Challenges for copyright in a digital age

I D Bramhill and M R C Sims

The act of breaching copyright is probably the most common civil offence, and is often not considered as being unlawful by the perpetrator. The revenue that is lost by a copyright owner when illegal copying takes place can be significant. Losses may become unacceptably large in the future given the expected explosion of computerised, multimedia services. This paper discusses the problems copyright owners face when trying to maintain cost-effective control of their copyright in a digital age. It then proposes an initial model of a software-based system that provides copyright protection of multimedia information when delivered by Internet-based services.

1. Introduction

Authors and artists have certain rights when they produce a work-of-art — these rights are automatically assigned to them and no registration is needed. These include copy rights. When a copy of a work-of-art is made some fee can lawfully be claimed by the author for its use. If an author[1] finds evidence that someone is making copies of his work-of-art without permission he can take the infringer to a court of law and reclaim lost revenue. Authors would naturally like to maximise the amount of revenue that comes to them from others making copies of their work-of-art with a minimum amount of effort on their own part. Copyright infringement is a civil offence and so the onus is on the author to protect his work-of-art. Traditionally this has been easy due to the physical nature of works-of-art — generally it costs less and is more desirable to buy a high-quality copy of a book from a store than to make an illegal copy. Due to the increase in electronic distibution of information and the reduction in cost of storage of such information, copyright infringement is increasing. New mechanisms are needed to ensure that authors preserve their revenue stream.

1.1 Copyright and copy protection

Data that is in the digital domain can be reproduced, error free, with as little effort as a 'drag-and-drop' operation using a graphical user interface. If the same process is repeated on the first generation copy the result is a perfect second- generation copy. An equivalent process in the analogue domain would be to repeatedly use a photocopier on its own output, but this results in a rapid reduction in quality after a small number of copy generations. When we work in the digital domain we have the ability to pass on a perfect copy to anyone, anywhere in the world.

The great benefit for a recipient of digital data is the increase in quality of the copy that he receives. Some of the benefits for the sender are that he can provide a better service, to more people, in less time, and at a fraction of the cost. Because the material is in digital form there is less physical protection available for it and so copyright owners[2] have lost some of the control they once had. This reduces the amount of revenue that they can collect. The international laws for copyright give the owner the right to make a charge for the supply of a copy of an original work-of-art. Therefore owners want to encourage copies to be made of their work-of-art to increase their revenue. Copyright owners also want to be able to control the copies once they have been made in order to protect future revenue. A copy protection system provides them with a method of **controlling** copies, it does not attempt to **prevent** copies from being made, because this is not possible.

Being unable to prevent a copy from being made would not be a problem if one could detect the act of copying. If this were the case, then copyright owners could still collect revenue when their works-of-art are used.

Unfortunately it is not feasible to detect the act of making a copy when it matters, that is, when combating organised piracy. For example, the digital information to be

[1] The author/owner/user, depicted as male throughout this paper, could equally be female.

[2] Copyright owner: a person, or organisation, that owns the copyright for a work-of-art (which can be a piece of text, music, painting, film). The copyright owner can be someone other than the author of a work-of-art, e.g. Michael Jackson is the owner of the copyright of many works-of-art of which Lennon and McCartney are the authors. Sometimes this paper shortens the term 'copyright owner' to just 'owner'.

copied can always be put into a computer that is not connected to any network, and that has no kind of communications capability. Although the initial recovery of the information can be detected and charged for, once put into the pirate computer the process of making multiple copies cannot be detected.

1.2 *The impact of new technology*

Copyright-protected material is starting to be provided by many new delivery methods; this makes it susceptible to new threats. An example of such a new delivery method is Digital Video Disc (DVD) which had its world market launch delayed by concern over copyright issues:

- '..the studios have said... that no titles will be released until all the outstanding copy protection issues have been resolved to the satisfaction of all parties' [1],

- '..everyone agrees that copy protection is the most visible issue. The movie industry has steadfastly upheld their intention to withhold publishing titles until they are convinced there is an acceptable means for protecting their assets from being copied. The method of copy protection used, they insist, must also be applied to computers. Therein lies the problem.' [2].

The DVD format allows 133 minutes of broadcast quality video and sound to be held on a disc that has the same physical dimensions as a music CD (compact disc). DVD is sometimes called Digital *Versatile* Disc because it can carry any information, not just video. It is therefore expected to be of significant interest to computer manufacturers who see it as providing a step change in the capacities available with CD-Read Only Memory (CD-ROM) giving DVD-ROM.

Initial capacity for a DVD-ROM will be 4.7 gigabytes, rising to a capacity of 17 gigabytes for double sided, dual-layer technology. It is expected that DVD-recordable drives will soon appear. A date of mid-1997 is currently predicted [3] and machine prices, when driven by a powerful computer industry, will quickly fall to be similar to that of CD-recordable drives (currently found for less than US$2000). It can therefore be seen that perfect copies of works in which the film industry have literally invested billions of American dollars, will now be available as source material for 'professional' and 'home' pirating using personal computers.

1.3 *DVD protection*

The agreed industry-wide mechanism for the protection of copyright in the DVD system comprises a number of techniques as described below.

Each DVD player and disc pressing will be supplied with one of six regional codes, this will ensure that a disc that is released in North America will not function on a DVD player that is bought in Europe.

Some of the digital information will be protected using a process called encryption[3]. The specific implementation will be licensed by a governing body so that the manufacture of DVD players can be controlled. The movie soundtrack and imagery will be encrypted as two separate streams of information (see Fig 1). The DVD player uses its licensed technology to access information on the disc that tells it how to decrypt the streams.

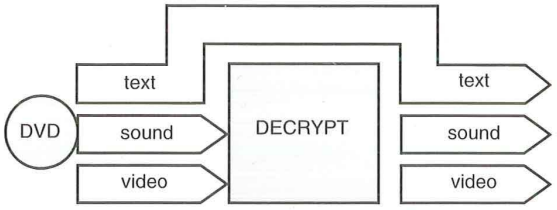


Fig 1 DVD protection.

A DVD player will not have connectors that give access to the decrypted digital information. The analogue video signal that is output will be protected by a technique owned by a company called Macrovision. This technique causes recorded video quality to be reduced.

It is hoped that laws will be imposed to make it illegal to sell or possess technology that tries to circumvent the copyright protection mechanism for the DVD system. An alternative approach is for industry to also design the circumvention technology and to patent it. This approach has the benefit that someone building and selling circumvention technology can be sued for patent violation and this is more easily achieved internationally in comparison to proving copyright violation.

1.4 *Identifying requirements*

In the DVD example requirements for the copyright protection mechanism came from the owners identifying the environment in which the work is going to be used. The environment is that of traditional retail distribution, selling physical items to anonymous customers. This paper considers a different environment having its own requirements and which possibly poses the greatest challenge to

[3] Encryption is a process that is part of an area called cryptography. We make reference to these areas many times in this paper and so will give a definition of some of the terms; greater depth of the subject can be found in Phoenix [4]. 'A cipher is a secret method of writing, whereby plaintext... is transformed into ciphertext. The process of transforming plaintext into ciphertext is called ... encryption; the reverse process ... is called ... decryption. Both encryption and decryption are controlled by a cryptographic key.' [5].

copyright in the digital age. The environment is that of providing works-of-art using Internet-based services.

There are a number of schemes published or currently in use such as that proposed by Choudhury et al [6] and Adobe Acrobat® [7]. This paper proposes alternatives to some of the published mechanisms and extends others. It also combines mechanisms to create a complete end-to-end solution.

This environment provides a significant challenge because owners wish to supply digital information on a world-wide basis into many individual environments where they have no direct control, a situation unlike that of DVD. The copyrighted material is therefore supplied to a user[4] by a copy protection system, but once on a user's personal computer he can make many attempts to subvert the copy protection system and so resell the material as his own over the Internet. Should the user find a significant weakness in the protection mechanism he could even render the entire system useless by publicising the weakness.

In addition to the requirements imposed by using the model of Internet-based services there are a number of requirements that must be satisfied if a copy protection mechanism is to be attractive to users and owners. For example, the owners do not want to have to perform many processes to gain an adequate level of protection. Also, users do not want to have to go through a registration phase each time they want access to information from a new source. Such requirements were considered when developing our proposed mechanism.

2. Can prevention work?

2.1 *An example of extreme prevention*

Consider a work-of-art that takes the form of written text that is the original manuscript of a poem. The owner can easily prevent copyright infringement by never allowing any user to read the poem, and this can be ensured by keeping it locked in a security vault. The obvious problem here is that this approach will not result in the collection of any revenue, unless he charges a fee for access to the vault.

For our fictional owner it appears that he is still maintaining control, but there is a problem. The user can easily reproduce the poem from memory and resell it once he leaves the vault. If the work-of-art is a novel the user can read it aloud into an audio recorder and reproduce it later, or even memorise it. The owner could make a restriction that no manner of copy technology, such as an audio recorder or camera, ever leaves the vault but he is still faced with the problem of a user with a photographic memory.

This copy protection system has a very high level of control but we can see from it that no copy protection system can justly make the claim of being absolutely secure. With the additional requirement of checking for users possessing recording devices, the amount of revenue that could be lost has been reduced to users having photographic memories. Each time a decision is made on how a copy protection system functions we must consider how to minimise the possible threats, and must decide if the maximum potential fraud is below the threshold of what is considered an unacceptable loss to the owner.

2.2 *Cryptography to the rescue*

Now we consider the scenario of the owner needing to take the manuscript out of the vault to allow access by a user who cannot physically get to it. The owner can take the original manuscript to the user but if the manuscript is stolen in transit then the owner will have lost the work-of-art. The owner can make a copy of the manuscript and take that to the user; but if the copy is stolen, he still suffers a significant loss. The owner is faced with a similar problem to that of a government wanting to send a message containing secret information to their spy in another country. If the message is intercepted by an enemy, then he should not be able to determine the secret information. Governments have long achieved such protection by use of cryptography 'which embraces methods for rendering data unintelligible to unauthorised parties' [8].

By using an encryption process the poem owner can create a copy of his poem as a ciphertext version which he takes to the user (see Fig 2). The owner uses the matching decryption process to recover a plaintext copy of the original which they show to the user. Here cryptography is being used to provide confidentiality; if the owner loses the ciphertext, no one can recover the original plaintext of the poem without access to the decryption process and the cryptographic key .

The fictitious owner has protected his poem in transit, but is faced with another problem. As soon as the

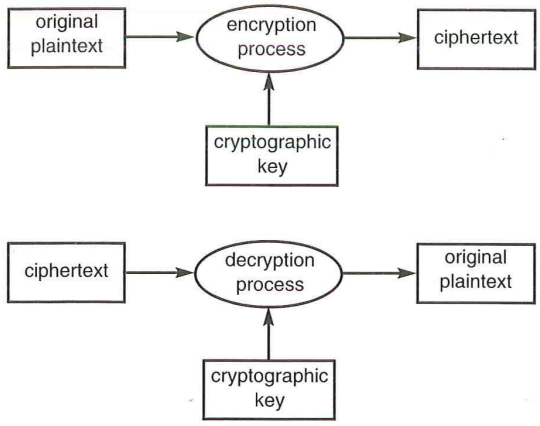


Fig 2 Cryptography terminology.

[4] A person, or organisation who makes use of a copyrighted work-of-art.

decryption process is applied, the plaintext is revealed, and so the amount of control he has over the work is again reduced. The poem's owner can maintain control by never leaving the plaintext unattended, but this is not possible when network delivery is involved.

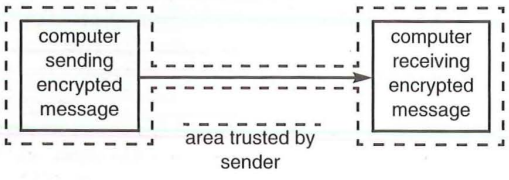
2.3 *Trust in cryptography*

Cryptography is normally used to protect the transfer of information between two parties that trust each other.

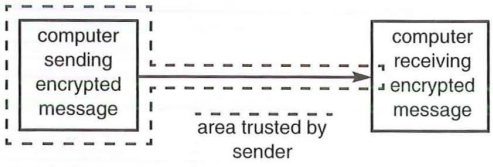
For example, our fictitious government encrypts plaintext and sends the ciphertext to their spy. The spy knows the decryption process and the cryptographic key and recovers the plaintext message. Once the spy has read the plaintext message, it is destroyed to ensure the spy's own safety.

Commercial companies use cryptography to protect information sent by computers operating between departments. These departments can trust that each will not disclose the decryption process or the cryptographic key.

When using cryptography in an Internet-based copy-protection mechanism, we cannot consider the computer of the user to be trustworthy. We must regard all of the users as potential pirates because we know there are a small number of real pirates trying to defraud the system. Figure 3 shows how the areas that the sender trusts alter between the traditional use of cryptography (a) and a situation where the recipient is untrustworthy (b).



a) traditional use - sender trusts receiver



b) protecting copyrights - sender does not trust receiver

Fig 3 Trust in cryptography.

[5] For the decryption process to succeed the cryptographic key must be the correct key. We must ensure that all parties who should have the correct key have it when they need it, and must ensure that any party who should not have the key cannot obtain it without expending a significant level of effort. To do this requires 'cryptographic key management' which is a large subject area and is not covered by this paper.

2.4 *Making a viable solution using cryptography*

If we are to use cryptography to protect information in an environment of limited trust, we must limit access to the plaintext. Figure 4 shows the journey a work-of-art takes to get to the brain of the user. At some point in this journey the decryption must happen, i.e. the work-of-art must leave the area trusted by its owner. This should happen as late as possible to make it difficult for a fraudster to get control of the plaintext.

Ideally we would like to perform the decryption when the encrypted work-of-art is in the brain of the user but this idea is clearly unachievable and unacceptable. The next best approach is to decrypt the information just before it reaches the eyes and ears of the user.

This can be achieved by requiring the user to have a special device that performs the decryption process but which is configurable only by the sender. This device must also control the use of the work-of-art, so that without it the work-of-art is unusable[6]. For example, to prevent quality copies of a video tape being made, a distributor could supply the user with a tape that is encrypted such that it can only be played in that user's video player. The video player must be tamper-proof, must incorporate a television screen and provide no means of attachment to any other recording device.

Clearly this would be an expensive way to distribute all video tapes, but could possibly be a solution when a small number of users require information of high value. Because the decryption process now occurs in hardware and not in the brain, fraudsters[7] have an opportunity to make copies, for example, by using a video camera to record the images on the screen. The quality of the copies made using such a technique would probably be so low as not to pose a significant threat to the copyright owner.

Any solution that requires expensive devices at the user's machine will be limited to special applications. This paper considers a model of information provided by Internet-based services to a world-wide client base. To reduce the costs of a copy-protection system to a level that is acceptable to both owners and users we consider that only a software-based copy protection mechanism utilising cryptography will be commercially viable. We therefore need to consider the problems that this may present.

[6] In some cases an owner may want to control the use of the work-of-art. For instance, an owner of a journal may wish to control how it is viewed, if it can be printed to paper, and the level of quality when printed.

[7] A fraudster is a person, or organisation, who attempts to make unauthorised copies for financial gain or attempts to provide users with the means to make unauthorised copies. A fraudster will usually be a user.

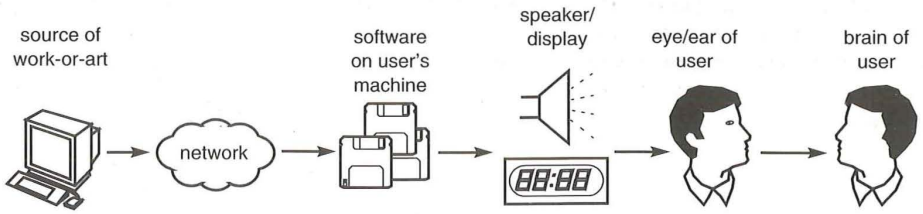


Fig 4 Where to decrypt.

3. Challenges for a software-only solution

3.1 *Binding software to a user*

The first problem to be considered is that a software-only solution is subject to all of the problems faced by information in the digital domain, i.e. its elements can be easily copied and distributed. We therefore need to ensure that a duplicate of the copy protection software of one user is of no use to anyone other than that user.

This implies the need for a strong[8] one-to-one binding between the software of a user, and the user. The binding could be achieved by making it undesirable for users to distribute copies of the software, e.g. by making it display sensitive information about the user, such as their home address or other personal information. However, this would probably be unacceptable to users.

The best way to achieve the binding is to use smart cards[9]. Smart cards have been designed to provide strong identification of a person, so the strong binding we require can be achieved by binding the software to the smart card, and the smart card to the user. Although smart cards provide a secure cryptographic environment they should not be used to decrypt the work-of-art. If smart cards were used in this way, a fraudster would only need to intercept the plaintext output to access the work-of-art (see Fig 5). Unfortunately the smart cards also need to be distributed to the users before the work-of-art can be used; this may be unacceptable in some circumstances.

3.2 *Binding software to a machine*

Another way to achieve the strong binding we require is to bind the decryption software to the computer on which it is run or the terminal from which it is used. Biometrics identify a human to a high level of probability. A number of characteristics are measured to do this. Similarly, a number of characteristics of a computer can be measured to achieve a similar level of probability of its identity, which we call a 'cybermetric'. Examples of such characteristics are:

- the physical components which the computer comprises (size of memory, presence of CD drive),
- characteristics of the physical components (manufacturer, number of tracks on a hard disk),
- location of static information on a hard disk (bad sectors),
- location of long-lived files on a hard disk (operating system executables),
- operational characteristics,
- logical directory and file structures,
- files specifically created to identify the machine,
- data added to long-lived files to identify the machine,
- the configuration of applications and the operating system.

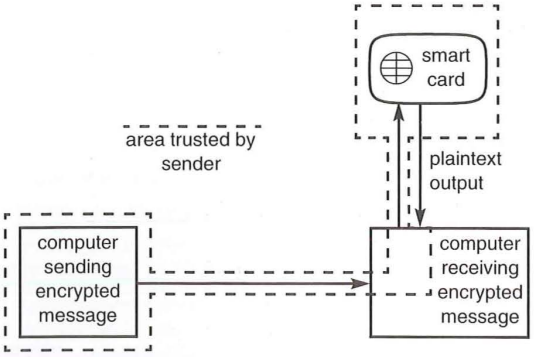


Fig 5 Smart card decryption.

For fraudsters to make use of a software decryption process belonging to another user, they would have to recreate both the logical and physical characteristics of that machine, and the characteristics of the way the original user operated all of the separate applications.

3.3 *Binding a work-of-art to a user*

In the earlier example of the tamper-proof video player, there was a one-to-one relationship between an instance of a work-of-art and the special viewing equipment. If a user gave their video tape to another user with a similar device then his video tape could not be played on the second user's equipment.

[8] Strong means that it cannot be easily tampered with, broken or forged.

[9] Smart cards are usually credit card sized devices made of plastic that have micro-electronic circuits embedded within. The circuitry provides a secure, tamper-resistant computing environment that can be used to implement cryptographic mechanisms.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.