Some tools to Protect HDTV-Content against Piracy

DIEHL Eric

Security Domain Manager, THOMSON Corporate Research, Rennes (F)

1. Problems

Digitalization of contents and high definition video quality are formidable growth promoters for the audio-visual industry. But digitalization also increases the risks of piracy. Current high level of piracy suffered by phonographic industry perfectly illustrates this risk [6]. To preserve the interests of audio-visual industry, it is necessary to set up traceability and effective protection systems for HD content.

Content protection breaks up into two distinct problems:

- Access control
- Copy protection

Access control prevents watching contents without having paid the necessary rights. The broadcast world uses conditional access systems. The IP world uses Digital Rights Management (DRM). Conditional access and DRM have the same functional role. But their implementations are different. For example DRM assumes the presence of a back channel. This is not necessarily true for conditional access. For both cases, access control implies some form of monetization.

Copy protection prevents illegal duplication of contents. Thus the user may be authorized to watch content, but not to record it. It is already the case for some DVD or VHS titles which inhibit analog copy. To have a complete protection, the two approaches are mandatory and complementary.

Due to the complexity of the topic [9], this paper explores only the copy protection. Section 2 presents the basic techniques. Section 3 brushes a panorama of some existing solutions or under development.

2. Techniques

2.1. Copy management

The basic element is the Copy Generation Management System (CGMS). Traditionally, it uses four states:

- Copy free; in this state, copy is authorized without limitation.
- Copy once; in this state, one first generation copy is authorized. Nevertheless, this copy cannot be duplicated.
- Copy No More; in this state, copy is forbidden. A “copy no more” marked content is indeed a copy of “copy once” marked content.
- Copy never; in this state, content cannot be copied.

2.2. Basic technologies

Copy protection systems use four types of techniques:

- Encryption
- Watermarking
- Revocation
- Compliance rules

2.2.1. Encryption

Content encryption, hereafter called scrambling, applies to content a cryptographic algorithm of symmetric encryption [13]. Figure 1 illustrates its operation. Contents are scrambled using a primary key. To retrieve clear contents, it will be necessary to apply the decryption algorithm with the same primary key. It is thus essential that only authorized devices can access the primary key. This is the role of the key management. The key management protects the primary key by applying some cryptographic algorithms. It generates data that we will call the secondary key. Only authorized devices will be able to derive the primary key from the secondary key. Each copy protection system employs its own key management.

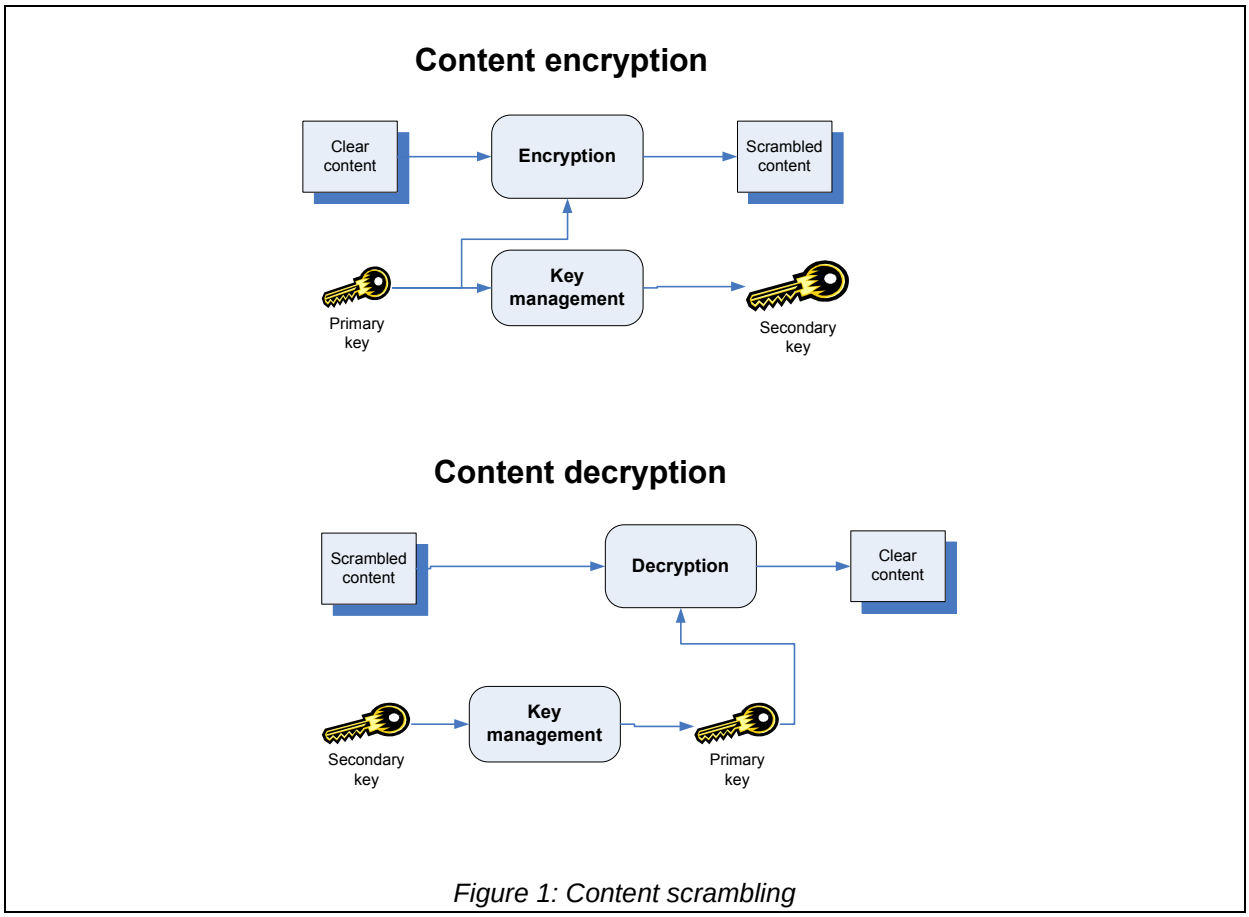

Figure 1: Content scrambling

Examples of encryption algorithm are DVB Common Scrambling Algorithm (DVB-CSA), AES [11] or DES [4]. For example, all DVB contents are scrambled using DVB-CSA. The primary key is called control word. The control word changes every 10 seconds. The control word is stored in an encrypted data structure called Entitlement Control Message (ECM). Conditional access's smart cards can decrypt ECMs and thus recover the control word. The smart cards pass back the control words to the decoders only if the user has the necessary rights.

2.2.2. Watermark

Image watermarking hides copy control information (CCI) within the image [10]. The principle of watermarking is to hide information of a message *m* by slightly altering the initial image C_o. This is the role of the watermark embedder. The watermark key enables to hide the message in a deterministic way. The result is a modified image C_w which carries message *m*. To be invisible, modification of the image takes into account the physiological characteristics of the human vision. A crude example is to use the less significant bit of the luminosity of pixels defined by the key. Human eye being less sensitive to luminosity, this alteration is not perceptible. Of course, modern watermarks are more sophisticated. Transmission of image C_w possibly introduced some noise. If noise is acceptable, the person will perceive an image that is "identical" to the original one. Nevertheless, an informed watermark detector, i.e. having the right watermark key, will be able to extract hidden message *m*. The same image may contain several hidden messages each using a different watermark key.

Watermarking is a complex tradeoff between invisibility, robustness against processing (voluntary or involuntary) and size of the hidden message *m*.

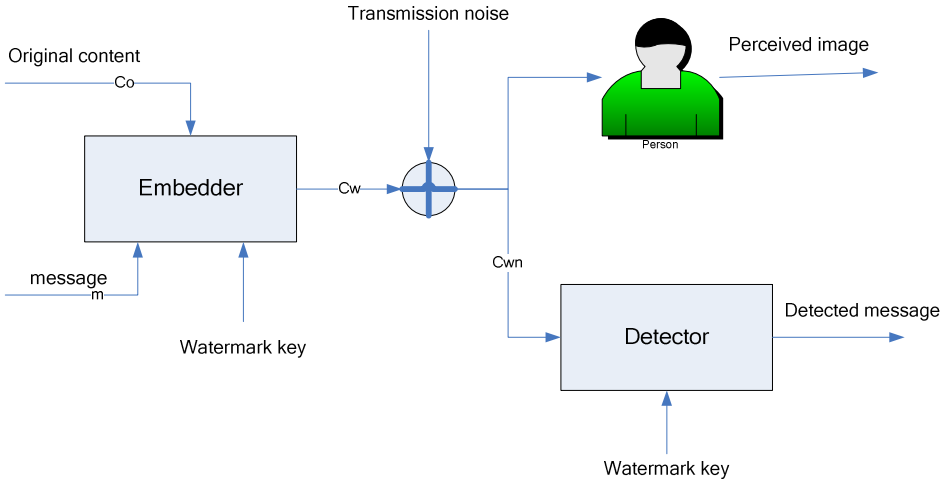

Figure 2: Watermarking content

The major interest of watermark is that it survives in the analog world. Encryption protects only digital data. But at the end, digital data must be rendered to analog world thus loosing the protection of encryption. Watermark carries the copy control information. Compliant analog inputs detect this watermark and react correspondingly. Thus, a digital recorder will refuse to record an analog content which would be watermarked as "copy never".

This use of watermark is different from the more frequent use as forensic tracking. In this latter case, watermark hides information identifying the original recipient of contents. In the event of illegal diffusion, it is possible to trace back the source of the leakage. Successive watermarks identify the transfer path.

2.2.3. Revocation

No security system is unbreakable. A good security system must survive to an attack. In some cases, revoking a device is sufficient. Two strategies are used to revoke compromised devices:

- Revocation list: each device receives the list of corrupted devices. A compliant device interacts only with devices that do not belong to this list. The installed devices must receive regular updates of this list.
- Broadcast encryption [12]; this family of key management is more recent. A central authority delivers a set of keys to each device. The transmitter defines the list of the devices authorized to access content. Broadcast encryption builds a data structure called Key Block. A device pertaining to the authorized list will find the primary key by applying a mathematical calculation using its set of keys and Key Block. Devices that do not belong to the authorized list will not find the primary key using the same mathematical calculation. The key management both protects the primary key and manages the revocation. Content itself defines the devices that will be able to access it. Broadcast encryption avoids sending revocation lists.

Unfortunately, revocation does not answer all attacks. For instance, some attacks may circumvent the revocation mechanism. The only effective answer is complete renewal of the security mechanisms. This can be done either by new software version uploading or by renewing removable secure tokens such as smart cards.

2.2.4. Compliance rules

Compliance rules enforce the respect of some constraints. These rules define device's behavior. For example, they can mandate the presence of watermark detector on analog inputs. Some copy protection systems assume that a recorder receiving copy never marked contents will refuse to record. Compliance rules will guarantee this behavior. Compliance rules require legal binding. Thus, they are often annexes of technological licenses.

3. Families of solutions

3.1. Protecting storage units

The objective is to prevent illegal duplication of stored contents. Traditionally, there are two types of attacks:

- Accessing stored content using a pirate system
- Making bit to bit copy

The traditional response to the first attack is encryption. Only compliant devices have the secrets needed to decrypt content. The security hypothesis is that a non-compliant device has not access to such secrets. This hypothesis was wrong for the protection system of the DVD (Content Scramble System). The pirate software mimics the CSS key management.

There are three responses against bit to bit copy:

- "Copy never" marked contents on a recordable medium are regarded as illegal. A compliant device will not play them.
- Content diversification; In this case, contents are cryptographically linked to the support. Traditionally key management uses a unique identifier of the support as additional parameter. Thus, the secondary key is unique for each support.
- Certain parts of the recordable disc cannot be burnt nor modified by the recorder. In this case, the copy protection system uses this space to store critical data. Compliant recorders will not be able to mimic it.

There are two new generation of pre-recorded medium: Blu-Ray Disc Copy Protection System (BD CPS) for Blu-ray DVD [2], and Advanced Access Content System (AACS) [1]. Both systems employ broadcast encryption for key management and AES to scramble content. The disc contains two types of information: contents scrambled by AES with a primary key and information necessary to calculate the primary key. Among this information is the table of revocation. Each player holds a unique set of keys. The table of revocation is built so that all the non revoked readers find the same value by using this table. On the other hand, a device having a revoked key will find another value. The good value is used to decrypt the primary key. Only the non-revoked devices can find the primary key which scrambles the contents of the disc.

3.2. Protecting the bus

The main objective is to prevent that the receiving device makes an illegal copy. The second one is to avoid theft of content through eavesdropping the communication link. The solution is scrambling content during transfer between the two devices. The two devices mutually authenticate. This authentication guarantees their compliance. Only compliant devices have the secrets necessary for authentication. These secrets are delivered by a certification authority. Once authenticated, they establish a common session key. The transmitter scrambles contents to be sent with this common key. The receiver descrambles received contents with this same key and acts in compliance with the copy control information of the content. The compliance rules define the expected behavior of the receiver.

It is important to include the difference between copy protection of a bus and its security. Indeed, security of a bus ensures only confidentiality and integrity of the message. Thus, it only answers the second requirement. For instance, IPSec guarantees the security of the contents during transfer on an Ethernet bus [3]. But IPSec does not guarantee the target does not make a copy of “copy never” marked content. IPSec does not define the test of copy conditions. First requirement is not fulfilled. Copy protection defines the behavior of transmitters and receivers according to the copy mode. The most known commercial solutions are Digital Transmission Copy Protection (DTCP) and High Definition Copy Protection (HDCP) [7]. DTCP protects compressed contents over Ethernet, IEEE1394, USB or MOST [5]. HDCP protects uncompressed contents over Digital Video Interfaces (DVI), or Multi-media High Definition Interfaces (HDMI).

We will detail HDCP. As indicated by Figure 3, authentication is the first step. HDCP Transmitter checks that the receiver is authorized to receive HDCP protected contents. According to a principle similar to broadcast encryption, each entity has a table of 40 private keys (noted *KSV*) and a single identifier. Transmitter A sends its identifier A_{KSV}. Receiver B returns its identifier B_{KSV}. Transmitter A checks that B_{KSV} is not revoked. The receiver must have the most recent revocation list. Now the transmitter A knows that B is a compliant HDCP receiver. They establish a common session key K_m. Each device uses its table KSV and the other device’s identifier to calculate K_m. Thus, each device can

find K_m without exchanging it over the bus. Only the devices having a valid table can establish a common key. B encrypts a random value R_0 with key K_m. B sends R_0 and the computed value to A which checks that they match. A has the proof that B is authenticated and that they share the same key. The encrypted transmission can begin. Scrambling is a basic stream cipher. The contents are bit wise xored with the output of a pseudo random generator. Receiver B performs the same operation. In the case of HDCP, there is no test of copy conditions because the compliance rules enforce that receiver cannot record received contents.

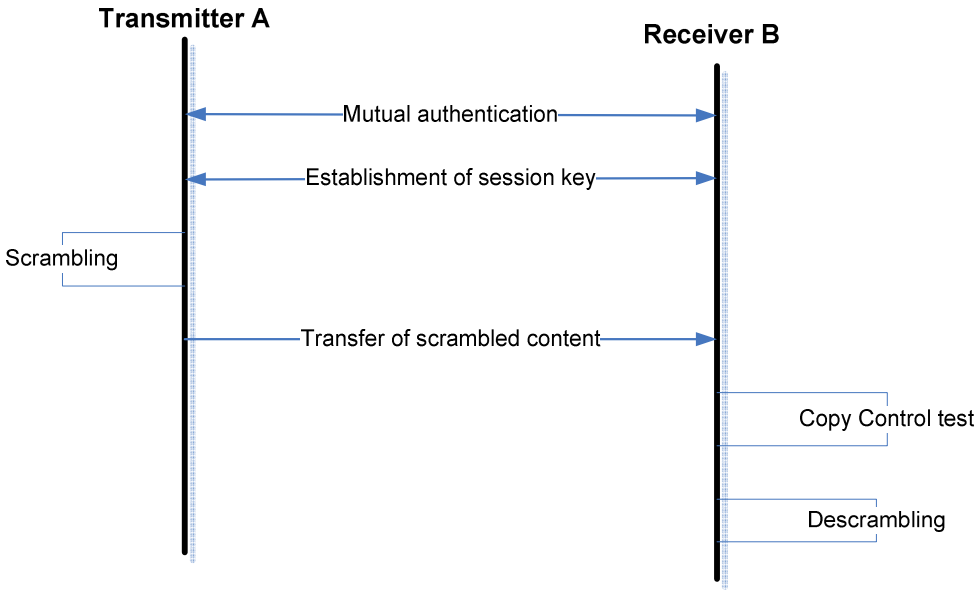

Figure 3: HDCP key management

3.3. Authorized domain

Recently, a new copy protection approach has taken into account the advent of digital home networks. Thus, DVB Copy Protection group defined the concept of authorized domain. The authorized domain is the set of devices belonging to a same family. It includes devices of the main residence, the second home and the portable devices. Within this domain, devices must be able to transparently access contents. One of the main advantages is the concept of private copy. Within the same authorized domain, it is possible to make an unlimited number of copies. But these copies are only usable in this domain. An effective implementation of the copy for private use is thus possible. Two systems propose such solution: SmartRight and xCP. SmartRight uses an approach similar to conditional access with smart cards. xCP uses broadcast encryption.

One of the major difficulties is the management of the authorized domain. The authorized domain is in constant mutation. New devices are added. The portable devices are not permanently connected. Moreover it is necessary to limit the domain to a reasonable size. This management must be transparent to the user. It is necessary to respect user's privacy. This list of requirements is not exhaustive.

For SmartRight [8], contents enter digital home network protected by Conditional Access Systems or DRM. The SmartRight system protects content within the digital home network. The contents are scrambled for example by AES. Only the television sets will descramble them. The descrambling key (or primary key of Figure 1) is protected by a network key common to all the devices from the same digital home network. The smart cards establish and manage this common network key as well as the protection of the descrambling keys. A card of Alice's authorized domain cannot descramble contents of Bob's authorized domain. Indeed, it does not have Bob's network key and it cannot thus reach the primary key.

Figure 4: SmartRight system

The SmartRight key management has the following characteristics:

- The size of the authorized domain is limited
- The authorized domains are isolated and cannot exchange contents
- The management of the authorized domain respects privacy because it does not require a back office
- The management of the authorized domain is transparent to the user.

Authorized domain based copy protection systems are more complete systems. They protect content within the storage units and on bus transfers. Other approaches require to associate several copy protection systems.

4. Conclusion

The protection of copy is essential to preserve the interests of audio-visual industry. Technical solutions appear. The range of protection starts from the protection of the physical support to the copy protection of a complete digital home network. Research in the field of the High Definition copy protection must be directed towards two axes. First one is commercial. It is necessary to find new methods of copy protection which reconcile the interests of content owners and users. The second axis is technical. One of the most important challenges is the renewability of the copy protection system once deployed

5. References

[1] http://www.aacsla.com/

[2] http://www.blu-ray.com/

[3] http://www.ietf.org/html.charters/ipsec-charter.html

[4] ***Data Encryption Standard***, NIST, 1991, FIPS 46-3, available at http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[5] ***Digital Transmission Content Protection white paper***, available at http://www.dtcp.com/data/wp_spec.pdf

[6] ***Commercial Piracy Report 2004***, July 2004, available at http://www.ifpi.org/site-content/library/piracy2004.pdf

[7] ***High-bandwidth Digital Content Protection specifications***, rev 1.1, 2003 available at http://www.digital-cp.com/data/HDCPSpecificationRev1_1.pdf

[8] ANDREAUX J.P., DIEHL E., DURAND A., FURON T., ***SmartRight a copy protection scheme for Digital Home Networks,*** IEEE Signal Processing, March 2004

[9] CHANTEPIE P., HERUBEL M., TARRIER F., ***Mesures techniques de protection des oeuvres et DRMs***, Janvier 2003, Ministère de la culture et communication, available at

http://www.ddm.gouv.fr/rubrique.php3?id_rubrique=88

[10] COX I., MILLER M., BLOOM J., ***Digital watermarking,*** Morgan Kaufmann Publishers, 2002

[11] DAEMEN J., RIJMEN V., ***The Design of Rijndael AES The advanced Encryption Standard***, SPRINGER, 2002

[12] Fiat S., Naor M., ***Broadcast encryption***, in advances in cryptology, Crypto '93, Lecture Notes in Computer Science 773, pp. 480-491

[13] Schneier B., ***Applied cryptography***, 2nd edition, John Wiley, 1996