CONTENT PROTECTION TECHNOLOGIES FOR CONSUMER EQUIPMENTS

Serkan EMEK serkan.emek@digiturk.tv
DigiTurk, Digital Platform İletişim Hizmetleri A.Ş., 34353, Beşiktaş, İstanbul
YTÜ FBE Elektronik ve Haberleşme Müh., Haberleşme Doktora Programı , Yıldız, İstanbul

ABSTRACT

Digital piracy is most important problem for multimedia services because of tremendous development of new IT technologies. There is no one solution to the challenge of digital piracy. There is today a robust and growing market for content protection systems, and a number of technologies have been developed and implemented, or are available for implementation.. In this work, we give a brief about current copy protection technology and effects of technology for consumer equipments as well as new STBs, DVRs, PVRs, DVD players and recorders, VCRs, DV Camcoders.

1. INTRODUCTION

The success of the Internet, cost-effective and popular digital recording, storage a and player devices, and the promise of higher bandwidth and quality of services for both wired and wireless networks have made it possible to create, replicate, transmit, and distribute analog and digital content in an effortless way. The protection and enforcement of intellectual property rights for analog and digital media has become an important issue. To provide copy protection and intellectual property rights for analog and digital content on the recorders, two primary goals are described:

- Plugging the "analog hole" that results from the fact that protected digital content can easily be converted into analog form and then reconverted to unprotected digital form, making it subject to widespread unauthorized copying and redistribution.
- Putting an end to the avalanche of copyright theft on so-called "file-sharing" services on peer-to-peer (p2p) networks.

Their treatment here is not a listing in order of priority, but rather reflects the current status in terms of progress toward the realization of these goals. The attainment of each of these goals is needed in order to construct an overall framework for content protection in the digital environment [1].

2. PREVENTING ANALOG RECONVERSION

The "Analog Hole" is a term used to describe a gap in protection that exists in digital content protection systems by virtue of the fact that digital content protection systems can generally protect content against unauthorized reproduction and distribution only in a digital environment. If protected digital content is converted to analog format these content protection mechanisms are eliminated or reduced. This presents a problem in that digital devices can capture and digitize unprotected analog signals with complete disregard for current copy protection mechanisms, thus enabling a major source of unauthorized duplication and/or redistribution. Such analog to digital conversions are easy to accomplish with the use of widely available, inexpensive PC technology and other digital recording devices with analog inputs.

2.1. WATERMARKING

The primary means to address the analog hole is via embedded watermarks Watermarking is a type of Copy Control Information (CCI) marking system. These systems allow usage rules to be conveyed with the content. Watermarking technology in particular allows for copy control information to be invisibly and securely embedded in the content, as well as markings to be embedded for forensic tracking purposes. Such watermarks are persistent and robust in that they survive the digital-to-analog conversion process and they are not easily removed.

In order to help plug the analog hole, watermark detectors would be needed in all new consumer equipments that perform analog to digital conversions. In such devices, the role of the watermark detector would be to detect the watermark and ensure that the device responds appropriately. The watermark would instruct the conversion device never to allow copying, allow only one copy, allow first generation copying but not serial copying, or to allow unlimited copying. Extended Copy Control Information (ExCCI) packet uses in both analog and digital video signals that would allow even more flexibility in the content usage information that could be conveyed via watermarking and other CCI marking systems

The realization of watermarking as a vehicle in plugging the analog hole has two steps:

1. A robust watermarking technology must be selected,
2. Compliance and enforcement rules for detection and response to this technology in various platforms must be drafted and agreed upon.

2.2. COPY GENERATION MANAGEMENT SYSTEM

Another form of CCI marking system is the Copy Generation Management System (CGMS). CGMS comes in two flavors: CGMS-A for analog output, and CGMS-D for digital. Unlike the APS, which is most often used to prevent copying by analog VCRs, CGMS-A is intended for digital devices like digital video recorders (DVRs), and DV camcorders. CGMS-A is a technology standard that allows a set of pulses to be applied to lines in the vertical blanking interval of an analog video signal to convey copy control information. Thus, CGMS-A technology allows such information to be conveyed with the content, but unlike watermark technology, does not allow for such information to be securely embedded within the content itself.

The system works by storing two bits of CGMS Copy-Control Information (CCI) in the header of each disc sector. Compliant players read and embed this data into audio and video output, and compatible recorders use it to determine access and copying privileges. CGMS-D has not yet been fully defined, and may ultimately be absorbed into other content-protection technologies. But in either case, it'll most likely be used to protect the digital outputs of devices like DVD recorders, DVRs and digital TVs.

In video streams, CGMS-A embeds CCI into the Extended Data Services (XDS) of line 21 of the NTSC video signal. The value of the CGMS CCI tells compliant downstream recording devices whether they can copy the signal without constraint (bits set to 00), record one generation of copies (01), or make no copies at all (11).

2.3. ANALOG COPY PROTECTION SYSTEM

All new consumer equipments are required to support an Analog Protection System that prevents copying by analog VCRs. The ACPS incorporated into about 75% of all DVD-Video discs is the Macrovision Copy Protection (MCP) system, which is an enhanced version of the technology long used to protect videotapes. MCP employs two techniques that exploit the differences between video recorders and players. Either or both mechanism can be implemented at the discretion of content owners. First, the system can add carefully timed pulses (Pseudo-Sync Pulses or PSPs) to a video signal's Vertical Blanking intervals. These confuse the Automatic Gain Control (AGC) circuitry built into nearly all video recorders, resulting in unstable recordings marred by tearing, intermittent video, noise, dimness, or color loss. They don't, however, affect the AGC circuits designed for television sets, which react slowly enough to ignore the pulses. This approach can theoretically protect against copying by both VCRs and digital recorders. It works about 85% of the equipment currently in use.

The system also offers Colorstripe technology, which produces rapidly modulated colorburst signals that confuse the chroma-processing circuitry in NTSC VCRs. This function inverts the phase of the first half of the colorburst signal on certain scan lines (a technique known as "split-burst operation"). This modification can take place on four-line blocks that occur every 21 lines, beginning at lines 24 and 297 or on pairs of adjacent lines that occur every 17 lines, starting at lines 30 and 301 (known as a two-line split-burst). Colorstripe-protected tapes play normally on a TV monitor, but attempting to copy them results in a recording marred by horizontal stripes or other types of artifacts.

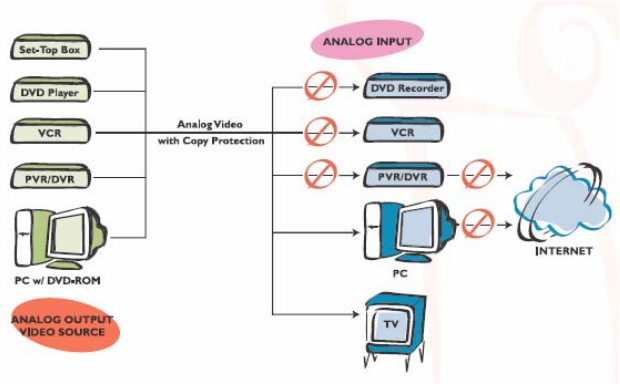

Figure 1. Analog Copy Protection System [2]

The MCP system is usually transparent to the user and difficult to defeat, but it isn't foolproof. The technology can cause problems with some high-end TVs, and won't prevent copying by some older VCRs. Despite all this, the MCP system continues to be one of the most successful copy-protection technologies on the market. It discourages the overwhelming majority of viewers from casual copying, and usually does so without affecting the quality of legitimate recordings [3].

3. KEEPING DIGITAL CONTENT WITHIN A PROTECTED ENVIRONMENT

Much work is being done to develop technological systems and architectures intended to create a secure environment for the distribution of digital content and to limit the sources of unauthorized content on p2p networks. Preventing analog reconversion through the use of watermark or other CCI marking system technology is another important effort aimed at ensuring that consumer devices with unprotected analog outputs do not continue as a long-term source of pirated content on p2p networks. A host of other technologies are available or under development -including encryption, authentication, conditional access, link protection, digital watermarking/CCI marking, and digital rights management technologies -that are intended to fit together in an overall framework that allows for the secure delivery of digital content to the home and

persistent protection against unauthorized access and redistribution once the content is delivered.

3.1. CONTENT PROTECTION SYSTEM ARCHITECTURE

One such model is the model of a "link-protected" architecture in which encryption, authentication and watermarking technologies are combined with licensing agreements to create a framework in which content is encrypted and transmitted digitally only via protected outputs and only to devices that are bound to provide a minimum level of persistent protection and, in some cases, to respond to usage rules conveyed by associated watermarks. This framework, called the Content Protection System Architecture (CPSA). CPSA is applicable to both computer and consumer-electronics devices, as well as to audio and video content in either analog or digital formats. CPSA guidelines also apply to technologies that protect streaming content, such as DTCP, HDCP, and Conditional Access, which safeguards PPV programming distributed via satellite or cable.

CPSA-compliant technologies can incorporate two types of content-protection mechanisms: digital watermarking and encryption. Watermarking embeds copy-protection information, which known as a "watermark", directly into an audio or video stream. Watermarks usually contain usage rules known as Content Management Information (CMI), which specify how the content's owner will allow his property to be accessed, played, or copied. This embedded data is intended to be transparent to the consumer, but is detected by the compliant hardware or software modules that enforce the system. If a content owner doesn't want to risk degrading content with a watermark, CPSA also allows CMI to be packaged as a discrete piece of data that accompanies, but is not embedded into, the content. The lock that enforces such a system in the digital domain is encryption, which scrambles content until it is decrypted by a compliant device, according to the rules specified by the CMI [4].

3.2. CONTENT SCRAMBLING SYSTEM

Like many content-protection technologies, CSS employs an authentication-and-encryption methodology. Such systems scramble content to prevent unauthorized copying and specify a two-stage playback process that requires a pair of compliant devices to authenticate each other before they can decrypt protected content. Authentication requires that a drive and a downstream device or a host device verify that both are legally licensed to use the copy-protection system. This is done by exchanging and comparing secret data that is stored in content, embedded into the devices or player software, or calculated using algorithms released only to licensees. The subsequent playback process consists of the sector-by-sector decryption of the stored content or, if streaming data is being protected, the encryption, transmission, and decryption of each frame. This task employs keys and special values that are exchanged or calculated during the authentication process.

3.3. CONTENT PROTECTION FOR PRERECORDED MEDIA

Regardless of the motivation, the CPTWG once again provided a platform to discuss a next-generation "CSS2" copy-protection scheme. The final result was industry-wide support of a 4C-developed technology called Copy Protection for Prerecorded Media (CPPM) and its related Copy Protection for Recordable Media (CPRM). Both employ what are essentially elaborations of the multi-key authentication-and-encryption methodology described by CSS.

Unlike the video-oriented CSS, CPPM is currently used only to protect prerecorded DVD-Audio content stored on either Audio DVDs or on mixed DVD-Audio/Video discs. Because its authentication procedure is so much like that of CSS, it can be added to DVD-Video and DVD-ROM players at little cost. But despite the similarities, CPPM is far more robust than CSS. CPPM also differs from CSS in other ways. It hides copy-control information in every encrypted sector, allowing content providers precise control over which sectors can be copied. Instead of CSS' Title Keys and Disc Key, it places an Album Identifier in a hidden area on each protected side of the disc. It replaces the CSS' single Player Key with a set of 16 secret Device Keys issued to every licensed manufacturer of hardware or software players. Most importantly, it employs more robust 56-bit encryption (based on the C2 Cipher algorithm) and can generate a new encryption key on the fly for every sector of data. CPPM-protected discs also contain a Media Key Block file that stores a table of encrypted key values. In order to unscramble a disc sector, a player must perform a complex sequence of mathematical operations that extract a Media Key from the MKB, and then combine that key with the Album Identifier to create a base decryption key. The final sector-specific decryption key is created by modifying this base value with data stored within the sector.

3.4. CONTENT PROTECTION FOR RECORDABLE MEDIA

CPRM differs from CPPM by binding copyrighted recordings to physical media. It allows discs to be recorded and played back on different drives, but does not let protected content be copied indiscriminately to another piece of media. In addition to a CPPM-style Media Key Block and Title Key, every writable-DVD blank contains an indelible 64-bit Media ID embossed into a hidden area of the disc. This Media ID specifies the type of media and its manufacturer, and also includes a 40-bit serial number that uniquely identifies the disc.

Because it can't be physically altered, the Media ID doesn't need to be kept secret.

When users copy protected content onto a disc, CPRM encrypts it with a multi-stage process that uses the Media ID to generate encryption and decryption keys. Simply copying recorded files to another piece of identical media prevents them from being properly decrypted because the second disc will have a different Media ID. As complex as they are, CSS, CPPM, and CPRM aren't designed to protect analog output signals. If they were the only security mechanisms available, content could be easily copied by routing a DVD player's analog output to any VCR, writable DVD, PC sound or graphics board, audio tape deck, or any other recording device equipped with analog inputs [5].

3.5. CONDITIONAL ACCESS SYSTEM

Content delivered over cable and satellite is protected by Conditional Access (CA) technologies that encrypt content and route to the home. Although it is transmitted to the home across a generally unsecured transmission infrastructure, the content remains protected because it is encrypted. Devices such as a set-top box must be licensed to receive the key necessary to decrypt the content [6].

3.6 DIGITAL TRANSMISSION CONTENT PROTECTION

Content owners have always been especially concerned about the digital outputs of DVD players, since a pirate who hijacks a digital data stream can create an unlimited number of perfect copies. The technology most commonly used to guard against this is the Digital Transmission Content Protection (DTCP), which safeguards data streams transmitted over digital interfaces like IEEE-1394 and USB. DTCP can be used to protect DVD content only if it has already been encrypted by CSS, CPRM or CPPM. Before such data can be transmitted through a digital output, the sending and receiving devices must first perform a joint authentication procedure. As with other CPSA-compliant technologies, authentication consists of a sequence of data swaps and key calculations that validate the licenses of both devices. This is intended to prevent pirates from inserting a circumvention device that would record the subsequent data stream or strip out its copy protection.

Compliant devices determine which access and copying activities are legal by examining two bits of Copy Control Information (CCI) transmitted with each packet of protected content. These bits can define four possible copy-protection states: "copy one generation" (CCI=10), "copy freely" (CCI=00), "copy never" (CCI=11, for original content that cannot be copied), and "no more copies" (CCI=01, which specifies that the content is a first-generation recording that can't be copied again) [7].

3.7. HIGH-BANDWIDTH DIGITAL CONTENT PROTECTION

IEEE-1394 does a good job of transporting compressed MPEG-2 video. But its 400-Mbps bandwidth is insufficient for high-resolution digital displays like flat-panel computer monitors and HDTVs. A better solution is the blazingly fast Digital Video Interface (DVI) protocol.. With a maximum bandwidth of 4.95 gigabits/second, DVI is fast enough to support computer-monitor resolutions up to 1,600 x 1,200 (or 2,048 x 1,536 in a dual-link configuration), as well as all popular HDTV formats.

Despite the rapidly dropping price of high-definition video equipment, the movie industry was reluctant to support the format unless DVI could be secured against unauthorized access and copying. This was accomplished to release the High-definition Digital Content Protocol (HDCP) specification. When layered on top of DVI, HDCP provides a secure connection between a video host device like a DVD player, set-top box, or DVI-equipped PC, and a downstream digital display or video receiver. It can also link a host to a repeater module that distributes a single video stream to multiple downstream devices.

HDCP describes a three-phase authentication and key-exchange procedure that requires each device to be identified by a secret 40-bit Key Selection Vector (KSV) and an array of forty secret 56-bit Device Keys. Each bit in the KSV corresponds to one of the forty Device Keys, and every compliant device is required to permanently store both data elements in a secure internal location. KSVs and Device Keys are generated and issued to manufacturers by Digital Content Protection, LLC, which licenses HDCP to manufacturers [8].

Table1. Copy Protection Effect Tables

TCHNLGY DEVICE	CSS CSS2	CGMS	ACP	WMK
VHS VCR	n/a	n/a	effective	effective
STB	n/a	effective	effective	effective
DVD REC	effective	effective	effective	effective
DV CMCR	n/a	effective	effective	effective
DVR \ PVR	effective	effective	effective	effective
PC	effective	effective	effective	effective

3.8. DIGITAL RIGHTS MANAGEMENT

Similarly, other software-based digital rights management (DRM) technologies have been and are being developed to provide for secure delivery of content over the Internet and adherence to copy control instructions and usage rules in the PC and home-network environments.

While DRM technologies may provide for secure delivery of digital content to the PC and home network environment, the existing PC architecture leads to a

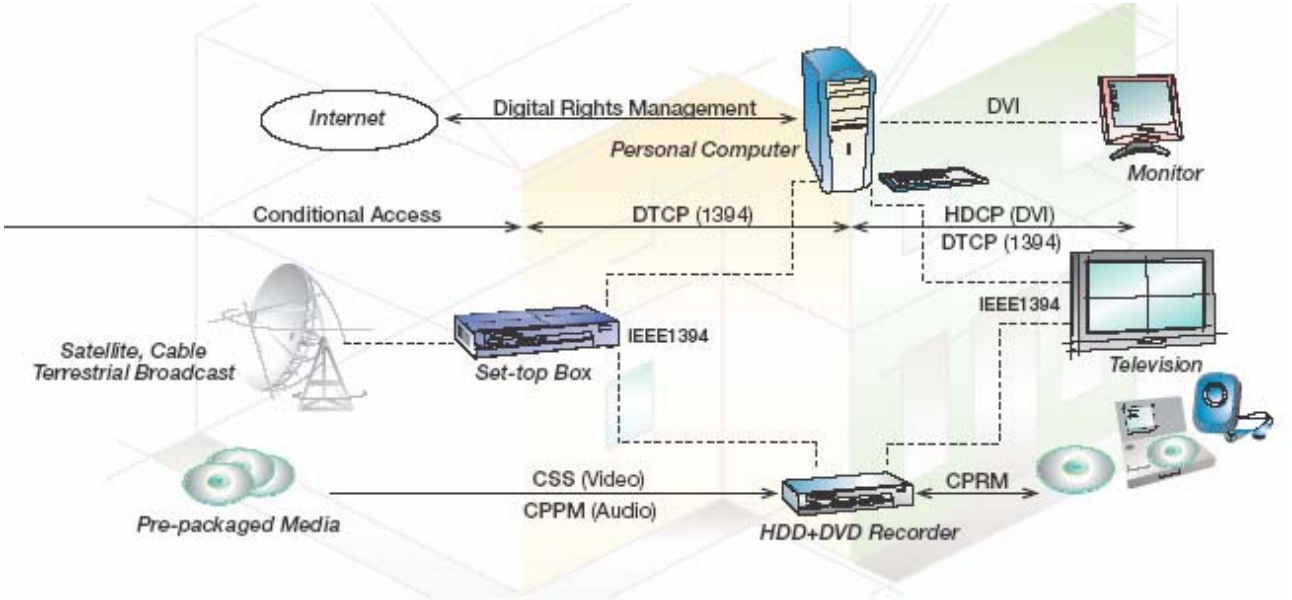

Figure 2. End to End Copy Protection System [9]

number of vulnerabilities that may expose such content to unauthorized access and redistribution once it arrives at its destination. For example, because the PC is user programmable, it is possible to install and run circumvention utilities and non-compliant "hacked" software media players that can circumvent the technological protections or the usage permissions associated with copyrighted audiovisual content. Moreover, software-based DRM systems are more vulnerable to security breaches than are hardware-based systems as software-based DRM system must rely on tamper resistant software techniques to prevent circumvention by end-users_ Even protected content may be exposed to unauthorized copying and redistribution whenever it passes over user-accessible buses or when transmitted over unprotected outputs to displays. These vulnerabilities have led to an increased focus on trusted computing technologies, or technologies that are intended to combine hardware (such as smart cards and silicon chips) and software solutions to provide a secure trusted platform for exchanging digital content and information [10].

Finally, one of the biggest sources of pirated movies on p2p networks is the big screen itself. All too often movies appear on p2p networks while they are still in the theatres because someone has simply gone into the theatre with a camcorder and recorded the movie directly from the screen. In some cases these individuals use sophisticated digital recorders and plug directly into the audio sources provided for the hearing impaired -or even the theatre's sound system itself -to produce a high quality camcorder version of the movie. That copy is then uploaded to a computer, digitally compressed, and redistributed to the world using p2p technology.

4. CONCLUSIONS

In this document, we will describe the goals of content protection and explain to solution to reach these goals. There is no one solution to the challenge of digital piracy. Depend on the Table 1, watermark solution seem to be acceptable both parties but it also needs to agree on compliance and enforcement rules. As a result, there is today a robust and growing market for content protection challenges posed by the growth of virtually unchecked and wholly unauthorized viral distribution of copyrighted works via digital networks.

5. REFERENCES

1. Comments of Motion Pictures Association of America "Technological Copy Protection Systems for Digitized Copyrighted Works", Jan 14, 2003.
2. MacroVision, "Is there leak in your DVD Copy Protection Strategy", 2005.
3. MacroVision, "Preserving an Effective DVD Copy Protection System", 2003.
4. Don Robliola, "Digital Content Protection", Broadcast Engineering May 2002.
5. http://www.4centitv.com/tech/cprm/
6. H. Benoit, "Digital Television, MPEG-1, MPEG-2, and Principles of the DVB System", J.W. Arrowsmith Ltd., 1997.
7. http://www.dtcp.com/data/wp_spec.pdf
8. High-bandwidth Digital Content Protection System, Intel Corporation, Feb 2000.
9. Protecting Content in the Digital Age, Intel Corporation, 2002.
10. http://www.digital-cp.com/