SECURITY AND RIGHTS MANAGEMENT IN DIGITAL CINEMA

Jeffrey A Bloom

Sarnoff Corporation, Princeton, NJ

ABSTRACT

This paper provides an overview of Digital Cinema including some of the architectural ideas that have been proposed and are being considered. There are a number of security tools that can be used with the goal of secure delivery of motion picture content to the projector. There are many technical and business constraints that guide these designs. Independently, there have been a number of efforts in the watermarking community to attach forensic tracking information to the motion picture content. Such information would provide persistent tracking beyond the projector and would be useful in identifying compromised equipment.

1. INTRODUCTION

Traditionally, motion pictures have been physically distributed on film and shown in movie houses around the world with film projectors. However this paradigm is about to change. Movies can now be digitized and exhibited on new digital projectors similar (in concept) to those used to project computer presentations. The new projectors have the ability to project high-resolution imagery to a screen over 100 feet away. Together, distribution of a motion picture in a digital format along with the use of a digital projector is called *Digital Cinema*.

In this paper we first provide an overview of digital cinema and some likely architectures and then discuss some tools that will be employed in assuring the security of the motion picture content. Note that this order of presentation is, in fact, backwards. Security is one of the fundamental issues driving the design of the architecture.

There are a number of advantages and disadvantages of digital cinema over film-based cinema. In this paper, we focus exclusively on the security aspects.

Digital movies can be duplicated without loss. This increases the quality of the movies delivered to the theater, but also increases the quality of an illicit copy. Digital movies can be protected with encryption so that even if a pirate gains access to a digital movie and is successful in making a copy, that copy has no value without the appropriate decryption key.

The technical problem of assuring that a digital movie is only played at authorized times, by authorized operators, on authorized equipment is only part of the problem. Movies are a business and any security system must not interfere with the ability of the theaters to exhibit movies and must not detract from the paying consumer's experience.

For example, a set of potential solutions involves the use of a third party *authority* that must be contacted and coerced into releasing a decryption key for each showing. This allows the possibility that, should the network go down or the server become unreachable (not an inconceivable event), the theater owner will have a room full of paying customers and a dark screen. Needless to say, theater owners (as represented by the National Association of Theatre Owners) would not support such a security scheme [1].

There are a number of groups very active in addressing this issue of security in digital cinema. Perhaps most notable is SMPTE DC28.4W: the Society of Motion Picture and Television Engineers, Working Group on Content Protection and Conditional Access for Digital Cinema.

2. DISTRIBUTION – PHYSICAL OR ELECTRONIC

There are a number of possibilities for distributing digital movies to theaters. The approach that would require the least change to the existing infrastructure would be the use of curriers to transport the digital films on a physical media. This would mimic the current practice of using curriers to transport the cans of film.

In order to examine what form of physical media would be appropriate for transportation of digital films, let us consider a simplified example. This will give us a ballpark appreciation for the amount of storage necessary. Consider a movie stored at 24 frames per second with each frame 1280 columns by 1024 rows and each pixel stored with 10 bits each of red, green, and blue. A two-hour movie would require almost 800 Gigabytes plus maybe 10% audio. But clearly, this digital movie will be compressed. Current expectation is that a two-hour movie can be compressed down to the range of 50-100 Gigabytes while still maintaining sufficient fidelity. This compressed movie can then be distributed on a stack of DVDs (using all 4 layers, current DVDs can hold about 16 Gigabytes each) or on a removable hard drive.

Alternatively, the movie can be distributed electronically. The digital data can be transmitted point-to-point over a coaxial or fiber optic cable or it can be broadcast from a single distribution point to many receivers via satellite. In November 2000, Boeing Digital Cinema compressed the Miramax film "Bounce" to 51 Gigabytes and transmitted it via satellite to Empire Theatre in NYC. Since then, they claim to have presented more than 10,000 screenings of satellite-delivered content [2].

3. SYSTEM ARCHITECTURE

Whether by physical media or by electronic transmission, a digital cinema theater will receive a copy of the digital movie file. This file, referred to as the Digital Cinema Distribution Master (DCDM), will likely be stored on a server in the theater. At exhibition time, the Master will be decompressed and transmitted to the projector. Alternatively, the decompression may take place inside the projector. This second scenario allows for a lower bandwidth transfer from the server to the projector and offers the potential for improved security [3].

The system must have security measures in place to prevent unauthorized access to the movie data. The primary tool for this is encryption, discussed in Section 4. Another useful tool, one that does not prevent theft but rather discourages thieves with the promise of capture, is watermarking, discussed in Section 5.

4. ENCRYPTION

The mainstay of information security is encryption. And here too it will play a critical role. En route to the theater, the movie is vulnerable to theft. In order to decrease the value of this stolen movie, it can be encrypted prior to distribution. In addition to stealing the movie, the thief now must also either decipher the movie without a decryption key or steal the key. There exists encryption technology sufficient to withstand the former (although there are often business and political reasons for choosing weaker encryption, as was the case with DVD encryption, but that's a story for another venue), and the latter becomes a problem of key management (as it always does) and tamper-resistant hardware and software.

The DCDM will be stored in its encrypted state in the theater, probably until showtime. Then it must be decrypted and decompressed. This decryption/decompression may take place in the server or in the projector itself. If in the server, then the uncompressed movie must be encrypted again for a safe journey to the projector. This encryption, protecting the data while in transit from one processing stage to the next, is called *link encryption*.

4.1 General DRM Tools

In a gross oversimplification of functionality of general DRM technologies we state that DRM tools encrypt an object and only allow decryption (provide the key) when a set of rules has been satisfied. Rules might be related to proof of payment, user authorization, or authentication of a connected device. Other rules might allow for additional content to be added to the object and additional rules to be required. Rules specify the actions that are permitted (decrypting, transferring, copying, editing, etc.), the people authorized to perform these actions, and the conditions under which these actions are permitted.

These rules can be expressed in a *rights management language*. There are a number of such languages including XrML (extensible rights markup language), XMCL (extensible media commerce language), and ODRL (open digital rights language). MPEG-21 Part 5 is one activity targeted at establishing a standardized Rights Expression Language (REL) [4].

In addition to rules, a DRM system needs a secure environment in which to execute [5]. Some typical capabilities of a DRM infrastructure include the ability to interpret the rules, gather enough information to determine if the rules are satisfied, arrange for payment, obtain authorizations from a third party, and obtain decryption keys. All of this must be done securely.

5. WATERMARKING

A second, yet less mature tool that may be useful for addressing security needs in digital cinema is watermarking. Watermarking is a technique for representing metadata by modifying the pixel values (color or brightness) or the audio samples of a movie such that the changes are imperceptible to the audience. A watermark embedder performs this modification, usually with the aid of a perceptual model. A watermark detector is capable of extracting the metadata from the modified movie. The basic principles behind watermarking, as well as a number of techniques and examples, can be found in [6].

5.1 Robustness and Fragility

Watermarks are often designed to survive a number of expected processes, including compression or transcoding, filtering, noise removal (or addition), etc. Some watermarking techniques seek robustness to geometric and temporal distortions such as changes in spatial scale, rotation, translation, perspective distortions (keystoning), changes in aspect ratio, changes in playback speed, and cropping. At the extreme end, watermarks have been proposed that survive exhibition, recapture by camcorder, reduction in size, and severe compression (as might be found shared on a peer-to-peer network). See for example [7, 8, 9].

Alternatively, some watermarks are designed not to survive any of these processes. *Fragile* watermarks become undetectable after processing. This can be used as an indication that the movie may have been modified since the watermark was embedded or it can be used as a "ticket" that allows a certain process to occur. This ticket is easily removed by slight modification of the movie.

5.2 Informed vs. Blind Detection

One issue of interest in watermarking technologies is the requirements of the detector. Some technologies require that the detector have access to the original, unwatermarked movie, or some important part of it, in order to extract the metadata. This process, called *informed detection*, typically projects the movie data to intermediate format and compares this to a similar projection applied to the original. In theory, informed detectors can also correct for spatial, temporal, and valumetric (brightness, contrast, gamma, etc.) misalignments prior to detection. Detectors that do not require access to the original movie are called *blind detectors*.

5.3 A Caution on the use of Watermarks

Watermarking creates a metadata channel by changing the imagery and the sound. Thus, it has the potential to degrade the quality of the motion picture. As such, it should only be used in situations where other, less invasive data channels, would be insufficient.

As an example, consider the case of copy prevention for DVD video. In one proposed system [10], the primary mechanisms responsible for copy control are the CSS encryption and the CCI (copy control information) metadata stored in the MPEG header. However, neither of these is present in the analog signal output from a consumer DVD player. Thus, the analog output is not protected from copying and can be provided as an input to a DVD recorder. Here is a case where watermarks can be used effectively. By redundantly encoding the CCI metadata in a watermark as well as in the MPEG header, a DVD recorder can recover the copy control requirements from an analog signal.

An analogous setting occurs in digital cinema. While we may design a number of encryption-based architectures for protecting a movie from being copied, all of those mechanisms will be lost when the movie is decrypted, decompressed, converted to photons, and displayed on a movie screen. At this point the movie is vulnerable to recording by a camcorder. Data embedded as a watermark has the potential to survive this journey up to the screen and into the camcorder.

Note that this argument is equally valid for traditional film-based cinema as it is for digital cinema. Watermarking can be used to attach metadata to films such that the data can be recovered after recording on a camcorder. However, watermarking embedding is more difficult in film-based media than it is in digital media.

5.4 Digital Cinema Applications

As just discussed, watermarking is an invasive process and should be limited to applications in which other technologies are insufficient. Within the domain of digital cinema, there are a number of potential watermarking applications that can be identified. Good general reviews of watermarking applications and the properties required of a watermark intended for those applications can be found in [6, 11].

Watermarking is probably not an appropriate tool for preventing theft in the digital cinema domain. Consider the problem of camcorder recording during exhibition. A watermark that carries the message "Do Not Copy This" will only be useful in preventing camcorder recording if all camcorder manufacturers suddenly agree to put watermark detectors in their devices and if all existing camcorders (those without watermark detectors) suddenly stop working. So, realistically, watermarks will not be effective in preventing camcorder recording. This is in contrast to ideas for DVD copy protection which were intended for adoption before any "legacy" consumer DVD recording devices became available. In that case, the watermark was used as a tool to *prevent* copying [10].

It can be expected that, at some point, some aspects of a digital cinema security system will become compromised. This will likely be the result of cipher keys that become known either due to poor implementation of some aspect of the system or because of a tampered piece of hardware. A second possibility is that a person with authorized access to the unencrypted movie (someone in production, post- production, or compression for example) has managed to circumvent any technical restrictions on copying and has betrayed the trust of the content owner. Such a security breech will result in the existence, sale, and distribution of unauthorized copies of the movie for which the content owner is not compensated.

The ability to track such an illicit copy back to its source is a desirable function and watermarking can provide this forensic tracking. As the movie content is passed from one production/distribution stage to the next, a unique watermark is added. If we assume that the movie content is encrypted between stages and that the watermark is embedded during encryption, then presence of an operator's watermark in the illicit copy clears that person of any wrongdoing. In this way, the watermarks can help identify where, in the production/distribution chain, the movie escaped from the secure environment.

A second use for forensic tracking watermarks is during exhibition. Encryption-based schemes cannot protect the movie after decryption and decryption is necessary in order to exhibit the movie. Once the movie arrives on the big screen, it is vulnerable to recording by camcorder.

A quick look at peer-to-peer file trading traffic reveals that movies recorded in this way make up the vast majority of illegally traded movies. The quality of these camcorder captures can range from quite poor (Kramer in the audience with a handheld camera) to quite good (tripod setup in the back of an empty theater with sound patched directly from the sound system). It is this second category of pirated movies that most threatens the movie industry.

A forensic watermark can be used to embed exhibition information into the movie. This may include a screen identifier (there are approximately 130,000 movie screens in the United States), the time and date of exhibition, identification of the projection operator (assuming that the operator needs a smart card or password in order to operate the equipment), and perhaps identification of the server and projection equipment used (such as serial numbers). All of this information can be embedded as metadata using a watermark. When extracted from an illicit copy of the movie, the content owners will gain a better understanding of the source of the piracy and will be able to put pressure on the responsible theater owner. The exact of that pressure is still being debated and there is currently no consensus regarding an appropriate studio reaction once the source of the piracy is known.

6. CAMCORDER JAMMING

The role of cryptographic tools in a digital cinema system is to *prevent* the misuse of the movie prior to exhibition. One role of a watermarking is to identify the

source of theft that occurs during exhibition. One nice feature of a digital cinema security system would be the ability to *prevent* theft during exhibition.

There are a number of research efforts underway to interfere with the ability of a camcorder to record a movie in a theater. Together, these technologies have come to be known as *camcorder jamming* technologies [12]. There is very little published literature describing camcorder jamming technologies. In general, the challenge is to interfere with the normal operation of the camcorder or insure that the resulting recording is of very low quality while at the same time insuring that the audience experience is not adversely affected.

Approaches include attempts to trick the automatic features of the camcorder such as automatic gain control, automatic focus, and automatic white balance. Other approaches modify the timing and modulation of the light in order to distort the image captured by any frame-based recording device.

7. SUMMARY

Digital Cinema offers the movie industry the potential of increased security and thus, decreased piracy rates. Encryption and standard DRM protocols can protect the motion picture when in storage and during transit from one process or location to another. Camcorder jamming technologies hold the promise of protecting a movie during exhibition from theft by camcorder recording. Finally, watermarking can be used as a forensic tracking tool to discourage theft by allowing the content owners to pinpoint when and from where a movie was stolen.

8. REREFERENCES

[1] National Association of Theatre Owners, “Digital Cinema User Requirements”, http://www.natoonline.org/digitalcinemauserreq.htm

[2] J. P. Lixvar, “Watermarking Requirements for Boeing Digital Cinema”, in *Security and Watermarking of Multimedia Contents V*, Edward J. Delp III, Ping Wah Wong, Editors, Proceedings of SPIE Vol. 5020, 2003.

[3] M. Karagosian, “Demystifying Digital Cinema”, In Focus Magazine, (three part article) October 2002, November 2002, and December 2002.

[4] MPEG-21 Rights Expression Language Working Draft. Information Technology -- Multimedia Framework -- Part 5: Rights Expression Language -- Working Draft. From: MPEG Multimedia Description Schemes (MDS) Group. December 07, 2001 [Pattaya, Thailand] http://xml.coverpages.org/MPEG-21-REL-WD-200212.pdf

[5] P. B. Schneck and J. A. Bloom, "Persistent Access Control & Watermarking: Primary Security and Forensics", Proceedings of the 3rd Annual Assessment of Enabling Technologies, Government Electronics and Information Technologies Association, 2001 Vision Conference.

[6] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*, Morgan Kaufmann Publishers, Inc., San Francisco, 2001).

[7] J. Lubin and J. A. Bloom, “Robust Second-generation Watermark for Tracking in Digital Cinema”, in *Security and Watermarking of Multimedia Contents V*, Edward J. Delp III, Ping Wah Wong, Editors, Proceedings of SPIE Vol. 5020, 2003.

[8] J. Haitsma and T. Kalker, “A Watermarking Scheme for Digital Cinema”, International Conference on Image Processing, 2001.

[9] C. Honsinger and M. Rabbani, “Data embedding using phase dispersion,” International Conference on Information Technology: Coding and Computing (Invited Paper), April 2000.

[10] J. A. Bloom, I. J. Cox, T. Kalker, J-P. Linnartz, M. L. Miller, and B. Traw, "Copy Protection for DVD Video", Proceedings of the IEEE Special Issue on Identification and Protection of Multimedia Information, Vol. 87, No. 7, pp. 1267-1276, 1999.

[11] I. J. Cox, M. L. Miller and J. A. Bloom, ``Watermarking applications and their properties", Invited Paper, Proceedings of the IEEE International Conference on Information Technology: Coding and Computing, pp. 6-10, 2000.

[12] 2002 NIST ATP Award, *Content Specific Camcorder Jamming for Digital Projectors*, (http://www.atp.nist.gov/awards/00005237.htm)