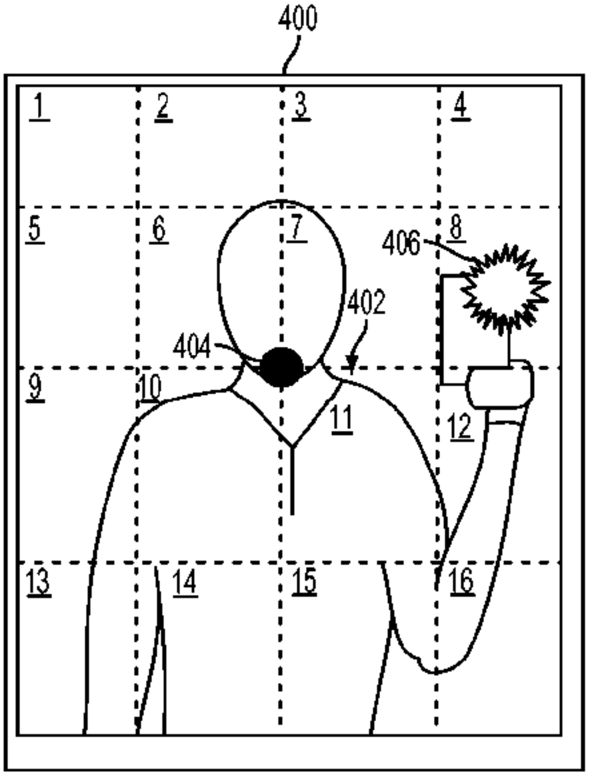


FIG. 4A

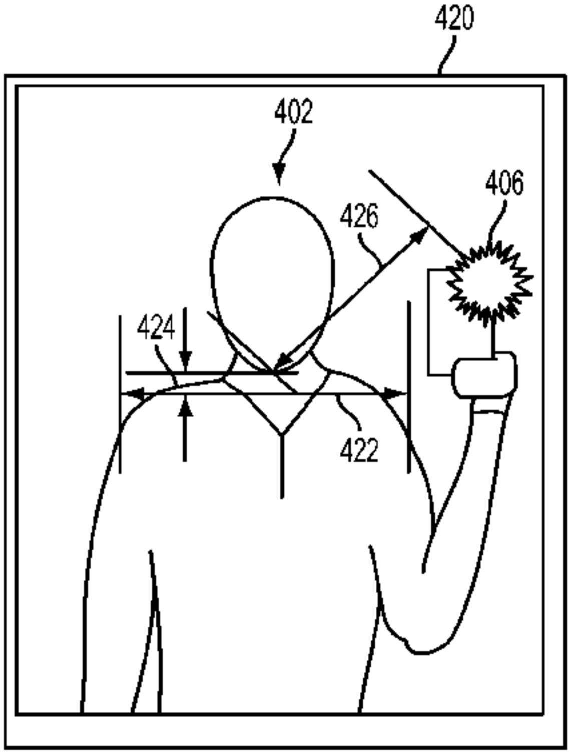


FIG. 4B

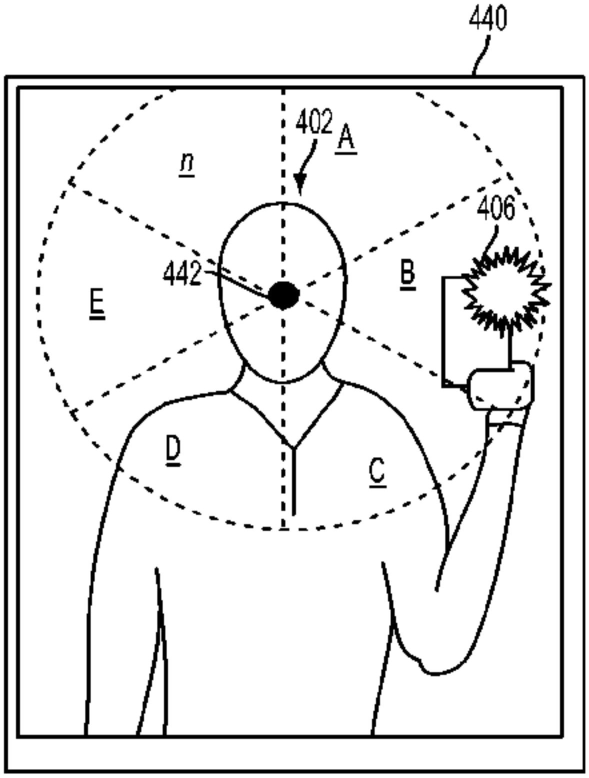


FIG. 4C

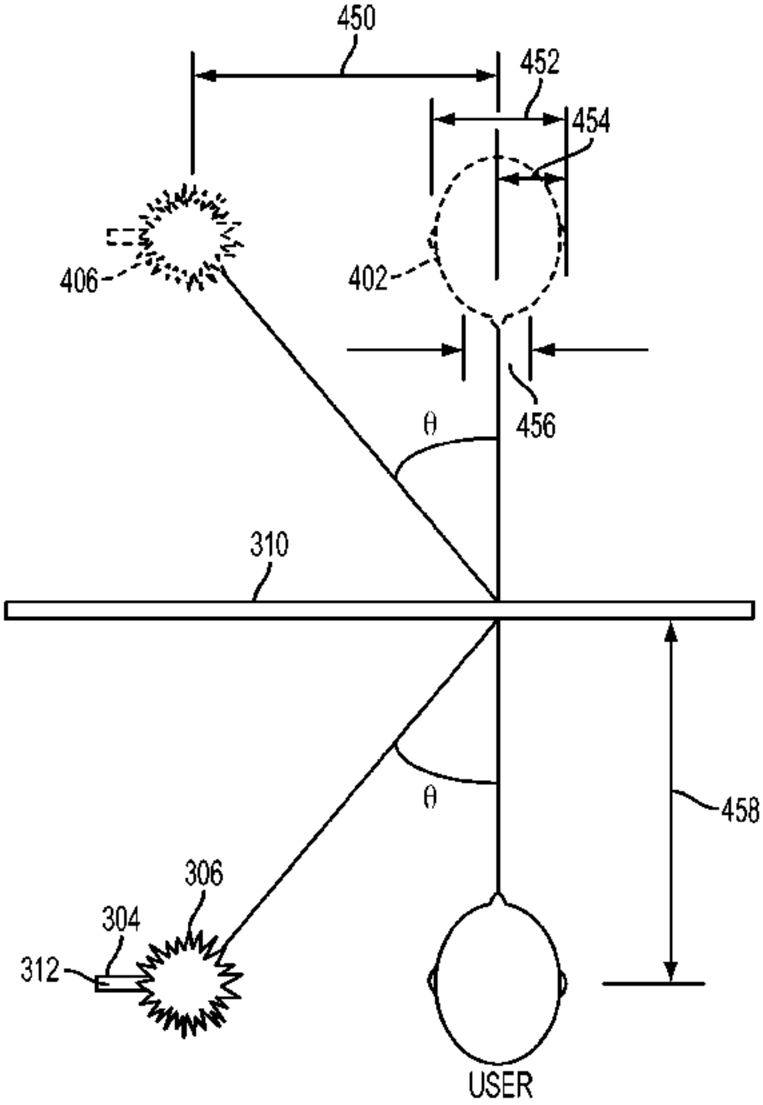


FIG. 4D

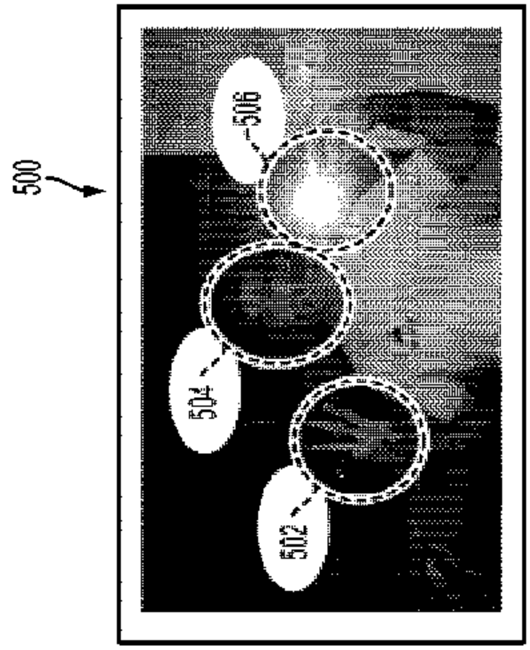


FIG. 5A

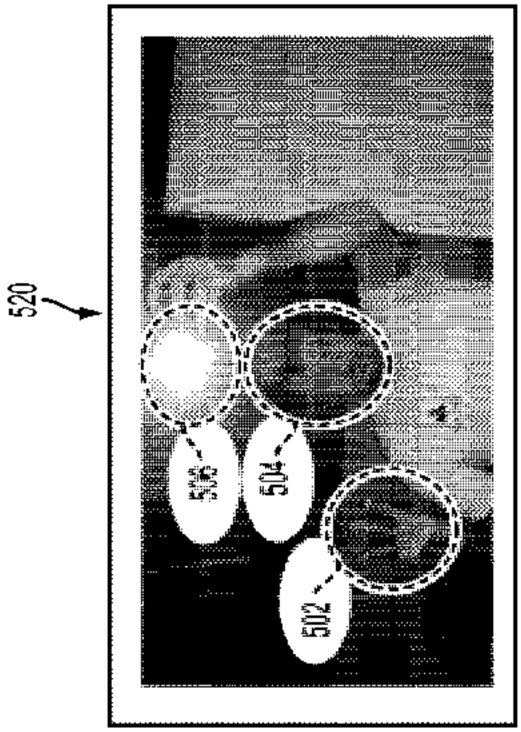


FIG. 5B

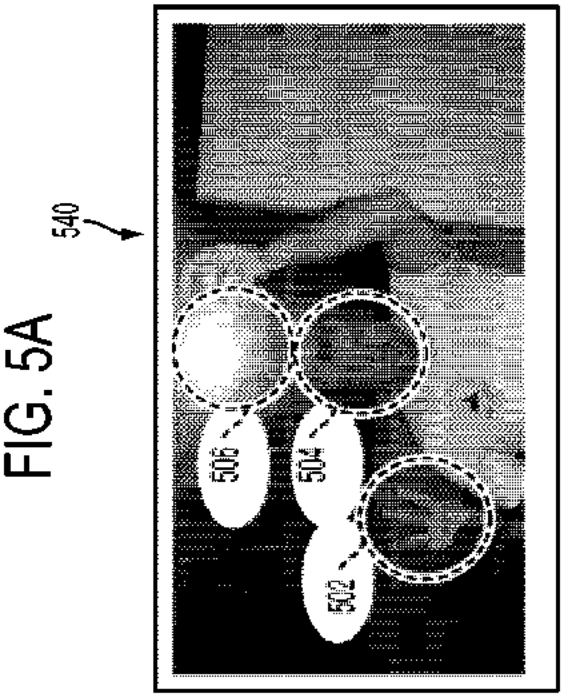


FIG. 5C

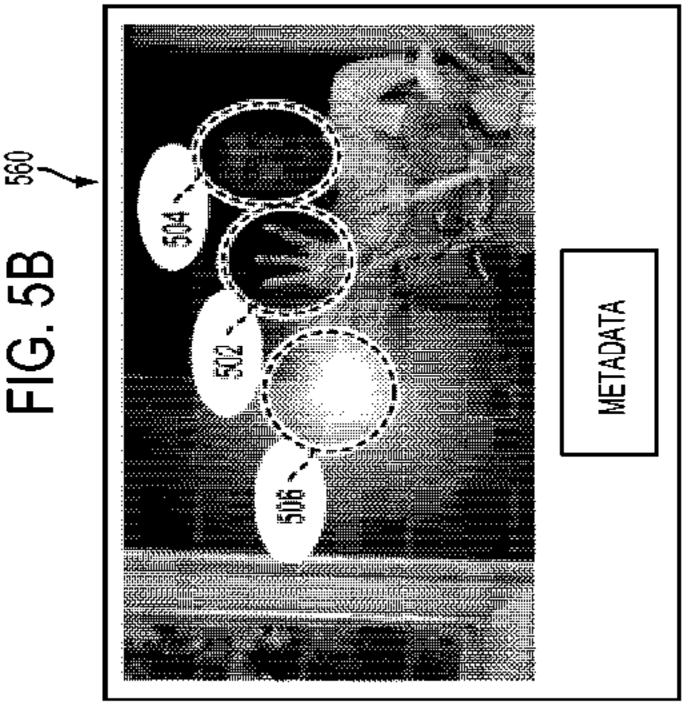


FIG. 5D

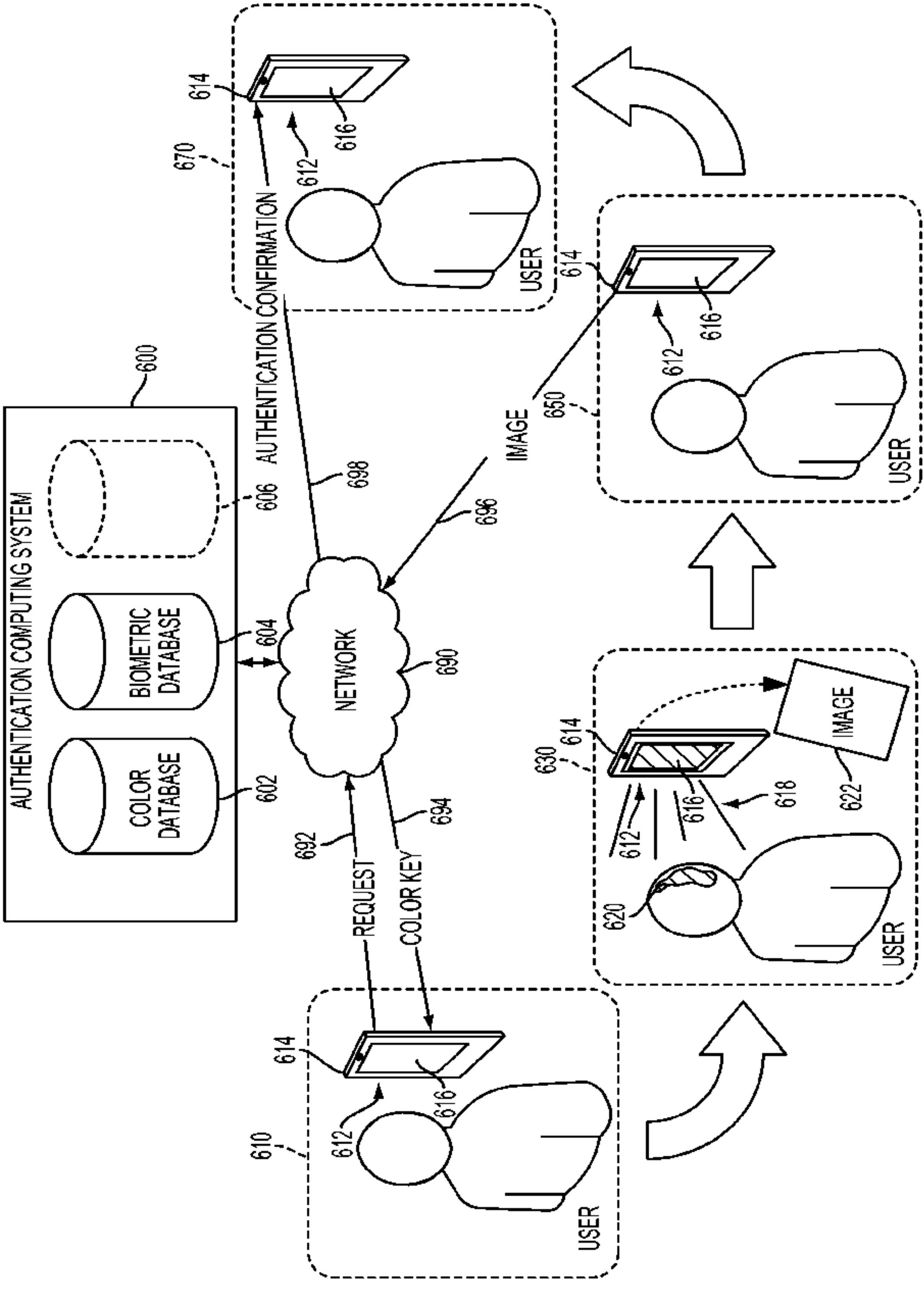

AUTHENTICATION COMPUTING SYSTEM
600
COLOR DATABASE
602
BIOMETRIC DATABASE
604
606
NETWORK
690
REQUEST
692
COLOR KEY
694
IMAGE
696
AUTHENTICATION CONFIRMATION
698
610
612
614
616
USER
630
618
620
622
IMAGE
650
670

FIG. 6

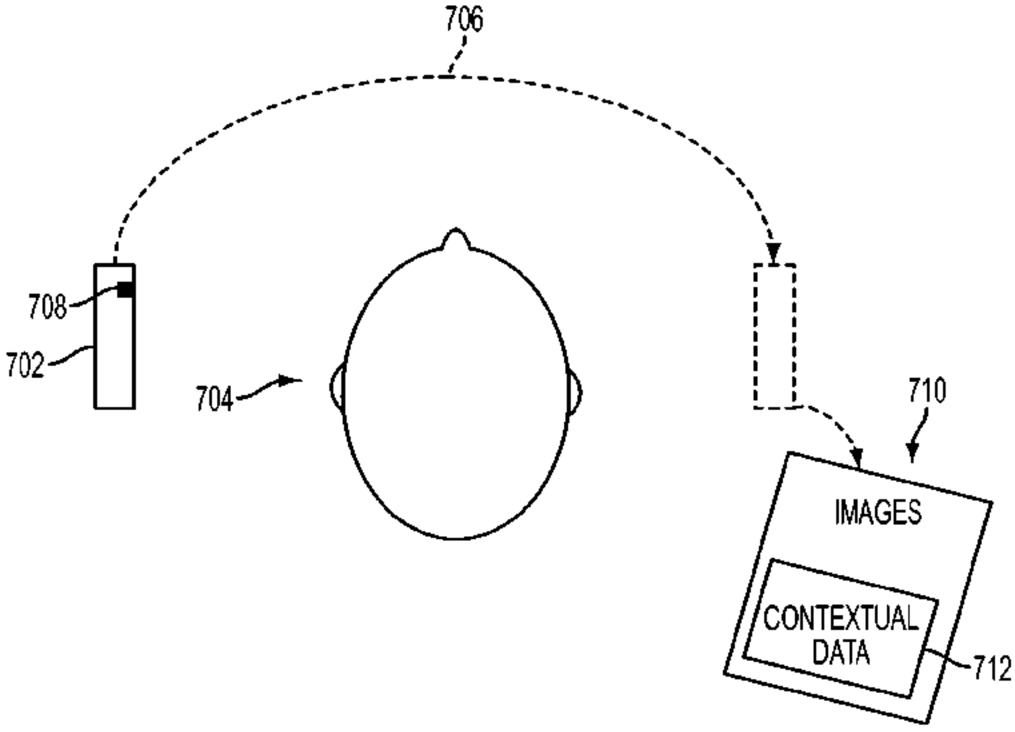

706
708
702
704
710
IMAGES
CONTEXTUAL DATA
712

FIG. 7A

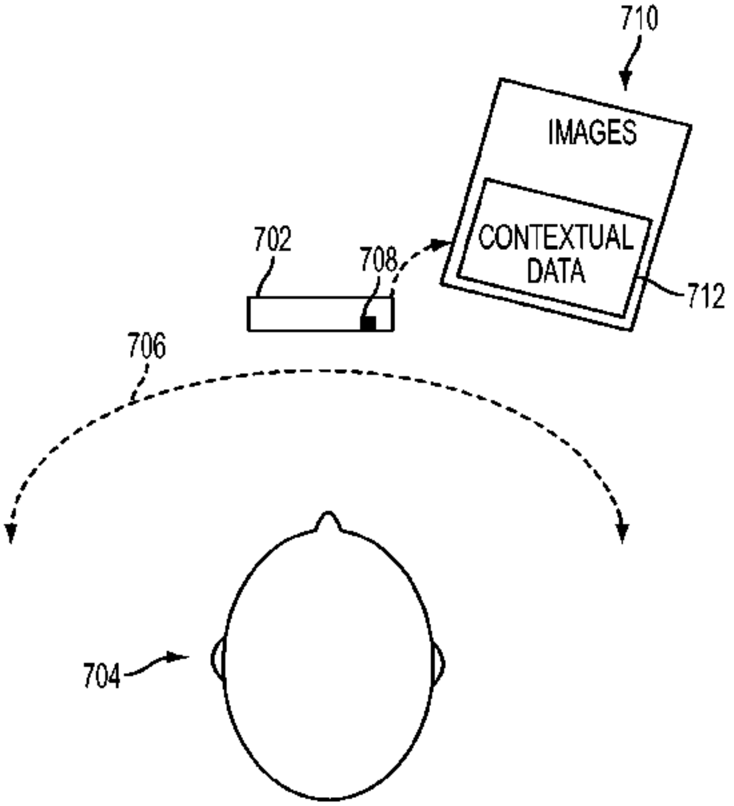

710
IMAGES
702
708
CONTEXTUAL DATA
712
706
704

FIG. 7B

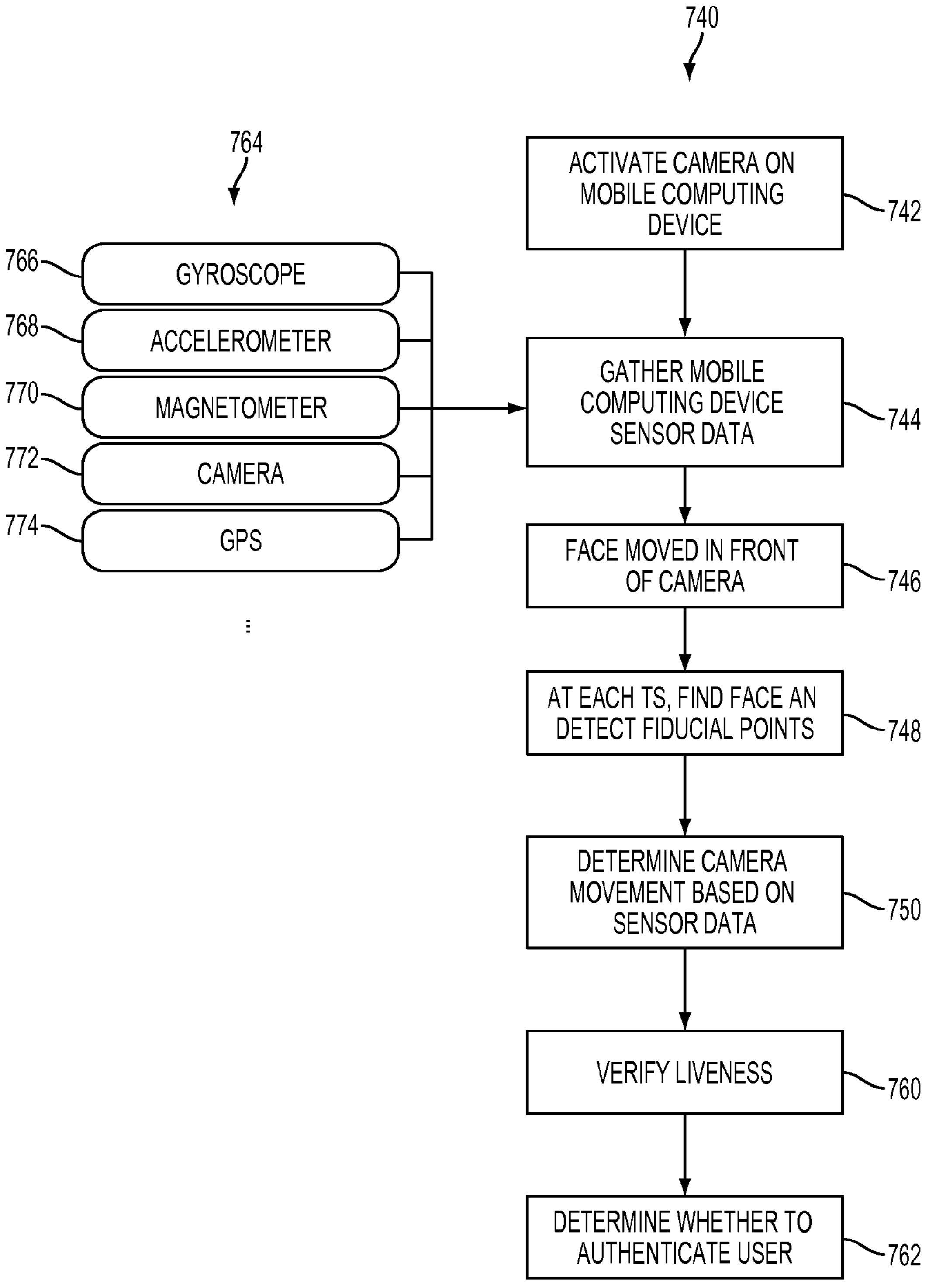

740
764
766
GYROSCOPE
768
ACCELEROMETER
770
MAGNETOMETER
772
CAMERA
774
GPS
⋮
ACTIVATE CAMERA ON MOBILE COMPUTING DEVICE
742
GATHER MOBILE COMPUTING DEVICE SENSOR DATA
744
FACE MOVED IN FRONT OF CAMERA
746
AT EACH TS, FIND FACE AN DETECT FIDUCIAL POINTS
748
DETERMINE CAMERA MOVEMENT BASED ON SENSOR DATA
750
VERIFY LIVENESS
760
DETERMINE WHETHER TO AUTHENTICATE USER
762

FIG. 7C

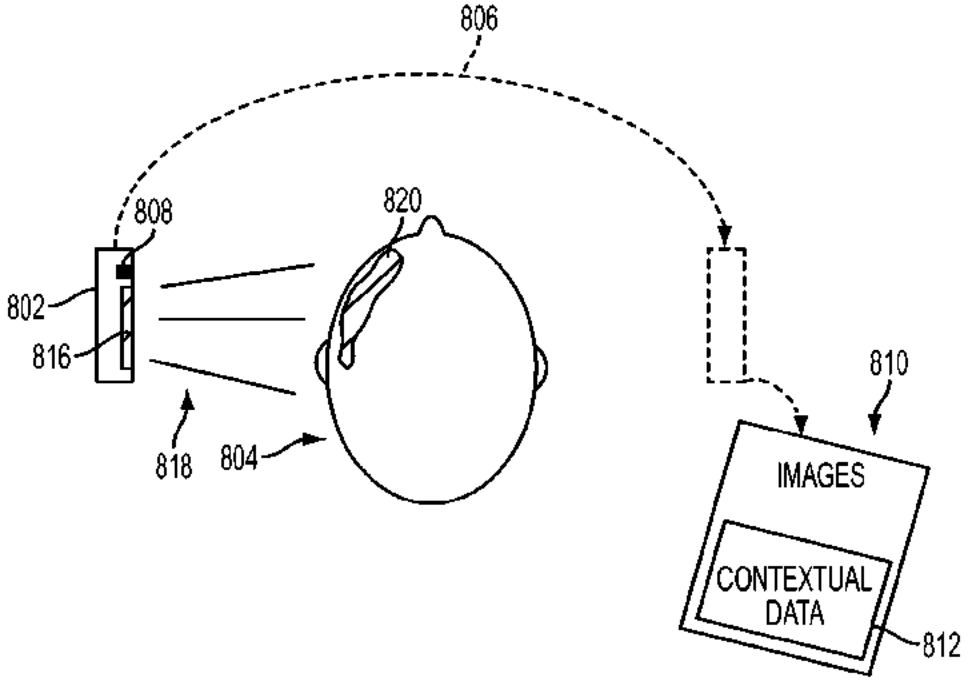


FIG. 8A

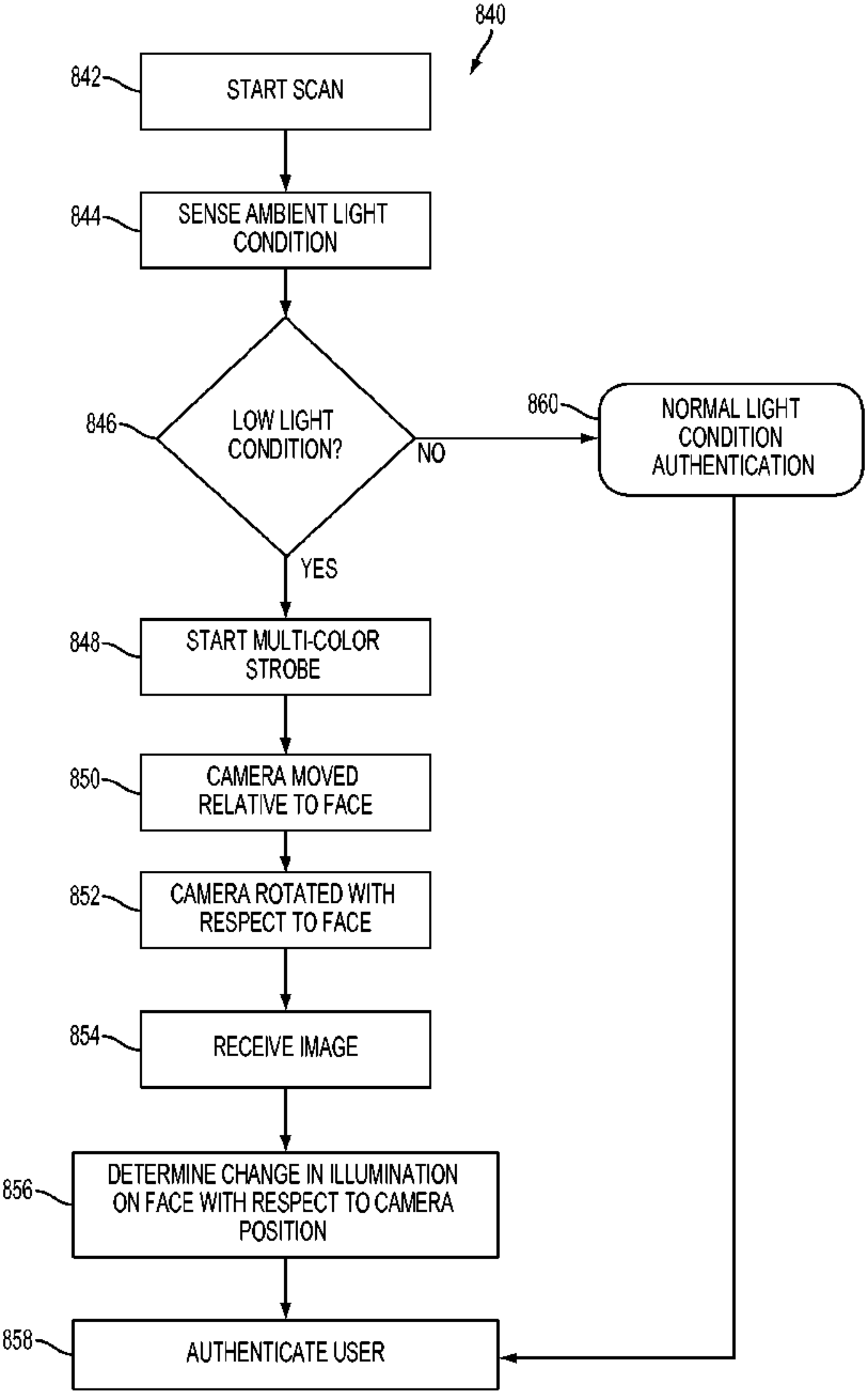

840
842
START SCAN
844
SENSE AMBIENT LIGHT CONDITION
846
LOW LIGHT CONDITION?
NO
860
NORMAL LIGHT CONDITION AUTHENTICATION
YES
848
START MULTI-COLOR STROBE
850
CAMERA MOVED RELATIVE TO FACE
852
CAMERA ROTATED WITH RESPECT TO FACE
854
RECEIVE IMAGE
856
DETERMINE CHANGE IN ILLUMINATION ON FACE WITH RESPECT TO CAMERA POSITION
858
AUTHENTICATE USER

FIG. 8B

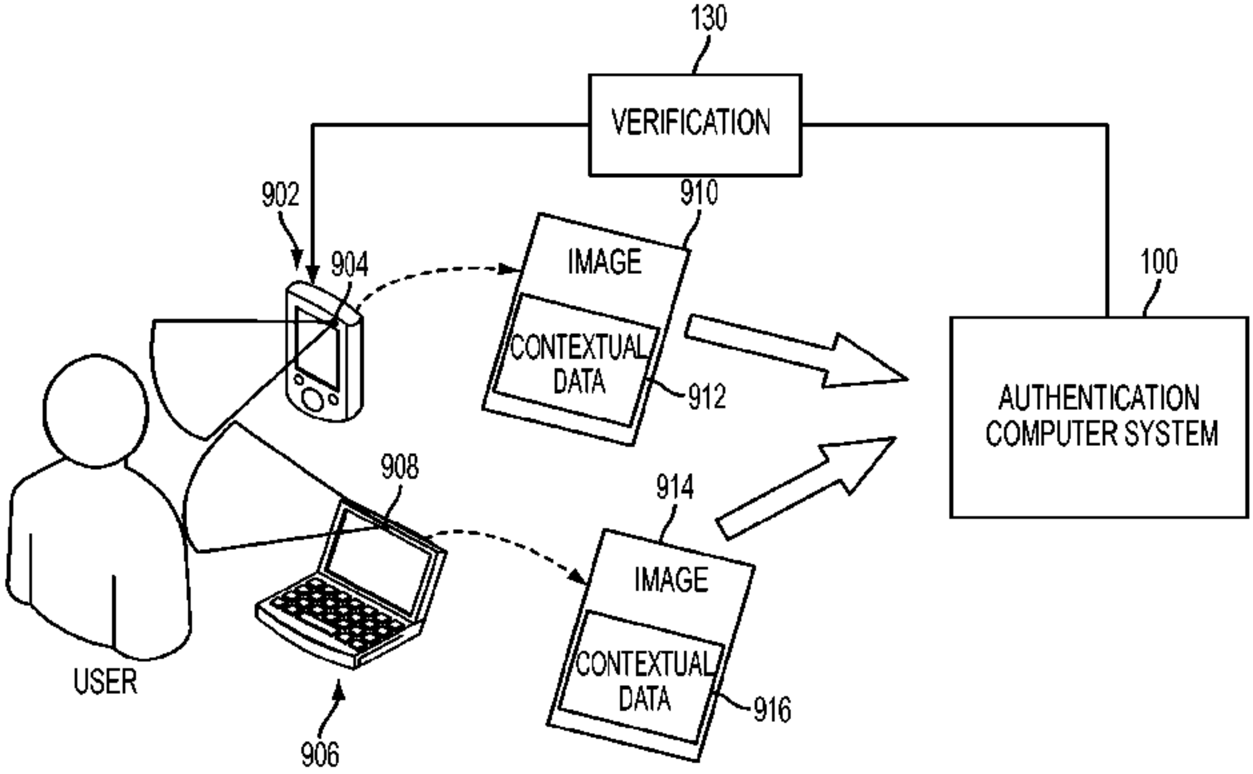

130
VERIFICATION
902
904
910
IMAGE
CONTEXTUAL DATA
912
100
AUTHENTICATION COMPUTER SYSTEM
908
914
IMAGE
CONTEXTUAL DATA
916
USER
906

FIG. 9

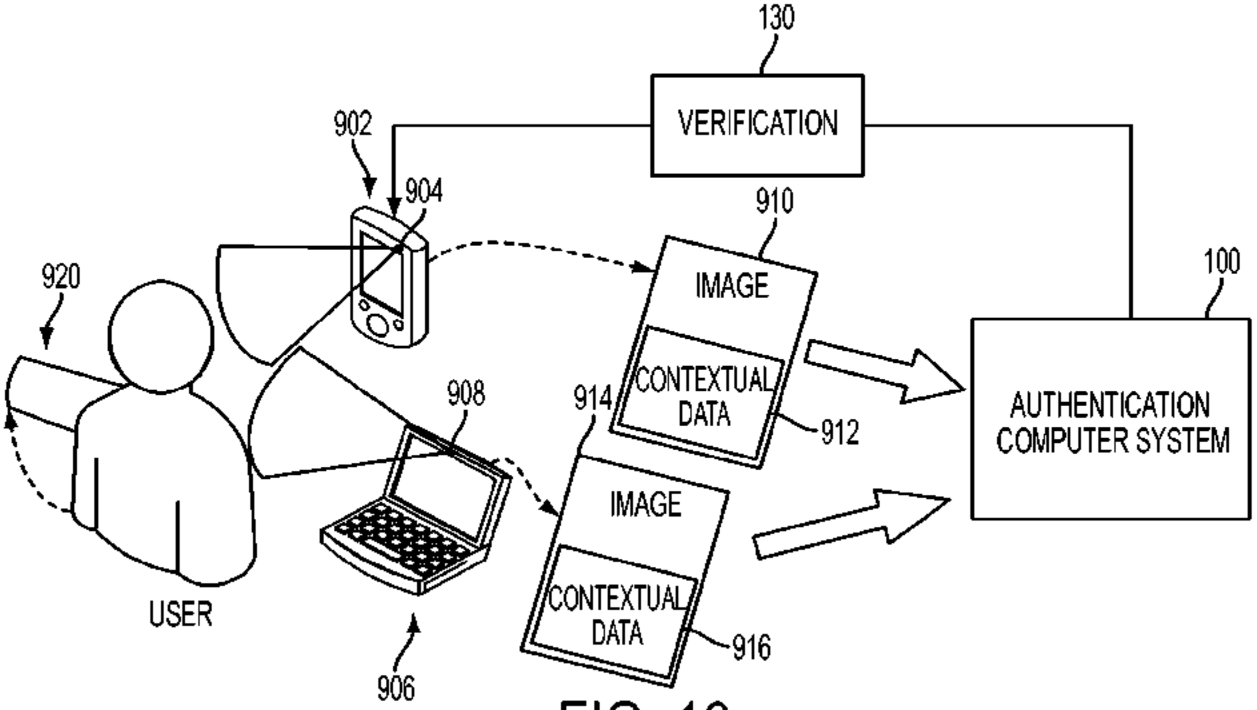

130
VERIFICATION
902
904
910
IMAGE
920
100
CONTEXTUAL DATA
912
AUTHENTICATION COMPUTER SYSTEM
908
914
IMAGE
CONTEXTUAL DATA
916
USER
906

FIG. 10

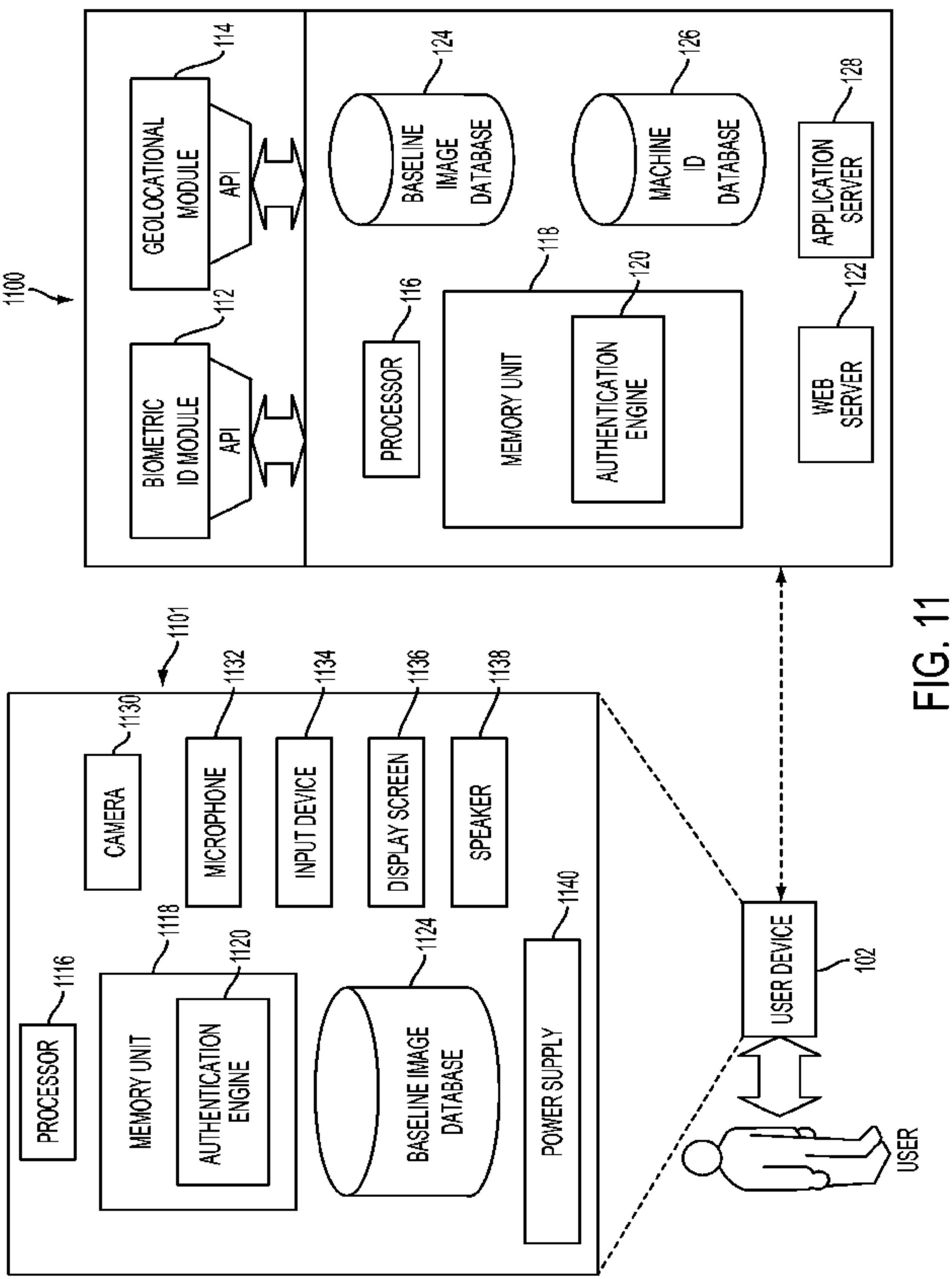

1100
BIOMETRIC ID MODULE
112
API
GEOLOCATIONAL MODULE
114
API
PROCESSOR
116
MEMORY UNIT
118
AUTHENTICATION ENGINE
120
BASELINE IMAGE DATABASE
124
MACHINE ID DATABASE
126
WEB SERVER
122
APPLICATION SERVER
128
1101
PROCESSOR
1116
MEMORY UNIT
1118
AUTHENTICATION ENGINE
1120
BASELINE IMAGE DATABASE
1124
POWER SUPPLY
1140
CAMERA
1130
MICROPHONE
1132
INPUT DEVICE
1134
DISPLAY SCREEN
1136
SPEAKER
1138
USER DEVICE
102
USER

FIG. 11

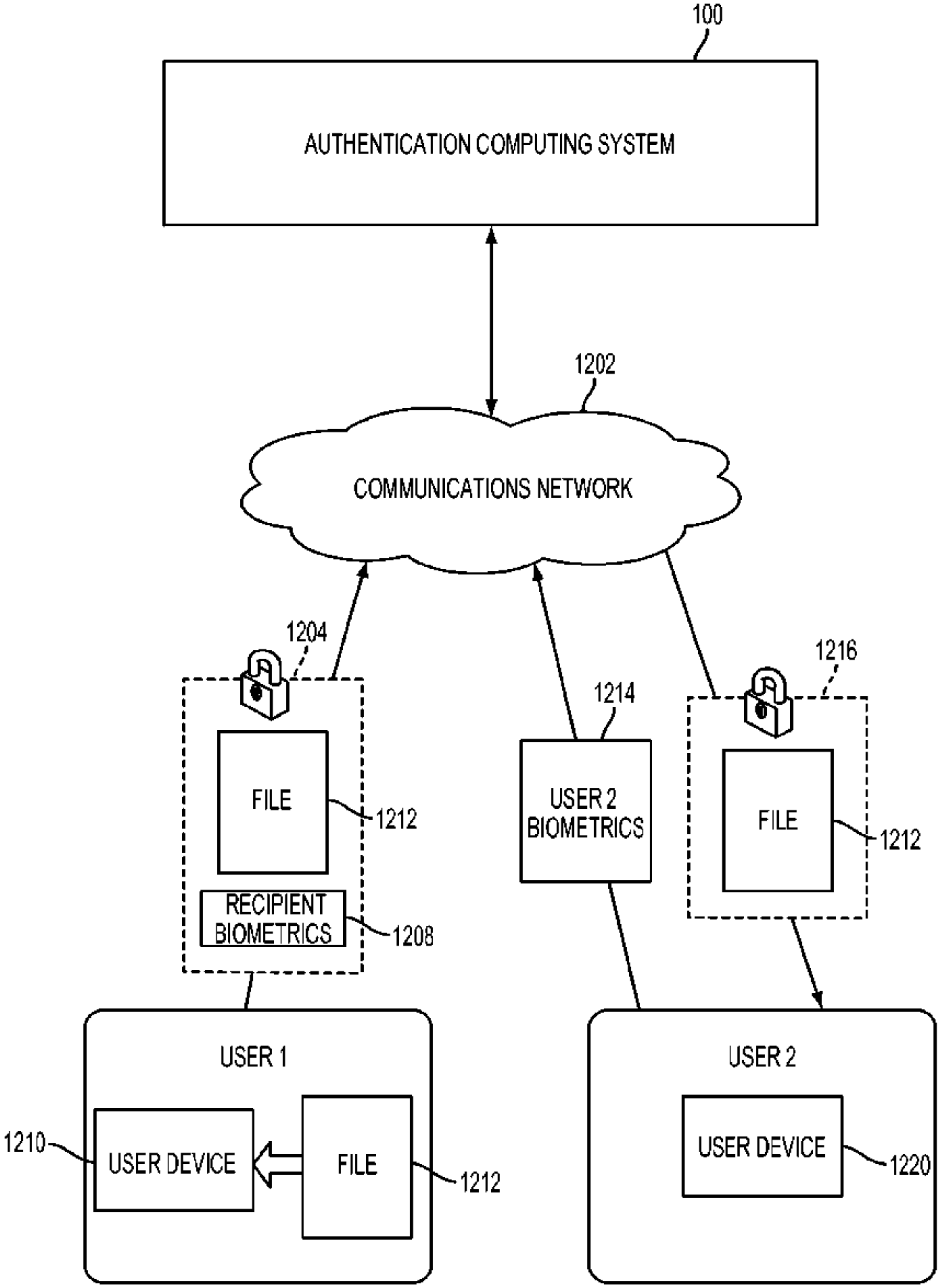

100
AUTHENTICATION COMPUTING SYSTEM
1202
COMMUNICATIONS NETWORK
1204
FILE
1212
RECIPIENT BIOMETRICS
1208
1214
USER 2 BIOMETRICS
1216
FILE
1212
USER 1
1210
USER DEVICE
FILE
1212
USER 2
USER DEVICE
1220

FIG. 12

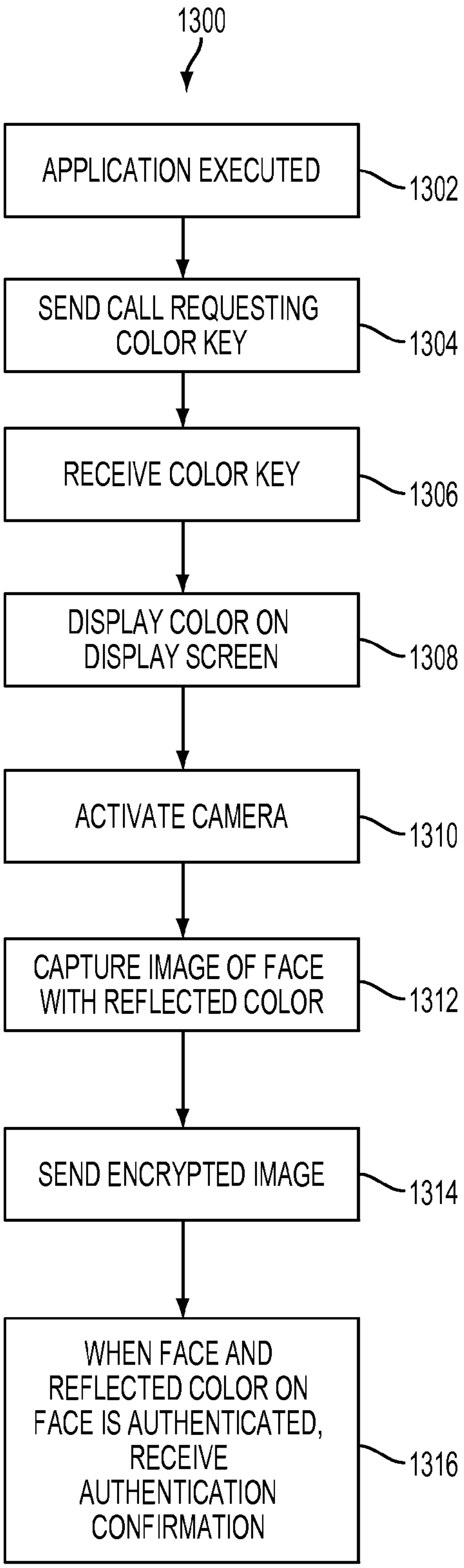

1300
APPLICATION EXECUTED
1302
SEND CALL REQUESTING COLOR KEY
1304
RECEIVE COLOR KEY
1306
DISPLAY COLOR ON DISPLAY SCREEN
1308
ACTIVATE CAMERA
1310
CAPTURE IMAGE OF FACE WITH REFLECTED COLOR
1312
SEND ENCRYPTED IMAGE
1314
WHEN FACE AND REFLECTED COLOR ON FACE IS AUTHENTICATED, RECEIVE AUTHENTICATION CONFIRMATION
1316

FIG. 13

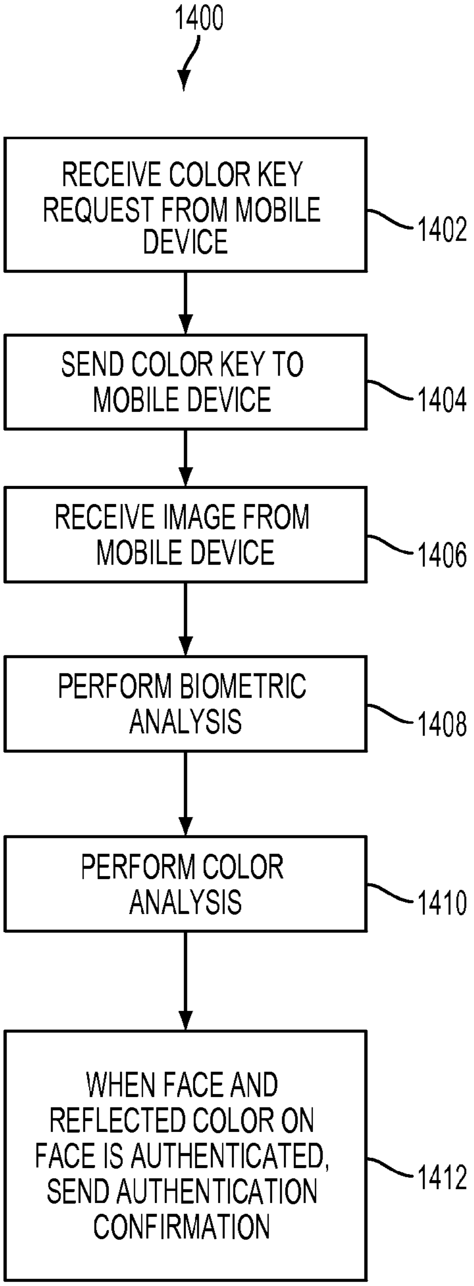

1400
RECEIVE COLOR KEY REQUEST FROM MOBILE DEVICE
1402
SEND COLOR KEY TO MOBILE DEVICE
1404
RECEIVE IMAGE FROM MOBILE DEVICE
1406
PERFORM BIOMETRIC ANALYSIS
1408
PERFORM COLOR ANALYSIS
1410
WHEN FACE AND REFLECTED COLOR ON FACE IS AUTHENTICATED, SEND AUTHENTICATION CONFIRMATION
1412

FIG. 14

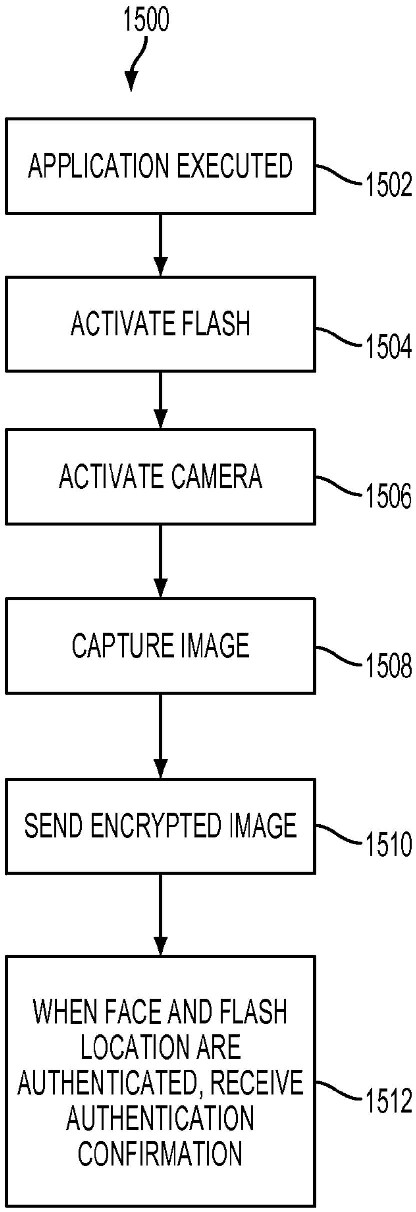


FIG. 15

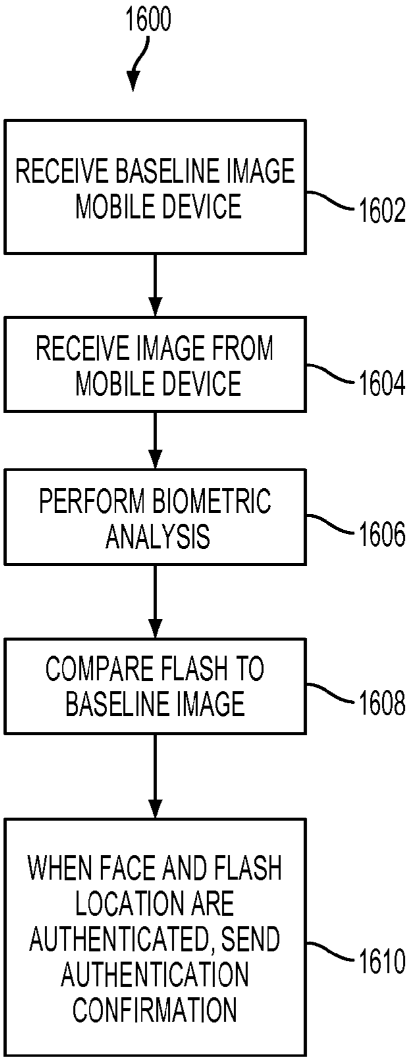

1600
RECEIVE BASELINE IMAGE MOBILE DEVICE
1602
RECEIVE IMAGE FROM MOBILE DEVICE
1604
PERFORM BIOMETRIC ANALYSIS
1606
COMPARE FLASH TO BASELINE IMAGE
1608
WHEN FACE AND FLASH LOCATION ARE AUTHENTICATED, SEND AUTHENTICATION CONFIRMATION
1610

FIG. 16

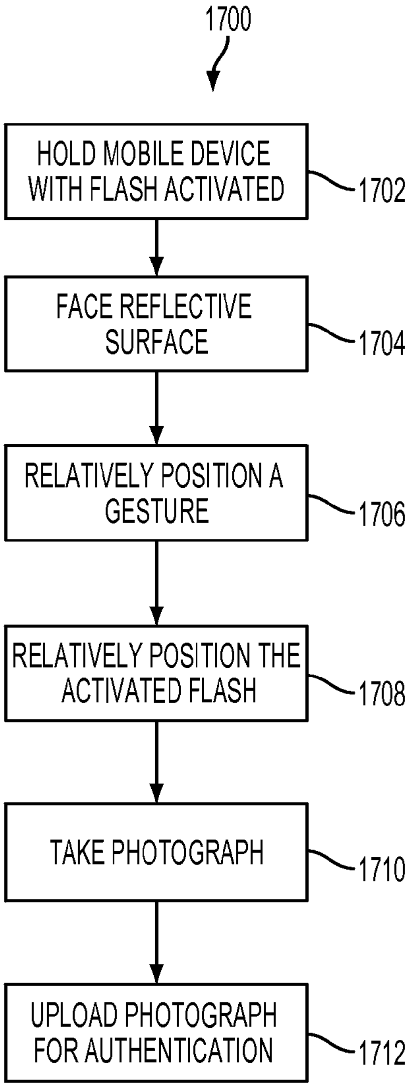

1700
HOLD MOBILE DEVICE WITH FLASH ACTIVATED
1702
FACE REFLECTIVE SURFACE
1704
RELATIVELY POSITION A GESTURE
1706
RELATIVELY POSITION THE ACTIVATED FLASH
1708
TAKE PHOTOGRAPH
1710
UPLOAD PHOTOGRAPH FOR AUTHENTICATION
1712

FIG. 17

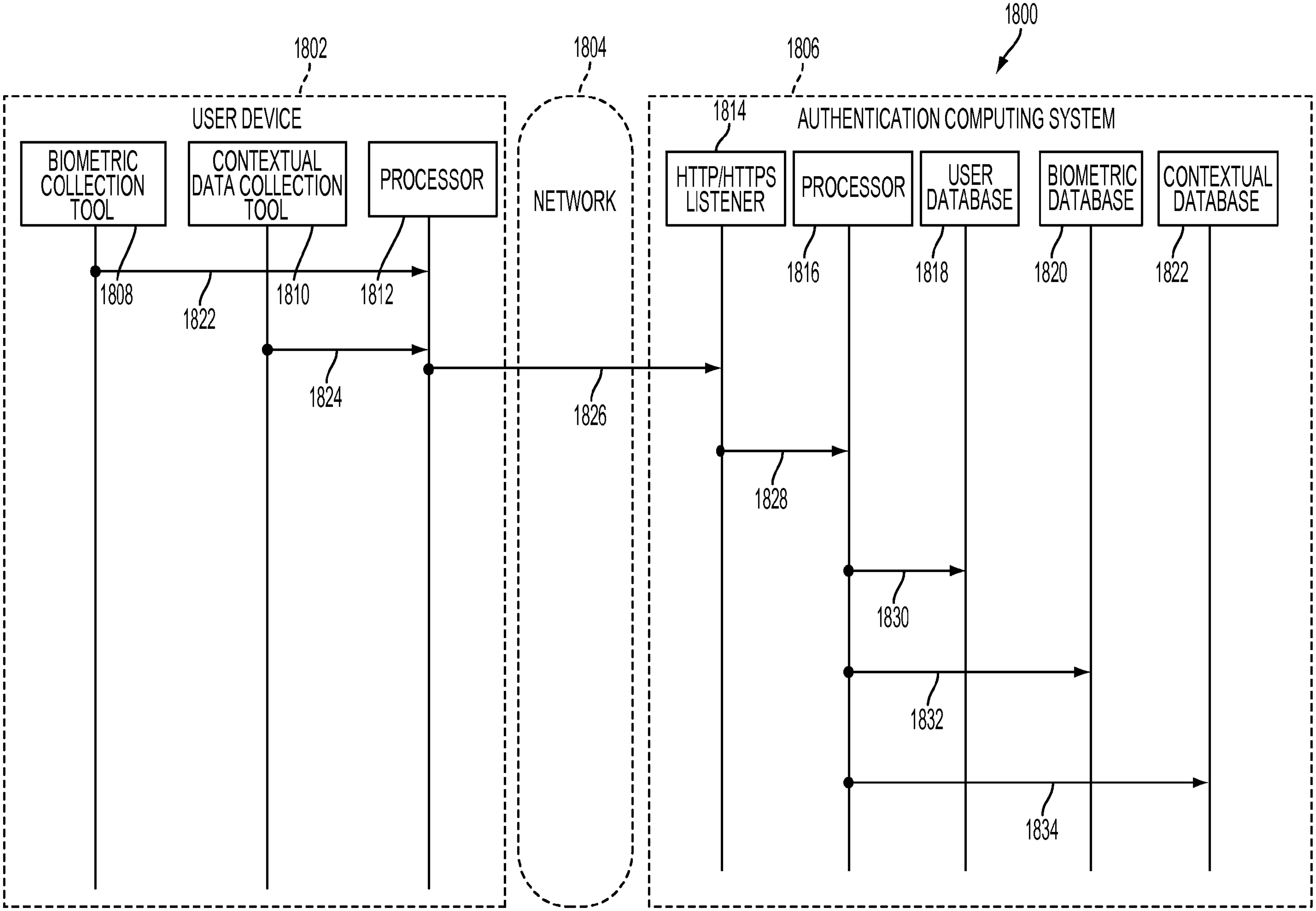

1800
1802
1804
1806
USER DEVICE
BIOMETRIC COLLECTION TOOL
CONTEXTUAL DATA COLLECTION TOOL
PROCESSOR
1808
1822
1810
1812
1824
NETWORK
1826
AUTHENTICATION COMPUTING SYSTEM
1814
HTTP/HTTPS LISTENER
PROCESSOR
USER DATABASE
BIOMETRIC DATABASE
CONTEXTUAL DATABASE
1816
1818
1820
1822
1828
1830
1832
1834

FIG. 18A

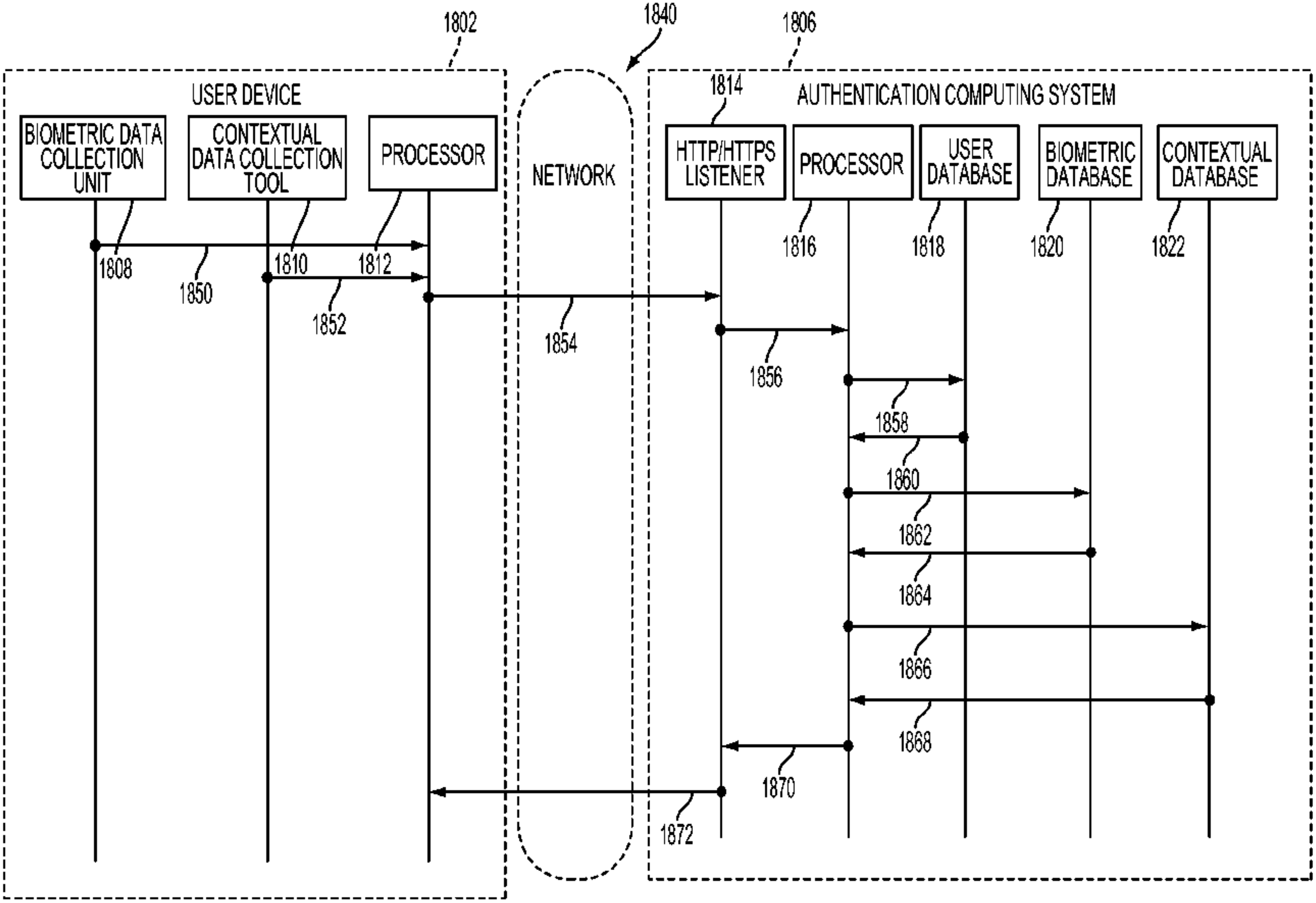

1802
1840
1806
USER DEVICE
BIOMETRIC DATA COLLECTION UNIT
CONTEXTUAL DATA COLLECTION TOOL
PROCESSOR
NETWORK
1814
AUTHENTICATION COMPUTING SYSTEM
HTTP/HTTPS LISTENER
PROCESSOR
USER DATABASE
BIOMETRIC DATABASE
CONTEXTUAL DATABASE
1816
1818
1820
1822
1808
1810
1812
1850
1852
1854
1856
1858
1860
1862
1864
1866
1868
1870
1872

FIG. 18B

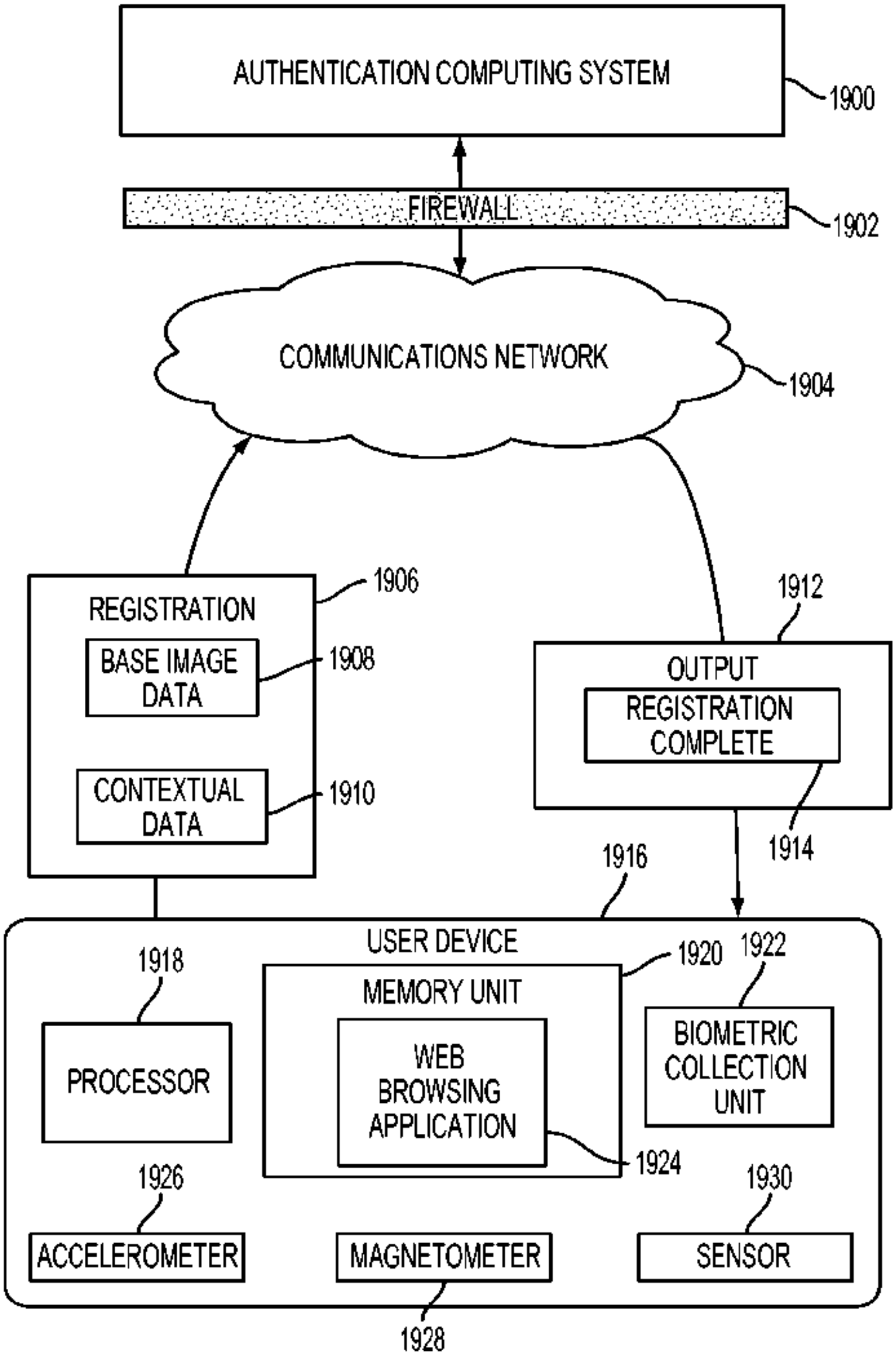

AUTHENTICATION COMPUTING SYSTEM
1900
FIREWALL
1902
COMMUNICATIONS NETWORK
1904
REGISTRATION
1906
BASE IMAGE DATA
1908
CONTEXTUAL DATA
1910
OUTPUT
1912
REGISTRATION COMPLETE
1914
1916
USER DEVICE
1918
PROCESSOR
MEMORY UNIT
1920
WEB BROWSING APPLICATION
1924
1922
BIOMETRIC COLLECTION UNIT
1926
ACCELEROMETER
MAGNETOMETER
1928
1930
SENSOR

FIG. 19A

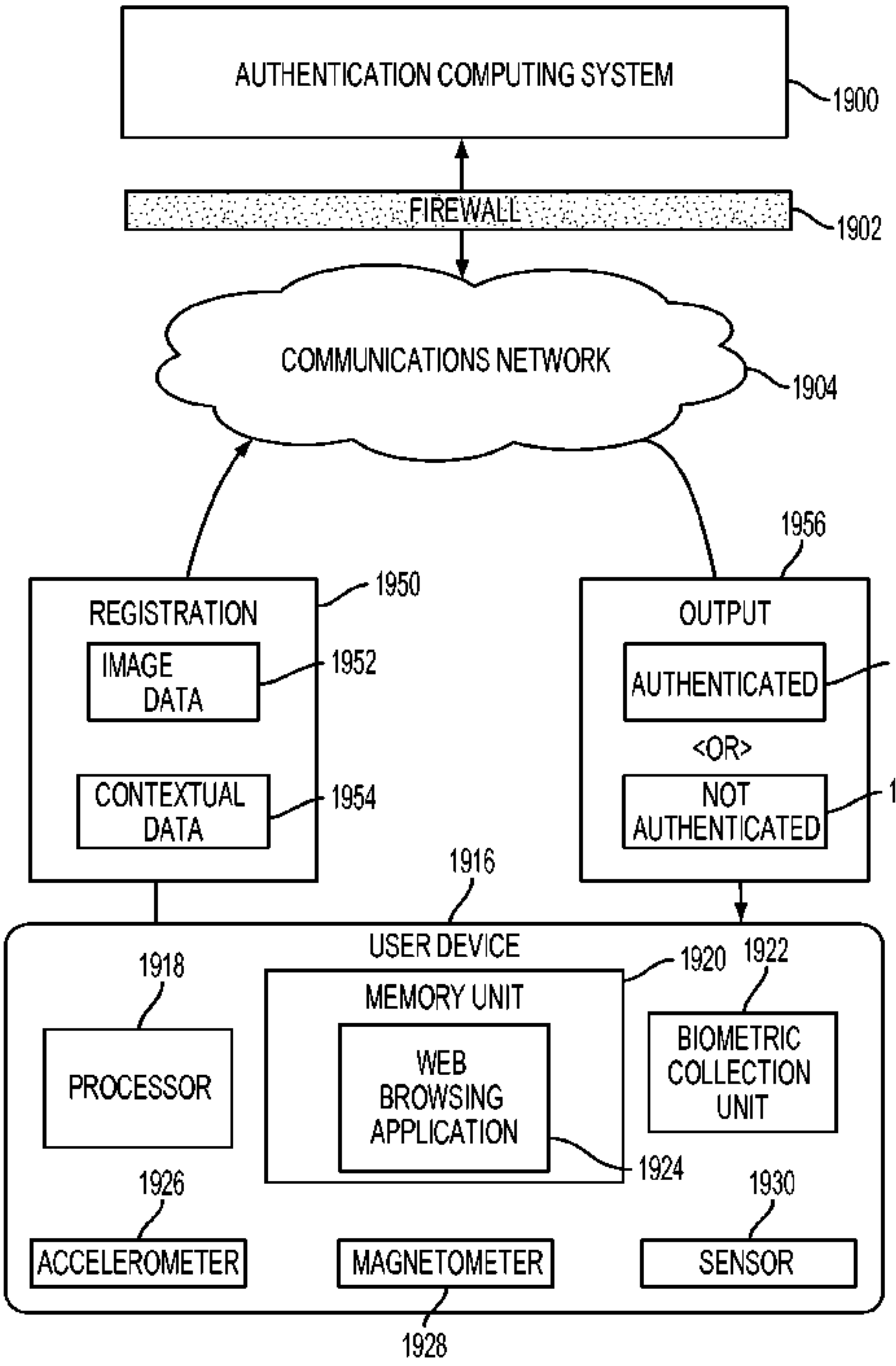

AUTHENTICATION COMPUTING SYSTEM
1900
FIREWALL
1902
COMMUNICATIONS NETWORK
1904
1956
REGISTRATION
1950
IMAGE DATA
1952
CONTEXTUAL DATA
1954
OUTPUT
AUTHENTICATED
1958
<OR>
NOT AUTHENTICATED
1960
1916
USER DEVICE
1918
PROCESSOR
MEMORY UNIT
1920
1922
WEB BROWSING APPLICATION
1924
BIOMETRIC COLLECTION UNIT
1926
1930
ACCELEROMETER
MAGNETOMETER
SENSOR
1928

FIG. 19B

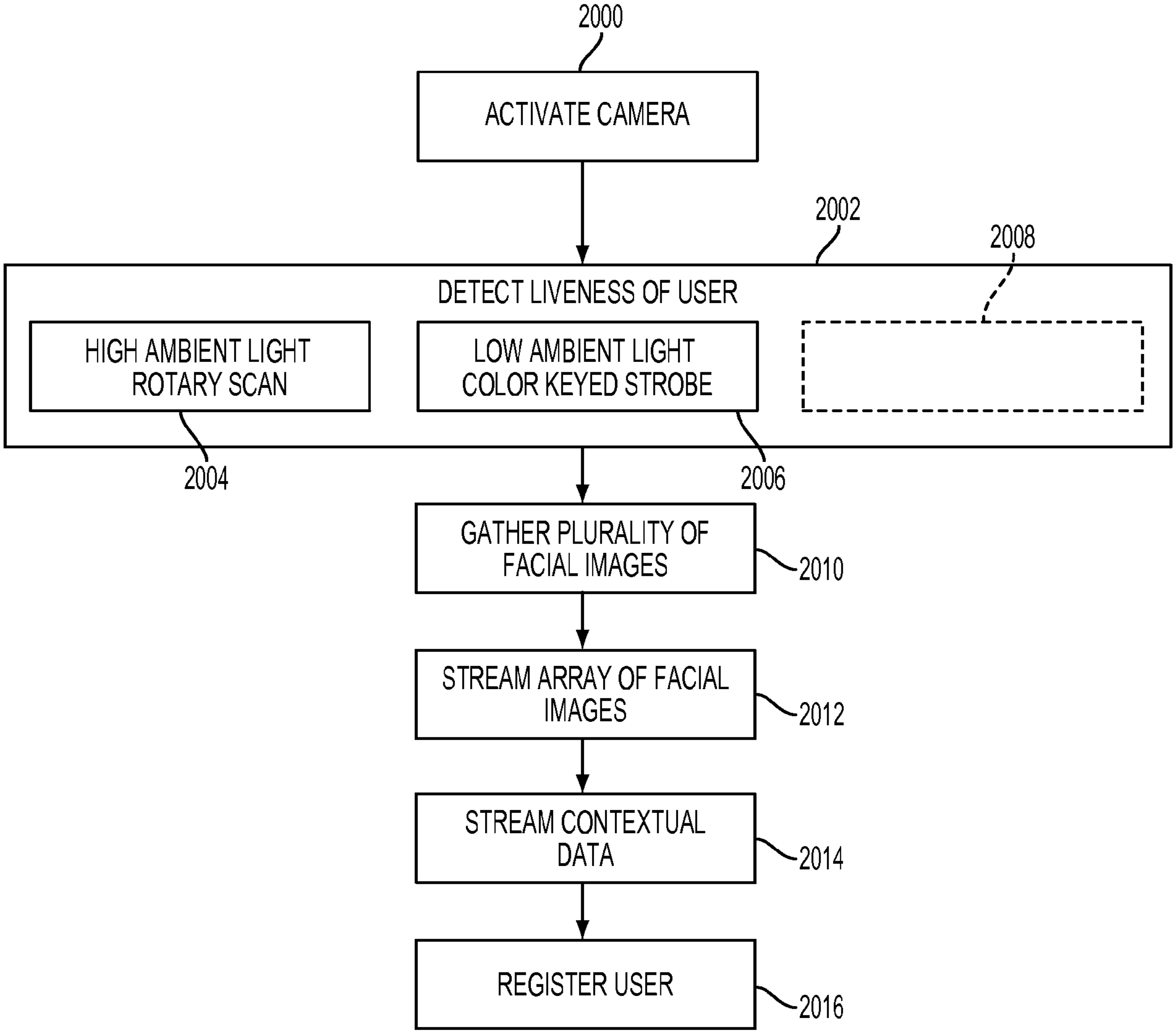

2000
ACTIVATE CAMERA
2002
2008
DETECT LIVENESS OF USER
HIGH AMBIENT LIGHT ROTARY SCAN
LOW AMBIENT LIGHT COLOR KEYED STROBE
2004
2006
GATHER PLURALITY OF FACIAL IMAGES
2010
STREAM ARRAY OF FACIAL IMAGES
2012
STREAM CONTEXTUAL DATA
2014
REGISTER USER
2016

FIG. 20A

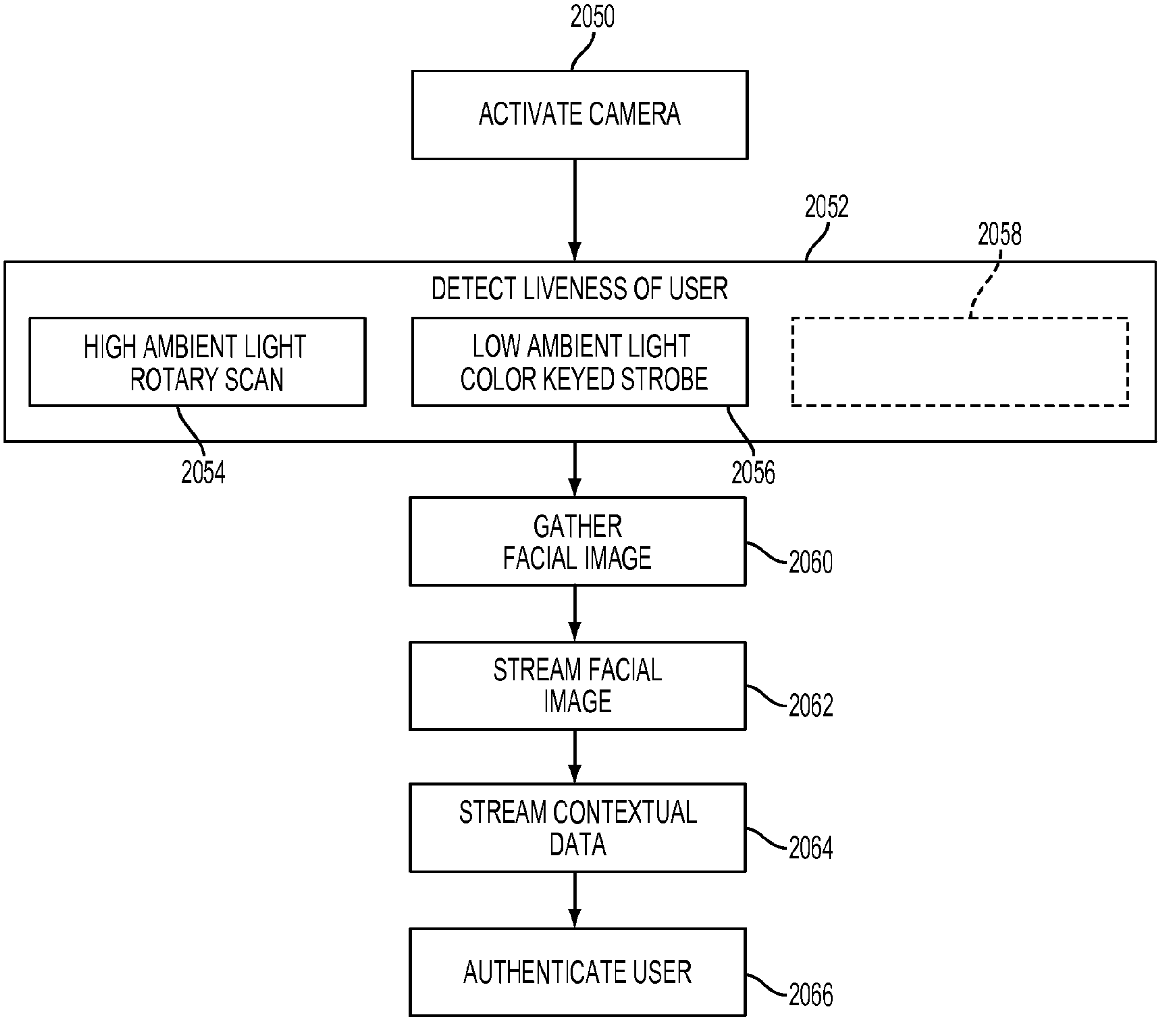

2050
ACTIVATE CAMERA
2052
2058
DETECT LIVENESS OF USER
HIGH AMBIENT LIGHT ROTARY SCAN
LOW AMBIENT LIGHT COLOR KEYED STROBE
2054
2056
GATHER FACIAL IMAGE
2060
STREAM FACIAL IMAGE
2062
STREAM CONTEXTUAL DATA
2064
AUTHENTICATE USER
2066

FIG. 20B

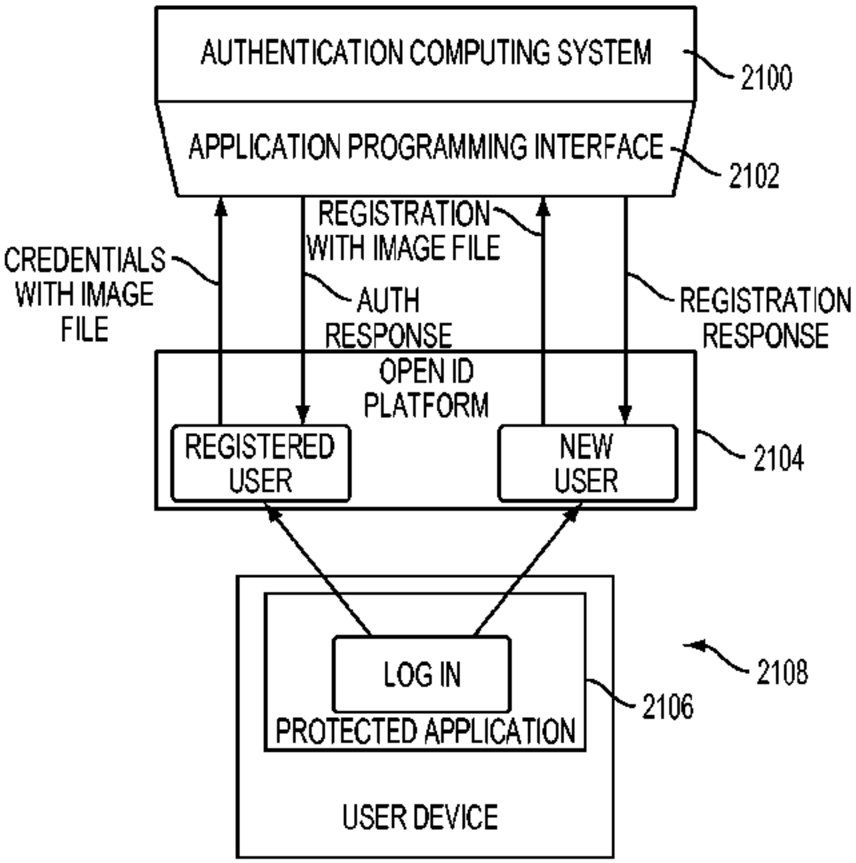

AUTHENTICATION COMPUTING SYSTEM
2100
APPLICATION PROGRAMMING INTERFACE
2102
CREDENTIALS WITH IMAGE FILE
REGISTRATION WITH IMAGE FILE
AUTH RESPONSE
REGISTRATION RESPONSE
OPEN ID PLATFORM
REGISTERED USER
NEW USER
2104
LOG IN
PROTECTED APPLICATION
2106
2108
USER DEVICE

FIG. 21

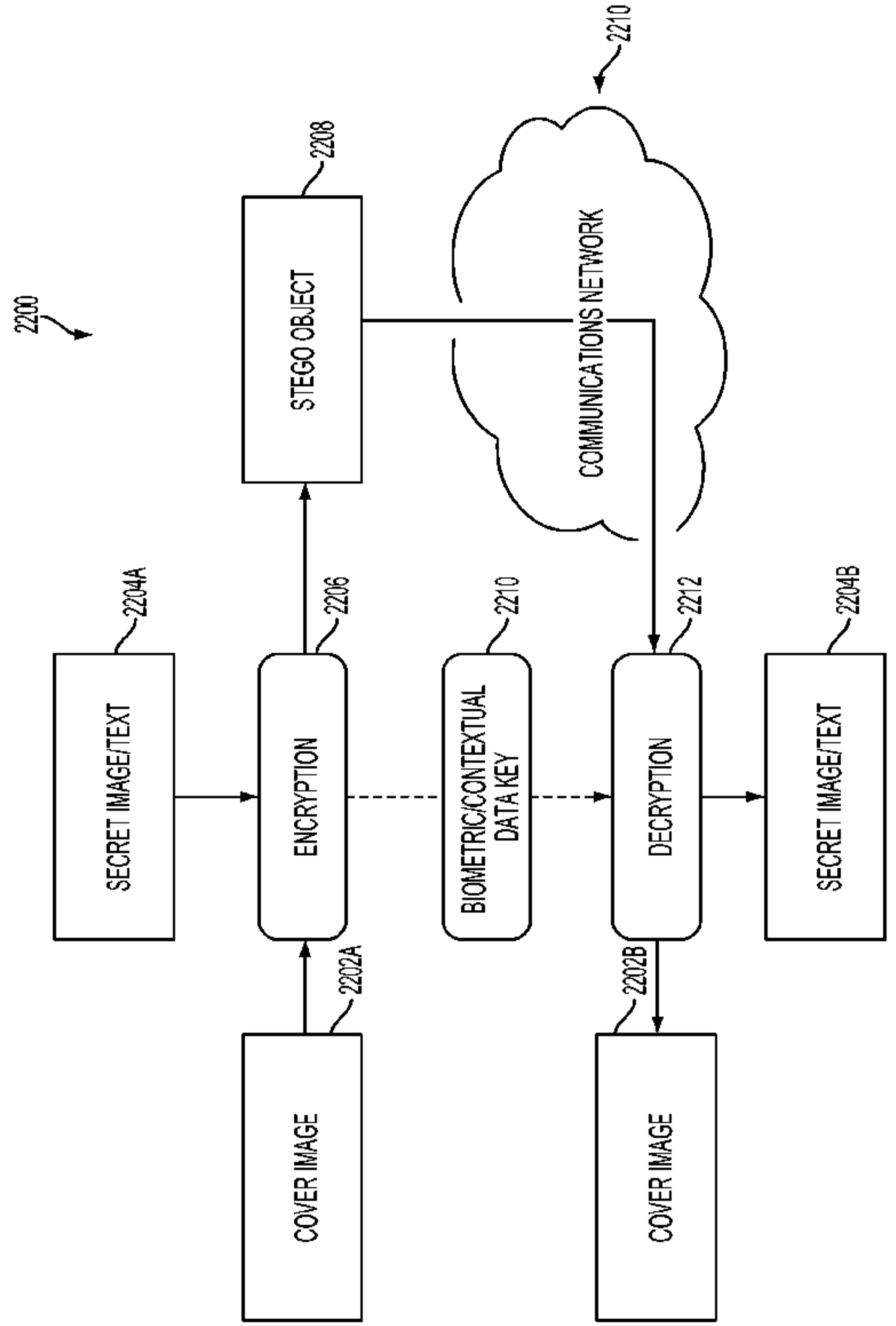

2200
COVER IMAGE
2202A
SECRET IMAGE/TEXT
2204A
ENCRYPTION
2206
STEGO OBJECT
2208
COMMUNICATIONS NETWORK
2210
BIOMETRIC/CONTEXTUAL DATA KEY
2210
DECRYPTION
2212
COVER IMAGE
2202B
SECRET IMAGE/TEXT
2204B

FIG. 22

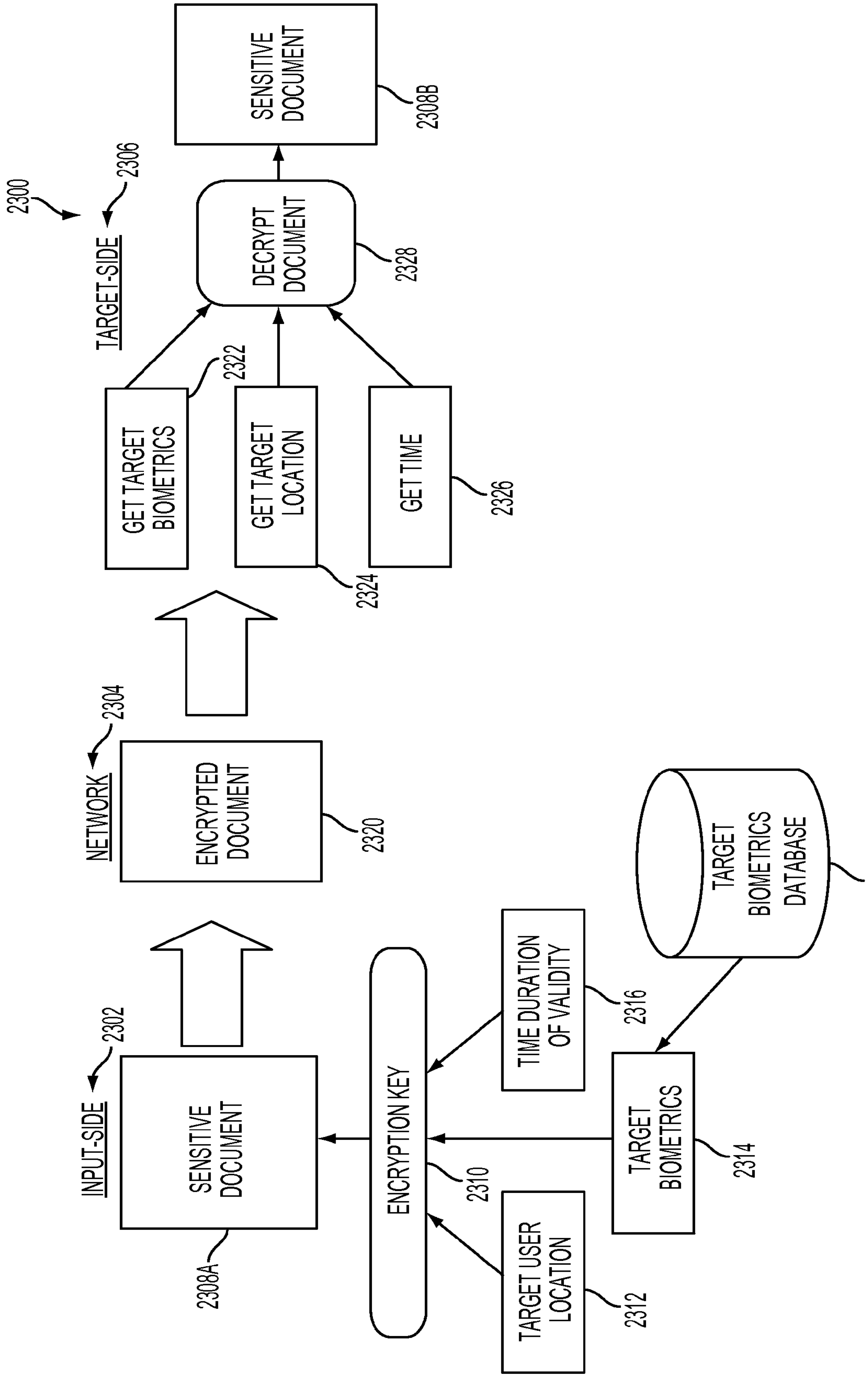

2300
INPUT-SIDE
2302
SENSITIVE DOCUMENT
2308A
NETWORK
2304
ENCRYPTED DOCUMENT
2320
TARGET-SIDE
2306
GET TARGET BIOMETRICS
2322
GET TARGET LOCATION
2324
GET TIME
2326
DECRYPT DOCUMENT
2328
SENSITIVE DOCUMENT
2308B
ENCRYPTION KEY
2310
TARGET USER LOCATION
2312
TARGET BIOMETRICS
2314
TIME DURATION OF VALIDITY
2316
TARGET BIOMETRICS DATABASE
2318

FIG. 23

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US13/35450

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06F 21/00 (2013.01)
USPC - 713/186; 455/433, 455
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) Classification(s): G06F 21/00; H04L 9/32 (2013.01)
USPC Classification(s): 713/186; 455/433, 455; 705/51, 52; 709/229, 238

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
MicroPatent (US-G, US-A, EP-A, EP-B, WO, JP-bib, DE-C,B, DE-A, DE-T, DE-U, GB-A, FR-A); DialogPro (Derwent, INSPEC, NTIS, PASCAL, Current Contents Search, Dissertation Abstracts Online, Inside Conferences); IEEE; Google/Google Scholar: authentication, biometric, contextual, user device

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 2011/0016534 A1 (JAKOBSSON, B et al.) January 20, 2011: abstract; paragraphs [0007], [0008], [0024], [0057], [0075]	1-4, 9, 15-17, 20-22 5-8, 10-14, 18, 19, 23, 24
Y	US 6,421,453 B1 (KANEVSKY, D et al.) July 16, 2002: abstract; column 8, lines 15-18; column 11, line 65- column 12, line 1; column 21, lines 59-66; column 24, lines 22-27	5-8, 18, 19, 23, and 24
Y	US 2003/0187798 A1 (MCKINLEY, T et al.) October 2, 2003: abstract; paragraphs [0020], [0048], [0135]	10, 11, and 14
Y	US 8,135,180 B2 (BALTATU, M et al.) March 13, 2012: abstract; column 3, lines 27-31	12 and 13

□ Further documents are listed in the continuation of Box C. □

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 12 September 2013 (12.09.2013)	Date of mailing of the international search report 20 SEP 2013
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Shane Thomas PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US13/35450

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. □ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. □ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. □ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
Group I: Claims 1-24; Group II: Claims 25-32; Group III: Claims 33-37

-***-Please see Supplemental Page-***-

1. □ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. □ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. □ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-24

Remark on Protest

□ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

□ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

□ No protest accompanied the payment of additional search fees.

-***-Continued from Box No. III - Observations where unity of invention is lacking-***-

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fee must be paid.

Group I: Claims 1-24 are directed toward an authentication system comprising: receiving a request for authentication of a user comprising a biometric feature of the user collected by a user device and contextual data from the user device; comparing the biometric feature of the user to a baseline biometric feature of the user; comparing the contextual data to an expected contextual data value; and determining whether to authenticate the user.

Group II: Claims 25-32 are directed toward instructions to: receive from a first user device a network packet comprising an electronic data file and recipient biometrics; receive from a second user device biometric data obtained from a user of the second device; and permit the electronic data file to be accessed on the second user device when the biometric data obtained from the user of the second use device matches the recipient biometrics.

Group III: Claims 33-37 are directed toward a method of electronically sharing data, comprising: identifying an electronic file; providing biometrics associated with a recipient; providing contextual data associated with a recipient; causing the electronic file to be encrypted based on the provided biometrics and the provided contextual data; and causing the transmission of the encrypted electronic file to the recipient.

The common technical feature shared by Groups I, II, and III is providing biometrics associated with a user; and providing contextual data. However, this common feature is previously disclosed by US 2004/0134690 A1 (Norris). Norris discloses providing biometrics associated with a user (method and system for capturing biometric information of a sender; Abstract); and providing contextual data (method and system also captures biometric metadata (contextual data); Abstract).

Since the common technical feature is previously disclosed by the Norris reference, this common feature is not special and so Groups I, II, and III lack unity.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 April 2010 (01.04.2010)

PCT

(10) International Publication Number
WO 2010/035202 A1

(51) International Patent Classification:
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/IB2009/054120

(22) International Filing Date:
21 September 2009 (21.09.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
08165202.6 26 September 2008 (26.09.2008) EP

(71) Applicant *(for all designated States except US)*: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: GUAJARDO MERCHAN, Jorge [VE/NL]; c/o High Tech Campus Building 44, NL-5656 AE Eindhoven (NL). PETKOVIC, Milan [NL/NL]; c/o High Tech Campus Building 44, NL-5656 AE Eindhoven (NL).

(74) Agents: VAN VELZEN, Maaike, M. et al.; High Tech Campus 44, NL-5600 AE Eindhoven (NL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) Title: AUTHENTICATING A DEVICE AND A USER

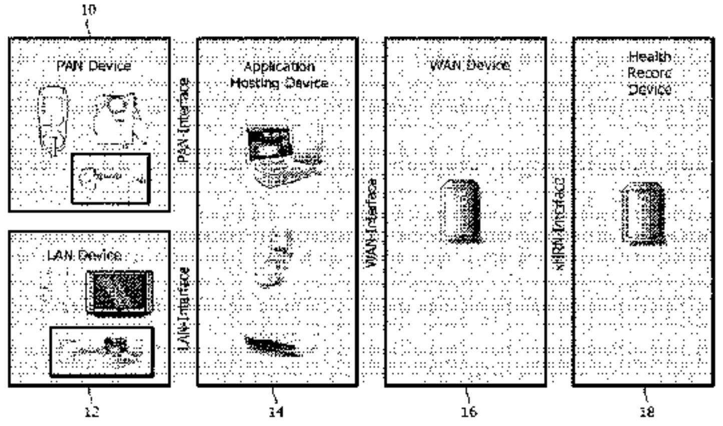


FIG. 1

(57) **Abstract**: A method of authenticating a device and a user comprises receiving a user input, generating a first key from the user input, performing a physical measurement of the device, obtaining helper data for the device, computing a second key from the physical measurement and the helper data, and performing an operation using the first and second keys. In a preferred embodiment, the method comprises performing a defined function on the first and second keys to obtain a third key. Additionally security can be provided by the step of receiving a user input comprising performing a biometric measurement of the user and the step of generating a first key from the user input comprises obtaining helper data for the user and computing the first key from the biometric measurement and the user helper data.

WO 2010/035202 A1

Authenticating a device and a user

FIELD OF THE INVENTION

This invention relates to a method of, and a system for, authenticating a device and a user. In one embodiment, the invention provides a combined device and patient authentication system for health services, especially those delivered as a part of a system in which the patient and healthcare provider are remote from one another and connected by an electronic system.

BACKGROUND OF THE INVENTION

An increasingly important trend in healthcare is one of consumer/patient involvement at all levels of healthcare. People are taking a more active role in their own health management. This trend of patient empowerment has already been widely supported. A number of solutions, (see for example, Capmed, http://www.phrforme.com/index.asp, Medkey, http://www.medkey.com/ and Webmd, http://www.webmd.com) have been introduced into the market that allow patients to collect their own health-related information and to store them on portable devices, computers, and in online services. These solutions are often referred to as Personal Health Record (PHR) services. Already a number of products in the market allow patients to enter automatically measurements and other medical data into their PHRs, see for example, Lifesensor, https://www.lifesensor.com/en/us/, and healthvault, http://search.healthvault.com/. For example a weight-scale sends its information via Bluetooth to a computer, from which the data is uploaded to a PHR. This allows patients to collect and manage their health data, but even more importantly to share the data with various healthcare professionals involved in their treatment.

Another important trend in healthcare is that the delivery of healthcare has gradually extended from acute institutional care to outpatient care and home care. Advances in information and communication technologies have enabled remote healthcare services (telehealth) including telemedicine and remote patient monitoring. A number of services in the market already deploy telehealth infrastructures where the measurement devices are connected via home hubs to remote backend servers. Health care providers use this architecture to remotely access the measurement data and help the patients. Examples are disease management services (such as Philips Motiva and PTS) or emergency response services (Philips Lifeline).

Interoperability of measurement devices, home hubs and backend services becomes very important for enabling and further growth of this market. This need is recognized by the Continua health alliance, see http://www.continuaalliance.org, for example. As shown in Fig. 1, this initiative aim to standardize protocols between measurement devices, home hub (application hosting) devices, online healthcare/wellness services (WAN) and health record devices (PHRs/EHRs). In addition to data format and exchange issues, the Continua alliance is also addressing security and safety issues.

One of the basic security and safety problems in the domain of telehealth is the problem of user and device authentication/identification. Namely, when data remotely measured by patients is used by telehealth services or in the medical professional world, the healthcare providers need to place greater trust in information that patients report. In particular, they have to be ensured that a measurement is coming from the right patient and that appropriate device was used to take the measurement. Consider a blood pressure measurement; it is crucial to know that the blood pressure of a registered user is measured (not of his friends/children), and that the measurement was taken by a certified device and not a cheap fake device. This is very important, because otherwise there can result critical health care decisions based on wrong data.

In current practice, a device identifier (device ID) is either used as a user identifier (user ID) or as a means to derive a user ID (if multiple users are using the same device). For example, in the Continua system, as described in "Continua Health Alliance, Recommendations for Proper User Identification in Continua Version 1 – PAN and xHR interfaces (Draft v.01)", December 2007, at the PAN interface, as shown in Fig. 1, each Continua device is required to send its own unique device ID. The user ID is optional (and can be just simple as 1, 2, A, B). The valid user ID is obtained at the hub device (application hosting device), which can provide mapping between a simple user ID associated with a device ID to a valid user ID. There might be also measurement devices that can send a valid user ID next to the device ID. Then the mapping is not needed.

There are several problems with the current approach. For example, the current approach does not support authentication of users/devices, it only appends the user ID to the measurement. Data provenance is not established, as a healthcare provider later in the process cannot securely find which device was used to create the measurement. Next to that, the current mapping approach does not quickly lock the user and device ID together, but it introduces room for mistakes. Either a user makes an unintended mistake (if manual mapping is required – the user has to select his ID (1 or A) at application hosting device or measurement device for each measurement) or the system can mix the users (the application designer should take special care to provide data management in a way to reduce the potential for associating measurements to the wrong user). In this type of arrangement, it is possible for a malicious user to introduce wrong measurements by impersonating the real user. Similarly, the device ID can be copied to forged devices, which can be easily introduced in the eco system. Then a user can use these devices to produce data that will look reliable but in fact will be unreliable.

It is therefore an object of the invention to improve upon the known art.

According to a first aspect of the present invention, there is provided a method of authenticating a device and a user comprising receiving a user input, generating a first key from the user input, performing a physical measurement of the device, obtaining helper data for the device, computing a second key from the physical measurement and the helper data, and performing an operation using the first and second keys.

According to a second aspect of the present invention, there is provided a system for authenticating a device and a user comprising a user interface arranged to receive a user input, a query component arranged to perform a physical measurement of the device, and a processing component connected to the user interface and the query component, and arranged to generate a first key from the user input, to obtain helper data for the device, to compute a second key from the physical measurement and the helper data, and to perform an operation using the first and second keys.

According to a third aspect of the present invention, there is provided a method of registering a device and a user comprising receiving a user input, generating a first key from the user input, performing a physical measurement of the device, generating a second key and helper data for the device from the physical measurement, performing an operation using the first and second keys, and transmitting an output of the operation to a remote data store.

According to a fourth aspect of the present invention, there is provided a system for registering a device and a user comprising a user interface arranged to receive a user input, a query component arranged to perform a physical measurement of the device, and a processing component arranged to generate a first key from the user input, to generate a second key and helper data for the device from the physical measurement, to perform an operation using the first and second keys, and to transmit an output of the operation to a remote data store.

Owing to the invention, it is possible to bind the identity of a user and a device so as to certify that data originating from the device originates from the particular device and the particular user. This supports data quality assurance and reliability in personal healthcare applications. In this system, there is delivered a method to bind the identity of a user and a device identifier as early as possible, so as to certify that data originating from the device originates from the particular device and the particular user. To ensure proper device and user authentication/identification it is possible to use a Physically Uncloneable Function (PUF, described in detail below) in combination with a user input.

As a result there is covered the three problems from the prior art by providing respectively, close coupling of the user ID and the identification of the device used to take the measurement (the use of unregistered device/user is immediately detected), strong user authentication and anti-counterfeiting and strong device authentication. This has the following benefits, patient safety (diagnosis and health decisions are based on reliable data), reduction of costs (reuse of patient provided data in the consumer health and the professional healthcare domain) and convenience for the patient (they can take healthcare measurements at home).

In a preferred embodiment, the step of receiving a user input comprises performing a biometric measurement of the user and the step of generating a first key from the user input comprises obtaining helper data for the user and computing the first key from the biometric measurement and the user helper data. The user of a biometric measurement, such as a fingerprint, increases the security of the system and ensures that any data taken from an individual is authenticated as being from that specific individual, when the data is analyzed by a remote health system.

Advantageously, the method comprises performing a defined function on the first and second keys to obtain a third key. The security of the system can be increased if the two keys, one from the device and one from the user are combined together to create a third key, prior to any transmittal to a remote location. The combination can be performed according to a function of both inputs. Such function can be for example: (i) the concatenation of both strings, the XORing of both strings, the concatenation of both strings and subsequent hashing of the resulting string, the XORing of both strings and then hashing the resulting string, the encryption of one string according to an encryption algorithm (e.g.

the Advanced Encryption Standard) using as key one of the strings and as plaintext the second string, etc.

In a further embodiment, the step of receiving a user input comprises receiving a password and the step of generating a first key from the user input comprises computing the first key from the password. Rather than using biometric data, a simple password can be used to authenticate the user. Although this does not have the highest level of security associated with using the biometric data, this still provides a system that is an improvement over current known systems.

Ideally, the step of obtaining helper data for the device comprises computing the helper data from the first key and a stored component. The key for the device (the second key) is created from the physical measurement performed on the device and the helper data. If the helper data is reconstructed from the first key (from the user) and some stored component, then the security of the system of authenticating the device and user is increased, because the helper data is never stored in the clear.

Advantageously, the method further comprises obtaining a user share, obtaining a device share, and performing a defined function on the user share, device share, first and second keys to obtain a third key. The use of a user share and device share allows more than one device to be authenticated to a specific user, which increases the efficiency of the registration and authentication system.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the present invention will now be described, by way of example only, with reference to the accompanying drawings, in which:-

Fig. 1 is a schematic diagram of a healthcare system,

Fig. 2 is a further schematic diagram of the healthcare system,

Fig. 3 is a schematic diagram of a device and user authentication system,

Fig. 4 is a flowchart of a registration procedure,

Fig. 5 is a flowchart of an authentication procedure,

Fig. 6a is a schematic diagram of a preferred embodiment of the authentication system, and

Fig. 6b is a further schematic diagram of a preferred embodiment of the authentication system, and

Fig. 7 is a schematic diagram of a further embodiment of the system.

DETAILED DESCRIPTION OF THE EMBODIMENTS

An example of a healthcare system is shown in Fig. 1. Various PAN (personal area network) devices 10 are shown such as a wristwatch and a blood pressure measuring device, which directly measure physiological parameters of a user. Additionally LAN (local area network) devices 12 are provided such as a treadmill which can also be used to gather healthcare information about the user. The PAN devices 10 and the LAN devices 12 are connected via suitable interfaces (wired and/or wireless) to an appropriate application hosting device 14, such a computer or mobile phone, which will be local to the PAN and LAN devices 10 and 12. This hosting device 14 will be running a suitable application which can gather and organize the outputs from the various PAN and LAN devices 10 and 12.

The application hosting device 14 is connected to a WAN (wide area network) device 16 such as a server. The WAN connection can be via a network such as the Internet. The server 16 is also connected via a suitable interface to a health record device 18, which is maintaining a health record for the users of the system. As discussed above, it is of paramount importance that the data recorded by the individual health records stored by the device 18 is assigned, firstly to the correct user, and additionally, that the device which recorded the data is known with absolute certainty. It is also advisable that the relevant PAN or LAN device 10 or 12 is also approved for use in the system.

Fig. 2 illustrates the system of Fig. 1, with a user 20 who is taking a measurement with a PAN device 10. Through the home hub 14, data can be communicated to the remote record device 18, which is maintaining the patient's record 22. The remote record device 18 also communicates directly with a GP record 24. In this example, the user 20 has wrongly identified themselves to the device 10, and is also using an incorrect device 10, for the measurement that they are trying to make. In a conventional system, this will result in an incorrect entry being made in their record 22, and could cause an incorrect alert to be raised with respect to the patient's condition.

In order to prevent the kind of error that is illustrated by Fig. 2, the system according to the present invention is summarized in Fig. 3. This Figure. shows a device 10 and the user 20, communicating with the remote healthcare device 18. The essential principle is that a key is derived from the user 20 and a key is derived from the device 10, and, in one embodiment, these are combined together and transmitted to the remote server 18 as a third key. The user 20 could supply a password, or in the preferred embodiment, there is performed a biometric measurement of the user 20 (such as a fingerprint) and the user key is generated from this biometric measurement. The key from the device 10 is derived from a physical measurement of the device. One method of achieving this is to use a function known as a PUF, described below.

The system of Fig. 3 for authenticating the device 10 and the user 20 comprises a user interface arranged to receive a user input, a query component arranged to perform a physical measurement of the device, and a processing component connected to the user interface and the query component, and arranged to generate a first key from the user input, to obtain helper data for the device, to compute a second key from the physical measurement and the helper data, and to perform an operation using the first and second keys. These three components, the user interface, the query component and the processing component could all be contained within the device 10, or could be distributed amongst different devices. Indeed the functions of the processing component could be split between different processors contained in different devices.

A Physical Uncloneable Function (PUF) is a function that is realized by a physical system, such that the function is easy to evaluate but the physical system is hard to characterize and hard to clone, see for example R. Pappu, "Physical One-Way Functions", Ph.D. thesis, MIT, 2001. Since a PUF cannot be copied or modeled, a device equipped with a PUF becomes uncloneable. Physical systems that are produced by an uncontrolled production process (i.e. that contains some randomness) are good candidates for PUFs. The PUF's physical system is designed such that it interacts in a complicated way with stimuli (challenges) and leads to unique but unpredictable responses. A PUF challenge and the corresponding response are together called a Challenge-Response-Pair. It is possible for a PUF to have a single challenge, or a limited (small) number of challenges (less than 32 for example), or a large number of challenges (2^n challenges for n>5).

One example of a PUF is the so-called SRAM PUFs. As far as experiments have shown today, these PUFs are present on any device having an SRAM on board. It is based on the phenomenon that when an SRAM cell is started up, it starts up in a random state. However, when this is done multiple times, the SRAM starts up, most of the time, in the same state and can therefore be used as a type of PUF. S-RAM PUFs are described in more detail in ID685102. Other PUFs include an optical PUF, disclosed in the above reference and a delay PUF (see Gassend et al., Su et al. – IC PUFs (Delay PUF) CCS 2002, ACSAC 2002).

As previously mentioned, PUF responses are noisy and not fully random. Thus, a Fuzzy Extractor or Helper Data Algorithm (see J.-P. M. G. Linnartz and P. Tuyls, "New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates," in Audio-and Video-Based Biometrie Person Authentication — AVBPA 2003, ser. LNCS, J. Kittler and M. S. Nixon, Eds., vol. 2688. Springer, June 9-11, 2003, pp. 393–402 and Y. Dodis, M. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in Advances in Cryptology —- EUROCRYPT 2004, ser. LNCS, C. Cachin and J. Camenisch, Eds., vol. 3027. Springer-Verlag, 2004, pp. 523–540.) is required to extract one (or more) secure keys from the PUF responses.

In the following, there is provided the intuition behind the algorithms. A fuzzy extractor requires two basic primitives, firstly information reconciliation or error correction and secondly privacy amplification or randomness extraction, which guarantees an output which is very close to being a uniformly distributed random variable. In order to implement those two primitives, helper data W is generated during the enrolment or registration phase. Later, during the key reconstruction or authentication phase, the key is reconstructed based on a noisy measurement Ri and the helper data W. During the enrolment phase (carried out in a trusted environment), a probabilistic procedure called Gen is run. This procedure takes as its input a PUF response R, and produces as output a key K and helper data W: (K,W) ← Gen(R). In order to generate the helper data W, an error correcting code C is chosen such that at least t errors can be corrected. The number of errors to be corrected depends on the particular application and on the PUF properties.

Once an appropriate code has been chosen, the helper data W is generated by first choosing a random code word C_S from C and computing $W1 = C_S \oplus R$. Furthermore a universal hash function (see L. Carter and M. N. Wegman, "Universal Classes of Hash Functions," J. Comput. Syst. Sci., vol. 18, no. 2, pp. 143–154, 1979) h_i is chosen at random from a set H and the key K is defined as $K \leftarrow h_i(R)$. The helper data is then defined as W = (W1, i). During the key reconstruction phase a procedure called Rep is run. It takes as input a noisy response R' and helper data W and reconstructs the key K (if R' originates from the same source as R) i.e. K ← Rep(R',W). Reconstruction of the key is achieved by computing $C_S' = W1 \oplus R'$, decoding C_S' to C_S via the decoding algorithm of C, recovering $R = C_S \oplus W1$, and finally computing $K = h_i(R)$. The present method will work also with other types of helper data. For example, instead of XORing, it is possible to also perform a permutation.

It should be noted that the symbol ⊕ is used to indicate an XOR operation. The logical operation exclusive disjunction, also called exclusive or (XOR), is a type of logical disjunction on two operands that results in a value of "true", if and only if, exactly one of the operands has a value of "true".

Fuzzy extractor construction can also be used to generate unique identifiers or keys from biometric data. Instead of having a PUF response, there is used a person's biometric data. This can be further enhanced by computing the hash (say SHA-2) of K (where K = h_i(R), and R is a biometric measurement). See T. Kevenaar, G.J. Schrijen, A. Akkermans, M. Damstra, P. Tuyls, M. van der Veen, Robust and Secure Biometrics: Some Application Examples. ISSE 2006 for an overview of different applications of this construction and Kevenaar, T.A.M, Schrijen, G.J., van der Veen, M., Akkermans, A.H.M. and Zuo, F.: Face Recognition with Renewable and Privacy Preserving Templates. Proc. 4th IEEE Workshop on Automatic Identification Advanced Technologies (AutoID 2005), 17-18 Oct. 2005 Page(s): 21 – 26 for an example applied to biometrics based on face recognition.

As previously mentioned, the system of the present invention is designed to link a measurement to both a device ID and the particular user. A stable device ID can be derived from a PUF response and associated helper data. The helper data can be chosen randomly from code words of an error correcting code. In a preferred embodiment, the helper data is derived from both an error correcting code and from a string derived from a biometric measurement of the user. By constructing such helper data, it is possible to authenticate both the device and the user at once.

In a preferred embodiment, it is assumed that the following are available on the device that is being used, a PUF such that when challenge with Ci produces a response Ri, which is written as Ri ← PUF(Ci), a GenPUF algorithm which upon getting a PUF response Ri outputs (Ki,Wi), with (Ki,Wi) ← GenPUF(Ri), a RepPUF algorithm which upon getting a PUF response Ri' and helper data Wi outputs the key Ki if Ri and Ri' are sufficiently close, with Ki ← RepPUF(Ri',Wi), a GenBio algorithm which upon getting a biometric measurement BMu from user U outputs (Ku,Wu), with (Ku,Wu) ← GenBio(BMu), and a RepBio algorithm which upon getting a biometric measurement BMu from user U and helper data Wu outputs the key Ku if BMu and BMu' are sufficiently close, Ku ← RepBio(BMu',Wu). It is assumed that the device that is used to perform the measurements has a PUF embedded in it. This can be easily expected from any device containing, for example an SRAM memory, such as any microprocessor or microcontroller. Clearly, the algorithms GenPUF, GenBio, RepPUF, and RepBio can be implemented on the device but do not have to. They could be implemented on a second device. The first option is better from the security stand point. However, the second option makes it possible to implement the system for devices with limited processing capabilities.

Fig. 4 shows how the system would work in relation to a preferred embodiment of the registration procedure. Firstly, a group of users has a device i which measures some signal of users U1, U2, U3, …, Un. Prior to using the device for the first time, one of the users (Uj) runs the procedure GenPUF on the PUF of device i and obtains (Ki,Wi) ← GenPUF(Ri) corresponding to a response Ri originating from device i. This is the step S1 of the process. Note that this step does not need to be run by device i. In particular, this procedure can be run by a separate entity. The only thing needed by the entity to run GenPUF is the response Ri.

At the second step S2, the helper data Wi is stored in non-volatile memory of device i. An individual user, user Uj runs GenBio on his/her biometric (such as a fingerprint) and obtains Kuj, which is step S3. At step S4, this value is XORED with Wi to produce Wi,uj, which is stored in the device in user's Uj memory profile space, at step S5. In other words, Wi,uj = Wi XOR Kuj. A database is stored in the device with entries as follows: (Kuj; Wi,uj). The next step is step s6, in which for the user Uj there is computed a key Kij as a function of Ki and Kuj, written Kij ← f(Ki,Kuj). At step S7, this key is transmitted in a secure manner to the health service provider. Steps 3 to 7 are repeated for every user who wants to use the device. An alternative to storing the pairs (Kuj; Wi,uj) in the device's database is to store a pair (Uj, Wi,uj). This assumes that the user has a string Uj that identifies him. This is more secure since the key Kuj is not stored in the device but reconstructed every time that is needed. The string Uj can be any identifying information such as the name of the user, his social security number, driver's license number, email address, etc.

In summary, the method of registering a device and a user comprising receiving the user input (which could be a biometric measurement or a password), generating the first key from the user input, performing a physical measurement (such as a PUF) of the device, generating a second key and helper data for the device from the physical measurement, performing an operation using the first and second keys, and transmitting an output of the operation to a remote data store.

A preferred embodiment of an authentication procedure is shown in Fig. 5. The procedure is used after the user and device have registered, as per the flowchart of Fig. 4. User Uj desires to use device i to perform a measurement. Before being able to operate the device, the first step S1, is that the user Uj runs Kuj ← RepBio(BMuj',Wuj) and recovers Kuj. At step S2, the device i searches in its database for a match with Kuj. If it finds such a match it continues to step 3, otherwise the device stops and tells the user to register first, in order to be able to use device i.

If there is a match, then at step S3, the device i XORs Kuj with Wi,uj to obtain Wi = Wi,uj XOR Kuj, followed by step S4, in which the device i runs Ki ← RepPUF(Ri',Wi) to recover Ki. At step S5, the device i computes a function of Ki and Kuj, written f(Ki,Kuj) resulting in a string Kij and, at step S6 the device i computes a Message Authentication Code (MAC) on the data measured with secret key Kij. Finally, at step S7, the device i sends the data and the MAC to the health service provider. The health service provider verifies the MAC and if the verification succeeds the data is accepted.

In this way a secure method of authenticating a device and a user is delivered. Neither the physical function of the device (in the preferred embodiment the PUF) nor the data from the user (in the preferred embodiment the biometric data) can be cloned or faked in any way, and the transmittal of these keys (or a single key derived from them both) to the health service provider allows both the device and user to be authenticated.

An alternative solution (Embodiment 2) to that provided by the procedures of flowcharts 4 and 5 is to perform separate authentication of the device and the patient and then combine these identifiers/keys or send them separately to the service provider. For example, it is possible to derive Ki from PUF, then derive Kuj from the user's biometrics and then combine the keys into a single key: Kij = Hash(Ki||Kuj). Based on this key (Kij) a MAC or a signature on the data can be computed before being sent to the service provider. However, this would fail to identify, in the beginning, a user that has not run the registration procedure before using the measuring device for the first time (i.e. the user has to register a new key, for each new device he obtains; and this registration has to be done with all service providers and/or health service infrastructures that use his data).

Other variations of the preferred embodiment are also possible. For example, the device does not perform the key reconstruction itself, but rather sends the measured signal together with a PUF response Ri' to a more powerful device, for example the home hub 14 in Fig. 2, where all the processing is performed. Note that in this particular case, there is no concern over the secrecy of the response. Rather the system is only interested in making sure that there is the correct data associated with the correct user and device.

The methodology above could also be adapted so that instead of computing a helper data Wi,uj, the device could simply store Wi and then compute Kij as the XOR of Ki and Kuj. However, this would fail to identify in the beginning a user that has not run the registration procedure before using the measuring device for the first time.

Another alternative could be that instead of using a symmetric-key based system the system can use an asymmetric key based system. Instead of considering Kij as a symmetric key, the system can use the secret-key of a public-key based system. Then in step S7 of the registration procedure (Fig. 4), instead of sending Kij to the service provider, the device can send the public-key associated with a secret-key Kij. This can be easily computed for typical public-key based systems.

In one embodiment there is performed a defined function on the first key from the user and the second key from the device to obtain a third key (Kij). The function used to compute Kij from Ki and Kuj could be, for example, a hash (SHA-1, SHA-2, MD5, RipeMD, etc.) of the concatenation of Ki and Kuj, an XOR of Ki and Kuj, an encryption of a constant string using as key Ki and Kuj, and encryption of Ki using Kuj as the encryption key of an encryption system, an encryption of Kuj using Ki as the encryption key of an encryption system, a value derived from a 2-out-n threshold scheme where two of the shares correspond to Ki and Kuj (see below for additional advantages of using threshold schemes), or any other function of Ki and Kuj appropriate for the application.

The preferred embodiment of the invention is shown in Fig. 6a and Fig. 6b. In Fig. 6a a processor 30 is connected to a device 10 and a user input device 32. The device 10 is a device for measuring the blood pressure of the user, and the user input device 32 is a device for measuring the fingerprint of the user, when the user places their finger into the device. The system of this Figure assumes that the registration process has already taken place and the user has performed the measurement of their blood pressure with the device 10. The user wishes to authenticate the acquired data prior to sending that acquired data to the third party health service provider.

Fig. 6b illustrates the actions taken by the processor 30. The user input 34, being a biometric measurement of the user's fingerprint is received by the processor 30, from the user input device 32. The PUF 36 is also received from a query applied to the device 10. Within the system is present a query component which makes a PUF query to the device 10. This component (not shown) could be built in within the device 10. The user input 34 is combined with user helper data 38 to generate a first key 40, and the PUF 36 is combined with device helper data 42 to generate a second key.

In this Figure, the key generation processes are shown as independent, but they could be configured in such a way that the key from one side is used to generate the helper data on the other side, and vice versa, as an extra security feature, using an additional stored component. The generation of the two keys 40 and 44 could occur simultaneously, or in the case where the key of one is used to generate the helper data of the other, then the generation would occur sequentially. Either key could be generated first. The reference to the user's key as the first key 40 does not mean that it is the first key to be generated by the processor 30.

After the keys 40 and 44 have been generated then they are passed to an operation stage 46, which performs an operation using the two keys 40 and 44. This operation could take a number of different forms. In the simplest embodiment, the operation is the transmission of the two keys 40 and 44, with the acquired data about the user's blood pressure, to the third party service provider. Another option would be to combine the two keys 40 and 44 into a third key and transmit this third key with the data. A third option would be to encrypt the user's health data with either the two keys 40 and 44, or using something (such as a hash function output) derived from the two keys 40 and 44. Another option would be the generation of a digital signature using the keys 40 and 44 to sign the data before it is sent. In this way the data gathered by the user is authenticated using the two keys 40 and 44.

The key Kuj derived from the user, which in the preferred embodiment is a biometric measurement, could be derived from a password for example. The intent is to make the key that is used to sign dependent on something that User Uj has to provide or enter into the system. It does not necessarily have to be a biometric, although this would make it less likely to be vulnerable to impersonation attacks. This embodiment is shown in Fig. 7.

In this embodiment, the user 20 provides a user input which is a password 28. The device 10 generates a key from the password, and also performs a physical measurement of the device (using a PUF). The device accesses the helper data for the device and computes a second key from the physical measurement and the helper data, as discussed in detail above. The device then transmits the first and second keys (or a third key derived from these two keys) to the health service provider 18.

The system can also be adapted to generating a single per user key from multiple devices. In this embodiment, there is provided an approach that uses only one key per patient/user regardless of the number of devices that are used for obtaining data (in contrast to previous embodiments where one key per each user-device combination was necessary). For this construction it is possible to use threshold secret sharing, which is described in the following.

Threshold secret-sharing is described in Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1997. A (t,n) threshold scheme (t<=n) is a method by which a trusted party computes secret shares S_i, 1 <= i <= n from an initial secret S, and securely distributes S_i to user P_i, such that the following is true: any t or more users who pool their shares may easily recover S, but any group knowing only t − 1 or fewer shares may not. A perfect threshold scheme is a threshold scheme in which knowing only t − 1 or fewer shares provide no advantage (no information about S whatsoever, in the information-theoretic sense) to an opponent over knowing no shares.

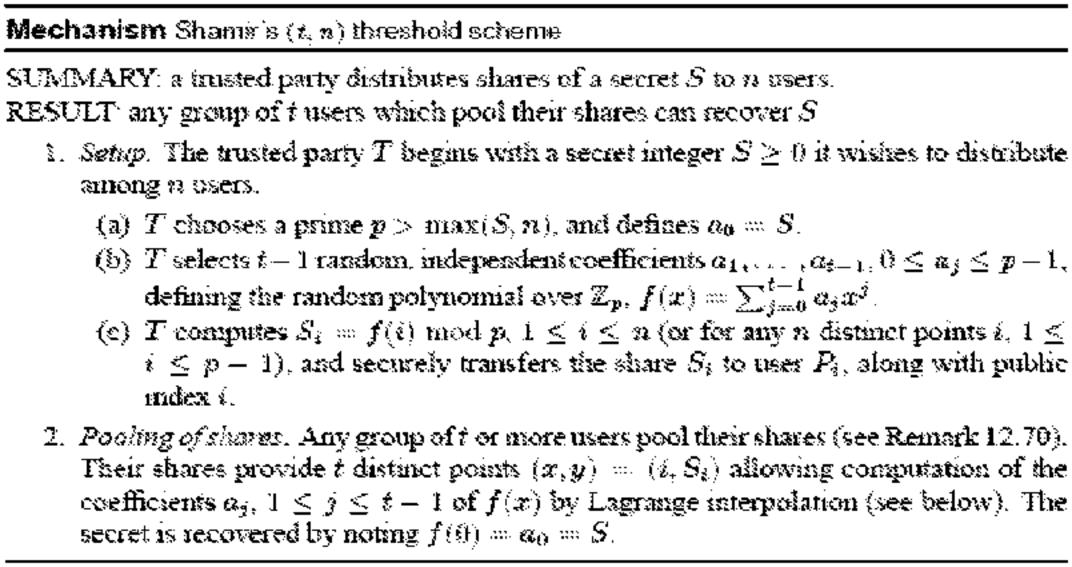
Shamir's threshold scheme is based on polynomial interpolation, and the fact that a univariate polynomial y = f(x) of degree t − 1 is uniquely defined by t points (x_i; y_i) with distinct x_i (since these define t linearly independent equations in t unknowns). The coefficients of an unknown polynomial f(x) of degree less than t, defined by points (x_i; y_i), 1 <= i <= t, are given by the Lagrange interpolation formula:

$$f(x) = \sum_{i=1}^{t} y_i \prod_{1 \leq j \leq t, j \neq i} \frac{x - x_j}{x_i - x_j}.$$

Since f(0) = a0 = S, the shared secret may be expressed as:

$$S = \sum_{i=1}^{t} c_i y_i , \quad \text{where } c_i = \prod_{1 \leq j \leq t, j \neq i} \frac{x_j}{x_j - x_i}.$$

Thus each group member may compute S as a linear combination of t shares y_i, since the c_i are non-secret constants (which for a fixed group of t users may be pre-computed). Below is shown Shamir's (t,n) threshold scheme. Shamir's threshold scheme is provided as an example, however, other threshold secret sharing schemes can also be used, for example, Oded Goldreich, Dana Ron, Madhu Sudan: "Chinese remaindering with errors" IEEE Transactions on Information Theory 46(4): 1330-1338 (2000).



Mechanism Shamir's (t, n) threshold scheme

SUMMARY: a trusted party distributes shares of a secret S to n users.
RESULT: any group of t users which pool their shares can recover S

1. *Setup.* The trusted party T begins with a secret integer $S \geq 0$ it wishes to distribute among n users.
   (a) T chooses a prime $p > \max(S, n)$, and defines $a_0 = S$.
   (b) T selects $t-1$ random, independent coefficients $a_1, \ldots, a_{t-1}$, $0 \leq a_j \leq p-1$, defining the random polynomial over $\mathbb{Z}_p$, $f(x) = \sum_{j=0}^{t-1} a_j x^j$.
   (c) T computes $S_i = f(i) \bmod p$, $1 \leq i \leq n$ (or for any n distinct points i, $1 \leq i \leq p-1$), and securely transfers the share S_i to user P_i, along with public index i.
2. *Pooling of shares.* Any group of t or more users pool their shares (see Remark 12.70). Their shares provide t distinct points $(x, y) = (i, S_i)$ allowing computation of the coefficients a_j, $1 \leq j \leq t-1$ of $f(x)$ by Lagrange interpolation (see below). The secret is recovered by noting $f(0) = a_0 = S$.

Using Shamir's Threshold scheme it is possible to combine several keys (in this particular case two keys) to generate a single key as follows. This uses a 2-out-n threshold scheme as follows. The user computes a different key Ki for every device as has been described in the previous embodiments. The user also computes a key based on his biometric Kuj. The user defines a 2-out-n threshold scheme as follows:

The user chooses a prime p large enough such that Ki < p and Kuj < p. Alternatively, it is possible to choose a prime p large enough for security purposes, and based on this, compute strings Ki' and Kuj', which (when interpreted as integers) are less than p. One possible way to compute such strings is simply as Ki' = Hash(Ki) mod p and Kuj' = Hash(Kuj) mod p, for some hash function Hash. The user chooses a random key Kij such that 2 <= Kij <= p-1, and sets a0 = Kij. The user then chooses one independent and random coefficient a1 such that 1<= a1 <= p-1. Note that a1 must be non-zero (in contrast to the general Shamir's threshold scheme). The user computes a share Yuj as follows: Yuj = a1*Kuj' + a0. The user stores in device i Yuj (Yuj is the same for all devices). The user then computes a share Yi for device i as follows: Yi = a1*Ki' + a0. The user stores in device i Yi. The Yi is device dependent. This is repeated for every device i that the user wants to use.

If the system supports only symmetric-key authentication then the key Kij (corresponding to a0) is sent to the service provider. If the system is public-key based then a corresponding public key is derived using a0 as the secret key of the system and the public-key is sent to the service provider via a secure and authenticated channel. To provide the authentication in such a system, the user obtains their biometric dependent key and obtains a user share (Kuj', Yuj). The device computes its key Ki (by any of the methods described above which might include the use of the user's biometric as well) and obtains a device share (Ki, Yi) for device i. Using Lagrange interpolation the key Kij is reconstructed from the two shares. The user uses Kij to compute a MAC or a signature on the data being sent to the service provider.

There are several advantages of the proposed system. Most importantly, the system allows for early coupling of device and user identifiers that can be obtained by strong authentication (for example using PUFs and biometrics). In the preferred embodiment, the key derivation is performed in one step which leads to higher reliability.

Furthermore, the system is advantageous because there it is necessary to register with the service provider only a single key per user. This supports separation of duties. The service provider or health service infrastructure does not have to take care of registration of measurement devices. A TTP (Trusted Third Party), such as a Continua certification centre, can perform the registration in a way that for each device a user has, the combined device/user key is the same, as described in the final embodiment. The TTP certifies the key which is registered by service providers and health service infrastructure. This is much simpler than continuously registering with the service provider the keys of each device the user has and will obtain (which is required by traditional approaches). Additionally, at the service provider and health service infrastructure site, the key management is much simpler as they have to deal with far fewer keys. They do not have to change much current practice of using one identifier/key per patient. Finally, depending on the embodiment chosen for the implementation, it is possible to identify a user which has not been registered before, which also contributes to the reliability of the measured data.

Next to that, there are important advantages of biometrics over other authentication approaches. Most importantly, some physiological measurements could serve a dual purpose. For example, measuring patient's vital signs (for example ECG) and at the same time using the measurement for patient authentication (biometric data can be extracted from the physiological measurement such as ECG). This methodology couples the measurement to the patient as strongly as possible. In addition, biometric data is more convenient and secure than a passwords or smartcards that can be forgotten or lost. Biometric data provides a stronger type of authentication when compared to smartcards or passwords, which can be easily handed over to other people.

CLAIMS:

1. A method of authenticating a device (10) and a user (20) comprising:
- receiving a user input (28, 34),
- generating a first key (40) from the user input (28, 34),
- performing a physical measurement (36) of the device (10),
- obtaining helper data (42) for the device (10),
- computing a second key (44) from the physical measurement (36) and the helper data (44), and
- performing an operation (46) using the first and second keys (40, 44).

2. A method according to claim 1, wherein the step of performing an operation (46) using the first and second keys (40, 44) comprises performing a defined function on the first and second keys (40, 44) to obtain a third key.

3. A method according to claim 1 or 2, wherein the step of receiving a user input (28) comprises receiving a password (28) and the step of generating a first key (40) from the user input (28) comprises computing the first key (40) from the password (28).

4. A method according to claim 1 or 2, wherein the step of receiving a user input (34) comprises performing a biometric measurement (34) of the user (20) and the step of generating a first key (40) from the user input (34) comprises obtaining helper data (38) for the user (20) and computing the first key (40) from the biometric measurement (34) and the user helper data (38).

5. A method according to claim 4, wherein the step of obtaining helper data (42) for the device (10) comprises computing the helper data (42) from the first key (40) and a stored component.

6. A method according to any preceding claim, and further comprising obtaining a user share, obtaining a device share, and performing a defined function on the user share, device share, first and second keys (40, 44) to obtain a third key.

7. A system for authenticating a device (10) and a user (20) comprising:

- a user interface (32) arranged to receive a user input (28, 34),
- a query component arranged to perform a physical measurement (36) of the device (10), and
- a processing component (30) connected to the user interface (32) and the query component, and arranged to generate a first key (40) from the user input (28, 34), to obtain helper data (42) for the device (10), to compute a second key (44) from the physical measurement (36) and the helper data (42), and to perform an operation (46) using the first and second keys (40, 44).

8. A system according to claim 7, wherein the processing component (30) is arranged, when performing an operation (46) using the first and second keys (40, 44), to perform a defined function on the first and second keys (40, 44) to obtain a third key.

9. A system according to claim 7 or 8, wherein the user input (28) comprises a password (28) and the processing component (30) is arranged, when generating a first key (40) from the user input (28), to compute the first key (40) from the password (28).

10. A system according to claim 7 or 8, wherein the user input (34) comprises a biometric measurement (34) of the user (20) and the processing component (30) is arranged, when generating a first key (40) from the user input (34), to obtain helper data (38) for the user (20) and to compute the first key (40) from the biometric measurement (34) and the user helper data (38).

11. A system according to claim 10, wherein the processing component (30) is arranged, when obtaining helper data (42) for the device (10), to compute the helper data (42) from the first key (40) and a stored component.

12. A system according to any one of claims 7 to 11, wherein the processing component (30) is further arranged to obtain a user share, obtain a device share, and to

perform a defined function on the user share, device share, first and second keys (40, 44) to obtain a third key

13. A system according to any one of claims 7 to 12, wherein the user interface, the query component and the processing component are contained within a single device.

14. A system according to any one of claims 7 to 12, wherein the user interface (32), the query component (10) and the processing component (30) are distributed across a plurality of devices.

15. A method of registering a device (10) and a user (20) comprising:

- receiving a user input (28, 34),
- generating a first key (40) from the user input (28, 34),
- performing a physical measurement (36) of the device (10),
- generating a second key (44) and helper data (42) for the device (10) from the physical measurement (36),
- performing an operation (46) using the first and second keys (42, 44), and transmitting an output of the operation (46) to a remote data store.

16. A method according to claim 15, wherein the step of receiving a user input (34) comprises performing a biometric measurement (34) of the user (20) and the step of generating a first key (40) from the user input (34) includes generating helper data (38) for the user (20).

17. A system for registering a device (10) and a user (20) comprising:

- a user interface (32) arranged to receive a user input (28, 34),
- a query component arranged to perform a physical measurement (36) of the device (10), and
- a processing component (30) arranged to generate a first key (40) from the user input (28, 34), to generate a second key (44) and helper data (42) for the device (10) from the physical measurement (36), to perform an operation (46) using the first and second keys (40, 44), and to transmit an output of the operation (46) to a remote data store.

18. A system according to claim 17, wherein the user input (34) comprises a biometric measurement (34) of the user (20) and the processing component (30) is further arranged, when generating a first key (40) from the user input (34), to generate helper data (38) for the user (20).

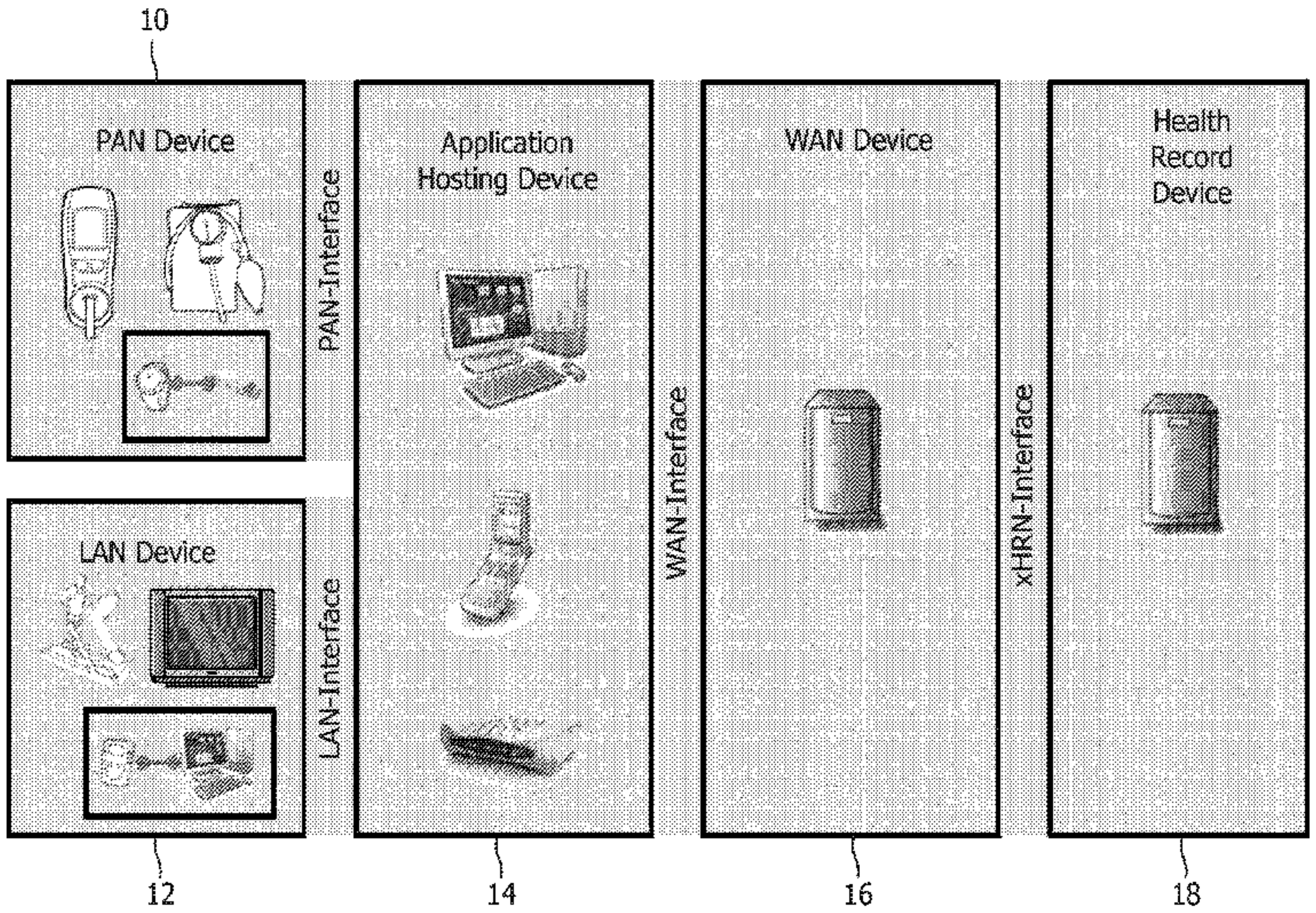

10
PAN Device
PAN-Interface
LAN Device
LAN-Interface
12
Application Hosting Device
14
WAN-Interface
WAN Device
16
xHRN-Interface
Health Record Device
18

FIG. 1

2/7

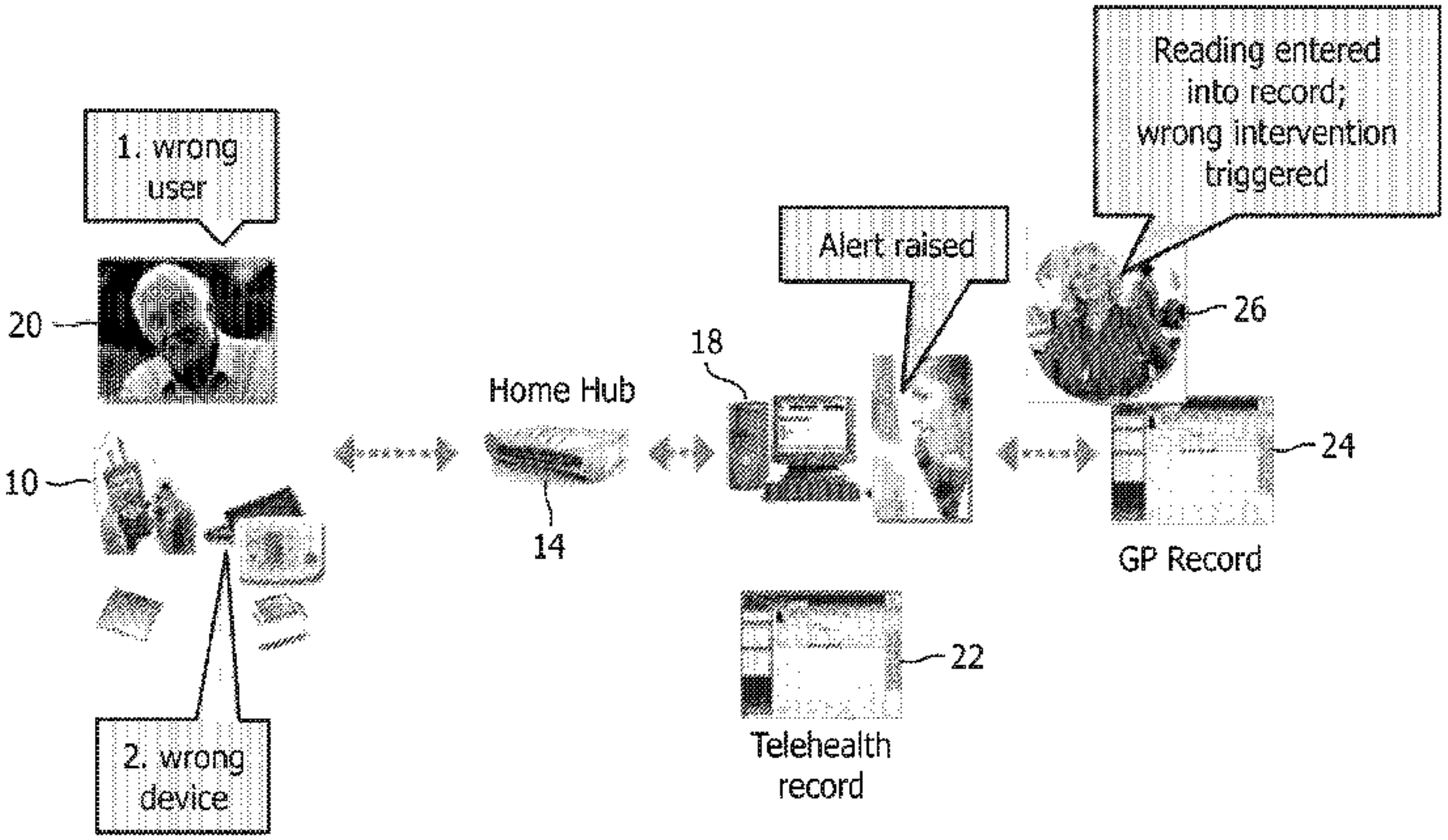

1. wrong user
20
10
2. wrong device
Home Hub
14
18
Alert raised
Telehealth record
22
Reading entered into record; wrong intervention triggered
26
24
GP Record

FIG. 2

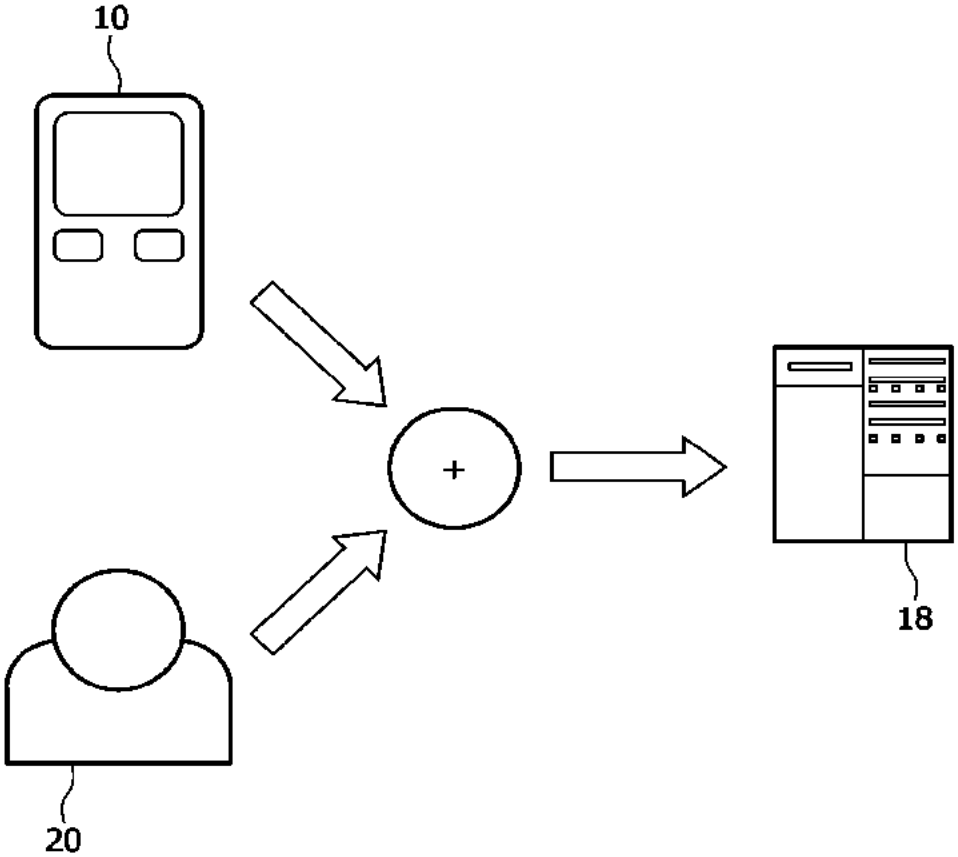


FIG. 3

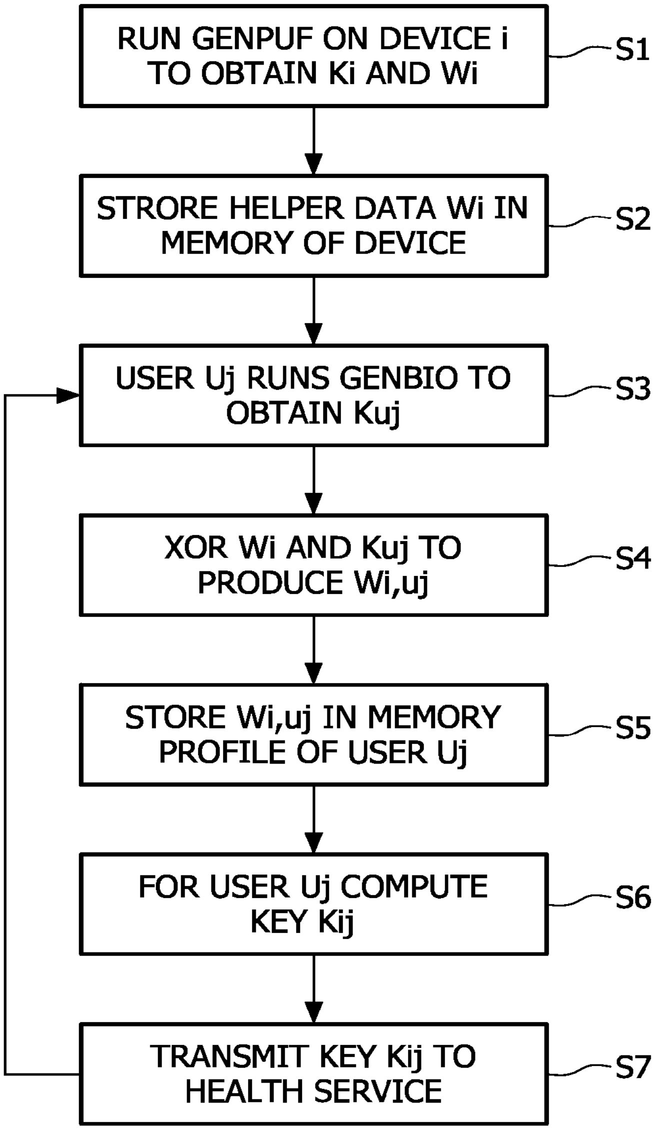

RUN GENPUF ON DEVICE i TO OBTAIN Ki AND Wi
S1
STRORE HELPER DATA Wi IN MEMORY OF DEVICE
S2
USER Uj RUNS GENBIO TO OBTAIN Kuj
S3
XOR Wi AND Kuj TO PRODUCE Wi,uj
S4
STORE Wi,uj IN MEMORY PROFILE OF USER Uj
S5
FOR USER Uj COMPUTE KEY Kij
S6
TRANSMIT KEY Kij TO HEALTH SERVICE
S7

FIG. 4

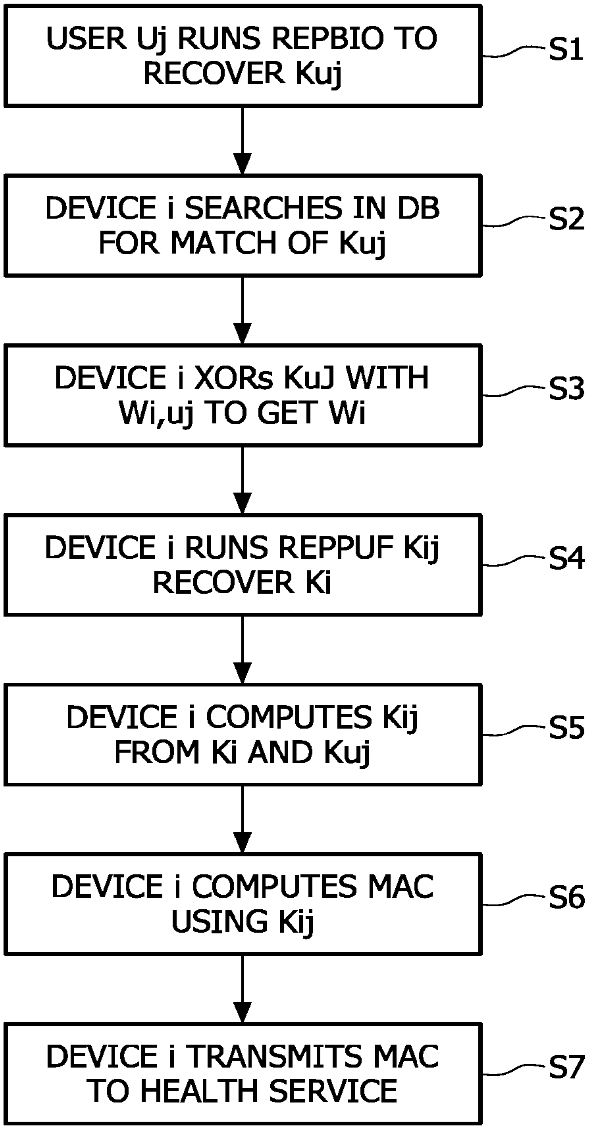

USER Uj RUNS REPBIO TO RECOVER Kuj
S1
DEVICE i SEARCHES IN DB FOR MATCH OF Kuj
S2
DEVICE i XORs KuJ WITH Wi,uj TO GET Wi
S3
DEVICE i RUNS REPPUF Kij RECOVER Ki
S4
DEVICE i COMPUTES Kij FROM Ki AND Kuj
S5
DEVICE i COMPUTES MAC USING Kij
S6
DEVICE i TRANSMITS MAC TO HEALTH SERVICE
S7

FIG. 5

6/7

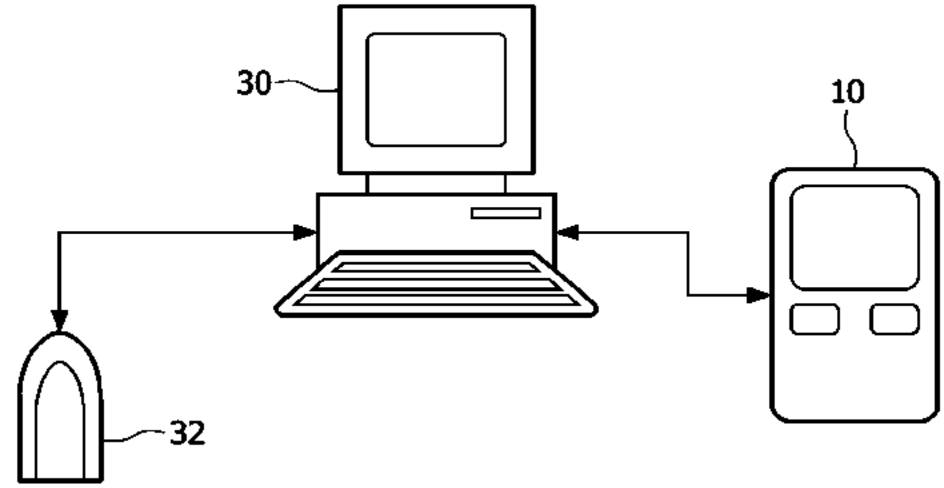


FIG. 6a

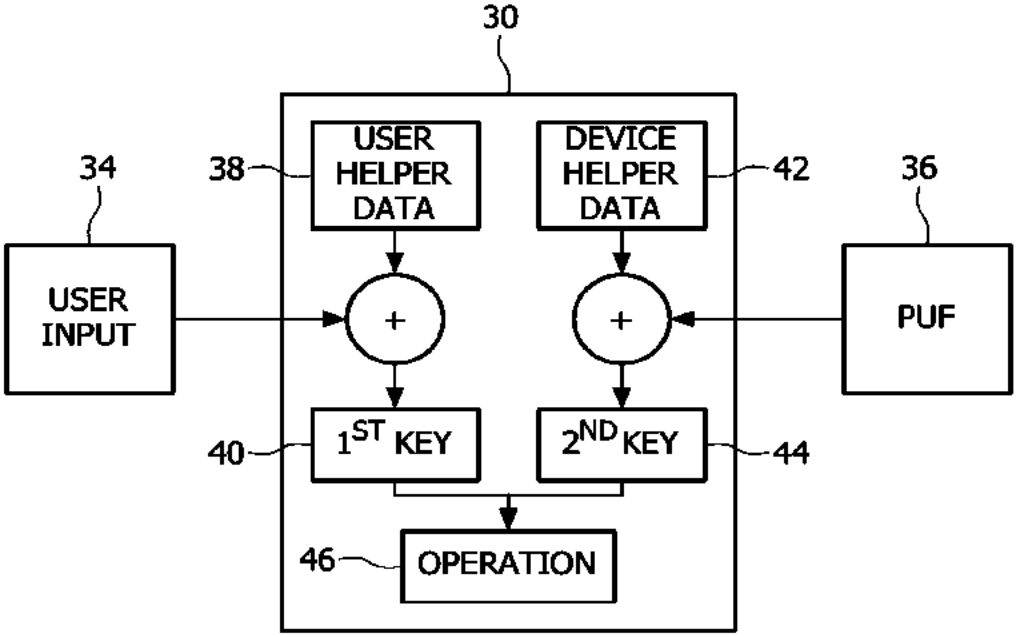


FIG. 6b

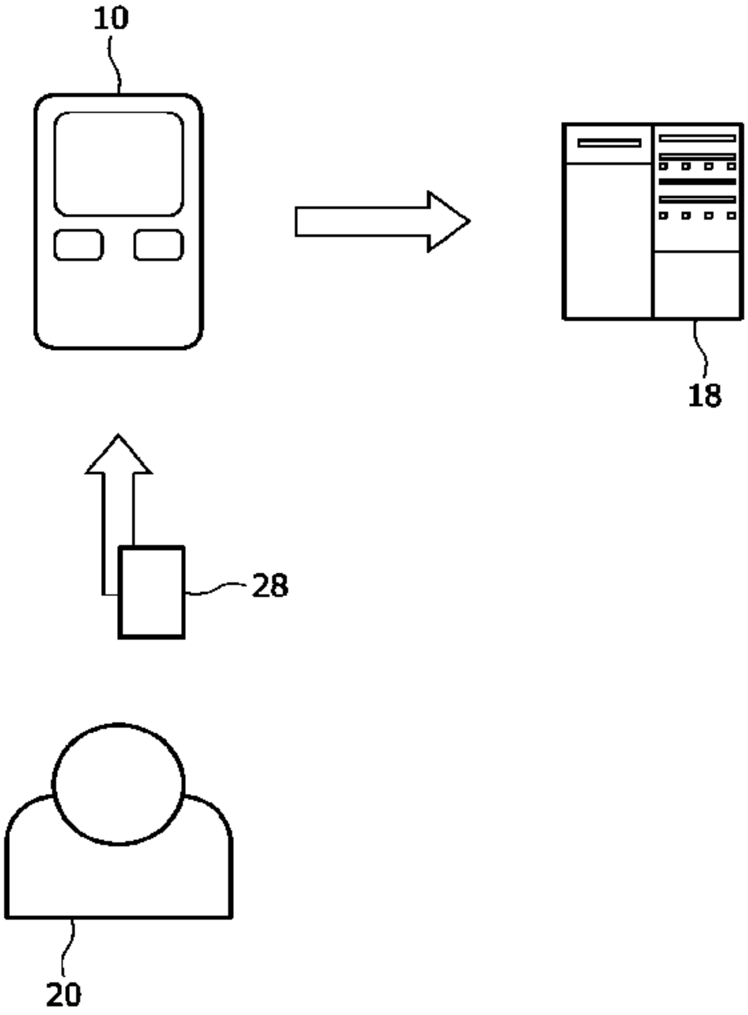


FIG. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2009/054120

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2007/044139 A1 (TUYLS PIM T [NL] ET AL) 22 February 2007 (2007-02-22) paragraph [0026] - paragraph [0052]; figures 1, 2A, 2B -----	1-18
Y	WO 2007/063475 A2 (KONINKL PHILIPS ELECTRONICS NV [NL]; SKORIC BORIS [NL]; BRUEKERS ALPHO) 7 June 2007 (2007-06-07) page 3, line 1 - page 3, line 15 -----	1-18
A	WO 2006/067739 A2 (KONINKL PHILIPS ELECTRONICS NV [NL]; TUYLS PIM T [BE]; GOSELING JASPER) 29 June 2006 (2006-06-29) abstract -----	1-18

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 12 February 2010	Date of mailing of the international search report 19/02/2010
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Jascau, Adrian

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/IB2009/054120

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007044139 A1	22-02-2007	CN 1792060 A	21-06-2006
		WO 2004104899 A2	02-12-2004
		JP 2007500910 T	18-01-2007
		KR 20060023533 A	14-03-2006
WO 2007063475 A2	07-06-2007	AT 426969 T	15-04-2009
		CN 101317361 A	03-12-2008
		EP 1958374 A2	20-08-2008
		JP 2009517911 T	30-04-2009
		US 2008260152 A1	23-10-2008
WO 2006067739 A2	29-06-2006	JP 2008526078 T	17-07-2008
		KR 20070095908 A	01-10-2007

Electronic Acknowledgement Receipt

EFS ID:	25319433
Application Number:	15075066
International Application Number:	
Confirmation Number:	1166
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul Timothy Miller
Customer Number:	27683
Filer:	David B. Bowls/Allison Hung
Filer Authorized By:	David B. Bowls
Attorney Docket Number:	47583.5US02
Receipt Date:	28-MAR-2016
Filing Date:	
Time Stamp:	14:52:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		5US02IDS.pdf	734918 29b07cfd2fbe82091f828addd3b2f83562cd338c	yes	4

	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Transmittal Letter		1	3	
	Information Disclosure Statement (IDS) Form (SB08)		4	4	
Warnings:					
Information:					
2	Foreign Reference	5US02WO2013138714A1.PDF	1886686 8ad4469839f025e60d414c653ef8eedfb35b15e4	no	42
Warnings:					
Information:					
3	Foreign Reference	5US02WO2013154936A1.PDF	3565462 3e0b81f32945b732eaa72acdfabc9611f1795080	no	89
Warnings:					
Information:					
4	Foreign Reference	5US02WO2010035202A1.PDF	1746507 a819ec318639035a0b0f192e6d4adc9dffc80a84	no	30
Warnings:					
Information:					
		Total Files Size (in bytes):	7933573		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventors:	Paul Timothy Miller and George Allen Tuvell		
Applicant:	mSignia, Inc.		
Title:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE		
Application No.:	15/075,066	Filing Date:	March 18, 2016
Examiner:	Not Yet Assigned	Group Art Unit:	2431
Docket No.:	47583.5US02	Confirmation No.:	1166

Costa Mesa, California
March 28, 2016

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT UNDER 37 C.F.R. §§1.56, 1.97, and 1.98

Sir:

Pursuant to 37 C.F.R. §§1.56, 1.97, and 1.98, the documents listed on the accompanying Substitute PTO Form 1449 are called to the attention of the Examiner for the above patent application.

Citation of these documents shall not be construed as:

(1) an admission that the documents are necessarily prior art with respect to the instant invention;

(2) a representation that a search has been made, other than as described above; or

(3) an admission that the information cited herein is, or is considered to be material to patentability.

Enclosed with this statement are the following:

☒ Substitute PTO Form 1449. The Examiner is requested to initial the form and return it to the undersigned in accordance with M.P.E.P. §609.

☒ A copy of each cited document as required by 37 C.F.R. §1.98 (*except where otherwise indicated*).

Complete copies are not submitted of U.S. patents and U.S. patent application publications per 37 C.F.R. §1.98(a)(2)(ii), and copies are not submitted of documents already cited or submitted in a parent application from which benefit under 35 U.S.C. §120 is claimed per 37 C.F.R. §1.98(d).

This statement should be considered because:

☒ This statement qualifies under 37 C.F.R. §1.97, subsection (b) because:

□ It is being filed within 3 months of the application filing date of a national application other than a continued prosecution application under §1.53(d);

-- OR --

□ It is being filed within 3 months of entry of the national stage as set forth in §1.491 in an international application;

-- OR --

☒ It is being filed before the mailing date of a first Office action *on the merits*;

-- OR --

□ It is being filed before the mailing date of a first Office action *after the filing of an RCE under §1.114.*

whichever occurs last.

□ Although it may not qualify under subsection (b), this statement qualifies under 37 C.F.R. §1.97, subsection (c) because:

(1) It is being filed before the mailing date of a FINAL Office Action and before a Notice of Allowance or another action closing prosecution (whichever occurs first);

-- AND *(check at least one of the following)* --

□ (1) It is accompanied by the $180 fee set forth in 37 C.F.R. §1.17(p);

-- OR --

□ (2) Pursuant to 37 C.F.R. §1.97(e), each item of information contained in the information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement.

--OR--

□ (3) Pursuant to 37 C.F.R. §1.97(e), no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than

three months prior to the filing of the information disclosure statement.

□ Although it may not qualify under subsections (b) or (c), this statement qualifies under 37 C.F.R. §1.97, subsection (d) because:

(1) It is being filed on or before payment of the Issue Fee:

-- AND --

□ (1) It is accompanied by the $180 fee set forth in 37 C.F.R. §1.17(p);

-- AND *(check at least one of the following)* --

□ (2) Pursuant to 37 C.F.R. §1.97(e), each item of information contained in the information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement.

--OR--

□ (3) Pursuant to 37 C.F.R. §1.97(e), no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

☒ ***Fee Authorization.*** The Commissioner is hereby authorized to charge any additional fee(s), charge any underpayment of fee(s), or credit any overpayment associated with this communication to Deposit Account No. 08-1394.

Certificate of Transmission

I hereby certify that this correspondence is sent electronically via EFS Web to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below.

Allison Hung **March 28, 2016**

Respectfully submitted,

David Bowls
Patent Agent
Reg. No. 39,915

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number
15/075,066

APPLICATION AS FILED - PART I

	(Column 1)	(Column 2)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE($)	FEE($)		RATE($)	FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	21 minus 20 =	* 1	x 40 =	40	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
			TOTAL	770		TOTAL	

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
15/075,066	03/18/2016	2431	770	47583.5US02	21	3

CONFIRMATION NO. 1166

FILING RECEIPT

27683
HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

Date Mailed: 04/06/2016

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Paul Timothy Miller, Irvine, CA;
George Allen Tuvell, Thompson's Station, TN;

Applicant(s)

mSignia, Inc., Irvine, CA;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 14/458,123 08/12/2014 PAT 9294448
which is a CON of 13/366,197 02/03/2012 PAT 8817984
which claims benefit of 61/462,474 02/03/2011

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted:

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/075,066**

Projected Publication Date: To Be Determined - pending completion of Security Review

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****
Title

CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE

Preliminary Class

380

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/075,066	03/18/2016	Paul Timothy Miller	47583.5US02

CONFIRMATION NO. 1166

NEW OR REVISED PPD NOTICE

OC000000083356782

27683
HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

NOTICE OF NEW OR REVISED PROJECTED PUBLICATION DATE

The above-identified application has a new or revised projected publication date. The current projected publication date for this application is 09/08/2016. If this is a new projected publication date (there was no previous projected publication date), the application has been cleared by Licensing & Review or a secrecy order has been rescinded and the application is now in the publication queue.

If this is a revised projected publication date (one that is different from a previously communicated projected publication date), the publication date has been revised due to processing delays in the USPTO or the abandonment and subsequent revival of an application. The application is anticipated to be published on a date that is more than six weeks different from the originally-projected publication date.

More detailed publication information is available through the private side of Patent Application Information Retrieval (PAIR) System. The direct link to access PAIR is currently http://pair.uspto.gov. Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Questions relating to this Notice should be directed to the Office of Data Management, Application Assistance Unit at (571) 272-4000, or (571) 272-4200, or 1-888-786-0101.

PART 1 - ATTORNEY/APPLICANT COPY

U. S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(use as many sheets as necessary)*				*Complete if Known*	
				Application Number	15/075,066
				Filing Date	March 18, 2016
				Applicant(s)	mSignia, Inc.
				Art Unit	2497
				Examiner Name	Ho, Dao Q.
SHEET	1	OF	1	Attorney Docket Number	47583.5US02

U. S. PATENT DOCUMENTS

Examiner's Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
	1.	8,213,907	07-03-2012	Etchegoyen, Craig Stephen
	2.	8,335,925	12-18-2012	Taugbol, Petter
	3.	2007/0240217	10-11-2007	Tuvell et al.
	4.	2010/0332400	12-30-2010	Etchegoyen, Craig Stephen
	5.	2011/0093503	04-21-2011	Etchegoyen, Craig S.
	6.	2014/0229386	08-14-2014	Tervo et al.

FOREIGN PATENT DOCUMENTS

Examiner's Initials	Cite No.	Foreign Patent Document (Country Code – Number – Kind)	Publication Date MM-DD-YYYY	Patentee or Applicant of Cited Document	Translation Y/N

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

Electronic Acknowledgement Receipt

EFS ID:	26105165
Application Number:	15075066
International Application Number:	
Confirmation Number:	1166
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul Timothy Miller
Customer Number:	27683
Filer:	David B. Bowls/Allison Hung
Filer Authorized By:	David B. Bowls
Attorney Docket Number:	47583.5US02
Receipt Date:	17-JUN-2016
Filing Date:	18-MAR-2016
Time Stamp:	18:42:58
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		5US02IDSTransmittalandPTO1449.pdf	660391 267607856ce7106523bd640e40b44e98690156e3	yes	4

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	3
	Information Disclosure Statement (IDS) Form (SB08)	4	4
Warnings:			
Information:			
	Total Files Size (in bytes):	660391	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

In The United States Patent And Trademark Office

Inventors:	Paul Timothy Miller and George Allen Tuvell		
Applicant:	mSignia, Inc.		
Title:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE		
Application No.:	15/075,066	Filing Date:	March 18, 2016
Examiner:	Ho, Dao Q.	Group Art Unit:	2497
Docket No.:	47583.5US02	Confirmation No.:	1166

Costa Mesa, California
June 17, 2016

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT UNDER 37 C.F.R. §§1.56, 1.97, and 1.98

Sir:

Pursuant to 37 C.F.R. §§1.56, 1.97, and 1.98, the documents listed on the accompanying Substitute PTO Form 1449 are called to the attention of the Examiner for the above patent application.

Citation of these documents shall not be construed as:

(1) an admission that the documents are necessarily prior art with respect to the instant invention;

(2) a representation that a search has been made, other than as described above; or

(3) an admission that the information cited herein is, or is considered to be material to patentability.

Enclosed with this statement are the following:

☒ Substitute PTO Form 1449. The Examiner is requested to initial the form and return it to the undersigned in accordance with M.P.E.P. §609.

☒ A copy of each cited document as required by 37 C.F.R. §1.98 (*except where otherwise indicated*).

Complete copies are not submitted of U.S. patents and U.S. patent application publications per 37 C.F.R. §1.98(a)(2)(ii), and copies are not submitted of documents already cited or submitted in a parent application from which benefit under 35 U.S.C. §120 is claimed per 37 C.F.R. §1.98(d).

This statement should be considered because:

☒ This statement qualifies under 37 C.F.R. §1.97, subsection (b) because:

☒ It is being filed within 3 months of the application filing date of a national application other than a continued prosecution application under §1.53(d);

-- OR --

☐ It is being filed within 3 months of entry of the national stage as set forth in §1.491 in an international application;

-- OR --

☐ It is being filed before the mailing date of a first Office action *on the merits*;

-- OR --

☐ It is being filed before the mailing date of a first Office action *after the filing of an RCE under §1.114.*

whichever occurs last.

☐ Although it may not qualify under subsection (b), this statement qualifies under 37 C.F.R. §1.97, subsection (c) because:

(1) It is being filed before the mailing date of a FINAL Office Action and before a Notice of Allowance or another action closing prosecution (whichever occurs first);

-- AND *(check at least one of the following)* --

☐ (1) It is accompanied by the $180 fee set forth in 37 C.F.R. §1.17(p);

-- OR --

☐ (2) Pursuant to 37 C.F.R. §1.97(e), each item of information contained in the information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement.

--OR--

☐ (3) Pursuant to 37 C.F.R. §1.97(e), no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than

three months prior to the filing of the information disclosure statement.

□ Although it may not qualify under subsections (b) or (c), this statement qualifies under 37 C.F.R. §1.97, subsection (d) because:

(1) It is being filed on or before payment of the Issue Fee:

-- AND --

□ (1) It is accompanied by the $180 fee set forth in 37 C.F.R. §1.17(p);

-- AND *(check at least one of the following)* --

□ (2) Pursuant to 37 C.F.R. §1.97(e), each item of information contained in the information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement.

--OR--

□ (3) Pursuant to 37 C.F.R. §1.97(e), no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

☒ ***Fee Authorization.*** The Commissioner is hereby authorized to charge any additional fee(s), charge any underpayment of fee(s), or credit any overpayment associated with this communication to Deposit Account No. 08-1394.

Certificate of Transmission

I hereby certify that this correspondence is sent electronically via EFS Web to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below.

June 17, 2016

Allison Hung

Respectfully submitted,

David Bowls
Patent Agent
Reg. No. 39,915

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas TX 75219

Doc Code: TRACK1.GRANT

Decision Granting Request for Prioritized Examination (Track I or After RCE)	Application No.: 15/075,066

1. THE REQUEST FILED March 18, 2016 IS **GRANTED**.

The above-identified application has met the requirements for prioritized examination
A. ☒ for an original nonprovisional application (Track I).
B. □ for an application undergoing continued examination (RCE).

2. **The above-identified application will undergo prioritized examination.** The application will be accorded special status throughout its entire course of prosecution until one of the following occurs:

A. filing a **petition for extension of time** to extend the time period for filing a reply;

B. filing an **amendment to amend the application to contain more than four independent claims, more than thirty total claims**, or a multiple dependent claim;

C. filing a **request for continued examination**;

D. filing a notice of appeal;

E. filing a request for suspension of action;

F. mailing of a notice of allowance;

G. mailing of a final Office action;

H. completion of examination as defined in 37 CFR 41.102; or

I. abandonment of the application.

Telephone inquiries with regard to this decision should be directed to Rebecca Eisenberg at (571) 270-5879. In her absence, calls may be directed to Vincent Trans at (571) 272-3613.

/Jose' G. Dees/ Petitions Examiner, Office of Petitions

[*Signature*] (Title)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Paul T. Miller, George A. Tuvell		
Applicant:	mSignia, Inc.		
Title:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE		
Serial No.:	15/075,066	Filing Date:	March 18, 2016
Examiner:	Dao Q. Ho	Group Art Unit:	2431
Docket No.:	47583.5US02	Confirmation No.:	1166

Costa Mesa, California
June 28, 2016

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRELIMINARY AMENDMENT

Prior to examination of the above-referenced patent application on the merits, Applicant requests entry of the following amendment.

Applicant includes the fee under 37 C.F.R. 1.16(i) for 2 additional claims in excess of 20 over the total number previously filed. No additional independent claims are being filed. The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 08-1394.

IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1-21. (Canceled)

22. (New) An identity recognition system comprising

a non-transitory memory storing information associated with one or more identities, wherein the information stored for an identity includes one or more previously-collected data values associated with such identity;

one or more hardware processors in communication with the memory and configured to execute instructions to cause the identity recognition system to recognize that the presentation of an identity by a computer is authentic, by performing operations comprising:

generating a challenge to the computer, wherein the challenge prompts the computer to provide a response based on one or more data values from the computer that correspond to one or more of the previously-collected data values associated with the identity to be recognized;

receiving, from the computer, the response to the challenge;

determining whether the response is allowable, wherein such determining comprises evaluating whether the response is based on an acceptable change to a previously-collected data value associated with the identity to be recognized; and

recognizing that the presentation of the identity by the computer is authentic, according to whether the computer has provided an allowable response to the challenge.

23. (New) The identity recognition system of claim 22, wherein the identity is associated with the computer and is a user identity or a device identity.

24. (New) The identity recognition system of claim 22, wherein the challenge prompts a response based on one or more user minutia data values.

25. (New) The identity recognition system of claim 24, wherein the operation of determining whether the response is allowable includes evaluating whether at least a portion

of the response is based on one or more acceptable changes to a previously-collected user minutia data valuc.

26. (New) The identity recognition system of claim 25, wherein the previously-collected user minutia data values used to determine whether the response is allowable comprise user secrets, user customization, entertainment data, bio-metric data, or contacts.

27. (New) The identity recognition system of claim 25, wherein the previously-collected user minutia data values used to determine whether the response is allowable comprise calling app data, geo-location data, frequently called phone numbers, email, or network connection data.

28. (New) The identity recognition system of claim 22, wherein a previously-collected data value is used to generate at least a portion of the challenge, and wherein the determining operation further comprises evaluating whether a data value on which the response is based is the same as the previously-collected data value.

29. (New) The identity recognition system of claim 22, wherein a change to the previously-collected data value is acceptable if a data value upon which the response is based is within a set of acceptable values for the previously-collected data value that are determined independently from receiving the response from the computer.

30. (New) The identity recognition system of claim 29, wherein the set of acceptable values includes one or more values based on predictable changes to the previously-collected data value.

31. (New) The identity recognition system of claim 29, wherein the set of acceptable values includes one or more values based on predicted changes to the previously-collected data value, based on industry updates to hardware, firmware, or software elements.

32. (New) The identity recognition system of claim 29, wherein the set of acceptable values includes one or more values based on a predictable user customization of the computer.

33. (New) The identity recognition system of claim 29, wherein the set of acceptable values includes one or more values based on a predictable usage of the computer by a user.

34. (New) The identity recognition system of claim 22, further comprising the operations of:

in response to evaluating that the response is based on an acceptable change to a previously-collected data value associated with the identity to be recognized, updating the memory to reflect the changed data value.

35. (New) The identity recognition system of claim 22, wherein the operation of determining whether the response is allowable further comprises comparing the received response to a member of a set of two or more allowable responses.

36. (New) The identity recognition system of claim 35, wherein the set of allowable responses is computed before the determining operation is performed.

37. (New) The identity recognition system of claim 35, wherein the set of allowable responses is computed concurrently with the determining operation being performed.

38. (New) The identity recognition system of claim 22, wherein the determining operation further comprises generating a rating of the allowability of the response, based on the previously collected data value and one or more changes to the previously-collected data values.

39. (New) The identity recognition system of claim 38, wherein the rating of the allowability of the response is based on a comparison of a data value upon which the response is based to one or more predictable changes to the previously-collected data values associated with the identity to be recognized.

40. (New) The identity recognition system of claim 39, wherein the rating of the allowability of the response is varied based on whether the response is based at least in part on one or more predicted changes to the previously-collected data values.

41. (New) The identity recognition system of claim 22, wherein the operation of recognizing that the presentation of the identity by the computer is authentic provides a basis for one or more of: authenticating a device, authenticating a user, validating a software program or an application, providing data protection of data transmitted to or from a device, or generating a digital signature of a message digest.

42. (New) The identity recognition system of claim 22, wherein the response does not contain any data values reflecting personally identifiable information.

43. (New) An identity recognition system comprising

a non-transitory memory storing information associated with one or more identities, wherein the information stored for an identity includes one or more verified data values associated with such identity;

one or more hardware processors in communication with the memory and configured to execute instructions to cause the identity recognition system to recognize that the presentation of an identity by a computer is authentic, by performing operations comprising

receiving, from the computer, one or more communications comprising an identity claim, wherein at least a portion of the identity claim is formed based on one or more data values;

determining whether the one or more communications received from the computer are sufficient to recognize that the identity claim is authentic, wherein such determining comprises evaluating whether a data value used to form the identity claim is based on an acceptable change to a previously-verified data value associated with the identity to be recognized.

44. (New) An identity recognition system comprising

a non-transitory memory storing information associated with one or more identities, wherein the information stored for an identity includes one or more previously-collected data values associated with such identity;

one or more hardware processors in communication with the memory and configured to execute instructions to cause the identity recognition system to recognize that the presentation of an identity at a computer is authentic, by performing operations comprising

receiving, from the computer, a communication based on one or more data values from the computer;

determining whether the communication received from the computer is sufficient to recognize that the use of an identity is authentic, wherein such determining comprises evaluating whether a data value upon which the communication is based reflects an acceptable change to a previously-collected data value associated with the identity to be recognized.

REMARKS

Claims 1-21 were pending in the present application. Claims 1-21 are caneeled without prejudice to their further prosecution. New claims 22 -44 are added. Accordingly, upon entry of this amendment claims 22-44 will be pending.

Claim Amendments

Support for the claims may be found in the specification and figures as filed, as well as as in the claims as previously filed. Thus, Applicant respectfully submits that no new matter is added.

Applicant believes that claims 22-44 are in condition for allowance; accordingly, Applicant respectfully requests consideration and allowance of claims 22-44.

CONCLUSION

In view of the foregoing, Applicant believes pending claims 22-44 are allowable, and a Notice of Allowance is respectfully requested.

If there are any questions regarding any aspect of the application, please call the undersigned at (949) 202-3011.

Certificate of Transmission

I hereby certify that this correspondence is being electronically transmitted via EFS Web to the Commissioner for Patents, on the date stated below.

June 28, 2016
Monique Le Sadahiro

Respectfully submitted,

David Bowls
Patent Agent
Reg. No. 39,915

Electronic Patent Application Fee Transmittal

Application Number:	15075066
Filing Date:	18-Mar-2016
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul Timothy Miller
Filer:	David B. Bowls/Monique Le Sadahiro
Attorney Docket Number:	47583.5US02

Filed as Large Entity

Filing Fees for **Utility under 35 USC 111(a)**

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Claims in Excess of 20	1202	2	80	160
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**160**

Electronic Acknowledgement Receipt

EFS ID:	26203408
Application Number:	15075066
International Application Number:	
Confirmation Number:	1166
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul Timothy Miller
Customer Number:	27683
Filer:	David B. Bowls/Monique Le Sadahiro
Filer Authorized By:	David B. Bowls
Attorney Docket Number:	47583.5US02
Receipt Date:	28-JUN-2016
Filing Date:	18-MAR-2016
Time Stamp:	20:14:18
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$160
RAM confirmation Number	6588
Deposit Account	081394
Authorized User	BOWLS, DAVID B.

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 CFR 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 CFR 1.19 (Document supply fees)

Charge any Additional Fees required under 37 CFR 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		20160628171153278.pdf	677308 0f2d8a8cbb5bbb29c97edc5a085997a384c0e97b	yes	7

Multipart Description/PDF files in .zip description

Document Description	Start	End
Preliminary Amendment	1	1
Amendment Copy Claims/Response to Suggested Claims	2	6
Applicant Arguments/Remarks Made in an Amendment	7	7

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
2	Fee Worksheet (SB06)	fee-info.pdf	30822 3dc122f7362a238ff4cba98f72eacdff1fd45dde	no	2

Warnings:

Information:

Total Files Size (in bytes):	708130

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 15/075,066	Filing Date 03/18/2016	□ To be Mailed

ENTITY: ☒ LARGE □ SMALL □ MICRO

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)		
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)
□ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
□ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
□ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
□APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
□ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)		
AMENDMENT	**06/28/2016**	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 23	Minus	** 21	= 2	x $80 =	160
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	x $420 =	0
	□ Application Size Fee (37 CFR 1.16(s))						
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	**160**

		(Column 1)		(Column 2)	(Column 3)		
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	□ Application Size Fee (37 CFR 1.16(s))						
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
PARTHENIA D. MERRILL

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/075,066	03/18/2016	Paul Timothy Miller	47583.5US02	1166

27683 7590 07/14/2016
HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

EXAMINER	
HO, DAO Q	
ART UNIT	PAPER NUMBER
2497	
NOTIFICATION DATE	DELIVERY MODE
07/14/2016	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ipdocketing@haynesboone.com

Office Action Summary	**Application No.** 15/075,066	**Applicant(s)** MILLER ET AL.	
	Examiner DAO HO	**Art Unit** 2497	**AIA (First Inventor to File) Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06/28/2016*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *22-44* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *22-44* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *03/18/2016* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date *03/28/2016, 06/17/2016*.

3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

The present application is being examined under the pre-AIA first to invent provisions.

This is a reply to the application filed on 06/28/2016, in which, claim(s) 1-44 are pending.

Claim(s) 22, 43 and 44 is/are independent.

Claim(s) 1-21 is/are cancelled.

Claim(s) 22-44 is/are newly added.

When making claim amendments, the applicant is encouraged to consider the references in their entireties, including those portions that have not been cited by the examiner and their equivalents as they may most broadly and appropriately apply to any particular anticipated claim amendments.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 03/28/2016 and 06/17/2016, has been reviewed. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Drawings

The drawings filed on 03/18/2016 is/are accepted by The Examiner.

Claim Objections

Claims 22, 43 and 44 objected to because of the following informalities:

Claims 22, 43 and 44 recited in the preamble a system comprising…; however, a colon (:) is missing after the word comprising.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim(s) 22-44 is/are rejected under 35 U.S.C. 101 because the claimed is being directed to non-statutory subject matter.

Regarding **claim(s) 22, 43 and 44**, the claimed invention is not directed to patent eligible subject matter. Based upon an analysis with respect to the claim as a whole, claim(s) 22, 43 and 44 do not recite something significantly different than a judicial exception. The rationale for this determination is explained below: *the claims recited a mere challenge and response method of authentication. The function can be done by a person and does not require significantly more, thus, are considered as abstract idea.* In additional, *the claim does not contain an 'inventive concept' to 'transform' the claimed abstract idea into patent-eligible subject matter because the claim simply instructs to implement the abstract idea with routine, conventional activity.* As discussed above, the claim is directed to an abstract idea and does not do significantly more than simply described that abstract method. Therefore, the claim is not directed to patent eligible matter. See *Alice Corporation v. CLS Bank International,* (S.Ct.2014) and *Ultramerical, Inc. v. Hulu, LLC.* (Fed. Cir. 2014).

Dependent **claim(s) 23-42** are also rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter for the same reason addressed above.

Claim Rejections - 35 USC § 103

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under pre-AIA 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 22-44 is/are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Buffam (Pat. No.: US 6,185,316 B1 – IDS filed on 03/28/2016) in view of Kang (Pub. No.: US 2011/0007177 A1).

Regarding **claims 22, 43 and 44**, Buffam discloses an identity recognition system comprising:

a non-transitory memory storing information associated with one or more identities, wherein the information stored for an identity includes one or more previously-collected data values associated with such identity (a master template database that that stored all the minutia created [Buffam; Fig. 5 – element 370]);

one or more hardware processors in communication with the memory and configured to execute instructions to cause the identity recognition system to recognize that the presentation of an identity by a computer is authentic, by performing operations comprising (the system used for determine the validity of the user [Buffam; Fig. 8 – elements 650]):

generating a challenge to the computer, wherein the challenge prompts the computer to provide a response based on one or more data values from the computer that correspond to one or more of the previously-collected data values associated with the identity to be recognized (challenging the user of to compare with the stored info for authenticating the user [Buffam; 19:30-61]);

receiving, from the computer, the response to the challenge (getting the response from the user [Buffam; 21:1-15]);

determining whether the response is allowable, wherein such determining comprises evaluating whether the response is based on an acceptable change to a previously-collected data value associated with the identity to be recognized (the challenge response is accepted [Buffam; 21:1-15]);and recognizing that the presentation of the identity by the computer is authentic, according to whether the computer has provided an allowable response to the challenge (allowing access once authenticated [Buffam; 21:1-15]).

Buffam use the user's fingerprint as a method for authentication and not the actual devices information; however, Kang teaches this feature.

In particular, Kang teaches using various elements as minutiae elements, including location and objects in natures as well as colors and other unique features [Kang; ¶55, 68]. It would have been obvious to one with ordinary skill in the art at time of invention to modify Buffam in view of Kang elements of minutiae with the motivation to create a varieties of elements in authentication for more secure protection.

Regarding **claim 23**, Buffam discloses the identity recognition system of claim 22, wherein the identity is associated with the computer and is a user identity or a device identity (Kang teaches using various elements as minutiae elements, including location and objects in natures as well as colors and other unique features [Kang; ¶55, 68]). It would have been obvious to one with ordinary skill in the art at time of invention to modify Buffam in view of Kang elements of minutiae with the motivation to create a varieties of elements in authentication for more secure protection.

Regarding **claim 24**, Buffam discloses the identity recognition system of claim 22, wherein the challenge prompts a response based on one or more user minutia data values (response is based on the users minutia [Buffam; 21:1-15]).

Regarding **claim 25**, Buffam discloses the identity recognition system of claim 24, wherein the operation of determining whether the response is allowable includes evaluating whether at least a portion of the response is based on one or more acceptable changes to a previously-collected user minutia data value (response is based on the users minutia [Buffam; 21:1-15]).

Regarding **claim 26**, Buffam discloses the identity recognition system of claim 25, wherein the previously-collected user minutia data values used to determine whether the response is allowable comprise user secrets, user customization, entertainment data, bio-metric data, or contacts (Kang teaches using various elements as minutiae elements, including location and objects in natures as well as colors and other unique features [Kang; ¶55, 68]). It would have been obvious to one with ordinary skill in the art at time of invention to modify Buffam in view of Kang elements of minutiae with the motivation to create a varieties of elements in authentication for more secure protection.

Regarding **claim 27**, Buffam discloses the identity recognition system of claim 25, wherein the previously-collected user minutia data values used to determine whether the response is allowable comprise calling app data, geo-location data, frequently called phone numbers, email, or network connection data (Kang teaches using various elements as minutiae elements, including location and objects in natures as well as colors and other unique features [Kang; ¶55, 68]). It would have been obvious to one with ordinary skill in the art at time of invention to modify Buffam in view of Kang elements of minutiae with the motivation to create a varieties of elements in authentication for more secure protection.

Regarding **claim 28**, Buffam discloses the identity recognition system of claim 22, wherein a previously-collected data value is used to generate at least a portion of the challenge, and wherein the determining operation further comprises evaluating whether a data value on which the response is based is the same as the previously-collected data value (authentication is based on current challenge response compared to stored templates [Buffam; ¶16:6-43; 21:1-15]).

Regarding **claim 29**, Buffam discloses the identity recognition system of claim 22, wherein a change to the previously-collected data value is acceptable if a data value upon which the response is based is within a set of acceptable values for the previously-collected data value that are determined independently from receiving the response from the computer (authentication is based on current challenge response compared to stored templates [Buffam; ¶16:6-43; 21:1-15]).

Regarding **claim 30**, Buffam discloses the identity recognition system of claim 29, wherein the set of acceptable values includes one or more values based on predictable changes to the previously-collected data value (authentication is based on current challenge response compared to stored templates [Buffam; ¶16:6-43; 21:1-15]).

Regarding **claim 31**, Buffam discloses the identity recognition system of claim 29, wherein the set of acceptable values includes one or more values based on predicted changes to the previously-collected data value, based on industry updates to hardware, firmware, or software elements (Kang teaches using various elements as minutiae elements, including location and objects in natures as well as colors and other unique features [Kang; ¶55, 68]). It would have been obvious to one with ordinary skill in the art at time of invention to modify Buffam in view of Kang elements of minutiae with the motivation to create a varieties of elements in authentication for more secure protection.

Regarding **claim 32**, Buffam discloses the identity recognition system of claim 29, wherein the set of acceptable values includes one or more values based on a predictable user customization of the computer (authentication is based on current challenge response compared to stored templates [Buffam; ¶16:6-43; 21:1-15]).

Regarding **claim 33**, Buffam discloses the identity recognition system of claim 29, wherein the set of acceptable values includes one or more values based on a predictable usage of the computer by a user (authentication is based on current challenge response compared to stored templates [Buffam; ¶16:6-43; 21:1-15]).

Regarding **claim 34**, Buffam discloses the identity recognition system of claim 22, further comprising the operations of:

in response to evaluating that the response is based on an acceptable change to a previously-collected data value associated with the identity to be recognized, updating the memory to reflect the changed data value (authentication is based on current challenge response compared to stored templates [Buffam; ¶16:6-43; 21:1-15]).

Regarding **claim 35**, Buffam discloses the identity recognition system of claim 22, wherein the operation of determining whether the response is allowable further comprises comparing the received response to a member of a set of two or more allowable responses (authentication is based on current challenge response compared to stored templates [Buffam; ¶16:6-43; 21:1-15]).

Regarding **claim 36**, Buffam discloses the identity recognition system of claim 35, wherein the set of allowable responses is computed before the determining operation is performed (authentication is based on current challenge response compared to stored templates [Buffam; ¶16:6-43; 21:1-15]).

Regarding **claim 37**, Buffam discloses the identity recognition system of claim 35, wherein the set of allowable responses is computed concurrently with the determining operation being performed (authentication is based on current challenge response compared to stored templates [Buffam; ¶16:6-43; 21:1-15]).

Regarding **claim 38**, Buffam discloses the identity recognition system of claim 22, wherein the determining operation further comprises generating a rating of the allowability of the response, based on the previously collected data value and one or more changes to the previously-collected data values (authentication is based on current challenge response compared to stored templates [Buffam; ¶16:6-43; 21:1-15]).

Regarding **claim 39**, Buffam discloses the identity recognition system of claim 38, wherein the rating of the allowability of the response is based on a comparison of a data value upon which the response is based to one or more predictable changes to the previously-collected data values associated with the identity to be recognized (authentication is based on current challenge response compared to stored templates [Buffam; ¶16:6-43; 21:1-15]).

Regarding **claim 40**, Buffam discloses the identity recognition system of claim 39, wherein the rating of the allowability of the response is varied based on whether the response is based at least in part on one or more predicted changes to the previously-collected data values (authentication is based on current challenge response compared to stored templates [Buffam; ¶16:6-43; 21:1-15; Fig. 8]).

Regarding **claim 41**, Buffam discloses the identity recognition system of claim 22, wherein the operation of recognizing that the presentation of the identity by the computer is authentic provides a basis for one or more of: authenticating a device, authenticating a user, validating a software program or an application, providing data protection of data transmitted to or from a device, or generating a digital signature of a message digest (authentication is based on current challenge response compared to stored templates [Buffam; ¶16:6-43; 21:1-15]).

Regarding **claim 42**, Buffam discloses the identity recognition system of claim 22, wherein the response does not contain any data values reflecting personally identifiable information (authentication is based on current challenge response compared to stored templates [Buffam; ¶16:6-43; 21:1-15]).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAO HO whose telephone number is (571)270-5998. The examiner can normally be reached on Monday-Thursday (8:00am - 6:00pm EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, HADI ARMOUCHE can be reached on (571) 270-3618. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/DAO HO/
Primary Examiner, Art Unit 2497

Notice of References Cited	Application/Control No. 15/075,066	Applicant(s)/Patent Under Reexamination MILLER ET AL.	
	Examiner DAO HO	Art Unit 2497	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-6,041,133 A	03-2000	Califano; Andrea	G06K9/00067	382/124
*	B	US-6,185,316 B1	02-2001	Buffam; William J.	G06F21/32	382/100
*	C	US-2006/0031676 A1	02-2006	Vantalon; Luc	G06Q10/02	713/176
*	D	US-2006/0104484 A1	05-2006	Bolle; Rudolf Maarten	G06K9/00885	382/115
*	E	US-2007/0174206 A1	07-2007	Colella; Brian	G06Q20/382	705/64
*	F	US-7,269,160 B1	09-2007	Friedman; David	G06Q30/0601	370/352
*	G	US-2008/0175449 A1	07-2008	Fang; Sung-Jen	G06F21/32	382/124
*	H	US-2008/0235515 A1	09-2008	Yedidia; Jonathan S.	G06K9/00073	713/186
*	I	US-2008/0267510 A1	10-2008	Paul; Mark G.	G06K9/00577	382/209
*	J	US-2009/0310779 A1	12-2009	Lam; Kwok Yan Karch	G06K9/00093	380/46
*	K	US-2011/0007177 A1	01-2011	Kang; Tae-hoon	H04N5/232	348/222.1
*	L	US-2012/0201381 A1	08-2012	Miller; Paul Timothy	H04L9/16	380/255
*	M	US-8,375,221 B1	02-2013	Thom; Stefan	G06F21/57	713/189

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

U.S. Patent and Trademark Office
PTO-892 (Rev. 01-2001) **Notice of References Cited** Part of Paper No. 20160710

Index of Claims	**Application/Control No.** 15075066	**Applicant(s)/Patent Under Reexamination** MILLER ET AL.
	Examiner DAO HO	**Art Unit** 2497

✓	**Rejected**	-	**Cancelled**	N	**Non-Elected**	A	**Appeal**
=	**Allowed**	÷	**Restricted**	I	**Interference**	O	**Objected**

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** □ **T.D.** □ **R.1.47**

CLAIM		DATE								
Final	Original	07/10/2016								
	1	-								
	2	-								
	3	-								
	4	-								
	5	-								
	6	-								
	7	-								
	8	-								
	9	-								
	10	-								
	11	-								
	12	-								
	13	-								
	14	-								
	15	-								
	16	-								
	17	-								
	18	-								
	19	-								
	20	-								
	21	-								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								
	27	✓								
	28	✓								
	29	✓								
	30	✓								
	31	✓								
	32	✓								
	33	✓								
	34	✓								
	35	✓								
	36	✓								

Index of Claims	**Application/Control No.** 15075066	**Applicant(s)/Patent Under Reexamination** MILLER ET AL.
	Examiner DAO HO	**Art Unit** 2497

✓	**Rejected**	-	**Cancelled**	N	**Non-Elected**	A	**Appeal**
=	**Allowed**	÷	**Restricted**	I	**Interference**	O	**Objected**

☐ **Claims renumbered in the same order as presented by applicant** ☐ **CPA** ☐ **T.D.** ☐ **R.1.47**

CLAIM		DATE								
Final	Original	07/10/2016								
	37	✓								
	38	✓								
	39	✓								
	40	✓								
	41	✓								
	42	✓								
	43	✓								
	44	✓								

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 1166

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
15/075,066	03/18/2016 **RULE**	380	2497	47583.5US02

APPLICANTS
mSignia, Inc., Irvine, CA;

INVENTORS
Paul Timothy Miller, Irvine, CA;
George Allen Tuvell, Thompson's Station, TN;

** **CONTINUING DATA** *************************
This application is a CON of 14/458,123 08/12/2014 PAT 9294448
which is a CON of 13/366,197 02/03/2012 PAT 8817984
which claims benefit of 61/462,474 02/03/2011

** **FOREIGN APPLICATIONS** *************************

** **IF REQUIRED, FOREIGN FILING LICENSE GRANTED** ** ** SMALL ENTITY **

Foreign Priority claimed □ Yes ☑ No
35 USC 119(a-d) conditions met □ Yes ☑ No
Verified and Acknowledged /DAO Q HO/ Examiner's Signature

□ Met after Allowance
Initials

STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
CA	11	21	3

ADDRESS

HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219
UNITED STATES

TITLE

CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE

FILING FEE RECEIVED
930

FEES: Authority has been given in Paper
No.____________ to charge/credit DEPOSIT ACCOUNT
No.____________ for following:

□ All Fees
□ 1.16 Fees (Filing)
□ 1.17 Fees (Processing Ext. of time)
□ 1.18 Fees (Issue)
□ Other ________________
□ Credit

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S94	3	(mSignia).as.	US-PGPUB; USPAT; USOCR	OR	OFF	2016/06/30 08:02
S95	953	((Paul) near2 (Miller)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2016/06/30 08:02
S96	4107	S95 a54 S94	US-PGPUB; USPAT; USOCR	OR	OFF	2016/06/30 08:02
S97	192	(hardware same firmware same software) and minutia	US-PGPUB; USPAT; USOCR	OR	ON	2016/06/30 08:02
S98	4	S96 and S97	US-PGPUB; USPAT; USOCR	OR	ON	2016/06/30 08:02
S99	1494838	(device with valu$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/30 08:02
S100	69497	S99 and (user near2 (specific defin$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/30 08:02
S101	445	S100 and (know$3 near2 update$)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/30 08:02
S102	6	S101 AND ((H04L63/0876 OR H04L9/0861 OR H04L9/0866).CPC. OR (380/255).CCLS.)	US-PGPUB; USPAT; USOCR	OR	ON	2016/06/30 08:02
S103	0	"15075066"	US-PGPUB; USPAT; USOCR	OR	OFF	2016/07/09 17:25
S104	42	("20060031676" | "20070240221" | "20080086676" | "20080086773" | "20080196104" | "20100229224" | "20110293094" | "6851316" | "8375221" | "20060104484" | "20080244744" | "20100027834" | "20130340052" | "7908662" |	US-PGPUB; USPAT; USOCR	OR	OFF	2016/07/09 17:26

		"7333871" | "20100332400" | "20070240219" | "20070240222" | "20120201381" | "6041133" | "7373669" | "20140229386" | "20070240218" | "20080235515" | "20110093503" | "8335925" | "20070124801" | "20110296170" | "6185316" | "20080175449" | "20090138975" | "20090310779" | "20110113388" | "7330871" | "20070240217" | "8213907" | "20070174206" | "20070214151" | "20070240220" | "20110082768" | "7937467" | "8312157").PN.				
S105	14	S104 and (minut$4)	US-PGPUB; USPAT; USOCR	OR	OFF	2016/07/09 18:18
S106	7	S105 and (challeng$3)	US-PGPUB; USPAT; USOCR	OR	OFF	2016/07/09 18:20
S107	1198	(minuti$3 with (location hardware firmware software call$3 frequently email))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/07/10 11:57
S108	11	("20070024801" | "20070214151" | "20080244744" | "20090138975" | "20100229224" | "20110082768" | "20110113388" | "7330871" | "7373669" | "7908662" | "7937467").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2016/07/10 11:58
S109	0	S108 and S107	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/07/10 11:58
S110	21	S107 AND ((H04L63/0876 OR H04L9/0861 OR H04L9/0866).CPC. OR (380/255).CCLS.)	US-PGPUB; USPAT; USOCR	OR	ON	2016/07/10 11:58
S111	144921	fingerprint$4	US-PGPUB; USPAT; USOCR	OR	ON	2016/07/10 12:00
S112	62	S107 NOT S111	US-PGPUB; USPAT; USOCR	OR	ON	2016/07/10 12:00
S113	87	(minuti$3 with (hardware firmware))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/07/10 12:58

EAST Search History (Interference)

<This search history is empty>

7/ 10/ 2016 1:24:04 PM
C:\ Users\ dho1\ Documents\ EAST\ Workspaces\ 15075066.wsp

U. S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(use as many sheets as necessary)

Complete if Known	
Application Number	15/075,066
Filing Date	March 18, 2016
Applicant(s)	mSignia, Inc.
Art Unit	2497
Examiner Name	Ho, Dao Q.
Attorney Docket Number	47583.5US02

SHEET 1 OF 1

U. S. PATENT DOCUMENTS

Examiner's initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
	1.	8,213,907	07-03-2012	Etchegoyen, Craig Stephen
	2.	8,335,925	12-18-2012	Taugbol, Petter
	3.	2007/0240217	10-11-2007	Tuvell et al.
	4.	2010/0332400	12-30-2010	Etchegoyen, Craig Stephen
	5.	2011/0093503	04-21-2011	Etchegoyen, Craig S.
	6.	2014/0229386	08-14-2014	Tervo et al.

FOREIGN PATENT DOCUMENTS

Examiner's Initials	Cite No.	Foreign Patent Document (Country Code – Number – Kind)	Publication Date MM-DD-YYYY	Patentee or Applicant of Cited Document	Translation Y/N

Examiner Signature	/DAO Q HO/	Date Considered	07/09/2016

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

U. S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(use as many sheets as necessary)*		*Complete if Known*	
		Application Number	15/075,066
		Filing Date	March 18, 2016
		Applicant(s)	mSignia, Inc.
		Art Unit	2431
		Examiner Name	Not Yet Assigned
SHEET 1	OF 1	Attorney Docket Number	47583.5US02

U. S. PATENT DOCUMENTS

Examiner's Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
		2007/0240218	10-11-2007	Tuvell et al.
		2007/0240219	10-11-2007	Tuvell et al.
		2007/0240220	10-11-2007	Tuvell et al.
		2007/0240221	10-11-2007	Tuvell et al.
		2007/0240222	10-11-2007	Tuvell et al.
		2008/0086773	04-10-2008	Tuvell et al.
		2008/0086776	04-10-2008	Tuvell et al.
		2008/0196104	08-14-2008	Tuvell et al.
		2011/0082768	04-07-2011	Eisen, Ori
		2011/0293094	12-01-2011	Os et al.
		2011/0296170	12-01-2011	Chen, Hu-Mu
		7,373,669	05-13-2008	Eisen, Ori
		2007/0124801	05-31-2007	Thomas et al.
		2007/0214151	09-13-2007	Thomas et al.
		2008/0244744	10-02-2008	Thomas et al.
		2011/0113388	05-12-2011	Eisen et al.
		7,908,662	03-15-2011	Richardson, Ric B.
		2009/0138975	05-28-2009	Richardon, Ric B.
		2010/0229224	09-09-2010	Etchegoyen, Craig S.
		7,333,871	02-19-2008	Schwarm, Alexander T.
		8,312,157	11-13-2012	Jakobsson et al.
		2013/0340052	12-19-2013	Jakobsson, Bjom Markus
		7,937,467 B2	05-03-2011	Barber, Timothy P.
		7,330,871 B2	02-12-2008	Barber, Timothy P.
		6,041,133	03-21-2000	Califano et al.
		6,185,316	02-06-2001	Buffam, William J.
		2006/0031676	02-09-2006	Vantalon et al.
		2006/0104484	05-18-2006	Bolle et al.
		2007/0174206	07-26-2007	Colella, Brian
		2008/0175449	07-24-2008	Fang et al.
		2008/0235515	09-25-2008	Yedidia et al.
		2009/0310779	12-17-2009	Lam et al.
		2010/0027834	02-04-2010	Spitzig et al.
		2012/0201381	08-09-2012	Miller et al.
		8,375,221	02-12-2013	Thom et al.

FOREIGN PATENT DOCUMENTS

Examiner's Initials	Cite No.	Foreign Patent Document (Country Code – Number – Kind)	Publication Date MM-DD-YYYY	Patentee or Applicant of Cited Document	Translation Y/N
		WO 2010/035202	04-01-2010	KONIN-KLIJKE PHILIPS ELECTRONICS N.V.	Y
		WO 2013/154936	10-17-2013	BRIVAS LLC	Y
		WO 2013/138714	09-19-2013	ACUITY SYSTEMS, INC.	Y

Examiner Signature	/DAO Q HO/	Date Considered	07/09/2016

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

Search Notes	**Application/Control No.** 15075066	**Applicant(s)/Patent Under Reexamination** MILLER ET AL.
	Examiner DAO HO	**Art Unit** 2497

CPC- SEARCHED

Symbol	Date	Examiner
H04L36/0876	07/10/2016	dqh
H04L9/0861, 0866	07/10/2016	dqh

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner
380	255	07/10/2016	dqh

SEARCH NOTES

Search Notes	Date	Examiner
see attached EAST search history	07/10/2016	dqh
inventor and assignee search in EAST	07/10/2016	dqh
NPL: minutia authentication	07/10/2016	dqh

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

	/DAO HO/ Primary Examiner.Art Unit 2497

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/075,066	03/18/2016	Paul Timothy Miller	47583.5US02

CONFIRMATION NO. 1166

PUBLICATION NOTICE

OC000000085650443

27683
HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

Title:CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE

Publication No.US-2016-0261416-A1
Publication Date:09/08/2016

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Paul T. Miller, George A. Tuvell		
Applicant:	mSignia, Inc.		
Title:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE		
Application No.:	15/075,066	Filing Date:	March 18, 2016
Examiner:	Dao Q. Ho	Group Art Unit:	2497
Docket No.:	47583.5US02	Confirmation No.:	1166

Costa Mesa, California
September 27, 2016

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE TO OFFICE ACTION

Dear Examiner Ho:

In response to the Office action dated July 14, 2016, Applicant submits the following amendments and remarks.

IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1-21. (Canceled)

22. (Currently amended) An identity recognition system comprising:

a non-transitory memory storing ~~information~~ data values associated with one or more identities, wherein the data values ~~information~~ stored for the one or more identities are based at least in part on information that is subject to change, the memory further storing information or instructions regarding one or more acceptable changes to the stored data values that are based at least in part on information that is subject to change ~~an identity includes one or more previously collected data values associated with such identity~~;

one or more hardware processors in communication with the memory and configured to execute instructions to cause the identity recognition system to recognize that the presentation of an identity by a computer is authentic, by performing operations comprising:

generating a challenge to the computer, wherein the challenge prompts the computer to provide a response based on one or more data values from the computer that correspond to one or more of the ~~previously-collected~~ stored data values associated with the identity, wherein at least one of the data values from the computer is based on information that is associated with the identity and that is subject to change ~~to be recognized;~~

receiving, from the computer, the response to the challenge;

determining whether the response is allowable, wherein such determining comprises evaluating whether the response is based on an acceptable change to a ~~previously-collected~~ stored data value associated with the identity ~~to be recognized~~; and

recognizing that the presentation of the identity by the computer is authentic, according to whether the computer has provided an allowable response to the challenge.

23. (Previously presented) The identity recognition system of claim 22, wherein the identity is associated with the computer and is a user identity or a device identity.

24. (Previously presented) The identity recognition system of claim 22, wherein the challenge prompts a response based on one or more user minutia data values.

25. (Currently amended) The identity recognition system of claim 24, wherein the operation of determining whether the response is allowable includes evaluating whether at least a portion of the response is based on one or more acceptable changes to a ~~previously-collected~~ user minutia data value.

26. (Currently amended) The identity recognition system of claim 25, wherein the ~~previously-collected~~ user minutia data values used to determine whether the response is allowable comprise user secrets, user customization, entertainment data, bio-metric data, or contacts.

27. (Currently amended) The identity recognition system of claim 25, wherein the ~~previously-collected~~ user minutia data values used to determine whether the response is allowable comprise calling app data, geo-location data, frequently called phone numbers, email, or network connection data.

28. (Currently amended) The identity recognition system of claim 22, wherein a ~~previously-collected~~ stored data value is used to generate at least a portion of the challenge, and wherein the determining operation further comprises evaluating whether a data value on which the response is based is the same as the ~~previously-collected~~ stored data value.

29. (Currently amended) The identity recognition system of claim 22, wherein a change to the ~~previously-collected~~ stored data value is acceptable if a data value upon which the response is based is within a set of acceptable values for the ~~previously collected~~ data value that are determined independently from receiving the response from the computer.

30. (Currently amended) The identity recognition system of claim 29, wherein the set of acceptable values includes one or more values based on predictable changes to the ~~previously-collected~~ data value.

31. (Currently amended) The identity recognition system of claim 29, wherein the set of acceptable values includes one or more values based on predicted changes to the ~~previously-collected~~ data value, based on industry updates to hardware, firmware, or software elements.

32. (Previously presented) The identity recognition system of claim 29, wherein the set of acceptable values includes one or more values based on a predictable user customization of the computer.

33. (Previously presented) The identity recognition system of claim 29, wherein the set of acceptable values includes one or more values based on a predictable usage of the computer by a user.

34. (Currently amended) The identity recognition system of claim 22, further comprising the operations of:

in response to evaluating that the response is based on an acceptable change to a ~~previously-collected~~ data value associated with the identity ~~to be recognized~~, updating the memory to reflect the changed data value.

35. (Previously presented) The identity recognition system of claim 22, wherein the operation of determining whether the response is allowable further comprises comparing the received response to a member of a set of two or more allowable responses.

36. (Previously presented) The identity recognition system of claim 35, wherein the set of allowable responses is computed before the determining operation is performed.

37. (Previously presented) The identity recognition system of claim 35, wherein the set of allowable responses is computed concurrently with the determining operation being performed.

38. (Currently amended) The identity recognition system of claim 22, wherein the determining operation further comprises generating a rating of the allowability of the response, based on the ~~previously collected~~ stored data value and one or more changes to the ~~previously-collected~~ stored data values.

39. (Currently amended) The identity recognition system of claim 38, wherein the rating of the allowability of the response is based on a comparison of a data value upon which the response is based to one or more predictable changes to the ~~previously-collected~~ stored data values associated with the identity to be recognized.

40. (Currently amended) The identity recognition system of claim 39, wherein the rating of the allowability of the response is varied based on whether the response is based at least in part on one or more predicted changes to the ~~previously-collected~~ stored data values.

41. (Previously presented) The identity recognition system of claim 22, wherein the operation of recognizing that the presentation of the identity by the computer is authentic provides a basis for one or more of: authenticating a device, authenticating a user, validating a software program or an application, providing data protection of data transmitted to or from a device, or generating a digital signature of a message digest.

42. (Previously presented) The identity recognition system of claim 22, wherein the response does not contain any data values reflecting personally identifiable information.

43. (Currently amended) An identity recognition system comprising:

a non-transitory memory storing data values ~~information~~ associated with one or more identities, wherein the data values ~~information~~ stored for the one or more identities are based at least in part on information that is subject to change, the memory further storing information or instructions regarding one or more acceptable changes to the stored data values that are based at least in part on information that is subject to change ~~an identity includes one or more verified data values associated with such identity~~;

one or more hardware processors in communication with the memory and configured to execute instructions to cause the identity recognition system to recognize that the presentation of an identity by a computer is authentic, by performing operations comprising:

receiving, from the computer, one or more communications comprising an identity claim, wherein at least a portion of the identity claim is formed based on one or more data values from the computer, and wherein at least one of the data values from the computer is based on information that is associated with the identity and that is subject to change; and

determining whether the one or more communications received from the computer are sufficient to recognize that the identity claim is authentic, wherein such determining comprises evaluating whether a data value used to form the identity claim is based on an acceptable change to a stored ~~previously verified~~ data value associated with the identity ~~to be recognized~~.

44. (Currently amended) An identity recognition system comprising:

a non-transitory memory storing data values ~~information~~ associated with one or more identities, wherein the data values ~~information~~ stored for the one or more identities are based at least in part on information that is subject to change, the memory further storing information or instructions regarding one or more acceptable changes to the stored data values that are based at least in part on information that is subject to change ~~an identity includes one or more previously collected data values associated with such identity~~;

one or more hardware processors in communication with the memory and configured to execute instructions to cause the identity recognition system to recognize that the presentation by a computer of an identity to be recognized ~~at a computer~~ is authentic, by performing operations comprising:

receiving, from the computer, a communication based on one or more data values from the computer, wherein at least one of the data values from the computer is based on information that is associated with the identity to be recognized and that is subject to change; and

determining whether the communication received from the computer is sufficient to recognize that the use of an identity is authentic, wherein such determining comprises evaluating whether a data value upon which the communication is based reflects an acceptable change to a stored ~~previously collected~~ data value associated with the identity to be recognized.

REMARKS

Claims 22-44 were pending in the present application. Claims 22, 25-31, 34, 38-40, 43, and 44 are amended. Accordingly, upon entry of this amendment claims 22-44 will be pending.

Examiner Interview

Applicant appreciates the courtesies extended to the undersigned representative during a telephone interview with Examiner Ho on August 31, 2016. An outline of Applicant's argument with respect to the Alice rejections was presented. The Examiner agreed that the section 101 rejections would be withdrawn in view of Applicants remarks, which are presented in this response.

The Buffam and Kang references were discussed in relation to the limitations of independent claims 22, 43, and 44. The Examiner submitted that Applicant's claim 22 (for example) can still be read on Buffam (combined with Kang) because claim 22 (as presented at the interview) reads on strictly hardware type minutia (e.g., hardware data values such as IMEI numbers). The Examiner suggested that some care may be needed to amend the claims so that they necessarily read on other than hardware minutia without excluding the case of hardware minutia. No further agreement was reached, and Applicant amends the present claims to address the Examiner's remarks and suggestions, for which Applicant thanks Examiner Ho.

Summary of the Office Action

Claims 22, 43, and 44 were objected to for informalities.

Claims 22-44 were rejected under 35 U.S.C. § 101 as being directed to a judicial exception without significantly more.

Claims 22-44 were rejected under pre-AIA 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 6,185,316 to Buffam (referred to as "**Buffam**") in view of U.S. Patent Application Publication 2011/0007177 to Kang (referred to as "**Kang**").

Claim Objections

Claims 22, 43, and 44 were objected to for informalities. Claims 22, 43, and 44 are amended to include a colon following the preamble of each claim, thus providing appropriate correction for each of claims 22, 43, and 44. In addition, Applicant has corrected some other minor informalities in claims 43 and 44 by the addition of a second colon after the second occurrences of the word "comprising" and addition of the word "and".

Applicant thus respectfully requests withdrawal of the objections to claims 22, 43, and 44.

Claim Amendments

Independent claims 22, 43, and 44 are amended. Numerous examples of support for the amendment to claims 22, 43, and 44 can be found in the specification as filed, among which at least, are the following:

at page 16, lines 13-15 (regarding "data values . . . subject to change"):

> Software minutia changes dynamically via various individual instantiations of service user 20 and includes elements that may require predictable, constant change in normal situations (i.e., frequently called contact phone numbers).

page 19, lines 5-14 (regarding "data values . . . subject to change"):

> dynamic key crypto provider 10, for example, may be able to know what all the possibilities are for the computer minutia 64 of a given computer 18 so that system 200 may be able to recognize a computer 18 in spite of changes not reflected or known by the current minutia DB 70.

at page 22, lines 25-30 (regarding "the memory further storing information or instructions regarding one or more acceptable changes to the stored data values that are based at least in part on information that is subject to change"):

> At step 2030, the dynamic key crypto provider 10 computes all responses that are acceptable for the computer 10 to make. The acceptable response computations can be based on the allowable range of possible changes to the defined subset of minutiae selected for the challenge. These computations can be performed beforehand (e.g., independently – whether prior, concurrently, or after – receiving the actual response from the computer 18) and stored in valid responses DB 130 for comparison to the actual response from computer 18.

at page 23, lines 1-9; and Figure 2B and Figure 5 (regarding "storing information or instructions regarding one or more acceptable changes"):

> The range of possible changes may be processed because of the constant and continuous collecting and cataloging of industry updates for the total set of minutia from which the particular combination of minutia (e.g., Hx, Fy, Sz for the example of Figure 2) to be used for challenging the particular device is selected. Because every allowable response to a challenge is therefore known (e.g., computed at step 2030) before the challenge is sent to the computer 18, the actual response that will be received from the computer 18 to the challenge may be among the range of pre-processed acceptable responses (and therefore among the **acceptable changes**) computed by the dynamic key crypto provider 10 that is challenging the computer 18 (emphasis added).

at page 24, lines 3-17; and Figure 2B (regarding "storing information or instructions regarding one or more acceptable changes"):

> As illustrated at step 2050, the validate response from computer 120 process can therefore be determined by simply comparing the actual response received from the computer 18 to the allowable responses that are pre-processed by the dynamic key crypto provider 10 to determine if there is a match. Decrypting or decoding of a response is not necessary so the validation can occur very quickly. On a match between the actual response and one of the pre-processed responses, the validate response from computer 120 process may then know what the particular actual

> minutia values from computer 18 are for the combination selected (e.g., triplet Hx-Fy-Sz) by knowing which possible response has matched the actual response even though neither response contains any direct or decipherable information about the actual minutia values.

at page 25, lines 16-22; and Figure 2B (regarding "storing information or instructions regarding one or more acceptable changes"):

> At step 2060, on a match between the actual response and one of the pre-processed responses, the update computer minutia 128 process may then know what the particular actual minutia values from computer 18 are for the combination selected (e.g., triplet Hx-Fy-Sz) by knowing which possible response has matched the actual response even though neither response contains any direct or decipherable information about the actual minutia values. The values from the valid responses DB 130 used in the response calculation can then be used to update the values stored in the minutia DB 70 database.

and at page 32, lines 8-14 and 21-25; and Figure 5 (regarding "storing information or instructions regarding one or more acceptable changes"):

> The collected data is then given to a data modeling, heuristics and permutations 92 process for analysis with regard, for example, to computer or user device identification. The data modeling, heuristics and permutations 92 process considers historical minutia trends and data mining 94 as well as the current minutia DB 70, the current anticipated minutia DB 98 and the event log 12 which may log actions and exchanges performed by the dynamic key crypto provider 10 for auditing and heuristic analysis at later times.
>
> Other related minutia values may change as a result of service user 20 usages. This is related but different to service user 20 behavior patterns; minutia values in minutia DB 70 (such as minutia values related to the computer 18) establish the behavior of the minutiae (such as computer 18) and, therefore, behavioral algorithms can be applied to the minutia DB 70 values.

Applicant submits that no new matter is added.

Rejections under 35 U.S.C. § 101

Claims 22-44 were rejected under 35 U.S.C. § 101 as being directed to a judicial exception (i.e., a law of nature, a natural phenomenon, or an abstract idea) without significantly more. The Office action states:

> Based upon an analysis with respect to the claim as a whole, claim(s) 22, 43 and 44 do not recite something significantly different than a judicial exception. The rationale for this determination is explained below: *the claims recited a mere challenge and response method of authentication. The function can be done by a person and does not require significantly more, thus, are considered as abstract idea.* In additional, *the claim does not contain an 'inventive concept' to 'transform' the claimed abstract idea into patent-eligible subject matter because the claim simply instructs to implement the abstract idea with routine, conventional activity.* As discussed above, the claim is directed to an abstract idea and does not do significantly more than simply described that abstract method. Therefore, the claim is not directed to patent eligible subject matter. See *Alice Corporation v. CLS Bank International,* (S.Ct.2014) and *Ultramerical, Inc. v.Hulu, LLC.* (Fed. Cir. 2014). Dependent claim(s) 23-42 are also rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter for the same reason addressed above.

Applicant respectfully traverses the rejection, in view of the following remarks.

Briefly, Applicant will show that the claims (e.g., amended claim 22) are not merely directed to an abstract idea without significantly more. Instead, the claims improve the functioning of the computer itself or an existing technological process (see, e.g., *Alice*, 134 S. Ct. at 2358-59) by providing an improved identity recognition system that uses changing information on a computer to recognize the identity of, e.g., the computer or the user. This would allow, for example, a smartphone using the claimed improvement to the technology of such hardware to be used as an identification (e.g., like an ID card). Notably, one way that the claimed invention differs from prior art systems, is that the identification need not be based on static information. Instead, the system functionality of "recognizing that the presentation of the identity by the computer is authentic" involves "evaluating whether the response is based on an acceptable change" (e.g., to stored data values associated with the identity). Applicant submits that claims 22-44, as being directed to an improvement to the technological capabilities of the claimed devices, thus, are directed to patent eligible subject matter.

These claims satisfy the subject matter eligibility set forth in the 2014 Interim Guidance on Patent Subject Matter Eligibility ("Interim Eligibility Guidance") as well as in the updates to that guidance.

Under step 1, the question is to determine whether the claims are directed to one of the statutory categories of invention, e.g., a process, machine, manufacture, or composition of matter. Because independent claims 22, 43, and 44 each recite a "system" (e.g., a machine), Applicant submits that each of the independent claims is directed to a statutory category of invention.

Under step 2A of the test, the question is to determine whether the claim is directed to a judicially recognized exception, e.g., "a law of nature, a natural phenomenon, or an abstract idea".

The Office action asserts that the claims are directed to a "mere challenge and response method of authentication." (Office Action at page 3.) The Office action does not tie the notion of "challenge and response method of authentication" to any of the judicially-recognized abstract ideas, such as mitigating settlement risk, hedging, creating a contractual relationship, using advertising as an exchange or currency, processing information through a clearinghouse, comparing new and stored information and using rules to identify options, using categories to organize, store, and transmit information, and organizing information through mathematical correlations. Moreover, there are significant differences between a system that uses a challenge/response method of authentication and these judicially-recognized "abstract ideas. A "challenge/response method of authentication" is not a fundamental economic principle or a method of organizing human behavior. Nor is it a process that involves identifying options or organizing information through mathematical correlations. None of the other judicially-recognized "abstract ideas" apply to a "challenge and response method of authentication" either. Thus, a challenge and response method of authentication is not similar to a judicially-recognized "abstract idea" under § 101.

Even if a "challenge and response method of authentication" were held to be an "abstract idea," the claims would still be patentable, because the claims are not directed to that notion.

Instead, the claims are directed towards an identity recognition system, not a mere challenge and response method of authentication. Indeed, claims 43 and 44 do not require either a challenge or response. Claim 22 does require a challenge, but it is a a specific type of challenge that prompts a response "based on one or more data values from the computer that correspond to one or more of the-stored data values associated with the identity, wherein at least one of the data values from the computer is based on information that is associated with the identity and that is subject to change". Claims 22, 43 and 44 require a specific type of message "wherein at least one of the data values from the computer is based on information that is associated with the identity and that is subject to change" and provide a new type of processing, i.e. processing the response and the information or instructions regarding one or more acceptable changes to the stored data values to determine "whether the response is allowable, wherein such determining comprises evaluating whether the response is based on an acceptable change to a stored data value associated with the identity". Thus, the claims are not directed to a mere challenge and response method of authentication. Instead, they recite a specific identity recognition *system* having new capabilities that previous challenge/response-based identity recognition systems did not have (e.g., an inventive concept that transforms an abstract idea into patent eligible subject matter). Thus, the claims are not directed to an abstract idea.

Moreover, the Office action asserts that: "*the claims recited a mere challenge and response method of authentication. The function can be done by a person and does not require significantly more, thus, are considered as abstract idea.*" Applicant respectfully submits that, contrary to the Office action allegation, the functions can <u>not</u> "*be done by a person*", because, for one thing, the computer is required to be present in order to perform the actions of the claim.

For example, the limitations of claim 22 require certain data values to come from the computer itself, for example:

> a non-transitory memory storing . . . data values associated with one or more identities. . . further storing information or instructions regarding one or more acceptable changes to the stored data values that are based at least in part on information that is subject to change;
>
> . . . the challenge prompts the computer to provide a response based on one or more data values from the computer that correspond to one or more of the stored data values . . . ; [and]
>
> . . . evaluating whether the response is based on an acceptable change to a stored data value . . . ;

The data values—whether they are stored data values or whether they are "data values from the computer that correspond to . . . the stored data values", and whether they are based on biometric information, hardware attributes or software attributes, for example—are bits of electronic information that are not accessible by a person without the use of the claimed computer, hardware processors, and non-transitory memory themselves and could not possibly be reliably remembered by any human person. Indeed, the claim requires that the "one or more data values from the computer" come from the computer and not from a person.

Moreover, even in principle, the operation (function) of "evaluating whether the response is based on an acceptable change to a stored data value" cannot be performed by a person because the range of acceptable changes is too vast for a person to be able to accommodate in the person's memory or cognition, even using "pencil and paper", without the use of a device (i.e., the claimed computer). It is the device itself, including its stored data values and what constitutes an acceptable change from those values, that is the fundamental object of the recognition (authentication) and cannot be substituted by activities performed by a person.

The conclusion of patent-eligibility is supported by recent Federal Circuit decisions. For example, in *Enfish*, the Federal Circuit stated:

> Nor do we think that claims directed to software, as opposed to hardware, are inherently abstract and therefore only properly analyzed at the second step of the *Alice* analysis. Software can make non-abstract improvements to computer technology just as hardware improvements can, and sometimes the improvements can be accomplished through either route. We thus see no reason to conclude that all claims directed to improvements in computer-related technology, including those directed to software, are abstract and necessarily analyzed at the second step of *Alice*, nor do we believe that *Alice* so directs. Therefore, we find it relevant to ask whether the claims are directed to an improvement to computer functionality versus being directed to an abstract idea, even at the first step of the *Alice* analysis.
>
> For that reason, the first step in the *Alice* inquiry in this case asks whether the focus of the claims is on the specific asserted improvement in computer capabilities (i.e., the self-referential table for a computer database) or, instead, on a process that qualifies as an "abstract idea" for which computers are invoked merely as a tool. . . . In this case, however, the plain focus of the claims is on an improvement to computer functionality itself, not on economic or other tasks for which a computer is used in its ordinary capacity.
>
> Accordingly, we find that the claims at issue in this appeal are not directed to an abstract idea within the meaning of *Alice*. Rather, they are directed to a specific improvement to the way computers operate, ...

HAYNES AND BOONE, LLP
600 Anton Blvd. Suite 700
Costa Mesa, CA 92612
Tel: (949) 202-3000
FAX (949) 202-3001

Here, as in *Enfish* (Case 2015-1244, Fed. Cir., May 12, 2016.), the focus of the claims is on a specific improvement in computer capabilities, namely, in claim 22, for example:

> . . . storing data values associated with one or more identities, wherein the data values stored for the one or more identities are based at least in part on information that is subject to change;
>
> determining whether the response is allowable, wherein such determining comprises evaluating whether the response is based on an acceptable change to a stored data value associated with the identity; and
>
> recognizing that the presentation of the identity by the computer is authentic, according to whether the computer has provided an allowable response to the challenge.

The focus of the claim here is not merely on an abstract process of "*challenge and response method of authentication*" for which the computer is invoked merely as a tool, but instead the focus is on the specific asserted improvement in computer capabilities that allows "presentation of the identity by the computer" to be recognized as authentic "based on an acceptable change to a stored data value associated with the identity". The computer is not invoked merely as a tool, used in its ordinary capacity for economic or other tasks, e.g., the task of authentication, but is an integral part of the authentication – i.e., the computer is required to be present in order to perform the actions of the claim – that is based on acceptable change related to data values from the computer, i.e. improvement to the computer functionality itself.

Applicant makes a similar argument for claim 43 based on the limitations:

> receiving, from the computer, one or more communications comprising an identity claim, wherein at least a portion of the identity claim is formed based on one or more data values from the computer, and wherein at least one of the data values from the computer is based on information that is associated with the identity and that is subject to change; and
>
> determining whether the one or more communications received from the computer are sufficient to recognize that the identity claim is authentic, wherein such determining comprises evaluating whether a data value used to form the identity claim is based on an acceptable change to a stored data value associated with the identity.

and Applicant makes a similar argument with respect to claim 44 based on the limitations:

> receiving, from the computer, a communication based on one or more data values from the computer, wherein at least one of the data values from

> the computer is based on information that is associated with the identity to be recognized and that is subject to change; and
>
> determining whether the communication received from the computer is sufficient to recognize that the use of an identity is authentic, wherein such determining comprises evaluating whether a data value upon which the communication is based reflects an acceptable change to a stored data value associated with the identity to be recognized.

Thus, Applicant submits that the claims, here, as in *Enfish*, are not directed to an abstract idea or other judicial exception within the meaning of *Alice*. Applicant, therefore, submits that claims 22-44 claim patent eligible subject matter. Applicant, nevertheless, proceeds to step 2B of the analysis.

Under step 2B of the test the question is to determine whether the claim recites additional elements that are sufficient to amount to significantly more than the judicial exception.

Contrary to the Office action allegation that "*the claim does not contain an 'inventive concept' to 'transform' the claimed abstract idea into patent-eligible subject matter because the claim simply instructs to implement the abstract idea with routine, conventional activity*", Applicant submits that the additional elements of "determining whether the response is allowable", "evaluating whether the response is based on an acceptable change to a stored data value", and "recognizing that the presentation of the identity by the computer is authentic, according to whether the computer has provided an allowable response to the challenge" as recited in claim 22, for example, are in fact sufficient to amount to significantly more than any judicial exception.

The court in *Bascom* has stated:

> The "inventive concept" may arise in one or more of the individual claim limitations or in the ordered combination of the limitations. Alice, 134 S. Ct. at 2355. An inventive concept that transforms the abstract idea into a patent-eligible invention must be significantly more than the abstract idea itself, and cannot simply be an instruction to implement or apply the abstract idea on a computer. Id. at 2358.

Here, the limitation "evaluating whether . . . an acceptable change to a stored data value associated with the identity" arises out of the computer technology itself, because the elements of the claims, the data values, about which acceptable change is evaluated, require for their presence the computer itself and the hardware processors, i.e., "a non-transitory memory storing data values associated with one or more identities, wherein the data values-stored for the one or more identities are based at least in part on information that is subject to change" as recited in claim 22, for example. Thus, the limitation of "evaluating whether . . . an acceptable change to a stored data value" requires more than a simple instruction to apply some abstract idea on a computer, but actually requires the computer itself for providing the data values.

Moreover, "evaluating . . . acceptable change" requires more than mere routine or conventional comparisons of static data values as, for example, in a conventional "*challenge and response method of authentication*" that uses a simple matching of corresponding values. Such a simple matching that does not allow for changing data values cannot of itself accomplish the limitation of "determining whether the response is allowable, wherein such determining comprises evaluating whether the response is based on an acceptable change to a stored data value associated with the identity to be recognized". Applicant thus submits that the limitation "evaluating . . . acceptable change" supplies an inventive concept that is significantly more than any abstract idea itself, and cannot simply be an instruction to implement or apply an abstract idea on a computer. Therefore, the limitation supplies an inventive concept that transforms an abstract idea into a patent-eligible invention.

Applicant submits that similar reasoning also applies to claim 43, which recites "evaluating whether a data value used to form the identity claim is based on an acceptable change to a stored data value associated with the identity to be recognized" and claim 44, which recites "evaluating whether a data value upon which the communication is based reflects an acceptable change to a stored data value associated with the identity to be recognized".

In addition, similar to the claims in *DDR Holdings*, the claims here address a problem arising in the realm of computer networks, and provide a solution necessarily rooted in computer technology. The problem may be characterized, in one way, as providing the recognition of an identity through the presentation of the identity by a computer. This is not merely the long-standing problem of recognizing an identity, but arises out of the comparatively recent evolution of personal computing devices that have become personalized to their owner or user, combined with the problem that methods such as username/password authentication protocols have become inadequate. To take an extreme example, such a problem did not exist, for example, in the days of mainframe computers, such as the IBM 360, which typically were owned or could be afforded only by institutions or corporations and were shared among several users or departments.

The solution to the current problem provided by the instant claims relies on "data values-stored for the one or more identities . . . based at least in part on information that is subject to change" and "at least one of the data values from the computer [that] is based on information that is associated with the identity and that is subject to change" (as recited in claim 22) such that the claims do not simply instruct to implement an abstract idea on the computer with routine, conventional activity. Rather the computer is an integral part of the solution by providing the "at least one of the data values from the computer [that] is based on information that is associated with the identity and that is subject to change" and the claimed memory is an integral part of the solution by providing the "data values-stored for the one or more identities" and "information or instructions regarding one or more acceptable changes to the stored data values". In addition, the solution of "determining whether the response is allowable, wherein such determining comprises evaluating whether the response is based on an acceptable change to a stored data value associated with the identity" requires a volume of information memory and processing to be completed in a practical period of time, such as a few seconds, that no human or team of humans would be mentally or physically capable of, such that the function cannot be done by a person. The solution is, thus, necessarily rooted in computer technology to address the problem arising in the realm of computer networks.

Accordingly, Applicant submits that the claims here, like those found to be patent eligible in *DDR Holdings*, improve the performance of the computer system itself, and thus recite additional elements that are sufficient to amount to significantly more than the judicial exception.

Here, as above, Applicant submits that similar reasoning also applies to claim 43, which recites "evaluating whether a data value used to form the identity claim is based on an acceptable change to a stored data value associated with the identity to be recognized" and claim 44, which recites "evaluating whether a data value upon which the communication is based reflects an acceptable change to a stored data value associated with the identity to be recognized".

Thus, Applicant submits that independent claims 22, 43, and 44 recite additional elements that are sufficient to amount to significantly more than an abstract idea or other judicial exception. Therefore, Applicant's claim 22 (and similarly independent claims 43 and 44) recites patent eligible subject matter.

Accordingly, Applicant respectfully requests that the rejection of claims 22-44 under 35 U.S.C. §101 be reconsidered and withdrawn.

Rejections under 35 U.S.C. § 103

Claims 22-44 were rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Buffam** in view of **Kang**.

Applicant submits that Buffam in view of Kang does not disclose or suggest:

> a non-transitory memory storing data values associated with one or more identities, wherein the data values-stored for the one or more identities are based at least in part on information that is subject to change, the memory further storing information or instructions regarding one or more acceptable changes to the stored data values . . . ;
>
> . . . a response based on one or more data values from the computer that correspond to one or more of the-stored data values associated with the identity, wherein at least one of the data values from the computer is based on information that is associated with the identity and that is subject to change;
>
> . . . evaluating whether the response is based on an acceptable change to a stored data value associated with the identity;

as in Applicant's claim 22, for example.

Instead, **Buffam** teaches fingerprint identification using fingerprint minutia (in combination with **Kang** which is relied on by the Office action to teach other types of minutia) which do not change over time, a property of fingerprint minutia needed by Buffam to provide fingerprint identification that works reliably over time. Thus, Buffam does not teach or suggest any of "[stored] data values . . . based at least in part on information that is subject to change"; "[stored] information or instructions regarding one or more acceptable changes to the stored data values"; "data values from the computer . . . based on information that is associated with the identity and that is subject to change"; or "acceptable change to a stored data value associated with the identity".

It follows, then, in connection to these limitations, not taught by Buffam, that Buffam also does not provide the ability to recognize an identity based on acceptable changes to data values (which makes sense, given that Buffam is a *fingerprint* recognition system, and fingerprints do not change over time). At best, Buffam suggests that a certain amount of data may be "missed", e.g., Buffam states: "the degree to which false negatives are accepted, can be adjusted by policy-based factors, including the acceptable number of missing true minutiae, or TIPs from structure 280, for example, as compared with a reference template 305" (see col. 16, lines 38-43). However, a willingness to disregard non-matching data is not the same as determining that the non-matching data actually reflects an *acceptable change* to what was previously stored.

Furthermore, even though **Kang**, which as noted above, is relied on by the Office action to teach various types of minutia (to which Applicant does not acquiesce) mentions the word "change," Kang's references to the word "change", at best, concern changes to the lighting environment of a camera (having to do with shooting modes of the camera), and not to changes to stored data values (see, e.g., paragraphs [0058], [0063], [0072], and [0094]). Therefore, there appears no logical or reasonable way to combine Kang with Buffam in this regard to arrive at any of Applicant's limitations concerning "data values . . . subject to change" or "acceptable change". Applicant thus submits that Kang does not cure the deficiencies of Buffam with regard to the limitations of "[stored] data values . . . based at least in part on information that is subject to change"; "[stored] information or instructions regarding one or more acceptable changes to the stored data values"; "data values from the computer . . . based on information that is associated with the identity and that is subject to change"; and "acceptable change to a stored data value associated with the identity". Applicant submits, therefore, that claims 22, 43, and 44 are patentable over the combination of Buffam and Kang.

With respect to the point of issue that Kang supplies the missing device information (e.g., Kang is cited by the Office action for teaching various elements as types of minutia), Applicant also traverses that argument. Kang is from the field of photography, not the field of identity recognition. Kang is also not "reasonably pertinent" to the problem of digital identity recognition. Thus, Kang is not "analogous" prior art that can be used in an obviousness combination against the Application. Moreover, the Office action does not explain how or why a person of ordinary skill in the art would have (1) selected Kang as a secondary reference; (2) added certain photography minutia from Kang to the fingerprint data of Buffam; or (3) been motivated to do so in order to get better "authentication for more secure protection." Office Action at 6. Thus, Applicant respectfully submits that the Office Action does not state a combination rationale sufficient to support a *prima facie* case of obviousness and for that additional reason that claims 22, 43, and 44 are patentable over the combination of Buffam and Kang.

Because Buffam and Kang do not provide either for data values that change or the ability to recognize an identity based on evaluating acceptable changes to data values, Buffam and Kang do not teach each and every element of Applicant's claims as recited in independent claims 22, 43, and 44. Therefore, Applicant respectfully requests that the section 103 rejections to claims 22, 43, and 44 be reconsidered and withdrawn.

The remaining claims, being dependent on claim 22, are patentable over any combination of Buffam and Kang for at least the same reasons. Accordingly, Applicant respectfully requests reconsideration and withdrawal of the section 103 rejections to all of pending claims 22-44.

CONCLUSION

Applicant respectfully submits that claims 22-44 are in condition for allowance. Reconsideration and withdrawal of the rejections are respectfully requested, and a timely Notice of Allowance is solicited.

If there are any questions regarding any aspect of the application, please call the undersigned at (949) 202-3011.

Certificate of Transmission

I hereby certify that this correspondence is being electronically transmitted via EFS Web to the Commissioner for Patents, on the date stated below.

Allison Hung September 27, 2016

Respectfully submitted,

David Bowls
Patent Agent
Reg. No. 39,915

Electronic Acknowledgement Receipt

EFS ID:	27051708
Application Number:	15075066
International Application Number:	
Confirmation Number:	1166
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul Timothy Miller
Customer Number:	27683
Filer:	David B. Bowls/Allison Hung
Filer Authorized By:	David B. Bowls
Attorney Docket Number:	47583.5US02
Receipt Date:	27-SEP-2016
Filing Date:	18-MAR-2016
Time Stamp:	19:14:08
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		5US02ResponsetoNonFinalOfficeAction.pdf	3998017 4450fafaa36d9780de146793fd025c554b01deff	yes	25

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	7
	Applicant Arguments/Remarks Made in an Amendment	8	25

Warnings:

Information:

Total Files Size (in bytes):	3998017

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 15/075,066	Filing Date 03/18/2016	□ To be Mailed

ENTITY: □ LARGE ☒ SMALL □ MICRO

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)		
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)
□ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
□ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
□ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
□APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
□ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)		
AMENDMENT	**09/27/2016**	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 23	Minus	** 23	= 0	x $40 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	x $210 =	0
	□ Application Size Fee (37 CFR 1.16(s))						
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	**0**

		(Column 1)		(Column 2)	(Column 3)		
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	□ Application Size Fee (37 CFR 1.16(s))						
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
PAUL STANBACK

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

27683 7590 11/04/2016

HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

EXAMINER	
HO, DAO Q	
ART UNIT	PAPER NUMBER
2497	

DATE MAILED: 11/04/2016

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/075,066	03/18/2016	Paul Timothy Miller	47583.5US02	1166

TITLE OF INVENTION: CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	02/06/2017

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

27683 7590 11/04/2016
HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/075,066	03/18/2016	Paul Timothy Miller	47583.5US02	1166

TITLE OF INVENTION: CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	02/06/2017

EXAMINER	ART UNIT	CLASS-SUBCLASS
HO, DAO Q	2497	380-255000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1____________________________

2____________________________

3____________________________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:

❑ Issue Fee
❑ Publication Fee (No small entity discount permitted)
❑ Advance Order - # of Copies ______________________

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

❑ A check is enclosed.
❑ Payment by credit card. Form PTO-2038 is attached.
❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____________ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

❑ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

❑ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature ____________________________________ Date ________________________________

Typed or printed name ___________________________________ Registration No. __________________________

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/075,066	03/18/2016	Paul Timothy Miller	47583.5US02	1166

27683 7590 11/04/2016

HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

EXAMINER	
HO, DAO Q	

ART UNIT	PAPER NUMBER
2497	

DATE MAILED: 11/04/2016

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Examiner-Initiated Interview Summary	**Application No.** 15/075,066	**Applicant(s)** MILLER ET AL.
	Examiner DAO HO	**Art Unit** 2497

All participants (applicant, applicant's representative, PTO personnel):

(1) *DAO HO*. (3)_____.

(2) *DAVID BOWLS*. (4)_____.

Date of Interview: *28 October 2016*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *22*.

Identification of prior art discussed: *Buffam, kang*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

The Applicant and The Examiner discussed the "determining…" limitation. The Examiner indicated that the current limitaton based on broadest reasonable interpretation indicated that if there is a match, then no further steps is necessary; thus, the subject to change is not invoke. The Examiner suggested to amend the limitation to indicate that the data values have to check for the changes. Agreement was reached.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/DAO HO/
Primary Examiner, Art Unit 2497

Notice of Allowability	Application No. 15/075,066	Applicant(s) MILLER ET AL.	
	Examiner DAO HO	Art Unit 2497	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *09/27/2016*.
   □ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on______.
2. □ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *22-46*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. □ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) □ All b) □ Some *c) □ None of the:
   1. □ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. ______ .
   3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE “MAILING DATE” of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. □ CORRECTED DRAWINGS (as “replacement sheets”) must be submitted.
   □ including changes required by the attached Examiner’s Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner’s comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. □ Notice of References Cited (PTO-892)
2. □ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date *10/28/2016* .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. □ Other _____.

/DAO HO/
Primary Examiner, Art Unit 2497

DETAILED ACTION

The present application is being examined under the pre-AIA first to invent provisions.

Response to Amendment

This is a reply to the application filed on 09/27/2016, in which, claim(s) **22-44** is/are pending.

Claim(s) 22, 25-31, 34, 38-40, 43 and 44 is/are amended.

Claim(s) 1-21 is/are cancelled.

Claim Rejections - 35 U.S.C. § 101:

Applicants' arguments with respect to claim(s) 22-44 have been fully considered and are persuasive. The rejection of 35 USC §101 have been withdrawn in view of the amendment to claim.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Attorney David Bowls on 10/28/2016.

The application has been amended as follows:

1-21. (Canceled)

22. (Currently amended) An identity recognition system comprising:

a non-transitory memory storing information ~~data values~~ associated with one or more identities, wherein the information ~~data values~~ stored for an identity includes (a) data values associated with that identity; and (b) information regarding anticipated changes to one or more of the stored data values associated with that identity; ~~the one or more identities are based at least in part on information that is subject to change, the memory further storing information or instructions regarding one or more acceptable changes to the stored data values that are based at least in part on information that is subject to change;~~

one or more hardware processors in communication with the memory and configured to execute instructions to cause the identity recognition system to recognize that the presentation of ~~an~~ identity information by a computer is authentic, by performing operations comprising:

generating a challenge to the computer, wherein the challenge prompts the computer to provide a response based on one or more data values from the computer that correspond to one or more of the-stored data values associated with the identity; ~~, wherein at least one of the data values from the computer is based on information that is associated with the identity and that is subject to change~~

receiving, from the computer, the response to the challenge;

determining whether the response is allowable, wherein such determining comprises ~~evaluating~~ using the stored information regarding anticipated changes to the stored data values associated with the identity to determine whether a data value used to form the response is based on an acceptable change to a corresponding stored data value ~~associated with the identity~~; and

recognizing that the presentation of ~~the~~ identity information by the computer is authentic, according to whether the computer has provided an allowable response to the challenge.

23. (Previously presented) The identity recognition system of claim 22, wherein the identity is associated with the computer and is a user identity or a device identity.

24. (Previously presented) The identity recognition system of claim 22, wherein the challenge prompts a response based on one or more user minutia data values.

25. (Previously presented) The identity recognition system of claim 24, wherein the operation of determining whether the response is allowable includes evaluating whether at least a portion of the response is based on one or more acceptable changes to a user minutia data value.

26. (Previously presented) The identity recognition system of claim 25, wherein the user minutia data values used to determine whether the response is allowable comprise user secrets, user customization, entertainment data, bio-metric data, or contacts.

27. (Previously presented) The identity recognition system of claim 25, wherein the user minutia data values used to determine whether the response is allowable comprise calling app data, geo-location data, frequently called phone numbers, email, or network connection data.

28. (Currently amended) The identity recognition system of claim 22, wherein a stored data value is used to generate at least a portion of the challenge, and wherein the determining operation ~~further~~ comprises evaluating whether [[a]] the data value used to form ~~on which~~ the response ~~is based~~ is the same as the stored data value.

29. (Currently amended) The identity recognition system of claim 22, wherein a change to the stored data value is acceptable [[if]] when [[a]] the data value used to form ~~upon which~~ the response ~~is based~~ is within a set of acceptable values for the stored data value that are determined independently from receiving the response from the computer.

30. (Currently amended) The identity recognition system of claim 29, wherein the set of acceptable values includes one or more values based on anticipated ~~predictable~~ changes to the data value.

31. (Currently amended) The identity recognition system of claim 29, wherein the set of acceptable values includes one or more values based on anticipated ~~predicted~~ changes to the data value, based on industry updates to hardware, firmware, or software elements.

32. (Currently amended) The identity recognition system of claim 29, wherein the set of acceptable values includes one or more values based on an anticipated ~~a predictable~~ user customization of the computer.

33. (Currently amended) The identity recognition system of claim 29, wherein the set of acceptable values includes one or more values based on an anticipated ~~a predictable~~ usage of the computer by a user.

34. (Currently amended) The identity recognition system of claim 22, further comprising the operations of:

in response to determining ~~evaluating~~ that the response is based on an acceptable change to a data value associated with the identity, updating the memory to reflect the changed data value.

35. (Previously presented) The identity recognition system of claim 22, wherein the operation of determining whether the response is allowable further comprises comparing the received response to a member of a set of two or more allowable responses.

36. (Previously presented) The identity recognition system of claim 35, wherein the set of allowable responses is computed before the determining operation is performed.

37. (Previously presented) The identity recognition system of claim 35, wherein the set of allowable responses is computed concurrently with the determining operation being performed.

38. (Previously presented) The identity recognition system of claim 22, wherein the determining operation further comprises generating a rating of the allowability of the response, based on the stored data value and one or more changes to the stored data values.

39. (Currently amended) The identity recognition system of claim 38, wherein the rating of the allowability of the response is based on a comparison of a data value upon which the response is based to one or more anticipated ~~predictable~~ changes to the stored data values associated with the identity to be recognized.

40. (Currently amended) The identity recognition system of claim 39, wherein the rating of the allowability of the response is varied based on whether the response is based at least in part on one or more anticipated ~~predicted~~ changes to the stored data values.

41. (Currently amended) The identity recognition system of claim 22, wherein the operation of recognizing that the presentation of ~~the~~ identity information by the computer is authentic provides a basis for one or more of: authenticating a device, authenticating a user, validating a software program or an application, providing data protection of data transmitted to or from a device, or generating a digital signature of a message digest.

42. (Previously presented) The identity recognition system of claim 22, wherein the response does not contain any data values reflecting personally identifiable information.

43. (Currently amended) An identity recognition system comprising:

a non-transitory memory storing information ~~data values~~ associated with one or more identities, wherein the information ~~data values~~ stored for an identity includes (a) data values associated with that identity; and (b) information regarding anticipated changes to one or more of the stored data values associated with that identity; ~~the one or more identities are based at least in part on information that is subject to change, the memory further storing information or instructions regarding one or more acceptable changes to the stored data values that are based at least in part on information that is subject to change;~~

one or more hardware processors in communication with the memory and configured to execute instructions to cause the identity recognition system to recognize that the presentation of ~~an~~ identity information by a computer is authentic, by performing operations comprising:

receiving, from the computer, one or more communications comprising an identity claim, wherein at least a portion of the identity claim is formed based on one or more data values from the computer, and wherein at least one of the data values used to form the identity claim corresponds to a stored data value ~~from the computer is based on information that is associated with the identity and that is subject to change~~; ~~and~~

determining whether the one or more communications received from the computer are sufficient to recognize that the identity claim is authentic, wherein such determining comprises ~~evaluating~~ using the stored information regarding anticipated changes to the stored data values to determine whether a data value used to form the identity claim is based on an acceptable change to a corresponding stored data value associated with the identity; and

recognizing that the presentation of identity information by the computer is authentic, according to whether the computer has provided an allowable response to the challenge.

44. (Currently amended) An identity recognition system comprising:

a non-transitory memory storing information ~~data values~~ associated with one or more identities, wherein the information ~~data values~~ stored for an identity includes (a) data values associated with that identity; and (b) information regarding anticipated changes to one or more of the stored data values associated with that identity; ~~the one or more identities are based at least in part on information that is subject to change, the memory further storing information or instructions regarding one or more acceptable changes to the stored data values that are based at least in part on information that is subject to change;~~

one or more hardware processors in communication with the memory and configured to execute instructions to cause the identity recognition system to recognize that the presentation by a computer of an identity to be recognized is authentic, by performing operations comprising:

receiving, from the computer, a communication based on one or more data values from the computer, wherein at least one of the data values upon which the communication is based corresponds to a stored data value for the identity ~~from the computer is based on information that is associated with the identity to be recognized and that is subject to change; and~~

determining whether the communication received from the computer is sufficient to recognize that the use of ~~an~~ the identity is authentic, wherein such determining comprises ~~evaluating~~ using the stored information regarding anticipated changes to the stored data values to determine whether a data value upon which the communication is based reflects an acceptable change to a corresponding stored data value associated with the identity ~~to be recognized~~; and

recognizing that the presentation of identity information by the computer is authentic, according to whether the computer has provided an allowable response to the challenge.

45. (New) The system of claim 22, further comprising using information from the allowable response to update the stored information regarding anticipated changes to the stored data values associated with the identity.

46. (New) The system of claim 22, further comprising using information from the allowable response to update the corresponding stored data value and the stored information regarding anticipated changes to the stored data values associated with the identity.

Allowable Subject Matter

Claims 22-46 are allowed.

The following is an examiner's statement of reasons for allowance:

Independent Claim(s) 22, 43, 44 and their respective dependent claims are allowable over prior arts since the prior arts taken individually or in combination fails to particular discloses, fairly suggest or render obvious the following italic limitations:

In claim(s) 22, 43 and 44:

"determining whether the response is allowable, wherein such determining comprises using the stored information regarding anticipated changes to the stored data values associated with the identity to determine whether a data value used to form the response is based on an acceptable change to a corresponding stored data value..." in combination with other limitations recited as specified in the independent claim(s).

The closest prior art of record teaches:

Buffam (Pat. No.: US 6,185,316 B1) teaches providing authenticating indicia and verifying the image thereby. One particular embodiment is a biometric application such as a fingerprint-based authentication system. The apparatus includes an image receiver for receiving the original image with true image point, a false image point generator providing false image points, and a transient template generator that selectively combines the true image points and the false image points.

Kang (Pub. No.: US 2011/0007177 Al) teaches imaging device that converts light of an image into an electrical signal, an image conversion unit that converts the electrical signal into image data, a scene recognition unit that recognizes the type of a scene to be photographed by analyzing the image data, a display unit that displays scene information regarding the recognized scene, a user input unit that receives user input, and a condition setting unit that locks a shooting condition as a shooting mode corresponding to the recognized type of the scene for photographing, according to the user input received via the user input unit.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAO HO whose telephone number is (571) 270-5998. The examiner can normally be reached on Monday thru Thursday 8:00am - 6:00pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, HADI ARMOUCHE can be reached on (571) 270-3618. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/DAO HO/
Primary Examiner, Art Unit 2497

Examiner-Initiated Interview Summary	**Application No.** 15/075,066	**Applicant(s)** MILLER ET AL.
	Examiner DAO HO	**Art Unit** 2497

All participants (applicant, applicant's representative, PTO personnel):

(1) *DAO HO*. (3)_____.

(2) *DAVID BOWLS*. (4)_____.

Date of Interview: *28 October 2016*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *22*.

Identification of prior art discussed: *Buffam, kang*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

The Applicant and The Examiner discussed the "determining…" limitation. The Examiner indicated that the current limitaton based on broadest reasonable interpretation indicated that if there is a match, then no further steps is necessary; thus, the subject to change is not invoke. The Examiner suggested to amend the limitation to indicate that the data values have to check for the changes. Agreement was reached.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/DAO HO/
Primary Examiner, Art Unit 2497

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 1166

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
15/075,066	03/18/2016 **RULE**	380	2497	47583.5US02

APPLICANTS

mSignia, Inc., Irvine, CA;

INVENTORS

Paul Timothy Miller, Irvine, CA;
George Allen Tuvell, Thompson's Station, TN;

** **CONTINUING DATA** *************************

This application is a CON of 14/458,123 08/12/2014 PAT 9294448
which is a CON of 13/366,197 02/03/2012 PAT 8817984
which claims benefit of 61/462,474 02/03/2011

** **FOREIGN APPLICATIONS** *************************

** **IF REQUIRED, FOREIGN FILING LICENSE GRANTED** ** ** SMALL ENTITY **

Foreign Priority claimed ❑ Yes ☑ No 35 USC 119(a-d) conditions met ❑ Yes ☑ No Verified and Acknowledged /DAO Q HO/ Examiner's Signature	❑ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	11	21	3

ADDRESS

HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219
UNITED STATES

TITLE

CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE

FILING FEE RECEIVED		
930	FEES: Authority has been given in Paper No.____________ to charge/credit DEPOSIT ACCOUNT No.____________ for following:	❑ All Fees ❑ 1.16 Fees (Filing) ❑ 1.17 Fees (Processing Ext. of time) ❑ 1.18 Fees (Issue) ❑ Other ________________ ❑ Credit

Search Notes	**Application/Control No.** 15075066	**Applicant(s)/Patent Under Reexamination** MILLER ET AL.
	Examiner DAO HO	**Art Unit** 2497

CPC- SEARCHED

Symbol	Date	Examiner
H04L36/0876	07/10/2016	dqh
H04L9/0861, 0866	07/10/2016	dqh
update	10/29/2016	

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner
380	255	07/10/2016	dqh
	update	10/29/2016	dqh

SEARCH NOTES

Search Notes	Date	Examiner
see attached EAST search history	07/10/2016	dqh
inventor and assignee search in EAST	07/10/2016	dqh
NPL: minutia authentication	07/10/2016	dqh
above searches update	10/29/2016	dqh

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
	general interference and searches of claim (PGPUB, USPAT)	10/29/2016	dqh

	/DAO HO/ Primary Examiner.Art Unit 2497

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S114	206	(hardware same firmware same software) and minutia	US-PGPUB; USPAT; USOCR	OR	ON	2016/10/29 10:42
S115	8	S114 and (challenge same triplet)	US-PGPUB; USPAT; USOCR	OR	ON	2016/10/29 10:42
S116	964	((Paul) near2 (Miller)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2016/10/29 10:43
S117	25	((George) near2 (Tuvell)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2016/10/29 10:43
S118	3	(mSignia).as.	US-PGPUB; USPAT; USOCR	OR	OFF	2016/10/29 10:43
S119	983	S118 S116 S117	US-PGPUB; USPAT; USOCR	OR	ON	2016/10/29 10:43
S120	6	S114 and S119	US-PGPUB; USPAT; USOCR	OR	ON	2016/10/29 10:43
S121	65	(plurality near2 minutia)	US-PGPUB; USPAT; USOCR	OR	ON	2016/10/29 10:47
S122	9	S121 and triplet	US-PGPUB; USPAT; USOCR	OR	ON	2016/10/29 10:47
S123	6	S122 AND ((H04L63/0876 OR H04L9/0861 OR H04L9/0866).CPC. OR (380/255).CCLS.)	US-PGPUB; USPAT; USOCR	OR	ON	2016/10/29 10:47
S124	45	("20060031676" | "20070240221" | "20080086676" | "20080086773" | "20080196104" | "20100229224" | "20110293094" | "6851316" | "8375221" | "20060104484" | "20080244744" | "20100027834" | "20130340052" | "7908662" | "20080267510" | "7333871" | "20100332400" | "20070240219" | "20070240222" | "20120201381" | "6041133" | "7373669" | "20140229386" | "20070240218" | "20080235515" | "20110093503" | "8335925" | "20070124801" | "20110296170" | "6185316" | "20080175449" | "20090138975" | "20090310779" | "20110113388" | "7330871" | "20070240217" | "8213907" | "20070174206" |	US-PGPUB; USPAT; USOCR	OR	ON	2016/10/29 10:47

		"20070214151" | "20070240220" | "20110082768" | "7937467" | "8312157" | "20110007177" | "7269160").PN.				
S125	34750	((minutia identit$3) with chang$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 10:48
S126	131	((minutia identit$3) with ((expect$3 anticipat$3) near5 chang$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 10:49
S127	9	((minutia) with ((expect$3 anticipat$3) near5 chang$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 10:50
S128	6	S114 and S126	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 10:50
S129	863	((minutia hardware firmware software) with ((expect$3 anticipat$3) near5 chang$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 10:51
S130	8	S129 and ((H04L63/0876 OR H04L9/0861 OR H04L9/0866).CPC. OR (380/255).CCLS.)	US-PGPUB; USPAT; USOCR	OR	ON	2016/10/29 10:51
S131	1565335	(device with valu$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 11:03
S132	72820	S131 and (user near2 (specific defin$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/10/29 11:03
S133	468	S132 and (know$3 near2 update$)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2016/10/29 11:03

			DERWENT; IBM_TDB			

S134	11	S133 AND ((H04L63/0876 OR H04L9/0861 OR H04L9/0866).CPC. OR (380/255).CCLS.)	US-PGPUB;
			USPAT;
			USOCR
				OR	ON	2016/10/29 11:03

S135	1	S124 and S129	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2016/10/29 11:30

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S136	28	(plurality near2 minutia).clm.	US-PGPUB; USPAT	OR	ON	2016/10/29 10:44
S137	5	S136 and (valu$3 with valid).clm.	US-PGPUB; USPAT	OR	ON	2016/10/29 10:44
S138	2825	((minutia identit$3) with chang$3).clm.	US-PGPUB; USPAT	OR	ON	2016/10/29 10:48
S139	14	((minutia identit$3) with ((expect$3 anticipat$3) near5 chang$3)).clm.	US-PGPUB; USPAT	OR	ON	2016/10/29 10:49
S140	296383	(device with valu$3).clm.	US-PGPUB; USPAT	OR	ON	2016/10/29 10:51
S141	2965	S140 and (user near2 (specific defin$3)).clm.	US-PGPUB; USPAT	OR	ON	2016/10/29 10:51
S142	3	S141 and (combin$5 near5 minutia).clm.	US-PGPUB; USPAT	OR	ON	2016/10/29 10:51
S143	33	((minutia hardware firmware fingerprint) with ((expect$3 anticipat$3) near5 chang$3)).clm.	US-PGPUB; USPAT	OR	ON	2016/10/29 11:26

10/29/2016 11:31:01 AM
C:\ Users\ dho1\ Documents\ EAST\ Workspaces\ 15075066.wsp

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15075066	MILLER ET AL.
	Examiner	**Art Unit**
	DAO HO	2497

CPC

Symbol	Type	Version
H04L 9 / 3271	F	2013-01-01
H04L 63 / 0861	I	2013-01-01
H04L 9 / 16	I	2013-01-01
H04L 9 / 3231	I	2013-01-01
H04L 9 / 3247	I	2013-01-01
H04L 63 / 0876	I	2013-01-01
H04L 9 / 0861	I	2013-01-01
H04L 9 / 0866	I	2013-01-01
H04L 9 / 0872	I	2013-01-01
H04L 63 / 0428	I	2013-01-01
/		
/		
/		
/		
/		

CPC Combination Sets

Symbol	Type	Set	Ranking	Version
/				
/				

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 25	
/DAO HO/ Primary Examiner.Art Unit 2497 (Primary Examiner)	10/29/2016 (Date)	O.G. Print Claim(s) 22	O.G. Print Figure 2B

Issue Classification	**Application/Control No.** 15075066	**Applicant(s)/Patent Under Reexamination** MILLER ET AL.
	Examiner DAO HO	**Art Unit** 2497

US ORIGINAL CLASSIFICATION

CLASS	SUBCLASS

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				

INTERNATIONAL CLASSIFICATION

CLAIMED					NON-CLAIMED				
H	0	4	L	29 / 06 (2006.01.01)					

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 25	
/DAO HO/ Primary Examiner.Art Unit 2497 (Primary Examiner)	10/29/2016 (Date)	O.G. Print Claim(s) 22	O.G. Print Figure 2B

Issue Classification	**Application/Control No.** 15075066	**Applicant(s)/Patent Under Reexamination** MILLER ET AL.
	Examiner DAO HO	**Art Unit** 2497

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** □ **T.D.** □ **R.1.47**

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		17	12	33										
	2		18	13	34										
	3		19	14	35										
	4		20	15	36										
	5		21	16	37										
	6	1	22	17	38										
	7	2	23	18	39										
	8	3	24	19	40										
	9	4	25	20	41										
	10	5	26	21	42										
	11	6	27	24	43										
	12	7	28	25	44										
	13	8	29	22	45										
	14	9	30	23	46										
	15	10	31												
	16	11	32												

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 25	
/DAO HO/ Primary Examiner.Art Unit 2497 (Primary Examiner)	10/29/2016 (Date)	O.G. Print Claim(s) 22	O.G. Print Figure 2B

Index of Claims	**Application/Control No.** 15075066	**Applicant(s)/Patent Under Reexamination** MILLER ET AL.
	Examiner DAO HO	**Art Unit** 2497

✓	**Rejected**		**-**	**Cancelled**		**N**	**Non-Elected**		**A**	**Appeal**
=	**Allowed**		**÷**	**Restricted**		**I**	**Interference**		**O**	**Objected**

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** □ **T.D.** □ **R.1.47**

CLAIM		**DATE**								
Final	Original	07/10/2016	10/29/2016							
	1	-	-							
	2	-	-							
	3	-	-							
	4	-	-							
	5	-	-							
	6	-	-							
	7	-	-							
	8	-	-							
	9	-	-							
	10	-	-							
	11	-	-							
	12	-	-							
	13	-	-							
	14	-	-							
	15	-	-							
	16	-	-							
	17	-	-							
	18	-	-							
	19	-	-							
	20	-	-							
	21	-	-							
1	22	✓	=							
2	23	✓	=							
3	24	✓	=							
4	25	✓	=							
5	26	✓	=							
6	27	✓	=							
7	28	✓	=							
8	29	✓	=							
9	30	✓	=							
10	31	✓	=							
11	32	✓	=							
12	33	✓	=							
13	34	✓	=							
14	35	✓	=							
15	36	✓	=							

U.S. Patent and Trademark Office

Part of Paper No. : 20161029

Index of Claims	Application/Control No. 15075066	Applicant(s)/Patent Under Reexamination MILLER ET AL.
	Examiner DAO HO	Art Unit 2497

✓	Rejected		-	Cancelled		N	Non-Elected		A	Appeal
=	Allowed		÷	Restricted		I	Interference		O	Objected

□ Claims renumbered in the same order as presented by applicant □ CPA □ T.D. □ R.1.47

CLAIM		DATE								
Final	Original	07/10/2016	10/29/2016							
16	37	✓	=							
17	38	✓	=							
18	39	✓	=							
19	40	✓	=							
20	41	✓	=							
21	42	✓	=							
24	43	✓	=							
25	44	✓	=							
22	45		=							
23	46		=							

U. S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(use as many sheets as necessary)*	*Complete if Known*	
	Application Number	15/075,066
	Filing Date	March 18, 2016
	Applicant(s)	mSignia, Inc.
	Art Unit	2497
	Examiner Name	Dao Q. Ho
SHEET 1 OF 1	Attorney Docket Number	47583.5US02

U. S. PATENT DOCUMENTS

Examiner's Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document

FOREIGN PATENT DOCUMENTS

Examiner's Initials	Cite No.	Foreign Patent Document (Country Code – Number – Kind)	Publication Date MM-DD-YYYY	Patentee or Applicant of Cited Document	Translation Y/N
	1.	JP2008516472	05-15-2008	KONIN-KLIJKE PHILIPS ELECTRONICS N.V.	Abstract only
	2.	JP2009111971	05-21-2009	Mitsubishi Electric Research Laboratories Inc.	Y

NON-PATENT LITERATURE DOCUMENTS

Examiner's Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article, title of the item, date, page(s), volume-issue number(s), publisher, city/country where published
	3.	MAEDA, Takashi, "Biometrics complex authentication system capable of realizing accurate, rapid identity authentication instantly," Monthly Bar Code, August 2, 2001, pp. 64-66, Vol. 14, Issue 9, Japan Industrial Publishing Co., Ltd., Japan.
	4.	SHIBATA, Yoichi, "Mechanism-based PKI," Computer Security Symposium, October 29, 2003, Vol. 2003, No. 15, pp. 181-186, Information Processing Society of Japan, Japan.
	5.	JUELS et al., "A Fuzzy Vault Scheme," Designs, Codes and Cryptography, February 2006, pp. 237-257, Vol. 38, No. 2, Springer Science + Business Media, Inc., New York/USA.
	6.	Notice of Reasons for Rejection dated September 6, 2016, Japanese Patent Application No. P2014/555571.

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

Espacenet

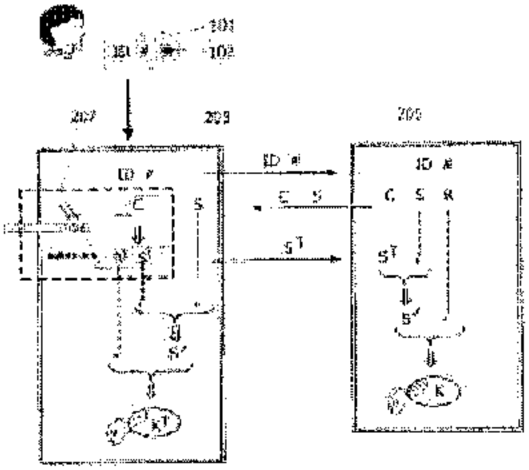
Bibliographic data: JP2008516472 (A) — 2008-05-15

TWO-WAY ERROR CORRECTION FOR PHYSICAL TOKENS

Inventor(s):	
Applicant(s):	
Classification:	- international: ***H04L9/32*** - cooperative: **H04L9/0838; H04L9/3234; H04L9/3278;** H04L2209/34
Application number:	JP20070534170 20051004
Priority number (s):	EP20040104842 20041004 ; WO2005IB53255 20051004
Also published as:	WO2006038183 (A1) US2009183248 (A1) KR20070058581 (A) EP1800433 (A1) CN101036340 (A)

Abstract not available for JP2008516472 (A)
Abstract of corresponding document: WO2006038183 (A1)

The invention relates to a method of establishing a shared secret between two or more parties, based on a physical token, wherein helper data from both the enrolment and the authentication measurement is used in such a way that only response data reliable at both measurements is used to generate the shared secret. The generated shared secret is therefore identical to both parties to a high degree of certainty. The invention further relates to a system for generating such a shared secret, comprising a central database server and a terminal, or any one of them.



(19)日本国特許庁(JP)　(12)公 表 特 許 公 報(A)　(11)特許出願公表番号
特表2008-516472
(P2008-516472A)
(43)公表日　平成20年5月15日(2008.5.15)

(51)Int.Cl.	F I	テーマコード（参考）
H04L 9/32 (2006.01)	H04L 9/00 675A	5J104

審査請求 未請求　予備審査請求 未請求　（全 15 頁）

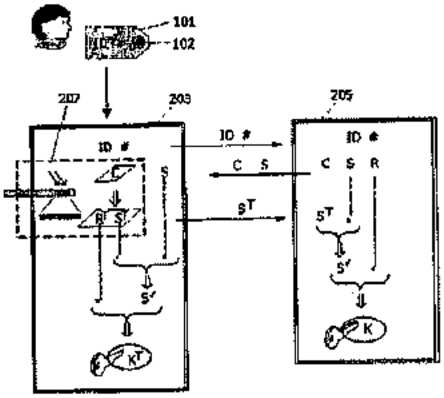
(21)出願番号	特願2007-534170 (P2007-534170)
(86)(22)出願日	平成17年10月4日 (2005.10.4)
(85)翻訳文提出日	平成19年4月3日 (2007.4.3)
(86)国際出願番号	PCT/IB2005/053255
(87)国際公開番号	WO2006/038183
(87)国際公開日	平成18年4月13日 (2006.4.13)
(31)優先権主張番号	04104842.2
(32)優先日	平成16年10月4日 (2004.10.4)
(33)優先権主張国	欧州特許庁(EP)

(71)出願人　590000248
コーニンクレッカ　フィリップス　エレクトロニクス　エヌ　ヴィ
オランダ国　５６２１　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　1
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(74)代理人　100107766
弁理士　伊東　忠重
(72)発明者　テュイルス，ピム　テー
オランダ国，５６５６　アーアー　アインドーフェン，プロフ・ホルストラーン　６

最終頁に続く

(54)【発明の名称】物理トークンのための二側誤り訂正

(57)【要約】
本発明は、物理トークンに基づいて、２以上の当事者の間で共有される秘密を確立する方法に関する。本方法では、登録および認証測定の両方からのヘルパーデータを使用して、両測定での信頼できるレスポンスデータだけが共有される秘密の生成に使われるようにする。したがって、生成された共有される秘密は高い確度をもって両当事者にとって同一である。本発明はさらに、そのような共有される秘密を生成する、中央データベースサーバーおよび諸端末またはそれらのうちのいずれか一つを有するシステムに関する。



【特許請求の範囲】

【請求項1】

証明者と検証者の間で、チャレンジをもってチャレンジされるとレスポンスを生成する物理トークンに基づいて共有される秘密を生成する方法であって、前記検証者は前記物理トークンにチャレンジするための一つまたは複数のチャレンジならびに該一つまたは複数のチャレンジの各チャレンジについて検証者固有レスポンスおよび検証者固有レスポンス信頼度情報を含む登録データへのアクセスを有しており、当該方法が：

・前記一つまたは複数のチャレンジからあるチャレンジを選択し、該選択されたチャレンジを送信して、前記証明者と前記検証者の両方が前記選択されたチャレンジへのアクセスを有するようにする段階と；

・前記選択されたチャレンジをもって物理トークンにチャレンジして証明者固有レスポンスを得て、その得られた証明者固有レスポンスから証明者固有レスポンス信頼度情報を導出する段階と；

・前記証明者におよび／または前記検証者に情報を送信して、前記証明者および前記検証者のうちの少なくとも一方が前記証明者固有レスポンス信頼度情報および前記検証者固有レスポンス信頼度情報にアクセスできるようにする段階と；

・前記証明者および前記検証者のうちの前記少なくとも一方において、前記証明者固有レスポンス信頼度情報、前記検証者固有レスポンス信頼度情報ならびに前記証明者固有レスポンスまたは前記検証者固有レスポンスに基づいて、前記共有される秘密を生成する段階
、
とを有する方法。

【請求項2】

前記証明者と前記検証者との間の前記共有される秘密に関係する情報を送信して、前記証明者および前記検証者のいずれもが前記共有される秘密を決定できるようにする段階をさらに有する、請求項１記載の方法。

【請求項3】

前記情報を送信する段階が、前記証明者固有ヘルパーデータを前記証明者から前記検証者に送信することを含んでおり、前記共有される秘密が前記検証者において生成される、請求項１記載の方法。

【請求項4】

前記情報を送信する段階が、前記検証者固有ヘルパーデータを前記検証者から前記証明者に送信することを含んでおり、前記共有される秘密が前記証明者において生成される、請求項１記載の方法。

【請求項5】

前記得られた証明者固有レスポンスから証明者固有レスポンス信頼度情報を導出する段階が、補助装置にアウトソーシングされる、請求項１記載の方法。

【請求項6】

前記登録データが暗号化された登録データを含み、当該方法がさらに前記暗号化された登録データを復号する段階をさらに有する、請求項１記載の方法。

【請求項7】

前記暗号化された登録データを復号する段階が第三者にアウトソーシングされる、請求項６記載の方法。

【請求項8】

前記共有される秘密が前記証明者と前記検証者の間で認証のために使われる、請求項１記載の方法。

【請求項9】

前記共有される秘密が識別のために使われる、請求項１記載の方法。

【請求項10】

前記共有される秘密が前記証明者と前記検証者の間の安全な通信のために使われる、請

求項１記載の方法。

【請求項11】

前記物理トークンがPUFである、請求項１記載の方法。

【請求項12】

前記物理トークンが光学式識別体（identifier）であり、前記チャレンジが入射光ビームである、請求項１記載の方法。

【請求項13】

物理トークンに基づいて共有される秘密を生成する、伝送手段によって互いに接続された二つの装置、証明装置と検証装置を有するシステムであって、前記物理トークンはチャレンジをもってチャレンジされるとレスポンスを生成し、前記検証装置は一つまたは複数のチャレンジならびに該一つまたは複数のチャレンジの各チャレンジについて検証者固有レスポンスおよび検証者固有レスポンス信頼度情報を含む登録データへのアクセスを有しており、当該システムが：

・前記一つまたは複数のチャレンジからあるチャレンジを選択する選択手段および該選択されたチャレンジを送信して前記証明者と前記検証者の両方が前記選択されたチャレンジへのアクセスを有するようにするユニットと；

・前記選択されたチャレンジをもって物理トークンにチャレンジして証明者固有レスポンスを得るため、および該証明者固有レスポンスを検出するための、証明装置内の、それぞれチャレンジ手段および検出手段と；

・前記得られた証明者固有レスポンスから証明者固有レスポンス信頼度情報を導出するレスポンス信頼度計算手段と；

・前記二つの装置のうちの少なくとも一方が前記証明者固有レスポンス信頼度情報および前記検証者固有レスポンス信頼度情報にアクセスできるようにする、前記二つの装置の間で情報を送信するための一つまたは複数のユニットと；

・前記証明者固有レスポンス信頼度情報、前記検証者固有レスポンス信頼度情報ならびに前記証明者固有レスポンスまたは前記検証者固有レスポンスに基づいて、前記共有される秘密を生成する共有秘密計算手段、

とを有するシステム。

【請求項14】

チャレンジをもってチャレンジされるとレスポンスを生成する物理トークンに基づいて、共有される秘密を生成するためのシステムにおいて使用する証明装置であって、前記システムは当該証明装置のほかに当該証明装置に伝送手段によって接続された検証装置を有しており、当該証明装置が：

・一つまたは複数のチャレンジからあるチャレンジを選択する選択手段または選択されたあるチャレンジを受信するユニットと；

・前記選択されたチャレンジをもって物理トークンにチャレンジして証明者固有レスポンスを得るため、および該証明者固有レスポンスを検出するための、それぞれチャレンジ手段および検出手段と；

・前記得られた証明者固有レスポンスから証明者固有レスポンス信頼度情報を導出するレスポンス信頼度計算手段と；

・前記検証装置から前記選択されたチャレンジに対応する検証者固有レスポンス信頼度情報を受け取るユニットと；

・前記証明者固有レスポンス、前記証明者固有レスポンス信頼度情報および前記検証者固有レスポンス信頼度情報に基づいて、前記共有される秘密を生成する共有秘密計算手段、

とを有する装置。

【請求項15】

チャレンジをもってチャレンジされるとレスポンスを生成する物理トークンに基づいて、共有される秘密を生成するためのシステムにおいて使用する検証装置であって、前記システムは当該検証装置のほかに当該検証装置に伝送手段によって接続された証明装置を有しており、当該検証装置が：

・一つまたは複数のチャレンジからあるチャレンジを選択する選択手段または選択されたあるチャレンジを受信するユニットと；
・前記一つまたは複数のチャレンジならびに前記一つまたは複数のチャレンジの各チャレンジについて検証者固有レスポンスおよび検証者固有レスポンス信頼度情報を含む登録データにアクセスする手段と；
・前記証明装置から、前記選択されたチャレンジに対応する証明者固有レスポンス信頼度情報を受信するユニットと；
・前記選択されたチャレンジに対応する検証者固有レスポンス、前記証明者固有レスポンス信頼度情報および前記検証者固有レスポンス信頼度情報に基づいて、前記共有される秘密を生成する共有秘密計算手段、
とを有する装置。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、安全なトランザクションにおける識別、認可および暗号の目的のために、物理トークンに基づいて、２以上の当事者の間で共有される秘密、特に物理的複製不能関数（PUF: Physical Uncloneable Function）を確立する方法に関する。本発明はさらに、そのような共有される秘密を生成する、証明装置および検証装置を有するシステムに関する。本発明はまた、前記証明装置および前記検証装置にも関する。

【背景技術】

【0002】

識別、認証および暗号化／復号鍵生成のための物理トークンの使用は当技術分野において知られている。トークンはたとえばスマートカードに埋め込まれ、安全なトランザクションにおいて使用されることができる。そのようなカードをユーザーに発行する前に、トークンは「登録段階」と呼ばれる段階で登録され、その際、一つまたは複数のチャレンジ〔誰何〕を受ける。チャレンジおよび対応するレスポンス〔応答〕はそのトークンを識別する情報と一緒に、可能性としては他のデータも一緒に保存され、「登録データ」をなす。「認証段階」と呼ばれる段階でユーザーがスマートカードを使うときは、そのトークンの素性は、そのトークンを識別する情報に対応する保存されているチャレンジのうちの一つまたは複数を用いてそのトークンにチャレンジすることによって検証される。得られる単数または複数のレスポンスが登録データに保存されている単数または複数のレスポンスと同じであれば、識別は成功である。いくつかのプロトコルでは、このチャレンジ・レスポンス手順は、トークンの物理的出力をビット列に変換する何らかの処理操作によってレスポンスから導出される共有される秘密をも生じる。するとこの共有される秘密は二者間の安全なトランザクションのためのセッション鍵として使うことができる。

【0003】

物理トークンには多くの例がある：平面ファイバー分布（planar fiber distributions）（たとえばIEEE ISIT Conference 2004の講演集録 p.173において参照されているような）、すべてのバイオメトリクスそして特に物理的複製不能関数（PUF）である。「物理トークン」とは、一般に、メモリアクセス以外の手段によって探査され、その応答が当該オブジェクトの物理的構造に依存するような物理的オブジェクトであると理解される。物理トークンの処理されていない直接的な応答はアナログでもデジタルでもよい。その応答を処理してデジタルビット列を得ることができる。これに対し、デジタルトークンは、与えられたチャレンジの組に対するレスポンス、たとえば各アドレスにおいて書き込まれたビット列を保存したデジタルメモリからなる。

【0004】

PUFは物理的ランダム関数または物理的一方向性関数としても知られている。米国特許2003/0,204,743は、一意的な測定可能特性をもつデバイスを認証目的で測定モジュールと一緒に使用することを記載している。３Ｄ構造、探査および比較に基づくもう一つの認証方法は、米国特許6,584,214において記載されている。一般に、PUFは複製がきわめて困難

な物理トークンである。ここで、「複製（cloning）」とは、(i)物理的なコピーの作成または(ii)その振る舞いをまねるコンピュータモデルの作成でありうる。PUFは多数のランダムに分布した構成要素を有する複雑な物理系である。好適なチャレンジで探査されると、PUFとチャレンジとの間の相互作用を支配する複雑な物理、たとえば乱れた媒質中での波動の多重散乱などが、各個別のチャレンジについてランダムに見える出力すなわちレスポンスを導く。PUFの複雑な小スケールの構造が物理的なコピー作成を難しくする一方、物理的な相互作用の複雑さはコンピュータによるモデル化を阻む。たとえば、光学式PUFは多数のランダムに分布した散乱体を含んだ光学媒質でありうる。チャレンジは入射ビームなどであり、その場合、レスポンスは検出器上で検出される結果としてのスペックルパターンとなる。明暗のスポットのパターンがビット列に変換できる。

【0005】

デジタルトークンに対し、あらゆる物理トークンに関する問題は、応答がノイズの影響を受けやすいということである。測定ノイズには多くの原因がありうる。たとえばトークン／検出器の整列乱れ、あるいは温度、湿気および振動のような環境の効果である。ノイズのため、レスポンスから引き出されるビット列が誤差を有しうる。たいていの暗号プロトコルは認証段階の間に得られたビット列が登録段階の間に得られたものと厳密に等しいことを要求する。たとえば、ビット列が暗号化鍵として使われる場合、鍵のうち１ビットでも反転すれば、認識できない役に立たない結果を生じる。

【0006】

当技術分野において知られている二つの方法が、上記の問題を少なくとも部分的に改善するために使用できる。

【0007】

一つの方法は、ビット列の全長のある割合に等しい数のビット誤りを検出および訂正することのできる誤り訂正符号の使用である。しかしながら、そのような符号の使用はビット列抽出のプロセスに負担を課すもので、訂正できる誤りの数とともに増大する。

【0008】

もう一つの方法は、レスポンス信頼度情報（response reliability information）の使用である。レスポンス信頼度情報は当技術分野において「ヘルパーデータ（helper data）」または副情報（side information）としても知られる。一般に、レスポンス信頼度情報は、対応するチャレンジおよびレスポンスと一緒に保存されている追加的な情報からなり、これによりビット列抽出プロセスの堅牢性が改善できる。たとえば、レスポンス信頼度情報は、アナログ形またはデジタル化された形でのレスポンスの信頼できる部分、すなわちノイズによる影響を受けていなさそうな部分を指すポインタからなっていてもよい。認証の際、レスポンス信頼度情報は、物理的出力のある部分をビット列抽出プロセスのための成分として選択するために、あるいはいくつかの部分に他の部分よりも高い重みを与えるために、あるいは信頼性のない部分を破棄するために使われる。

【0009】

レスポンス信頼度情報と誤り訂正符号の方法を組み合わせることも可能である。

【0010】

レスポンス信頼度情報の方法の欠点は、「信頼性」という属性の割り当てが登録段階しか反映していないということである。その時点では、認証の際に生じるノイズの属性はわかっていない。多くの応用では、レスポンスデータは、登録の際には認証の際とは異なる試験ステーションで得られる。各試験ステーションはその固有の摂動および整列乱れを有する。さらに、スマートカードなどトークンの多くの応用では、認証の際には多数の試験ステーションから選ぶことができるので、ユーザーが使用する試験ステーションの特性を予期することは不可能である。最後に、上述したような環境の効果もノイズを生じるので、データの信頼性は同じ試験ステーションでも測定ごとに変わりうる。よって、登録の際に信頼できるとラベル付けされたビットが認証の際には実際には反転してしまい、その結果、二者間での共通の共有された秘密を生成することに失敗する確率が相変わらずかなりある。

【発明の開示】

【発明が解決しようとする課題】

【0011】

　したがって、二者間で共有される秘密を生成するより堅牢な方法を提供することが本発明の目的である。

【0012】

　そのような共有される秘密を生成する、証明装置および検証装置を有するより堅牢なシステムを提供し、前記証明装置および前記検証装置を提供することが本発明のさらなる目的である。

【課題を解決するための手段】

【0013】

　本発明によれば、第一の目的は請求項によって定義される方法によって達成される。

【0014】

　この方法では、証明者固有のレスポンス信頼度情報を、検証者固有のレスポンス信頼度情報と組み合わせて使用することで、証明者固有レスポンスおよび／または検証者固有レスポンスから共有された秘密を生成する。その結果、共有される秘密を不揃いに生成してしまう、すなわち共有される秘密を生成し損なう確率は著しく低下する。

【0015】

　換言すれば、本発明によれば、ヘルパーデータの二側（two-way）使用が採用されるのである。

【0016】

　本発明に基づく方法のある実施形態によれば、両当事者が証明者固有レスポンス信頼度情報および検証者固有レスポンス信頼度情報へのアクセスを有し、両当事者が共有される秘密を生成する。ある代替的な実施形態では、一当事者のみが証明者固有レスポンス、証明者固有レスポンス信頼度情報および検証者固有レスポンス信頼度情報へのアクセスを有し、したがって共有される秘密を生成できる。この場合、共有される秘密を生成した当事者は他方の当事者に共有される秘密に関係した情報を送信し、他方の当事者も共有される秘密を判別できるようにする。

【0017】

　前記の共有される秘密に関係した情報は、レスポンスのうち、証明者固有レスポンス信頼度情報および検証者固有レスポンス信頼度情報の両方によって信頼できるとマークされているある部分へのポインタで、それに基づいて鍵が生成されるのでもよい。

【0018】

　本発明は以下の効果を有する：

・同じ物理的測定から、従来技術よりも信頼できる形でより長い識別ストリングを構築することが可能であり、識別番号のより大きな範囲が提供される；

・同じ物理的測定から、従来技術よりも長い暗号鍵を構築することが可能であり、セキュリティが改善される；

・従来技術と同じ鍵長を保ちながら今では改良されたノイズ許容度をもつことが可能である；

・前記の改良されたノイズ許容度によりトークンおよび測定装置についてのコスト削減が可能になる。

【0019】

　本発明のある実施形態では、共有される秘密の大きさは柔軟でありうる。前記二つのヘルパーデータが組み合わされたのち、共有される秘密の大きさが予見されたものとは実質的に異なるということが起こりうる。すると両当事者は使用すべき鍵の大きさを交渉し、一緒に、事前に定められたものとは異なるある鍵長を決定できる。物理トークンを含んでいるスマートカードの所有者が関与してもよい。たとえば、該所有者に若干短いセッション鍵を許容できるかどうかを尋ねてもよい。

【0020】

さらに、誤り訂正符号は使用されたとしても従来ほど複雑ではなく、堅牢だが単純な誤り訂正方式を与える。

【0021】

本発明によってビット列の導出における誤りの期待数が低減されるので、誤り訂正符号による誤り訂正の計算努力がさらに低減され、線形以上の計算に関する利点がある。このように、二側ヘルパーデータの誤り訂正符号との組み合わせにより、２つの部分の単なる合計以上の利点が得られるのである。

【0022】

誤り確率の違いの簡単な例として、標準偏差σの単一のガウス分布の変数を考えることができる。第一の測定（登録）によって絶対値が何らかの閾値Tより大きいある値fが与えられる場合に、その変数は「堅牢」と見なされる。そのような堅牢な変数を与えられると、第二の測定においてビット反転が起こる確率は、従来技術の方法（一側（one-way）ヘルパーデータ）によれば、第二の測定がfとは符号が反対の数Fを与える確率に等しい。この確率は次式で与えられる。

【0023】

ErrorProb(一側)＝(1/2)[1−Erf(f/2σ)]

しかし、本発明に基づく二側データ法を使う場合は、ビット反転の確率は、Fが逆符号をもつだけでなく、その絶対値が前記閾値Tより大きくもある確率

ErrorProb(二側)＝(1/2)[1−Erf((f−T)/2σ)]

に等しい。以下の諸例のようにσより大きい閾値Tを選ぶのが論理的である。T＝1.5σでfがその閾値よりやや上だとすると、一側法は14%の誤り確率をもつが、二側法の誤り確率はたった2%である。T＝2σについては、割合は8%対0.2%となる。いずれの場合にも、本発明は誤り確率の劇的な低下をもたらす。

【0024】

最後に、証明者と検証者の間の通信チャネルは公開チャネルであると想定される。本発明に基づいて交換されるあらゆる情報は開かれた公開チャネル上を危険なしにやりとりされることができる。情報の量および種類は、第三者が何らかの秘密を暴いたり、秘密のビット列のコピーを生成したりするには不十分なのである。さらに、一般にさらされる情報の量（高々：チャレンジの型と二組のヘルパーデータ）は二当事者が共同の秘密を決定できるようにするのにちょうど十分なものである。

【0025】

異なる諸実施形態では、共有される秘密は前記二者間での識別、認可または安全な通信のために使用される。

【0026】

本発明はさらに、証明者および検証者における処理ユニットをしてそれぞれ上記の方法を実行せしめるための命令が記憶されたコンピュータ可読媒体に関する。

【0027】

本発明に基づく方法のさまざまな実施形態は従属請求項において定義される。

【0028】

本発明によれば、前記さらなる目的は請求項によって定義されるシステム、請求項によって定義される証明装置および請求項によって定義される検証装置によって達成される。

【0029】

選択手段は証明装置または検証装置または第三者のいずれに位置していてもよい。

【0030】

選択手段とは独立に、レスポンス信頼度計算手段は証明装置または第三者のいずれかに位置していてよい。

【0031】

選択手段およびレスポンス信頼度計算手段とは独立に、共有秘密計算手段は証明装置および検証装置のいずれかもしくは両方に、あるいは第三者に位置していてもよい。ある実施形態では、レスポンス信頼度計算手段および共有秘密計算手段は、証明装置の一部とし

て一体であるか、または第三者に位置している。

【0032】

本発明の好ましい実施形態についてこれから図面を参照しつつ説明する。

【発明を実施するための最良の形態】

【0033】

図１は、本発明に基づく物理トークンの登録またはブートストラップ段階を示している。物理トークン１０２は図においてID#と称されている識別タグとともに試験装置１０５に挿入され、一連のチャレンジC_iを受ける。ここで、添え字iはチャレンジ番号である。本発明のある実施形態では、物理トークンはスマートカード１０１に埋め込まれている。例として、物理トークンはPUF、たとえば再現不能な散乱体をもつ3D不均一媒体からなっていてもよい。チャレンジは、入射角、波長などの何らかのパラメータによって識別される入射ビーム１０６である。

【0034】

理論上は、物理トークンをチャレンジする方法は非常に多数ありうる。しかしながら、実際上は、登録の際に物理トークンが受けるチャレンジの数はむしろ、たとえば数百のオーダーである。それは主に二つの理由によるもので、第一に、物理的測定に費やされる時間を短縮するため、そして第二に、必要な記憶容量を合理的な範囲で低レベルに保つためである。したがって、チャレンジは必要な数だけなされうる。さらに、スマートカード上のデータはいつでも更新でき、新しいチャレンジの組を物理トークンに対してなすことができる。

【0035】

物理トークンをチャレンジする各チャレンジC_iについて対応するレスポンスR_iが検出され、登録固有の副情報S_i（ヘルパーデータ・レスポンス信頼度情報とも呼ばれる）が導出される。登録固有ヘルパーデータS_iは、信頼できるデータと信頼できないデータについての情報を含む。試験がPUFの照射である例では、レスポンスは2Dスペックルパターンをフィルタ処理してビット列としたものでありうる。ここで、各ビットは特定の位置における光強度を表す。その際、ヘルパーデータは、レスポンスにおける、信頼できるデータを含んでいるビット、たとえば光強度が確実に低または確実に高である位置に対応するビットへのポインタの組からなる。ヘルパーデータはレスポンスのマスクの形をとってもよい。レスポンスのマスクとはすなわち、レスポンスを表すビット列と同じビット数をもち、「1」がレスポンス中の対応するビットが信頼できることを示し、「0」が信頼できないことを示すようなビットの配列である。

【0036】

最後に、共同して登録データをなす物理トークンの識別情報ID#、チャレンジC_i、対応する検出されたレスポンスR_iおよび副情報S_iがデータベースサーバー１０３に保存され、その後の認証段階の間に検証装置によってアクセスできるようになる。データは、チャレンジならびに対応するレスポンスおよびヘルパーデータが物理トークンの識別情報ID#にリンクされているように格納されるので、これらのデータはのちにトークンの識別情報だけから引き出せる。

【0037】

応用によっては、中央データベースは存在しないことも可能である。チャレンジ・レスポンス・データは完全に、または部分的にスマートカード上に必要なら暗号化された形で保存されてもよい。代替的に、チャレンジおよびレスポンスのデータは数多くの異なるデータ担体に分散されてもよい。

【0038】

図２は、本発明の 一つの実施形態に基づく証明装置２０３および検証装置２０５を用い、二側誤り訂正方式を使って二当事者がどのように共通かつ秘密の鍵Kを得るかを示している。識別情報ID#および物理トークン１０２を含むスマートカード１０１が証明装置２０３または端末において使用される。ID#が検証装置２０５に送られる。検証装置はたとえば、物理トークンの登録段階での保存された全測定すなわち登録データを含んでいるか

、該登録データへの直接アクセスを有するかする中央データベースサーバーである。ID#はこれらの測定にリンクされており、測定のうちから保存されているチャレンジの一つCが選ばれて、対応するサーバー固有副情報Sとともに、開かれた公開通信チャネル上で端末に送り返される。端末（terminal）では、図２で破線で示されている測定／試験ステーション２０７において物理トークン１０２に対してチャレンジCが実行され、対応する端末固有レスポンスR^Tおよび端末固有副情報S^Tが得られる。一般に、測定ステーション２０７は、図１のブートストラップ段階で使われたものとは異なっている。端末固有副情報S^Tは、登録の際に用いられたのと同じ手順をヘルパーデータ抽出に使うことで得られる。物理的な測定におけるノイズならびに試験装置における可能性のある不正確さのため、レスポンスR^Tはおそらくは登録段階で最初に測定されたRと同じではない。端末２０３による使用の際に生成されたレスポンスR^Tに関する端末固有副情報S^Tがデータベースサーバー２０５に送り返される。端末２０３およびデータベースサーバー２０５のいずれのシステムでも、二組のヘルパーデータ、すなわちサーバー固有のSおよび端末固有のS^Tが組み合わされて、両システムに共通の組み合わされたヘルパーデータS´を生じる。最後に、両当事者は共通の手順を使って秘密鍵を生成する。サーバーはKをRおよびS´から生成する。端末はK^TをR^TおよびS^Tから生成する。非常に高い確率で、KおよびK^Tは同一である。というのも、これらは今や両当事者によって信頼できると見出されている物理的出力の部分に基づいているからである。

【0039】

本発明のある実施形態によれば、鍵長は柔軟でありうる。両当事者がS´を知っているとき、両者は共同して事前に定められたのとは異なるある鍵長を決定することができる。使用後、鍵Kは破棄され、前記のチャレンジCはこの特定の物理トークンに対しては二度と使用されない。

【0040】

上述した二側ヘルパーデータの使用は、何らかの種類の誤り訂正符号と組み合わせて、共有される秘密におけるビット誤りの確率をさらに低下させることもできる。

【0041】

広い意味では、本発明は端末およびデータベースサーバーをカバーするのみならず、より一般に物理トークンをもつ証明者および検証者をもカバーする。

【0042】

やはり図１に関連して述べたように、本発明によれば、登録データは全くどこに存在していてもよい。たとえばトークンのすぐ隣のスマートカード上（必要なら暗号化された形で）、あるいは種々の記憶媒体（たとえばインターネットを介してオンラインでアクセスできるもの）にわたって分散して存在していてもよい。一つの有望な選択肢は、端末とスマートカードだけを残して中央サーバーの必要をなくすことである。同様に、チャレンジはどこに保存されていてもよく、検証者がもっていなくてもよい。本発明によれば、検証者はチャレンジについてすべてを知っている必要はない。

【0043】

さらに、証明者または端末は新しい端末固有ヘルパーデータをその文字通りの形で送る必要はない。証明者はたとえば、検証者がS^TまたはS´を導出できるようにするS´またはS^Tの任意の関数を送るのでもよい。

【0044】

本発明によれば、端末または証明者はほとんど計算資源をもたないことも可能である。この場合、端末または証明者はいくぶん生のままのレスポンスデータをサーバーに送ることができ、サーバーがヘルパーデータの第二の組を計算して端末にS^TまたはS´の結果について伝えるようになる。このすべては、適正な暗号化が用いられていれば、安全な方法で行える。

【0045】

上述した場合では、本発明は生のデータの前処理を含んでいて、サーバーに送られるデータが扱いやすいサイズになるようにしてもよい。

【0046】

本発明のさらに別の実施形態では、認証の際のヘルパーデータの抽出は登録からのヘルパーデータに依存しうる。これはいかなる種類の関数の依存性でもよい。

【0047】

本発明のあるさらなる実施形態では、検証者固有ヘルパーデータを生成するために使われた閾値は、証明者固有のヘルパーデータの抽出に関して助けるために証明者によってアクセスされうる。

【0048】

上記の諸実施形態は本発明を限定するのではなく解説するものであり、当業者は付属の請求項の範囲から外れることなく数多くの代替的な実施形態を設計できるであろうことは注意しておくべきである。

【0049】

請求項において、括弧内に参照符号があったとしてもその請求項を限定するものと解釈してはならない。動詞「有する」およびその活用形の使用は請求項において述べられているもの以外の要素またはステップの存在を排除しない。要素の単数形の表現はそのような要素の複数の存在を排除しない。本発明は、いくつかの相異なる要素を有するハードウェアによって、および好適にプログラミングされたコンピュータによって実装されてもよい。いくつかの手段を列挙している装置請求項においては、それらの手段のいくつかが同一のハードウェア項目によって具現されてもよい。ある種の施策が互いに異なる従属請求項において言及されているというだけの事実がそれらの施策の組み合わせが有利に使用できないことを示すものではない。

【図面の簡単な説明】

【0050】

【図1】PUFカードのための登録すなわちブートストラップ段階を示す図である。

【図2】本発明に基づく二側誤り訂正方式に基づく、PUFカードの使用の際のPUFのチャレンジ、情報の流れおよびセッション鍵生成を示す図である。

【図1】

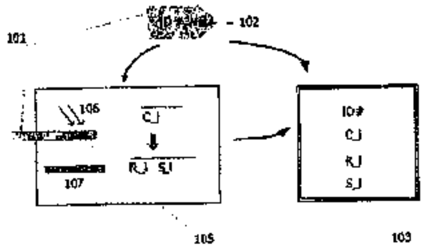


FIG.1

【図2】

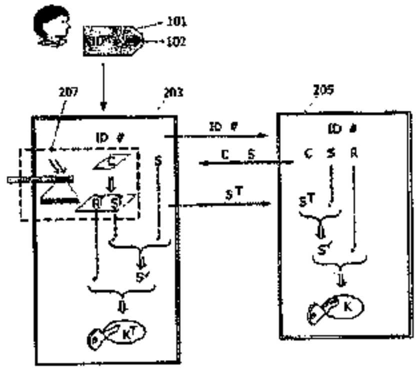
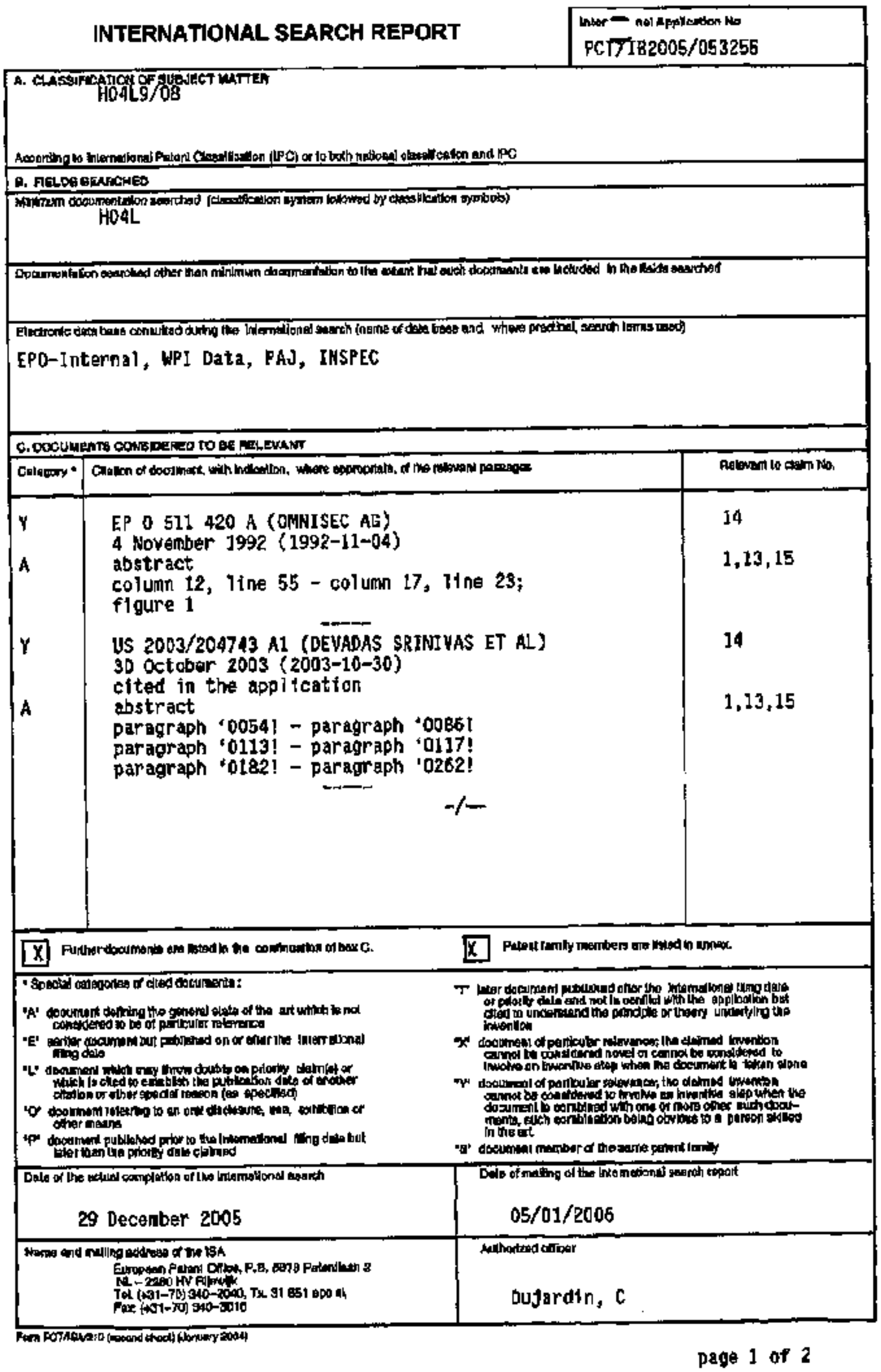


FIG.2



INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB2005/053256

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 511 420 A (OMNISEC AG) 4 November 1992 (1992-11-04)	14
A	abstract column 12, line 55 - column 17, line 23; figure 1	1,13,15
Y	US 2003/204743 A1 (DEVADAS SRINIVAS ET AL) 30 October 2003 (2003-10-30) cited in the application	14
A	abstract paragraph '0054! - paragraph '0086! paragraph '0113! - paragraph '0117! paragraph '0182! - paragraph '0262!	1,13,15

-/--

☒ Further documents are listed in the continuation of box C.　　☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

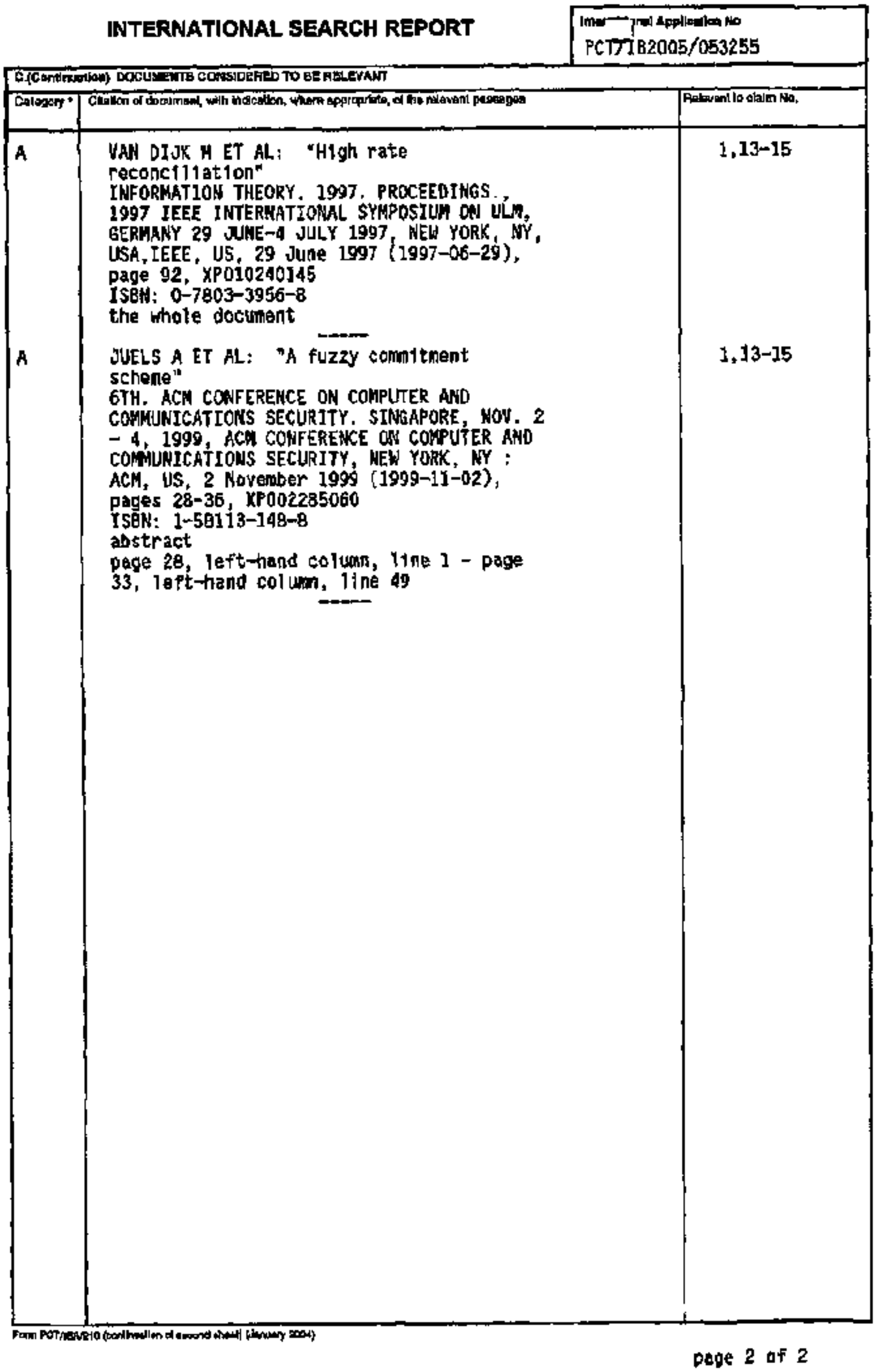
"&" document member of the same patent family

Date of the actual completion of the international search 29 December 2005	Date of mailing of the international search report 05/01/2006
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Dujardin, C

2

Form PCT/ISA/210 (second sheet) (January 2004)

page 1 of 2



INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB2005/053255

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	VAN DIJK M ET AL: "High rate reconciliation" INFORMATION THEORY. 1997. PROCEEDINGS., 1997 IEEE INTERNATIONAL SYMPOSIUM ON ULM, GERMANY 29 JUNE-4 JULY 1997, NEW YORK, NY, USA,IEEE, US, 29 June 1997 (1997-06-29), page 92, XP010240145 ISBN: 0-7803-3956-8 the whole document	1,13-15
A	JUELS A ET AL: "A fuzzy commitment scheme" 6TH. ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY. SINGAPORE, NOV. 2 - 4, 1999, ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, NEW YORK, NY : ACM, US, 2 November 1999 (1999-11-02), pages 28-36, XP002285060 ISBN: 1-58113-148-8 abstract page 28, left-hand column, line 1 - page 33, left-hand column, line 49	1,13-15

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

page 2 of 2

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB2005/053255

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0511420 A	04-11-1992	AT 129366 T	15-11-1995
		DE 69113988 D1	23-11-1995
		US 5161244 A	03-11-1992
US 2003204743 A1	30-10-2003	AU 2003221927 A1	03-11-2003
		CA 2482635 A1	30-10-2003
		EP 1497863 A2	19-01-2005
		JP 2005523481 T	04-08-2005
		WO 03090259 A2	30-10-2003

(81)指定国　AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,LY,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(72)発明者　スコリック，ボリス
オランダ国，５６５６　アーアー　アインドーフェン，プロフ・ホルストラーン　６
(72)発明者　ファン　デイク，マールテン　エー
オランダ国，５６５６　アーアー　アインドーフェン，プロフ・ホルストラーン　６
Ｆターム(参考) 5J104 AA07　KA01　KA04　KA06　PA07

Espacenet

Bibliographic data: JP2009111971 (A) — 2009-05-21

METHOD OF PRE-PROCESSING BIOMETRIC PARAMETERS BEFORE ENCODING AND DECODING

Inventor(s):	YEDIDIA JONATHAN S; DRAPER STARK C; SUTCU YAGIZ; ANTHONY VETRO ± (YEDIDIA JONATHAN S, ; DRAPER STARK C, ; SUTCU YAGIZ, ; ANTHONY VETRO)
Applicant(s):	MITSUBISHI ELECTRIC RES LAB ± (MITSUBISHI ELECTRIC RESEARCH LABORATORIES INC)
Classification:	**- international:** ***G06T7/00; H04L9/32;*** *A61B5/117* **- cooperative:**
Application number:	JP20080206773 20080811
Priority number (s):	US20070928687 20071030
Also published as:	JP5288935 (B2)

Abstract of JP2009111971 (A)

PROBLEM TO BE SOLVED: To provide a method of preprocessing biometric parameters acquired from human faces, voices, fingerprints, and irises to use them for user authentication and access control. ;SOLUTION: Since the biometric parameters are continuous and vary from one reading to the next, syndrome codes are used to discriminate biometric syndrome vectors. The biometric syndrome vectors can be stored securely while the variability specific to the biometric data is permitted. The stored biometric syndrome vectors are decoded during user authentication using biometric parameters acquired at that time. The syndrome codes can also be used to encrypt and decrypt data. The biometric parameters can be pre-processed to form a binary representation having a set of predetermined statistical properties given under a set of binary logical conditions. ;COPYRIGHT: (C)2009,JPO&INPIT

(19)日本国特許庁(JP)　(12)**公開特許公報(A)**　(11)特許出願公開番号

特開2009-111971
(P2009-111971A)

(43)公開日　平成21年5月21日(2009.5.21)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	***9/32***	***(2006.01)***	H04L	9/00	673D	4C038
G06T	***7/00***	***(2006.01)***	G06T	7/00	510B	5B043
A61B	*5/117*	*(2006.01)*	H04L	9/00	675A	5J104
			A61B	5/10	320A	

審査請求 未請求　請求項の数 21　ＯＬ　外国語出願　（全 121 頁）

(21)出願番号　特願2008-206773(P2008-206773)
(22)出願日　平成20年8月11日(2008.8.11)
(31)優先権主張番号　11/928,687
(32)優先日　平成19年10月30日(2007.10.30)
(33)優先権主張国　米国(US)

(71)出願人　597067574
ミツビシ・エレクトリック・リサーチ・ラボラトリーズ・インコーポレイテッド
アメリカ合衆国、マサチューセッツ州、ケンブリッジ、ブロードウエイ　２０１
２０１　ＢＲＯＡＤＷＡＹ，　ＣＡＭＢＲＩＤＧＥ，　ＭＡＳＳＡＣＨＵＳＥＴＴＳ　０２１３９，　Ｕ．Ｓ．Ａ．
(74)代理人　100110423
弁理士　曾我　道治
(74)代理人　100084010
弁理士　古川　秀利
(74)代理人　100094695
弁理士　鈴木　憲七

最終頁に続く

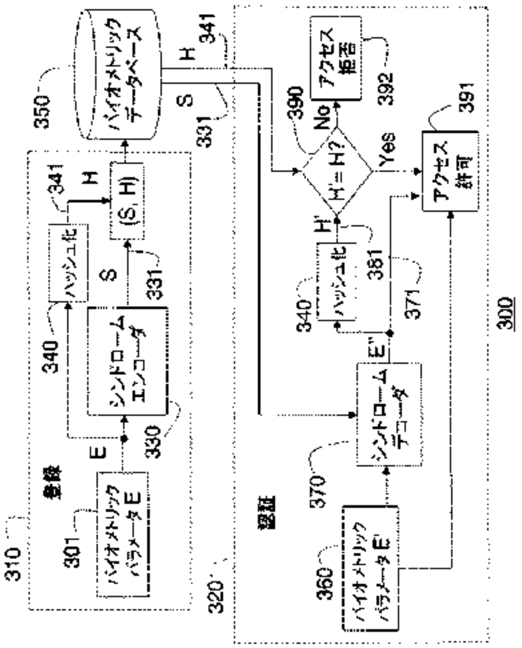
(54)【発明の名称】コード化および復号化前のバイオメトリックパラメータの前処理方法

(57)【要約】

【課題】人間の顔、声、指紋、および虹彩から取得されるバイオメトリックパラメータは、ユーザ認証およびアクセス制御ために使用することができる前処理方法を得る。

【解決手段】バイオメトリックパラメータは１つの読取りから次の読取りまで連続しており、また変動するので、シンドロームコードがバイオメトリックシンドロームベクトルを判別するために適用される。バイオメトリックデータの固有の変動性を許容しつつ、バイオメトリックシンドロームベクトルを安全に格納できる。格納されたバイオメトリックシンドロームベクトルは、ユーザ認証の間に、その時取得されたバイオメトリックパラメータを使用して復号される。また、データを暗号化したり、解読するために、シンドロームコードを使用できる。１組のバイナリロジック条件によって課された１組の所定の統計的性質を有するバイナリ表示を形成するために、バイオメトリックパラメータを前処理することができる。

【選択図】図３



【特許請求の範囲】

【請求項1】

登録段階の間、ユーザのバイオメトリックパラメータが取得される、データベースに安全にバイオメトリックパラメータを格納するためのコンピュータにより実行される前処理方法であって、

１組のバイナリロジック条件をユーザの登録バイオメトリックパラメータへ適用して２進表示を生成するステップであって、前記２進表示が、前記１組のバイナリロジック条件によって課される１組の所定の統計的性質を有するステップと、

シンドロームエンコーダを使用して前記２進表示をコード化して登録シンドロームベクトルを生成するステップであって、前記コード化が前記２進表示および前記１組の所定の統計的性質と互換性があるステップと、

登録バイオメトリックベクトルにハッシュ関数を適用して登録ハッシュを生成するステップと、

データベースに前記登録シンドロームベクトルと前記登録ハッシュを格納するステップと、

前記データベースを使用してユーザを認証するステップと、からなるコンピュータにより実行されるコード化および復号化前のバイオメトリックパラメータの前処理方法。

【請求項2】

請求項１の方法であって、認証ステップはさらに、

ユーザの認証バイオメトリックパラメータを取得するステップと、

前記１組のバイナリロジック条件を前記認証バイオメトリックパラメータに適用して認証バイオメトリックパラメータの２進表示を生成するステップであって、前記２進表示が、前記１組の所定の統計的性質により課された前記１組のバイナリロジック条件を有するステップと、

シンドロームデコーダを使用して前記バイオメトリックパラメータの２進表示を復号して認証シンドロームベクトルを生成するステップであって、コード化が前記バイオメトリックパラメータの２進表示と前記１組の所定の統計的性質と互換性があるステップと、

認証バイオメトリックベクトルにハッシュ関数を適用して認証ハッシュを生成するステップと、

前記認証シンドロームベクトルと前記認証ハッシュで前記データベースへアクセスしてユーザを検証するステップと、からなる方法。

【請求項3】

請求項１の方法であって、前記１組の統計的性質は前記２進表示における各ビットが零または１のどちらかである確率が等しいことを強制する方法。

【請求項4】

請求項１の方法であって、前記１組の統計的性質は前記２進表示における異なるビットが互いに独立していることを強制する方法。

【請求項5】

請求項１の方法であって、前記１組の統計的性質は異なるユーザからの２進表示が互いに独立していることを強制する方法。

【請求項6】

請求項１の方法であって、前記１組の統計的性質は同一のユーザからの２進表示が統計的に互いに依存することを強制する方法。

【請求項7】

請求項１の方法であって、前記バイオメトリックパラメータは指紋に対するマニューシャ点の位置である方法。

【請求項8】

請求項７の方法であって、前記１組のバイナリロジック条件は、与えられた２次元領域におけるマニューシャ点の数が閾値Ｍより大きいか否かを判別する条件を含む方法。

【請求項9】

請求項７の方法であって、前記１組のバイナリロジック条件は、１つの線よりも上のマニューシャ点の数と、該線よりも下のマニューシャ点の数の差に基づく条件を含む方法。

【請求項10】

請求項７の方法であって、前記１組のバイナリロジック条件は、第１矩形部内のマニューシャ点の数と、第２矩形部内のマニューシャ点の数の差に基づく方法。

【請求項11】

請求項１の方法であって、前記バイオメトリックパラメータは、指紋に対するマニューシャ点の位置および方位である方法。

【請求項12】

請求項１１の方法であって、前記１組のバイナリロジック条件は、与えられた三次元領域におけるマニューシャ点の数が閾値Ｍより大きいか否かを判別する条件を含む方法。

【請求項13】

請求項１の方法であって、前記所定の統計的性質は、パターンベースのデータと互換性がある方法。

【請求項14】

請求項１の方法であって、前記所定の統計的性質は、周波数ドメイン（領域）のデータと互換性がある方法。

【請求項15】

請求項１の方法であって、論理的なバイナリ条件の適用により中間値を生成するとともに、前記方法はさらに、中間値を２値化することを含む方法。

【請求項16】

請求項１５の方法であって、前記２値化はさらに、中間値を閾値化することを含む方法。

【請求項17】

請求項１６の方法であって、前記２値化はさらに、前記閾値化の前に、中間値に変換を適用することを含む方法。

【請求項18】

請求項１７の方法であって、前記２値化はさらに、前記中間値を正規化することを含む方法。

【請求項19】

請求項１７の方法であって、前記変換は無作為の投影である方法。

【請求項20】

請求項１７の方法であって、前記変換は主成分分析である方法。

【請求項21】

請求項１の方法であって、前記２進表示を分析して前記１組の統計的性質が課されることを保障、確認することを含む方法。

【発明の詳細な説明】

【技術分野】

【0001】

関連出願

本願は、Ｄｒａｐｅｒ外によって２００６年１１月２９日に、「Ｂｉｏｍｅｔｒｉｃ Ｂａｓｅｄ Ｕｓｅｒ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ（バイオメトリックに基づくユーザ認証とデータ暗号化）」という名称で出願された、米国特許出願第１１／５６４，６３８の一部係属出願であり、その米国特許出願１１／５６４，６３８は、また、Ｍａｒｔｉｎｉａｎ外によって２００５年9月1日に、「Ｂｉｏｍｅｔｒｉｃ Ｂａｓｅｄ Ｕｓｅｒ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ（バイオメトリックに基づくユーザ認証とデータ暗号化）」という名称で出願された米国特許出願第１１／２１８，２６１（米国公開２００６－０１２３２４１）の一部係属出願であり、またその米国特許出願第１１／２１８，２６１は、Ｍａｒｔｉｎｉａｎ外により２００４年１２月７日に、「Ｂｉｏｍｅｔｒｉｃ Ｂ ａｓｅｄ　Ｕｓｅｒ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｗｉｔｈ　Ｓｙｎｄｒｏｍｅ　Ｃｏｄｅｓ（シンドロームコードを有するバイオメトリックに基づくユーザ認証）」という名称で出願された米国特許出願第１１／００６，３０８（米国公開２００６－０１２３２３９）の一部係属出願である。

【0002】

一般に、この発明は、暗号の分野に関連し、特に、ユーザ認証およびデータ暗号化のために、バイオメトリックパラメータを取得し、前処理し、コード化し、格納することに関する。

【背景技術】

【0003】

従来のパスワードベースのセキュリティシステム

【0004】

従来のパスワードに基づくセキュリティシステムは、典型的に２つのフェイズ（段階）を含む。具体的には、登録段階の間、ユーザはパスワードを選択し、それらのパスワードはサーバなどの認証デバイスに格納（記憶）される。認証段階の間、リソースやデータへのアクセスを得るために、ユーザは彼らのパスワードを入力し、それらのパスワードは該パスワードの格納されたバージョンに対して検証される。パスワードがプレーンテキストとして格納されるなら、システムへのアクセスを得る敵対者は、あらゆるパスワードを得ることができるかもしれない。このようにして、単一の成功している攻撃でさえも、全体システムのセキュリティを危険に曝しうる。

【0005】

図１に示されているように、従来のパスワードに基づくセキュリティシステム１００は、登録段階１０の間に、コード化１１０されたパスワード１０１をパスワードデータベース１２０に格納（記憶）１１１５する。具体的には、Ｘが格納１１５されるパスワード１０１であるならば、システム１００は実際にｆ（Ｘ）を格納し、ここでｆ（．）は或る暗号化すなわちハッシュ関数１１０である。認証段階２０の間、ユーザは候補パスワードＹ１０２を入力し、システムはｆ（Ｙ）を判別１３０して、ｆ（Ｙ）が格納されたパスワードｆ（Ｘ）に一致するとき、システムへのアクセス１５０を許可し、そうでなければ、アクセスは否定１６０される。

【0006】

利点としては、暗号化されたパスワードは、通常、インバート（逆転、逆行）させることが非常に難しいので、暗号化関数なしでは、敵対者には役に立たない。

【0007】

従来のバイオメトリックに基づくセキュリティシステム

【0008】

バイオメトリックセキュリティシステムは、しばしば観測と呼ばれるバイオメトリックパラメータを得るため、肉体的なバイオメトリック特徴を計測する。従来のバイオメトリックセキュリティシステムには、暗号化されていないパスワードを格納する、パスワードに基づくシステムと同じような脆弱性がある。具体的には、データベースが暗号化されていないバイオメトリックパラメータを格納するならば、それらのパラメータは攻撃と誤用を被りやすい。

【0009】

たとえば、顔認識システムまたは音声認識を使用するセキュリティシステムでは、敵対者は、該敵対者と同様のバイオメトリックパラメータを捜し求めることができるかもしれない。適当なバイオメトリックパラメータが見つけ出された後に、敵対者は、不正アクセスを得るために、該パラメータを変更して該敵対者の外観または声と一致するようにすることができるかもしれない。同様に、指紋或いは虹彩認識を使用するセキュリティシステムでは、敵対者は、不正アクセスを得るために、一致する指紋または虹彩を模造するデバイスを制作することができるかもしれない。たとえば、そのようなデバイスは、偽造の指または偽造の目である。

【0010】

基本的なバイオメトリック特徴の変動可能性ばかりでなく、それらの特徴が測定される方法における変動可能性によっても、バイオメトリックパラメータを暗号化することが常に可能であるというわけではない。この変動可能性すなわち差を「ノイズ」と呼ぶことができる。

【0011】

具体的には、バイオメトリックパラメータＸは登録段階の間に入力される。たとえば、パラメータＸが暗号化すなわちハッシュ化関数ｆ（Ｘ）を使用して暗号化されて、格納されるとする。認証段階の間に、同じユーザから得られたバイオメトリックパラメータは異なる場合がある。たとえば、顔認証を使用するセキュリティシステムでは、登録および認証のために使用されるカメラは、異なる方向、感度および分解能を持つことができる。通常、照明はかなり異なる。肌の色合い、ヘアスタイル、およびその他の顔の特徴は簡単に変えることができる。このようにして、認証の間に、新たに観測されたパラメータＹが同じ暗号化関数ｆに通されるならば、その結果ｆ（Ｙ）はｆ（Ｘ）と一致せず、拒否を引き起こすであろう。同様の問題は、虹彩および指紋パターンなどの他のバイオメトリックに基づくユーザ認証でも存在する。

【0012】

誤り訂正符号（コード）

【0013】

アルファベットＱ上の、（Ｎ、Ｋ）誤り訂正符号（ＥＣＣ）Ｃは長さＮのQ^Kベクトルを含む。リニア（Ｎ、Ｋ）ＥＣＣは、Ｎ行Ｋ列の生成行列Ｇを使用するか、またはＮ－Ｋ行Ｎ列のパリティチェックマトリクスＨを使用することによって、説明できる。名称「生成行列」は、ベクトルｗとして表される符号語が、ベクトルｖにマトリクスＧを後から（右から）掛けることにより、すなわちｗ＝ｖＧにより、どんな長さＫの入力行ベクトルｖからも生成され得るという事実に基づいている。同様に、ベクトルｗが符号語であるかどうかをチェックするために、$Hw^T=0$であるか否かチェックしてもよく、ここで、列ベクトルw^Tは行ｗの転置である。

【0014】

誤り訂正符号の標準的用法では、入力ベクトルｖはベクトルｗにコード化（符号化）されて、格納されるか、或いは伝送される。ベクトルｗの崩壊した（間違いのある）バージョンが受信されるならば、デコーダは、エラーを修正するために、コードに冗長性を使用する。直観的に、コードのエラー修正能力はコードの冗長性の量に依存する。

【0015】

スレピアン－ウォルフ、ウイナージブ、およびシンドロームコード

【0016】

ある意味で、スレピアン－ウォルフ（ＳＷ）コードは誤り訂正符号の逆（反意語）である。誤り訂正符号は冗長性を加えてデータを拡大するが、ＳＷコードは冗長性を取り除いてデータを圧縮する。具体的に、ベクトルｘおよびｙは関連付けられたデータを表している。エンコーダが既にベクトルｙを持っているデコーダにベクトルｘを伝えることを望むならば、該エンコーダは、デコーダにはベクトルｙがあるという事実を考慮に入れて、データを圧縮することができる。

【0017】

極端な例として、ベクトルｘおよびｙが１ビットだけ異なるならば、エンコーダは、単にベクトルｘおよび相違の位置を記載することにより、データの圧縮を実現することができる。勿論、より現実的な相関モデルに対しては、より高度なコードが要求される。

【0018】

ＳＷコーディングおよび関連するウイナージブ（ＷＺ）コーディングの基本理論は、ＩＥＥＥ Ｔｒａｎｓａｃｔｉｏｎｓ ｏｎ Ｉｎｆｏｒｍａｔｉｏｎ Ｔｈｅｏｒｙ（情報理論に関するＩＥＥＥトランザクション）、Ｖｏｌ．１９、ページ４７１～４８０、１９７３年7月発行の「Ｎｏｉｓｅｌｅｓｓ ｃｏｄｉｎｇ ｏｆ ｃｏｒｒｅｌａｔｅｄ ｉｎｆｏｒｍａｔｉｏｎ ｓｏｕｒｃｅｓ（相関情報ソースの無雑音符号化）」において、スレピアンおよびヴォルフによって記載されているとともに、ＩＥＥＥ Ｔｒａｎｓａｃｔｉｏｎｓ ｏｎ Ｉｎｆｏｒｍａｔｉｏｎ Ｔｈｅｏｒｙ、Ｖｏｌ．２２、ページ１～１０、１９７６年1月発行の「Ｔｈｅ ｒａｔｅ－ｄｉｓｔｏｒｔｉｏｎ ｆｕｎｃｔｉｏｎ ｆｏｒ ｓｏｕｒｃｅ ｃｏｄｉｎｇ ｗｉｔｈ ｓｉｄｅ ｉｎｆｏｒｍａｔｉｏｎ ａｔ ｔｈｅ ｄｅｃｏｄｅｒ（デコーダでの副情報を有するソースコーディングに対する速度－歪み関数」において、ＷｙｎｅｒおよびＺｉｖによっても記載されている。より最近、プラダン（Ｐｒａｄｈａｎ）およびラムチャンドラン（Ｒａｍｃｈａｎｄｒａｎ）が、ＩＥＥＥ Ｔｒａｎｓａｃｔｉｏｎｓ ｏｎ Ｉｎｆｏｒｍａｔｉｏｎ Ｔｈｅｏｒｙ、Ｖｏｌ．４９、ページ６２６～６４３、２００３年3月発行の「Ｄｉｓｔｒｉｂｕｔｅｄ Ｓｏｕｒｃｅ Ｃｏｄｉｎｇ Ｕｓｉｎｇ Ｓｙｎｄｒｏｍｅｓ （ＤＩＳＣＵＳ）：Ｄｅｓｉｇｎ ａｎｄ Ｃｏｎｓｔｒｕｃｔｉｏｎ（シンドロームを使用する分散型ソースコーディング：設計と構成）」において、そのようなコードの実用的な実用化について記載している。

【0019】

本質的には、シンドロームコードは、Ｎ－Ｋ行Ｎ列を有するパリティチェックマトリクスＨを使用することによって、動作する。長さＮのバイナリ（２進）ベクトルｘを長さＫのシンドロームベクトルに圧縮するために、Ｓ＝Ｈｘを判定する。復号化は、しばしば、使用された特定のシンドロームコードの詳細に依存する。たとえば、シンドロームコードがトレリス（ｔｒｅｌｌｉｓ）に基づくならば、パラダン（Ｐｒａｄｈａｎ）外により記述されているように、シンドロームベクトルＳに対応する最も有望なソースシーケンスＸおよび副情報のシーケンスを見つけるために、周知のヴィテルビ（Ｖｉｔｅｒｂｉ）アルゴリズムなどの様々なダイナミックプログラミングに基づく検索アルゴリズムを使用できる。

【0020】

或いはまた、低密度のパリティチェックシンドロームコードが用いられるならば、２００４年3月発行のＤａｔａ Ｃｏｍｐｒｅｓｓｉｏｎ Ｃｏｎｆｅｒｅｎｃｅ（データ圧縮カコンファレンス）の予稿集、ページ２８２～２９１、「Ｏｎ ｓｏｍｅ ｎｅｗ ａｐｐｒｏａｃｈｅｓ ｔｏ ｐｒａｃｔｉｃａｌ Ｓｌｅｐｉａｎ－Ｗｏｌｆ ｃｏｍｐｒｅｓｓｉｏｎ ｉｎｓｐｉｒｅｄ ｂｙ ｃｈａｎｎｅｌ ｃｏｄｉｎｇ（チャネル符号化で鼓舞された実用的なスレピアンーウォルフ圧縮への幾つかの新アプローチ）」に、コールマン外により記載されているように、確率伝搬復号化を適用できる。

【0021】

ファクター（要素）グラフ

【0022】

従来技術では、上述したようなコードは、しばしば「ファクターグラフ」と呼ばれる２部グラフによって表される。Ｆ．Ｒ．Ｋｓｃｈｉｓｃｈａｎｇ、Ｂ．Ｊ．ＦｒｅｙおよびＨ．Ａ．Ｌｏｅｌｉｇｅｒ、「Ｆａｃｔｏｒ Ｇｒａｐｈｓ ａｎｄ ｔｈｅ Ｓｕｍ－Ｐｒｏｄｕｃｔ Ａｌｇｏｒｉｔｈｍ（ファクターグラフと加算値積のアルゴリズム）」、ＩＥＥＥ Ｔｒａｎｓａｃｔｉｏｎｓ ｏｎ Ｉｎｆｏｒｍａｔｉｏｎ Ｔｈｅｏｒｙ、ｖｏｌ．４７、ページ４９８～５１９、２００１年2月、およびＧ．Ｄ．Ｆｏｒｎｅｙ，Ｊｒ．、「Ｃｏｄｅｓ ｏｎ Ｇｒａｐｈｓ：Ｎｏｒｍａｌ Ｒｅａｌｉｚａｔｉｏｎｓ（グラフに関するコード：通常の実現」、ＩＥＥＥ Ｔｒａｎｓａｃｔｉｏｎｓ ｏｎ Ｉｎｆｏｒｍａｔｉｏｎ Ｔｈｅｏｒｙ、ｖｏｌ．４７、ページ５２０～５４９、２００１年2月、およびＲ．Ｍ．Ｔａｎｎｅｒ、「Ａ Ｒｅｃｕｒｓｉｖｅ Ａｐｐｒｏａｃｈ ｔｏ Ｌｏｗ－Ｃｏｍｐｌｅｘｉｔｙ Ｃｏｄｅｓ（低複雑さコードへの反復アプローチ）」、ＩＥＥＥ Ｔｒａｎｓａｃｔｉｏｎｓ ｏｎ Ｉｎｆｏｒｍａｔｉｏｎ Ｔｈｅｏｒｙ、ｖｏｌ．２７、ページ５３３～５４７、１９８１年9月、を参照。また、これらはすべて本明細書中に引用して援用される。

【0023】

一般に、ファクター（要素）グラフは２部グラフであり、「可変ノード」および「ファクター（要素）ノード」と呼ばれる２つのタイプのノードを含んでいる。可変ノードはファクターノードに接続されるだけであり、また、逆も同様である。ファクターノードは慣習的に四角形を使用して描かれ、また、可変ノードは慣習的に円を使用して描かれ、また、可変ノードおよびファクターノードの間の接続は対応する円および四角形を接続する線によって表される。時々、符号（シンボル）、すなわち「＋」は、それが実行する制約条件の種類を表すために、ファクターノードの中に描かれる。

【0024】

可変ノードはコードで使用される符号を表しており、またファクターノードはそれらの符号に対する制約条件を表している。可変ノードは該当する制約条件を受ける場合にだけ、ファクターノードに接続される。

【0025】

バイオメトリックパラメータをコーディングする従来技術

【0026】

この発明に関連する従来技術は３つのカテゴリになる。まず最初に、そのようなバイオメトリックパラメータの安全な格納に関係ない、特徴抽出、記録およびバイオメトリックパラメータの使用について記述している多くの従来技術がある。この発明は安全な格納に関係しており、主に、バイオメトリックパラメータをどのように取得するかに関する詳細には関わらないので、従来技術のこのカテゴリの詳細は省略される。

【0027】

この発明に関連する２番目のクラスの従来技術は、安全な格納とバイオメトリックス（生物測定学）の認証のために設計された以下のシステムを含む。「Ｍｅｔｈｏｄ　ａｎｄ　ｓｙｓｔｅｍ　ｆｏｒ　ｎｏｒｍａｌｉｚｉｎｇ　ｂｉｏｍｅｔｒｉｃ　ｖａｒｉａｔｉｏｎｓ　ｔｏ　ａｕｔｈｅｎｔｉｃａｔｅ　ｕｓｅｒｓ　ｆｒｏｍ　ａ　ｐｕｂｌｉｃ　ｄａｔａｂａｓｅ　ａｎｄ　ｔｈａｔ　ｅｎｓｕｒｅｓ　ｉｎｄｉｖｉｄｕａｌ　ｂｉｏｍｅｔｒｉｃ　ｄａｔａ　ｐｒｉｖａｃｙ（公開データベースからユーザを認証するためにバイオメトリックなバラツキを正規化して、個々のバイオメトリックデータのプライバシーを保障する方法およびシステム）」、米国特許６，０３８，３１５；Ｐｒｏｃｅｅｄｉｎｇｓ　ｏｆ　ｔｈｅ　ＩＥＥＥ　Ｓｙｍｐｏｓｉｕｍ　ｏｎ　Ｓｅｃｕｒｉｔｙ　ａｎｄ　Ｐｒｉｖａｃｙ，Ｍａｙ　１９９８における、Ｄａｖｉｄａ，Ｇ．Ｉ．，Ｆｒａｎｋｅｌ，Ｙ．，Ｍａｔｔ，Ｂ．Ｊ．による「Ｏｎ　ｅｎａｂｌｉｎｇ　ｓｅｃｕｒｅ　ａｐｐｌｉｃａｔｉｏｎｓ　ｔｈｒｏｕｇｈ　ｏｆｆ－ｌｉｎｅ　ｂｉｏｍｅｔｒｉｃ　ｉｄｅｎｔｉｆｉｃａｔｉｏｎ（オフラインバイオメトリック認証で安全な応用を可能にすることについて）」；Ｐｒｏｃｅｅｄｉｎｇｓ　ｏｆ　ｔｈｅ　２００２　ＩＥＥＥ　Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ｓｙｍｐｏｓｉｕｍ　ｏｎ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｔｈｅｏｒｙ，Ｊｕｎｅ　２００２における、Ｊｕｅｌｓ，Ａ．，Ｓｕｄａｎ，Ｍ．，による「Ａ　Ｆｕｚｚｙ　Ｖａｕｌｔ　Ｓｃｈｅｍｅ（ファジィボールトスキーム）」；２００１年１１月２６日に出願された米国特許出願第０９／９９４，４７６、「Ｏｒｄｅｒ　ｉｎｖａｒｉａｎｔ　ｆｕｚｚｙ　ｃｏｍｍｉｔｍｅｎｔ　ｓｙｓｔｅｍ（順序不変ファジィコミットメントシステム」；Ｐｒｏｃ．　５th　ＡＣＭ　Ｃｏｎｆ．　ｏｎ　Ｃｏｍｐ．　ａｎｄ　Ｃｏｍｍｕｎ．　Ｓｅｃｕｒｉｔｙ，Ｎｅｗ　Ｙｏｒｋ，ＮＹ，ｐｇｓ．２８－３６，１９９９における、Ｊｕｅｌｓ　ａｎｄ　Ｗａｔｔｅｎｂｅｒｇの「Ａ　ｆｕｚｚｙ　ｃｏｍｍｉｔｍｅｎｔ　ｓｃｈｅｍｅ（ファジィコミットメントスキーム）」；Ａｓｉｌｏｍａｒ　Ｃｏｎｆ．　ｏｎ　Ｓｉｇｎａｌｓ，Ｓｙｓｔｅｍｓ，ａｎｄ　Ｃｏｍｐ．，ｖｏｌ．１，ｐｐ．５７７－５８１，Ｎｏｖｅｍｂｅｒ　２００４における、Ｓ．Ｙａｎｇ　ａｎｄ　Ｉ．Ｍ．Ｖｅｒｂａｕｗｈｅｄｅの「Ｓｅｃｕｒｅ　ｆｕｚｚｙ　ｖａｕｌｔ　ｂａｓｅｄ　ｆｉｎｇｅｒｐｒｉｎｔ　ｖｅｒｉｆｉｃａｔｉｏｎ　ｓｙｓｔｅｍ（安全なファジィボールトに基づく指紋照合システム」；Ｐｒｏｃ．　Ｗｏｒｋｓｈｏｐ：Ｂｉｏｍｅｔｒｉｃｓ：Ｃｈａｌｌｅｎｇｅｓ　ａｒｉｓｉｎｇ　ｆｒｏｍ　ｔｈｅｏｒｙ　ｔｏ　ｐｒａｃｔｉｃｅ，ｐｐ．１３－１６，Ａｕｇｕｓｔ　２００４

における、Ｕ．Ｕｌｕｄａｇ　ａｎｄ　Ａ．Ｊａｉｎの「Ｆｕｚｚｙ　ｆｉｎｇｅｒｐｒｉｎｔ　ｖａｕｌｔ（ファジィ指紋ボールト」。

【0028】

図２は、米国特許６，０３８，３１５に記載されている基本的方法の詳細の幾つかを示す。登録フェーズ（段階）２１０では、バイオメトリックパラメータが、Ｅで表されたビットのシーケンスの形式で取得２０１される。次に、ランダムな符号語Ｗ２０２が２進の誤り訂正符号から選択され、エクスクルーシブＯＲ（排他的論理和）関数２２０を使用してパラメータＥに加算的に結合されて、リファレンス（基準）Ｒを生成２２１する。任意ではあるが、リファレンスＲはさらにコード化２３０されうる。何れの場合でも、リファレンスＲはパスワードデータベース２４０に格納される。

【0029】

認証段階２２０では、バイオメトリックパラメータＥ’２０５が認証のために提示される。その方法は、Ｅ’でＲのＸＯＲ（排他的論理和）を判定２５０し、これらの２つを減算してＺ＝Ｒ－Ｅ＝Ｗ＋Ｅ－Ｅ’を得る２５１。次に、この結果が誤り訂正符号で復号２６０されて、Ｗ’を生成２６１する。ステップ２７０で、Ｗ’がＷと一致するならば、アクセスが許可２７１され、そうでなければ、アクセスが拒否２７２される。

【0030】

その方法は、本質的には、ハミング距離、すなわち登録されたバイオメトリックＥ２０１と認証バイオメトリックＥ’２０５との間で異なるビット数を測定する。その差が或る所定の閾値より小さいならば、アクセスが許可される。この方法は実際のバイオメトリックパラメータＥではなく、リファレンスＲだけを格納するので、安全である。

【0031】

ダビダ外（Ｄａｖｉｄａ　ｅｔ　ａｌ．）およびジュエルス外（Ｊｕｅｌｓ　ｅｔ　ａｌ．）は、図２に示される方法の変形例を記述する。具体的には、両者とも、結果として得られる符号語を安全にする操作が後に続く登録段階の間、誤り訂正符号でバイオメトリックデータをコード化する。ダビダ外は、チェックビットを送るだけで符号語を隠し、他方、ジュエルス外は「チャフ」と呼ばれる幾らかの量のノイズを加算する。

【0032】

「多因子のバイオメトリック認証デバイスおよび方法」という名称の米国特許６，３６３，４８５は、秘密鍵を生成するために、バイオメトリックデータと誤り訂正符号およびパスワードや個人識別番号（ＰＩＮ）などの或る秘密情報を結合するための方法について記載している。ゴッパコードやＢＣＨコードなどの誤り訂正符号が様々な排他的論理和操作で使われる。

【0033】

図２に図示した固定データベースアクセス制御システムに加えて、３番目のクラスの従来技術は、データ保護、具体的には、ラップトップ、ＰＤＡ、携帯電話、およびデジタルカメラなどの、メモリを含むモバイル機器ためのデータ保護のための生体認証を使用することを含む。モバイル機器は容易に紛失したり、盗まれたりし易いので、モバイル機器に格納されたデータを保護することが必要になる。

【0034】

従来技術に関する問題

【0035】

図４は、データＤを格納するための現存する手法での問題を図示する。コード化プロセス４１０では、データＤを暗号化４４０して暗号文Ｃを生成４４１するために、バイオメトリックパラメータＰ４０２がユーザから得られ、キーとして使用される。バイオメトリックパラメータＰおよび暗号文Ｃの両方ともストリッジ４５０にセーブ（保存）される。ユーザがデータＤを解読４２０したがっているとき、バイオメトリックパラメータＰ’４６０がユーザから得られて、格納されたバイオメトリックパラメータＰ４０２と比較される。Ｐ’がＰと一致４７０するならば、システムはアクセスを許して、格納された暗号文Ｃを解読してデータＤを生成４０１するためにＰを使用し、さもなければ、データは解読

されない４７１。

【0036】

記憶媒体が危険にさらされていない限りでのみ、そのような従来のシステムは有効である。しかし、敵対者がそのようなメディア（媒体）へアクセスすることができるならば、敵対者はＰを得て、データを復号する。

【0037】

第１に、ビットベースの従来の方法は疑わしいセキュリティ（安全性）しか提供しない。さらに、バイオメトリックパラメータは、バイナリ（２進）値の代わりに、しばしば実数或いは整数である。一般に、従来技術は、バイオメトリックパラメータが一様に分布しているランダムな（無作為の）ビットで構成され、格納されたバイオメトリックからこれらのビットを正確に判別するのが難しいと仮定する。実際には、バイオメトリックパラメータはしばしばバイアスをかけられており、これがセキュリティにネガティブに影響する。また、敵対者が格納されたバイオメトリックの大体（近似）のバージョンだけを再生したとしても、敵対者の攻撃により重要な害が引き起こされる場合がある。従来の方法は、敵対者がコード化されたバージョンから実際のバイオメトリックを推定するのを防止するように設計されていない。

【0038】

たとえば、米国特許６，０３８，３１５は、ランダムな符号語Ｗを加算することによって、基準値Ｒ＝Ｗ＋Ｅが効果的にバイオメトリックＥを暗号化するという事実に頼る。ところで、その方法は劣悪なセキュリティを実現する。ＥをＲから再生する多くの方法がある。たとえば、ベクトルＥが１と等しいほんの数ビットを有するならば、ＲとＷの間のハミング距離は小さい。このようにして、誤り訂正デコーダは容易にＷをＲから再生することができるかもしれないし、したがってＥを再生することができるかもしれない。或いはまた、たとえば、符号語の分布が悪く、すなわちコードの重さスペクトルが小さくて、多くの符号語がすべてゼロベクトルの回りに群がるならば、敵対者はＲからＥの良い近似を得ることができるかもしれない。

【0039】

第２に、疑わしいセキュリティに加えて、従来の方法は、格納されるデータ量を増大させるという実用的な不都合を有する。バイオメトリックデータベースがしばしば多数の個々のユーザのためのデータを格納するので、追加のストリッジ（記憶装置）によりシステムの費用と複雑さがかなり増大される。

【0040】

第３に、多くの従来の方法は、高い計算量（複雑さ）を有する誤り訂正符号またはアルゴリズムを必要とする。たとえば、従来技術のリード－ソロモン（Ｒｅｅｄ－Ｓｏｌｏｍｏｎ）およびリード－ミューラー（Ｒｅｅｄ－Ｍｕｌｌｅｒ）復号アルゴリズムは一般に、２次関数的な大きな計算量（複雑さ）を有し、また、しばしばコード化されたバイオメトリックの長さにおいて、より高位に（大きく）なる。

【0041】

第４に、従来技術では既知のモバイルセキュリティシステム用の基本アーキテクチャに基本的な問題がある。図４に示されているようなモバイルセキュリティシステムは、それ自体が危険にさらされない場合にだけ、有効であり得る。ラップトップ上のモバイルセキュリティシステムの例に戻ると、敵対者がＰとＣが格納された媒体へ物理的にアクセスすることができない場合にだけ、セキュリティは有効であり得る。敵対者が、たとえばラップトップからハードディスクを取り外すことによって、そのようなメディアへアクセスすることができるならば、敵対者は、直ちに、Ｃを生成するのに使用された暗号化キーであったＰを得て、Ｃを解読できる。

【0042】

従来のモバイルセキュリティシステムにおける主な困難は、ユーザのバイオメトリックパラメータに対応する暗号キーが、デバイスに格納されているということである。このようにして、デバイスが盗まれるならば、格納されたパラメータを使用することでデータを

復号できる。

【0043】

第５に、バイオメトリックス（生体認証）に特有のノイズ構造に対する、誤り訂正符号化またはシンドロームコード復号化を行うための良い方法がないので、或いは、該ノイズ構造をモデル化するまでの多くの考察も行われていないので、安全なバイオメトリック（生体測定認証）システムに関する殆どの従来技術は、無記憶な雑音モデルや、ノイズの本質を単純化しすぎて実際の運用条件を反映しない、他のモデルを使用している。すなわち、従来のモデルは、バイオメトリック特徴の時間とともに変動するダイナミックス（動力学）および取得と測定のプロセスを正確に表していない。その代わりに、それらのモデルは、ノイズが無記憶であり、空間的或いは時間的な構造も持っていないと仮定する。

【0044】

しばしば、バイオメトリック特徴は、１つの計測から別の計測まで変動する。たとえば、指紋生体認証では、「マニューシャ（特徴；ｍｉｎｕｔｉａｅ）」点が設定された特徴集合（ｆｅａｔｕｒｅ　ｓｅｔ）としてしばしば使用される。マニューシャ点の相対的な位置と方向は、登録および認証の間、かなり異なる場合がある。これにより、認証過程が複雑になる。この問題を解決するためのほとんどの簡単な試みは、非常に高次元であるために、実用化のためには非実用的であるモデルを使用する。

【0045】

したがって、構造化されたノイズを含むバイオメトリックデータのためのモデルを提供することが望ましい。さらに、チャネルコードを使用してバイオメトリックパラメータを前処理し、前処理されたパラメータが符号化および復号化のために最適な形式を有するようにすることが望ましい。

【発明の開示】

【発明が解決しようとする課題】

【0046】

たとえば、人間の顔、声、指紋、および虹彩から取得されるバイオメトリックパラメータは、ユーザ認証およびデータアクセス制御ために使用することができる。バイオメトリックパラメータは、通常連続しており、同じユーザに対しても、１つの読取りから次の読取りまでに変動することがあるので、パスワードで行われているように、ハッシュ化すなわち暗号化された形式でデータベースに格納することができない。たとえば、顔または指紋のサンプリングされた外観や、声の調子は時間経過とともに変化することがある。

【課題を解決するための手段】

【0047】

この発明の実施の形態１では、バイオメトリックデータ、たとえばウイナージブまたはスレピアンーウォルフコーディングに基づくシンドロームコードを保護するために、シンドロームコードを使用する。我々がシンドロームベクトルと呼ぶシンドロームコード化の出力は、生のバイオメトリックデータの固有の変動性を許容しつつ、データベースに安全に格納することができる。

【発明の効果】

【0048】

具体的には、この発明によるバイオメトリックシンドロームベクトルには、以下の特性がある。

【0049】

第１に、シンドロームコードは元のバイオメトリック特性に関する情報を効果的に隠す、すなわち暗号化し、シンドロームデータベースが危険にさらされるとしても、格納されたシンドロームベクトルが、システムのセキュリティを回避する際に、ほとんど役に立たないようにする。

【0050】

第２に、各バイオメトリックの２回目のノイズの混じった計測の場合でも、対応する格納されたシンドロームベクトルを復号して、元のバイオメトリックパラメータを生成して

、該元のバイオメトリックパラメータで暗号化されたデータを解読することができる。

【0051】

第３に、本シンドロームコーディング方法論は、ユーザ認証ために使用できる。

【0052】

この発明の第２の実施の形態は、時間経過とともにバイオメトリック特徴の変動（バラツキ）により変動することがあるバイオメトリックパラメータであって、さらに、測定プロセスをモデル化するバイオメトリックパラメータを効率的にモデル化するための方法を記述する。

【0053】

本方法により、バイオメトリック特徴の複数の読取りの間の関係を、計算上効率的に、正確に利用できる。特に、本方法により、現存する従来の方法よりも遙かに良く、そのようなバイオメトリック特徴のシンドローム復号化を成功裏に行うことができる。

【0054】

実施の形態１では、バイオメトリックパラメータは１組のロジック条件にしたがって前処理されて、１組の所定の統計的性質を有するバイナリ（２進）表示を形成する。なお、統計的性質は我々が実現することを望んでいる目標特性であることに注意するべきである。

【発明を実施するための最良の形態】

【0055】

実施の形態１．

この発明の実施の形態は以下の構成部を含む：

バイオメトリックパラメータを安全に格納するためのシンドロームエンコーダとハッシュ化方法、バイオメトリックキーで暗号化されたデータを安全に格納するためのシンドロームコードに基づく暗号化方法、および前の２つの方法などの安全なバイオメトリック応用のために使用されるシンドロームコードを最適化する方法。

【0056】

安全なバイオメトリックパラメータのためのシンドロームおよびハッシュ化方法

【0057】

図３は、この発明によるシンドロームとハッシング（ハッシュ化）に基づくバイオメトリックセキュリティシステム３００を示している。ユーザのバイオメトリック特徴が、バイオメトリックパラメータ（データまたは観測）を得るために、測定される。この発明による方法は、圧縮されたシンドロームベクトルに生成するために、シンドロームコードでバイオメトリックパラメータを圧縮する。

【0058】

従来の圧縮とは違って、シンドロームコードによって生成されたシンドロームベクトルのみから、元のバイオメトリックデータを再構成或いは近似することはできない。シンドロームベクトルおよび元のバイオメトリックパラメータのハッシュはバイオメトリックデータベースに格納される。

【0059】

ユーザを認証するために、バイオメトリックパラメータが再び測定される。そのバイオメトリックパラメータは、元のバイオメトリックパラメータを復号するために、格納されたシンドロームベクトルに結合される。シンドローム復号化が失敗するならば、元のバイオメトリックパラメータが再生されず、また復号されたパラメータのハッシュは格納されたハッシュと一致しない。したがって、ユーザはアクセスを拒否される。シンドローム復号化が成功するならば、元のバイオメトリックパラメータのハッシュは復号されたパラメータのハッシュと一致し、それはユーザの真正性を証明する。ハッシュの役割は、ユーザエントリ制御を提供し、ユーザによって提供されたバイオメトリックパラメータが、元のバイオメトリックパラメータを正確に再構成することができるくらいに、充分に良いことを確認することである。シンドロームエンコーダとハッシュの両方とも多対１マッピングであるが、シンドロームコードは、元のバイオメトリックパラメータを再構成するのに有

用な構造を有する。他方、ハッシュ関数は、たとえば、暗号のハッシュでもよいが、それは元のバイオメトリックを推定するのに役に立つ情報を提供しない。

【0060】

登録フェーズ（段階）

【0061】

登録段階３１０では、ユーザの肉体的（身体的）な特徴についてのバイオメトリックデータを取得する。たとえば、バイオメトリックデータは、顔の画像、スピーチ（音声）の録音、指紋の画像、または虹彩のスキャンから得られる。

【0062】

以下、バイオメトリックデータとは、ユーザの身体的な特徴から感知され、測定され、または別の方法で取得された生のバイオメトリック信号のことを言及する。特徴はバイオメトリックデータから抽出される。特徴はｄ次元の特徴ベクトルに配設される。特徴ベクトルは登録バイオメトリックパラメータ３０１を形成する。様々な形式のバイオメトリックデータから特徴を抽出するための方法は、上述したように、当技術分野では周知である。特徴ベクトルのバイオメトリックパラメータへの変換および最適なシンドロームコードは以下に詳述する。

【0063】

バイオメトリックパラメータＥ３０１は、登録シンドロームベクトルがＳ３３１を生成するために、シンドロームエンコーダ３３０を使用してコード化される。次に、登録ハッシュＨ３４１を生成するために、メッセージ認証符号すなわちハッシュ関数がバイオメトリックパラメータＥに適用３４０される。ハッシュ関数は、ＲＦＣ１３２１、１９９２年４月の「Ｔｈｅ ＭＤ５ Ｍｅｓｓａｇｅ Ｄｉｇｅｓｔ Ａｌｇｏｒｉｔｈｍ（ＭＤ５メッセージダイジェストアルゴリズム）」において、ロン リベスト（Ｒｏｎ Ｒｉｖｅｓｔ）により記述された周知のＭＤ５暗号ハッシュ関数でもよい。登録シンドロームベクトルーハッシュペア（Ｓ、Ｈ）３３１、３４１はバイオメトリックデータベース３５０に格納される。

【0064】

如何なるタイプのシンドロームコード、たとえば、上述したＳＷコードやＷＺコード、でも使用できる。この発明の好適な実施の形態では、いわゆる「反復−累積（ｒｅｐｅａｔ−ａｃｃｕｍｕｌａｔｅ）コード」から得られたコード、すなわち「積−累積（ｐｒｏｄｕｃｔ−ａｃｃｕｍｕｌａｔｅ）コード」および我々が「拡張ハミング−累積（ｅｘｔｅｎｄｅｄ Ｈａｍｍｉｎｇ−ａｃｃｕｍｕｌａｔｅ）コード」と呼ぶコードを使用する。

【0065】

我々は一般に、これらを直列に連結された累積（ＳＣＡ）コードと言及する。一般的な意味における、これらのクラスのコードに関する詳しい情報ためには、以下を参照。Ｊ．Ｌｉ，Ｋ．Ｒ．Ｎａｒａｙａｎａｎ，ａｎｄ Ｃ．Ｎ．Ｇｅｏｒｇｈｉａｄｅｓ、「Ｐｒｏｄｕｃｔ Ａｃｃｕｍｕｌａｔｅ Ｃｏｄｅｓ：Ａ Ｃｌａｓｓ ｏｆ Ｃｏｄｅｓ Ｗｉｔｈ Ｎｅａｒ−Ｃａｐａｃｉｔｙ Ｐｅｒｆｏｒｍａｎｃｅ ａｎｄ Ｌｏｗ Ｄｅｃｏｄｉｎｇ Ｃｏｍｐｌｅｘｉｔｙ（積累積コード：能力に近いパフォーマンスおよび低い復号化複雑さのクラスのコード）」、ＩＥＥＥ Ｔｒａｎｓａｃｔｉｏｎｓ ｏｎ Ｉｎｆｏｒｍａｔｉｏｎ Ｔｈｅｏｒｙ，Ｖｏｌ．５０，ｐｐ．３１−４６，Ｊａｎｕａｒｙ ２００４；Ｍ．Ｉｓａｋａ ａｎｄ Ｍ．Ｆｏｓｓｏｒｉｅｒ、「Ｈｉｇｈ Ｒａｔｅ Ｓｅｒｉａｌｌｙ Ｃｏｎｃａｔｅｎａｔｅｄ Ｃｏｄｉｎｇ ｗｉｔｈ Ｅｘｔｅｎｄｅｄ Ｈａｍｍｉｎｇ Ｃｏｄｅｓ（拡張ハミングコードを有する高速直列連鎖コーディング）」、ｓｕｂｍｉｔｔｅｄ ｔｏ ＩＥＥＥ Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ Ｌｅｔｔｅｒｓ，２００４；Ｄ．Ｄｉｖｓａｌａｒ ａｎｄ Ｓ．Ｄｏｌｉｎａｒ、「Ｃｏｎｃａｔｅｎａｔｉｏｎ ｏｆ Ｈａｍｍｉｎｇ Ｃｏｄｅｓ ａｎｄ Ａｃｃｕｍｕｌａｔｏｒ Ｃｏｄｅｓ ｗｉｔｈ Ｈｉｇｈ Ｏｒｄｅｒ Ｍｏｄｕｌａｔｉｏｎ ｆｏｒ Ｈｉｇｈ Ｓｐｅｅｄ Ｄｅｃｏｄｉｎｇ（高速デコーディングための上

位変調によるハミングコードと累算器コードとの連結）」、ＩＰＮ　Ｐｒｏｇｒｅｓｓ　Ｒｅｐｏｒｔ　４２－１５６，Ｊｅｔ　Ｐｒｏｐｕｌｓｉｏｎ　Ｌａｂｏｒａｔｏｒｙ，Ｆｅｂ．１５，２００４。

【0066】

Ｙｅｄｉｄｉａ，ｅｔ　ａｌ．により２００４年８月２７日に出願された、「Ｃｏｍｐｒｅｓｓｉｎｇ　Ｓｉｇｎａｌｓ　Ｕｓｉｎｇ　Ｓｅｒｉａｌｌｙ－Ｃｏｎｃａｔｅｎａｔｅｄ　Ａｃｃｕｍｕｌａｔｅ　Ｃｏｄｅｓ（直列連鎖累積コードを使用して信号を圧縮する）」という発明の名称の米国特許出願第１０／９２８，４４８が、引用によりここに援用されるが、これには、この発明によって使用されるようなＳＣＡコードに基づく、我々の好適なシンドロームエンコーダの動作が記載されている。

【0067】

バイオメトリックパラメータ３０１ための我々のシンドロームエンコーダ３３０には、多くの利点がある。そのシンドロームエンコーダ３３０は整数値入力で作動することができる。対照的に、従来のエンコーダは一般的に２進値入力で作動する。シンドロームエンコーダは、バイオメトリックデータベース３５０のストリッジ（格納）要求条件を最小にするために、非常に高い圧縮率を有する。シンドロームエンコーダは、レート（ｒａｔｅ）適応型になるように設計できて、増加形式（漸増的）に作動することができる。

【0068】

認証フェーズ（段階）

【0069】

認証段階３２０では、ユーザからバイオメトリックデータを再び取得する。認証バイオメトリックパラメータＥ’３６０を得るために、特徴が抽出される。マッチ（一致）する登録シンドロームベクトルＳ３３１および登録ハッシュＨ３４１を見つけるために、データベース３５０が検索される。

【0070】

この検索によりデータベース３５０のあらゆるエントリ（Ｓ－Ｈペア）をチェックすることができ、或いはまたヒューリスティック（発見的）に順序付けられた検索を使用して、マッチするエントリを見つけるプロセスを加速することができる。具体的には、データベースのｉ番目のシンドロームベクトル－ハッシュペアを（$Ｓ_{ｉ}$、$Ｈ_{ｉ}$）と表すならば、全数探索により最初に、シンドローム復号化をＥ’および$Ｓ_{１}$に適用して、シンドロームデコーダ出力のハッシュを$Ｈ_{１}$と比較する。アクセスが拒否されるならば、同じプロセスが（$Ｓ_{２}$、$Ｈ_{２}$）で試みられ、次に（$Ｓ_{３}$、$Ｈ_{３}$）など、すべてのエントリが試みられるまで、或いはまた、アクセスが許可されるまで、実行される。

【0071】

登録ユーザ名などのその他の情報が利用可能であれば、検索を加速できる。たとえば、登録ユーザ名のハッシュ（バイオメトリックパラメータのハッシュＨと混同すべきではない）は、登録段階の間、ペアＳおよびＨとともに格納される。次に、認証段階では、ユーザは認証ユーザ名を提供し、またシステムはその認証ユーザ名のハッシュを判別して、マッチ（一致）するハッシュ化登録ユーザ名でＳ－Ｈペアに対してデータベースを検索し、その結果得られたＳ－Ｈペアを有するＥ’を認証するよう試みる。

【0072】

具体的には、シンドロームデコーダ３７０が登録シンドロームベクトルＳに適用され、この際、認証パラメータＥ’３６０は「副」情報として働く。シンドロームデコーダは、当技術分野では一般的に知られている。典型的には、確率伝播すなわちターボ符号を使用するデコーダは、低い複雑さで素晴らしいエラー復元力を持っている。シンドロームデコーダ３７０の出力は復号された登録パラメータＥ”３７１である。復号された値Ｅ”３７１は、シンドロームベクトルＳ３３１を生成するのに使用された元のバイオメトリックパラメータＥ３０１の推定値である。ハッシュ関数３４０は、認証ハッシュＨ’３８１を生成するために、Ｅ”３７１に適用される。

【0073】

登録値および認証値Ｈ３４１およびＨ’３８１が互いに比較３９０される。それらの値が一致しないならば、アクセスは拒否３９２される。そうでなければ、値Ｅ”３８１は元のバイオメトリックＥ３０１にほぼ（実質的に）一致する。この場合、ユーザはアクセス３９１を許可されることができる。

【0074】

また、ユーザを認証するため、復号されたパラメータＥ”３８１と認証バイオメトリックパラメータＥ’３６０とを直接比較してもよい。たとえば、Ｅ’およびＥ”が顔認識システムでバイオメトリックパラメータに対応するならば、顔の間の類似性を比較するための在来型アルゴリズムをパラメータＥ’およびＥ”に適用してもよい。

【0075】

シンドロームに基づくデータ暗号化

【0076】

図5は、データ５０１をコード化（符号化）５１０および復号化５２０するための方法５００を示している。コード化プロセス５１０では、第１のユーザから最初のバイオメトリックパラメータＰ５０２を得る。パラメータは、暗号文Ｃ５４１を生成するために、入力データＤ５０１を暗号化５４０するのに使用される。ところで、従来技術と対比して、第1のバイオメトリックパラメータＰはメ決してモリに格納されない。その代わりに、シンドロームエンコーダ５３０は、シンドロームベクトルＳ５３１を生成するために、第１のバイオメトリックパラメータＰをコード化し、また、ペア（Ｓ、Ｃ）が互いに関連付けられてメモリ５５０に格納される。この発明の実施の形態１では、入力データは、登録プロセスの間にユーザから取得された生のバイオメトリックデータである。

【0077】

人が暗号文５４１を解読５２０したいと思うとき、第2のユーザからバイオメトリックパラメータＰ’５６０を取得する。格納されたシンドロームベクトルＣ５３１は、第２のバイオメトリックパラメータを使用してシンドローム復号化され、第3のバイオメトリックパラメータＰ”５７１を生成する。そして、第3のバイオメトリックパラメータＰ”は、出力データＤ’５０９を生成するために、暗号文５４１を解読５８０するのに使用される。明らかに、第２または第3のバイオメトリックパラメータが第1のバイオメトリックパラメータと一致しないならば、出力データＤ’５０９は入力データＤ５０１と一致しない。出力データは、第１のユーザと第２のユーザが正確に同一人である場合にだけ、入力データと一致するであろう。

【0078】

この発明の実施の形態１では、前述と同様に、バイオメトリックパラメータのハッシュＨもまた格納できる。ハッシュ同士が一致するのをチェックすることにより、復号化が成功したことを確認する。ハッシュがなければ、セキュリティは維持されるが、デコーダは、復号化が成功したことを確認できない。多くの形式のソースデータには、不正確な復号化に起因するファイルは有用なものは何ら対応しないので、ハッシュは必要でない。

【0079】

本方法には、以下の利点がある。敵対者がシンドロームベクトルおよび暗号文（Ｓ、Ｃ）へのアクセスを得たとしても、データを解読することができない。これは、シンドロームベクトルから暗号キー、すなわち第１のバイオメトリックパラメータＰを再生できないからである。また、シンドロームコードの誤り訂正特性により、第２のバイオメトリックパラメータＰ’が第１のバイオメトリックパラメータＰと若干異なっても、適切に設計されたシンドロームデコーダは、暗号キーＰ５０２として使用された第１のバイオメトリックパラメータと正確に同じ第３のバイオメトリックパラメータＰ”を成功裏に生成することができる。

【0080】

シンドロームコード化は、バイオメトリックパラメータを安全に格納する効果的な方法を提供し、また、バイオメトリックな情報を安全に格納する他の方法にも適用できる。なお、バイオメトリックデータから特徴ベクトルを抽出できることに注意するべきである。

したがって、上述したバイオメトリックパラメータのいずれも、対応する特徴ベクトルで代替することができる。

【0081】

暗号化された形式でバイオメトリックパラメータを格納することの追加の利点は、これが、安全なバイオメトリックストリッジアプリケーション（バイオメトリック格納への適用）がバイオメトリック認識アプリケーション（バイオメトリック認識への適用）で使用されたものと異なる特徴ベクトルで作動するのを可能にすることである。たとえば、指紋認識システムは、しばしば指紋の画像から抽出された、いわゆる「マニューシャ（特徴：ｍｉｎｕｔｉａｅ）」に基づく特徴ベクトルを使用する。同様に、虹彩認識システムは、虹彩画像を１列のガボール（Ｇａｂｏｒ）フィルタに通過させることにより抽出された特徴を使用することもある。

【0082】

多くの場合、バイオメトリック認識（たとえば、顔認証や指紋による本人確認）用の理想的な特徴ベクトルは、シンドロームコード化／復号化のための理想的な特徴ベクトルと異なる場合がある。多くの場合、これは、認識（ｒｅｃｏｇｎｉｔｉｏｎ）または確認（ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）システムのための分類子、たとえば、ガウス混合モデル（GMM）、或いはニューラルネットワーク、或いは隠れマルコフ（Ｍａｒｋｏｖ）モデルに基づく分類子、を訓練するためのプロセスは、シンドロームエンコーダやデコーダの確率伝搬デコーダとともに用いられるヒストグラムを訓練するために使用されるプロセスとは異なる特徴ベクトルを生成することによる。

【0083】

図６は、入力バイオメトリックデータ６０１の暗号化されたバージョンを格納するための方法６００を示している。上述したように、バイオメトリックデータは、ユーザのバイオメトリック特性を測定或いは検知するのに使用される生の信号から得る。

【0084】

アクセス制御システムの登録段階６１０では、たとえば、ユーザから最初のバイオメトリックデータＢ６０１を取得する。次に、最初のバイオメトリックデータＢ６０１から第１のバイオメトリックパラメータＰ６０２の特徴ベクトルを得る。第１のバイオメトリックデータＢは、暗号キーとして第１のバイオメトリックパラメータＰを使用して暗号化６４０され、暗号文Ｃ６４１を生成する。さらに、第１のバイオメトリックパラメータは、シンドロームコード化されて、シンドロームベクトルＳ６３１を生成する。そして、関連付けられたペア（Ｓ、Ｃ）がバイオメトリックデータベース６５０に格納される。

【0085】

認証段階６２０では、ユーザから認証用の第２のバイオメトリックデータＢ’６６０を得る。この第２のデータは、第２のバイオメトリックパラメータＰ’６６１の特徴ベクトルを生成するのに使用される。そして、シンドロームデコーダ６７０は、第１のバイオメトリックパラメータを復号して、第３のバイオメトリックパラメータＰ”６７１を生成する。次に、第３のバイオメトリックパラメータをキーとして使用して暗号文Ｃを解読６８０して、第３のバイオメトリックデータＢ”６８１を生成する。その後、認証バイオメトリックデータＢ’および復号されたバイオメトリックデータＢ”をバイオメトリック認識法６９０のより比較して、特有の関数へのアクセスが許可されるか拒否されるかを判別する６９２。前述したように、第１および第３バイオメトリックデータが正確に同じである場合、すなわち最初および次のユーザが同じ人間である場合にだけ、アクセスが許可される。

【0086】

別の変形例では、比較ステップは、バイオメトリックデータから抽出された特徴ベクトルを使用できる。それらの特徴ベクトルは、バイオメトリックパラメータと同じである必要はない。さらに、検証ステップは完全に異なるプロセスを使用できるので、比較されるそれら２つの特徴ベクトルは、ほぼ（実質的に）同じであればよい。このようにして、特徴ベクトルは、時間経過とともに特定のユーザを特徴付けるバイオメトリックデータの変

動（バラツキ）における、より広い範囲を許容することができる。

【0087】

我々は、図６に示されるプロセスの幾つかの利点を列挙する。認証システムは、ステップ６９０で従来の認識システムを使用できる。また、シンドロームエンコーダ／デコーダによって使用されるバイオメトリックパラメータＰおよびＰ’は、バイオメトリックな検証ステップ６９０によって使用されるパラメータまたは特徴ベクトルの如何にかかわらず選択できる。その上、シンドロームコード化はバイオメトリックパラメータを安全に格納する効果的な方法である。ところで、図６に示される方法は、バイオメトリックパラメータを安全に格納する他の方法にも適用できる。

【0088】

安全なバイオメトリックパラメータのための最適のシンドロームコードの設計

【0089】

一般に、バイオメトリックパラメータとバイオメトリック特徴とを保護するためにシンドロームコードを使用する際のセキュリティと精度との間には、トレードオフがある。具体的には、如何なるシンドロームコードのキーパラメタも、シンドロームベクトルにおけるビットの数である。多くのビットを有するシンドロームベクトルは、バイオメトリックデータに関するより多くの情報を伝達して、バイオメトリックデータにおけるノイズと変動を許容することをより容易にする。対照的に、より小さなシンドロームベクトルは、より少ない情報を敵対者に与えるが、エラーをより生じやすい傾向がある。

【0090】

或る極端な場合、シンドロームベクトルの長さがその基礎となるバイオメトリックデータの長さとほぼ同じであるとき、元のバイオメトリックデータはシンドロームベクトルのみから正確に再生できるので、如何なる量のノイズも許容できる。勿論、この場合、シンドロームベクトルを得る敵対者はまたバイオメトリックデータを再生することができるので、システムのセキュリティを危険にさらすことになる。

【0091】

それとは正反対に、非常に少ないビット数のシンドロームベクトルは、敵対者がそのシンドロームベクトルからバイオメトリックデータを再生できないという意味で、非常に良いセキュリティを提供する。しかし、この場合、登録バイオメトリックデータと認証バイオメトリックデータとの間の許容できる変動（バラツキ）は限定的である（小さい）。

【0092】

明らかに、シンドロームに基づくエンコーダおよびデコーダは、セキュリティとバイオメトリック変動（バラツキ）に対する許容度とをバランスさせるシンドロームベクトルのための長さを選択するべきである。ところで、入念に設計されたシンドロームコードはエラー復元力を改善できる。

【0093】

図１２に示されるように、以下の用語でシンドロームコードのデザインと動作について記述する。バイオメトリックデータ１２０１は、たとえば、顔や指紋の画像でよい。完全な特徴ベクトル１２０２はトレーニングバイオメトリックデータから抽出される。完全な特徴ベクトル１２０２はシンドローム特徴ベクトル１２０３まで減少される。シンドローム特徴ベクトルは、デザイナーがシンドロームコード化および復号化のために適切であると判断する、完全な特徴ベクトルの部分をキャプチャする。シンドローム特徴ベクトルからシンドロームベクトル１２０４をコード化するのに、シンドロームコードが使用される。シンドローム特徴ベクトル１２０３は図3においてバイオメトリックパラメータＥ３１０の役割を担い、一方、シンドロームベクトルはＳ３３１である。

【0094】

バイオメトリック統計モデル

【0095】

図１３は、この発明の実施の形態によるシンドロームコード１２０４および対応するデコーダ１２０５（すなわちエンコーダおよびデコーダ）を構成するためのプロセス１３０

０を示している。トレーニングバイオメトリックデータ１３０１を取得する。選択された特徴モデル１３０４のパラメータ１３０２を、トレーニングデータから決定１３１０する。コーデックに関して、特徴モデルは本質的には「ソース」モデルである。同様に、選択された測定モデル１３０５のパラメータ１３０３を１３２０決定する。測定モデルは、実質的には、「チャンネル」モデルである。そして、パラメータ１３０２－１３０３およびモデル１３０４－１３０５は、シンドロームコードおよび対応デコーダを構成するのに使用される。なお、チャネルモデルは計測プロセスにおける構造化ノイズに対処するように設計されていることに注意するべきである。このノイズはたとえば、異なる計測インスタンスで観測されるようなバイオメトリックデータの特徴における変化や、インスタンス間の特徴の挿入および削除によって引き起こされ得る。

【0096】

機械学習の多くのツールは上記の設計プロセス（工程）で役立ち得るが、結果として得られるモデルがシンドロームコード化のために適切な「ハード」特徴ベクトルを有するので、この問題は、機械学習における多くのモデル化問題とは可成り異なる。「ハード」および「ソフト」特徴ベクトル間の相異について、以下で詳細に議論する。

【0097】

図１２に示されるように、シンドローム特徴ベクトル１２０３は、シンドローム復号化を取り扱い易くするために、典型的には、減少されたサイズ（大きさ）である。シンドロームコードを構成するために、デンシティエボリューション（ｄｅｎｓｉｔｙ　ｅｖｏｌｕｔｉｏｎ）を度数分布（ｄｅｇｒｅｅ　ｄｉｓｔｒｉｂｕｔｉｏｎ）に適用できる。シンドロームコードは、シンドロームベクトル１２０４をユーザ間に亘るバイオメトリック特徴における変動（バラツキ）に一致させるために、シンドローム特徴ベクトル１２０３の有限ブロック長などの特徴、或いは可変レートコードを使用する必要性、を考慮に入れるためにさらに洗練される。

【0098】

シンドロームコードが構成されて選択された後に、以下に述べるように、繰り返しの確率伝搬デコーダを構成する。

【0099】

量子化

【0100】

図７に示されるプロセス１３００のインスタンス７００を詳しく述べる前に、先ず、認証のときに登録中および認証中のバイオメトリックデータの使用を区別する以下の用語を定義する。特徴ベクトルの量子化バージョンに言及するために「ハード」特徴ベクトルという用語を使用し、非量子化特徴ベクトル、または細かく量子化された特徴ベクトルのバージョンに言及するために「ソフト」特徴ベクトルという用語を使用する。

【0101】

幾つかのバイオメトリックパラメータは、比較的大きな数値範囲に亘って、整数および実数を含むことができるため、量子化が使用されている。暗号化、キー発行、および他の認証プロセス（過程）は小さな範囲に亘って整数でベストに働く。

【0102】

「ハード」特徴ベクトルと「ソフト」特徴ベクトルとを区分けする理由は、シンドロームベクトルが「ハードな」特徴ベクトルから得られるためである。したがって、「ハード」特徴ベクトルは通常、量子化される。対照的に、認証段階の間、シンドロームデコーダは、「ハード」特徴ベクトルを復号するために、シンドロームベクトルに「ソフト」特徴ベクトルを結合してもよい。したがって、「ソフト」特徴ベクトルは、量子化される必要がないか、またはシステムにおけるエラーを小さくするために異なるように量子化され得る。たとえば、ソフト特徴ベクトルの使用により、シンドロームデコーダは各特徴の最も可能性のありそうな選択の困難な決断より、むしろ各特徴の尤度（ｌｉｋｅｌｉｈｏｏｄｓ）を入力として取ることが可能になる。

【0103】

一般に、バイオメトリックデータから完全な特徴ベクトルに抽出する複数の方法があり、また、完全な特徴ベクトルから「ハード」および「ソフト」特徴ベクトルを抽出する複数の方法がある。したがって、図１３のプロセスを各可能性に適用して、トレーニングの間、最も良い総合的な結果をもたらすシンドローム特徴ベクトル１３０４を選択する。

【0104】

図7は、最適のシンドロームを構成するためのプロセス１３００のインスタンスの詳細を示しており、ここで、バイオメトリック特徴１３０４に対する統計モデルはバイオメトリック特徴の間のマルコフ関係を表す。トレーニングバイオメトリックデータを取得８００する。バイオメトリックデータは、エラーヒストグラム８９０を生成するのに使用される。エラーヒストグラムはシンドローム特徴ベクトルを選択９００するのに使用される。このような関係において、すべてのバイオメトリックパラメータを表すのに「完全な特徴ベクトル」１２０２（図１２を参照）という用語を使用し、また、完全な特徴ベクトルの部分集合を表すのに「シンドローム特徴ベクトル」１２０３という用語を使用する。シンドローム特徴ベクトルを任意の特徴空間に変形することができる。

【0105】

シンドローム特徴ベクトル１２０３が選択された後に、私たちはシンドローム特徴ベクトルの異なる係数の間の相関関係を測定１０００する。次に、シンドローム特徴ベクトルと係数間相関関係に対するエラー統計を使用することによって、デンシティエボリューション７４０を適用して、所与の長さの最適のシンドロームコード１２０４をもたらす度数分布を検索する。シンドローム特徴ベクトルおよびシンドロームコードが選択された後に、係数間相関関係を利用する確率伝搬デコーダを構成１１００する。

【0106】

エラーヒストグラムを構成する

【0107】

図8は、エラーヒストグラム８９０を生成するためのプロセス８００を示している。最初に、異なる機会に採られた特定のユーザのためのトレーニングバイオメトリックデータを取得８１０する。次に、一対のバイオメトリックパラメータＢおよびＢ’を選択８２０して、完全な「ソフト」特徴ベクトルＶＳ（Ｂ）８３０および完全な「ハード」特徴ベクトルＶＨ（Ｂ’）８４０を決定する。そして、完全な特徴ベクトルの中の各特徴または寸法（ｄｉｍｅｎｓｉｏｎ）ｉに対して、位置ｉのＶＳ（Ｂ）から対応する特徴ｉにおけるＶＨ（Ｂ’）の値を推定８４５し、その推定値が正しいか否かを判定８５０する。その推定値が正しくなければ、エラーヒストグラム８９０における特徴ｉでのＶＨ（Ｂ’）およびＶＳ（Ｂ）の対応する値に対する階級（ｂｉｎ）をインクリメントする。各特徴ｉに対してこの過程を完了した後に、すべてのペアのバイオメトリクス（生体認証）ＢおよびＢ’が処理されたか否かをチェック８６０する。そうでなければ、ステップ８２０に戻って、別のペアのバイオメトリックパラメータを選択する。すべてのペアが既に処理されていれば、エラーヒストグラムが完了し、本プロセスは終了８８０する。

【0108】

シンドローム特徴ベクトルの選択

【0109】

図9は、図8のエラーヒストグラムの支援によりシンドローム特徴ベクトルを選択するためのプロセス９００を示している。まず最初に、エラーヒストグラムは信頼性の最も高い特徴から最も低い特徴９２０へソート（並べ替え）される。具体的には、Ｅ（ｉ）がＶＳ（Ｂ）の特徴ｉからＶＨ（Ｂ’）の特徴ｉを予測するさいの平均誤差であるならば、特徴ｉは、Ｅ（ｉ）＜Ｅ（ｊ）のときに、特徴ｊよりも信頼できると考えられる。エラーヒストグラムがソートされた後に、エラーヒストグラムから次に最も信頼できる特徴をシンドローム特徴ベクトルに含めて９３０、現在のシンドローム特徴ベクトルに対する最も良いシンドロームコードを構成し９４０、最新の特徴を含めることがセキュリティすなわちエラー復元力を増大させるか否かをテスト９５０する。セキュリティすなわちエラー復元力が増大するならば、シンドローム特徴ベクトルに付加的な特徴を追加し続ける。さもな

ければ、特徴ベクトルから最も最近に加算された特徴を取り除き９６０、そして、本プロセスを終了９７０する。

【0110】

セキュリティのレベルを特定して、エラー復元力を最適化することを望むならば、ステップ９４０および９５０に対して以下のステップを使用できる。まず最初に、ステップ９４０で、ｋシンドロームを有する低密度パリティチェック（ＬＤＰＣ）コードを固定度数分布から生成することによって、特徴ベクトルの中の現在の特徴の数に対応する長さＮの新しいシンドロームコードが構成される。この場合、セキュリティのレベルは、数量Ｎ－ｋを固定して、且つ本プロセス中それを一定に保っことによって一定に保たれる。そして、バイオメトリックデータのランダムなバイオメトリックサンプルがデータベースから選択され、ＬＤＰＣコードのパリティチェックマトリクスを適用することによって、シンドロームベクトルへマッピングされ、この結果得られたシンドロームベクトルは、同じユーザからの別のランダムなバイオメトリックサンプルに適用された確率伝搬を使用して復号される。これを何回も繰り返すことにより、与えられた特徴ベクトルに対するシンドロームコードのエラー復元力の推定値を生成する。或いはまた、計算上の更なる複雑さが設計プロセス（工程）で許容できるならば、そのコードに対する度数分布を最適化して、より精度よく誤り確率を推定するためにデンシティエボリューションプロセスを使用できる。これに関して、Ｔ．Ｊ．Ｒｉｃｈａｒｄｓｏｎ，Ｍ．Ａ．Ｓｈｏｋｒｏｌｌａｈｉ，ａｎｄ Ｒ．Ｌ．Ｕｒｂａｎｋｅ，ｄｉｓｃｕｓｓｅｄ，「Ｄｅｓｉｇｎ ｏｆ ｃａｐａｃｉｔｙ－ａｐｐｒｏａｃｈｉｎｇ ｉｒｒｅｇｕｌａｒ ｌｏｗ－ｄｅｎｓｉｔｙ ｐａｒｉｔｙ－ｃｈｅｃｋ ｃｏｄｅｓ」、ＩＥＥＥ Ｔｒａｎｓａｃｔｉｏｎｓ ｏｎ Ｉｎｆｏｒｍａｔｉｏｎ Ｔｈｅｏｒｙ，Ｖｏｌｕｍｅ ４７，Ｉｓｓｕｅ ２，ｐｐ．６１９－６３７，Ｆｅｂｒｕａｒｙ ２００１を参照。なお、この文献は引用によりここに援用される。

【0111】

エラー復元力のレベルを特定して、最高のセキュリティを得ることを望むならば、ステップ９４０および９５０に対して以下のステップを使用できる。まず最初に、ステップ９４０では、特徴ベクトルの中で現在の特徴の数に対応する長さＮの新しいシンドロームコードが、デンシティエボリューションを使用して、設計される。具体的には、デンシティエボリューションによって評価されるように、エラー復元力の特定のレベルを満たす最も高いレートコードが見つかるまで、デンシティエボリューションを使用して、一連の異なるレートコードが構成される。

【0112】

このプロセスによって選択された特徴ベクトルは、そのシンドロームコードのために特別に設計された特徴ベクトルであるため、「シンドローム特徴ベクトル」として言及される。なお、この特徴ベクトルは、顔或いは物体の認識などのバイオメトリック認識のために構成された他のタイプの特徴ベクトルとは異なる特性を持つことができることに注意すべきである。

【0113】

係数間相関関係を測定する

【0114】

シンドローム特徴ベクトルが選択された後、次のステップは、データが互いに相関すると信じられるならば、その係数間相関関係を測定することである。図７によりエラーヒストグラムは完全な特徴ベクトル１２０２に対して生成されたものなので、そのエラーヒストグラムからこの情報を抽出することはできない。ステップ９００は、シンドローム特徴ベクトル１２０３を生成するために、完全な特徴ベクトルの中の特徴の部分集合だけを選択する。

【0115】

図１０は、バイナリ（２進の）シンドローム特徴ベクトルにおける一次相関関係を測定するためのプロセス１０００を示している。このプロセスはまた、非バイナリ特徴ベクト

ルまたは高次相関に適用できる。まず最初に、バイオメトリックトレーニングデータセットから要素が選択され、そして、シンドローム特徴ベクトルがその要素から抽出される。それから、カウンタ変数ｉがゼロに初期化１０１０される。次に、特徴ｉが０であるか１であるかを検査して、前者（すなわち０）の場合にはステップ１０３０へ進み、後者（すなわち１）の場合にはステップ１０４０へ進む。その後、特徴ｉ－１、すなわち１つ前の特徴、が０であったか１であったかを検査して、ヒストグラム中の適切な階級（ｂｉｎ）をインクリメント（増分）１０３５する。直観的には、階級ｐ００はａ０が後続するａ０の出現を計数し、また、階級ｐ０１はａ１が後続するａ０の出現を計数する、などである。次に、カウンタｉを増分１０５０し、更なる（処理されていない）特徴がシンドローム特徴ベクトルに残っていないか検査１０６０して、次の特徴に対して本プロセスを繰り返す。そうでなければ、すなわち各特徴を既に処理していれば、本プロセスを終了１０７０する。

【0116】

図１０のプロセスがバイオメトリックトレーニングセット（生体認証訓練集合）の各要素に対して実行された後、シンドローム特徴ベクトルの一次相関関係を測定するために、階級ｐ００、ｐ０１、ｐ１０、およびｐ１１の値を該バイオメトリックトレーニングセットのサイズ（大きさ）で除算する。

【0117】

最適のシンドロームコードを構成するためにデンシティエボリューションを使用する

【0118】

シンドローム特徴ベクトル１２０３が選択されて、係数間相関関係が測定された後、デンシティエボリューションを使用してシンドロームコード１２０４を設計する。具体的には、ＬＤＰＣシンドロームコードに対して、シンドロームコード用の度数分布を設計する。

【0119】

実際に最適度分布を構成するために、デンシティエボリューション技術を適用して幾つかの候補度数分布を生成する。

【0120】

ところで、当技術分野で知られているような従来のデンシティエボリューションプロセスは係数間相関関係を考慮していない。したがって、デンシティエボリューションによって生成された候補度数分布は、係数間相関関係がないケースに対して適切であるかもしれないが、係数間相関関係が存在するときには、一般的には、異なった振る舞い方をする。

【0121】

シンドロームコードに対して最も良い度数分布を得るために、バイオメトリックトレーニングデータセットでデンシティエボリューションによって得られた候補度数分布同士を比較して、最善に振る舞う度数分布を選択する。代わりの実施の形態では、係数間相関関係を考慮に入れるように、従来のデンシティエボリューションアルゴリズムを変更する。

【0122】

シンドロームコードに対する確率伝搬デコーダを構成する

【0123】

シンドロームコードを設計する際の最終的なステップは、関連付けられた確率伝搬シンドロームデコーダ１２０５を構成することである。

【0124】

図１１Ａは登録段階のハイレベル構造を示しており、ここで、エンコーダ３３０は、シンドロームコード１１０２を使用して、シンドローム特徴ベクトル１２０３からシンドロームベクトル１２０４を生成する。

【0125】

図１１Ｂは、認証段階の間に使用される相補型（ｃｏｍｐｌｅｍｅｎｔａｒｙ）デコーダ１１０７に対する構造を示している。再び、認証を試みるユーザについてバイオメトリックデータ１１０４のノイズの入った観測が取得される。元のシンドローム特徴ベクトル

１２０３の推定値１１０８を復号１１０７して生成するために、バイオメトリックデータ１１０４は、その測定モデル１３０５（および測定モデルパラメータ１３０３）とともに、反復確率伝搬ネットワーク（ファクタ（要素）グラフ）におけるシンドロームベクトル１２０４および特徴モデル１３０４（およびその特徴モデルのパラメータ１３０２）とともに使用される。復号化が成功するならば、推定されたシンドローム特徴ベクトル１１０８と元のシンドローム特徴ベクトル１２０３とは一致する。

【0126】

図１１Ｃに示されるように、我々の確率伝搬ファクターグラフの構成１１００は、シンドロームコード１１０２および可変ノード（＝）１１２０を特定するチェックノード（＋）１１１０に加えて、特徴モデル１３０４（およびモデルパラメータ１３０２）を特定する相関関係ノード（Ｃ）１１３０を含む。具体的には、相関関係ノードは各ペアの連続した可変ノードの間に加えられる。可変ノードから隣接するチェックノードまでメッセージを流通させる方法は、他のメッセージで乗算される、各隣接相関ファクターノードからの追加メッセージを含むように変更される。

【0127】

具体的には、Ｋｓｃｈｉｓｃｈａｎｇ外の表記を使用して、μ_{y}→ｆ（ｘ）がチェックｆから可変ノードｙへの状態ｘに対する入力メッセージであり、Ｌ（ｘ）が左の相関関係ノードからの入力メッセージであるならば、可変ノードから右の相関関係ノードへの出力メッセージは、次式で表される。

Ｌ（ｘ）・$\Pi\mu_{y}\rightarrow_{f}$（ｘ），

一方、左の相関関係ノードへの出力メッセージは次式で表される。

Ｒ（ｘ）・$\Pi\mu_{y}\rightarrow_{f}$（ｘ），

ここで、Ｒ（ｘ）は右の相関関係ノードからの入力メッセージである。

【0128】

また、この発明の実施の形態による、メッセージを相関関係ノードに対して流通（入出力）する方法についても記述する。具体的には、メッセージＬ（ｘ）およびＲ（ｘ）を判別するための処理手順について記述する。μ（０）が左の相関関係ノードへの入力メッセージであるならば、その相関関係ノードの右側への出力メッセージ、すなわちその相関関係ノードの右側の可変ノードへの入力メッセージ、は次式で表される。

Ｌ（０）＝ｐ００・μ（０）＋ｐ１０・μ（１）　ａｎｄ　Ｌ（１）＝ｐ１０・μ（０）＋ｐ１１・μ（１），

ここで、ｐ００、ｐ０１、ｐ１０、およびｐ１１の項は、図１０に示されるように、測定された一次相関関係値である。

【0129】

同様に、その相関関係ノードの左側の出力メッセージ、すなわちその相関関係ノードの左の可変ノードへの入力メッセージ、は次式で表される。

【0130】

Ｒ（０）＝ｐ００・μ（０）＋ｐ０１・μ（１）　ａｎｄ　Ｒ（１）＝ｐ０１・μ（０）＋ｐ１１・μ（１）．

【0131】

虹彩バイオメトリックパラメータに対するシンドロームコード設計

【0132】

次に、処理手順７００の虹彩バイオメトリックパラメータの特定のケースへの適用について記述する。完全な「ハード」特徴ベクトルは、「Ｈｏｗ　ｉｒｉｓ　ｒｅｃｏｇｎｉｔｉｏｎ　ｗｏｒｋｓ」，ｂｙ　Ｊ．Ｄａｕｇｍａｎ　ｉｎ　ＩＥＥＥ　Ｔｒａｎｓａｃｔｉｏｎｓ　ｏｎ　Ｃｉｒｃｕｉｔｓ　ａｎｄ　Ｓｙｓｔｅｍｓ　ｆｏｒ　Ｖｉｄｅｏ　Ｔｅｃｈｎｏｌｏｇｙ，Ｖｏｌｕｍｅ　１４，Ｉｓｓｕｅ　１，Ｊａｎ．２００４　ｐａｇｅｓ　２１－３０に記述されるように、１組のガボールフィルタから抽出されたビットのシーケンスであるように選択される。この文献は引用によりここに援用される。

【0133】

完全な「ハード」特徴ベクトルはバイナリ（２元）であるが、完全な「ソフト」特徴ベクトルはクオターナリ（４元）であるように選択される。具体的には、特徴ｉの完全な「ソフト」特徴ベクトルの値は、その特徴が「ハード」特徴ベクトルにおいて最良の推測であるように選択され、また信頼レベル（信頼度）を示すビットが追加される。詳細には、その特徴に対する判定に自信があるか、または自信が無いかを示すビットが追加された。

【0134】

たとえば、「ハード」特徴ベクトルの幾つかの特徴は、予測するのが難しいかもしれない。その理由は、たとえば、それらの特徴が、瞼或いは睫毛よって覆われて、「自信が無い」という信頼度数値を受けるべきであるからである。

【0135】

次に、図８について上述したように、エラーヒストグラムを作成するために、バイオメトリックトレーニングデータを使用し、それから図９の特徴ベクトル設計方法を適用する。完全な特徴ベクトルは約１万の長さを有するが、我々は、多くの特徴１２０２が信頼できないことを発見した。たとえば、目の上端に対応する特徴ベクトルの構成要素はしばしば瞼または睫毛で覆われる。最も信頼の低い特徴が図９の処理手順によって捨てられた後、シンドローム特徴ベクトル中のおよそ２，０００の最も信頼できる特徴が残される。

【0136】

図７におけるステップ９００で処理を止めると、結果として得られるシンドロームベクトルは、単一ユーザに対する虹彩バイオメトリックパラメータにおける自然な変動（バラツキ）を許容しうるようなエラー復元力を有さないであろう。具体的には、或る日に採られたユーザの虹彩の計測が異なる日に採られ同じ虹彩からの計測に結合された状態でコード化されたシンドロームベクトルは、その時の約１２％の復号に失敗する。これは、図７における残りのステップに対する必要性を正当化する。

【0137】

図１０の手続きを使用して一次相関関係を測定した後、我々は、「ハード」シンドローム特徴ベクトルにおける或るビットが隣接ビットと同じ値を取る見込み（可能性）が、該隣接ビットの反対の値を取る見込み（可能性）の約２倍であることを検出した。そして、我々は、高い相関関係を利用するために、図７のステップ７４０を続けて、デンシティエボリューションを使用して最適化されたシンドロームコードを構成した。最終的に、高い一次相関関係を考慮に入れるために、ステップ１１００にしたがって確率伝搬デコーダを構成した。

【0138】

これらのステップに従うことにより、我々の初期のコードより１桁以上も信頼できるシンドロームコードを生成でき、したがって、図７の全体の手続きに従う利点を実証することができる。

【0139】

指紋特徴に対するシンドロームコード

【0140】

手続き１３００を指紋に適用する。指紋に基づくシステムは、一般に、パターンに基づくか、或いはマニューシャ（特徴）に基づく。ここでは、後者を使用する。指紋マニューシャから特徴ベクトルを抽出する。一般的な手順１３００を殆どのバイオメトリックデータに適用できるが、我々は、指紋のマニューシャに対する手続きの詳細について記述する。指紋マニューシャは、その特性として、時間経過とともに変動することがあり、また、計測プロセスは構造化ノイズを受け易い。

【0141】

図１４は、一例の指紋１４０１および抽出された特徴ベクトル１４０２を示している。抽出された特徴ベクトル１４０２はシンドローム特徴ベクトル１２０３の一例である。特徴は計測フィールド（観測窓）１４０３で測定されるのみである。便宜上、マニューシャは格子状の四角形で示される。各マニューシャはトリプレットにマッピングされ、たとえば、（ａ、ｂ、ｃ）は空間的な位置座標（ａ、ｂ）とマニューシャの角度（ｃ）を表す。

以下に述べるように、１つのマニューシャはアラインメント（位置合わせ、整列）の目的のための「コア」として指定することができる。

【0142】

指紋１４０１が測定される平面はピクセルのアレーを有するディジタルセンサによって量子化されるので、特徴はマトリクスとして格納される。各センサーピクセルはマトリクス１４０２における特定のエントリに対応している。マニューシャの存在（有ること）は「１」により表されるが、検知されたマニューシャの欠如（無いこと）はマトリクス１４０２において「０」で表される。より一般的な表示では、マニューシャの存在を意味する「１」の代わりに、マトリクスにおけるエントリはマニューシャの角度ｃであろう。

【0143】

マニューシャの数、位置、および角度は指紋の或る計測から次の計測までに変化する。たとえば、或る計測で（７４、５２、３６°）にマニューシャが存在すれば、別の計測では、それは（８０、４５、６３°）として現れるかも知れないし、或いは全く現れないかも知れない。

【0144】

様々な理由により、或る計測から次の計測までのマニューシャのこの変動性は、指紋を処理するための多くの従来の方法に対して問題を生じさせる。

【0145】

明白なバイオメトリックデータの変動性

【0146】

図に１５Ａ－１５Ｃに示されているように、我々のモデルはバイオメトリックデータにおける変動性に対処することができる。これらの図では、破線１５００はローカル（局所的）な近傍を示す。図１５Ａはマニューシャの運動１５０１（ｐｉ、ｊ）を示している。図１５Ｂは削除ｐｅ１５０２を示しており、また、図１５Ｃは挿入ｐｓを示している。

【0147】

図１６Ａおよび１６Ｂは、この発明の実施の形態による確率伝搬復号化１１０７を実施するために使用されるファクターグラフ１６００の高レベルおよび低レベルの詳細をそれぞれ示す。

【0148】

高レベルでは、バイオメトリックデータ１２０１は、シンドロームベクトル１２０４を生成するために使用されるシンドローム特徴ベクトル１２０３を生成するために使用される。しかし、シンドローム特徴ベクトル１２０３はデコーダにより知られていないが、シンドロームベクトル１２０４は知られている。シンドロームベクトル１２０４とシンドローム特徴ベクトル１２０３とは、コード構造１６２３によって関連付けられる。また、デコーダはバイオメトリックデータ１１０４のノイズの入った計測を得る。雑音構造は統計モデル１３０５により記述される。シンドロームベクトル１２０３とともに、コード構造１６２３、観測１１０４および測定モデル１３０５は、復号１１０７を行って、元のシンドローム特徴ベクトル１２０３の推定値１１０８を生成するために使用される。

【0149】

図１６Ｂはシンドローム特徴ベクトル、シンドロームベクトルおよびノイズの入った観測の統計モデルを記述するファクターグラフ１６００の低レベル構造を示している。

【0150】

特徴ベクトルグリッド（格子）１４０２の各位置ｔは、ファクターグラフ１６００における対応するバイナリ確率変数ｘ［ｔ］ノード１６０９を有する。この確率変数は登録の間、位置ｔに存在し、それ以外はゼロである、１つのマニューシャである。

【0151】

特徴ベクトルの格子位置とラベルｔとの関連付けは任意であり得る、たとえば、ラスタスーキャン順序でもよい。特徴集合の２次元的性質は、我々のモデルでも考慮に入れられる。

【0152】

各格子位置に対して、マニューシャが登録の間存在しているという事前確率がある。この事前確率、Ｐｒ［ｘ［ｔ］＝１］、はファクターノード１６０８により表される。

【0153】

その登録格子に対する可変ノード１６０９の各位置に対して、対応する認証格子に対する対応位置ノード１６０１がある。認証の間の格子位置ｔにおけるマニューシャの存在はバイナリ（２進）確率変数ｙ［ｔ］によって表される。マニューシャがプローブに存在していれば、この変数は1と等しく、そうでなければ、ゼロに等しい。ファクターグラフの目標は、登録時の指紋の最初の計測と認証時の２番目の計測との同時分布を表すことである。

【0154】

我々のモデルでは、各登録位置は、ｘ［ｔ］＝１の場合、位置ｔのマニューシャがプローブ内の位置ｔの近傍の位置へ移動する確率を持っているか、或いはまた、削除の場合には、測定されない。

【0155】

変数１６０４は登録マニューシャの位置の相対変化を表し、また、ファクターノード１６０３は挿入されたマニューシャの移動および確率に関する事前確率分布を表す。特に、図１６Ｂに示された１次元の移動モデルに対して、ｚ［ｔ］＝ｉは、登録時の位置ｘ［ｔ＋ｉ］のマニューシャが認証時に位置ｚ［ｔ］へ移動することを表す。より一般には、そして我々の実施では、２次元移動モデルを使用する。

【0156】

このような変位（移動）｛ｉ｝のドメインまたは近域（ｎｅｉｇｈｂｏｒｈｏｏｄ）は、破線１５００で表す設計パラメータである。変数ｚ［ｔ］＝ｓであれば、偽マニューシャが認証時に位置ｔに挿入され、また、ｚ［ｔ］＝＊は、認証時にマニューシャが位置ｔ存在しないことを示す。ｚ［ｔ］＝＊などのような変数ｚ［ｔ］とｙ［ｔ］＝0などのような変数ｙ［ｔ］との間には、正確な対応がある。

【0157】

位置ｔの登録マニューシャ、すなわちｘ［ｔ］＝１、は、ｔの近傍におけるたかだか１つの観測されたマニューシャについて説明できるだけであるという制約条件を表すために、我々はファクターノード１６０７を含める。これらのノードに接続される確率変数ｈ［ｔ］１６０６は、ｘ［ｔ］の削除を表すバイナリ変数である。削除は、検知されなかった或いは抽出されなかったマニューシャ、または登録時に検知された偽のマニューシャ、または大きな移動から生じ得る。ノード１６０５は各ｈ［ｔ］に対する事前分布を表す。

【0158】

各ノードｙ［ｔ］をその対応ノードｚ［ｔ］に接続するファクターノード１６０２は、該対応ノードｚ［ｔ］が＊でない場合にのみ、各認証マニューシャｙ［ｔ］がノンゼロでなければならないという概念を表す。

【0159】

このモデルに、シンドロームコード１１０２から生じる制約条件を加える。各シンドロームノードｓ［ｉ］１６１１はローカルコード制約条件１６１０を満し、その制約条件１６１０は、シンドロームの値が特徴ベクトルｘ１、ｘ２、…に適合する場合には１に等しく、そうでなければ、ゼロに等しい特性関数である。

【0160】

それらのマニューシャの方位をファクターグラフに加えることができる。方位情報を加えるために、登録ノード１６０９はマニューシャについて位置ｔと方位の両方を示す。また、この情報は事前確率ノード１６０８に反映される。登録時の方位をシンドロームコード化に必要なハード特徴ベクトルに適合させるために、該登録時の方位は量子化される。

【0161】

シンドロームビット１６１１のベクトルは、以上と同様にコード化されるが、今度は、マニューシャの存在の有無およびもし存在すれば、その方位を表す登録変数１６０９のベクトルからである。削除１６０５の事前確率は、移動に関する制約条件１６０７と同様に

、変化しないままである。移動と挿入１６０４の事前確率も変化しないままである。認証ノード１６０２上の制約条件ノードは、登録ノード１６０９と認証ノード１６０１との間の方位の変化がより少なるであろうという概念を反映するように変更される。

【0162】

メッセージ通過規則と最適化

【0163】

ファクターグラフ１６００によって表される計測および移動モデルを考えると、従来からの技術を使用することによりメッセージ通過規則を導き出すことができる。以下、複雑さの減少を実現するために、メッセージを通過させるための幾つかの簡素化について記述する。

【0164】

第１の簡素化は制約条件ノード１６０２からのメッセージに関連する。私たちは、観測されないマニューシャを取り除くためにファクターグラフから「余分なものを取り除く」。具体的には、制約条件１６０２の形式にしたがって、ｙ［ｔ］＝０であるなら、ノード１６０２からｚ［ｔ］可変ノード１６０４への唯一のノンゼロメッセージは状態ｚ［ｔ］＝＊に対するものである。

【0165】

その結果、隣接するノード１６０７に送られる唯一のノンゼロメッセージｚ［ｔ］は、＊状態に対するものである。我々は、この一定のメッセージが１に正規化されると仮定することができる。たとえば、ｙ［ｔ］＝ｙ［ｔ＋２］＝ｙ［ｔ＋４］＝ｙ［ｔ＋５］＝＊であれば、図１６Ｂの完全なファクターグラフを使用する代わりに、必要なメッセージ通過作用を導き出すために、図１７に示すように、余分なものを取り除いたグラフ１７００を使用する。これは、ノード１６０７に対するメッセージ計算の複雑さを大幅に減少させることに通じる。

【0166】

ファクターノード１６０７に出入りするメッセージを演算することによって、第２の簡素化が得られる。ｚ［ｔ］可変ノードからの完全なメッセージを使用する必要はない。代わりに、これらのメッセージを、ｘ［ｔ’］におけるマニューシャが位置ｚ［ｔ］に対応する位置へ移動するか否かを示すバイナリメッセージに減少させることができる。ノードｚ［ｔ］に対するバイナリ情報を使用することによって、可成り演算量を削減することができる。

【0167】

最初に１組の中間的数量を計算して、その後これらの中間的数量を再利用することにより、様々な規則に対する第３の簡素化を図ることができる。たとえば、可変ノードｚ［ｔ］からの出力メッセージは他のすべてのノードからの入力メッセージの積である。可変ノードｚ［ｔ］へのＫ個の接続があれば、この規則の簡単な実施は、他のＫ－１個の接続からのメッセージを結合しなければならないので、$Ｋ^2$ に比例する演算を必要とする。これをより効率的に行うためには、ノードｚ［ｔ］に対する限界確率（ｍａｒｇｉｎａｌ　ｂｅｌｉｅｆ）を計算するプロセスにおいて、一度、ノードｚ［ｔ］に入ってくるすべてのメッセージを結合する。そして、特定の接続に対する出力メッセージを得るために、対数尤度ドメインにおいて、その接続からの入力メッセージにより全メッセージを割り算或いは減算する。

【0168】

また、三角形ノードからの出力メッセージを計算する際に、中間的数量の同様の再利用を適用できる。特に、ｚ’［ｔ］が、可変ノードｚ［ｔ］から位置ｔ’のノード１６０７へのバイナリメッセージを表すものとする。数量ｚ’［ｔ］は、マニューシャが認証の間、位置ｔ’から位置ｔまで移動するか否かを示す。これらのバイナリメッセージに関するノード１６０７に対する簡単な合計積（ｓｕｍ－ｐｒｏｄｕｃｔ）の規則は、１６０４が位置ｔ’でノード１６０７に接続される可変ノードのすべての可能な組合せに亘って積算することを必要とする。たとえば、位置ｔ’におけるノード１６０７がノードｚ［１］、 ｚ［２］、ｚ［３］およびｚ［４］に接続されるならば、ｚ’［１］へのメッセージを演算することは、ｚ’［２］、ｚ’［３］およびｚ’［４］のすべての可能な組合せに亘って積算することを必要とする。この方法は、各三角形ノードに接続された可変ノードの数で指数関数的な計算の複雑さを有する。

【0169】

制約条件ノード１６０７が、高々ｚ’［ｔ］ノードの１つがノンゼロであることを許容することを実現することによって、この指数関数的な複雑さを解消することができる。このようにして、ノードｚ’［ｔ］に対する各出力メッセージは、他のすべてのノードｚ’［ｔ］がゼロであることに対応する項と、１つのノードがゼロであることを除いて他のすべてのノードｚ’［ｔ］に対応する項とを含む。これらの項をあらかじめ計算することによって、ファクターノード１６０７に対するメッセージ通過規則を、接続の数における指数関数的複雑さから接続の数における１次関数的複雑さへ減少させることができる。

【0170】

バイオメトリックパラメータの統計を収集する

【0171】

図１８は、ファクターグラフ１６００、すなわちこの発明によるモデル、のパラメータ１３０３を設定するためのプロセス１８００を示す。バイオメトリックトレーニングデータ１３０１を取得する。未処理の指紋Ｆが選択１８０２される。指紋Ｆの測定値Ｂおよび
Ｂ’の未処理のペアが選択１８０３される。それらのそれぞれのマニューシャＭ（Ｂ）およびＭ（Ｂ’）が判別１８０４される。マニューシャを比較１８０５して、移動、回転、挿入および削除の統計を判別１８０６する。統計はファクターグラフにおける統計を改訂（ｒｅｖｉｓｅ）１８０７するのに使用される。まだ処理１８０８されていない指紋Ｆの一対の測定値があれば、ステップ１８０３へ戻る。そうでなければ、まだ処理１８０９されていない指紋があれば、ステップ１８０２に戻る。すべての指紋とそれらのマニューシャペアが処理済になった後、統計収集はステップ１８１０で完了する。

【0172】

データアラインメント

【0173】

生体測定システムでは、登録バイオメトリックデータはしばしば認証データに対して位置がずれる。同じバイオメトリックデータの異なる測定値は、平行移動、回転、拡大縮小などのグローバル（大域的）変換（ｇｌｏｂａｌ　ｔｒａｎｓｆｏｒｍａｔｉｏｎｓ）によりしばしば変動する。そのような変動は、パターンに基づくバイオメトリック認証、すなわちシンドロームコーディングを使用しない認証方式ではそれほど問題ではない。

【0174】

対照的に、我々のシステムでは、登録バイオメトリックパラメータのシンドロームベクトル３３１だけが比較のために利用できる。したがって、異なるアラインメント（配列、配置）に亘る検索は、各可能なアラインメントに対する復号化を伴う。マニューシャ移動モデルは細かいミスアラインメント（位置ずれ）に対応できるが、復号化の演算費用を最小にするために、探索空間を最小にすることが望まれる。

【0175】

図１９は、この発明の実施の形態による、登録或いは認証時の指紋のアラインメントプロセス（整合処理）の各々のステップを示している。指紋が取得１９０１され、マニューシャパラメータが、そのコア（中心）点の位置および方位とともに、抽出１９０２される。そのコア点と方位は指紋に対する慣性基準フレームを定義し、ここで、コア点の位置は原点であり、その方位はＹ軸として機能する。そのコア点に関連する慣性基準フレームに対するマニューシャの位置と方位が再計算１９０３される。その結果１９０４、指紋に対する基準フレームで測定された１組のマニューシャが得られる。

【0176】

利点としては、この手続きにより、平行移動および回転の効果の大部分またはすべてを取り除くことができる。典型的には、そのような前処理は、復号化がより少ない組の平行

移動および回転で実行される、計算上より強力（集中的）なローカルサーチ（局所検索）と結合される。この前処理手続きは、マニューシャ抽出ルーチンの一部として使用できる。

【0177】

パラメータ設定に関するアラインメント後のリビジョン（改訂）

【0178】

登録および認証バイオメトリック特徴が復号化前にお互いに対して変位する毎に、ファクターグラフのパラメータはこの変位を反映するように変更される。このような例は、登録および認証機能がアラインメント手続き１９００により、或いはローカルサーチに対応する多数の小変位により移行する時である。

【0179】

変位、および登録と認証観測窓１４０３（図１４を参照）の相対的大きさによっては、認証の間、幾つかの登録特徴位置を全く観測できないかも知れない。したがって、これらの観測されない位置に対して、マニューシャ消去の確率を１に設定することによって、これを反映するようにファクターグラフを変更する。これは、ファクターノード１６０５における消去確率を１に等しく設定することによって、図１６Ｂに反映される。観測される多少の尤度および観測されない多少の尤度を持っている窓１４０３のエッジ（縁部）の近くのマニューシャに対して、その事前確率１６０５がそれに応じて変更される。

【0180】

シンドローム前処理

【0181】

図3のバイオメトリックセキュリティシステム３００では、登録段階の間、バイオメトリックパラメータ３０１はシンドロームエンコーダ３３０に直接入力される。同様に、認証段階では、バイオメトリックパラメータ３６０はシンドロームデコーダ３７０に直接入力される。

【0182】

図１４はマニューシャ点位置を表示しており、マニューシャ点位置は指紋に対するバイオメトリックパラメータとしてしばしば使用される。図３、５および６に記載したようなバイオメトリックセキュリティシステム用のシンドロームに基づくフレームワークにおいて、この表示を使用することに関して幾つかの問題がある。

【0183】

第１に、その表示は、まばら（ｓｐａｒｓｅ）であり、モデル化するのは難しい。図１５に示されるモデルは、マニューシャに固有の移動、挿入および削除をモデル化することを試みる。しかしながら、それらのモデルは複雑である。

【0184】

第２に、その表示は従来のシンドロームコードに余り適していない。その表示はバイナリデータの形式であっても、データは、偏っており、従来のチャネルコードおよび対応する復号方法がデータに適用されるとき高性能をもたらすような固有の統計的性質を持っていない。

【0185】

その性能は、ソースの偏った性質および計測チャンネルの非対称性を説明する新しいシンドロームコードを設計することによって、改善できる。これは興味深く且つ複雑なプロセスである。

【0186】

図２０はこの発明の実施の形態によるバイオメトリックパラメータをシンドロームコード化する方法を表している。第１のバイオメトリックパラメータ２０１０が、たとえば登録段階１０の間に（図１を参照）、ユーザから取得される。第１のバイオメトリックパラメータ２０１０は、バイオメトリックパラメータ２０３０のバイナリ表示を生成するために、シンドローム前処理２０２０される。前処理２０２０は、１組（１以上）のバイナリロジック条件２０２２を、取得されたバイオメトリックパラメータ２０１０に適用する。

１組のバイナリロジック条件２０２２は、そのバイナリ表示２０３０に１組（１以上）の望ましい所定の統計的性質２０２５を持たせるように、強制或いは試みる。その１組の所定の統計的性質２０２５について、以下でさらに記述する。バイオメトリックパラメータ２０３０のバイナリ表示はシンドロームコード化２０４０されて、第1のシンドローム２０５０を生成する。ここで、ロジック条件が目標統計的性質を達成しようとすることができることに注意するべきである。また、その処理の間、その統計的性質をダイナミックに調整できることに注意するべきである。

【0187】

次に、ハッシュ関数を適用することによって、第１のシンドロームをさらに処理して登録ハッシュを生成することができ、生成された登録ハッシュは、後でユーザを認証する際に使用するために、シンドロームベクトルとともに格納されることができる。

【0188】

我々は、バイナリ表示２０３０および望ましい統計的性質２０２５と互換性があるように、我々のエンコーダ２０４０を明確に設計する。我々は、コード化をバイナリ表示および望ましい統計的性質に適合させることにより、我々のシステムの性能と信頼性が改善されると信じる。

【0189】

図２１は、この発明の実施の形態にしたがってシンドローム復号化する方法の詳細を示す。バイオメトリックパラメータは、たとえば認証段階２０の間に、再び獲得される。第２のバイオメトリックパラメータ２１１０は、シンドローム前処理２０２０されて、バイオメトリックパラメータ２１３０のバイナリ表示を生成する。上述したように、バイナリ表示２１３０は、登録時に課されるのと同じ組の望ましい所定の統計的性質２０２５を有する。そして、前処理されたバイナリ表示２１３０は、シンドローム復号化２１４０への入力として使用されて、再構成されたバイオメトリックパラメータが２１４５を生成する。上述したように、デコーダは望ましい統計的性質を持っているバイナリ表示と互換性がある。コード化および復号化をバイナリ表示および望ましい統計的性質に適合させることにより、我々のシステムの性能と信頼性とを改善する。

【0190】

第1および第２のバイオメトリックパラメータが同じ人から来ているならば、譬え第1および第２のパラメータからのバイオメトリックパラメータが詳細では異なっていたとしても、再構成されたバイオメトリックパラメータは、第1のバイオメトリックパラメータと同じでなければならない。

【0191】

本明細書に記載されたシンドローム前処理は、図３、５および６に示された方法に適用できる。

【0192】

望ましい目標統計的性質

【0193】

シンドローム前処理２０２０は、バイオメトリックパラメータを、望ましい統計的性質２０２５を有するバイナリ表示すなわちバイナリストリング（文字列）に変形するのに使用される。それらの性質は、いつも得られるわけではないかも知れないので、目標性質であると考えられる。

【0194】

統計的性質は、シンドロームコードが最適性能を実現できることを保証する。我々の前処理２０２０により、バイオメトリックパラメータ間の複雑な関係をモデル化するのに関わる複雑さは大きく減少される。

【0195】

バイナリ表示２０３０／２１３０の望ましい１組の統計的性質２０２５は以下の通り概括される：バイナリ表示における各ビットには、ゼロまたは1のどちらかであるという等しい確率がある；同じバイナリ表示における異なるビットはお互いに独立している；異な

るユーザからのバイナリ表示はお互いに独立している；同じユーザの異なる読取りに対するバイナリ表示はお互いに統計的に依存している。

【0196】

この発明のこれらの実施の形態に具現された手法は図１３の実施の形態に対比することができる。図１３に示された実施の形態では、特徴モデル１３０４および測定モデル１３０５は、トレーニング（訓練）集合におけるバイオメトリックデータの基底構造をモデル化するとともに、バイオメトリックデータが、単一ユーザに対するおよび複数のユーザに亘る、複数の読取りの中でどう変動するかをモデル化する。コード化および復号化をそれらのモデルに適合させるために、何も行わない。

【0197】

対照的に、図２０に示されるようなシンドローム前処理手法は、図１３のように、バイオメトリックデータから直接取得された特徴集合を使用しない。その代わりに、図２０－２１の特徴集合、すなわちバイナリ表示、は、シンドロームコード化および復号化手続きと互換性があるように設計される。

【0198】

我々は、特徴集合を、既存の、コード設計、シンドロームコード化およびシンドローム復号化手続きと互換性があるように明確に設計する。本明細書に記述した所定の統計的性質を有する特定の組の特徴に対して、設計された特徴集合に適合するバイナリ（２進）対称チャネルに対するチャネルコードを利用できる。そのようなチャネルコードの構造およびそれらに関連するシンドロームコード化および復号化手続きは、よく理解され且つ深く探究されたトピックである。

【0199】

図２２Ａ－２２Ｃはそれぞれ２００ビットを有する１組のバイナリ表示のビットストリング（列）に対応する１組の統計的性質を示す。

【0200】

図２２Ａはその組のバイナリストリングにおける平均数のヒストグラムを示す。理想的な分布は１００を中心しており、それはビットの半分が1であることを含意する。

【0201】

図２２Ｂは各ストリングにおける、ビットのペア平均情報量（ｐａｉｒ－ｗｉｓｅ ｅｎｔｒｏｐｙ）を示す。理想的には、各対のビットが独立していれば、平均情報量はすべての対に対して2である。しかしながら、ビットの中に幾らか依存性があれば、平均情報量の値は2未満となる。最悪の場合には、プロセスバイオメトリックパラメータにおける特定のビットがいつも別のビットから予測できて、その他のビットが等しい確率でゼロまたは1であるなら、ペア平均情報量は1である。

【0202】

図２２Ｃは、イントラユーザ（ユーザ内）変動（ｉｎｔｒａ－ｕｓｅｒ ｖａｒｉａｔｉｏｎｓ）２２１０とインターユーザ（ユーザ間）変動（ｉｎｔｅｒ－ｕｓｅｒ ｖａｒｉａｔｉｏｎｓ）２２２０を示す。イントラユーザ変動２２１０は、同じユーザの複数のサンプルに対応するビットストリング（ビット列）の間の正規化されたハミング距離を表す。インターユーザ変動２２２０は、異なるユーザのサンプルに対応するビットストリングの間の正規化されたハミング距離を表す。理想的には、イントラユーザ変動とインターユーザ変動は重ね合わせるべきでなく、また、それぞれが狭い範囲に亘って分布するべきである。その上、イントラユーザ変動２２１０はできるだけ低く（小さく）なるべきであり、たとえば、図示されるように、分布約０．１は、同じユーザの各ビットには１０％のエラー確率があることを示す。他方、インターユーザ変動に対する分布は０．５を中心にするべきであり、これは、異なるユーザからのビットストリングがお互いに独立していることを示す。

【0203】

シンドローム前処理の実行

【0204】

図２３は、我々のシンドローム前処理方法を示す。シンドローム前処理は１組（１以上）のバイナリロジック条件を適用する、すなわち、バイナリ表示すなわちバイナリストリング「００１１１０００１０１１１０００１…．．」をもたらすバイオメトリックパラメータに関してイエス（ｙｅｓ）／ノー（ｎｏ）応答を有する条件を適用する。

【0205】

図２４に示される我々の方法では、１組のバイナリロジック条件２０２２がバイオメトリックパラメータに適用される。その適用結果の出力が非バイナリ２４３０であるならば、その出力は、必要なバイナリ表示をもたらすために２値化４２０２される。

【0206】

たとえば、バイオメトリックパラメータは指紋に対するマニューシャ点の位置である。１つのバイナリ（２値）条件は、与えられた２次元（２Ｄ）領域のマニューシャの数が閾値Mより大きいか否かを判別する。

【0207】

バイナリロジック条件

【0208】

図２５Ａ－２５Ｃに示されるように、幾つかのタイプのバイナリロジック条件がバイオメトリックパラメータに適用できる。図２５Ａ－２５Ｃのドットは指紋マニューシャの座標（サンプル位置）を表す。図２５Ａおよび２５Ｂにおいて（ｘ－位置、ｙ－位置）座標、或いはまた図２５Ｃにおいて（ｘ－位置、ｙ－位置、方位）座標（ｚ）。

【0209】

図２５Ａでは、各条件はサンプルを通して描かれた線２５０１に基づいている。バイナリロジック条件はｙ－ｍｘ－ｎ＝０である。線はランダムな傾きとｙ切片値を持つことができる。この発明の実施の形態１では、線より上の（すなわち、条件ｙ－ｍｘ－ｎ＞０を満たす領域に位置する）マニューシャ点の数と線より下の（すなわち、条件ｙ－ｍｘ－ｎ＜０を満たす領域に位置する）マニューシャ点の数の差が得られる。これは範囲［－Ｍ、Ｍ］の値のベクトルをもたらし、ここで、Ｍは指紋のマニューシャ点の最大数である。必要ならば、ベクトルを２値化することができる。

【0210】

図２５Ｂでは、条件は１組の長方形２５０２である。各長方形は、幅と高さとともに、該長方形の左上隅を表す原点で生成される。１組の長方形は、これらの点のランダムな値で、または所定の配置により生成できる。この発明の実施の形態１では、条件は与えられた長方形の中のマニューシャ点の数である。

【0211】

この発明の実施の形態１では、条件は、特定の閾値よりも大きな、与えられた長方形内のマニューシャ点の数であり、ここで、その閾値は、各長方形に対して、その位置および領域、および／又はユーザデータサンプルのグローバルな統計に基づいて変動してもよい。

【0212】

この発明の別の実施の形態では、条件は１つの長方形内のマニューシャの数と２番目の長方形内のマニューシャの数の差である。

【0213】

マニューシャ方位などの指紋に関する追加データを含めるために、長方形条件を立方体や直方体２５０３に拡張でき、ここで、最初の２つの寸法（ｄｉｍｅｎｓｉｏｎｓ）は、上述したように、マニューシャ点位置を表し、また、３番目の寸法（ｄｉｍｅｎｓｉｏｎ）（ｚ）はマニューシャ方位を表す。図２５Ｃでは、条件は１組の直方体を含んでいる。各直方体は、幅、高さおよび深さとともに、該直方体の左上隅を示す原点で生成される。１組の直方体は、これらの点のランダムな値で、または所定の配置により生成できる。この発明の実施の形態１では、条件は与えられた直方体内のマニューシャ点の数である。この発明の実施の形態１では、条件は、特定の閾値よりも大きな、与えられた長方体内のマニューシャ点の数であり、ここで、その閾値は、各直方体に対して、その位置および体積

、および／又はユーザデータサンプルのグローバルな統計に基づいて変動してもよい。この発明の更に別の実施の形態では、条件は１つの直方体内のマニューシャの数と２番目の直方体内のマニューシャの数の差である。

【0214】

この発明は本明細書に記述した特定のロジック条件に限定されない。バイオメトリックの特性によって、円形、球形、および多角形に基づく他の様々な条件もまた使用できる。

【0215】

さらに、これらの方法は、マニューシャに基づく特徴集合の変換および２値化に制限されない。その目的は、シンドロームコード化および復号化に適合する、統計情報を有するバイナリ表示を生成するために、バイナリロジック条件をバイオメトリックデータに適用することである。たとえば、この発明は、とりわけ他のタイプの指紋データの中で、パターンに基づくデータや周波数領域データに適用できる。

【0216】

一般的に言えば、条件の間のオーバラップは、結果として得られるバイナリ表示における相関関係に影響する。条件は、この影響を考えて設計され得る。たとえば、２つの長方形の間の許容できるオーバラップの量に関して制限を課すことができるであろう。また、シンドロームコード化および復号化手続きも、そのような相関関係を考えて設計され得る。しかしながら、この発明の目的は、市販のコード設計やコード化および復号化手続きに対するそのような調整の必要性を最小にすることである。

【0217】

２値化

【0218】

図２６は２値化の幾つかのタイプを示す。図２６Ａでは、閾値２６０１が、バイナリベクトル２６０３を生成ために、ベクトル２６０２のすべての値に適用される。この閾値は、すべてのビット位置に対して同じでもよいし、或いは各ビット位置に対して変化してもよい。

【0219】

図２６Ｂでは、正規直交基底へのランダム投影２６０４が最初に非バイナリのベクトル２６０２に適用され、ここで、このランダム投影はすべてのユーザに対して同じである。そして、この投影の結果は、バイナリベクトル２６０３を生成するために、閾値化プロセスを加えられる。ランダム投影の代わりに、本物のユーザと詐欺師（偽者）とから取得されたサンプルの分離を改善するために、たとえば、主成分分析（ｐｒｉｎｃｉｐａｌ　ｃｏｍｐｏｎｅｎｔ　ａｎａｌｙｓｉｓ）や線形判別分析（ｌｉｎｅａｒ　ｄｉｓｃｒｉｍｉｎａｎｔ　ａｎａｌｙｓｉｓ）などの他の線形（リニア）或いは非線（ノンリニア）変換を使用することができる。

【0220】

図２６Ｃでは、非バイナリ（非２値）ベクトル２６０２が最初に正規化２６０５され、次に、１組のランダム投影（ＲＰ）２６０４が各ユーザに対して適用され、それに続いて、各ランダム投影に対する閾値化２６０１が行われる。この閾値化は各投影に対して同じでもよいし、それらの投影の中で変動してもよい。そして、バイナリベクトル２６０３を生成するため、連結（ｃｏｎｃａｔｅｎａｔｉｏｎ）２６０７がこの後に続いて行われる。

【0221】

統計的分析

【0222】

望ましい目標統計的性質が達成されることを保証、確認するために、シンドローム前処理の設計の一部として、統計的分析をバイナリ表示に対して実行することができる。このように、統計的分析が、シンドローム前処理の最終的な結果に対して実行され、シンドローム前処理の動作に対してフィードバックは行われない。

【0223】

或いは、シンドローム前処理の動作を導くために、シンドローム前処理の間、統計的分析はまた中間的バイナリストリングに対しても実行することができる。このようにして、シンドローム前処理の間、統計的性質の明確なフィードバックが提供される。

【0224】

シンドローム前処理に対するセキュリティの考察

【0225】

バイナリ表示におけるビット数および同じユーザの異なるサンプル間の相関関係により、セキュリティのレベルが判別される。たとえば、バイナリストリングが４００ビットであり、相関関係が十分に強いためユーザの復号に成功するために３００ビットのシンドロームを必要とするだけであるならば、セキュリティのレベルは１００ビットである。

【0226】

セキュリティがシンドロームコード化段階から得られる。事実、シンドローム前処理の結果、所定の統計的相関を有するバイナリストリングが生成される。この場合、本システムによって提供されるセキュリティの推定値は、シンドロームコード化および復号化がモデル化の難しい相関関係を有するバイナリストリングを使用して実行される場合と比較して、より正確であると考えられる。

【0227】

発明の効果

【0228】

この発明はバイオメトリックパラメータに基づく安全なユーザ認証を実現する。シンドロームベクトルが元のバイオメトリックデータ或いは如何なる特徴ベクトルの代わりに格納されるので、この発明は安全である。これにより、基礎となるバイオメトリックデータを学習することによりデータベースへのアクセスを得る敵対者を防ぐことができる。

【0229】

多重記述（ｍｕｌｔｉｐｌｅ　ｄｅｓｃｒｉｐｔｉｏｎｓ）の周知の問題から従来のツールを使用することにより、敵対者がシンドロームベクトルＳだけを使用することで作り出すことができる元のバイオメトリックパラメータＥの可能な限り良い推定値を制限することが可能である。たとえば、Ｖ．Ｋ．Ｇｏｙａｌ，Ｍｕｌｔｉｐｌｅ　ｄｅｓｃｒｉｐｔｉｏｎ　ｃｏｄｉｎｇ：ｃｏｍｐｒｅｓｓｉｏｎ　ｍｅｅｔｓ　ｔｈｅ　ｎｅｔｗｏｒｋ」，ＩＥＥＥ　Ｓｉｇｎａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｍａｇａｚｉｎｅ，Ｖｏｌｕｍｅ：１８，ｐａｇｅｓ　７４－９３，Ｓｅｐｔｅｍｂｅｒ　２００１を参照。その上、推定値の品質が絶対誤差、２乗誤差、重み付け誤差方法、或いは如何なる任意の誤差関数により測定されるか否かに関係なく、これらの制限（限界）を策定することが可能である。対照的に、すべての従来技術の方法はバイナリ値に基づいている。そこでは、セキュリティはハミング距離に依存する。

【0230】

本質的には、シンドロームベクトルＳのセキュリティは、それが元のバイオメトリックパラメータＥの圧縮されたバージョンであるという事実による。その上、この圧縮表現はＥの「最下位ビット」に対応している。データ圧縮理論から周知のツールを使用して、「高圧縮のシンドロームコードが使用されるならば、これらの最下位ビットはせいぜい元のパラメータＥの劣悪な（不十分な）推定値しか生成することができない」ことを立証することが可能である。たとえば、Ｅｆｆｒｏｓ、「Ｄｉｓｔｏｒｔｉｏｎ－ｒａｔｅ　ｂｏｕｎｄｓ　ｆｏｒ　ｆｉｘｅｄ－　ａｎｄ　ｖａｒｉａｂｌｅ－ｒａｔｅ　ｍｕｌｔｉ－ｒｅｓｏｌｕｔｉｏｎ　ｓｏｕｒｃｅ　ｃｏｄｅｓ」、ＩＥＥＥ　Ｔｒａｎｓａｃｔｉｏｎｓ　ｏｎ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｔｈｅｏｒｙ，ｖｏｌｕｍｅ　４５，ｐａｇｅｓ　１８８７－１９１０，Ｓｅｐｔｅｍｂｅｒ　１９９９、および「Ｓｔｅｉｎｂｅｒｇ　ａｎｄ　Ｍｅｒｈａｖ，「Ｏｎ　ｓｕｃｃｅｓｓｉｖｅ　ｒｅｆｉｎｅｍｅｎｔ　ｆｏｒ　ｔｈｅ　Ｗｙｎｅｒ－Ｚｉｖ　ｐｒｏｂｌｅｍ」、ＩＥＥＥ　Ｔｒａｎｓａｃｔｉｏｎｓ　ｏｎ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｔｈｅｏｒｙ，ｖｏｌｕｍｅ　５０，ｐａｇｅｓ　１６３６－１６５４，Ａｕｇｕｓｔ　２００４を参照。

【0231】

第２に、偽造は基礎となるハッシュ関数３４０における衝突を見つけるのと少なくとも同じくらい難しいので、この発明は安全である。特に、復号されたバイオメトリックＥ”のハッシュＨ’が元のハッシュＨと一致する場合にだけ、本システムは認証段階３９０におけるシンドロームペア（Ｓ、Ｈ）を受け付ける。ＭＤ５などの暗号化ハッシュ関数にとって、Ｅと異なっているがＥのハッシュと一致するハッシュを持つ要素Ｅ”を見つけ出すことは、一般的に、不可能であると考えられている。而して、シンドローム復号化が、適切なハッシュでＥ”を復号するのに成功するならば、本システムは事実上、Ｅ”がＥと同じであると確信することができ、すべての認証決定が元のバイオメトリックパラメータで行われる。

【0232】

第３に、この発明は、シンドロームベクトルＳを生成する際に、元のバイオメトリックパラメータＥを圧縮する。特にバイオメトリックデータの質問がたとえば顔画像或いは音声信号などの多量のデータを必要とする場合には、多くのユーザに対するバイオメトリックデータベースは大容量ストレージを必要とすることがある。したがって、必要とされるストリッジ容量を小さくすることにより、費用とエラー復元力の両方で劇的な改良をもたらすことができる。対照的に、バイオメトリックデータの安全な格納に対する殆どの従来技術の方法は、暗号化や誤り訂正のオーバヘッドにより実際に記憶データのサイズ（大きさ）を増大させ、したがって安全でない（セキュリティ保護されていない）システムよりも多くのストリッジ容量を必要とする。

【0233】

第４に、この発明は、シンドロームコードの理論で作られるので、精巧なコード構造と復号アルゴリズムを適用することができる。特に、この発明によるシンドロームコーディングは、バイナリおよびマルチレベル両方の符号化構造に対して、周知のビタビ（Ｖｉｔｅｒｂｉ）アルゴリズム、確率伝搬、およびターボデコーディングを用いたソフトデコーディングの使用を容易にする。対照的に、殆どの従来技術の方法はバイナリコード、リードーソロモンコード、および代数的復号化に基づいているので、バイオメトリックデータが、バイナリ値とは反対に、実際の値（ｒｅａｌ　ｖａｌｕｅｓ）をとるとき、ソフトデコーディングを効果的に適用することができない。たとえば、幾つかの方法は、リファレンス（基準）を生成するために、登録段階におけるランダムな符号語でバイオメトリックデータの排他的論理和（ＸＯＲ）を計算することを特に要求し、また、認証段階におけるバイオメトリックデータでそのリファレンスの排他的論理和を計算することを要求する

【0234】

第５に、安全なバイオメトリックスに関する殆どの従来技術は誤り訂正符号化を使用するが、この発明はシンドローム符号化を使用する。通常、誤り訂正符号化の計算の複雑さは、入力サイズ（大きさ）において超線形（ｓｕｐｅｒ　ｌｉｎｅａｒ）である。対照的に、様々なタイプの低密度パリティチェックに基づくシンドロームコードを使用することによって、シンドローム符号化の計算の複雑さ（量）が入力サイズ（大きさ）においてリニアのみであるシンドロームエンコーダを構成することが容易になる。

【0235】

第６に、シンドロームコーディングフレームワークを使用することによって、「直列連鎖累積コードを使用して信号を圧縮する」という発明の名称の米国特許出願第１０／９２８，４４８（引用によりここに援用される）にＹｅｄｉｄｉａ外によって記載されたＳＣＡコードのような強力な新しい埋め込まれたシンドロームコードを使用することが可能である。これらのコードは、シンドロームエンコーダが、登録の間、バイオメトリックデータの固有の変動性を推定して、シンドローム復号化に成功するのを許容するのに丁度充分なだけのシンドロームビットを符号化することを許容する。

【0236】

第７に、データを暗号化するために、上述したようなシンドロームコードを使用できる。その上、所与のレベルの性能とエラー復元力とを有する最適のシンドロームコードのた

めの設計を可能にする方法が記述される。

【0237】

第８に、計測チャンネルが構造化ノイズを受けることがあっても、シンドローム特徴ベクトルを正しく復号できる。

【0238】

第９に、符号化および復号化は、バイナリロジック条件によって課される望ましい統計的性質と互換性があるように設計することができる。

【0239】

この発明は好適な実施の形態を例に挙げて説明したが、この発明の精神および範囲内で種々の他の改変および変更を行うことができることを理解すべきである。したがって、この発明の精神および範囲内に入るすべての変更例および変形例をカバーすることが、付加されたクレームの目的である。

【図面の簡単な説明】

【0240】

【図1】従来技術のパスワードに基づくセキュリティシステムのブロック図である。

【図2】従来技術のバイオメトリックに基づくセキュリティシステムのブロック図である。

【図3】この発明の実施の形態１によるバイオメトリックセキュリティシステムのブロック図である。

【図4】データを保護するための従来技術のセキュリティシステムのブロック図である。

【図5】この発明の実施の形態によるデータセキュリティシステムのブロック図である。

【図6】この発明の実施の形態によるセキュリティシステムのブロック図である。

【図7】この発明の実施の形態によるシンドロームコードを構成するためのプロセスのブロック図である。

【図8】この発明の実施の形態によるヒストグラムを生成するためのプロセスのブロック図である。

【図9】この発明の実施の形態による特徴ベクトルを選択するためのプロセスのブロック図である。

【図10】この発明の実施の形態による係数間相関関係を測定するためのブロック図である。

【図11AB】登録時に、この発明の実施の形態によるシンドロームベクトルを生成するためのバイオメトリックエンコーダのブロック図、および、この発明の実施の形態による、認証の間に使用される図１１Ａのエンコーダのための相補型デコーダのブロック図である。

【図11C】この発明の実施の形態による相関関係ノードを有する確率伝搬ファクターのグラフである。

【図12】この発明の実施の形態による、バイオメトリック特徴、完全な特徴ベクトル、シンドローム特徴ベクトル、および符号化されたシンドロームベクトルの間の依存関係を示すブロック図である。

【図13】この発明の実施の形態によるシンドロームコードを構成するためのプロセスのブロック図である。

【図14】この発明の実施の形態による指紋マニューシャ符号化のブロック図である。

【図15A】この発明の実施の形態による、測定されたバイオメトリックデータにおける変動性のブロック図である。

【図15B】この発明の実施の形態による、測定されたバイオメトリックデータにおける変動性のブロック図である。

【図15C】この発明の実施の形態による、測定されたバイオメトリックデータにおける変動性のブロック図である。

【図16A】この発明の実施の形態による確率伝搬ファクターグラフの高レベルの詳細のブロック図である。

【図16B】この発明の実施の形態による確率伝搬ファクターグラフの低レベルの詳細のブ

ロック図である。

【図17】この発明の実施の形態による、余分なものを取り除いた確率伝搬ファクターのグラフである。

【図18】この発明の実施の形態による指紋マニューシャの移動および測定モデルのパラメータを推定するためのプロセスのブロック図である。

【図19】この発明の実施の形態によるマニューシャのアラインメントを行うブロック図である。

【図20】この発明の実施の形態によるシンドローム前処理を有するシンドローム符号化プロセスのブロック図である。

【図21】この発明の実施の形態によるシンドローム前処理を有するシンドローム復号化プロセスのブロック図である。

【図22A】この発明の実施の形態による所定の統計的性質のグラフである。

【図22B】この発明の実施の形態による所定の統計的性質のグラフである。

【図22C】この発明の実施の形態による所定の統計的性質のグラフである。

【図23】この発明の実施の形態によるバイナリロジック条件に基づくシンドローム前処理のブロック図である。

【図24】この発明の別の実施の形態による、シンドローム前処理に基づくバイナリロジック条件のブロック図である。

【図25A】この発明の実施の形態によるシンドローム前処理の一部としてのロジック条件のグラフである。

【図25B】この発明の実施の形態によるシンドローム前処理の一部としてのロジック条件のグラフである。

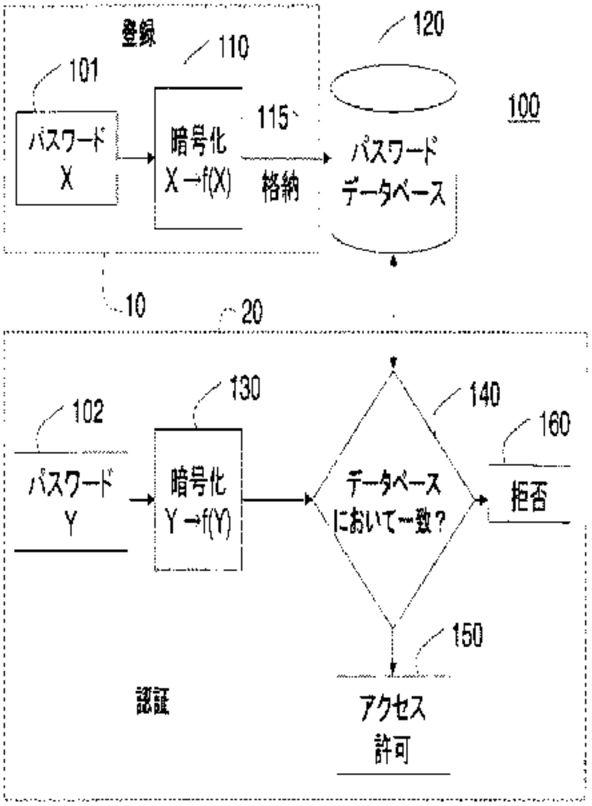
【図25C】この発明の実施の形態によるシンドローム前処理の一部としてのロジック条件のグラフである。

【図26A】この発明の実施の形態によるシンドローム前処理の一部としての２値化のグラフである。

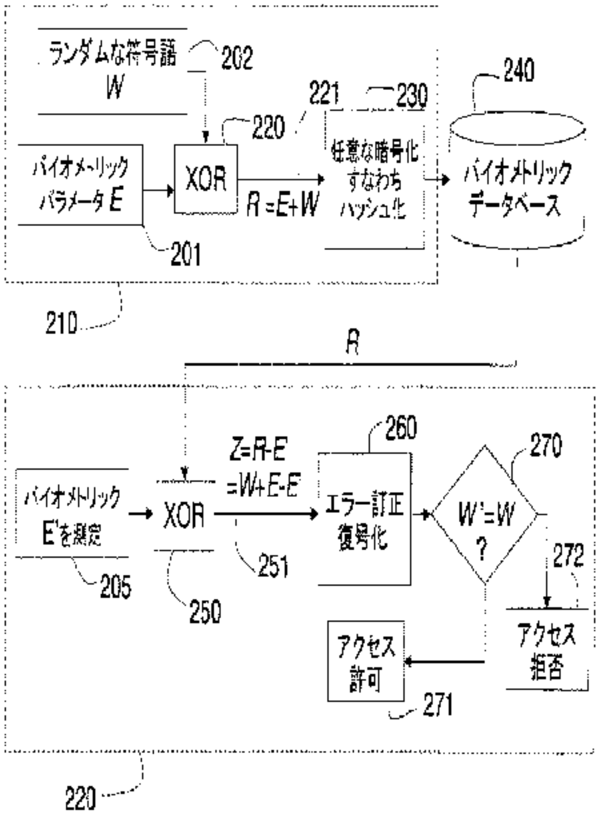
【図26B】この発明の実施の形態によるシンドローム前処理の一部としての２値化のグラフである。

【図26C】この発明の実施の形態によるシンドローム前処理の一部としての２値化のグラフである。

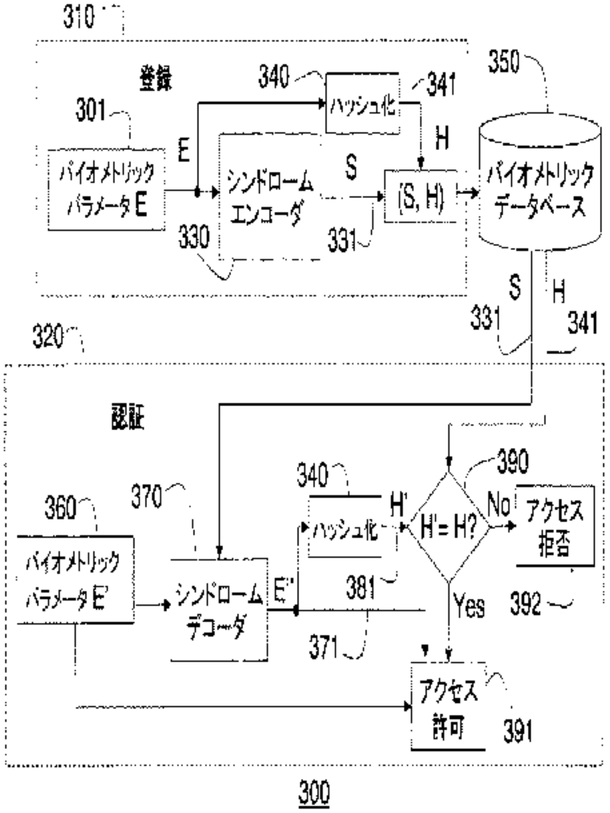
【図１】


100
登録
10
101
パスワード X
110
暗号化 X→f(X)
115
格納
120
パスワード データベース
20
102
パスワード Y
130
暗号化 Y→f(Y)
140
データベース において一致？
160
拒否
150
認証
アクセス 許可

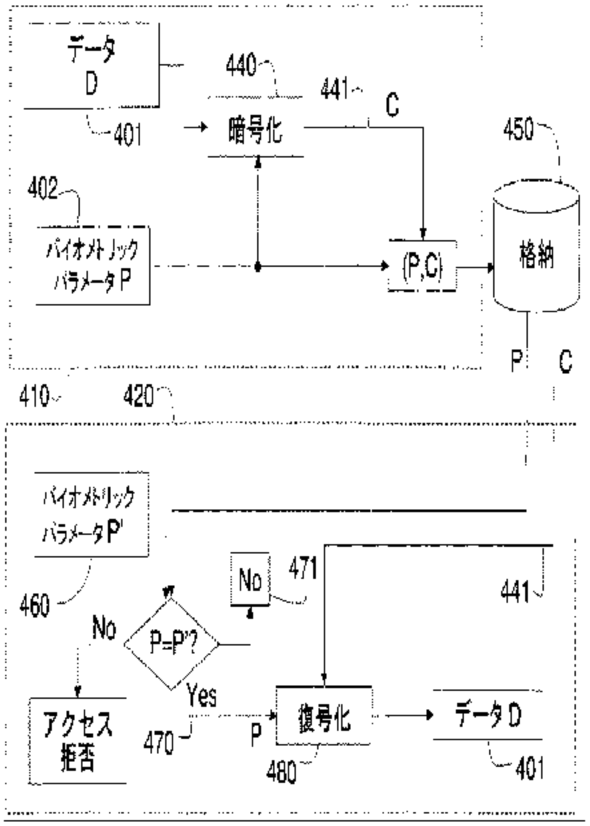
【図２】


ランダムな符号語 W
202
221
230
240
220
バイオメトリック パラメータ E
XOR
R=E+W
任意な暗号化 すなわち ハッシュ化
バイオメトリック データベース
201
210
R
Z=R-E' =W+E-E'
260
270
バイオメトリック E'を測定
XOR
エラー訂正 復号化
W'=W ?
205
251
250
272
アクセス 許可
アクセス 拒否
271
220

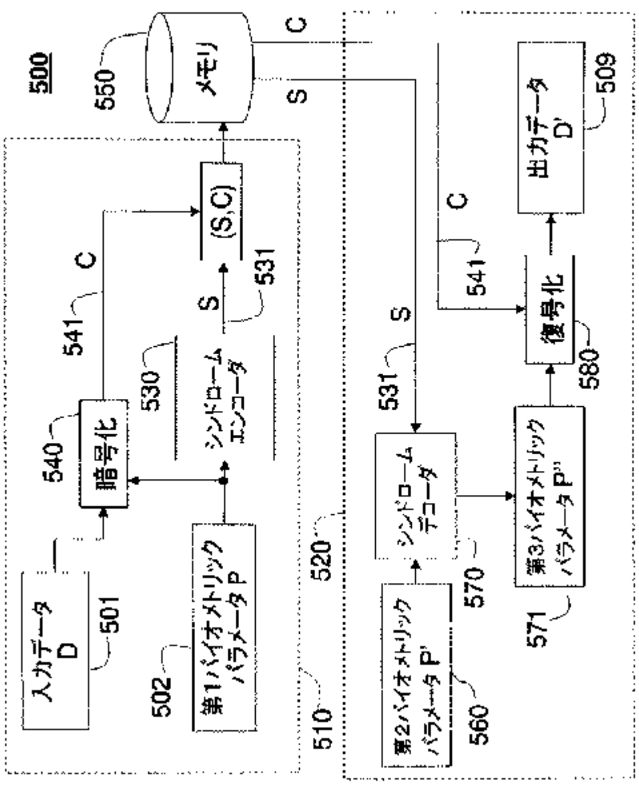
【図３】


310
登録
340
341
350
301
ハッシュ化
H
E
S
バイオメトリック パラメータE
シンドローム エンコーダ
(S, H)
バイオメトリック データベース
330
331
S
H
331
341
320
認証
340
390
360
370
ハッシュ化
H'
H'=H?
No
アクセス 拒否
バイオメトリック パラメータE'
シンドローム デコーダ
E''
381
Yes
392
371
アクセス 許可
391
300

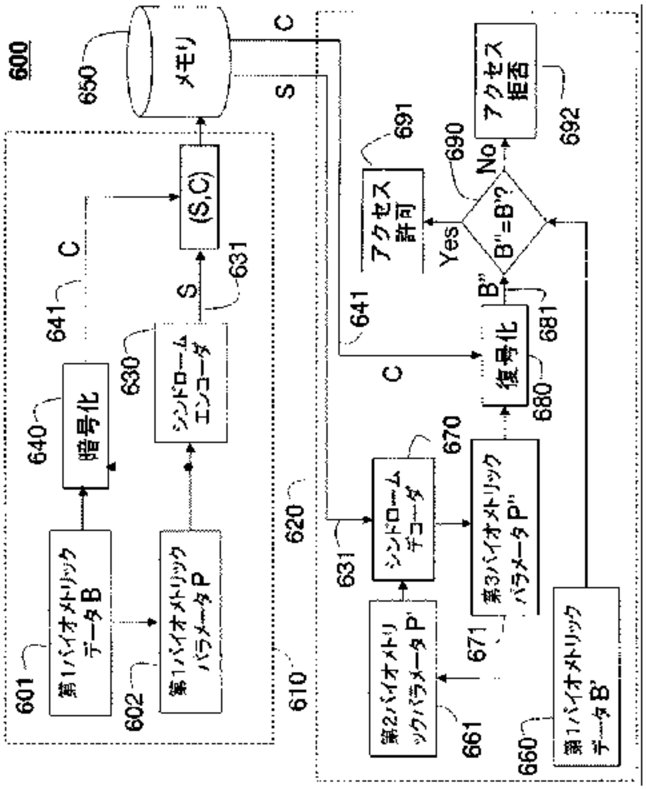
【図４】


データ D
440
441
C
401
暗号化
450
402
バイオメトリック パラメータP
(P,C)
格納
P
C
410
420
バイオメトリック パラメータP'
460
No
471
441
P=P'?
Yes
復号化
データD
アクセス 拒否
470
P
480
401

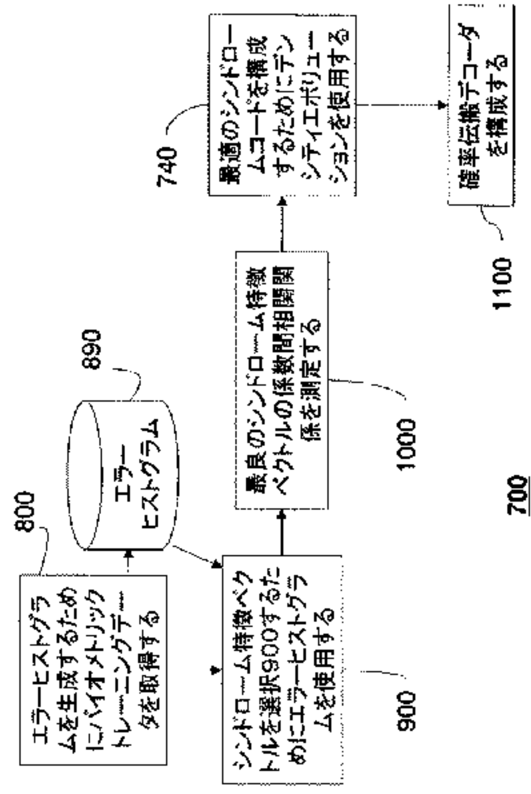
【図5】


500
入力データ
D
501
第1バイオメトリック
パラメータP
502
510
暗号化
540
541
C
シンドローム
エンコーダ
530
S
531
(S,C)
メモリ
550
C
S
第2バイオメトリック
パラメータP'
560
シンドローム
デコーダ
570
520
531
S
第3バイオメトリック
パラメータP''
571
復号化
580
541
C
出力データ
D'
509

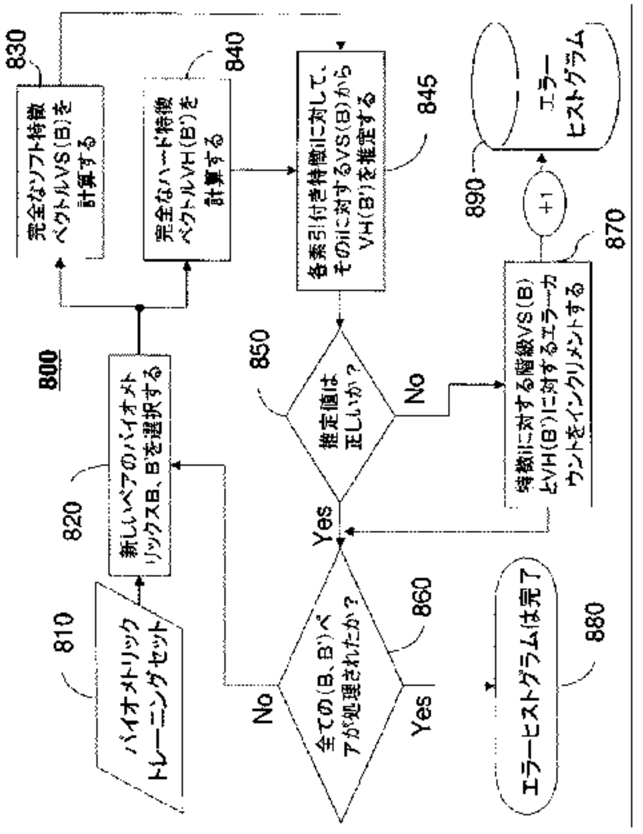
【図6】


600
メモリ
650
C
S
第1バイオメトリック
データB
601
第1バイオメトリック
パラメータP
602
暗号化
640
641
C
シンドローム
エンコーダ
630
S
631
(S,C)
610
620
631
シンドローム
デコーダ
670
第2バイオメトリックパラメータP'
661
第3バイオメトリック
パラメータP''
671
第1バイオメトリック
データB'
660
復号化
680
681
C
641
B''
B''=B'?
690
Yes
No
アクセス
許可
691
アクセス
拒否
692

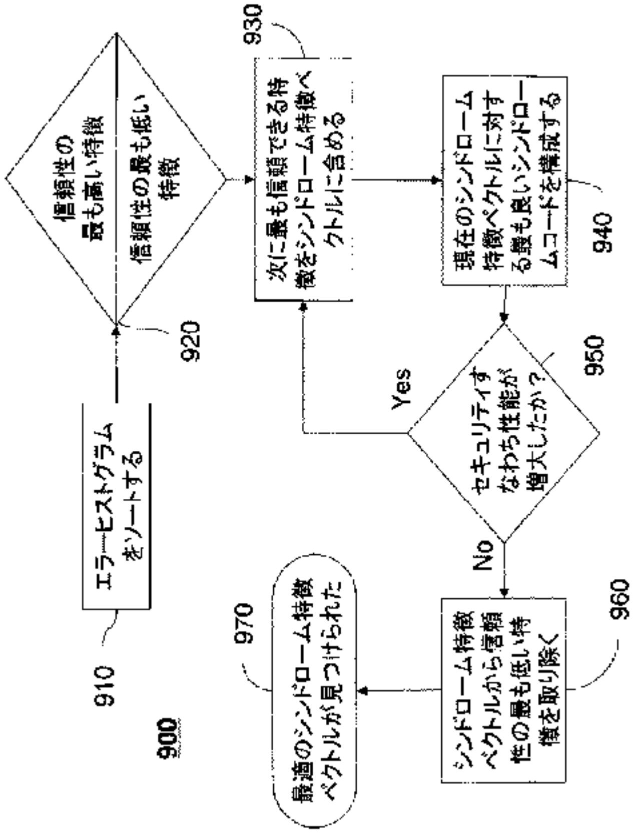
【図7】


700
エラーヒストグラムを生成するためにバイオメトリックトレーニングデータを取得する
800
エラー
ヒストグラム
890
シンドローム特徴ベクトルを選択900するためにエラーヒストグラムを使用する
900
最良のシンドローム特徴ベクトルの係数間相関関係を測定する
1000
最適のシンドロームコードを構成するためにデンシティエボリューションを使用する
740
確率伝搬デコーダを構成する
1100

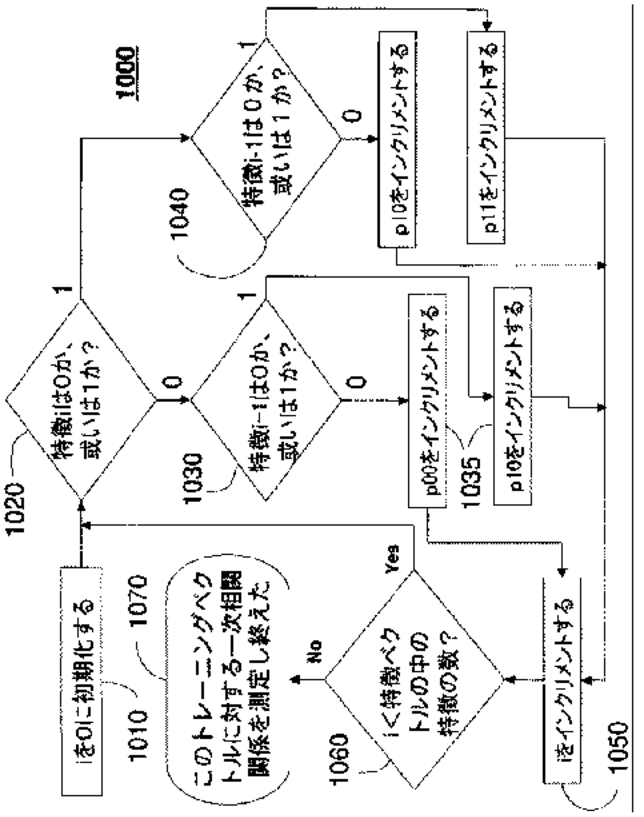
【図8】


800
バイオメトリック
トレーニングセット
810
新しいペアのバイオメトリックスB、B'を選択する
820
完全なソフト特徴ベクトルVS(B)を計算する
830
完全なハード特徴ベクトルVH(B)を計算する
840
各索引付き特徴iに対して、そのiに対するVS(B)からVH(B')を推定する
845
推定値は正しいか？
850
Yes
No
特数iに対する階級VS(B)とVH(B')に対するエラーカウントをインクリメントする
870
+1
エラー
ヒストグラム
890
全ての(B, B')ペアが処理されたか？
860
No
Yes
エラーヒストグラムは完了
880

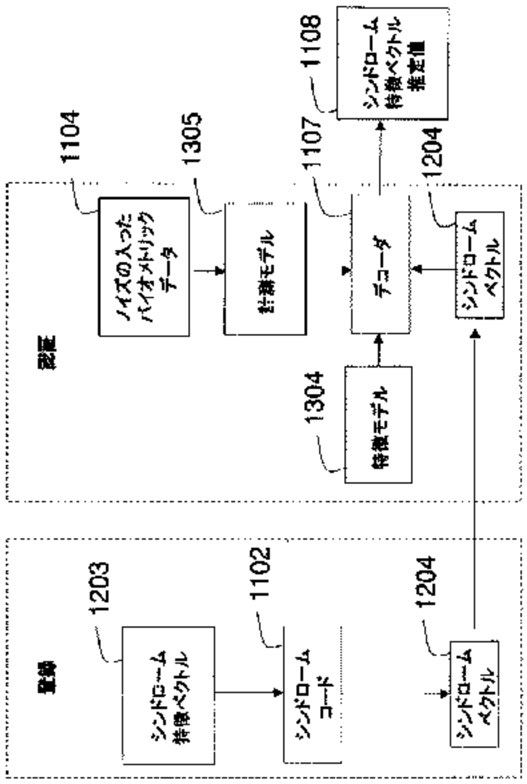
【図9】


900
910
エラーヒストグラムをソートする
920
信頼性の最も高い特徴
信頼性の最も低い特徴
930
次に最も信頼できる特徴をシンドローム特徴ベクトルに含める
940
現在のシンドローム特徴ベクトルに対する最も良いシンドロームコードを構成する
950
セキュリティすなわち性能が増大したか？
Yes
No
960
シンドローム特徴ベクトルから信頼性の最も低い特徴を取り除く
970
最適のシンドローム特徴ベクトルが見つけられた

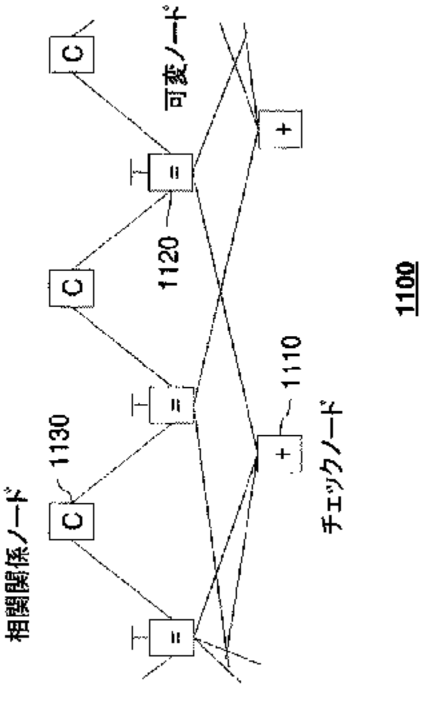
【図10】



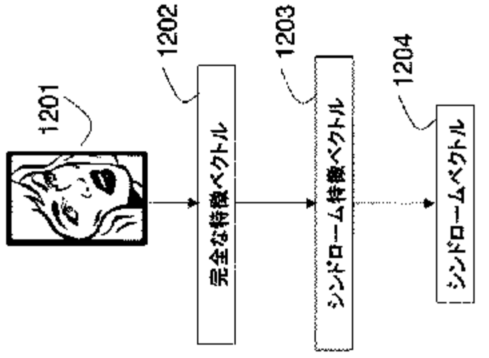
【図11AB】



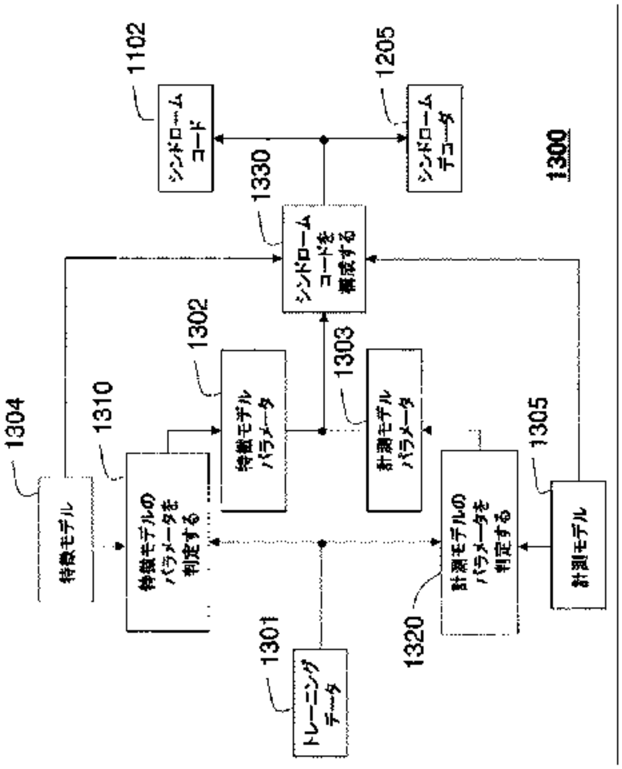
【図11C】



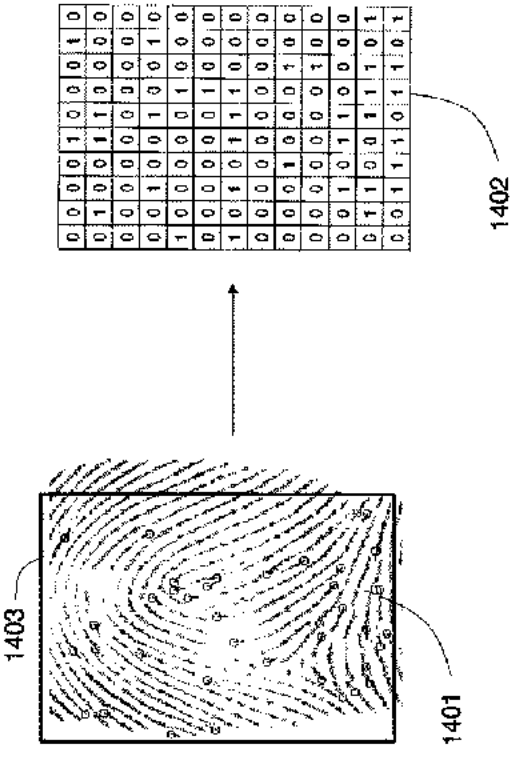
【図12】



【図13】

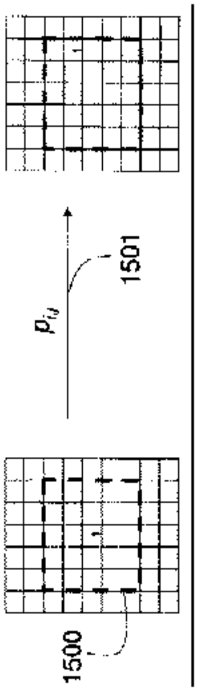


【図14】

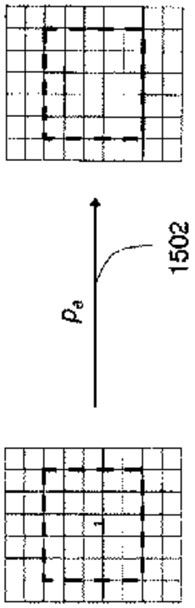


1	0	1	1	0	1	1	1	0	0
1	0	1	1	1	0	0	1	1	0
0	0	0	0	1	1	0	1	0	0
0	0	1	0	0	0	0	0	0	0
0	0	1	0	0	0	1	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	1	1	1	0	1	0	1
0	0	0	1	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0	1
0	1	0	0	1	0	0	1	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	1	1	0	0	1	0
0	1	0	0	0	1	0	0	0	0

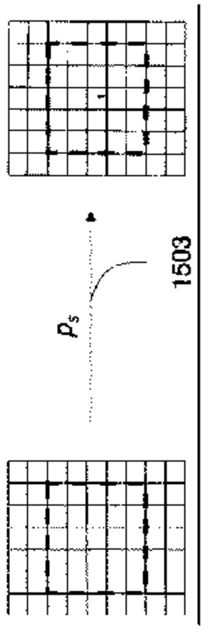
【図15A】



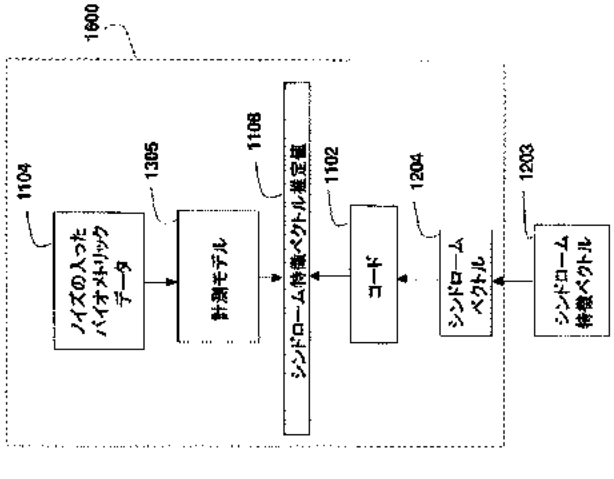
【図15B】



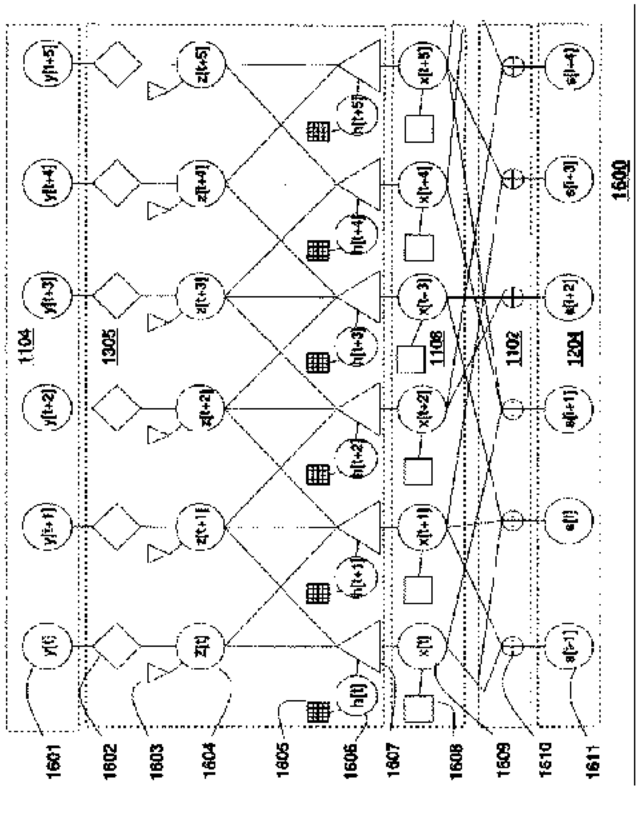
【図15C】



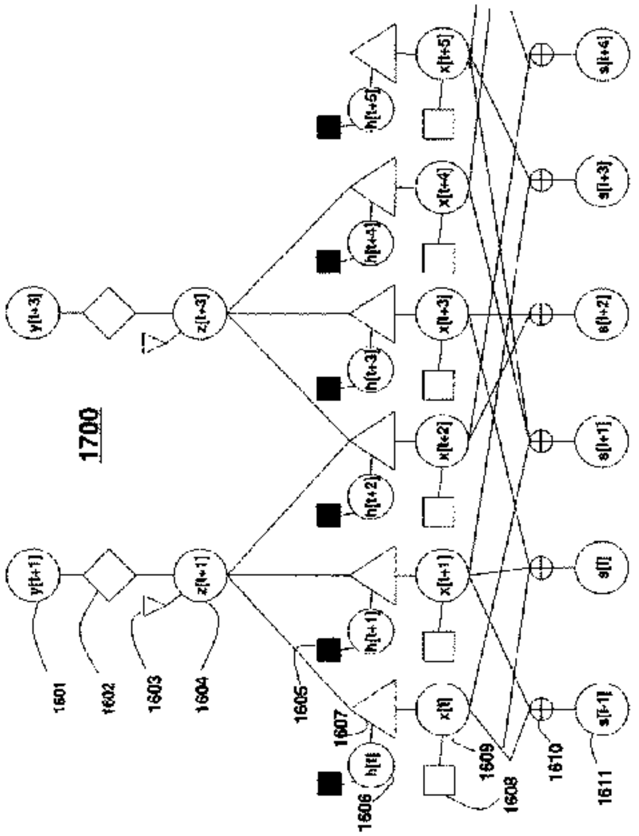
【図16A】



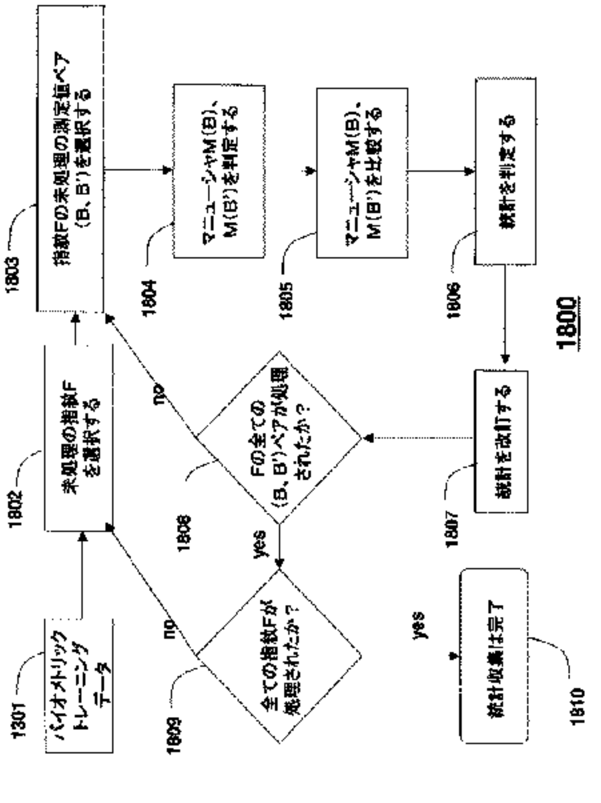
【図16B】



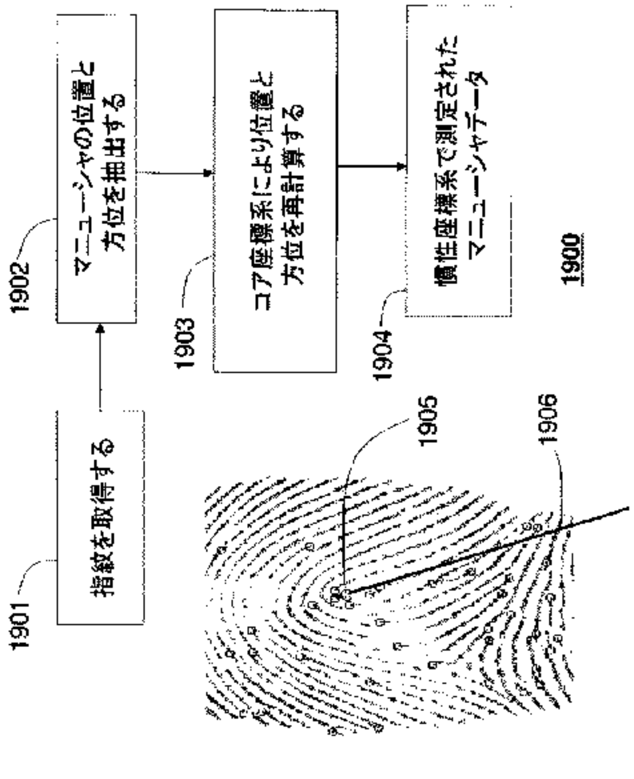
【図17】



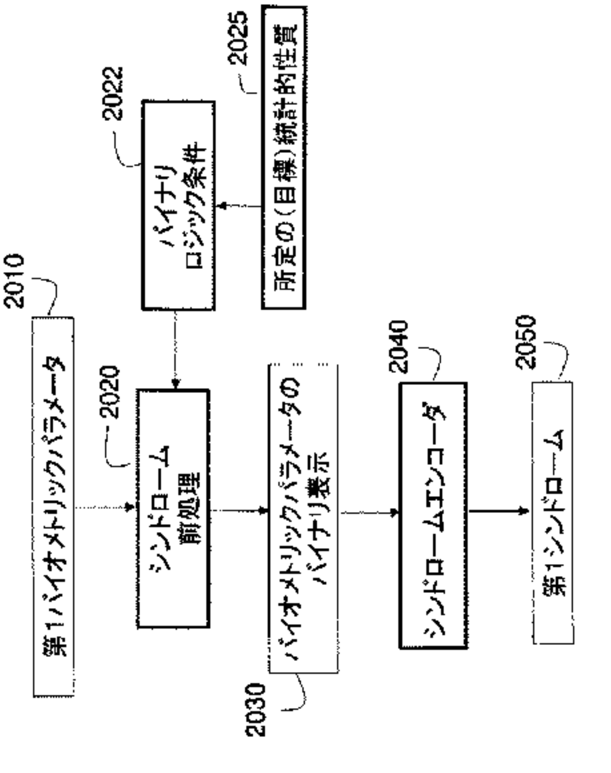
【図18】


1800
1301
バイオメトリックトレーニングデータ
1802
未処理の指紋Fを選択する
1803
指紋Fの未処理の測定値ペア(B, B')を選択する
1804
マニューシャM(B)、M(B')を判定する
1805
マニューシャM(B)、M(B')を比較する
1806
統計を判定する
1807
統計を改訂する
1808
Fの全ての(B, B')ペアが処理されたか？
no
yes
1809
全ての指紋Fが処理されたか？
no
yes
1810
統計収集は完了

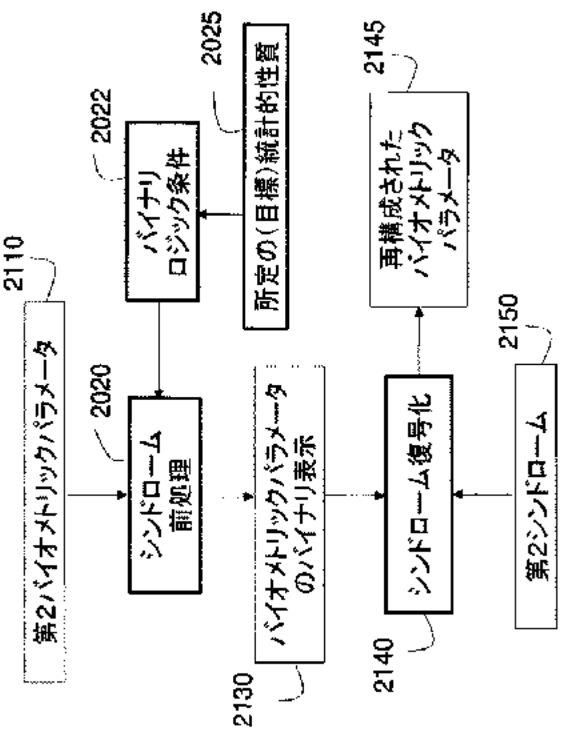
【図19】


1900
1901
指紋を取得する
1902
マニューシャの位置と方位を抽出する
1903
コア座標系により位置と方位を再計算する
1904
慣性座標系で測定されたマニューシャデータ
1905
1906

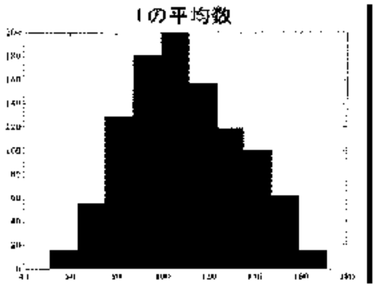
【図20】



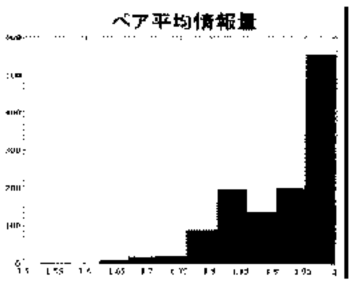
【図21】



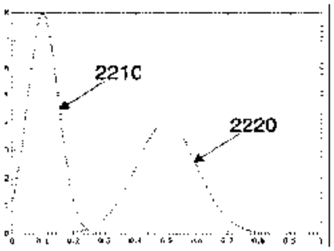
【図22A】



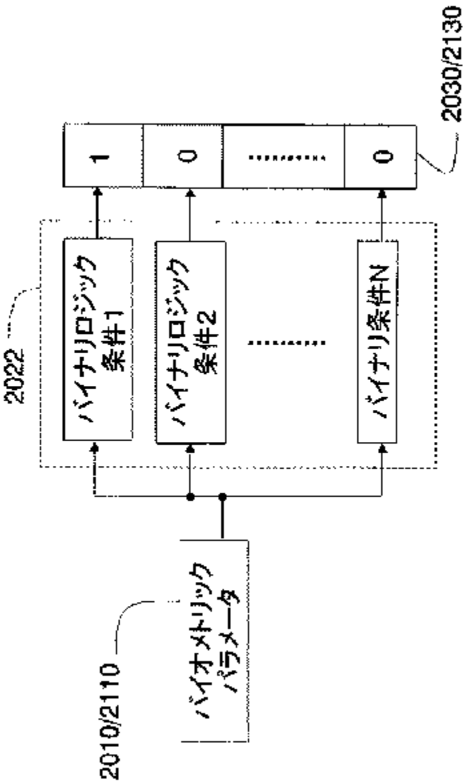
【図22B】



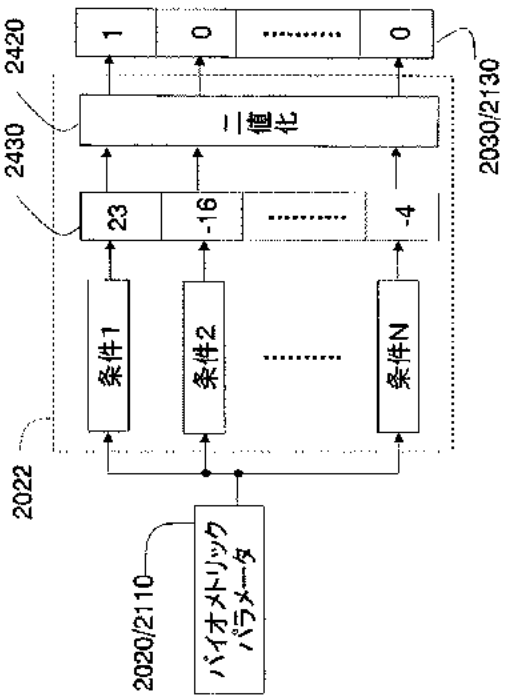
【図22C】



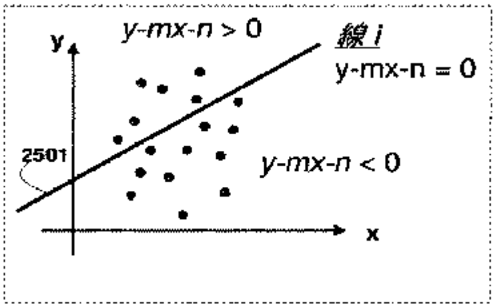
【図23】



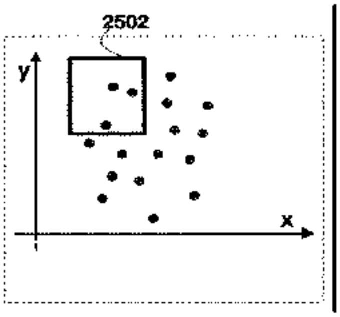
【図24】



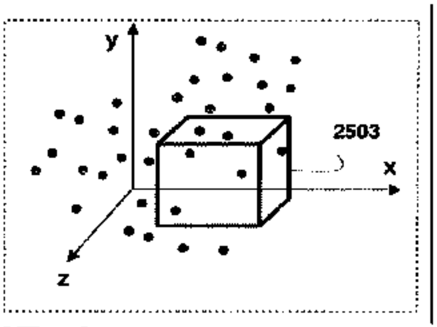
【図25A】



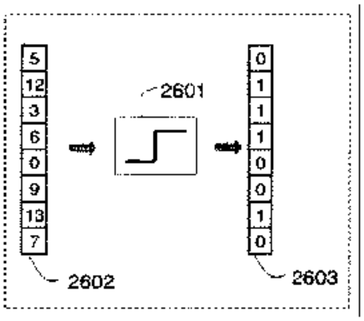
【図25B】



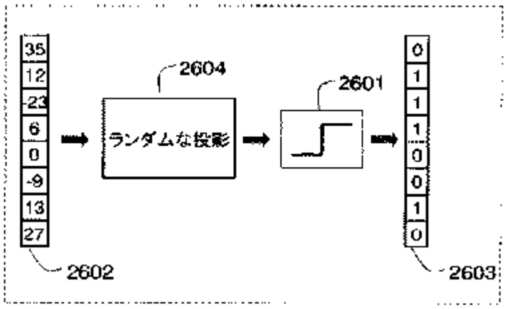
【図25C】



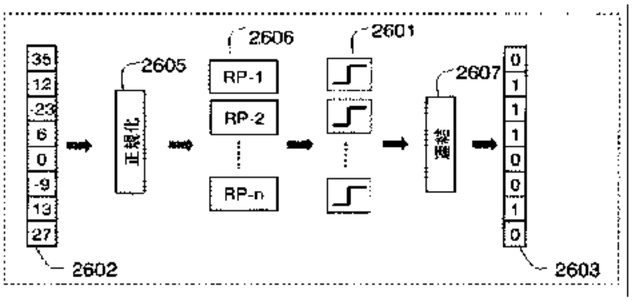
【図26A】



【図26B】



【図26C】



(74)代理人　100111648
弁理士　梶並　順
(74)代理人　100122437
弁理士　大宅　一宏
(74)代理人　100147566
弁理士　上田　俊一
(72)発明者　ジョナサン・エス・イェディディア
アメリカ合衆国、マサチューセッツ州、ケンブリッジ、ハーバード・ストリート　３１０
(72)発明者　スターク・シー・ドレーパー
アメリカ合衆国、ウィスコンシン州、マディソン、イートン・リッジ　２３３０
(72)発明者　ヤギズ・ストゥク
アメリカ合衆国、マサチューセッツ州、アーリントン、マサチューセッツ・アベニュー　２３０、アパートメント　３
(72)発明者　アンソニー・ヴェトロ
アメリカ合衆国、マサチューセッツ州、アーリントン、ウォーレン・ストリート　１３３、ユニット　２
Ｆターム(参考) 4C038 VA07　VA20　VB01
5B043 AA09　BA02　BA04　BA07　DA05　EA05　EA07　EA08　EA12　EA13
FA07　FA09　GA02　GA17
5J104 AA07　KA16　PA07

【外国語明細書】

Pre-processing Method for Biometric Parameters before Encoding and Decoding

Related Application

[001] This is a Continuation-in-Part Application of U.S. Patent Application Sn. 11/564,638, "Biometric Based User Authentication and Data Encryption," filed by Draper et al., on November 29, 2006, which is a Continuation-in-Part Application of U.S. Patent Application Sn. 11/218,261, "Biometric Based User Authentication and Data Encryption," filed by Martinian et al., on September 1, 2005, U.S. Publication 2006-0123241, which is a Continuation-in-Part Application of U.S. Patent Application serial number 11/006,308, "Biometric Based User Authentication with Syndrome Codes," filed by Martinian et al. on December 7, 2004, U.S. Publication 2006-0123239.

Field of the Invention

[002] The invention relates generally to the fields of cryptography, and more particularly to acquiring, pre-processing, encoding, and storing biometric parameters for user authentication and data encryption.

Background of the Invention

[003] Conventional Password Based Security Systems

[004] Conventional password based security systems typically include two phases. Specifically, during an enrollment phase, users select passwords,

which are stored on an authentication device, such as server. To gain access to resources or data during an authentication phase, the users enter their passwords, which are verified against the stored versions of the passwords. If the passwords are stored as plain text, then an adversary who gains access to the system could obtain every password. Thus, even a single successful attack can compromise the security of the entire system.

[005] As shown in Figure 1, a conventional password based security system 100 stores 115 encrypted 110 passwords 101 in a password database 120 during an enrollment phase 10. Specifically, if X is password 101 to be stored 115, the system 100 actually stores $f(X)$ where $f(.)$ is some encryption or hash function 110. During an authentication phase 20, a user enters a candidate password Y 102, the system determines 130 $f(Y)$, and only grants access 150 to the system when $f(Y)$ matches 140 the stored password $f(X)$, otherwise, access is denied 160.

[006] As an advantage, encrypted passwords are useless to an adversary without the encryption function, which are usually very difficult to invert.

[007] Conventional Biometric Based Security Systems

[008] A biometric security system measures physical biometric features to obtain biometric parameters, sometimes called observations. A conventional biometric security system has the same vulnerability as a password based system, which stores unencrypted passwords. Specifically, if the database stores unencrypted biometric parameters, then the parameters are subject to attack and misuse.

[009] For example, in a security system using facc recognition system or voice recognition, an adversary could search for biometric parameters similar to the adversary. After suitable biometric parameters are located, the adversary could modify the parameters to match the appcarance or voice of the adversary to gain unauthorized acccss. Similarly, in security system using fingerprint or iris recognition, the adversary could construct a device that imitates a matching fingerprint or iris to gain unauthorized access, e.g., the device is a fake finger or fake eye.

[0010] It is not always possible to encrypt biometric parameters due to not only the possible variability of thc underlying biometric features, but also in the way the featurcs are measured. This difference can be termed "noise."

[0011] Specifically, biometric parameters *X* arc entered during the enrollment phase. Say that the parameters *X* are encrypted using an encryption or hashing function *f*(*X*), and stored. During the authentication phase, the biometric parameters obtaincd from the same user can be different. For examplc, in a security system using face recognition, the cameras used for enrollment and authentication can have different oricntations, sensitivities, and resolution. The lighting is usually quite different. Skin tone, hairstyle and other facial features are easy to change. Thus, during authentication, if the newly observed parameters *Y* are passed through thc same cncryption function *f*, the rcsult *f(Y)* will not match *f(X)* causing rejection. Similar problems exist with other biometrically based user authentication, such as iris and fingcrprint patterns.

[0012] Error Correcting Codes

[0013] An (N, K) error correcting code (ECC) C, over an alphabet Q, includes Q^K vectors of length N. A linear (N, K) ECC can be described either by using a generator matrix $\mathbf{G}$, with N rows and K columns, or by using a parity check matrix $\mathbf{H}$, with N-K rows and N columns. The name 'generator matrix' is based on the fact that a codeword expressed as a vector $\mathbf{w}$, can be generated from any length K input row vector $\mathbf{v}$, by right multiplying the vector $\mathbf{v}$ by the matrix $\mathbf{G}$ according to $\mathbf{w} = \mathbf{vG}$. Similarly, to check if the vector $\mathbf{w}$ is a codeword, one can check whether $\mathbf{Hw}^T = 0$, where a column vector $\mathbf{w}^T$ is a transpose of the row $\mathbf{w}$.

[0014] In the standard use of error correcting codes, an input vector $\mathbf{v}$ is encoded into the vector $\mathbf{w}$, and either stored or transmitted. If a corrupted version of the vector $\mathbf{w}$ is received, a decoder uses redundancy in the code to correct for errors. Intuitively, the error capability of the code depends on the amount of redundancy in the code.

[0015] Slepian-Wolf, Wyner-Ziv, and Syndrome Codes

[0016] In some sense, a Slepian-Wolf (SW) code is the opposite of an error correcting code. While an error correcting code adds redundancy and expands the data, the SW code removes redundancy and compresses the data. Specifically, vectors $\mathbf{x}$ and $\mathbf{y}$ represent the correlated data. If an encoder desires to communicate the vector $\mathbf{x}$ to a decoder that already has the vector $\mathbf{y}$, then the encoder can compress the data to take into account the fact that the decoder has the vector $\mathbf{y}$.

[0017] For an extreme example, if the vectors **x** and **y** are different by only one bit, then the encoder can achieve compression by simply describing the vector **x**, and the positions of the differences. Of course, more sophisticated codes are required for more realistic correlation models.

[0018] The basic theory of SW coding, as well as a related Wyner-Ziv (WZ) coding, are described by Slepian and Wolf in "Noiseless coding of correlated information sources," IEEE Transactions on Information Theory, Vol. 19, pp. 471-480, July 1973, and Wyner and Ziv in "The rate-distortion function for source coding with side information at the decoder," IEEE Transactions on Information Theory, Vol. 22, pp. 1-10, January 1976. More recently, Pradhan and Ramchandran described a practical implementation of such codes in "Distributed Source Coding Using Syndromes (DISCUS): Design and Construction," IEEE Transactions on Information Theory, Vol. 49, pp. 626-643, March 2003.

[0019] Essentially, the syndrome codes work by using a parity check matrix **H** with N-K rows and N columns. To compress a binary vector **x** of length N to a syndrome vector of length K, determine $S = \mathbf{Hx}$. Decoding often depends on details of the particular syndrome code used. For example, if the syndrome code is trellis based, then various dynamic programming based search algorithms such as the well known Viterbi algorithm can be used to find the mostly likely source sequence X corresponding to the syndrome vector S, and a sequence of side information as described by Pradhan et al.

[0020] Alternatively, if low density parity check syndrome codes are used, then belief propagation decoding can be applied as described in "On some new approaches to practical Slepian-Wolf compression inspired by channel coding" by Coleman et al., in Proceedings of thc Data Compression Conference, March, 2004, pages 282 – 291.

[0021] Factor Graphs

[0022] In the prior art, codes as described above are often represented by a bipartite graph that is called a "factor graph," see F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor Graphs and the Sum-Product Algorithm," IEEE Transactions on Information Theory, vol. 47, pp. 498-519, February 2001, G. D. Forney, Jr., "Codes on Graphs: Normal Realizations," IEEE Transactions on Information Thcory, vol. 47, pp. 520-549, February 2001, and R. M. Tanner, "A Recursive Approach to Low-Complexity Codes," IEEE Transactions on Information Theory, vol. 27, pp. 533-547, September, 1981, all incorporated herein by reference.

[0023] Generally, a factor graph is a bipartite graph, containing two types of nodes, called "variable nodes" and "factor nodcs." Variable nodes are only connected to factor nodes and vice-versa. Factor nodes are conventionally drawn using squares, variablc nodes are conventionally drawn using circles, and connections between variable and factor nodes are denoted by lines connecting the corresponding circles and squares. Sometimes a symbol, i.e., '+', is drawn inside a factor node to represent the kind of constraint that it enforces.

[0024] The variable nodes represent the symbols that arc used in the code, and the factor nodes represent the constraints on the symbols. A variable node is only connccted to a factor node if it is subject to the corresponding constraint.

[0025] Biometric Parameter Coding Prior Art

[0026] Prior art related to the current invention falls into three categories. First, there is a great deal of prior art describing feature extraction, recording, and use of biometric parameters unrelatcd to the secure storage of such biometric parameters. Becausc our invention is concerned with secure storage, and largely independent of the details of how the biometric parameters are acquired, details of this category of prior art are omitted.

[0027] The second class of prior art, which is relevant to the invention, includes the following systems designcd for secure storage and authentication of biometrics, "Method and system for normalizing biometric variations to authenticate users from a public database and that ensures individual biometric data privacy," US Patent 6,038,315; "On enabling secure applications through off-line biometric identification," by Davida, G.I., Frankel, Y., Matt, B.J. in Proceedings of the IEEE Symposium on Security and Privacy, May 1998; "A Fuzzy Vault Scheme," by Juels, A., Sudan, M., in Proceedings of the 2002 IEEE International Symposium on Information Theory, June 2002; US Patent Application SN 09/ 994,476, "Order invariant fuzzy commitment system," filed November 26, 2001; Juels and Wattenberg, "A fuzzy commitment scheme," in Proc. 5th ACM Conf. on Comp. and Commun. Security, New York, NY, pgs. 28-36, 1999;

S. Yang and I. M. Verbauwhede, "Secure fuzzy vault based fingerprint verification system," in Asilomar Conf. on Signals, Systems, and Comp., vol. 1, pp. 577-581, November 2004. U. Uludag and A. Jain, "Fuzzy fingerprint vault," in Proc. Workshop: Biometrics: Challenges arising from theory to practice, pp. 13-16, August 2004.

[0028] Figure 2 shows some of the details of the basic method described in U.S. Patent 6,038,315. In the enrollment phase 210, biometric parameters are acquired in the form of a sequence of bits denoted E 201. Next, a random codeword W 202 is selected from a binary error correcting code and additively combined with the parameters E using an exclusive OR (XOR) function 220 to produce a reference R 221. Optionally, the reference R can be further encoded 230. In any case, the reference R is stored in a password database 240.

[0029] In the authentication phase 220, a biometric parameters E' 205 are presented for authentication. The method determines 250 the XOR of R with E' to essentially subtract the two to obtain $Z = R - E' = W + E - E'$ 251. This result is then decoded 260 with the error correcting code to produce W' 261. In step 270, if W' matches W, then access is granted 271, and otherwise, access is denied 272.

[0030] That method essentially measures the Hamming distance, i.e., the number of bits that are different, between the enrolled biometric E 201, and the authentication biometric E' 205. If the difference is less than some predetermined threshold, then, then access is granted. Because the method stores only the reference *R*, and not the actual biometric parameters *E*, the method is secure.

[0031] Davida et al. and Juels et al. describe variations of the method shown in Figure 2. Specifically, both encode the biometric data with an error correcting code during the enrollment phase followed by an operation to secure the resulting codeword. Davida et al. hide the codeword by only sending the check bits, while Juels et al. add some amount of noise referred to as 'chaff'.

[0032] US Patent 6,363,485, "Multi-factor biometric authenticating device and method," describes a method for combining biometric data with an error correcting code and some secret information, such as a password or personal identification number (PIN), to generate a secret key. Error correcting codes, such as Goppa codes or BCH codes, are employed with various XOR operations.

[0033] In addition to fixed database access control systems illustrated in Figure 2, a third class of prior art includes using biometrics for data protection, specifically data protection for mobile devices that include memory, such as laptops, PDAs, cellular telephones, and digital cameras. Because mobile devices are easily lost or stolen, it becomes necessary to protect data stored in mobile devices.

[0034] Problems with the Prior Art

[0035] Figure 4 illustrates the problem with existing approaches for storing data D 401. In an encoding process 410, biometric parameters P 402 are obtained from a user and used as a key to encrypt 440 data D to produce the ciphertext C 441. Both P and C are saved in storage 450. When a user wishes to decrypt 420 the data 420, biometric parameters P' 460 are obtained from a user and compared to the stored biometric P 402. If P' matches P, 470, then the system allows access and uses P to decrypt the stored ciphertext C to produce the data D 401, otherwise the data are not decrypted 471.

[0036] Such a prior art system is only effective as long as the storage medium is not compromised. If an adversary can access such media, then the adversary obtains P and decodes the data.

[0037] First, the bit-based prior art method provides dubious security. In addition, biometric parameters are often real-valued or integer-valued, instead of binary valued. The prior art assumes generally that biometric parameters are composed of uniformly distributed random bits, and that it is difficult to determine these bits exactly from the stored biometric. In practice, biometric parameters are often biased, which negatively affect security. Also, an attack can cause significant harm, even if the adversary recovers only an approximate version of the stored biometric. Prior art methods are not designed to prevent the adversary from estimating the actual biometric from the encoded version.

[0038] For example, US Patent 6,038,315 relies on the fact that the reference value $R = W + E$ effectively encrypts the biometric E by adding the random codeword *W*. However, that method achieves poor security. There are a number of ways to recover *E* from *R*. For example, if the vector *E* has only a few bits equal to one, then the Hamming distance between *R* and the *W* is small. Thus, an error correction decoder could easily recover *W* from *R*, and hence also recover *E*. Alternatively, if the distribution of codewords is poor, e.g., if the weight spectrum of the code is small and many codewords are clustered around the all zero vector, then an adversary could obtain a good approximation of *E* from *R*.

[0039] Second, in addition to dubious security, prior art methods have the practical disadvantage of increasing the amount of data stored. Because biometric databases often store data for many individual users, the additional storage significantly increases the cost and complexity of the system.

[0040] Third, many prior art methods require error correction codes or algorithms with a high computational complexity. For example, the Reed-Solomon and Reed-Muller decoding algorithms of the prior art generally have a computational complexity, which is at least quadratic, and often a higher order in the length of the encoded biometric.

[0041] Fourth, there are fundamental problems with the basic architecture for the mobile security systems known in the prior art. Mobile security systems such as the one shown in Figure 4 can only be effective if the mobile security system itself is not compromised. Returning to the example of a mobile security system on a laptop, the security can only be effective if an adversary cannot physically access the media where P and C are stored. If an adversary can access such media, e.g., by removing the hard disk from the laptop, then the adversary immediatcly obtains P which was the encryption key used to generate C and therefore decrypt C.

[0042] The main difficulty with prior mobile security systems is that the encryption key corresponding to the user's biometric parameters are stored in the dcvice. Thus, if the device is stolen, then the data can be decoded using the stored parameters.

[0043] Fifth, because there are no good methods for performing crror correcting coding or syndrome code decoding for the noise structure particular to biometrics, nor has much thought even gone into modeling thc noise structure, most prior art on secure biometric systems use a memoryless noise model, or other models that ovcrsimplify the nature of the noise, and do not rcflect actual operational conditions. That is, the prior art models do not accurately represent the time varying dynamics of biometric features and the acquisition and measurement processes. Instcad, those models assume that the noise is memoryless and has no spatial or temporal structurc.

[0044] Oftcn, biometric features vary from one measurement to another. For example, in fingerprint biometrics "minutiae" points are often used as the feature set. The relative positions and orientations of minutiac can bc quite different during enrollment and authentication. This makes the authentication process difficult. Most straightforward attempts to solvc this problem use models that are cxtremcly high-dimensional and therefore impractical for practical implementations.

[0045] Therefore, it is desired to provide a model for biometric data including structured noise. In addition is desired to pre-process the biometric parameters so pre-processed parameters have a form that is best suited for encoding and decoding using channel codes.

Summary of the Invention

[0046] Biometric parameters, which are acquired from human faces, voices, fingerprints and irises for example, can be used for user authentication and data access control. Biometric parameters cannot be stored in hashed or encrypted forms in databases as is done with passwords because the parameters are usually continuous and can vary from one reading to the next, for the same user. For example, a sampled appearance of a face or fingerprint, or tone of a voice can change over time.

[0047] One embodiment of the invention uses syndrome codes to protect the biometric data, e.g., syndrome codes based on Wyner-Ziv or Slepian-Wolf coding. The output of syndrome encoding, which we term a syndrome vector, can be stored securely in a database, while still tolerating the inherent variability of the raw biometric data.

[0048] Specifically, the biometric syndrome vector according to the invention has the following properties.

[0049] First, the syndrome code effectively hides or encrypts information about the original biometric characteristics so that if the syndrome database is compromised, the stored syndrome vector is of little use in circumventing the security of the system.

[0050] Second, given a second noisy measurement of each biometric, the corresponding stored syndrome vector can be decoded to yield the original biometric parameters, and to decrypt data that was encrypted with the original biometric parameters.

[0051] Third, the syndrome coding methodology can be used for user authentication.

[0052] A second embodiment of the invention describes a method for efficiently modeling biometric parameters that can vary over time due to variations in the biometric features, and additionally models the measurement process.

[0053] The method allows one to accurately exploit relationships between multiple readings of biometric features in a computationally efficient manner. In particular, the method enables one to successfully perform syndrome decoding of such biometric features much better than existing prior art methods.

[0054] In one embodiment, the biometric parameters are pre-processed according to a set of logical conditions to form a binary representation that has a set of predetermined statistical properties. It should be noted that the statistical properties are target properties we desire to achieve.

Detailed Description of the Preferred Embodiment

[0055] Embodiments of our invention include thc following components: a syndrome encoder and hashing method for securely storing biometric parameters, a syndrome code based encryption method for securely storing data encrypted with biometric keys, and a method of optimizing syndrome codes used for secure biometric applications such as the former two methods.

[0056] Syndrome and Hashing Method for Secure Biometric parameters

[0057] Figure 3 shows a syndrome and hashing based biometric security system 300 according to our invention. Biometric features of a user are measured to obtain biometric parameters (data or observations). The method according to our invention compresses biometric parameters with a syndrome code to produce a compressed syndrome vector.

[0058] Unlike conventional compression, the original biometric data cannot be reconstructed or approximated solely from the syndrome vector produced by the syndrome code. The syndrome vector and a hash of the original biometric parameters are stored in a biometric database.

[0059] To authenticate the user, biometric parameters are measured again. The biometric parameters are combined with the stored syndrome vector to decode the original biometric parameters. If syndrome decoding fails, the original biometric parameters are not recovered and the hash of the decoded parameters does not match the stored hash. Therefore, the user is denied access. If syndrome decoding succeeds, then the hash of the original biometric parameters matches the hash of the decoded parameters, which verifies the authenticity of the user. The role of the hash is to provide user entry control, to make sure that the biometric parameters provided by the user are good enough to exactly reconstruct the original biometric parameters. While both the syndrome encoder and hash are a many-to-one mapping, the syndrome code has a structure that is useful in reconstructing the original biometric parameters. On the other hand, the hash function can be, e.g., a cryptographic hash, which provides no useful information in estimating the original biometric.

[0060] Enrollment Phase

[0061] In the enrollment phase 310, biometric data are acquired of physical features of a user. For example, the biometric data are derived from an image of a face, a recording of speech, an image of a fingerprint, or a scan of an iris.

[0062] Hereinafter, biometric data refers to the raw biometric signal sensed, measured or otherwise acquired from the physical features of the user. Features are extracted from the biometric data. The features are arranged in a *d*-dimensional feature vector. The feature vector forms enrollment biometric parameters 301. Methods for extracting features from various forms of biometric data are well known in the art, as described above. Conversion of the feature vector to biometric parameters and an optimal syndrome code are described in greater detail below.

[0063] The biometric parameters *E* 301 are encoded using a syndrome encoder 330 to produce an enrollment syndrome vector *S* 331. Next, a message authentication code or hash function is applied 340 to the biometric parameters E to produce an enrollment hash *H* 341. The hash function can be the well-known MD5 cryptographic hash function described by Ron Rivest in “The MD5 Message Digest Algorithm,” RFC 1321, April 1992. The enrollment syndrome vector—hash pair (*S*, *H*) 331, 341 is stored in a biometric database 350.

[0064] Any type of syndrome code, e.g., the SW code or the WZ code described above, can be used. The preferred embodiment of the invention uses codes derived from so-called “repeat-accumulate codes,” namely “product-accumulate codes,” and codes that we call “extended Hamming-accumulate codes.”

[0065] We refer generally to these as *serially concatenated accumulate* (SCA) *codes*. For more information on these classes of codes in a general sense, see J. Li, K.R. Narayanan, and C.N. Georghiades, “Product Accumulate Codes: A Class of Codes With Near-Capacity Performance and Low Decoding Complexity,” IEEE Transactions on Information Theory, Vol. 50, pp. 31-46, January 2004; M. Isaka and M. Fossorier, “High Rate Serially Concatenated Coding with Extended Hamming Codes,” submitted to IEEE Communications Letters, 2004; and D. Divsalar and S. Dolinar, “Concatenation of Hamming Codes and Accumulator Codes with High Order Modulation for High Speed Decoding,” IPN Progress Report 42-156, Jet Propulsion Laboratory, Feb. 15, 2004.

[0066] U.S. Patent Application Sn. 10/928,448, "Compressing Signals Using Serially-Concatenated Accumulate Codes," filed by Yedidia, et al. on August 27, 2004, incorporated herein by reference, describes the operation of our preferred syndrome encoder based on SCA codes as used by the present invention.

[0067] Our syndrome encoder 330 for the biometric parameters 301 has a number of advantages. The syndrome encoder 330 can operate on integer-valued inputs. In contrast, prior art encoders generally operate on binary valued inputs. The syndrome encoder has very high compression rates to minimize the storage requirements of the biometric database 350. The syndrome encoder can be designed to be rate-adaptive, and can operate in an incremental fashion.

[0068] Authentication Phase

[0069] In an authentication phase 320, biometric data are again acquired from the user. Features are extracted to obtain authentication biometric parameters *E'* 360. The database 350 is searched to locate the matching enrollment syndrome vector *S* 331 and enrollment hash *H* 341 for this user.

[0070] The search can check every entry (*S*-*H* pairs) in the database 350, or a heuristically ordered search can be used to accelerate the process of finding a matching entry. Specifically, if we denote the i^{th} syndrome vector—hash pair in the database as (S_i, H_i), then an exhaustive search first applies syndrome decoding to *E*' and S_1 and compares the hash of the syndrome decoder output to H_1. If access is denied, the same process is attempted with

(S_2, H_2), then (S_3, H_3), etc. until all entries have been tried or access was granted.

[0071] If extra information such as an enrollment user-name is available, then the search can be accelerated. For example, the hash of the enrollment user-name (not to be confused with the hash *H* of the biometric parameters) is stored with the pair *S* and *H* during the enrollment phase. Then, in the authentication phase, the user supplies an authentication user-name, and the system determines the hash of the authentication user-name, and search the database for an *S-H* pair with a matching hashed enrollment user-name, and attempts to authenticate *E*' with the resulting *S-H* pair.

[0072] Specifically, a syndrome decoder 370 is applied to the enrollment syndrome vector *S*, with the authentication parameters *E*' 360 acting as 'side' information. Syndrome decoders are known in the art generally. Typically, decoders that use belief propagation or turbo codes have excellent error resiliency with low complexity. An output of the syndrome decoder 370 are decoded enrollment parameters *E*'' 371. The decoded value *E*'' 371 is an estimate of the original biometric parameter *E* 301 that were used to produce the syndrome vector *S* 331. The hash function 340 is applied to *E*'' 371 to produce an authentication hash *H*' 381.

[0073] The enrollment and authentication values *H* 341 and *H*' 381 are compared 390. If the values do not match, then access is denied 392. Otherwise, the value *E*'' 381 substantially matches the original biometric *E* 301. In this case, the user can be granted access 391.

[0074] In addition, a direct comparison can be made between the decoded parameters *E*'' 381 and the authentication biometric parameters *E*' 360 to authenticate the user. For example, if *E*' and *E*'' correspond to biometric parameters in a face recognition system, conventional algorithms for comparing the similarity between faces could be applied to the parameters *E*' and *E*''.

[0075] Syndrome Based Data Encryption

[0076] Figure 5 shows a method 500 for encoding 510 and decoding 520 data 501. In the encoding process 510, first biometric parameters P 502 are obtained from a first user. The parameters are used to encrypt 540 input data D 501 to produce the ciphertext C 541. In contrast to the prior art, however, the first biometric parameters P are never stored in a memory. Instead, a syndrome encoder 530 encodes the first biometric parameters P to produce a syndrome vector S 531, and the pair (S, C) are associated with each other, and stored in a memory 550. In one embodiment of the invention, the input data are the raw biometric data acquired from a user during an enrollment process.

[0077] When a person wishes to decrypt 520 the ciphertext 541, second biometric parameters P' 560 are acquired from a second user. The stored syndrome vector C 531 is syndrome decoded using the second biometric parameters to produce third biometric parameters P'' 571. The third biometric parameters P'' are then used to decrypt 580 the ciphertext 541 to produce output data D' 509. Obviously, if the second or third biometric parameters do not match the first biometric parameters, the output data D'

509 do not match the input data D 501. The output data will only match the input data exactly if the first user and the second user are the identical person.

[0078] In one embodiment of this invention, the hash *H* of the biometric parameters can also be stored, as described above. Checking that the hashes match confirms that decryption was successful. Without the hash, security is maintained but the decoder cannot confirm that decryption was successful. For many types of source data, the hash is not necessary because the file that results from incorrect decryption does not correspond to anything useful.

[0079] The method has the following advantages. If an adversary gains access to the syndrome vector and the ciphertext (S, C), the data cannot be decrypted. This is because the encryption key, i.e., the first biometric parameters P cannot be recovered from the syndrome vector. In addition, because of error correcting properties of syndrome codes, even if the second biometric parameters P' differs slightly from the first biometric parameters P, a suitably designed syndrome decoder can successfully produce the third biometric parameters P'' that are exactly the same as the first biometric parameters used as the encryption key P 502.

[0080] Syndrome encoding provides an effective way to securely store biometric parameters, and can be applied to other methods of securely storing biometric information. It should be noted that feature vectors can be extracted from biometric data. Therefore, any of the above described biometric parameters can be replaced by a corresponding feature vector.

[0081] An additional advantage of storing the biometric parameters in an encrypted form is that this enables secure biometric storage applications to operate on different feature vectors from those used in biometric recognition applications. For example, fingerprint recognition systems often use a feature vector based on so-called 'minutiae' extracted from an image of a fingerprint. Similarly, iris recognition systems sometimes use features extracted from passing the iris image through a bank of Gabor filters.

[0082] In many cases, the ideal feature vector for biometric recognition, e.g., face recognition or fingerprint identification, can be different than the ideal feature vector for syndrome encoding/decoding. In many cases this is due to the fact that a process for training a classifier for a recognition or identification system, e.g., a classifier based on a Gaussian mixture model (GMM), neural networks, or hidden Markov models, produce different feature vectors from a process used for training a histogram used with a belief propagation decoder of syndrome encoders and decoders as described herein.

[0083] Figure 6 shows a method 600 for storing an encrypted version of input biometric data 601. As described above, the biometric data are derived from the raw signal used to measure or sense biometric characteristics of a user.

[0084] In the enrollment phase 610 of an access control system, for example, first biometric data B 601 are acquired from a user. Then, a feature vector of first biometric parameters P 602 is obtained from the first biometric data B 601. The first biometric data B are encrypted 640 using the first biometric parameters P as the encryption key to produce ciphertext C 641. In addition, the first biometric parameters are syndrome encoded to produce a syndrome vector S 631. The associated pair (S, C) is then stored in a biometric database 650.

[0085] In an authentication phase 620, authentication second biometric data B' 660 are obtained from a user. The second data are used to generate a feature vector of the second biometric parameters P' 661. Then, a syndrome decoder 670 decodes the first biometric parameters to produce third biometric parameters P'' 671. The third biometric parameters are then used as a key to decrypt 680 the ciphertext C to produce third biometric data B'' 681. Then, the authentication biometric data B' and the decoded biometric data B'' are compared by a biometric recognition method 690 to determine whether access to a particular function is granted or denied 692. As before, the access is only granted if the first and third biometric data are exactly identical, i.e., the first and second users are the same person.

[0086] In another variation, the comparison step can use feature vectors extracted from the biometric data. The feature vectors do not need to be same the as the biometric parameters. Furthermore, the two feature vectors that are being compared only need to be substantially the same because the verification step may use a totally different process. Thus, the feature vectors can admit a wider range in variation in the biometric data that characterize a particular user over time.

[0087] We list some advantages of the process shown in Figure 6. The authentication system can use a conventional recognition system in step 690. In addition, the biometric paramcters P and P' used by the syndrome encoder/decoder can be selected independently of parameters or feature vectors used by the biometric verification step 690. Furthermore, syndrome encoding is an effective method of securely storing biometric parameters. However, the method shown in Figure 6 can also be applied to other methods of securely storing biometric parameters.

[0088] Designing Optimal Syndrome Codes for Secure Biometric Parameters

[0089] In general there is a trade-off between security and accuracy in using syndrome codes to protect biometric parameters and biometric features. Specifically, a key parameter of any syndrome code is the number of bits in the syndrome vector. A syndrome vector with a large number of bits conveys more information about the biometric data and makes it easier to tolerate noise and variations in the biometric data. In contrast, a smaller syndrome vector gives less information to an adversary but is more prone to error.

[0090] At one extreme, when the length of the syndrome vector is substantially the same as the length of the underlying biometric data, any amount of noise can be tolerated because the original biometric data can be exactly recovered from only the syndrome vector. Of course, in this case an adversary who obtains the syndrome vector can possibly also recover the biometric data, compromising the security of the system.

[0091] At the other extreme, a syndrome vector of a very small number of bits provides extremely good security, in the sense that the adversary cannot recover the biometric data from the syndrome vector. However, in this case, permissible variations between the enrollment biometric data and the authentication biometric data are limited.

[0092] Obviously, a syndrome based encoder and decoder should select a length for the syndrome vector that balances security and toleration of biometric variations. However, a carefully designed syndrome code can improve error resiliency.

[0093] The design and operation of the syndrome code is described with the following terminology as shown in Figure 12. The biometric data 1201 can be, e.g., an image of a face or fingerprint. A full feature vector 1202 is extracted from the training biometric data. The full feature vector 1202 is reduced down to a syndrome feature vector 1203. The syndrome feature vector captures those parts of the full feature vector that the designer decides are appropriate for syndrome encoding and decoding. A syndrome code is used to encode the syndrome vector 1204 from the syndrome feature vector. The syndrome feature vector 1203 plays the role of the biometric parameter E 310 in Figure 3 while the syndrome vector is S 331.

[0094] Biometric Statistical Model

[0095] Figure 13 shows a process 1300 for constructing the syndrome code 1204 and a corresponding decoder 1205 (i.e., encoder and decoder) according to an embodiment of the invention. The training biometric data 1301 are acquired. Parameters 1302 of a selected feature model 1304 are determined 1310 from the training data. In terms of codecs, the feature model essentially is the "*source*" model. Similarly, parameters 1303 of a selected measurement model 1305 are determined 1320. The measurement model effectively is the "*channel*" model. The parameters 1302-1303 and models 1304-1305 are then used to construct the syndrome code and corresponding decoder. It should be noted that that the channel model is designed to cope with the structured noise in the measurement process. The noise can be due, e.g., to changes in the features of the biometric data as observed at different measurement instances, as well as insertions and deletions of features between instances.

[0096] While many tools of machine learning can help in the above design process, this problem is quite different from many modeling problems in machine learning because the resultant model has a "hard" feature vector that is appropriate for syndrome encoding. We discuss the difference between "hard" and "soft" feature vectors in greater detail below.

[0097] As shown in Figure 12, the syndrome feature vector 1203 is typically of a reduced size to make syndrome decoding tractable. To construct the syndrome code, we can apply a density evolution to a degree distribution. The syndrome code is further refined to take into account features such as a finite block-length of the syndrome feature vector 1203, or the need to use a variable-rate code to match the syndrome vector 1204 to the variations in biometric features across users.

[0098] After the syndrome code has been constructed selected, we construct an iterative belief propagation decoder as described below.

[0099] **Quantization**

[00100] Before detailing an instance 700 of the process 1300, which is shown in Figure 7, we first define the following terminology that distinguishes between the use of biometric data during enrollment and during authentication. We use the term 'hard' feature vector to refer to a quantized version of a feature vector, and the term 'soft' feature vector to refer to either an unquantized feature vector or a version of the feature vector that is quantized finely.

[00101] Quantization is used because some biometric parameters can include integers and real numbers over a relatively large numeric range. Encryption, key generation, and other authentication processes work best with integers over a small range.

[00102] The reason that we distinguish between a 'hard' feature vector and a 'soft' feature vector is that the syndrome vector is derived from a 'hard' feature vector. Therefore, the 'hard' feature vector is usually quantized. In contrast, during the authentication phase, the syndrome decoder may combine a 'soft' feature vector with the syndrome vector to decode the 'hard' feature vector. Therefore the 'soft' feature vector does not need to be quantized or may be quantized differently to decrease errors in the system. For example, the use of a soft feature vector makes it possible for the syndrome decoder to take as inputs likelihoods of each feature rather than a hard decision of the most likely choice of each feature.

[00103] In general, there are multiple ways to extract a full feature vector from biometric data, as well as multiple ways to extract 'hard' and 'soft' feature vectors from the full feature vector. Therefore, we apply the process of Figure 13 to each possibility and select the syndrome feature vector 1304 that yields the best overall results during training.

[00104] Figure 7 shows the details of an instance of process 1300 for constructing an optimal syndrome code where the statistical model for the biometric features 1304 represents a Markovian relationship between biometric features. Training biometric data are acquired 800. The biometric data are used to generate an error histogram 890. The error histogram is used to select 900 the syndrome feature vector. In this context, we use the term "full feature vector" 1202, see Figure 12, to denote all biometric parameters, and the term "syndrome feature vector" 1203 to refer to a subset of the full feature vector. The syndrome feature vector can be transformed into an arbitrary feature space.

[00105] After the syndrome feature vector 1203 is selected, we measure 1000 a correlation between different coefficients of the syndrome feature vector. By using the error statistics for the syndrome feature vector and the inter-coefficient correlation, we then apply density evolution 740 to search for a degree distribution that yields an optimal syndrome 1204 code of a given length After the syndrome feature vector and syndrome code have been selected, we construct 1100 a belief propagation decoder that exploits the inter-coefficient correlation.

[00106] Constructing an Error Histogram

[00107] Figure 8 shows a process 800 for generating an crror histogram 890. First, we acquire 810 the training biometric data for a particular user taken on different occasions. Next, we select 820 a pair of biometric parameters B and B', and determine a full 'soft' fcature vector VS(B) 830 and the full 'hard' fcature vector VII(B') 840. Then, for each feature or dimcnsion *i* in the full feature vector, we estimate 845 the value of VH(B') at the corresponding feature *i* from VS(B) at position *i*, and dctermine 850 if the estimate is correct. If thc estimate is incorrect, then we increment 870 a bin for the corresponding values of VH(B') and VS(B) at feature *i* in the error histogram 890. After complcting this proccss for each feature *i*, we check 860 if all pairs of biometrics B and B' have been processed. If not, we return to step 820 and select another pair of biometric parameters. If all pairs have already been processed, then the error histogram is complete and the process terminates 880.

[00108] Selecting a Syndrome Feature Vector

[00109] Figure 9 shows a process 900 for selecting a syndrome feature vector with the aid of the error histogram of Figure 8. First, the error histogram is sortcd 910 from most reliablc to lcast reliablc fcatures 920. Specifically, if E(*i*) is an average error in predicting feature *i* of VH(B') from feature *i* of VS(B), then feature *i* is considcred morc reliablc than featurc *j* whcn E(*i*) < E(*j*). After the error histogram is sorted, we include 930 the next most reliable feature from the error histogram in the syndrome

feature vector, and construct 940 the best syndrome code for the current syndrome feature vector, and test 950 whether including the most recent feature increases security or error resiliency. If security or error resiliency is increased, then we continue adding additional features to the syndrome feature vector. Otherwise, we remove 960 the most recently added feature from the feature vector and we terminate 970 the process.

[00110] If it is desired to specify the level of security and optimize error resilience, then the following steps can be used for steps 940 and 950. First, in step 940, a new syndrome code with length *N* corresponding to the number of features currently in the feature vector is constructed by generating a low density parity check (LDPC) code with *k* syndromes from a fixed degree distribution. In this case, the level of security is held constant by fixing the quantity *N-k*, and keeping it constant throughout the process. Then a random biometric sample of biometric data is selected from the database, mapped to a syndrome vector by applying the parity check matrix of the LDPC code, and the resulting syndrome vector is decoded using belief propagation applied to another random biometric sample from the same user. Repeating this many times, yields an estimate of the error resilience of the syndrome code for the given feature vector. Alternatively, if more computationally complexity is tolerable in the design process, then a density evolution process can be used to optimize the degree distribution for the code, as well as to estimate the error probability more accurately, see T. J. Richardson, M. A. Shokrollahi, and R. L. Urbankediscussed, "Design of capacity-approaching irregular low-density parity-check codes," IEEE Transactions on Information Theory, Volume 47, Issue 2, pp. 619-637, February 2001, incorporated herein by reference.

[00111] If it is desired to specify the level of error resiliency and obtain the best security, the following steps can be used for steps 940 and 950. First, in step 940 a new syndrome code with length *N* corresponding to the number of features currently in the feature vector is designed using the density evolution. Specifically, a sequence of different rate codes are constructed using the density evolution, until the highest rate code is found that meets the specified level of error resiliency as evaluated by the density evolution.

[00112] We refer to the feature vector selected by this process as the "syndrome feature vector" because it is a feature vector designed specifically for the syndrome code. We note that this feature vector can have different properties than other types of feature vectors constructed for biometric recognition, such as face or object recognition.

[00113] Measuring Inter-Coefficient Correlation

[00114] After the syndrome feature vector has been selected, the next step is to measure the inter-coefficient correlation if the data is believed to be correlated. This information cannot be extracted from the error histogram generated according to Figure 7 because that error histogram was generated for the full feature vector 1202, while step 900 selects only a subset of the features in the full feature vector to produce the syndrome feature vector 1203.

[00115] Figure 10 shows a process 1000 for measuring a first-order correlation in a binary syndrome feature vector. This process can also be

applied to non-binary feature vectors or higher order correlations. First, an element from the biometric training data set is selected and a syndrome feature vector is extracted from the element. Then, a counter variable *i* is initialized 1010 to zero. Next, we test 1020 if feature *i* is 0 or 1 and proceed to step 1030 in the former case and step 1040 in the latter. Then, we test 1030 if feature *i*-1, i.e., the previous feature, was 0 or 1, and increment 1035 the appropriate bin in the histogram. Intuitively, bin p00 counts the occurrences of a 0 followed by a 0, and bin p01 counts the occurrences of a 0 followed by a 1, and so forth. Next, we increment 1050 the counter *i*, and test 1060 if more features remain in the syndrome feature vector, and we repeat the process for the next feature. Otherwise, if we have already processed each feature then we terminate 1070 the process.

[00116] After the process in Figure 10 is performed for each element in the biometric training set, we divide the values of the bins p00, p01, p10, and p11 by the size of the biometric training set to measure the first order correlation of the syndrome feature vector.

[00117] Using Density Evolution to Construct an Optimal Syndrome Code

[00118] After the syndrome feature vector 1203 has been selected and the inter-coefficient correlation has been measured, we then design the syndrome code 1204 using density evolution. Specifically, for an LDPC syndrome code, we design the degree distribution for the syndrome code.

[00119] To actually construct the optimal degree distribution, we apply the density evolution technique to produce several candidate degree distributions.

[00120] However, conventional density evolution processes as known in the art do not take into account inter-coefficient correlation. Therefore, while the candidate degree distributions produced by the density evolution may be adequate for the case of no inter-coefficient correlation, they will generally perform differently when inter-coefficient correlation is present.

[00121] In order to obtain the best degree distribution for the syndrome code, we compare the candidate degree distributions obtained by the density evolution on the biometric training data set, and select the degree distribution that performs best. In alternative embodiments, we modify the conventional density evolution algorithm to take into account the inter-coefficient correlation.

[00122] Constructing a Belief Propagation Decoder for the Syndrome Code

[00123] The final step in designing a syndrome code is to construct the associated belief propagation syndrome decoder 1205.

[00124] Figure 11A shows the high level structure of the enrollment phase, where using the syndrome code 1102 an encoder 330 produces a syndrome vector 1204 from the syndrome feature vector 1203.

[00125] Figure 11B shows the structure for the complementary decoder 1107 used during the authentication phase. Again, noisy observations of the biometric data 1104 are acquired of a user attempting to authenticate. The biometric data 1104, together with its measurement model 1305, (and the measurement model parameters 1303), are used together with the syndrome vector 1204 and the feature model 1304 (and the parameters 1302 of that feature model) in an iterative belief propagation network (factor graph) to decode 1107 and produce an estimate 1108 of the original syndrome feature vector 1203. If the decoding is successful, then the estimated syndrome feature vector 1108 and the original syndrome feature vector 1203 match.

[00126] As shown in Figure 11C, our construction 1100 of the belief propagation factor graph includes correlation nodes (C) 1130 that specifies the feature model 1304 (and the model parameters 1302), in addition to the check nodes (+) 1110 that specify the syndrome code 1102, and variable nodes (=) 1120. Specifically, the correlation node is added between each pair of consecutive variable nodes. The method for passing a message from the variable node to adjacent check nodes is modified to include an additional message from each adjacent correlation factor node that is multiplied with the other messages.

[00127] Specifically, using the notation of Kschischang et al., if $\mu_{y \to f}(x)$ is the incoming message for state x to variable node y from check f, and $L(x)$ is the incoming message from the correlation node on the left, then the outgoing message from the variable node to the correlation node on the right is

$$L(x) \cdot \prod \mu_{y \to f}(x),$$

while the outgoing message to the correlation node on the left is

$$R(x) \cdot \prod \mu_{y \rightarrow t}(x),$$

where $R(x)$ is the incoming message from the correlation node on the right.

[00128] We also describe a method for passing a message to and from the correlation nodes according to an embodiment of our invention. Specifically, we describe the procedure for determining the messages $L(x)$ and $R(x)$. If $\mu(0)$ is the incoming message to a correlation node on the left, then the outgoing message on the right side of the correlation node, which is the incoming message to the variable node to the right of the correlation node, is

$$L(0) = \mathrm{p00} \cdot \mu(0) + \mathrm{p10} \cdot \mu(1) \text{ and } L(1) = \mathrm{p10} \cdot \mu(0) + \mathrm{p11} \cdot \mu(1),$$

where the p00, p01, p10, and p11 terms are the first order correlation values measured as shown in Figure 10.

[00129] Similarly, the outgoing message on the left side of the correlation node, which is the incoming message to the variable node on the left of the correlation node, is

[00130] $R(0) = \mathrm{p00} \cdot \mu(0) + \mathrm{p01} \cdot \mu(1)$ and $R(1) = \mathrm{p01} \cdot \mu(0) + \mathrm{p11} \cdot \mu(1)$.

[00131] Syndrome Code Design for Iris Biometric parameters

[00132] Next, we describe the application of the procedure 700 to the specific case of iris biometric parameters. We select the full 'hard' feature vector to be the sequence of bits extracted from a set of Gabor filters as described in "How iris recognition works," by J. Daugman in IEEE

Transactions on Circuits and Systems for Video Tcchnology, Volume 14, Issue 1, Jan. 2004 pages 21-30, incorporated herein by reference.

[00133] While the full 'hard' feature vector is binary, we select the full 'soft' feature vector to be quaternary. Specifically, we select the value of the full 'soft' feature vector of feature *i* to be the best guess of what that feature should be in the 'hard' feature vector, and we further append a bit indicating a reliability level. Specifically, we appended a bit indicating whether we werc confident or not-confident in the decision for that feature.

[00134] For example, some features of the 'hard' feature vector may be difficult to predict, e.g., because thc features are covered by the eyelid or eyelashes, and these features should receive the "not-confident" reliability value.

[00135] Next, we use the biometric training data to generate the error histogram as described above for Figure 8, and then apply the feature vector design method of Figure 9. While the full feature vector has a length of about 10,000, wc discovered that many features 1202 are not reliable. For example, the components of the feature vector corresponding to the top of the eye are often covered by the eyelid or eyelashes. After thc lcast reliable features are discarded by the procedure of Figure 9, we are left with the roughly 2,000 most reliable features in the syndrome feature vector.

[00136] If we stop at stcp 900 in Figure 7, the resulting syndrome vector will not be error resilient to tolerate the natural variation in iris biometric parameters for a single user. Specifically, the syndrome vector encoded from

a measurement of a user's iris taken on one day combined with a measurement from the same iris taken on a different day fails to decode about 12% of the time. This justifies the need for the remaining steps in Figure 7.

[00137] After we measured the first-order correlation using the procedure in Figure 10, we detect that a bit in the 'hard' syndrome feature vector was about twice as likely to take the same value as an adjacent bit as it was to take the opposite value of the adjacent bit. We then continued with step 740 in Figure 7 to construct optimized syndrome codes using density evolution to exploit the high correlation. Finally, we followed step 1100 to construct a belief propagation decoder to take into account the high first-order correlation.

[00138] Following these steps yields syndrome codes that were more than an order of magnitude more reliable than our initial codes, thus demonstrating the advantage of following the entire procedure in Figure 7.

[00139] Syndrome Code for Fingerprint Features

[00140] We apply the procedure 1300 to fingerprints. Fingerprint based systems are generally either *pattern*-based or *minutiae*-based. We use the later. We extract a feature vector from fingerprint minutiae. While the general procedure 1300 can be applied to most biometric data, we describe the details of the procedure for minutiae of a fingerprint. As a characteristic, fingerprint minutiae can vary over time, and the measuring process is subject to structured noise.

[00141] Figure 14 shows an cxample fingerprint 1401 and extracted feature vector 1402. The extracted feature vector 1402 is an example of a syndrome feature vector 1203. The features are only measured in a measurement field (observation window) 1403. For convenience, the minutiae are indicated by the squares in a grid. Each minutia is mapped to a triplet, e.g., (a, b, c) representing spatial position coordinates (a, b) and an angle (c) of the minutia. As describe below, one minutia can be designated as the "core" for the purpose of alignment.

[00142] Because a plane in which the fingerprint 1401 is measured is quantized by a digital sensor with an array of pixels, we store the feature as a matrix. Each sensor pixel corresponds to a particular entry in the matrix 1402. The presencc of a minutia is indicated by a '1', while the lack of a sensed minutia is represented by a '0' in the matrix 1402. In a more general representation, instead of a '1' to signify the presence of a minutia, the entries in the matrix would be thc anglc c of the minutia.

[00143] The number, position and angle of thc minutiae change from one mcasurcment of a fingerprint to the next. For example, if a minutia at (74, 52, 36°) is present in one measurement, it may appear as (80, 45, 63°) in another measurement, or not at all.

[00144] For a variety of reasons, this variability of the minutiae from one measurement to the next causes problems for many convcntional methods for processing fingcrprints.

[00145]　　Explicit Biometric Data Variability

[00146]　　As shown in Figures 15A-15C, our model can deal with the variability in biometric data. In these Figures, the dashed lines 1500 indicate a local neighborhood. Figure 15A shows movement ($p_{i,j}$) 1501 of a minutia. Figure 15B shows deletion p_e 1502, and Figure 15C shows insertion p_s.

[00147]　　Figures 16A and 16B show respectively high-level and low-level details of a factor graph 1600 used to implement belief propagation decoding 1107 according to an embodiment of our invention.

[00148]　　At a high level, the biometric data 1201 is used to generate the syndrome feature vector 1203 which is used to produce the syndrome vector 1204. The syndrome feature vector 1203 not known by the decoder, but the syndrome vector 1204 is. The syndrome vector 1204 and syndrome feature vector 1203 are related by a code structure 1623. The decoder also obtains a noisy measurement of biometric data 1104. The noise structure is described by a statistical model 1305. Together the syndrome vector 1203, the code structure 1623, the observation 1104, and the measurement model 1305, are used to decode 1107 and produce an estimate 1108 of the original syndrome feature vector 1203.

[00149]　　Figure 16B show the low-level structure of the factor graph 1600 that describe the statistical model of the syndrome feature vector, the syndrome vector, and the noisy observations.

[00150]　Each position t in the feature vector grid 1402 has a corresponding binary random variable $x[t]$ node 1609 in the factor graph 1600. This random variable is one minutia is present at position t during enrollment and zero otherwise.

[00151]　The association of grid positions and labels t of the feature vector can be arbitrary, e.g., in a raster-scan order. The two-dimensional nature of the feature set is taken into account in our model.

[00152]　For each grid position, there is a prior probability that a minutia is present during enrollment. This prior probability, $\Pr[x[t] = 1]$, is denoted by factor node 1608.

[00153]　For each position of the variable nodes 1609 for the enrollment grid there is a corresponding position node 1601 for the corresponding authentication grid. The presence of a minutia at grid position t during authentication is represented by a binary random variable $y[t]$. This variable equals one if a minutia is present in the probe, and zero otherwise. The goal of the factor graph is to represent the joint distribution of a first measurement of the fingerprint during enrollment and a second measurement during authentication.

[00154]　In our model, each enrollment position, where $x[t] = 1$, has a probability that the minutia at position t moves to position in a neighborhood of position t in the probe, or is not measured, in the case of a deletion.

[00155] The variables 1604 represent the relative change in position of an enrollment minutia, while the factor nodes 1603 represent the prior probability distribution on the movement and the probability of inserted minutiae. In particular, for the one-dimensional movement model shown in Figure 16B, $z[t] = i$ indicates that a minutia at position $\underline{x}[t + i]$ during enrollment moved to position $z[t]$ during authentication. More generally, and in our implementation, we use a two-dimensional movement model.

[00156] A domain or neighborhood of such shifts $\{i\}$ is a design parameters indicated by the dashed lines 1500. If the variable $z[t] = s$, then a spurious minutia is inserted during authentication at position t, and $z[t] = *$ indicates there is no minutiae at position t during authentication. There is an exact correspondence between the variables $z[t]$, such that $z[t] = *$, and those $y[t]$ such that $y[t] = 0$.

[00157] To represent the constraint that an enrollment minutiae at position t, i.e., $x[t] = 1$, can explain at most one observed minutia in the neighborhood of t, we include the factor nodes 1607. The random variable $h[t]$ 1606 connected to these nodes are binary variables representing deletions of $x[t]$. Deletions can result from non-sensed or non-extracted minutiae, or a false minutiae sensed during enrollment, or from large movement. The nodes 1605 represent the prior distribution for each $h[t]$.

[00158] The factor nodes 1602 connecting each node $y[t]$ to its corresponding node $z[t]$ express the notion that each authentication minutiae $y[t]$ should only be non-zero if the corresponding node $z[t]$ is not *.

[00159] To this model, we add the constraints resulting from the syndrome code 1102. Each syndrome node $s[j]$ 1611 satisfies a local code constraint 1610, which is an indicator function equal to one if the value of the syndrome is compatible with the feature vector $x[1]$, $x[2]$, ..., and zero otherwise.

[00160] The orientations of the minutiae can be added to the factor graph. To add the orientation information, the enrollment nodes 1609 indicate both the position t and the orientation of the minutia. This information is also reflected in the prior probability node 1608. We quantize the orientation during enrollment to make the orientation compatible with the hard feature vector necessary for syndrome encoding.

[00161] The vector of syndrome bits 1611 are encoded as before, but now from the vector of enrollment variables1609 indicating the presence or absence of a minutiae, and its orientation, if present. The prior probabilities of deletions 1605 remain unchanged, as do the constraints 1607 on movement. The prior probabilities on movement and insertions 1604 remain unchanged. The constraint nodes on the authentication nodes 1602 are changed to reflect the notion that smaller changes in orientation between enrollment nodes 1609 and authentication nodes 1601 are likely.

[00162] Message Passing Rules and Optimizations

[00163] Given the measurement and movement model as represented by the factor graph 1600, message passing rules can be derived using

conventional techniques. In the following, we describe several simplifications of message passing to achieve a reduced complexity.

[00164] A first simplification relates to messages from the constraint nodes 1602. We “prune” the factor graph to remove unobserved minutiae. Specifically, according to the form of the constraint 1602, if $y[t] = 0$, then the only non-zero message from node 1602 to the $z[t]$ variable node 1604 is for the state $z[t] = *$.

[00165] Consequently, the only non-zero message $z[t]$ that is sent to the neighboring nodes 1607 is for the * state. We can assume this constant message is normalized to one. For example, if $y[t] = y[t + 2] = y[t + 4] = y[t + 5] = *$, then instead of using the full factor graph of Figure 16B, we instead use a pruned graph 1700 as shown in Figure 17 to derive the necessary message passing operations. This leads to a large reduction in the complexity of calculating messages for the nodes 1607.

[00166] We obtain a second simplification by computing messages going into or out of the factor nodes 1607. We do not need to use the full messages from the $z[t]$ variable nodes. Instead, we can reduce these messages to binary messages indicating whether the minutia at $x[t']$ moves to a position corresponding to position $z[t]$. By using binary information for the node $z[t]$, we obtain significant computational savings.

[00167] We obtain a third simplification for various rules by first computing a set of intermediate quantities and reusing these intermediate quantities later. For example, the outgoing message from a variable node $z[t]$

is the product of incoming messages from all other nodes. If there are K connections to a variable node $z[t]$, the straightforward implementation of this rule requires computation proportional to K^2, because for each connecting edge, one should combine messages from the other K-1 connections. To do this more efficiently, we combine all the messages coming into the node $z[t]$ once, in the process computing the marginal belief for the node $z[t]$. Then, to obtain the outgoing message for a particular connection, we divide or subtract in the log-likelihood domain, the total message by the incoming message from that connection.

[00168] A similar re-use of intermediate quantities can also be applied in computing the outgoing messages from the triangle nodes. In particular, let $z'[t]$ represent the binary message from variable node $z[t]$ to node 1607 at position t'. The quantity $z'[t]$ indicates whether the minutia moves from position t' to position t during authentication. The straightforward sum-product rule for the nodes 1607 on these binary messages requires summing over all possible combinations of the variable nodes 1604 connected to the node 1607 at position t'. For example, if node 1607 at position t' is connected to nodes $z[1]$, $z[2]$ $z[3]$, and $z[4]$, then computing the message to $z'[1]$, requires summing over all possible combinations of $z'[2]$, $z'[3]$, and $z'[4]$. This method has a computational complexity that is exponential in the number of variable nodes connected to each triangle node.

[00169] We can eliminate this exponential complexity by realizing that the constraint node 1607 allows at most one of the z'[t] nodes to be non-zero. Thus, each outgoing message for node $z'[t]$ contains a term corresponding to all the other nodes $z'[t]$ being zero, as well as a term corresponding to all the

other nodes $z'[t]$, except one node being zero. By pre-computing these terms, the message passing rules for the factor nodes 1607 can be reduced from exponential complexity in the number of connections to a linear complexity in the number of connections.

[00170] Gathering Statistics of Biometric Parameters

[00171] Figure 18 shows a process 1800 for setting the parameters 1303 of the factor graph 1600, i.e., the model according to the invention. Biometric training data 1301 are acquired. An unprocessed fingerprint F is selected 1802. An unprocessed pair of measurements B and B' of the fingerprint F are selected 1803. We determine 1804 their respective minutiae M(B) and M(B'). We compare 1805 the minutiae 1806, and determine 1806 statistics of movements, rotations, insertions and deletions. The statistics are used to revise 1807 the statistics in the factor graph. If there is a pair of measurements of the fingerprint F not yet processed 1808, we return to step 1803. Else, if there is a fingerprint not yet processed 1809, we return to step 1802. After all the fingerprints and their minutiae pairs are processed, the statistics gathering is complete in step1810.

[00172] Data Alignment

[00173] In biometric systems, the enrollment biometric data are often misaligned with the authentication data. Different measurements of the same biometric data often vary by global transformations such as translation, rotation, and scaling. Such variations pose less of a problem for pattern-

based biometric authentication, or authentication schemes which do not use syndrome coding.

[00174] In contrast, in our system, only the syndrome vector 331 of the enrollment biometric parameters are available for comparison. Therefore, a search over different alignments entails a decoding for each possible alignment. The minutiae movement model can accommodate fine-scale mis-alignment, but to minimize the computational expense of decoding, we want to minimize the search space.

[00175] Figure 19 shows the steps of an alignment process for fingerprints during enrollment or authentication according to an embodiment of our invention. A fingerprint is acquired 1901, and minutiae parameters are extracted 1902 as well as the core point location and orientation. The core point and its orientation defines an inertial reference frame for the fingerprint, where the position of the core point is an origin and the orientation serves as a *y*-axis. We recalculate 1903 the position and orientation of the minutiae with respect to the inertial reference frame associated with the core point. The result 1904 is a set of minutiae measured in a reference frame for the fingerprint.

[00176] As an advantage, this procedure can remove most or all of the effects of translations and rotations. Typically such pre-processing is combined with a computationally more intensive local search where decoding is performed at a smaller set of translations and rotations. This pre-processing procedure can be used as part of the minutiae extraction routines.

[00177] Post-Alignment Revision of Parameter Settings

[00178] Whenever the enrollment and authentication biometric features are shifted with respect to each other before decoding, the parameters of the factor graph are modified to reflect this shifting. An example of this is when the enrollment and authentication features are shifted with respect to each other, either due to the alignment procedure 1900, or due to a number of small shifts corresponding to a local search.

[00179] Depending on the shift, and the relative sizes of the enrollment and authentication observation windows 1403, see Figure 14, some enrollment feature locations may not be observed at all during authentication. Therefore, we modify the factor graph to reflect this by setting the probability of minutiae erasure to one for these non-observed positions. This is reflected in Figure 16B by setting the erasure probability in factor node 1605 equal to one. For minutiae near the edge of the window 1403, which have some likelihood of being observed, and some of not being observed, the prior probabilities 1605 are modified accordingly.

[00180] Syndrome Pre-Processing

[00181] In the biometric security systems 300 of Figure 3, the biometric parameters 301 are input directly into the syndrome encoder 330 during the enrollment phase. Similarly, in the authentication phase, the biometric parameters 360 are input directly into the syndrome decoder 370.

[00182] Figure 14 shows a representation of minutiae point locations, which are often used as biometric parameters for fingerprints. There are several issues regarding the usage of this representation in the syndrome-based framework for biometric security systems, such as that described for Figures 3, 5 and 6.

[00183] First, that representation is sparse and difficult to model. The models shown in Figure 15 attempt to model the movement, insertion, and deletions intrinsic to minutiae. However, those models are complex.

[00184] Second, that representation is not well suited for conventional syndrome codes. Even if the representation is in the form of binary data, the data is biased and does not have the inherent statistical properties that would yield high performance when conventional channel codes and corresponding decoding methods are applied to the data.

[00185] The performance can be improved by designing new syndrome codes that account for the *biased* nature of the source and the asymmetry of the measurement channel. This is a challenging and complicated process.

[00186] Figure 20 describes a method of syndrome encoding the biometric parameters according to an embodiment of this invention. First biometric parameters 2010 are acquired from a user, e.g., during the enrollment phase 10, see Figure 1. The first biometric parameters 2010 are syndrome pre-processed 2020 to produce a binary representation of biometric parameters 2030. The pre-processing 2020 applies a set (one or more) of binary logical conditions 2022 to the acquired biometric parameters

2010. The set of binary logical conditions 2022 compels or attempt to make the binary representation 2030 have a set (one or more) of desired predetermined statistical properties 2025. The set of predetermined statistical properties 2025 are described further below. The binary representation of the biometric parameters 2030 are syndrome encoded 2040 to produce a first syndrome 2050. It should be noted the logical conditions can try to achieve the target statistical properties. It should also be noted that the statistical properties can be adjusted dynamically during the processing.

[00187] The first syndrome can then be further processed by applying a hash function to produce an enrollment hash, which can be stored along with the syndrome vector, for later use in authenticating the user

[00188] We explicitly design our encoder 2040 to be compatible with the binary representation 2030 and the desired statistical properties 2025. We believe that matching the encoding to the binary representation and the desired statistical properties improves the performance and reliability of our system.

[00189] Figure 21 shows further details of the method of syndrome decoding according to an embodiment of this invention. The biometric parameters are reacquired, e.g., during the authentication phase 20. The second biometric parameters 2110 are subject to the syndrome pre-processing 2020 to produce a binary representation of biometric parameters 2130. As before, the binary representation 2130 has the same set of desired predetermined statistical properties 2025 as imposed during the enrollment. The pre-processed binary representation 2130 is then used as input to the

syndrome decoding 2140 to produce reconstructed biometric parameters 2145. As before the decoder is compatible with the binary representation having the desired statistical properties. Making the encoding and the decoding compatible with the binary representation and the desired statistical properties improves the performance and reliability of our system.

[00190] If the first and second biometric parameters are from the same person, then the reconstructed biometric parameters should be identical to the first biometric parameters, even if the biometric parameters from the first and second parameters are different in detail.

[00191] The syndrome pre-processing as described herein can be applied to the methods shown in Figure 3, 5, and 6.

[00192] Desired Target Statistical Properties

[00193] The syndrome pre-processing 2020 is used to transform the biometric parameters into the binary representation, or binary string, with the desired statistical properties 2025. Because the properties may not always be attainable, they can be considered target properties.

[00194] The statistical properties ensure syndrome codes can achieve optimal performance. With our pre-processing 2020, the complexities involved in modeling complex relations between biometric parameters is greatly reduced.

[00195] One desirable set of statistical properties 2025 of the binary representation 2030/2130 are summarized as follows:

each bit in the binary representation has an equal probability of being either a zero or a one;

different bits in the same binary representation are independent of each other;

binary representations from different users are independent of each other; and

binary representations for different readings of same user are statistically dependent of each other.

[00196] The approach embodied in these embodiments of the invention can be contrasted with the embodiments of Figure 13. In the embodiment shown in Figure 13, a feature model 1304 and measurement model 1305 model the underlying structure of the biometric data in the training set and how biometric data vary among multiple readings for a single user and across users. Nothing is done to match the encoding and decoding to the models.

[00197] In contrast, the syndrome pre-processing approach as shown in Figure 20 does not use the feature set directly acquired from the biometric data as in Figure 13. Instead, the feature sets in Figures 20-21, i.e., the binary representations, are engineered to be compatible with the syndrome encoding and decoding procedure.

[00198] We explicitly design the feature set to be compatible with code designs, syndrome encoding and syndrome decoding procedures that already

exist. For a particular set of features with the predetermined statistical properties as described herein, we can utilize a channel code for a binary-symmetric channel that matches thc designed feature set. The construction of such channcl codes and their associated syndrome-encoding and decoding procedures are well-understood and deeply explored topics.

[00199] Figures 22A-22C show a set of statistical properties corresponding to a set of binary presentations of bit strings with 200 bits each.

[00200] Figure 22A shows a histogram of thc average number of ones in the set of binary strings. An ideal distribution is centered around 100, which implies that half the bits are one.

[00201] Figure 22B shows the pair-wise entropy of the bits in each string. Ideally, if each pair of bits is independent, then the entropy is two for all pairs. However, if there is some dependence among bits, then entropy values less than two occur. In the worst case, if a particular bit in the process biometric parameter can always be predicted from another bit, and that othcr bit is equally-likely zero or one, then the pair-wise cntropy is 1.

[00202] Figure 22C shows intra-user variations 2210 and inter-user variations 2220. The intra-user variation 2210 indicates a normalized Hamming distance between bit strings corresponding to multiple samples of the same user. The inter-user variation 2220 indicates that thc normalized Hamming distance between bit strings corresponding to samples of different users. Ideally, the intra-user and inter-user variation should not overlap and

each should be distributed over a narrow range. Furthermore, the intra-user variation 2210 should be as low as possible, e.g., a distribution around 0.1, as shown, indicates that each bit of the same user has a 10% probability of error. On the other hand, the distribution for the inter-user variation should be centered around 0.5, which indicates that bit strings from different users are independent of each other.

[00203] Syndrome Pre-Processing Implementations

[00204] Figure 23 shows our syndrome pre-processing method. The syndrome pre-processing applies a set (one or more) of binary logical conditions, i.e., conditions with a yes/no answer, about the biometric parameters to yield the binary representation, i.e., a binary string "00111000101110001….."

[00205] In our method as shown in Figure 24, the set of binary logical conditions 2022 are applied to the biometric parameters. If the output of the application is non-binary 2430, then the output is binarized 2420 to yield the required binary representation.

[00206] For example, the biometric parameters are locations of minutiae points for a fingerprint. One binary condition determines whether the number of minutiae in a given two-dimensional (2D) region is greater than a threshold *M*.

[00207] Binary Logical Conditions

[00208] Several types of binary logical conditions can be applied to the biometric parameters, as shown in Figures 25A-25C. The dots in Figures 25A-25C represent coordinates (sample locations) of fingerprint minutiae. Either (x-location, y-location) coordinates in Figures 25A and 25B or (x-location, y-location, orientation) coordinates (z) in Figure 25C.

[00209] In Figure 25A, each condition is based on a line 2501 drawn through the samples. The binary logical condition is $y-mx-n = 0$. The lines can have random slopes and y-intercept values. In one embodiment of the invention, a difference between the number of minutiae points above the line, i.e., located in the region satisfying the condition $y-mx-n > 0$, and the number of minutiae points below the line, i.e., located in the region satisfying the condition $y-mx-n < 0$, is obtained. This yields a vector of values in the range $[-\underline{M}, M]$, where M is the maximum number of minutiae points in a fingerprint. The vector can be binarized if needed.

[00210] In Figure 25B, the condition is a set of rectangles 2502. Each rectangle is generated at an origin point that indicates the upper-left corner of the rectangle, as well as a width and height. A set of rectangles can be generated with random values of these points, or through a pre-determined arrangement. In one embodiment of the invention, the condition is the number of minutiae points within a given rectangle.

[00211] In one embodiment of the invention, the condition is the number of minutiae points within a given rectangle greater than a specified threshold, where the threshold may vary for each rectangle based on its position and area, and/or global statistics of user data samples.

[00212] In another embodiment of the invention, the condition is a difference between the number of minutiae in one rectangle and the number of minutiae in a second rectangle.

[00213] In order to include additional data about fingerprints, such as the minutiae orientation, the rectangle condition can be extended to cubes 2503, where the first two dimensions account for minutiae point locations as before, and the third dimension (z) accounts for minutiae orientation. In Figure 25C, the condition includes a set of cubes. Each cube is generated at an origin point that indicates the upper-left corner of the cube, as well as a width, height and depth. A set of cubes can be generated with random values of these points, or through a pre-determined arrangement. In one embodiment of the invention, the condition is the number of minutiae points within a given cube. In another embodiment of the invention, the condition is the number of minutiae points within a given cube greater than a specified threshold, where the threshold can vary for each cube based on its position and volume, and/or global statistics of user data samples. In yet another embodiment of the invention, the condition is a difference between the number of minutiae in one cube and the number of minutiae in a second cube.

[00214] The invention is not limited to the particular logical conditions described herein. Various other conditions base on circles, spheres and polygons can also be used, depending on the characteristics of the biometric.

[00215] In addition, these methods are not limited to the transformation and binarization of minutiae-based feature sets. The objective is to apply binary logical conditions to biometric data to produce a binary representation with statistics compatible with syndrome encoding and decoding. For example, the invention can be applied to pattern-based data, or frequency-domain data, among other types of fingerprint data.

[00216] Generally speaking, an overlap between the conditions affects the correlations in the resulting binary representation. The conditions can be designed to account for this affect. For example, restrictions could be placed on the amount of allowable overlap between two rectangles. In addition, the syndrome encoding and decoding procedures can be designed to account for such correlations. However, the purpose of the invention is to minimize the need for such adjustments to off-the-shelf code designs or encoding and decoding procedures.

[00217] Binarizations

[00218] Figure 26 shows several types of binarizations. In Figure 26A, a threshold 2601 is applied to all values of a vector 2602 to yield a binary vector 2603. The threshold may be the same for all bit positions or vary for each.

[00219] In Figure 26B, a random projection 2604 onto an orthonormal basis is first applied to the non-binary vector 2602, where this random projection is the same for all users. The results of this projection are then subject to the thresholding process to yield the binary vector 2603. Instead of

a random projection, other linear or non-linear transformations can be used to improve the separation of samples acquired from genuine users and impostors, e.g., principal component analysis, and linear discriminant analysis.

[00220] In Figure 26C, the non-binary vector 2602 is first normalized 2605, then a set of random projections (RP) 2604 are applied for each user, followed by the thresholding 2601 for each random projection, which may be the same for each projection or vary among the projections. This is then followed by a concatenation 2607 to yield the binary vector 2603.

[00221] Statistical Analysis

[00222] As part of the design of the syndrome pre-processing, a statistical analysis can be performed on the binary representation to ensure and confirm that the desired target statistical properties are achieved. In this way, the statistical analysis is performed on the final result of the syndrome pre-processing and does not incur any feedback to the operation of the syndrome pre-processing.

[00223] Alternatively, a statistical analysis can also be performed on intermediate binary strings during the syndrome pre-processing to guide operation of the syndrome pre-processing. In this way, explicit feedback of the statistical properties is provided during the syndrome pre-processing.

[00224] Security Considerations for Syndrome Pre-processing

[00225] The number of bits in the binary representation and the correlation between different samples of the same user determine the level security. For example, if we have 400 bits in the binary string, and the correlations are strong enough so that we only need a syndrome of 300 bits to successfully decode a user, then we have 100 bits of security.

[00226] Security is obtained from the syndrome encoding phase. In fact, as a result of the syndrome pre-processing, binary strings with predetermined statistical correlations are produced. In this case, estimates of the security provided by the system can be considered more accurate compared to the case in which the syndrome encoding and decoding are performed using binary strings with correlations that are difficult to model.

[00227] Effect of the Invention

[00228] The invention achieves secure user authentication based on biometric parameters. The invention is secure because syndrome vectors are stored instead of the original biometric data or any feature vectors. This prevents an adversary who gains access to the database from learning the underlying biometric data.

[00229] It is possible to bound a best possible estimate of an original biometric parameters *E*, which an adversary can make using only the syndrome vector *S*, using conventional tools from the well known problem of multiple descriptions, e.g., see V. K. Goyal, "Multiple description coding: compression meets the network," IEEE Signal Processing Magazine, Volume: 18, pages 74 – 93, September 2001. Furthermore, it is

possible to develop these bounds whether a quality of the estimate is measured via absolute error, squared error, weighted error measures, or any arbitrary error function. In contrast, all prior art methods are based on binary values. There, security depends on the Hamming distance.

[00230] Essentially, the security of the syndrome vector *S* is due to the fact that it is a compressed version of the original biometric parameter *E*. Furthermore, this compressed representation corresponds to the "least significant bits" of *E*. Using well known tools from data compression theory, it is possible to prove that if a syndrome code with a high compression is used, then these least significant bits can at best yield a poor estimate of the original parameters *E*, for example, see Effros "Distortion-rate bounds for fixed- and variable-rate multi-resolution source codes," IEEE Transactions on Information Theory, volume 45, pages1887-1910, September 1999, and Steinberg and Merhav, "On successive refinement for the Wyner-Ziv problem," IEEE Transactions on Information Theory, volume 50, pages 1636-1654, August 2004.

[00231] Second, the invention is secure because forgery is at least as difficult as finding a collision in the underlying hash function 340. In particular, the system only accepts a syndrome pair (S, H) in the authentication phase 390 if the hash *H*' of the decoded biometric *E*'' matches the original hash *H*. For cryptographic hash functions, such as MD5, finding an element *E*'', which differs from *E*, but has a hash that matches the hash of *E* is generally considered impossible. Thus, if syndrome decoding succeeds in decoding *E*'' with the proper hash, the system can be confident

that E'' is in fact the same as E, and all authentication decisions are made with the original biometric parameters.

[00232] Third, the invention compresses the original biometric parameters E in producing the syndrome vector S. Biometric databases for many users can require large amounts of storage, especially if the biometric data question requires large amounts of data, e.g., face images or speech signals. Therefore decreasing the storage required can yield drastic improvements in both cost and error resiliency. In contrast, most prior art methods for the secure storage of biometric data actually increase size of the stored data due to the overhead of encryption or error correction, and therefore require more storage than insecure systems.

[00233] Fourth, the invention can apply sophisticated code construction and decoding algorithms because the invention is built on the theory of syndrome codes. In particular, the syndrome coding according to the invention facilitates the use of soft decoding using the well known Viterbi algorithm, belief propagation, and turbo decoding for both binary and multilevel code constructions. In contrast, because most prior art methods are based on binary codes, Reed-Solomon codes, and algebraic decoding, soft decoding cannot be applied effectively when the biometric data take on real values, as opposed to binary values. For example, some methods specifically require computing the XOR of the biometric data with a random codeword in the enrollment phase to produce the reference and requires computing the XOR of the reference with the biometric data in the authentication phase.

[00234] Fifth, while most prior art on secure biometrics using error correction encoding, the invention uses syndrome encoding. The computational complexity of error correction encoding is usually super linear in the input size. In contrast, by using various types of low density parity checks based syndrome codes, it is easy to construct syndrome encoders where the computational complexity of the syndrome encoding is only linear in the input size.

[00235] Sixth, by using the syndrome coding framework, it is possible to use powerful new embedded syndrome codes as the SCA codes described by Yedidia et al in U.S. Patent Application Sn. 10/928,448, "Compressing Signals Using Serially-Concatenated Accumulate Codes," incorporated herein by reference. These codes allow the syndrome encoder, during enrollment, to estimate an inherent variability of biometric data, and encode just enough syndrome bits to allow successful syndrome decoding.

[00236] Seventh, the syndrome codes as describe above can be used to encrypt data. Furthermore, methods are described to enable the design for an optimal syndrome code with a given level of performance and error resiliency.

[00237] Eighth, the syndrome feature vector can be correctly decoded even if the measurement channel is subject to structured noise.

[00238] Ninth, the encoding and decoding can be designed to be compatible with desired statistical properties, which are imposed by binary logical conditions.

[00239] Although the invention has been described by way of examples of preferred embodiments, it is to be understood that various other adaptations and modifications may be made within the spirit and scope of the invention. Therefore, it is the object of the appended claims to cover all such variations and modifications as come within the true spirit and scope of the invention.

Brief Description of the Drawings

Figure 1 is a block diagram of prior art password based security system;

Figure 2 is a block diagram of prior art biometric based security system;

Figure 3 is a block diagram of a biometric security system according to one embodiment of the invention;

Figure 4 is a block diagram of a prior art security system for protecting data;

Figure 5 is a block diagram of a data security system according to an embodiment of the invention;

Figure 6 is a block diagram of a security system according to an embodiment of the invention;

Figure 7 is a block diagram of a process for constructing a syndrome code according to an embodiment of the invention;

Figure 8 is a block diagram of a process for generating a histogram according to an embodiment of the invention;

Figure 9 is a block diagram of a process for selecting a feature vector according to an embodiment of the invention;

Figure 10 is a block diagram for measuring inter-coefficient correlation according to an embodiment of the invention;

Figure 11A is a block diagram of a biometric encoder for producing a syndrome vector according to an embodiment of the invention during enrollment;

Figure 11B is a block diagram for a complementary decoder for the encoder of Figure 11A to be used during authentication according to an embodiment of the invention;

Figure 11C is a belief propagation factor graph with correlation nodes according to an embodiment of the invention;

Figure 12 is a block diagram indicating dependency relationships between biometric features, full feature vector, syndrome feature vector, and encoded syndrome vector according to an embodiment of the invention;

Figure 13 is a block diagram of a process for constructing a syndrome code according to an embodiment of the invention;

Figure 14 is a block diagram of fingerprint minutiae encoding according to an embodiment of the invention;

Figures 15A-15C are block diagrams of variability in measured biometric data according to an embodiment of the invention;

Figure 16A and Figure 16B are respectively block diagrams of high and low level details of a belief propagation factor graph according to an embodiment of the invention;

Figure 17 is a pruned belief propagation factor graph according to an embodiment of the invention;

Figure 18 is a block diagram of a process for estimating parameters of the movement and measurement model of fingerprint minutiae according to an embodiment of the invention;

Figure 19 is a block diagram for performing alignment of minutiae according to an embodiment of the invention;

Figure 20 is a block diagram of a syndrome encoding process with syndrome pre-processing according to an embodiment of the invention;

Figure 21 is a block diagram of a syndrome decoding process with syndrome prc-processing according to an embodiment of the invention;

Figure 22A-22C are graphs of predetermined statistical properties according to an embodiment of the invention;

Figure 23 is a block diagram of syndrome pre-processing based on binary logical conditions according to an embodiment of the invention;

Figure 24 is a block diagram of syndrome pre-processing based binary logical conditions according to another embodiment of the invention;

Figures 25A-25C are graphs of logical conditions as part of the syndrome pre-processing according to an embodiment of the invention; and

Figures 26A-26C are graphs of binarizations as part of the syndrome pre-processing according to an cmbodiment of the invention.

1. A pre-processing method for biometric parameters before encoding and decoding by implementing computer for securely storing the biometric parameters in a database, in which the biometric parameters are acquired of a user during an enrollment phase, comprising the steps of:

applying a set of binary logical conditions to enrollment biometric parameters of a user to produce a binary representation, in which the binary representation has a set of predetermined statistical properties imposed by the set of binary logical conditions;

encoding the binary representation using a syndrome encoder to produce an enrollment syndrome vector, in which the encoding is compatible with the binary representation and the set of predetermined statistical properties;

applying a hash function to the enrollment biometric vector to produce an enrollment hash; and

storing the enrollment syndrome vector and the enrollment hash in a database; and

authenticating the user using the database.

2. The method of claim 1, in which the authenticating further comprises:

acquiring authentication biometric parameters of the user;

applying the set of binary logical conditions to the authentication biometric paramcters to produce thc binary representation of the authentication biometric parameters, in which the binary representation has the set of predetermined statistical properties imposed by the set of binary logical conditions;

decoding the binary representation of the biometric parameters using a syndrome decoder to produce an authentication syndrome vector, in which the encoding is compatible with the binary representation of the biometric parameters and the set of predetermined statistical properties;

applying a hash function to the authentication biometric vector to produce an authentication hash; and

accessing the database with the authentication syndrome vector and the authentication hash to verify the user.

3. The method of claim 1, in which the set of statistical properties compels each bit in the binary representation to have an equal probability of being either a zero or a one.

4. The method of claim 1, in which the set of statistical properties compels different bits in the binary representation to be independent of each other.

5. The method of claim 1, in which the set of statistical properties compels binary representations from different users to be independent of each other.

6. The method of claim 1, in which the set of statistical properties compels binary representations of same user be statistically dependent on each other.

7. The method of claim 1, in which the biometric parameters are locations of minutiae points for a fingerprint.

8. The method of claim 7, in which thc set of binary logical conditions includes a condition that dctermines whether a number of the minutiae points in a given two-dimensional region is greater than a threshold *M*.

9. The method of claim 7, in which the set of binary logical conditions includes a condition that is based on a difference between a number of minutiae points above a line and below the linc.

10. Thc method of claim 7, in which the set of binary logical conditions is based on a difference between a number of minutiae points within a first rectanglc and the number of minutiae in a second rectangle.

11. The method of claim 1, in which the biometric parameters are locations and orientations of minutiae points for a fingerprint.

12. The method of claim 11, in which the sct of binary logical conditions includcs a condition that determines whether a number of the minutiae points in a given three -dimensional region is greater than a threshold *M*.

13. The mcthod of claim 1, in which the predetermined statistical properties are compatible with pattern-based data.

14. The method of claim 1, in which the predetermined statistical properties are compatible with frequency-domain data.

15. The method of claim 1, in which the application of the logical binary condition produces an intermediate value, and further comprising:

binarizing the intermediate value.

16. The method of claim 15, in which the binarizing further comprises:
thresholding the intermediate value.

17. The method of claim 16, in which the binarizing further comprises:
applying a transformation to the intermediate value before the thresholding.

18. The method of claim 17, in which the binarizing further comprises:
normalizing the intermediate value.

19. The method of claim 17, in which the transformation is a random projection.

20. The method of claim 17, in which the transformation is a principal component analysis.

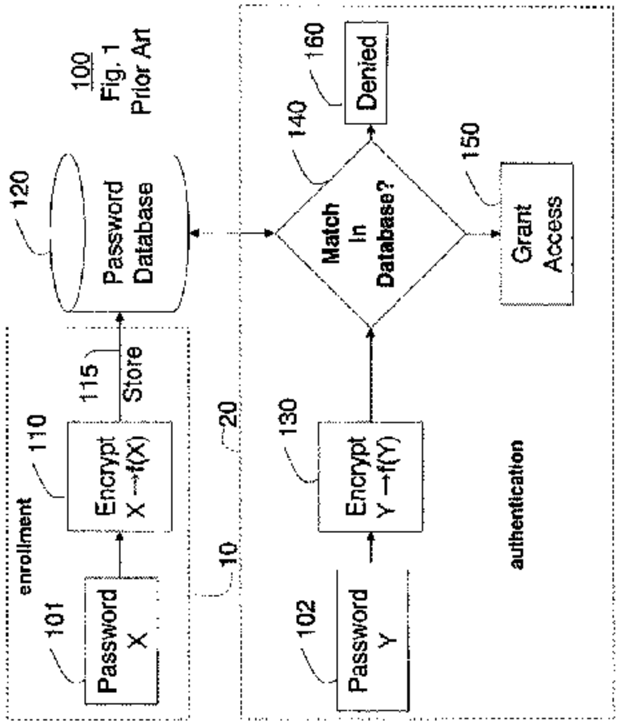
21. The method of claim 1, further comprising:
analyzing the binary representation to ensure and confirm that the set of statistical properties are imposed .

Abstract of the Disclosure

The method in which biometric parameters acquired from human faces, voices, fingerprints, and irises are used for user authentication and access control. Because the biometric parameters are continuous and vary from one reading to the next, syndrome codes are applied to determine biometric syndrome vectors. The biometric syndrome vectors can be stored securely, while tolerating an inherent variability of biometric data. The stored biometric syndrome vector is decoded during user authentication using biometric parameters acquired at that time. The syndrome codes can also be used to encrypt and decrypt data. The biometric parameters can be pre-processed to form a binary representation, in which the binary representation has a set of predetermined statistical properties enforcedimposed by a set of binary logical conditions.

Representative Drawings

Figure 3



100
Fig. 1
Prior Art

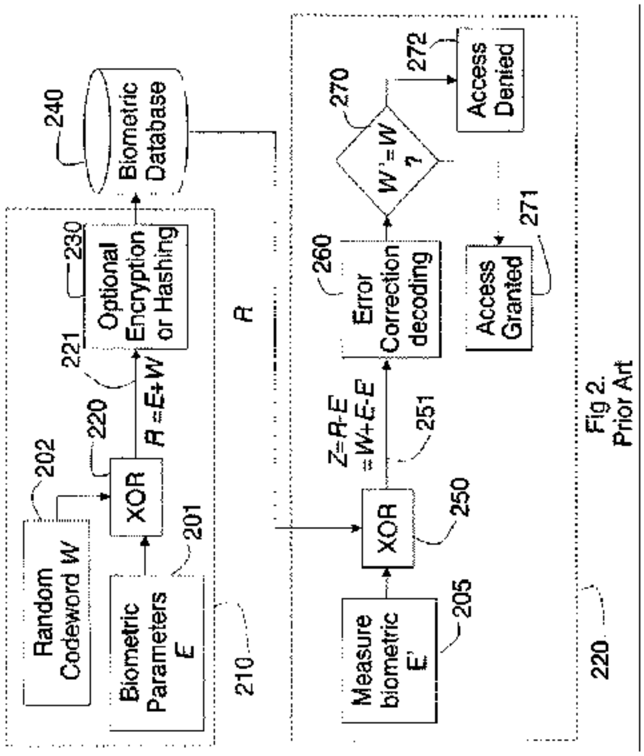
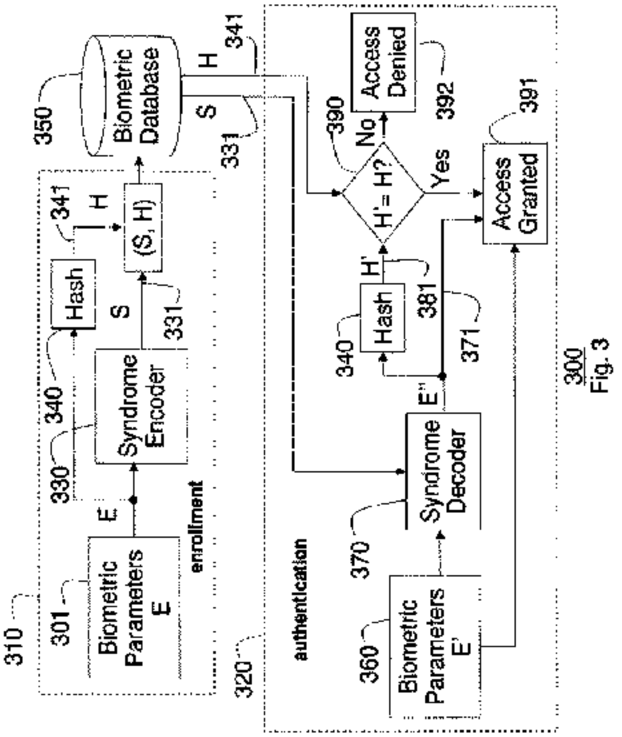
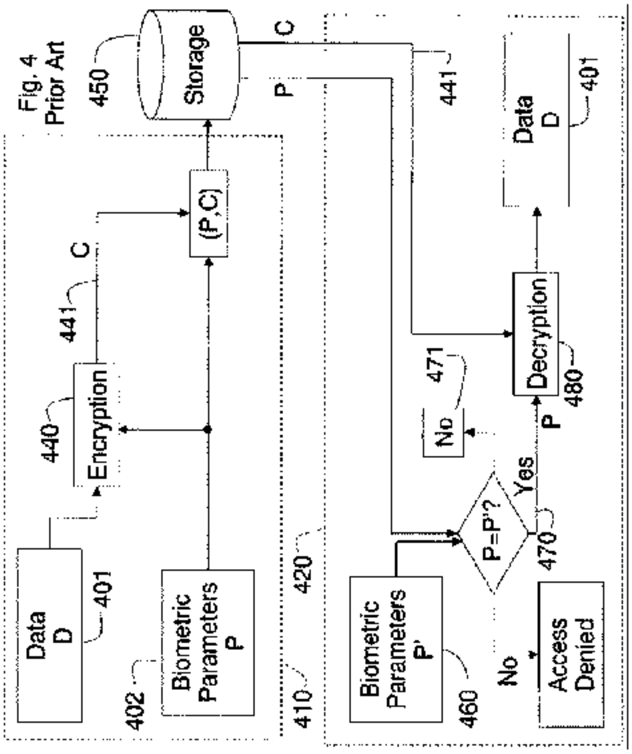


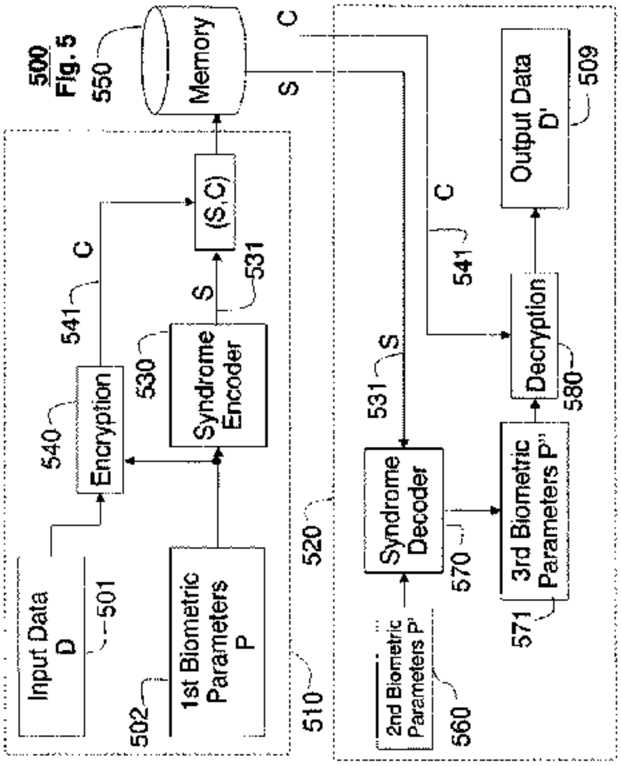
Fig 2.
Prior Art



300
Fig. 3

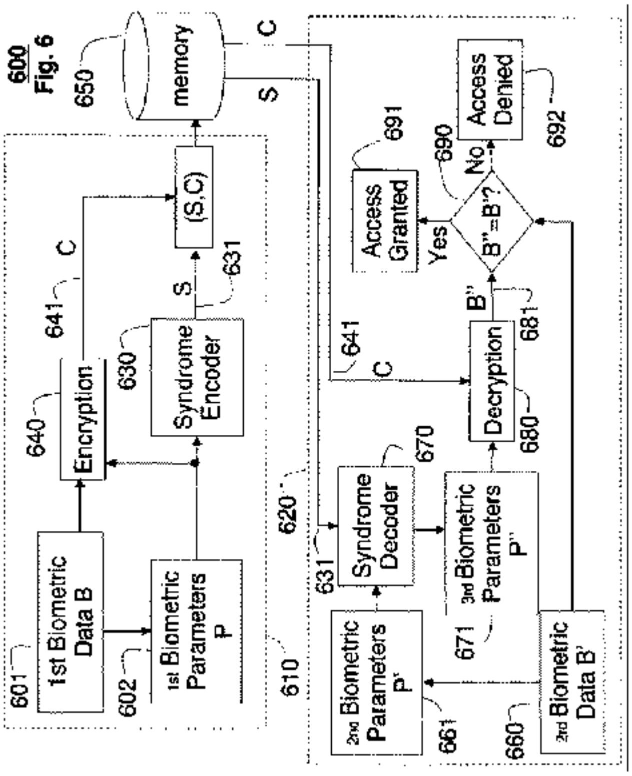
Fig. 4
Prior Art

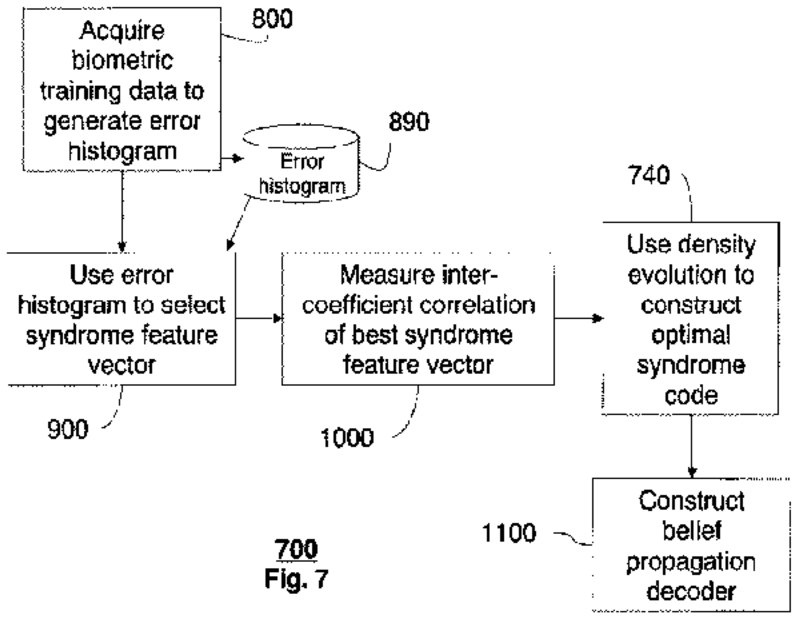




500
Fig. 5

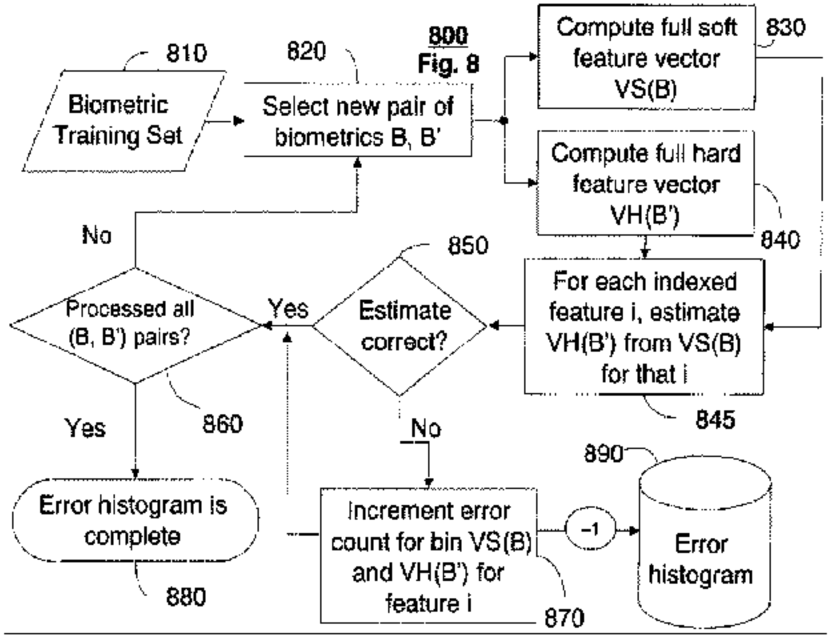
550
Memory
S
C
510
Input Data
D
501
502
1st Biometric
Parameters
P
540
Encryption
541
C
530
Syndrome
Encoder
S
531
(S,C)
520
2nd Biometric
Parameters P'
560
Syndrome
Decoder
570
531
S
3rd Biometric
Parameters P''
571
Decryption
580
541
C
Output Data
D'
509

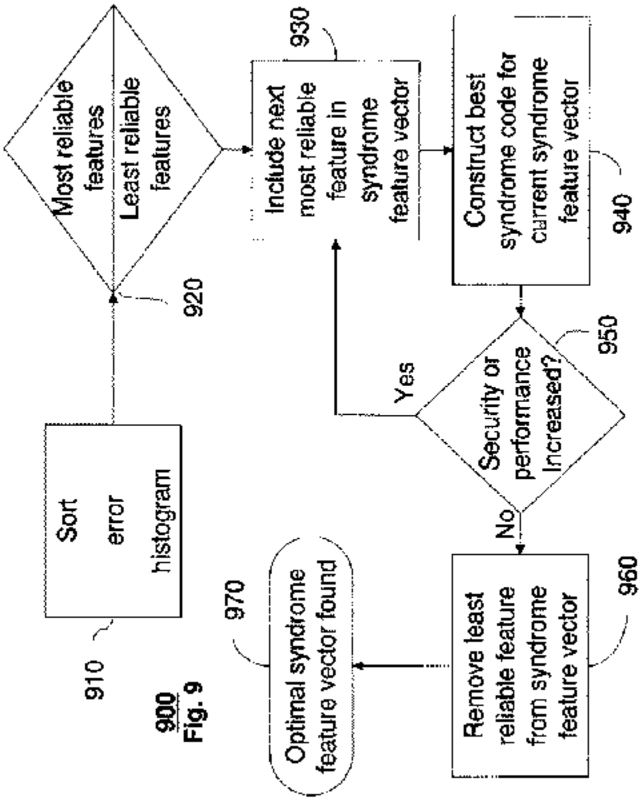

600
Fig. 6
650
memory
C
S
601
1st Biometric Data B
602
1st Biometric Parameters P
610
640
Encryption
641
C
630
Syndrome Encoder
S
631
(S,C)
620
631
Syndrome Decoder
670
3rd Biometric Parameters P''
671
2nd Biometric Parameters P'
661
660
2nd Biometric Data B'
641
C
Decryption
680
681
B''
B''=B'?
690
Yes
No
Access Granted
691
Access Denied
692


Acquire biometric training data to generate error histogram
800
Error histogram
890
Use error histogram to select syndrome feature vector
900
Measure inter-coefficient correlation of best syndrome feature vector
1000
740
Use density evolution to construct optimal syndrome code
Construct belief propagation decoder
1100

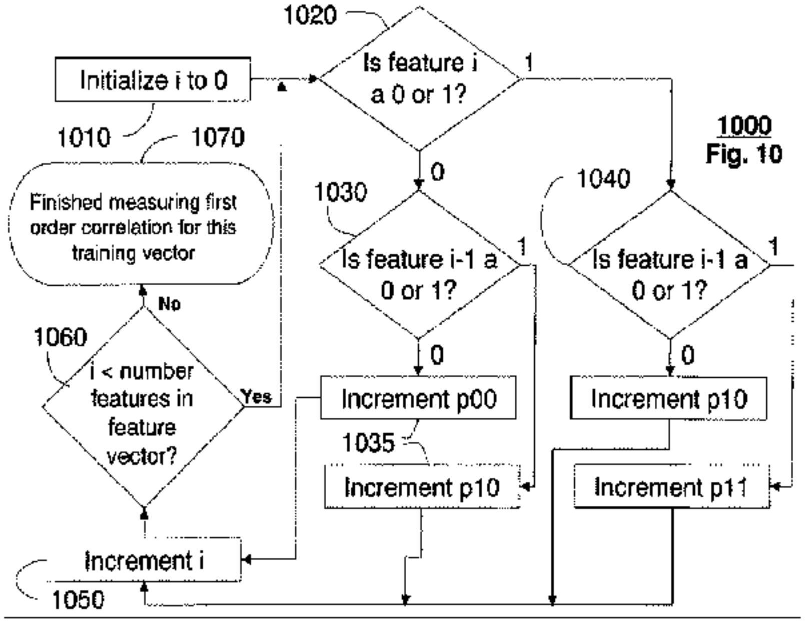
700
Fig. 7

800
Fig. 8


810
Biometric Training Set
820
Select new pair of biometrics B, B'
830
Compute full soft feature vector VS(B)
840
Compute full hard feature vector VH(B')
845
For each indexed feature i, estimate VH(B') from VS(B) for that i
850
Estimate correct?
Yes
No
860
Processed all (B, B') pairs?
No
Yes
870
Increment error count for bin VS(B) and VH(B') for feature i
-1
890
Error histogram
880
Error histogram is complete


910
Sort error histogram
920
Most reliable features
Least reliable features
930
Include next most reliable feature in syndrome feature vector
940
Construct best syndrome code for current syndrome feature vector
950
Security or performance Increased?
Yes
No
960
Remove least reliable feature from syndrome feature vector
970
Optimal syndrome feature vector found

900
Fig. 9


1020
Is feature i a 0 or 1?
1
0
Initialize i to 0
1010
1070
Finished measuring first order correlation for this training vector
1030
Is feature i-1 a 0 or 1?
1
0
Increment p00
1035
Increment p10
1040
Is feature i-1 a 0 or 1?
1
0
Increment p10
Increment p11
1060
i < number features in feature vector?
No
Yes
Increment i
1050

1000
Fig. 10

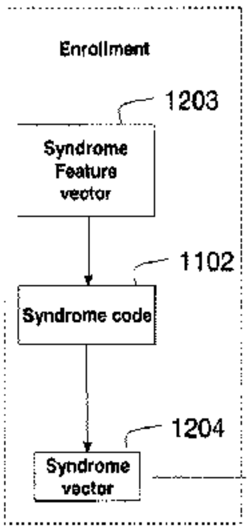


Fig. 11A

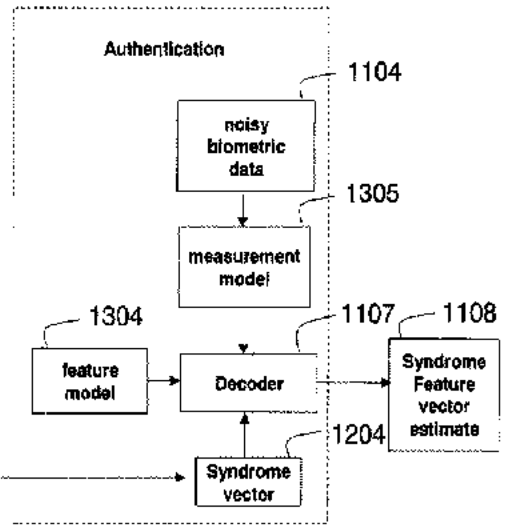
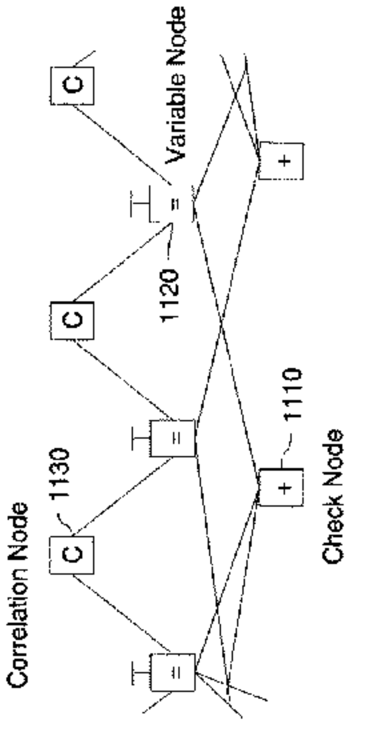


Fig. 11B


Correlation Node
1130
C
C
C
=
=
=
1120
Variable Node
+
+
1110
Check Node

1100
Fig. 11C

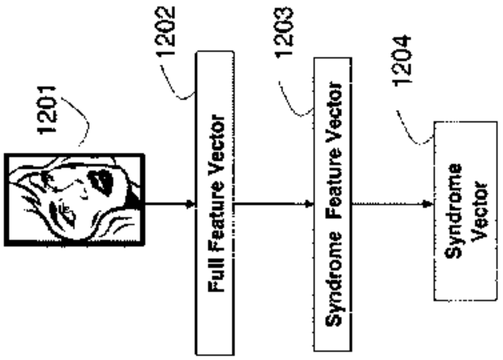

1201
1202
Full Feature Vector
1203
Syndrome Feature Vector
1204
Syndrome Vector

Fig. 12

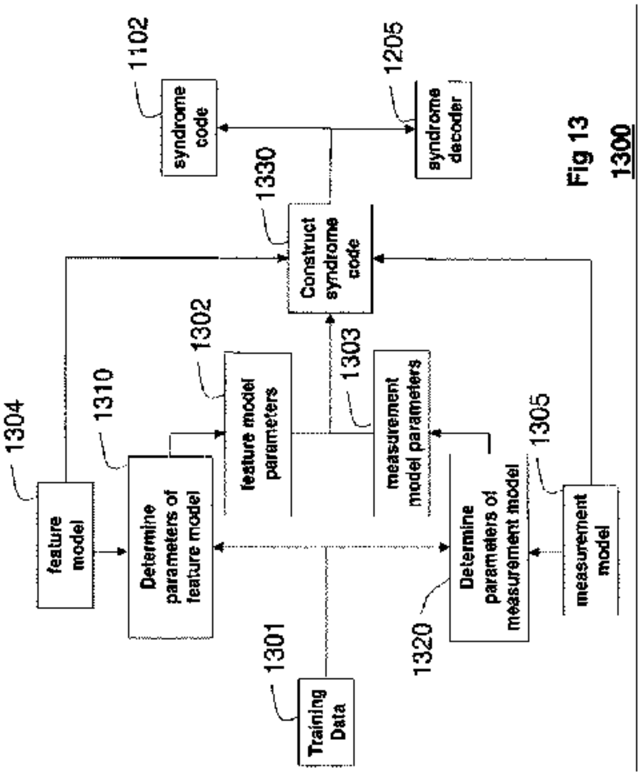
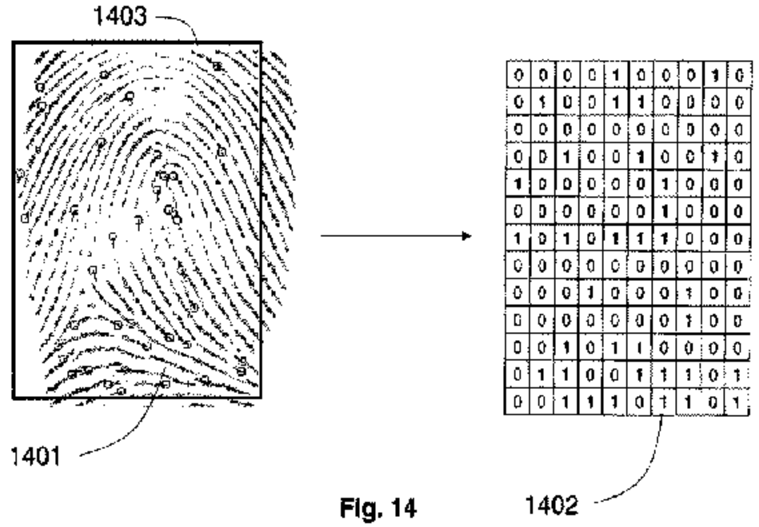

Training Data
1301
feature model
1304
Determine parameters of feature model
1310
feature model parameters
1302
measurement model parameters
1303
Determine parameters of measurement model
1320
measurement model
1305
Construct syndrome code
1330
syndrome code
1102
syndrome decoder
1205

Fig 13

1300



0	0	0	0	1	0	0	0	1	0
0	1	0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	1	0	0	1	0	0	1	0
1	0	0	0	0	0	1	0	0	0
0	0	0	0	0	0	1	0	0	0
1	0	1	0	1	1	1	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1	0	0
0	0	0	0	0	0	0	1	0	0
0	0	1	0	1	1	0	0	0	0
0	1	1	0	0	1	1	1	0	1
0	0	1	1	1	0	1	1	0	1

Fig. 14

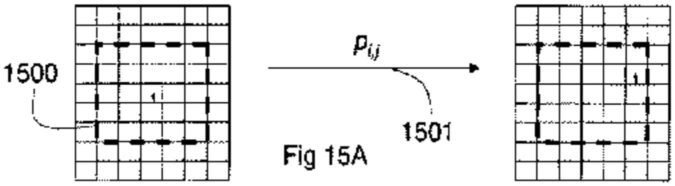


Fig 15A

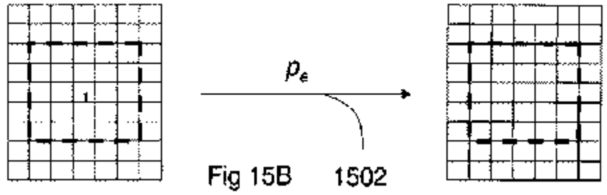


Fig 15B

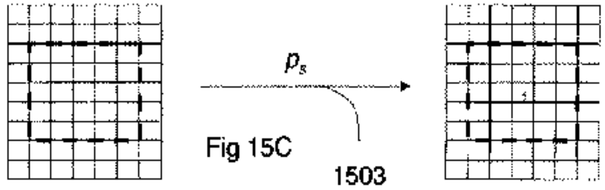


Fig 15C

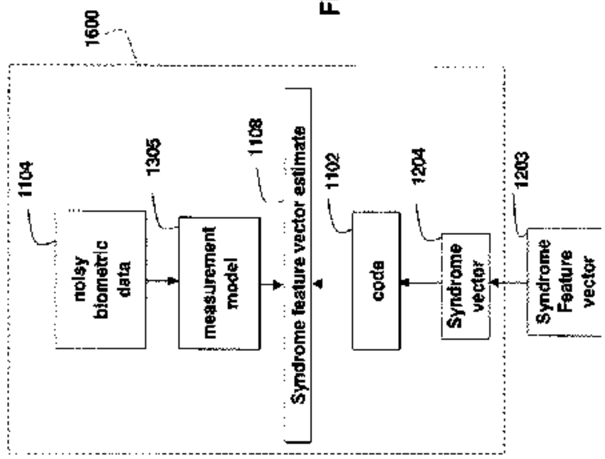

1600
1104
noisy biometric data
1305
measurement model
1108
Syndrome feature vector estimate
1102
code
1204
Syndrome vector
1203
Syndrome Feature vector

Fig. 16A

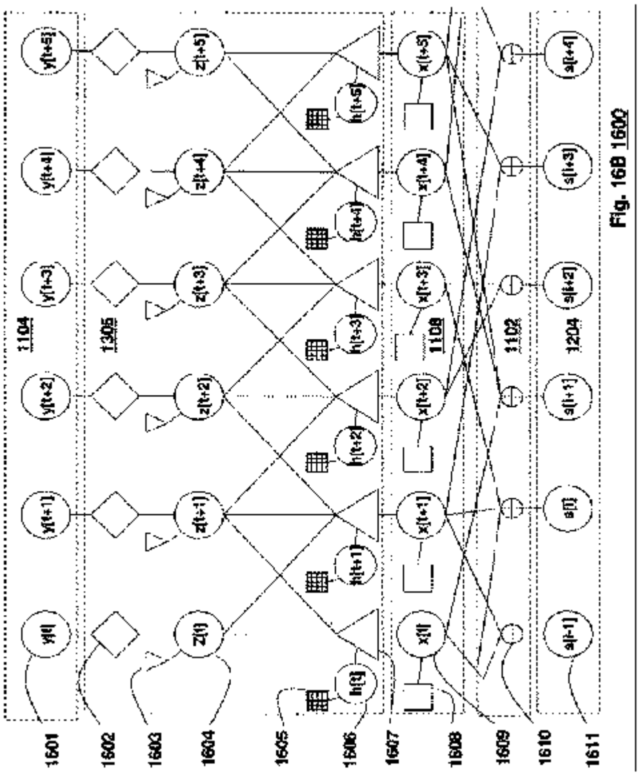

1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1104
1305
1108
1102
1204
y[t]
y[t+1]
y[t+2]
y[t+3]
y[t+4]
y[t+5]
Z[t]
z[t+1]
z[t+2]
z[t+3]
z[t+4]
z[t+5]
h[t]
h[t+1]
h[t+2]
h[t+3]
h[t+4]
h[t+5]
x[t]
x[t+1]
x[t+2]
x[t+3]
x[t+4]
x[t+5]
s[t-1]
s[t]
s[t+1]
s[t+2]
s[t+3]
s[t+4]

Fig. 16B 1600

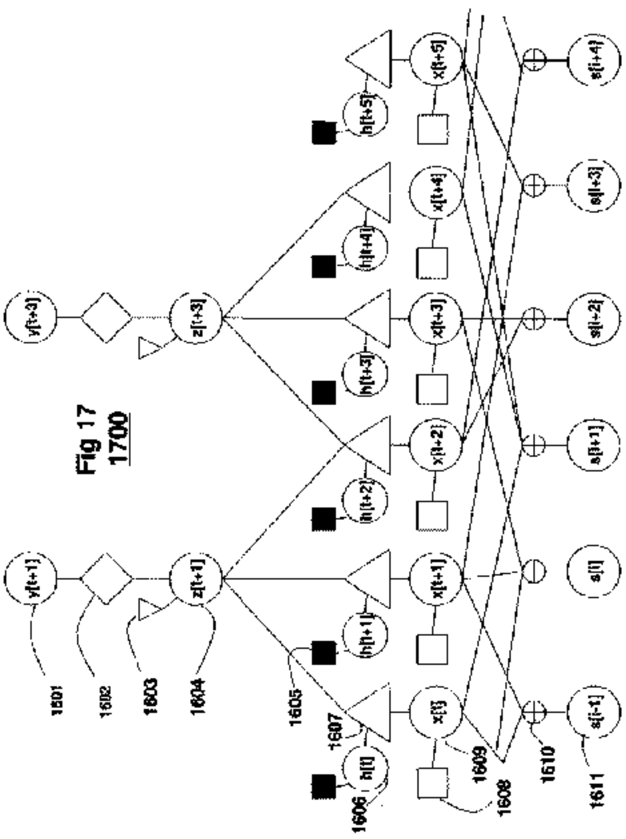


Fig 17
1700

y[t+1]
y[t+3]
z[t+1]
z[t+3]
h[t]
h[t+1]
h[t+2]
h[t+3]
h[t+4]
h[t+5]
x[t]
x[t+1]
x[t+2]
x[t+3]
x[t+4]
x[t+5]
s[t-1]
s[t]
s[t+1]
s[t+2]
s[t+3]
s[t+4]
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611

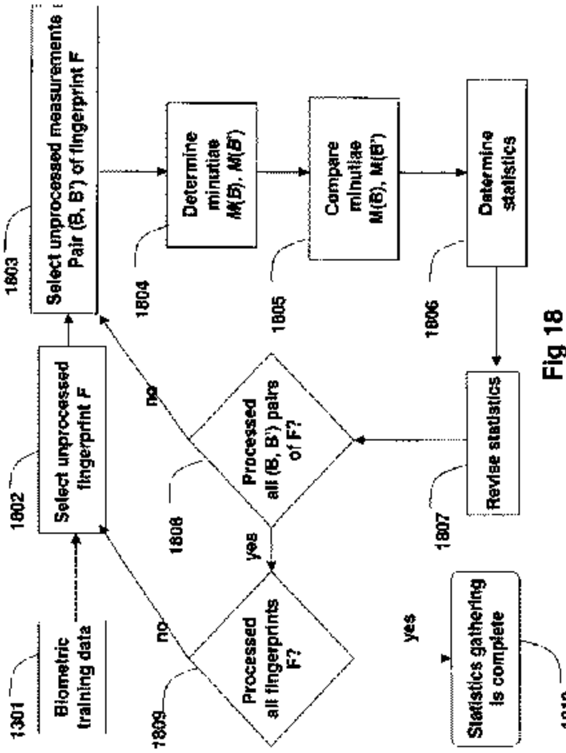

1301
Biometric training data
1802
Select unprocessed fingerprint F
1803
Select unprocessed measurements
Pair (B, B') of fingerprint F
1804
Determine minutiae M(B), M(B')
1805
Compare minutiae M(B), M(B')
1806
Determine statistics
1807
Revise statistics
1808
Processed all (B, B') pairs of F?
no
yes
1809
Processed all fingerprints F?
no
yes
1810
Statistics gathering is complete

Fig 18
1800

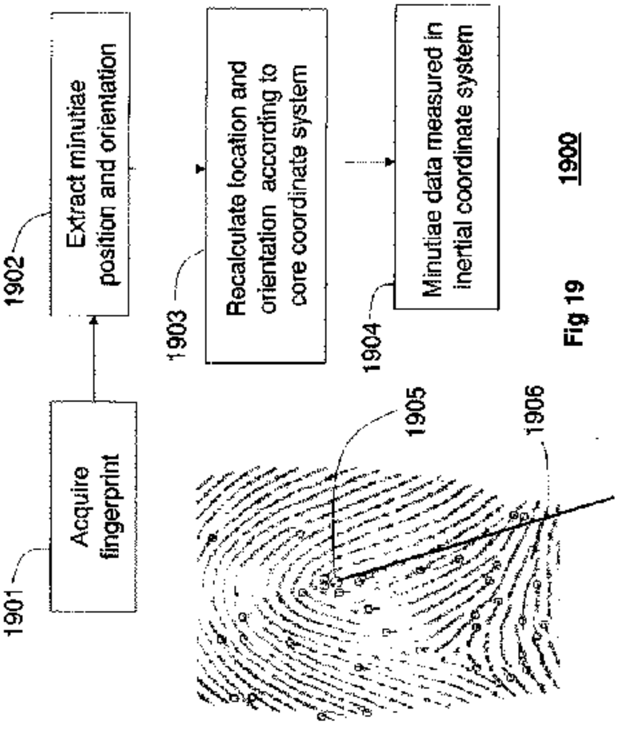

1901
Acquire fingerprint
1902
Extract minutiae position and orientation
1903
Recalculate location and orientation according to core coordinate system
1904
Minutiae data measured in inertial coordinate system
1905
1906
1900

Fig 19

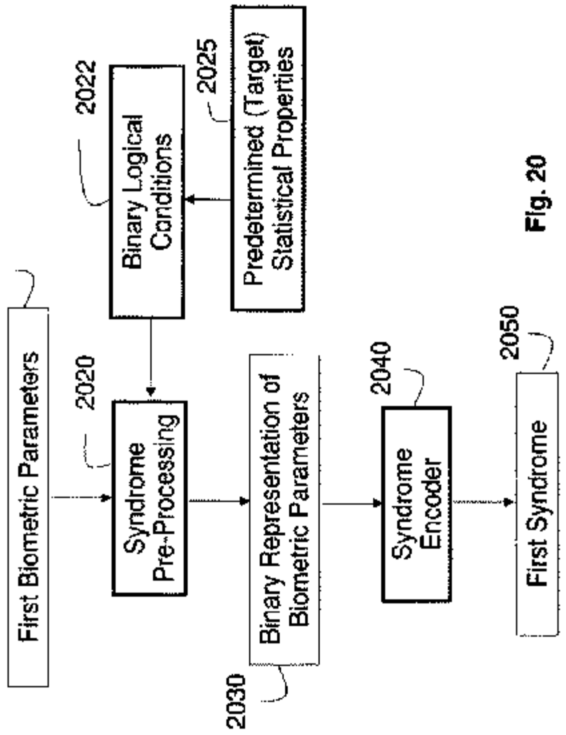

First Biometric Parameters
2010
Syndrome Pre-Processing
2020
Binary Logical Conditions
2022
Predetermined (Target) Statistical Properties
2025
Binary Representation of Biometric Parameters
2030
Syndrome Encoder
2040
First Syndrome
2050

Fig. 20

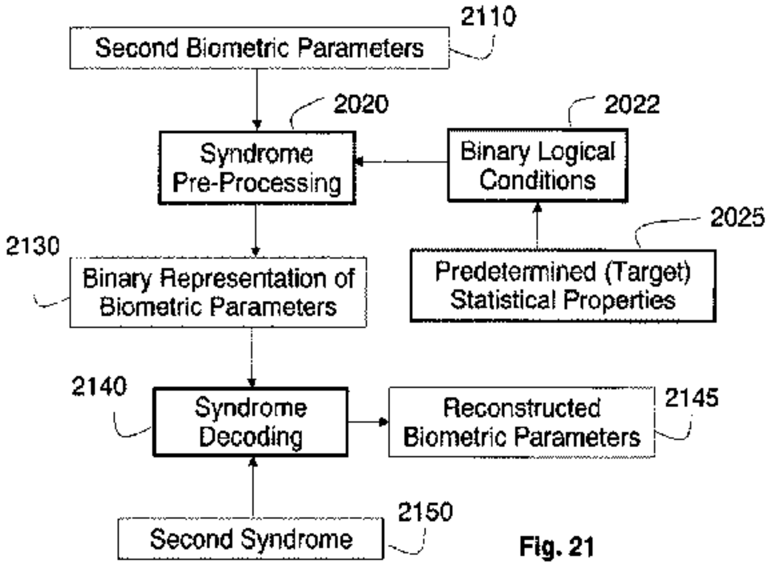

Second Biometric Parameters
2110
Syndrome Pre-Processing
2020
Binary Logical Conditions
2022
Predetermined (Target) Statistical Properties
2025
Binary Representation of Biometric Parameters
2130
Syndrome Decoding
2140
Reconstructed Biometric Parameters
2145
Second Syndrome
2150

Fig. 21

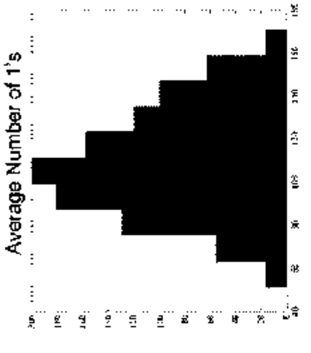


Fig. 22A

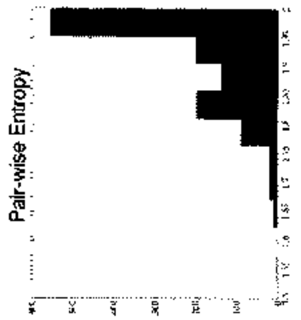


Fig. 22B

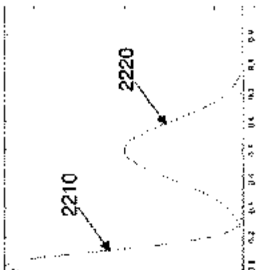


Fig. 22C

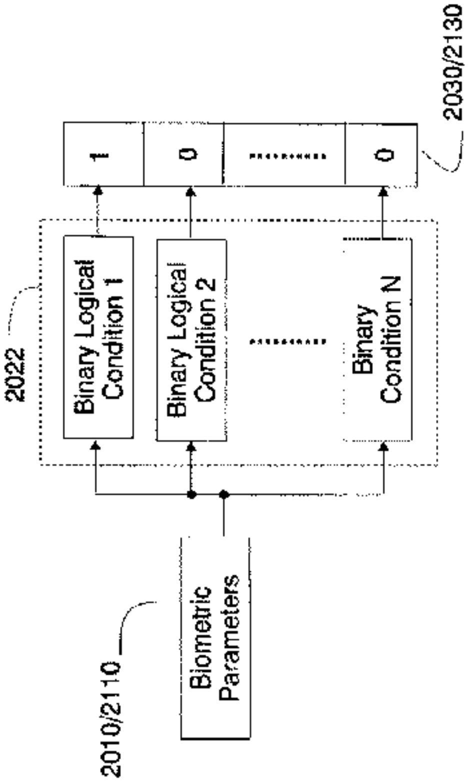

2010/2110
Biometric Parameters
2022
Binary Logical Condition 1
Binary Logical Condition 2
....
Binary Condition N
1
0
....
0
2030/2130

Fig. 23

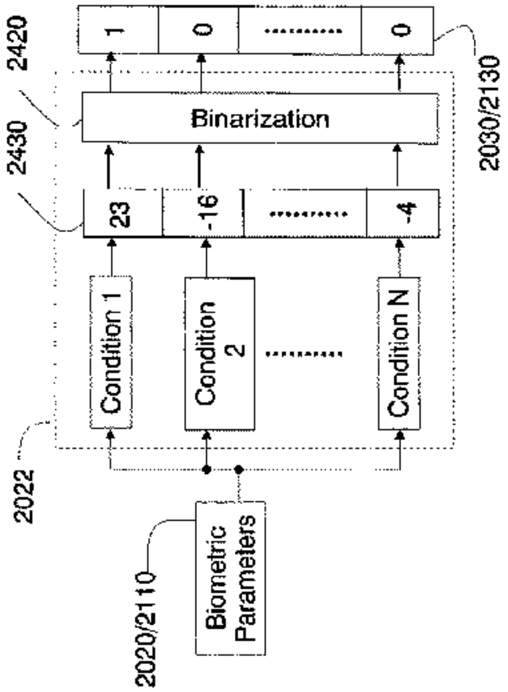

2420
2430
2022
2020/2110
Biometric Parameters
Condition 1
Condition 2
....
Condition N
23
-16
....
-4
Binarization
1
0
....
0
2030/2130

Fig. 24

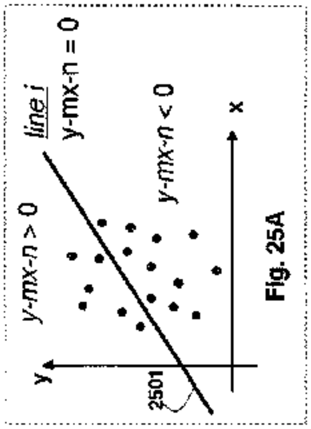


Fig. 25A

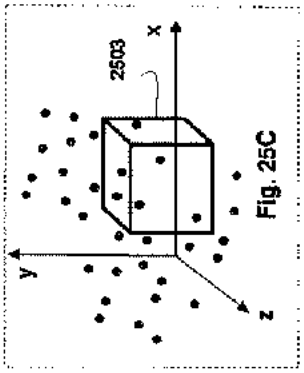


Fig. 25C

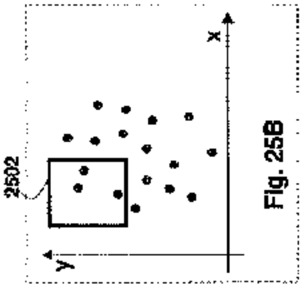


Fig. 25B

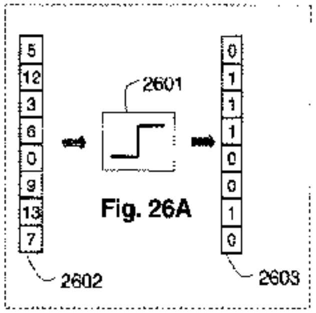


Fig. 26A

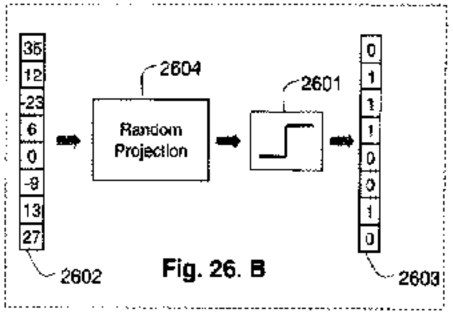


Fig. 26. B

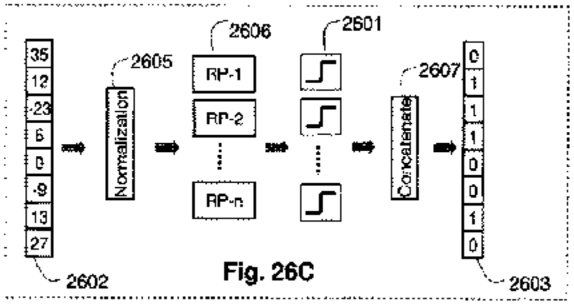


Fig. 26C

Electronic Patent Application Fee Transmittal

Application Number:	15075066
Filing Date:	18-Mar-2016
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul Timothy Miller
Filer:	David B. Bowls/Allison Hung
Attorney Docket Number:	47583.5US02_82053

Filed as Small Entity

Filing Fees for **Utility under 35 USC 111(a)**

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt

EFS ID:	27474940
Application Number:	15075066
International Application Number:	
Confirmation Number:	1166
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul Timothy Miller
Customer Number:	27683
Filer:	David B. Bowls/Allison Hung
Filer Authorized By:	David B. Bowls
Attorney Docket Number:	47583.5US02_82053
Receipt Date:	10-NOV-2016
Filing Date:	18-MAR-2016
Time Stamp:	14:59:27
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$90
RAM confirmation Number	111416INTEFSW15013100
Deposit Account	081394
Authorized User	Allison Hung

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		1_5US02IDSTransmittalandForm.pdf	687220 8ebf392757229cb3d8b1e94efc3ba5b8a65aae0a	yes	4

Multipart Description/PDF files in .zip description

Document Description	Start	End
Transmittal Letter	1	3
Information Disclosure Statement (IDS) Form (SB08)	4	4

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
2	Foreign Reference	2_5US02JP2008516472A.pdf	2190861 3d1a28926fe3ea170134e7ab2567e6dcef1515cb	no	16

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
3	Foreign Reference	3_5US02JP2009111971A.pdf	4195920 dcf847e500bd377f1859057a540c2a4af8b98ae3	no	162

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
4	Non Patent Literature	4_5US02NPL-Maeda.pdf	1014002 fe4bee79fa41dba3a552a808a1b996311af9103e	no	4

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
5	Non Patent Literature	5_5US02NPL-Shibata.pdf	1587097 707b41af4c69fd65eea15ac0299003e4264110de	no	7

Warnings:

Information:

6	Non Patent Literature	6_5US02NPL-Juels.pdf	3931550 619747b60eced8bb1c3aeb13ee3e89c3b8ddf9d4	no	21
Warnings:					
Information:					
7	Other Reference-Patent/App/Search documents	7_5US02JPOA.pdf	1814993 3153f52af5d705f56aa72390aa0fed956f14c8e2	no	12
Warnings:					
Information:					
8	Fee Worksheet (SB06)	fee-info.pdf	30668 9fed49ce885f7307882b7c9053d564108f5e6ad1	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	15452311		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

In The United States Patent And Trademark Office

Inventor(s):	Paul T. Miller, George A. Tuvell		
Applicant:	mSignia, Inc.		
Title:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE		
Application No.:	15/075,066	Filing Date:	March 18, 2016
Examiner:	Dao Q. Ho	Group Art Unit:	2497
Docket No.:	47583.5US02	Confirmation No.:	1166

Costa Mesa, California
November 10, 2016

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT UNDER 37 C.F.R. §§1.56, 1.97, and 1.98

Dear Examiner:

Pursuant to 37 C.F.R. §§1.56, 1.97, and 1.98, the documents listed on the accompanying Substitute PTO Form 1449 are called to the attention of the Examiner for the above patent application. The documents were cited in a Japanese Office Action mailed September 6, 2016, in Japanese Patent Application No. 2014-555571. A copy of the Japanese Office Action is also enclosed for the Examiner's review.

Citation of these documents shall not be construed as:

(1) an admission that the documents are necessarily prior art with respect to the instant invention;

(2) a representation that a search has been made, other than as described above; or

(3) an admission that the information cited herein is, or is considered to be material to patentability.

Haynes and Boone, LLP
600 Anton Blvd.,
Suite 700
Costa Mesa, CA 92626
Tele: (949) 202-3000
Fax: (949) 202-3001

Enclosed with this statement are the following:

☒ Substitute PTO Form 1449. The Examiner is requested to initial the form and return it to the undersigned in accordance with M.P.E.P. §609.

☒ A copy of each cited document as required by 37 C.F.R. §1.98 (*except where otherwise indicated*).

Complete copies are not submitted of U.S. patents and U.S. patent application publications per 37 C.F.R. §1.98(a)(2)(ii), and copies are not submitted of documents already cited or submitted in a parent application from which benefit under 35 U.S.C. §120 is claimed per 37 C.F.R. §1.98(d).

This statement should be considered because:

□ This statement qualifies under 37 C.F.R. §1.97, subsection (b) because:

□ It is being filed within 3 months of the application filing date of a national application other than a continued prosecution application under §1.53(d);

-- OR --

□ It is being filed within 3 months of entry of the national stage as set forth in §1.491 in an international application;

-- OR --

□ It is being filed before the mailing date of a first Office action *on the merits*;

-- OR --

□ It is being filed before the mailing date of a first Office action *after the filing of an RCE under §1.114.*

whichever occurs last.

□ Although it may not qualify under subsection (b), this statement qualifies under 37 C.F.R. §1.97, subsection (c) because:

(1) It is being filed before the mailing date of a FINAL Office Action and before a Notice of Allowance or another action closing prosecution (whichever occurs first);

-- AND *(check at least one of the following)* --

□ (1) It is accompanied by the $90 fee set forth in 37 C.F.R. §1.17(p);

-- OR --

□ (2) Pursuant to 37 C.F.R. §1.97(e), each item of information contained in the information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement.

--OR--

□ (3) Pursuant to 37 C.F.R. §1.97(e), no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than

three months prior to the filing of the information disclosure statement.

☒ Although it may not qualify under subsections (b) or (c), this statement qualifies under 37 C.F.R. §1.97, subsection (d) because:

(1) It is being filed on or before payment of the Issue Fee:

-- AND --

☒ (1) It is accompanied by the $90 fee set forth in 37 C.F.R. §1.17(p);

-- AND *(check at least one of the following)* --

☒ (2) Pursuant to 37 C.F.R. §1.97(e), each item of information contained in the information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement.

--OR--

□ (3) Pursuant to 37 C.F.R. §1.97(e), no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

☒ ***Fee Authorization.*** The Commissioner is hereby authorized to charge any additional fee(s), charge any underpayment of fee(s), or credit any overpayment associated with this communication to Deposit Account No. 08-1394.

Certificate of Transmission

I hereby certify that this correspondence is sent electronically via EFS Web to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below.

Allison Hung **November 10, 2016**

Respectfully submitted,

David Bowls
Agent for Applicant
Reg. No. 39,915

U. S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(use as many sheets as necessary)

SHEET	1	OF	1

	Complete if Known
Application Number	15/075,066
Filing Date	March 18, 2016
Applicant(s)	mSignia, Inc.
Art Unit	2497
Examiner Name	Dao Q. Ho
Attorney Docket Number	47583.5US02

U. S. PATENT DOCUMENTS

Examiner's Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document

FOREIGN PATENT DOCUMENTS

Examiner's Initials	Cite No.	Foreign Patent Document (Country Code – Number – Kind)	Publication Date MM-DD-YYYY	Patentee or Applicant of Cited Document	Translation Y/N

NON-PATENT LITERATURE DOCUMENTS

Examiner's Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article, title of the item, date, page(s), volume-issue number(s), publisher, city/country where published
	1.	JAKOBSSON et al., "Implicit Authentication for Mobile Devices," HotSec'09 Proceedings of the 4th USENIX conference on Hot topics in security, 2009, USENIX Association, Berkeley, California/USA. Retrieved from the Internet on 2016-11-18: <URL:https://www.usenix.org/legacy/event/hotsec09/tech/full_papers/jakobsson.pdf>

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

Electronic Patent Application Fee Transmittal

Application Number:	15075066
Filing Date:	18-Mar-2016
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul Timothy Miller
Filer:	David B. Bowls/Allison Hung
Attorney Docket Number:	47583.5US02_82053

Filed as Small Entity

Filing Fees for **Utility under 35 USC 111(a)**

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt

EFS ID:	27579701
Application Number:	15075066
International Application Number:	
Confirmation Number:	1166
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul Timothy Miller
Customer Number:	27683
Filer:	David B. Bowls/Allison Hung
Filer Authorized By:	David B. Bowls
Attorney Docket Number:	47583.5US02_82053
Receipt Date:	21-NOV-2016
Filing Date:	18-MAR-2016
Time Stamp:	19:27:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$90
RAM confirmation Number	112216INTEFSW19324000
Deposit Account	081394
Authorized User	Allison Hung

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		1_5US02IDSTransmittalandForm.pdf	658561 53deb52c330761bcc4e0083a7ac5a3c235d946f3	yes	4

Multipart Description/PDF files in .zip description

Document Description	Start	End
Transmittal Letter	1	3
Information Disclosure Statement (IDS) Form (SB08)	4	4

Warnings:

Information:

2	Non Patent Literature	2_5US02NPL-Jakobsson.pdf	1523487 eb998d08bb902d42a0d681281cd95b243bdeda7b	no	6

Warnings:

Information:

3	Fee Worksheet (SB06)	fee-info.pdf	30668 9f41205d5875f20786d1998598fb3a1f7173d5cf	no	2

Warnings:

Information:

Total Files Size (in bytes):	2212716

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Paul T. Miller, George A. Tuvell		
Applicant:	mSignia, Inc.		
Title:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE		
Application No.:	15/075,066	Filing Date:	March 18, 2016
Examiner:	Dao Q. Ho	Group Art Unit:	2497
Docket No.:	47583.5US02	Confirmation No.:	1166

Costa Mesa, California
November 21, 2016

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT
UNDER 37 C.F.R. §§1.56, 1.97, and 1.98

Dear Examiner:

Pursuant to 37 C.F.R. §§1.56, 1.97, and 1.98, the documents listed on the accompanying Substitute PTO Form 1449 are called to the attention of the Examiner for the above patent application. The documents were cited in a Japanese Office Action mailed September 6, 2016, in Japanese Patent Application No. 2014-555571. A copy of the Japanese Office Action is also enclosed for the Examiner's review.

Citation of these documents shall not be construed as:

(1) an admission that the documents are neccssarily prior art with respect to the instant invention;

(2) a representation that a search has been made, other than as described above; or

(3) an admission that the information cited herein is, or is considered to be material to patentability.

Haynes and Boone, LLP
600 Anton Blvd.,
Suite 700
Costa Mesa, CA 92626
Tele: (949) 202-3000
Fax (949) 202-3001

Enclosed with this statement are the following:

☒ Substitute PTO Form 1449. The Examiner is requested to initial the form and return it to the undersigned in accordance with M.P.E.P. §609.

☒ A copy of each cited document as required by 37 C.F.R. §1.98 (*except where otherwise indicated*).

Complete copies are not submitted of U.S. patents and U.S. patent application publications per 37 C.F.R. §1.98(a)(2)(ii), and copies are not submitted of documents already cited or submitted in a parent application from which benefit under 35 U.S.C. §120 is claimed per 37 C.F.R. §1.98(d).

This statement should be considered because:

□ This statement qualifies under 37 C.F.R. §1.97, subsection (b) because:

□ It is being filed within 3 months of the application filing date of a national application other than a continued prosecution application under §1.53(d);

-- OR --

□ It is being filed within 3 months of entry of the national stage as set forth in §1.491 in an international application;

-- OR --

□ It is being filed before the mailing date of a first Office action *on the merits*;

-- OR --

□ It is being filed before the mailing date of a first Office action *after the filing of an RCE under §1.114.*

whichever occurs last.

□ Although it may not qualify under subsection (b), this statement qualifies under 37 C.F.R. §1.97, subsection (c) because:

(1) It is being filed before the mailing date of a FINAL Office Action and before a Notice of Allowance or another action closing prosecution (whichever occurs first);

-- AND *(check at least one of the following)* --

□ (1) It is accompanied by the $90 fee set forth in 37 C.F.R. §1.17(p);

-- OR --

□ (2) Pursuant to 37 C.F.R. §1.97(e), each item of information contained in the information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement.

--OR--

□ (3) Pursuant to 37 C.F.R. §1.97(e), no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than

three months prior to the filing of the information disclosure statement.

☒ Although it may not qualify under subsections (b) or (c), this statement qualifies under 37 C.F.R. §1.97, subsection (d) because:

(1) It is being filed on or before payment of the Issue Fee:
-- AND --

☒ (1) It is accompanied by the $90 fee set forth in 37 C.F.R. §1.17(p);
-- AND *(check at least one of the following)* --

□ (2) Pursuant to 37 C.F.R. §1.97(e), each item of information contained in the information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement.
--OR--

☒ (3) Pursuant to 37 C.F.R. §1.97(e), no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

☒ ***Fee Authorization.*** The Commissioner is hereby authorized to charge any additional fee(s), charge any underpayment of fee(s), or credit any overpayment associated with this communication to Deposit Account No. 08-1394.

Certificate of Transmission

I hereby certify that this correspondence is sent electronically via EFS Web to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below.

Allison Hung **November 21, 2016**

Respectfully submitted,

David Bowls
Agent for Applicant
Reg. No. 39,915

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/075,066	03/18/2016	Paul Timothy Miller	47583.5US02_82053	1166

27683 7590 11/22/2016
HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

EXAMINER	
HO, DAO Q	

ART UNIT	PAPER NUMBER
2497	

NOTIFICATION DATE	DELIVERY MODE
11/22/2016	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ipdocketing@haynesboone.com

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
15/075,066	18 March, 2016	MILLER ET AL.	47583.5US02_82053

HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

EXAMINER	
DAO HO	
ART UNIT	PAPER
2497	20161115

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

The IDS filed on 11/10/2016 have been considered by The Examiner; however, NPL No.3 is not consider. The attached NPL does not have an english abstract and is not considered.

/DAO HO/
Primary Examiner, Art Unit 2497

PTO-90C (Rev.04-03)

U. S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(use as many sheets as necessary)

SHEET	1	OF	1

Complete if Known	
Application Number	15/075,066
Filing Date	March 18, 2016
Applicant(s)	mSignia, Inc.
Art Unit	2497
Examiner Name	Dao Q. Ho
Attorney Docket Number	47583.5US02

U. S. PATENT DOCUMENTS

Examiner's Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document

FOREIGN PATENT DOCUMENTS

Examiner's Initials	Cite No.	Foreign Patent Document (Country Code – Number – Kind)	Publication Date MM-DD-YYYY	Patentee or Applicant of Cited Document	Translation Y/N
	1.	JP2008516472	05-15-2008	KONIN-KLIJKE PHILIPS ELECTRONICS N.V.	Abstract only
	2.	JP2009111971	05-21-2009	Mitsubishi Electric Research Laboratories Inc.	Y

NON-PATENT LITERATURE DOCUMENTS

Examiner's Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article, title of the item, date, page(s), volume-issue number(s), publisher, city/country where published
	3.	MAEDA, Takashi, "Biometrics complex authentication system capable of realizing accurate, rapid identity authentication instantly," Monthly Bar Code, August 2, 2001, pp. 64-66, Vol. 14, Issue 9, Japan Industrial Publishing Co., Ltd., Japan.
	4.	SHIBATA, Yoichi, "Mechanism-based PKI," Computer Security Symposium, October 29, 2003, Vol. 2003, No. 15, pp. 181-186, Information Processing Society of Japan, Japan.
	5.	JUELS et al., "A Fuzzy Vault Scheme," Designs, Codes and Cryptography, February 2006, pp. 237-257, Vol. 38, No. 2, Springer Science + Business Media, Inc., New York/USA.
	6.	Notice of Reasons for Rejection dated September 6, 2016, Japanese Patent Application No. P2014/555571.

Examiner Signature	/DAO Q HO/	Date Considered	11/15/2016

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Paul T. Miller, George A. Tuvell		
Applicant:	mSignia, Inc.		
Title:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE		
Application No.:	15/075,066	Filing Date:	March 18, 2016
Examiner:	Dao Q. Ho	Group Art Unit:	2497
Docket No.:	47583.5US02	Confirmation No.:	1166

Costa Mesa, California
December 1, 2016

Mail Stop Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT UNDER 37 C.F.R. § 1.312

Dear Examiner Ho:

Pursuant to 37 C.F.R. § 1.312, Applicant respectfully requests entry of the following amendment, which is submitted before payment of the issue fee.

Amendments to the Claims begin on page 2 of this paper.

Remarks begin on page 8 of this paper.

IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1-21. (Canceled)

22. (Previously presented) An identity recognition system comprising:

a non-transitory memory storing information associated with one or more identities, wherein the information stored for an identity includes (a) data values associated with that identity; and (b) information regarding anticipated changes to one or more of the stored data values associated with that identity;

one or more hardware processors in communication with the memory and configured to execute instructions to cause the identity recognition system to recognize that the presentation of identity information by a computer is authentic, by performing operations comprising:

generating a challenge to the computer, wherein the challenge prompts the computer to provide a response based on one or more data values from the computer that correspond to one or more of the-stored data values associated with the identity;

receiving, from the computer, the response to the challenge;

determining whether the response is allowable, wherein such determining comprises using the stored information regarding anticipated changes to the stored data values associated with the identity to determine whether a data value used to form the response is based on an acceptable change to a corresponding stored data value; and

recognizing that the presentation of identity information by the computer is authentic, according to whether the computer has provided an allowable response to the challenge.

23. (Previously presented) The identity recognition system of claim 22, wherein the identity is associated with the computer and is a user identity or a device identity.

24. (Previously presented) The identity recognition system of claim 22, wherein the challenge prompts a response based on one or more user minutia data values.

25. (Previously presented) The identity recognition system of claim 24, wherein the operation of determining whether the response is allowable includes evaluating whether at least a portion of the response is based on one or more acceptable changes to a user minutia data value.

26. (Previously presented) The identity recognition system of claim 25, wherein the user minutia data values used to determine whether the response is allowable comprise user secrets, user customization, entertainment data, bio-metric data, or contacts.

27. (Previously presented) The identity recognition system of claim 25, wherein the user minutia data values used to determine whether the response is allowable comprise calling app data, geo-location data, frequently called phone numbers, email, or network connection data.

28. (Previously presented) The identity recognition system of claim 22, wherein a stored data value is used to generate at least a portion of the challenge, and wherein the determining operation comprises evaluating whether the data value used to form the response is the same as the stored data value.

29. (Previously presented) The identity recognition system of claim 22, wherein a change to the stored data value is acceptable when the data value used to form the response is within a set of acceptable values for the stored data value that are determined independently from receiving the response from the computer.

30. (Previously presented) The identity recognition system of claim 29, wherein the set of acceptable values includes one or more values based on anticipated changes to the data value.

31. (Previously presented) The identity recognition system of claim 29, wherein the set of acceptable values includes one or more values based on anticipated changes to the data value, based on industry updates to hardware, firmware, or software elements.

32. (Previously presented) The identity recognition system of claim 29, wherein the set of acceptable values includes one or more values based on an anticipated user customization of the computer.

33. (Previously presented) The identity recognition system of claim 29, wherein the set of acceptable values includes one or more values based on an anticipated usage of the computer by a user.

34. (Previously presented) The identity recognition system of claim 22, further comprising the operations of:

in response to determining that the response is based on an acceptable change to a data value associated with the identity, updating the memory to reflect the changed data value.

35. (Previously presented) The identity recognition system of claim 22, wherein the operation of determining whether the response is allowable further comprises comparing the received response to a member of a set of two or more allowable responses.

36. (Previously presented) The identity recognition system of claim 35, wherein the set of allowable responses is computed before the determining operation is performed.

37. (Previously presented) The identity recognition system of claim 35, wherein the set of allowable responses is computed concurrently with the determining operation being performed.

38. (Previously presented) The identity recognition system of claim 22, wherein the determining operation further comprises generating a rating of the allowability of the response, based on the stored data value and one or more changes to the stored data values.

39. (Previously presented) The identity recognition system of claim 38, wherein the rating of the allowability of the response is based on a comparison of a data value upon

which the response is based to one or more anticipated changes to the stored data values associated with the identity to be recognized.

40. (Previously presented) The identity recognition system of claim 39, wherein the rating of the allowability of the response is varied based on whether the response is based at least in part on one or more anticipated changes to the stored data values.

41. (Previously presented) The identity recognition system of claim 22, wherein the operation of recognizing that the presentation of identity information by the computer is authentic provides a basis for one or more of: authenticating a device, authenticating a user, validating a software program or an application, providing data protection of data transmitted to or from a device, or generating a digital signature of a message digest.

42. (Previously presented) The identity recognition system of claim 22, wherein the response does not contain any data values reflecting personally identifiable information.

43. (Currently amended) An identity recognition system comprising:

a non-transitory memory storing information associated with one or more identities, wherein the information stored for an identity includes (a) data values associated with that identity; and (b) information regarding anticipated changes to one or more of the stored data values associated with that identity;

one or more hardware processors in communication with the memory and configured to execute instructions to cause the identity recognition system to recognize that the presentation of identity information by a computer is authentic, by performing operations comprising:

generating a challenge, wherein the challenge originates at the computer and prompts the computer to transmit an identity claim comprising identity information;

receiving, from the computer, one or more communications comprising the ~~an~~ identity claim comprising identity information, wherein at least a portion of the identity claim is formed based on one or more data values from the computer, and wherein at least one of the data values used to form the identity claim corresponds to a stored data value;

determining whether the one or more communications received from the computer are sufficient to recognize that the identity claim is allowable ~~authentic~~, wherein such determining comprises using the stored information regarding anticipated changes to the stored data values to determine whether a data value used to form the identity claim is based on an acceptable change to a corresponding stored data value associated with the identity; and

recognizing that the presentation of identity information by the computer is authentic, according to whether the computer has provided an allowable identity claim in response to the challenge.

44. (Currently amended) An identity recognition system comprising:

a non-transitory memory storing information associated with one or more identities, wherein the information stored for an identity includes (a) data values associated with that identity; and (b) information regarding anticipated changes to one or more of the stored data values associated with that identity;

one or more hardware processors in communication with the memory and configured to execute instructions to cause the identity recognition system to recognize that the presentation by a first computer of an identity claim ~~to be recognized~~ is authentic, by performing operations comprising:

generating a challenge, wherein the challenge originates at a second computer distinct from the first computer and prompts the first computer to transmit an identity claim comprising identity information;

receiving, from the first computer, a communication comprising the identity claim comprising identity information, wherein the identity claim is based on one or more data values from the first computer, and wherein at least one of the data values upon which the communication is based corresponds to a stored data value for the identity;

determining whether the communication received from the first computer is sufficient to recognize that ~~the use of~~ the identity claim is ~~authentic~~ allowable, wherein such determining comprises using the stored information regarding anticipated changes to the stored data values to determine whether a data value upon which the communication is based reflects an acceptable change to a corresponding stored data value associated with the identity; and

recognizing that the presentation of identity information by the first computer is authentic, according to whether the first computer has provided an allowable identity claim in response to the challenge.

45. (Previously presented) The system of claim 22, further comprising using information from the allowable response to update the stored information regarding anticipated changes to the stored data values associated with the identity.

46. (Previously presented) The system of claim 22, further comprising using information from the allowable response to update the corresponding stored data value and the stored information regarding anticipated changes to the stored data values associated with the identity.

REMARKS

Pursuant to 37 C.F.R. § 1.312, Applicant respectfully requests entry of the foregoing amendment. The amendment is submitted in response to the Examiner's amendment provided in the Notice of Allowance dated November 4, 2016, for which Applicant expresses appreciation.

The amendment is submitted to correct various issues in claims 43 and 44. The amendment is submitted to address, for example, an issue of antecedent basis for the term "the challenge", in claims 43 and 44; to address consistency in the use of the terms "allowable" and "authentic" as between claim 22 and claims 43 and 44; and to address differences in scope among the claims. Applicant notes that the amendment of additional limitations to claims 43 and 44 narrows the scope of those claims.

Amendment to claim 43 in regard to the limitation of "the challenge originates at the computer" and claim 44 in regard to the limitation of "the challenge originates at a second computer distinct from the first computer" is supported by the specification as filed at least at page 45, lines 23-24 and lines 27-29. Applicant therefore submits that no new matter is added.

Applicant also notes that claims 45 and 46 were added by the Examiner's amendment, for which additional claim fees are submitted along with this amendment. Should any fees be required for this submission, the Commissioner is hereby authorized to charge any fees due or credit any overpayments in regard to this communication to Deposit Account No. 08-1394.

If there are any questions regarding any aspect of the application, please call the undersigned at (949) 202-3011.

Certificate of Transmission

I hereby certify that this correspondence is being electronically transmitted via EFS Web to the Commissioner for Patents, on the date stated below.

December 1, 2016

Allison Hung

Respectfully submitted,

David Bowls
Patent Agent
Reg. No. 39,915

Electronic Patent Application Fee Transmittal

Application Number:	15075066
Filing Date:	18-Mar-2016
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul Timothy Miller
Filer:	David B. Bowls/Allison Hung
Attorney Docket Number:	47583.5US02_82053

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	2202	2	40	80
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**80**

Electronic Acknowledgement Receipt

EFS ID:	27671608
Application Number:	15075066
International Application Number:	
Confirmation Number:	1166
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul Timothy Miller
Customer Number:	27683
Filer:	David B. Bowls/Allison Hung
Filer Authorized By:	David B. Bowls
Attorney Docket Number:	47583.5US02_82053
Receipt Date:	01-DEC-2016
Filing Date:	18-MAR-2016
Time Stamp:	19:24:30
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$80
RAM confirmation Number	120216INTEFSW19251400
Deposit Account	081394
Authorized User	Allison Hung

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		5US02312Amendment.pdf	1281259 954d658ca91893ca779825a444b3e595b1bcc42e	yes	9

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment after Notice of Allowance (Rule 312)	1	1
Claims	2	7
Applicant Arguments/Remarks Made in an Amendment	8	9

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
2	Fee Worksheet (SB06)	fee-info.pdf	30641 4e71deda057b2b8e2bb103855a97f5723850a6da	no	2

Warnings:

Information:

Total Files Size (in bytes):	1311900

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/075,066	03/18/2016	Paul Timothy Miller	47583.5US02_82053	1166

27683 7590 12/02/2016
HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

EXAMINER
HO, DAO Q

ART UNIT	PAPER NUMBER
2497	

NOTIFICATION DATE	DELIVERY MODE
12/02/2016	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ipdocketing@haynesboone.com

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address : COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
15/075,066	18 March, 2016	MILLER ET AL.	47583.5US02_82053

HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

EXAMINER	
DAO HO	
ART UNIT	PAPER
2497	20161129

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

The IDs filed on 11/21/2016 has been considered by The Examiner.

/DAO HO/
Primary Examiner, Art Unit 2497

PTO-90C (Rev.04-03)

U. S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(use as many sheets as necessary)

SHEET	1	OF	1

	Complete if Known
Application Number	15/075,066
Filing Date	March 18, 2016
Applicant(s)	mSignia, Inc.
Art Unit	2497
Examiner Name	Dao Q. Ho
Attorney Docket Number	47583.5US02

U. S. PATENT DOCUMENTS

Examiner's Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document

FOREIGN PATENT DOCUMENTS

Examiner's Initials	Cite No.	Foreign Patent Document (Country Code – Number – Kind)	Publication Date MM-DD-YYYY	Patentee or Applicant of Cited Document	Translation Y/N

NON-PATENT LITERATURE DOCUMENTS

Examiner's Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article, title of the item, date, page(s), volume-issue number(s), publisher, city/country where published
	1.	JAKOBSSON et al., "Implicit Authentication for Mobile Devices," HotSec'09 Proceedings of the 4th USENIX conference on Hot topics in security, 2009, USENIX Association, Berkeley, California/USA. Retrieved from the Internet on 2016-11-18: <URL:https://www.usenix.org/legacy/event/hotsec09/tech/full_papers/jakobsson.pdf>

Examiner Signature	/DAO Q HO/	Date Considered	11/29/2016

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.Q.H/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/075,066	03/18/2016	Paul Timothy Miller	47583.5US02_82053	1166

27683 7590 12/09/2016
HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

EXAMINER	
HO, DAO Q	

ART UNIT	PAPER NUMBER
2497	

NOTIFICATION DATE	DELIVERY MODE
12/09/2016	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ipdocketing@haynesboone.com

Response to Rule 312 Communication	**Application No.** 15/075,066	**Applicant(s)** MILLER ET AL.
	Examiner DAO HO	**Art Unit** 2497

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address –

1. ☒ The amendment filed on *12/01/2016* under 37 CFR 1.312 has been considered, and has been:

a) ☒ entered.

b) □ entered as directed to matters of form not affecting the scope of the invention.

c) □ disapproved because the amendment was filed after the payment of the issue fee.
Any amendment filed after the date the issue fee is paid must be accompanied by a petition under 37 CFR 1.313(c)(1) and the required fee to withdraw the application from issue.

d) □ disapproved. See explanation below.

e) □ entered in part. See explanation below.

/DAO HO/
Primary Examiner, Art Unit 2497

OK TO ENTER: /D.Q.H/

12/05/2016

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Paul T. Miller, George A. Tuvell		
Applicant:	mSignia, Inc.		
Title:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE		
Application No.:	15/075,066	Filing Date:	March 18, 2016
Examiner:	Dao Q. Ho	Group Art Unit:	2497
Docket No.:	47583.5US02	Confirmation No.:	1166

Costa Mesa, California
December 1, 2016

Mail Stop Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT UNDER 37 C.F.R. § 1.312

Dear Examiner Ho:

Pursuant to 37 C.F.R. § 1.312, Applicant respectfully requests entry of the following amendment, which is submitted before payment of the issue fee.

Amendments to the Claims begin on page 2 of this paper.

Remarks begin on page 8 of this paper.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

27683 7590 11/04/2016
HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Allison Hung	(Depositor's name)
	(Signature)
December 9, 2016	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/075,066	03/18/2016	Paul Timothy Miller	47583.5US02	1166

TITLE OF INVENTION: CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	02/06/2017

EXAMINER	ART UNIT	CLASS-SUBCLASS
HO, DAO Q	2497	380-255000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Haynes and Boone, LLP
2 ____________
3 ____________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE	(B) RESIDENCE: (CITY and STATE OR COUNTRY)
mSignia, Inc.	Irvine, California

Please check the appropriate assignee category or categories (will not be printed on the patent): □ Individual ☒ Corporation or other private group entity □ Government

4a. The following fee(s) are submitted:
☒ Issue Fee
☒ Publication Fee (No small entity discount permitted)
□ Advance Order - # of Copies ____________

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
□ A check is enclosed.
☒ Payment by credit card. Form PTO-2038 is attached.
□ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number ____________ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

□ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

□ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

□ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature ____________ Date December 9, 2016

Typed or printed name David Bowls Registration No. 39,915

Electronic Patent Application Fee Transmittal

Application Number:	15075066
Filing Date:	18-Mar-2016
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul Timothy Miller
Filer:	David B. Bowls/Allison Hung
Attorney Docket Number:	47583.5US02_82053

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
UTILITY APPL ISSUE FEE	2501	1	480	480
PUBL. FEE- EARLY, VOLUNTARY, OR NORMAL	1504	1	0	0
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**480**

Electronic Acknowledgement Receipt

EFS ID:	27747515
Application Number:	15075066
International Application Number:	
Confirmation Number:	1166
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul Timothy Miller
Customer Number:	27683
Filer:	David B. Bowls/Allison Hung
Filer Authorized By:	David B. Bowls
Attorney Docket Number:	47583.5US02_82053
Receipt Date:	09-DEC-2016
Filing Date:	18-MAR-2016
Time Stamp:	14:13:28
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$480
RAM confirmation Number	121216INTEFSW14141601
Deposit Account	081394
Authorized User	Allison Hung

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	5US02IssueFeeTransmittal.pdf	230816 465a89777ff15cf0c15cf250f7c8c08b943cf0a9	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	32260 2c1538c8a374adf5465966480cfcbeede3178f9f	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	263076		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/075,066	01/31/2017	9559852	47583.5US02_82053	1166

27683 7590 01/11/2017

HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Paul Timothy Miller, Irvine, CA;
mSignia, Inc., Irvine, CA;
George Allen Tuvell, Thompson's Station, TN;

<u>IN THE UNITED STATES PATENT AND TRADEMARK OFFICE</u>

Inventors:	Paul T. Miller, George A. Tuvell		
Applicant:	mSignia, Inc.		
Title:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE		
Patent No.:	9,559,852 B2	Issue Date:	January 31, 2017
Appln. No.:	15/075,066	Filing Date:	March 18, 2016
Examiner:	Dao Q. Ho	Group Art Unit:	2497
Docket No.:	47583.5US02	Confirmation No.:	1166

Costa Mesa, California
February 8, 2017

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REQUEST FOR CERTIFICATE OF CORRECTION PTO'S ERROR

Dear Examiner:

The Patentees submit herewith PTO Form PTO/SB/44 Certificate of Correction. This submission corrects errors by the U.S. Patent and Trademark Office (PTO). Accordingly, the Applicant/Assignee requests a Certificate of Correction or an otherwise corrected patent at the expense of the PTO to correct this error.

We believe that no fee is due. However, if a fee is required, please charge Deposit Account No. 08-1394. If any questions remain or anything additional is required to correct this patent copy, please contact the undersigned at (949) 202-3011.

Certificate of Transmission

I hereby certify that this correspondence is being electronically transmitted via the USPTO Web to the United States Patent and Trademark Office on the date shown below.

Allison Hung **February 8, 2017**

Respectfully submitted,

David Bowls
Agent for Applicant
Reg. No. 39,915

HAYNES AND BOONE, LLP
600 Anton Blvd., Suite 700
Costa Mesa, CA 92626
(949) 202-3000
FAX (949) 202-3001

PTO/SB/44 (09-07)
Approved for use through 08/31/2013. OMB 0651-0033
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.
(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

Page 1 of 1

PATENT NO. : 9,559,852 B2

APPLICATION NO.: 15/075,066

ISSUE DATE : January 31, 2017

INVENTOR(S) : Paul T. Miller, George A. Tuvell

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

IN THE CLAIMS:

Claim 24, Column 36, Lines 7-10, change:

"a non-transitory memory storing information associated with one or more identities, wherein the information stored for an identity includes (a) data values associated with that identity;"

to:

--a non-transitory memory storing information associated with one or more identities, wherein the information stored for an identity includes (a) data values associated with that identity; and (b) information regarding anticipated changes to one or more of the stored data values associated with that identity;--

MAILING ADDRESS OF SENDER (Please do not use customer number below):

Haynes and Boone, LLP
2323 Victory Avenue, Suite 700
Dallas, TX 75219

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1.0 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Attention Certificate of Corrections Branch, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt

EFS ID:	28304593
Application Number:	15075066
International Application Number:	
Confirmation Number:	1166
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul Timothy Miller
Customer Number:	27683
Filer:	David B. Bowls/Allison Hung
Filer Authorized By:	David B. Bowls
Attorney Docket Number:	47583.5US02_82053
Receipt Date:	08-FEB-2017
Filing Date:	18-MAR-2016
Time Stamp:	17:33:42
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Certificate of Correction	5Us02RequestforCertificateofCorrection.pdf	288471 5d90f197f890a852d5cfbbe70dc1ad8de7656097	no	2

Warnings:

Information:	
Total Files Size (in bytes):	288471

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO.	: 9,559,852 B2	Page 1 of 1
APPLICATION NO.	: 15/075066	
DATED	: January 31, 2017	
INVENTOR(S)	: Paul T. Miller et al.	

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Claims

Claim 24, Column 36, Lines 7-10, change:

"a non-transitory memory storing information associated with one or more identities, wherein the information stored for an identity includes (a) data values associated with that identity;"

to:

--a non-transitory memory storing information associated with one or more identities, wherein the information stored for an identity includes (a) data values associated with that identity; and (b) information regarding anticipated changes to one or more of the stored data values associated with that identity;--

Signed and Sealed this
Eighteenth Day of April, 2017

Michelle K. Lee

Michelle K. Lee
Director of the United States Patent and Trademark Office