NEW CHANNELS FOR CARRYING COPYRIGHT AND USAGE RIGHTS DATA IN DIGITAL MULTIMEDIA DISTRIBUTION

Ahmet M. Eskicioglu
Department of Computer and Information Science, CUNY Brooklyn College
2900 Bedford Avenue, Brooklyn, NY 11210
Edward J. Delp
Video and Image Processing Laboratory (*VIPER*), School of Electrical and Computer Engineering
Purdue University, West Lafayette, IN 47907
Mehmet R. Eskicioglu
Department of Computer Science, University of Manitoba
Winnipeg, MB, Canada R3T 2N2

ABSTRACT

Protection of intellectual property is a critical issue in digital multimedia distribution systems. Cryptographic tools are commonly used for secure delivery of content and access keys to consumers via terrestrial, satellite, cable and Internet transmissions. A third requirement is the distribution of the copyright or usage rights associated with the digital content. The integrity, as opposed to security, of this data is essential to prevent unauthorized modification. Two approaches have been proposed in the open literature: allocating special fields in the transport stream and embedding a watermark into multimedia content. We present two new methods, based on secret sharing, to create channels with guaranteed data integrity.

1. INTRODUCTION

Secret sharing is one of the approaches used for developing multi-party protocols for key establishment [1]. Schemes based on secret sharing:

- provide a reliable mechanism for the protection of cryptographic keys without increased risk of disclosure.
- facilitate distributed trust or shared control for critical activities.

A prepositioned secret sharing scheme has been applied to conditional access, message authentication and multicast-based digital rights management systems [2,3,4,5,6].

The availability of digital technologies and broadband Internet access in recent years have increased the demand for new multimedia services. The Internet service providers are now deploying new technologies for group communication. Service types include teleconferencing, pay-per-view, video-on-demand, and real-time delivery of stock market information. Security is an important requirement for the distribution networks when the delivery includes either confidential or commercial data.

Secure multicast communication [7,8,9] in a computer network involves efficient packet delivery from one or more sources to a large group of receivers having the same security attributes. The security of the packets is made possible using a common *group key* shared by the members at the specified destinations. Several factors such as the multicast application type and group dynamics influence the way the group key is generated and distributed to members. The desirable attributes for a key management system include:

- securely rekeying the members when a new member joins the group (backward access control),
- securely rekeying the members when a member leaves the group (forward access control),
- minimizing the storage, communication and computation requirements of the participants.

A number of schemes has been proposed for scalable secure multicasting [7,10,11].

Undoubtedly, a common need in all of the above secure distribution architectures is three-fold:

- encryption of the multimedia content
- cryptographic protection of the decryption keys (by encryption or other means)
- integrity of the critical data (copyright or usage rights) associated with the content.

Secret sharing not only provides a method for key distribution but also a channel with data integrity. In the next section, we will propose a low bandwidth channel for the transmission of critical data associated with multimedia content.

2. THE USE OF SECRET SHARING: A LOW BANDWIDTH CHANNEL

We will start with three definitions for a formal introduction to our proposal:

0-7803-7724-9/03/$17.00 © 2003 IEEE

Definition 1: A (t, n) *threshold scheme* $(t \le n)$ is a method that enables a trusted third party to divide a secret S into n secret shares S_i, $(1 \le i \le n)$ in such a way that at least t shares are required to reconstruct S. Each S_i is securely distributed to user P_i and stored as confidential information.

Definition 2: A *perfect* threshold scheme is a threshold scheme in which a knowledge of $(t$-1) or fewer shares does not provide any advantage to the opponent to find the secret.

Definition 3: A (t, n) *prepositioned secret sharing scheme* is a secret sharing scheme in which n secret shares are stored by the participants in advance of the activation of the scheme [12]. Even if all of the n pieces are exposed, the secret key cannot be recovered until some additional information is provided.

Shamir's (t, n) threshold scheme [13] defines the secret S to be the coefficient a_0 of a random $(t$-1)-degree polynomial

$$f(x) = (a_{t-1}x^{t-1} + \ldots + a_1 x + a_0) \bmod p$$

over the finite Galois Field GF(p). To share the secret among n users, the trusted party performs the following tasks:

1. Choose a prime p larger than n and the secret S.
2. Construct $f(x)$ by selecting $(t$-1) random coefficients $a_1, \ldots, a_{t-1}$.
3. Compute the shares S_i by evaluating $f(x)$ at n distinct points.
4. Securely distribute S_i to user $P_i (1 \le i \le n)$.

The secret S is recovered by constructing the polynomial

$$f(x) = \sum_{i=0}^{t-1} y_i \prod_{0 \le j \le t-1, j \ne i} (x - x_j)/(x_i - x_j).$$

from any t of the n shares, and obtaining the value of $f(x)$ at x=0.

In our design, we will use Shamir's scheme as a prepositioned secret sharing method with $n = t$-1, i.e., the method is designed to recover the secret by requiring only one more piece (the "activating" share). The activating share will be used to establish the separate low bandwidth channel to carry information.

The prepositioned secret sharing scheme we proposed earlier [2,3,4] allows the reconstruction of different keys by communicating different activating shares for the same prepositioned information. The activating shares are used by the receivers to generate the content decryption keys. As there is sufficient flexibility in choosing their values, they can be used to create a channel to transmit critical data for multimedia content protection. The general architecture is depicted in Fig. 1.

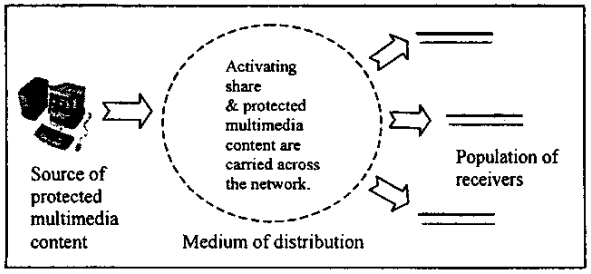


Figure 1. Distribution of digital multimedia content

If multiple keys are to be generated, the activating share is chosen and the keys are obtained after the construction of the corresponding polynomials. Let l be the number of keys to be generated, and $S_1, S_2, \ldots, S_l$ be the sets of shares to be used. The sender uses the following procedure for key generation:

1. Choose the activating share.
2. for $i = 1$ to l do
   begin
   Construct the polynomial $f_i(x)$ passing through the activating share and all the elements in S_i;
   Compute $f_i(0)$;
   Assign $f_i(0) = K_i$
   end.

The receivers construct the decryption keys when they receive the activating share together with the encrypted multimedia content.

There may be several uses of the proposed channel. Today, the most critical information includes time stamps, the CCI and data about copyright ownership.

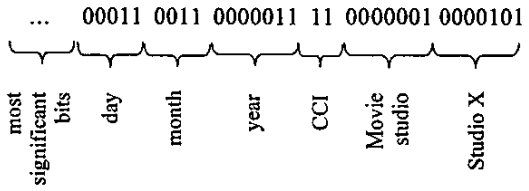
- *Time stamps*: If a time stamp is needed in a multimedia application to determine the time of delivery or broadcast, this can be inserted in the binary bit sequence representing the value of the activating share. If the content is of type "never-copy," then an authorized playback device would prevent the playback of this content at a later time.
- *Copy Control Information (CCI)*: The CCI expresses the conditions under which a consumer is allowed to make a copy of a content legally accessed. An important subset of CCI is the two Copy Generation Management System (CGMS) bits for digital copy control: "11" (copy-never), "10" (copy-once), "01" (no-more-copies), and "00" (copy-free). The CCI can be associated with the content in two ways: (1) the CCI is included in a designated field in the A/V stream, and (2) the CCI is embedded as a watermark into the A/V stream.
- *Copyright ownership:* The names of the artist, the distributors or any other copyright information need to be associated, and carried with, the content.

Note that data integrity is guaranteed for this channel; if there is a malicious attempt to modify the activating share, the receiver will not be able to construct the proper key for decryption. We will give a numerical example to explain the use of the proposed channel:

Example: The following information will be inserted in the activating share: time stamp, CCI and content provider's identification.

Time stamp:	3 March 2003
CCI:	11 (copy never)
Content provider's ID:	Is consisted of two parts: the class of the content provider and the provider in that class

The binary fields allocated for the 3 pieces of information are:



A similar approach is used in the Digital Transmission Content Protection (DTCP) Specification [14] that defines a cryptographic protocol for protecting audio/visual entertainment content from illegal copying, intercepting and tampering as it traverses digital buses such as the IEEE 1394 interface. For the transfer of the CCI from a source device to a sink device, two methods can be used:

- The Encryption Mode Indicator (EMI): The CGMS bits are carried via the most significant two bits of the synch field of the isochronous* packet header defined by the interface specification. The EMI allows immediate access to CGMS information without extracting embedded CCI. The CGMS information is used as an argument in the function to generate the keys for encrypting the content across the interface. Modifying the EMI bits in an unauthorized way will result in erroneous decryption of the content.

- Embedded CCI: The CCI is carried as part of the multimedia content stream. Some transport formats (including MPEG) include fields allocated for the CCI associated with the stream. The CCI can also be embedded as a watermark directly into the content.

The capacity of the channel can be estimated based on a number of assumptions. If we assume that 8 bytes of the activating share are used, and the activating share is renewed every 10 seconds, the potential capacity would be 6.4 bits/sec. Normally, the CCI and content provider's ID would not change for the entire length of a given content (e.g., a movie).

3. GENERALIZATION TO MULTICASTING

The proposed communication channel can be established in any of the following Internet delivery mechanisms:

- *Unicast*: point-to-point communication between a server and a client device
- *Broadcast*: communication of the same data to an entire client population
- *Multicast*: communication of the same data from a source to a large group of clients identified by a group address

We will extend the idea to a multicast architecture where the group manager will be able to send a different activating share to each group member. This idea has been inspired by the *watercasting* concept [15] where each recipient receives a slightly different version of the watermarked video stream, allowing those who illegally distribute the stream to be traced.

* A form of data transmission that provides a certain minimum data rate as required for time-dependent data such as video or audio.

Assume a multicast distribution tree with maximum depth d. For watercasting, the source generates a total of n differently watermarked copies of each packet such that $n \geq d$. Each group of n alternate packets is called a *transmission group*. On receiving a transmission group, a router forwards all but one of those packets to each downstream interface on which there are receivers. Each last hop router in the distribution tree will receive $n\text{-}d_r$ packets from each transmission group, where d_r is the depth of the route to this router. Exactly one of these packets will be forwarded onto the subnet with receivers. The goal of this filtering process is to provide a stream for each receiver with a unique sequence of watermarked packets. To trace an illegal copy, the information about the entire tree topology needs to be stored by the server. A major potential problem with watercasting is the support required from the network routers. The network providers may not be willing to provide a security-related functionality unless video delivery is a promising business for them.

The traditional mechanism to support multicast communications is IP multicast. It uses the notion of a group of members identified with a group address. When a sender sends a message to this group address, the network uses a multicast routing protocol to optimally replicate the message at intermediate nodes and forward copies to group members. For secure group communications, the group key needs to change every time a member joins or leaves the group. In some applications involving entertainment content, the group key also needs to change periodically to increase the robustness against cryptographic attacks.

Let d be the maximum depth of the distribution tree. In periodic rekeying, the sender generates a total of n different activating shares such that $n \geq d$. Each group of n alternate activating shares is called a *transmitted share group* (TSG). We propose the following algorithm that is similar to that of watercasting:

Step 1: On receiving a TSG, a router forwards all but one of the shares to each downstream interface on which there are members.

Step 2: Each last hop router in the tree will receive $n\text{-}d_r$ packets from each TSG, where d_r is the depth of the route to this router. Exactly one of these packets will be forwarded onto the subnet with members.

The filtering process results in a stream with a unique sequence of activating shares for each member. This can be considered to be a generalization of the low bandwidth channel to *personalize* content delivery for each member. Such a channel would be very appropriate for Conditional Access (CA) or Digital Rights Management (DRM) systems with secure processing and storage environments. The unique sequence of activating shares delivered to a receiver can be stored securely on a hard disk and sent to a Clearing House where financial transactions are processed. The Clearing House would therefore know exactly which *personalized* content is delivered to the member. Furthermore, if the unique sequence of activating shares is mapped to the unique sequence of watermarked packets obtained by watercasting, the server does not need to store information about the tree topology to trace an illegal copy.

4. A MEDIA-DEPENDENT CHANNEL TO CARRY THE ACTIVATING SHARE

Encryption and watermarking each provide a different "*line of defense*" in protecting content. Recent research has therefore followed two different avenues resulting in encryption techniques that are independent from watermarking techniques. In our work, we will investigate a unified approach, combining encryption with watermarking. One possible avenue of research is to establish a relation between the data encryption key and the watermark. If the watermark represents the activating share, we would have a media-dependent channel to carry key-related data.

Encryption makes the content unintelligible through a reversible mathematical transformation based on a secret key. In secure multimedia content distribution, the audio/visual stream is compressed, packetized and encrypted [16]. One of the most challenging problems in distribution architectures is the delivery of the decryption key. Symmetric key ciphers are commonly used for the protection of multimedia content. The protection of the decryption keys is usually defined privately by CA or DRM systems. MSEC is an IETF Working Group whose purpose is to standardize protocols for securing group communication over internets, and, in particular, over the global Internet [17]. In some of the modern CA systems, a security module is assigned the critical task of recovering the decryption keys. These keys are then passed to the receiver for decrypting the A/V streams. Recently, two separate standards have evolved to remove the security functionality from navigation devices. In the US, the National Renewable Security Standard (NRSS) [18] defines a renewable and replaceable security element for use in consumer electronics devices such as digital set-top boxes and digital TVs. In Europe, the Digital Video Broadcasting (DVB) [19] project has specified a standard for a common interface (CI) between a host device and a security module.

Watermarking (data hiding) [20,21] is the process of embedding hidden data into a multimedia element such as image, audio or video. This embedded data can later be extracted from, or detected in, the multimedia element for security purposes or other purposes such as binding advertising to a specific content. A watermarking algorithm consists of the watermark structure, an embedding algorithm and an extraction, or a detection, algorithm. Watermarks can be embedded in the pixel domain or the transform domain. In multimedia applications, embedded watermarks should be invisible, robust and have a high capacity [22]. Invisibility refers to the degree of distortion introduced by the watermark and its affect on the viewers or listeners. Robustness is the resistance of an embedded watermark against intentional attacks and normal A/V processes such as noise, filtering (blurring, sharpening, etc.), resampling, scaling, rotation, cropping and lossy compression. Capacity is the amount of data that can be represented by an embedded watermark. The approaches used in watermarking still images include: least-significant bit encoding, basic M-sequence, transform techniques and image-adaptive techniques [23]. As video watermarking possesses additional requirements, development of more sophisticated models for the encoding of video sequences is currently being investigated [24].

In periodic rekeying, if there is no need for a key update, the multimedia data is encrypted with the key corresponding to the current activating share. When the encryption key needs to change, the server generates a new activating share and embeds it into the multimedia stream. The composite stream is encrypted with the key constructed from the old activating share. Each receiver can extract the watermark after the decryption process and compute the new key.

The watermarking scheme to be used for this purpose needs to include a watermark extraction algorithm (as opposed to a watermark detection algorithm). The structure of the watermark is determined by the embedding key, K_{emb}. We have developed a very robust watermarking protocol for key-based video watermarking [25, 26]. In this protocol, we generate keys that are both very secure and content dependent using a cryptographically strong state machine. The protocol is robust against many types of video watermarking attacks and supports many kinds of embedding and detection schemes. In embedding the activating share, we will use a robust video watermarking system [27] since this system provides the type of payload size needed.

The advantages of distributing the activating shares via data embedding are:

- *Additional level of security*: The hacker will have to attack both the encryption key generation algorithm and the watermark embedding algorithm.
- *Multiple uses*: The embedded activating share can be used as a multi-purpose watermark, representing both the key-related data and copyright or copy control information.

Note that the requirements for the proposed watermarking scheme are different from those in typical copyright or content protection applications. If the watermark in our scheme is successfully removed by the hacker before authorized access, the content will not be decrypted correctly.

5. CONCLUSIONS

The transition from analog to digital technologies for multimedia content distribution necessitates the protection of intellectual property. There are three important considerations in secure content distribution: Protection of content with encryption, protection of decryption keys, and integrity of critical data associated with protected content. Many key management schemes are in place in today's CA and DRM systems, and new techniques are proposed in the open literature. When a digital multimedia content is released for distribution, the content providers need to send data that describes how the content should be used by the consumers. This data, which includes CCI and copyright information, can be attached to transport A/V streams in two ways: using specially allocated fields in the transport stream and by embedding directly into content.

We have proposed two new complementary schemes to carry critical data associated with digital multimedia content: (1) a communication channel with a low bandwidth, and (2) a watermarking scheme. This is an extension of the secret sharing idea used to distribute the decryption keys to authorized receivers. In both schemes, the integrity of the data is assured as unauthorized modification of the activating share results in incorrect decryption of the content by the receivers. The proposed

schemes can be used in satellite, terrestrial and cable systems using unicast, broadcast or multicast delivery mechanisms.

In spite of reasonable success in protecting multimedia content in digital distribution, the protection of content in local storage (e.g., a hard disk) remains to be an open issue. Future research in this area may prove to be highly promising to provide end-to-end security systems.

REFERENCES

[1] J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[2] A. M. Eskicioglu, "A Key Transport Protocol for Conditional Access Systems," in *Proceedings of SPIE Security and Watermarking of Multimedia Content III*, Vol. 4314, San Jose, CA, January 22-25, 2001, pp. 139-148.

[3] A. M. Eskicioglu, "A Prepositioned Secret Sharing Scheme for Message Authentication in Broadcast Networks," in *Communications and Multimedia Security Issues of the New Century, IFIP TC6/TC11 Fifth Joint Working Conference on Communications and Multimedia Security (CMS'01)*, Darmstadt, Germany, May 21-22, 2001, pp. 363-373.

[4] A. M. Eskicioglu and M. R. Eskicioglu, "Multicast Security Using Key Graphs and Secret Sharing," in *Proceedings of the Joint International Conference on Wireless LANs and Home Networks (ICWLHN 2002) and Networking (ICN 2002)*, Atlanta, GA, August 26-29, 2002, pp. 228-241.

[5] A. M. Eskicioglu and E. J. Delp, "An Integrated Approach to Encrypting Scalable Video," in *Proceedings of the 2002 IEEE International Conference on Multimedia and Expo*, Lausanne, Switzerland, August 26-29, 2002, pp. 573-576.

[6] A. M. Eskicioglu, S. Dexter and E. J. Delp, "Protection of Multicast Scalable Video by Secret Sharing: Simulation Results," in *Proceedings of SPIE Security and Watermarking of Multimedia Content V*, Santa Clara, CA, January 21-24, 2003.

[7] L. R. Dondeti, S. Mukherjee and A. Samal, "Survey and Comparison of Secure Group Communication Protocols," Technical Report, University of Nebraska-Lincoln, June 1999.

[8] M. J. Moyer, J. R. Rao and P. Rohatgi, "A Survey of Security Issues in Multicast Communications," *IEEE Network*, pp. 12-23, November/December 1999.

[9] T. Hardjono and G. Tsudik, "IP Multicast Security: Issues and Directions," *Annales de Telecom*, pp. 324-334, July-August 2000.

[10] D. Bruschi and E. Rosti, "Secure Multicast in Wireless Networks of Mobile Hosts and Protocols and Issues," *ACM Baltzer MONET Journal, Special Issue on Multipoint Communication in Wireless Networks*, 2000.

[11] S. Rafaeli, "A Decentralized Architecture for Group Key Management," PhD Appraisal, Computing Department, Lancaster University, England, September 2000.

[12] G. J. Simmons, "Prepositioned shared secret and/or shared control schemes," in *Advances in Cryptology – EUROCRYPT '89 Proceedings*, Springer-Verlag, 1990, pp. 436-467.

[13] A. Shamir, "How to share a secret," *CACM*, 22(11), pp. 612-613, November 1979.

[14] www.dtcp.com

[15] I. Brown, C. Perkins and J. Crowcroft, "Watercasting: Distributed Watermarking of Multicast Media," in *First International Workshop on Networked Group Communication (NGC '99)*, Pisa, November 17-20, 1999.

[16] A. M. Eskicioglu, J. Town and E. J. Delp, "Security of Digital Entertainment Content from Creation to Consumption," (Invited paper) in *Proceedings of SPIE Applications of Digital Image Processing XXIV*, Vol. 4472, San Diego, CA, July 31-August 3, 2001, pp. 187-211.

[17] www.securemulticast.org/msec-index.htm

[18] EIA-679B National Renewable Security Standard, September 1998.

[19] www.dvb.org

[20] M. D. Swanson, M. Kobayashi and A. H. Tewfik, "Multimedia data embedding and watermarking techniques," *Proceedings of the IEEE*, Vol. 86, No. 6, pp. 1064-1088, June 1998.

[21] F. A. P. Petitcolas, R. J. Anderson, M. G. Kuhn, "Information hiding – a survey," *Proceedings of the IEEE*, Vol. 87. No. 7, pp. 1062-1078, July 1999.

[22] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proceedings of the IEEE*, Vol. 87. No. 7, pp. 1079-1107, July 1999.

[23] R. B. Wolfgang, C. I. Podilchuk and D. J. Delp, "Perceptual Watermarks for Digital Images and Video," *Proceedings of the IEEE*, Vol. 87, No. 7, pp. 1108-1126, July 1999.

[24] E. T. Lin, C. I. Podilchuk, T. Kalker, and E, J. Delp, "Streaming Video and Rate Scalable Compression: What Are the Challenges for Watermarking?" to appear in *Journal of Electronic Imaging*.

[25] E. T. Lin and E. J. Delp, "Temporal Synchronization in Video Watermarking," in *Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents IV*, Vol. 4675, San Jose, CA, January 20-25, 2002.

[26] E. T Lin and E. J. Delp, "Temporal Synchronization In Video Watermarking: Further Studies," in *Proceedings of the SPIE/IS&T Conference on Security and Watermarking of Multimedia Contents V*, Santa Clara, CA, January 21-24, 2003.

[27] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," *Signal Processing*, vol. 66, no. 3, pp. 283-301, May 1998.