System Aspects of Copy Management for Digital Video

Jean-Paul Linnartz, Joop Talstra, Ton Kalker, and Maurice Maes
Philips Research, WY, Holstlaan 4, 5656 AA Eindhoven, The Netherlands
Tel: +31 40 2742302 Fax: +31 40 2744660 Email: J.P.Linnartz@philips.com

ABSTRACT - THIS PAPER REVIEWS BASIC PRINCIPLES OF COPY PROTECTION FOR DIGITAL VIDEO. WE DISTINGUISH BETWEEN THE ROLE OF CRYPTOGRAPHY AND EMBEDDED SIGNALING, AS SEEN BY STANDARDIZATION BODIES SUCH AS THE DVD COPY PROTECTION TECHNICAL WORKING GROUP (CPTWG). WE IDENTIFY SEVERAL ISSUES THAT ARE UNRESOLVED AND/OR CURRENTLY UNDER DISCUSSION. IN PARTICULAR, WE ELABORATE ON PLAY CONTROL, COPY GENERATION CONTROL, AND UNIQUE IDENTIFICATION OF DIGITAL STORAGE MEDIA.

1 INTRODUCTION

Digital multimedia technology paves the way for new applications, features and services. However the transition from analog to digital has been seriously affected by a slow release of content. Film and music content owners are afraid to lose revenues as digital content, if unprotected, can be copied rapidly, perfectly, at large scale and without limitations on the number of generations of copies. Copy control issues have come on the "critical time path" of the market introduction of several digital products, including DVD video [1, 2], the IEEE 1394 (firewire) digital interface [3], digital broadcasting, and improved digital audio carriers such as Super Audio-CD, DVD-Audio, and secure solid-state audio carriers [4]. The standardization of DVD video has unleashed an unprecedented debate over copy protection, which has influenced the entire digital multimedia landscape. Recent security breaches of the DVD-video encryption proved once again that encryption with essentially fewer than 40 key bits, thus also relying on the secrecy of the algorithms, does not work, particularly not in a situation with dozens of manufacturers, each employing hundreds of designers. Meanwhile, improved cryptographic protection and additional techniques including watermarking are considered. Weaknesses in the algorithms led to the collapse of an entire system, after an event that should have been contained as a single isolated security incident.

Given the current status, this paper cannot describe a fully defined and mature system. It must be regarded as a status report from an ongoing discussion. We present our findings from active participation in several fora. Portions of this paper have previously appeared as white papers or responses to Calls for Proposals, e.g. [5 - 9]. We strongly believe in open, publicly evaluated systems and solutions which have been discussed not only in industrial standardization meetings but also at academic symposia. Some technologies, such as encryption on DVD video discs have been standardized in the Copy Protection Technical Working Group for DVD. Other technologies described in this paper are currently under discussion or are most likely to become topic of discussion any time soon. Although the underlying technologies are mostly well understood, it appeared less trivial to standardize a complete copy protection system. We focus on system aspects, particularly on the watermarking and copy generation control.

The outline is as follows: Section 2 covers the basic mechanisms, in particular encryption and embedded signaling. It identifies issues of particular concern, weaknesses or unresolved issues which will be addressed in Section 3. We acknowledge that the overview can not be complete. References to previously published documents are given. Besides giving a useful introduction to readers new to this field (mainly in Section 2), the paper intends to provide (in Section 3) further insight and generate new ideas for readers who have been following the standardization in detail.

2. THE BASIC CONCEPTS

Copy management can not easily be formalized into "Alice and Bob" protocols, as commonly studied for other fields of security and cryptography [13]. In fact, Alice, in our case the content owner, intends to sell information to an unreliable customer Bob, without allowing Bob to further disseminate this information. Evidently there is no cryptographic or information theoretical solution to this problem. Nonetheless, international standardization efforts have recognized that a workable way to redefine the problem is as follows: Alice sells digital data to an unreliable Bob, who can only process this data on a trusted device. The protection relies on Bob's inability to access the data directly. This concept is further worked further in the following sections.

2.1 *Encryption*

Protection by encryption leads to the notion of a *compliant world* of consumer devices which communicate over authenticated and encrypted digital links, using frequently updated session keys. A device is compliant when its manufacturer has agreed to follow specific copy protection rules described in a licensing agreement, in return for knowledge of cryptographic keys to get access to protected digital content. Hence, non-compliant devices never get access to the digital content in the clear. Without claiming to be exhaustive in our summary, important consequences of this approach are:

0-7803-6536-4/00/$10.00 (c) 2000 IEEE

- Protected digital content must be encrypted on any "open interface." This includes digital interconnects (e.g. IEEE 1394, USB), over the air broadcast, PCMCIA connectors, internal PC busses. The licensing agreement prohibits the use of 'insecure' interfaces.
- Encryption as such is not sufficient. An attacker can copy data, which compliant devices inherently would understand during playback. Thus
  - An authentication mechanism and session key generation is needed for all interfaces.
  - The digital representation on a storage medium, such as a recordable CD or DVD disc needs protection against bit-by-bit copying of encrypted data. One way of dealing with this is through unique media and disc identifiers, which may not be changeable by hackers.
- Internally, devices need to interpret and process data. For instance, users want to navigate through large video files. Video often needs to be reformatted and converted before storage, transmission and display. Therefore, end-to-end encryption, though favoured from a security point of view is less workable. Link-by-link encryption was preferred for DVD-Video and IEEE 1394 firewire.
- Content eventually needs to be presented in the clear to the human consumer. While the protection of digital protection can be extended all the way to digital monitors and speakers, eventually an analog signal, vulnerable to (non-compliant) copying must be created. Additional protection is needed to prevent that this analog signal can successfully be offered to a (compliant) recorder, as if it were the users personal creation.
- There must be a business mechanism to marginalize the market for non-compliant devices, and a consumer incentive to buy compliant rather than non-compliant devices.
- In order to enforce licensing rules, the technology must be patented and licensable. Rules can only be imposed on products which fall under the scope of the licensed patents. In DVD, licensing addresses the *playback* equipment, rather than the *recording* functionality of devices. Recent legislative developments, such as the WIPO treaty and its national derivates such as the US Digital Millennium act and EU directive outlaw certain classes of so-called circumvention devices. This provide a second layer of protection.
- Devices must be 'tamper-resistant'. This is presumably the least understood aspect of todays copy protection solutions.

2.2 Embedded signaling

To prevent copying through an analog circumvention route, some (water-) mark is added as an indelible part of the content. Modern advances in the modelling of the Human Visual/Auditory System (HVS and HAS) have opened the possibility to embed these marks physically imperceptibly in the content, usually by making minor modifications to the signal values. Such embedded signalling resemble electronic "tattoos" as these ensure that marks are not lost in typical operations, including format conversions. [1, 10-11]

Watermark detectors can be incorporated in compliant recorders. Copyrighted 'never-copy' content will then be recognised as such, and the 'record control' functionality of the recorder refuses to store material for which the user has no rights to copy it. For at least two reasons this approach is insufficient. Firstly, for a hacker or small-scale pirate it would be a relatively simple task to modify his own recorder and to create discs that play on the devices used by his customers. Secondly, the DVD licensing mechanism for compliance has been build upon playback devices, thus not around recorders. Both aspects can be resolved by 'play control', which is illustrated in Figure 1. The basic concept of 'play control' is that the player (also) recognizes the copy state of the content by detecting the watermark, and compares this with a physical mark on the disc. If the physical mark is correct and matches with the watermark, the device is authorized to play. Section 3.3 addresses this physical mark.

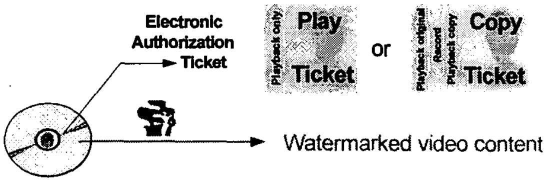

Figure 1: Basic elements of play control: if a player detects watermarks, it verifies the presence of an appropriate mark, which acts as an authorization ticket.

3 ISSUES

This section discusses a few aspects that are on the agenda for copy protection standardization.

3.1 Location of watermark detector and copy control

Security requirements for copy protection sometimes conflict with the architecture of PCs and consumer electronic devices. From a security perspective, the effectuation of play control can best be located in the drive, i.e., as early as possible in the chain of circuits that handle digital video coming from a storage medium. This suggests that one would also like to include a watermark detector in the playback drive, where sectors of data are read from the disc surface. However, PC DVD drives are designed to obediently deliver sector data to the PC bus, without having any natural ability to interpret the (video audio or other) data. Watermark detection in the drive involves recognition of the type of data in the sectors, concatenation of data from multiple sectors, decryption, demultiplexing, and (partial) MPEG decompression. None of these tasks occur naturally within the drive. It has been proposed to skip watermark checks whenever data is encrypted, but evidently this opens many circumvention methods. Another solution [7] is to outsource the watermark detection to a device that can perform this task more naturally, such as an MPEG decoder, and to rely on a secure authenticated link between the drive and decoder. Such link is already available in the DVD-ROM concept, but would require some additional features. In particular an integrity mechanism is needed to ensure that the drive and decoder negotiate about the same video data. It would allow the drive to effectuate play control, based on watermarks checked by the decoder. This also prevents the 'local scrambling' or 'bit inversion' attack [9].

3.2 Copy Generation Control

Having covered the case of content that may never be copied, we must also deal with the much less straightforward implementation of `(only) one (generation of) copy allowed'. Because of the nature of this 'Copy Once' requirement, information has to be passed along with the content to allow a recorder to distinguish between original and copy. Two basic principles are known:

- Embedding of a secondary watermark by the recorder (the *remarking* concept).
- Removal of a 'volatile' piece of information from the content during recording (the *ticket* concept).

Both solutions have their own pros and cons. Remarking requires that a consumer recorder must be able to embed a watermark. This implies that content must made accessible in a form that allows embedding (e.g. partial MPEG decoding). Reliable and invisible embedding may require evaluation of the content using a perceptual model. Another disadvantage is that pirates can compare the input and output of such storage device, and find the embedded secondary watermark. Almost inevitably that provides information on how to remove the watermark. The ticket approach [6, 10] avoids the above issues. The volatile piece of information, i.e., the "ticket" acts as an authorization identifier. It can either be embedded in the content or passed on as a separate signal. Failure of a device to handle the ticket leads to a loss of rights to copy. The remarking and ticket concept have fundamentally different failure modes. In particular, remarking tends to allow recorder to make copies in cases when a legacy or modified recorder has failed to add the secondary watermark, whereas the ticket concept may deny the user rights to copy when a legacy device has accidentally mishandled the ticket.

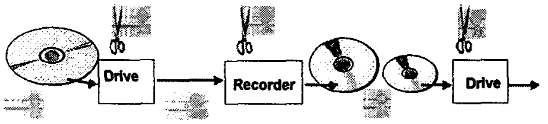

Figure 2: The ticket is clipped (cryptographically modified) during each playback or recorder passage.

There are several options to cryptographically bind the ticket to the content, and to ensure that the ticket is specific for a particular title or for any specific transfer (e.g. copy) of the content. One solution is to make the ticket a digital signature over the content itself. This appeared less advantageous for the very same reason as why link-by-link encryption is preferred over end-to-end encryption: video needs to be processed, and any processing would invalidate the ticket. User devices would have to be able to create a new valid ticket each time such processing occurs. The private key to sign must be hidden in the consumer device. It is more effective is to bind the ticket to the watermark payload, rather than to the content directly. As the watermark is (required to be) preserved under processing, the ticket can remain the same. The ticket is used as a proof that the source of the content has prior knowledge of the watermark [6, 10]. A random number is generated by the copyright owner, which then becomes the versatile ticket. The ticket acts as a cryptographic counter that can be decremented, but not incremented. Depending on how many generations of recording and playback the content owner desires to grant to the user, she sets the system by passes the ticket through a cryptographic function $F()$, n times. Here $F()$ is a publicly known cryptographic one-way function. Neither the player nor the recorder pass T transparently. Instead, the ticket is clipped, i.e., the counter is decremented by passing the ticket data through a one-way function, on every passage through a recorder or player (see Fig. 2). Verification of the ticket occurs in players and in recorders. It is done checking for a watermark. If that is present, the ticket data is passed through the one-way function m times and compared with the watermark data. Players check for m = 1 or 3. Recorders check for m = 2. Mastering equipment checks for m =2 or m = 4 before creating stampers for 'copy never' or 'copy once' discs, respectively. A real life analogy would be a movie-theater where the entrance ticket is stripped by the attendant at the entrance (record control), but where viewers have to hang on to the stub to allow wardens to check whether nobody snuck into the theater through the emergency exit (playback control). The ticket concept also allows play control of copy-once material. It also provides an extension to anti-piracy measures. In the remarking system, the first and any further generation of copies would all carry the both the primary and secondary watermark. Thus play control can not distinguish between these.

The cryptography behind the ticket system does not rely on a global secret. From a cryptographic point of view it is not necessary that $F()$ is kept secret to potential attackers. Compliant consumer devices check for the watermark. If it is present and has payload W, it also interprets the ticket data T to verify whether $F^m(T)$, with m = 1, 2, .. equals W. If m = 1 the device is entitled to playback the content. If m = 2 the device is entitled to record the content, and to store $T' = F(T)$ along with the content.

3.3 Media Type Recognition

Several reasons exist why recordable storage media should be distinguished from pressed media, and need a unique identifier that may not be modifiable in a consumer device.

- The watermark 'play control' system needs information about whether the disc is original pre-mastered (stamped) one or a recordable.
- To prevent that both the encrypted content and the associated keys can be bit copied from pressed discs to recordables, some uncopyable data should be stored on pressed media.
- Copy-Once content stored on a recordable disc must be encrypted in a way such that cloning to another recordable disc is not possible. A solution is to use a unique disc identifier to generate the encryption key. If the encrypted content, but not the ID is transferred to another disc with a different ID, a player will not be able to generate the appropriate decryption key.

Many proposals have been brought up to distinguish between pressed (ROM) and recordable discs. To some extent, the DVD standard relies on data stored in ROM sectors which should not be write-accessible by recorders. This is now recognized as being both too weak to stop hackers and inadequate from a licensing point of view.

Measurement of the **disc reflectivity** initially was one of the solutions discussed extensively, but this idea was abandoned as it conflicts with the current development of better materials for recordable discs.

Also, the **pre-groove wobble**, a positioning technique used by all known *recordable* disc formats appears less suitable. Different wobble frequencies are used by different standards. Thus a pre-groove wobble detector does not necessarily recognize recordable disc using a new format. None of these two concepts are future-proof, in that they inherently deal with new formats.

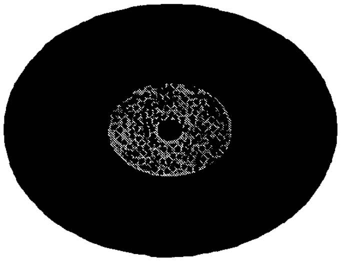

Figure 3: Artist impression of wobbled pits on DVD disc

The most secure solution proposed thus far is the **pit wobble** of *pressed* (i.e., DVD-ROM) media. As illustrated in Figure 3, the wobble is a rapid radial deviation from the track spiral on the disc. The deviations are at tens of kHz or faster and can be detected electronically in the servo control circuitry of the player. However the mechanics of the optical pick do not allow the laser head to precisely follow the deviations. The optical head thus follows an (unwobbled) spiral and the wobble is experienced as a minor detracking which does not affect the detector of the video data that resides in the pits. The security resides in the fact that although consumer readers can detect it, consumer recorders can fundamentally not write a wobble. Data embedded in the wobble carries a payload of cryptographic data that is specific for every title produced on ROM. This is tied to the watermark in the same manner described in the previous section for the ticket.

4 CONCLUSIONS

Although copy protection has received ample attention in the standardization of digital video in the past 5 years, the issues has not yet been fully resolved. It is unlikely that a bulletproof solution will ever be found, but the discussions are converging on what technical mechanisms should be involved and against what these can protect. We identified several issues that will be on the agenda in the coming year(s). We also discussed solutions to some of these problems.

REFERENCES

1. J.A. Bloom, I.J. Cox, T. Kalker, J.P. Linnartz, M. Miller and C. Traw, "Copy Protection for DVD video", IEEE Proceedings, July 1999, Vol. 87, No. 7, pp. 1267
2. A. E. Bell, The dynamic digital disk, IEEE Spectrum, Vol. 36. No. 10, Oct. 1999, pp. 28-35.
3. 5C digital transmission content protection white paper. [Online] Available WWW: http://www.dtcp.com
4. B. Ponce, "The impact of MP3 and the future of digital entertainment products", IEEE Communications Magazine, September 1999, Vol. 37, No. 9, pp. 68-70
5. G. Wirtz, Philips Electronics Response to Call For Proposals Digital Transmission, Copy Protection Technical Working Group, Burbank, CA
6. J.P. Linnartz, A. Kalker G. Depovere, Philips Electronics Response to Call For Proposals Data Hiding (Watermarking), Copy Protection Technical Working Group, Burbank, CA
7. J.P. Linnartz, J. Talstra A. Kalker G. Depovere, M. Maes, Philips Electronics Response to Call For Proposals WG 9, Tokyo, Japan, September 1998
8. J.P. Linnartz, J. Talstra A. Kalker G. Depovere, M. Maes, Philips Electronics Response to Call For Proposals WG 6, Tokyo, Japan, October 1998
9. I.J. Cox and J.P.M.G. Linnartz, "Some general methods for tampering with watermarks", IEEE Journ. of Sel. Areas in Comm., Vol. 16. No. 4, May 1998, pp. 587-593.
10. J.P.M.G. Linnartz, "The ticket concept for copy control based on embedded signalling", ESORICS '98, 5th. European Symposium on research in Computer Security, Louvain-La-Neuve, September 1998, Lecture Notes in Computer Science, 1485, Springer, pp. 257-274.
11. Ton Kalker, Digital Video Watermarking for DVD Copy Protection, Proceedings of SPIE Multimedia Systems and Applications, 1999
12. Ton Kalker, Digital Video Watermarking for DVD Copy Protection, Proceeding of Erlangen Watermark Workshop '99, http://www.lnt.de/~watermarking, 1999
13. Bruce Schneier, "Applied Cryptography", Wiley, NYC, 1997