CERIAS Tech Report 2005-124

Advances in Digital Video Content Protection

by EUGENE T. LIN and AHMET M. ESKICIOGLU and REGINALD L. LAGENDIJK and EDWARD J. DELP

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

Advances in Digital Video Content Protection

EUGENE T. LIN, STUDENT MEMBER, IEEE, AHMET M. ESKICIOGLU,
REGINALD L. LAGENDIJK, SENIOR MEMBER, IEEE, AND EDWARD J. DELP, FELLOW, IEEE

Invited Paper

The use of digital video offers immense opportunities for creators; however, the ability for anyone to make perfect copies and the ease by which those copies can be distributed also facilitate misuse, illegal copying and distribution ("piracy"), plagiarism, and misappropriation. Popular Internet software based on a peer-to-peer architecture has been used to share copyrighted movies, music, software, and other materials. Concerned about the consequences of illegal copying and distribution on a massive scale, content owners are interested in digital rights management (DRM) systems which can protect their rights and preserve the economic value of digital video. A DRM system protects and enforces the rights associated with the use of digital content. Unfortunately, the technical challenges for securing digital content are formidable and previous approaches have not succeeded. We overview the concepts and approaches for video DRM and describe methods for providing security, including the roles of encryption and video watermarking. Current efforts and issues are described in encryption, watermarking, and key management. Lastly, we identify challenges and directions for further investigation in video DRM.

Keywords*—Content protection, digital video, encryption, security, watermarking.*

I. INTRODUCTION

WHILE the use of digital video offers immense opportunities for creators, the ability for anyone to make perfect copies and the ease by which those copies can be distributed also facilitate misuse, illegal copying and distribution ("piracy"), plagiarism, and misappropriation. Content creators and owners are concerned about the consequences of illegal copying and distribution on a massive scale. This problem is not merely theoretical. Popular Internet software based on a peer-to-peer (P2P) architecture (such as *Kazaa* [1], *BitTorrent* [2], *eDonkey* [3], and *Gnutella*) has been used to share (distribute) copyrighted music, movies, software, and other materials. Furthermore, future P2P systems may encrypt the data being shared, preserve the anonymity of its users, support a larger number of users, and be more robust [4], [5]. These advances in P2P systems will create considerable challenges for copyright enforcement. Thus, there is a great desire for digital rights management (DRM) systems that can preserve the economic value of digital video and protect the rights of the owners.

The technical challenges of protecting digital content are daunting and previous approaches have not always succeeded. One well-known example of an approach that was not completely successful is the content scrambling system (CSS) for protecting prerecorded movies stored on digital video discs (DVD) [6]–[8]. CSS is a complex system with many components to hinder copying the video stored on CSS-protected discs, including encryption to scramble the video data written on the discs, a protocol for obfuscating the communications between the DVD reader and attached devices (such as a general-purpose computer), and copy protection for digital and analog outputs. The keys to decrypt the movie are stored on special areas of the disc that are only accessible to the reader, which prevents non-CSS compliant devices from decrypting the movie and creating perfect copies of the disc. However, the CSS encryption algorithm was successfully reverse-engineered and hacked, leading to the development of "DeCSS" [9] software programs which can decrypt any CSS-encrypted video. Once the encryption has been removed from a movie, copies of the unencrypted movie may be distributed and read by any DVD reader, even on readers that do not recognize CSS protection. Another effort which did not succeed is the secure digital music initiative (SDMI) for protecting digital audio [10].

In this paper, we overview the current approaches for video content protection systems and describe recent advances in the tools and methods for providing security in such systems,

Manuscript received January 3, 2004; revised June 3, 2004.

E. T. Lin and E. J. Delp are with the School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907-2035 USA (e-mail: linet@ecn.purdue.edu; ace@ecn.purdue.edu).

A. M. Eskicioglu is with the Department of Computer and Information Science, Brooklyn College, City University of New York, Brooklyn, NY 11210 USA (e-mail: eskicioglu@sci.brooklyn.cuny.edu).

R. L. Lagendijk is with the Information and Communication Theory Group, Faculty of Electrical Engineering, Mathematics, and Computer Science, Delft University of Technology, 2600 GA Delft, The Netherlands (e-mail: R.L.Lagendijk@EWI.TUDelft.nl).

Digital Object Identifier 10.1109/JPROC.2004.839623

including encryption and watermarking. We shall also identify significant technical problems for further research [11].

II. Content Protection Overview

A. Key Players in Content Protection

The International Intellectual Property Alliance (IIPA) [12] is a private sector coalition formed in 1984 to represent the U.S. copyright-based industries in bilateral and multilateral efforts to improve international protection of copyrighted materials. IIPA reports that the U.S. copyright-based industries are one of the fastest growing and most dynamic sectors of the U.S. economy. Nevertheless, the availability of inexpensive digital reproduction technologies encourages illegal copying of copyrighted materials. Excluding Internet piracy, the annual worldwide losses of copyrighted materials are estimated to be $20 billion–$22 billion. In collaboration with the U.S. government, foreign governments, and private sector representatives, IIPA and its member associations monitor copyright legislative and enforcement developments in more than 80 countries.

There are three industries with vested interest in the digital content protection arena: motion picture, consumer electronics, and information technology. The key players represent companies that range from content owners to device manufacturers and service providers. They include the organizations shown in Table 1.

Table 1
Players in Content Protection

ATSC	Advanced Television Systems Committee [13] is an international, non-profit organization developing voluntary standards for digital television.
CEA	Consumers Electronics Association [14] represents more than 1000 companies within the U.S. consumer technology industry.
CPTWG	Copy Protection Technical Working Group [15] was formed in early 1996 with the initial focus of protecting linear motion picture content on DVD. Supported by the motion picture, consumer electronics, information technology, and computer software industries, the scope of CPTWG now covers a range of issues from digital watermarking to protection of digital television.
DVD Forum	DVD Forum [16] is an international association of hardware manufacturers, software firms and other users of Digital Video Discs.
SCTE	Society of Cable Telecommunications Engineers [17] is a non-profit professional organization which is involved in the development of cable television standards.
MPAA	Motion Picture Association of America [18] represents the American motion picture, home video and television industries.
IETF	Internet Engineering Task Force [19] is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture.
MPEG	Moving Pictures Expert Group [20] developed a family of international standards used for coding audio-visual information.
DVB	Digital Video Broadcasting Project [21] is a consortium of over 300 broadcasters, manufacturers, network operators, software developers, regulatory bodies committed to designing standards for the global delivery of digital television and data services.
TV-Anytime	The global TV-Anytime Forum [22] is an association of organizations which seeks to develop specifications to enable audio-visual and other services based on mass-market high volume digital storage in consumer platforms.

B. What Is Digital Rights Management?

A digital rights management system protects and enforces the rights associated with the use of digital content [23]–[25]. The primary objective for DRM is to ensure that access to protected content (such as video) is possible only under the conditions specified by the content owner. Unauthorized access must be prevented because such access is an opportunity for an unprotected version of the content to be obtained. If unprotected content is obtained, then it can be distributed and used in any manner, bypassing DRM. The DRM system also prevents the creation of unauthorized copies (copy protection) and provides a mechanism by which copies can be detected and traced (content tracking).

Fulfilling the primary objective imposes four requirements on a DRM system. First, the DRM system "packages" the content to be protected in a secure manner. Second, the DRM system must obtain the access conditions specified by the owner of the protected content. Third, the DRM system must determine if the access conditions have been fulfilled. Finally, components of the DRM system must be tamper-proof [26] to prevent or deter attempts to circumvent, modify, or reverse-engineer the security protocols used by the DRM system.

The objective of packaging is to force all accesses to the protected content to be governed by the DRM system. If content was made available without secure packaging, then the content could be accessed or copied directly. This would render the DRM system useless. On the other hand, access to or copying the packaged content does not provide the content itself unless the security of the package is defeated. Packaging is usually accomplished by encryption [27], [28], where the content is scrambled and rendered unintelligible unless a decryption key is known. The DRM system provides

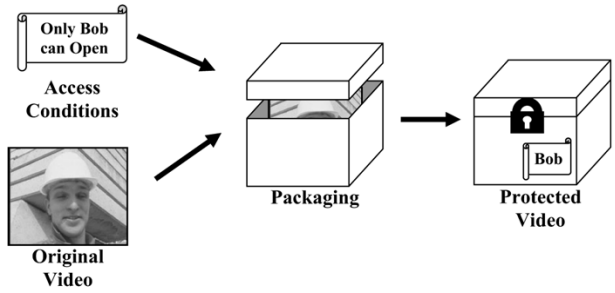

Fig. 1. Example of packaging.

the decryption key to unseal the package only when all the access conditions specified by the content owner are satisfied. Encryption will be discussed in Section III-A.

The DRM system must obtain the access conditions for protected content. This requirement is three-fold: first, a means by which the content owner expresses the access conditions is needed. DRM systems may use rights expression languages (REL) or protocols to allow flexible access rules, while other DRM systems may have rigid access rules that are assumed to apply to all protected content. Two competing proposals for REL standards are the open digital rights language (ORDL) and the eXtensible rights Markup Language (XrML). Second, a mechanism is needed for the DRM system to associate or bind the access conditions to the content. This is typically performed by using metadata or watermarks. Metadata is information that is stored alongside (but separate from) the content, while watermarks are embedded directly into the content itself. The DVD regional management system [6], [7] is one example of using metadata. The third requirement is security. Security prevents users from circumventing DRM by modifying the access conditions.

Having obtained the access conditions for protected content, the DRM system also requires a secure means for determining if the access conditions have been fulfilled. The ease of satisfying this requirement depends greatly on the flexibility of the access conditions supported by the DRM system. If the conditions specify that only certain users can access the content, then it is necessary for the DRM system to determine which user is attempting to gain access. If the conditions specify that access to the content "expires," or is available for a limited time, then a secure means for obtaining the current date and time is needed. If the conditions specify that the content can be accessed only a limited number of times, then a secure means for obtaining the number of previous accesses (or the number of remaining accesses) is needed. If the conditions specify that access requires payment to the content owner or content provider, then a secure means for payment is needed. Security is essential to prevent users from circumventing the DRM by supplying false credentials.

An example is useful in visualizing the concepts of a DRM system. Fig. 1 shows the process of packaging video content and describing the conditions by which the content may be accessed. In this example, the content owner has specified that only the user Bob is allowed to view the video. Once the video has been packaged, the package is made available to users. Fig. 2 shows how Bob would access the video, as well as several methods by which the hacker Alice may attack the DRM system. In path (A), Bob identifies himself to the DRM system, which determines that the access conditions have been satisfied and authorizes Bob to view the video. The remaining paths show methods by which Alice can defeat DRM protection and obtain access to the video. In path (B), Alice uses a method of copying the video that a user has legitimately accessed to make herself a copy. For example, she may record the video as it is being displayed to the user, which is known as exploiting the "analog hole" [29]. In path (C), Alice takes advantage of a security vulnerability in how the DRM decides if the access conditions are fulfilled by providing false credentials (in this case, impersonating herself as Bob). In path (D), Alice takes advantage of a security vulnerability in how the DRM system obtains the access conditions with the content and replaces the legitimate access condition ("Only Bob can view the video") with another ("Anyone can view the video"). In path (E), Alice "hacks" or modifies a device to provide her with a copy of the video or provide her with information (decryption keys, etc.) that allow her to unseal the package. A secure DRM system prevents or hinders paths (B)–(E).

Most digital video applications involve many interconnected devices that can record, display, process, and store video. These devices communicate the video data through a delivery network or the video may be recorded on and read from storage media. For DRM, it is essential that video delivery mechanisms prevent unauthorized access from the source to the consumption device. This is sometimes referred to as "end-to-end" security. There may be few or many steps from the source to the consumption device, depending on the application. Examples of such steps include broadcasting, distribution on a network (including the Internet, a private network, or a network of devices in the user's home), and storage on media (such as digital video disc, compact disc, computer hard disk, or magnetic tape).

One way to achieve "end-to-end" security is for devices to authenticate themselves prior to sending or receiving the video. This authentication process establishes that both the sending and receiving devices are compliant. A *compliant* device is one that supports the access and security protocols of the DRM system. All other devices are *noncompliant*. If one device cannot produce evidence that it is compliant, then other compliant devices will refuse to communicate video with that device. The device authentication process makes it more difficult to use noncompliant devices that ignore the rules imposed by DRM. Device authentication also plays a role in DRM system renewability, which is discussed later.

Another consideration for security is how the video is delivered. Video delivery systems generally use one of three methods for distributing video: *unicast*, *broadcast*, and *multicast* [30], [31]. In the unicast delivery model, the video is transferred from a single device to another. If the video is to be delivered to multiple consumption devices, then a separate copy of the video is delivered from the source to each consumption device. Video distributed using recorded

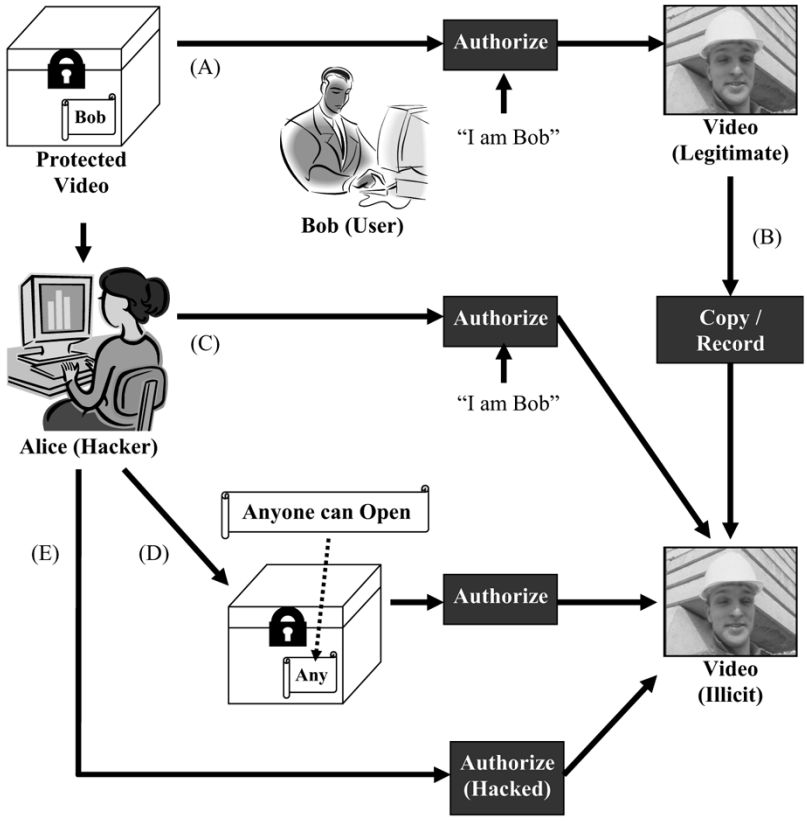

Fig. 2. Examples of DRM use and attack: (A) standard (legal) use, (B) illicit copying, (C) false credentials, (D) alteration of access conditions, (E) use of "hacked" or modified devices.

media (like DVD) resembles the unicast delivery model. In the broadcast delivery model, the video source simultaneously distributes the video to any device which is capable of receiving the video. In multicast, the devices in the delivery network (such as routers) use unicast to transmit the video amongst each other; however, the video is delivered from the source to all consumption devices in such a way that additional copies of the video are created only when necessary. We shall elaborate in Section III-C how these delivery models affect security.

DRM systems may also support *renewability*, where security can be restored or upgraded even after some devices have been compromised. Many content protection systems define renewability as device revocation. Suppose secret information (keys, etc.) contained in a compliant device are compromised by a hacker. The hacker can then use the secret information to modify noncompliant devices to make them appear like compliant devices. When such "pirated devices" appear in the black market in large numbers and are identified by law enforcement agencies, the technology provider can add the hacked device's ID to a revocation list that is securely distributed to all compliant devices. When the new revocation list reaches the compliant devices, any pirated device will fail the authentication process and be unable to process protected content.

C. Legal and Technical Solutions for DRM

Since the mid 1990s, there have been important legislative and technical solutions regarding copyright protection and management of digital rights in the U.S. In this section, current legal and technical efforts in DRM are summarized.

1) Legislative Efforts: Two treaties by the World Intellectual Property Organization (WIPO) [32]—the WIPO Copyright Treaty and the WIPO performances and Phonograms Treaty—obligate the member states to prohibit circumvention of technological measures used by copyright owners to protect their works and to prevent the removal or alteration of copyright management information.

The Digital Millennium Copyright Act of 1998 (DMCA) was the first legislation in a series of efforts by the U.S. Congress to update the U.S. copyright law for the digital age. President Clinton signed the Act into law on October 28, 1998. The DCMA is divided into five titles [33], of which the first title implements the WIPO treaties. Similar legislation was passed in the European parliament and council in Directive 2001/29/EC [34]. Both the DMCA and the European directive have provisions that make illegal the circumvention of technical security measures as well as against manufacturing, offering for sale, or trading in equipment which circumvent these technical security measures.

Recently, a draft legislation was introduced by Senator S. Brownback on September 16, 2003, known as the "Consumers, Schools, and Libraries Digital Rights Management Awareness Act of 2003." With several important provisions, the bill prevents copyright holders from compelling an Internet service provider (ISP) to disclose the names or other identifying information of its subscribers prior to the filing of a civil lawsuit, requires conspicuous labeling of all digital media products that limits consumer uses with access or

Table 2
Summary of DRM Systems for Video

Media protected		Secure delivery of content	Device authentication	Association of digital rights	Licensed technology	System renewability
Prerecorded media	Video on DVD-ROM	encryption	Mutual between DVD drive and PC	metadata	CSS [8]	Device revocation
	Audio on DVD-ROM	encryption	Mutual between DVD drive and PC	metadata	CPPM [35]	Device revocation
		watermarking	n/a	watermark	4C/Verance Watermark [36]	n/a
	Video or audio on DVD-R/RW/RAM	encryption	Mutual between DVD drive and PC	metadata	CPRM [37]	Device revocation
	Video on digital tape	encryption	n/a	metadata	High Definition Copy Protection [38]	Device revocation
Digital interface	IEEE 1394	encryption	Mutual between source and sink	metadata	DTCP [39]	Device revocation
	Digital Visual Interface (DVI)	encryption	Mutual between source and sink	metadata	HDCP [40]	Device revocation
	NRSS interface	encryption	Mutual between host and removable security device	metadata	Open standards [41]–[43]	Service revocation
Broadcast	Satellite	encryption	None	metadata	Conditional access system [44], [45]	Smartcard revocation
	Terrestrial	encryption	None	metadata	Conditional access system [45]	Smartcard revocation
Cable transmission		encryption	None	metadata	Conditional access system [46]	Smartcard revocation
Internet	Unicast	encryption	Receiver	metadata	DRM [47], [48]	Software update
	Multicast (A few watermarking schemes have been proposed for multicast data [49])	encryption	Sender and receiver (depends on the authentication type)	metadata	Group key management [49]	tbd

redistribution restrictions, imposes strict limits on the Federal Communication Commission's ability to impose federal regulations on digital technologies, and preserves the right to donate digital media products to libraries and schools.

2) Technical Efforts: Current DRM systems for distribution and storage are summarized in Table 2. For Internet-based DRM systems, a number of organizations are in the process of standardizing DRM for handling different types of content. MPEG and IETF have been leading the major efforts.

MPEG-4 applications may have different security requirements for video information. The design of the intellectual property management and protection (IPMP) framework recognizes the complexity of the MPEG-4 standard and the diversity of its applications. Hence, MPEG-4 standardizes only the MPEG-4 IPMP interface and not the IPMP systems. The IPMP-Descriptors and IPMP-Elementary Streams defined by this interface provide a communication mechanism between IPMP systems and the MPEG-4 terminal. IPMP systems are also being considered for MPEG-21, which describes an open framework which allows the integration of all elements of a delivery chain necessary to generate, use, manipulate, manage, and deliver multimedia content across a wide range of networks and devices.

Internet Digital Rights Management (IDRM) [50] was an Internet Research Task Force (IRTF) Research Group formed to research issue and technologies relating to DRM on the Internet. The IRTF is a sister organization of the Internet Engineering Task Force (IETF). The IDRM group is now closed.

D. User

The use of DRM is a controversial issue with many potential social and economic ramifications. It is not our intention to advocate any position in this technical overview; however, because DRM affects users and consumers of digital video (including those who do not seek to misuse lawfully purchased or licensed video data) it is important that DRM systems consider the needs of users and customers. The concerns of users include the following.

1) DRM systems may be used to unilaterally enforce usage rules that contravene the rights and privileges granted to the public under copyright law [51]. Such privileges include the doctrines of Fair Use (including "time-shifting" and "space-shifting") and First Sale [52]. Circumventing the DRM system may be unlawful under the DMCA, even if the intended use of the video is lawful [53], [54].
2) DRM systems may force users to release information that violate expectations of privacy [55]. Examples of such information include which videos are viewed by the user, where and when the videos are viewed, and which type of player was used to decode the video.
3) DRM systems may be used reduce competition and "lock" users into using products chosen by the vendor [56]. This is caused by a lack of interoperability. The vendor may refuse to provide authorization information or decryption keys to devices produced by competitors.
4) Users are wary that they shall burden the costs for DRM systems, even though the primary beneficiaries of DRM will be content owners and providers. That is, users may pay increased costs to obtain video and devices that provide them with less functionality and control. These costs include increased economic costs, increased complexity, and decreased compatibility or interoperability between devices.

III. DRM Methods and Tools

To fulfill the objectives of DRM discussed in Section II-B, several tools are available in the design and implementation of DRM systems. This section describes encryption and watermarking, as well as their roles in DRM systems. Finally, we shall briefly mention issues in key management and security in multicast and broadcast networks.

A. Encryption

Encryption is the process for controlling access to confidential data, known as *plaintext*, by scrambling the data into an unintelligible form. The scrambled data is known as the *ciphertext*. Producing the ciphertext requires knowledge of a secret *encryption key*. The inverse process of recovering the original plaintext from the ciphertext is known as decryption. Decryption is very easy to perform with knowledge of the *decryption key* and very difficult to perform without the key. The security of an effective encryption technique lies in the secrecy of the encryption and decryption keys. In particular, if data to be protected is encrypted, then only devices with knowledge of the decryption key can access the protected data.

One example application of encryption for a video DRM system is packaging. The plaintext is the video whose access is to be controlled. Once the video has been encrypted, the ciphertext may be transmitted over a distribution network or recorded onto media. The encrypted video cannot be decoded or displayed without the decryption key. When the video is to be decoded and displayed, the decryption key is provided to the decoder only after the DRM system has verified that the conditions for accessing to the video are satisfied. In this way, a video DRM system can secure the distribution of video content and ensure that access to the video is consistent with the usage rights. Other examples of using encryption in DRM include device authentication and the secure exchange of keys and authorization information.

Encryption has been studied extensively and many techniques are available for general-purpose encryption [27], [28], [57]. While general purpose encryption techniques are useful for device authentication and transferring security information (for example, keys) from one device to another in the DRM system, they have some shortcomings for encrypting digital video data. One of the shortcomings is that the ciphertext is very fragile. The ciphertext must generally be decrypted sequentially from beginning to end and no error in the ciphertext is tolerated. If the ciphertext is modified, or if parts of the ciphertext are not available or become lost during delivery, then the decryption process will not be able to recover the plaintext even with the proper decryption key. Another concern is the computational cost for encryption and decryption. This is of particular importance in real-time applications on low-cost consumer electronics devices. The computational cost of video processing is significantly increased if the video must be decrypted prior to the processing and then re-encrypted for secure delivery after processing.

The fragileness of encrypted video is an obstacle in applications where the loss of video data is possible and for applications that do not access the video in sequential fashion. Real-time video streaming is one example where error and loss may be introduced into the video data as it is delivered over a network [30], [58], [59]. The use of scalable video compression techniques [60]–[63] is another example where video data may be lost. Scalable compression allows a single compressed video data stream to be decoded and displayed at various data rates and quality levels, which implies that not all receivers will obtain or decode the entirety of the compressed video stream. Also, some video applications (such as secure video browsing) require "random access" to the video. In these applications, the user may desire to skip to arbitrary sections of the video or display the video backward. The constraint that the ciphertext must be decrypted from beginning to end is an impediment.

Recent encryption techniques have been proposed to address some of the video-specific issues. One approach is to use selective encryption of the video data [64] or joint compression encryption [65], [66]. The goal of selective encryption is to encrypt or scramble only a portion of the video data such that the displayed video quality is unacceptable if decryption is not performed [67]. Selective encryption reduces the computational cost for video encryption and may also allow a video decoder to identify structures in the compressed video data (such as headers, timing, or synchronization information) without decryption. The latter is beneficial for applications such as browsing, where efficient access to specific portions of the video is desired and decryption is necessary only when these portions are displayed. One approach for performing selective encryption is to code only selected frames of the video, such as the intracoded frames of compressed video streams. However, the security of such an approach is not very good [68], [69]. Other selective encryption techniques shuffle the video data or encrypt parts of the video data with a stream or block cipher [70]–[72].

In some applications, users obtain videos at various quality levels because of network issues [58], [73] or other reasons. One way to obtain the differentiated quality is to transcode [74] the video. However, transcoding is generally computationally expensive, particularly if the video needs to be decrypted, transcoded, and then re-encrypted for secure delivery. Another method is to make multiple copies of the video available, where each copy is encoded using different parameters.[1] A third method is to use scalable compression. There are many strategies for scalable video coding, including layered scalability [76], [77] and fine-grain coding [60], [62], [78].

As mentioned previously, encrypting scalable video is challenging because decoders may not obtain the complete video stream. One approach for encrypting layered scalable video is to encrypt only the base layer. However, this approach may not be sufficiently secure [79]. Some techniques for encrypting scalable compressed video are described in [79]–[81]. These techniques allow the decryptor to tolerate loss or truncation of the video data, particularly in the enhancement layer(s).

B. Watermarking

Encryption is useful in restricting access to data; however, it has one significant disadvantage: encryption techniques do not offer any protection once the encrypted data has been decrypted. This is a significant limitation and encryption alone may not be sufficient for DRM [82]. Watermarking [83]–[90] has been proposed as a means for content protection even after data has been decrypted. The role of watermarking complements (and does not replace) encryption.

A watermark is a signal that is embedded into an original video to produce the watermarked video. The watermark describes information that can protect the video, for example identifying the video owner or recipient. Distortion is introduced into the video when the watermark is embedded; however, the watermarked video and the original video appear similar when the videos are displayed. Ideally, there is no perceptible difference between the original and the watermarked videos. The embedded watermark may be detected by a watermark detector, which uses signal processing to obtain the watermark from the watermarked video. For DRM, it is desirable that the inserted watermark be *robust* or difficult to remove or erase without causing significant damage to the watermarked signal. Ideally, the inserted watermark is an indelible and inseparable part of the watermarked video.

A DRM system can use watermarking in a variety of ways. Some examples of (potential) applications include the following.

1) Copyright or Owner Identification: The embedded watermark identifies the owner of the video. The watermark provides a proof of ownership if the copyright notice has been altered or removed [84].
2) Copy Protection: The watermark encodes the number of times the video may be (legally) copied. A compliant device checks the watermark and determines whether creating an additional copy is allowed. Each time a copy is made, the watermarked video is modified to decrement the count of allowable copies [82].
3) Access Control: This is a generalization of the use of watermarking for copy protection. The watermark encodes the usage and access rights that are granted by the content owner. Compliant devices detect the watermark and obey the encoded usage restrictions.
4) Content Tracking, Fingerprinting, or Traitor Tracing: The watermark encodes the identification of the user or recipient of the video. This implies that each user obtains a unique or personalized copy of the video. If a copy of the video is found in a suspicious location (such as being shared by a peer-to-peer program), the embedded watermark can identify the source of the suspect copies.
5) Content tracking is not necessarily directed at individual users. One example is the mass production of prerecorded video. Suppose the video owner contracts the services of various mastering and distribution companies to create and distribute the video on media. However, the owner is worried that some companies may have insufficient security to safeguard the video. Unscrupulous companies or employees may even conspire to "leak" illicit copies to pirates. For security, the owner embeds a different watermark into the copies he provides to each mastering company. If illegal copies bearing a specific company's watermark are found before the official release of the video, the video owner may choose not to deal with that company in the future. A similar application is digital cinema, where the movie owner or distributor is worried about collusion between some theater owners and pirates.

There are three principal processes involved in watermarking: watermark embedding, attack, and watermark detection. In watermark embedding, the watermark is created and inserted into the original video to produce the watermarked video. The simplest method for watermark

[1]It is possible to switch between the copies dynamically [75] using some compression schemes.

insertion is additive, where the watermark is added to the original video signal analogous to additive noise. Other embedding methods include multiplicative embedding [91] and quantization embedding [92], [93]. The watermark may be inserted directly in the spatial domain (i.e., the pixels of the video) [94]–[96] or after the video has been transformed. Common transformations include the discrete Fourier transform (DFT) [97], [98], discrete cosine transform (DCT) [90], [99]–[102], and wavelet transforms (WT) [90], [98], [103], [104]. The watermark may be inserted into the visual portion of the video as well as the audible portion [105]. Many watermarks are video adaptive, which reduces watermark visibility [90], [106] and increases robustness against attacks [107]–[109].

The watermark detector examines the input test video and determines whether the watermark is present or not. The test video may be a watermarked video, a watermarked video that has been attacked, or a video that is not watermarked. To detect the watermark, the watermark detector requires a secret detection key. Most watermarking techniques are symmetric, where the embedding key and corresponding detection key are identical. For DRM applications, the watermark detector is usually *blind*, which means that the detector does not have access to the original (unwatermarked) video. Some DRM applications (such as content tracking) and other watermarking applications may use nonblind watermark detection, where the original video is available to the detector. If the watermark is detected and the watermarking technique supports a payload, the watermark detector extracts the payload and makes it available to the DRM system.

The watermarked video may be subjected to attack before being examined by the detector [110]–[112]. An attack is a process which may remove the embedded watermark, increase the difficulty in detecting the watermark, or subvert the security of the watermark. The watermarked video may be attacked multiple times. Attacks are not necessarily malicious. Some attacks arise from processing of the watermarked video by users without hostile intent. Of course, there is motivation for hackers and pirate users to remove a watermark used for DRM. If an attacker successfully removes the embedded watermark, or renders it undetectable in the watermarked video, then the benefits and protection that watermarking confers in the DRM system are lost.

The computational cost of watermark embedding is an issue for some DRM applications. If the same watermark will be embedded into many copies of the video and real-time embedding is not needed, then the computational cost for watermark embedding is incurred only when the master copy is created. On the other hand, if a different watermark will be inserted into each of many copies of video, or if real-time watermark embedding is needed, then the computational cost of embedding is a much greater concern. Some DVD copy protection techniques propose real-time watermark embedding [82], and real-time embedding may be needed for watermarking streaming video [58].

One way to reduce the computational cost of watermark embedding is compressed-domain watermark embedding, particularly if the original video is already in a compressed format. In compressed-domain watermarking, the original compressed video is partially decoded to expose the syntactic elements of the compressed video data for watermarking, such as encoded DCT coefficients [99]–[101] or motion information [113], [114]. The watermark may also be inserted by selectively replacing the codewords of the compressed video data [115]. Efficient methods for drift compensation and controlling the data rate of the watermarked video are challenges for compressed-domain watermark embedding [99].

In some applications, such as those that require the watermark to be detected frequently or in real time, the computational cost for watermark detection is a concern. One hypothetical example is a DRM system which uses a watermark to encode access conditions to the video. Then, it will be necessary for the media reader or receiver to detect the watermark when the video is accessed. In addition, some media readers and receivers may be devices with limited computational resources. These applications may consider sequential detection techniques [116] or other means to lessen the cost for watermark detection.

C. Key Management and Delivery Network Issues

Key management [117] is a recognized challenge in encryption and watermarking. The security of cryptography and watermarking techniques is reliant on ensuring secrecy of the keys, known as Kerckhoff's principle [28], and not by the intricacies or secrecy of the encryption, decryption, watermark embedding, or watermark detection techniques (which would be "security" by obscurity). Thus, safeguarding the keys is paramount to maintaining the security of the DRM system. Unfortunately, implementing secure key management and exchange protocols to satisfy the needs of the application may add significant complexity to the DRM system.

Key management encompasses a variety of issues, including key generation, secure transfer (exchange) of keys, secure storage of keys, key revocation, key escrow, and key verification [28]. These issues have been extensively studied in cryptography. For video DRM involving multiple devices or networks, secure key exchange is one of the important management issues. Classical key exchange and authentication protocols [118], [119] may be used by DRM systems for secure key exchanges between devices.

Multicast and broadcast networks present several challenges for key management and secure delivery of video [120]. One of the challenges is controlling access to the video when it is delivered to a group of users or group key management [121]–[125]. Security must be maintained when new users join the multicast network or when users leave the network. Group key management techniques are also reviewed in [126].

Another challenge in multicast and broadcast content distribution is that all receivers will obtain the same video. This is an issue for content tracking and fingerprinting, where it is desired for each user to have a personalized (unique) copy of the video. Several approaches have been proposed to deliver a personalized video to each receiver while retaining the

bandwidth efficiency of multicast [49]. One approach [127] assigns a unique binary string to each receiver and then delivers two copies of the video to each receiver via multicast. A different watermark is embedded into each of the two copies. For each video frame, the receiver decodes exactly one of the two watermarked videos, depending on the unique binary string. This approach is advantageous because it requires no support from the network infrastructure, such as routers. Its disadvantage is that two copies of the video are being delivered to each receiver, which effectively doubles the bandwidth requirement to send the video. Another approach [128] suggests modifying the watermarked video as it is delivered within the network. The disadvantage is that this approach requires network infrastructure support, which may not be available in many networks. Other techniques are mentioned in [129] and [130].

IV. Research Issues

Considerable more effort is needed to provide secure content protection for digital video. First, we examine the tools discussed in Section III.

1) Selective encryption techniques have drawbacks that need to be addressed [64].
2) Encryption of scalable video streams is relatively unexplored.
3) Despite the considerable effort that has been spent on developing robust watermarks for digital video, the robustness and security of current watermarking techniques may not be sufficient for some DRM applications. Removal attacks [10], [131], [132] and spatial and temporal synchronization attacks [94]–[97], [99], [133]–[140] remain challenging for watermark detection. Current methods for devising anti-collusion watermarks [141]–[144] for content tracking are vulnerable to collusion attacks from a party consisting of a relatively low number of conspirators. Security is also an issue [145]–[150].
4) Evaluating the performance of watermarking techniques remains an issue [151], [152]. There is little consensus in measuring and fairly comparing watermark performance.
5) There is little consensus in deciding where watermark embedding and detection should occur in video DRM. Should watermark detectors be placed in consumer electronics devices? Where should watermark embedding and detection occur in DRM applications involving a delivery network? Is it practical and cost effective to place a watermark detector in all devices?
6) Content tracking under multicast and broadcast networks remains challenging. These networks can efficiently deliver a common video stream to all receivers, but content tracking requires each copy of the video to be personalized.

Even if these technical hurdles in the encryption and watermarking tools are overcome, there are other issues that affect DRM systems.

1) Copy protection and the analog hole: Users possess the means to make analog recordings of displayed video, often through the use of "legacy" devices that are not DRM compliant. Once the analog recordings are converted to digital format, the video can be distributed and copied without incurring loss. Copy protection is very difficult, or perhaps even impossible, so long as the analog hole exists to circumvent DRM.
2) Tamper-proofing of devices: The best cryptographic and watermarking techniques confer relatively little protection if devices can be easily hacked and compromised. Devices must be designed to be difficult to tamper and modify to deter attempts to reverse engineer the DRM security protocols.
3) System renewability is an important issue in DRM systems. Without renewability, the DRM system has little means for recovering after security has been compromised. Some challenging questions remain for using device revocation. What is the cost? If a user's device is revoked and no longer functions, who assumes the liability? What happens if the user's device was revoked in error?

DRM systems are required to govern all access, use, and copying of protected content and do so securely. The DRM system will face the innovation and technical resources of a countless number of motivated attackers. The hackers possess the economic motive to defeat the DRM protection, and they will cooperate their efforts to defeat the system. Even legitimate users see more value in an unprotected (unrestricted) copy of the video compared to the same video "locked down" with DRM restrictions placed by the content owner. The attackers only need to succeed once to make an unprotected copy and distribute the copy on a large scale. On the other hand, the DRM system must stand impervious against attack for a long period of time. Against such circumstances, it is not surprising that many DRM systems have not succeeded.

V. Conclusion

We have described recent developments in methods used to protect video content. In particular, we describe advances in DRM systems including encryption and watermarking. We believe that a "technology" fix will not solve the mess we are in today with respect to the protection of multimedia content. The protection of intellectual property rights is perhaps one of the last major barriers to the "digital world." There is hope.

References

[1] Kazaa software version 2.6 [Online]. Available: http://www.kazaa.com
[2] B. Cohen. (2001) BitTorrent. [Online]. Available: http://bitconjurer.org/BitTorrent/index.html
[3] edonkey and overnet [Online]. Available: http://www.edonkey2000.com
[4] P. Biddle, P. England, M. Peinado, and B. Willman, "The darknet and the future of content distribution," in *Proc. ACM Workshop Digital Rights Management 2002*. [Online] Available: http://crypto.stanford.edu/DRM2002/darknet5.doc.
[5] R. Parloff, "Morpheus falling?," *IEEE Spectr.*, vol. 40, no. 12, pp. 18–19, Dec. 2003.

[6] J. A. Bloom, I. J. Cox, T. Kalker, J.-P. M. G. Linnartz, M. L. Miller, and C. B. S. Traw, "Copy protection for DVD video," in *Proc. IEEE*, vol. 87, Jul. 1999, pp. 1267–1276.
[7] J. Taylor, *DVD Demystified*. New York: McGraw Hill, 1998.
[8] Content Scramble System [Online]. Available: http://www.dvdcca.org
[9] D. S. Touretzky. (2000) Gallery of CSS Descramblers. [Online]. Available: http://www.cs.cmu.edu/~dst/DeCSS/Gallery
[10] S. A. Graver, M. Wu, B. Liu, A. Stubblefield, B. Swartzlander, D. W. Wallach, D. Dean, and E. W. Felten, "Reading between the lines: Lessons from the SDMI challenge," presented at the 10th USENIX Security Symp., Washington, DC, 2001.
[11] E. T. Lin, A. M. Eskicioglu, R. L. Lagendijk, and E. J. Delp. (2004) Advances in video content protection (technical report). School of Elect. Comput. Eng., Purdue Univ., West Lafayette, IN. [Online]. Available: http://dynamo.ecn.purdue.edu/~ace/vid-content/
[12] International Intellectual Property Alliance [Online]. Available: http://www.iipa.com
[13] Advanced Television Systems Committee [Online]. Available: http://www.atsc.org
[14] Consumers Electronics Association [Online]. Available: http://www.ce.org
[15] Copy Protection Technical Working Group [Online]. Available: http://www.cptwg.org
[16] DVD forum [Online]. Available: http://www.dvdforum.org
[17] Soc. Cable Telecommun. Eng. [Online]. Available: http://www.scte.org
[18] Motion Picture Association of America [Online]. Available: http://www.mpaa.org
[19] Internet Engineering Task Force [Online]. Available: http://www.ietf.org/overview.html
[20] Moving Pictures Expert Group [Online]. Available: http://mpeg.telecomitalialab.com
[21] Digital Video Broadcasting Project [Online]. Available: http://www.dvb.org
[22] TV-Anytime forum [Online]. Available: http://www.tv-anytime.org
[23] A. M. Eskicioglu, J. Town, and E. J. Delp, "Security of digital entertainment content from creation to consumption," *Signal Process. Image Commun. (Special Issue on Image Security)*, vol. 18, no. 4, pp. 237–262, Apr. 2003.
[24] A. M. Eskicioglu, "Protecting intellectual property in digital multimedia networks," *IEEE Comput.*, vol. 36, pp. 39–45, Jul. 2003.
[25] F. Hartung and F. Ramme, "Watermarking of multimedia content for m-commerce applications," *IEEE Commun. Mag.*, vol. 38, pp. 78–84, Nov. 2000.
[26] G. Naumovich and N. Memon, "Preventing piracy, reverse engineering, and tampering," *IEEE Comput.*, vol. 36, pp. 64–71, Jul. 2003.
[27] J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC, 1997.
[28] B. Schneier, *Applied Cryptography*. New York: Wiley, 1996.
[29] E. Diehl and T. Furon, "©watermark: Closing the analog hole," in *Proc. IEEE Int. Conf. Consumer Electronics*, 2003, pp. 52–53.
[30] D. Wu, Y. T. Hou, W. Zhu, Y.-Q. Zhang, and J. M. Peha, "Streaming video over the internet: Approaches and directions," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 11, pp. 282–300, Mar. 2001.
[31] W. R. Stevens, *TCP/IP Illustrated, Volume 1: The Protocols*. Reading, MA: Addison-Wesley Longman, 1994.
[32] World Intellectual Property Organization [Online]. Available: http://www.wipo.org
[33] Digital Millennium Copyright Act of 1998, U.S. Copyright Office summary [Online]. Available: http://www.loc.gov/copyright/legislation/dmca.pdf
[34] European Copyright Directive [Online]. Available: http://www.eurorights.org/eudmca/CopyrightDirective.html
[35] Protection for Prerecorded Media [Online]. Available: http://www.4Centity.com
[36] 4C/Verance Watermark [Online]. Available: http://www.verance.com
[37] Content Protection for Recordable Media [Online]. Available: http://www.4Centity.com
[38] High Definition Copy Protection [Online]. Available: http://www.jvc-victor.co.jp/english/products/vcr/D-security.html
[39] Digital Transmission Content Protection [Online]. Available: http://www.dtcp.com
[40] High-Bandwidth Digital Content Protection [Online]. Available: http://www.digital-CP.com
[41] *EIA-679B National Renewable Security Standard*, Sep. 1998.
[42] OpenCable CableCARD Copy Protection System Interface Specification [Online]. Available: http://www.opencable.com
[43] ATSC Standard A/70: Conditional Access System for Terrestrial Broadcast [Online]. Available: http://www.atsc.org
[44] Proprietary Conditional Access System for DirecTV [Online]. Available: http://www.directv.com
[45] Proprietary Conditional Access System [Online]. Available: http://www.dishnetwork.com
[46] OpenCable System Security Specification [Online]. Available: http://www.opencable.com
[47] Windows Media DRM [Online]. Available: http://www.rnicrosoft.com/windows/windowsmedia/drm.aspx
[48] Helix DRM [Online]. Available: http://www.realnetworks.com/products/dnn/index.html
[49] A. M. Eskicioglu, "Multimedia security in group communications: Recent progress in key management, authentication, and watermarking," *ACM Multimedia Syst. J. (Special Issue on Multimedia Security)*, pp. 239–248, Sep. 2003.
[50] Internet Digital Rights Management (IDRM) Research Group [Online]. Available: http://www.idrm.org
[51] P. Samuelson, "DRM {And, Or, Vs.} the law," *Commun. ACM: Special Issue Digital Rights Management and Fair Use by Design*, vol. 46, no. 4, pp. 41–45, Apr. 2003.
[52] E. W. Felten, "A skeptical view of DRM and fair use," *Commun. ACM: Special Issue Digital Rights Management Fair Use by Design*, vol. 46, no. 4, pp. 56–59, Apr. 2003.
[53] D. Clark, "How copyright became controversial," presented at the 12th Annu. Conf. Computers, Freedom and Privacy, San Francisco, CA, 2002.
[54] J. Litman, *Digital Copyright*. Amherst, NY: Prometheus, 2001.
[55] D. K. Mulligan, J. Han, and A. J. Burstein, "How DRM-based content delivery systems disrupt expectations of "personal use"," in *Proc. ACM Workshop Digital Rights Management*, 2003, pp. 77–89.
[56] R. Anderson, "Cryptography and competition policy-issues with 'trusted computing'," in *Proc. 22nd Annu. Symp. Principles of Distributed Computing*, 2003, pp. 3–10.
[57] Announcing the Advanced Encryption Standard (AES) (2001, Nov.). [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[58] E. T. Lin, C. I. Podilchuk, T. Kalker, and E. J. Delp, "Streaming video and rate scalable compression: What are the challenges for watermarking?," *J. Electron. Imaging*, vol. 13, no. 1, pp. 198–205, Jan. 2004.
[59] S. Wenger, "H.264/AVC over IP," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, pp. 645–656, Jul. 2003.
[60] M. van der Schaar and H. Radha, "Adaptive motion-compensation fine-granular-scalability (AMC-FGS) for wireless video," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 12, pp. 360–371, Jun. 2002.
[61] W.-T. Tan and A. Zakhor, "Video multicast using layered FEC and scalable compression," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 11, pp. 373–386, Mar. 2001.
[62] W. Li, "Overview of fine granularity scalability in MPEG-4 video standard," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 11, pp. 301–317, Mar. 2001.
[63] K. Shen and E. J. Delp, "Wavelet based rate scalable video compression," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 9, pp. 109–122, Feb. 1999.
[64] X. Liu and A. M. Eskicioglu, "Selective encryption of multimedia content in distribution networks: Challenges and new directions," presented at the 2nd Int. Conf. Communications, Internet, and Information Technology, Scottsdale, AZ, Nov. 17–19, 2003.
[65] N. Bourbakis and A. Dollas, "SCAN-based compression-encryption-hiding for video on demand," *IEEE Trans. Multimedia*, pp. 79–87, Jul.–Sep. 2003.
[66] C.-P. Wu and C.-C. J. Kuo, "Efficient multimedia encryption via entropy codec design," *Proc. SPIE Security Watermarking Multimedia Contents III*, vol. 4314, pp. 128–138, Jan. 2001.
[67] B. Macq and J.-J. Quisquater, "Cryptology for digital TV broadcasting," *Proc. IEEE*, vol. 83, no. 6, pp. 944–957, Jun. 1995.
[68] I. Agi and L. Gong, "An empirical study of secure MPEG video transmissions," in *Proc. Symp. Network Distributed System Security*, 1996, pp. 137–144.
[69] A. M. Alattar and G. I. Al-Regib, "Evaluation of selective encryption techniques for secure transmission of MPEG-compressed bitstreams," in *Proc. IEEE Int. Symp. Circuits and Systems*, 1999, pp. 340–343.

[70] W. Zeng and S. Lei, "Efficient frequency domain selective scrambling of digital video," *IEEE Trans. Multimedia*, vol. 5, pp. 118–129, Mar. 2003.
[71] J. G. Wen, M. Severa, W. Zeng, M. H. Luttrell, and W. Jin, "A format-compliant configurable encryption framework for access control of video," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 12, pp. 545–557, Jun. 2002.
[72] H. Cheng and X. Li, "Partial encryption of compressed images and videos," *IEEE Trans. Signal Process.*, vol. 48, pp. 2439–2451, Aug. 2000.
[73] D. Wu, Y. T. Hou, and Y.-Q. Zhang, "Transporting real-time video over the internet: Challenges and approaches," *Proc. IEEE*, vol. 88, no. 12, pp. 1855–1875, Dec. 2000.
[74] A. Vetro, C. Christopoulos, and H. Sun, "Video transcoding architectures and techniques: An overview," *IEEE Signal Process. Mag.*, vol. 20, pp. 18–29, Mar. 2003.
[75] M. Karczewicz and R. Kurceren, "The SP- and Si-frames design for H.264/AVC," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, pp. 637–644, Jul. 2003.
[76] T. Ebrahimi and C. Home, "MPEG-4 natural video coding—An overview," *Signal Process. Image Commun.*, vol. 15, no. 4, pp. 365–385, 2000.
[77] G. Cote, B. Erol, M. Gallant, and F. Kossentini, "H.263+: Video coding at low bit rates," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 8, pp. 849–866, Nov. 1998.
[78] H.-C. Huang, C.-N. Wang, and T. Chiang, "A robust fine granularity scalability using trellis-based predictive leak," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 12, no. 6, pp. 372–385, Jun. 2002.
[79] C. Yuan, B. B. Zhu, Y. Wang, S. Li, and Y. Zhong, "Efficient and fully scalable encryption for MPEG-4 FGS," in *Proc. Int. Symp. Circuits Syst.*, vol. 2, 2003, pp. 620–623.
[80] A. M. Eskicioglu and E. J. Delp, "An integrated approach to encrypting scalable video," in *Proc. IEEE Int. Conf. Multimedia Expo*, vol. 1, 2002, pp. 573–576.
[81] S. J. Wee and J. G. Apostolopoulos, "Secure scalable streaming enabling transcoding without decryption," in *Proc. Int. Conf. Image Processing*, vol. 1, 2001, pp. 437–440.
[82] M. Maes, T. Kalker, J.-P. M. G. Linnartz, J. Talstra, G. F. G. Depovere, and J. Haitsma, "Digital watermarking for DVD video copy protection," *IEEE Signal Process. Mag.*, vol. 17, pp. 47–57, Sep. 2000.
[83] G. Doërr and J.-L. Dugelay, "A guide tour of video watermarking," *Signal Process. Image Commun.*, vol. 18, no. 4, pp. 263–282, Apr. 2003.
[84] I. Cox, M. Miller, and J. Bloom, *Digital Watermarking*. San Francisco, CA: Morgan Kaufmann, 2002.
[85] C. I. Podilchuk and E. J. Delp, "Digital watermarking: Algorithms and applications," *IEEE Signal Process. Mag.*, vol. 18, pp. 33–46, Jul. 2001.
[86] M. Barni, C. I. Podilchuk, F. Bartolini, and E. J. Delp, "Watermark embedding: Hiding a signal within a cover image," *IEEE Commun. Mag.*, pp. 102–108, Aug. 2001.
[87] G. Langelaar, I. Setyawan, and R. Lagendijk, "Watermarking digital image and video data: A state-of-the-art overview," *IEEE Signal Process. Mag.*, vol. 17, pp. 20–46, Sep. 2000.
[88] M. Kutter. (2000) Digital Watermarking World. [Online]. Available: http://www.watennarkingworld.org
[89] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proc. IEEE*, vol. 87, no. 7, pp. 1079–1107, Jul. 1999.
[90] R. Wolfgang, C. Podilchuk, and E. Delp, "Perceptual watermarks for digital images and video," *Proc. IEEE*, vol. 87, no. 7, pp. 1108–1126, Jul. 1999.
[91] M. Barni, F. Bartolini, and A. D. Rosa, "Advantages and drawbacks of multiplicative spread spectrum watermarking," *Proc. SPIE Security Watermarking of Multimedia Contents V*, pp. 290–299, Jan. 2003.
[92] J. J. Eggers, R. Bäuml, R. Tzschoppe, and B. Girod, "Scalar costa scheme for information embedding," *IEEE Trans. Signal Process.*, vol. 15, pp. 1003–1019, Apr. 2003.
[93] B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Trans. Inform. Theory*, vol. 47, pp. 1423–1443, May 2001.
[94] I. Setyawan, G. Kakes, and R. L. Lagendijk, "Synchronization-insensitive video watermarking using structured noise pattern," *Proc. SPIE Security Watermarking of Multimedia Contents IV*, pp. 520–530, Jan. 2002.
[95] J. Dittmann, T. Fiebig, and R. Steinmetz, "A new approach for transformation invariant image and video watermarking in the spatial domain: SSP—Self spanning patterns," *Proc. SPIE Security Watermarking of Multimedia Contents II*, vol. 3971, pp. 176–185, Jan. 2000.
[96] T. Kalker, G. Depovere, J. Haitsma, and M. Maes, "A video watermarking system for broadcast monitoring," *Proc. SPIE Security Watermarking of Multimedia Contents*, vol. 3657, pp. 103–112, Jan. 1999.
[97] F. Deguillaume, G. Csurka, J. O'Ruanaidh, and T. Pun, "Robust 3D DFT video watermarking," *Proc. SPIE Security Watermarking Multimedia Contents I*, vol. 3657, pp. 113–124, Jan. 1999.
[98] X. Kang, J. Huang, Y. Q. Shi, and Y. Lin, "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, pp. 776–786, Aug. 2003.
[99] A. M. Alattar, E. T. Lin, and M. U. Celik, "Digital watermarking of low bit-rate advanced simple profile MPEG-4 compressed video," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, pp. 787–800, Aug. 2003.
[100] G. C. Langelaar and R. L. Lagendijk, "Optimal differential energy watermarking of DCT encoded images and video," *IEEE Trans. Image Process.*, vol. 10, pp. 148–158, Jan. 2001.
[101] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," *Signal Process.*, vol. 66, no. 3, pp. 283–301, May 1998.
[102] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, pp. 1673–-1687, Dec. 1997.
[103] C. V. Serdean, M. A. Ambroze, M. Tomlinson, and J. G. Wade, "DWT-based high capacity blind video watermarking, invariant to geometrical attacks," in *Proc. IEEE Vision, Image Signal Processing*, vol. 150, 2003, pp. 51–58.
[104] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Multiresolution scene-based video watermarking using perceptual models," *IEEE J. Sel. Areas Commun.*, vol. 16, pp. 540–550, May 1998.
[105] J. Dittmann, M. Steinebach, I. Rimac, S. Fischer, and R. Steinmetz, "Combined video and audio watermarking: Embedding content information in multimedia data," *Proc. SPIE Security Watermarking Multimedia Contents II*, vol. 3971, pp. 455–464, Jan. 2000.
[106] J. F. Delaigle, C. Devleeschouwer, B. Macq, and I. Lagendijk, "Human visual system features enabling watermarking," in *Proc. IEEE Int. Conf. Multimedia Expo*, vol. 2, 2002, pp. 489–492.
[107] J. Eggers and B. Girod, *Informed Watermarking*. Boston, MA: Kluwer, 2002.
[108] J. K. Su and B. Girod, "Power-spectrum condition for energy-efficient watermarking," *IEEE Trans. Multimedia*, vol. 4, pp. 551–560, Dec. 2002.
[109] S. Voloshynovskiy, F. Deguillaume, S. Pereira, and T. Pun, "Optimal adaptive diversity watermarking with channel state estimation," *Proc. SPIE Security Watermarking Multimedia Contents III*, vol. 4314, pp. 673–685, Jan. 2001.
[110] S. Voloshynovskiy, S. Pereira, V. Iquise, and T. Pun, "Attack modeling: Toward a second generation watermarking benchmark," *Signal Process.*, vol. 81, no. 6, pp. 1177–1214, Jun. 2001.
[111] S. Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers, and J. K. Su, "Attacks on digital watermarks: Classification, estimation-based attacks, and benchmarks," *IEEE Commun. Mag.*, vol. 39, pp. 118–126, Aug. 2001.
[112] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Attacks on copyright marking systems," in *Proc. 2nd Int. Workshop Information Hiding*, 1998, pp. 219–239.
[113] Y. Bodo, N. Laurent, and J.-L. Dugelay, "Watermarking video, hierarchical embedding in motion vectors," in *Proc. IEEE Int. Conf. Image Processing*, vol. 2, 2003, pp. 739–742.
[114] J. Zhang, J. Li, and L. Zhang, "Video watermark technique in motion vector," in *Proc. 14th Brazilian Symp. Computer Graphics and Image Processing*, 2001, pp. 179–182.
[115] G. C. Langelaar, R. L. Lagendijk, and J. Biemond, "Real-time labeling of MPEG-2 compressed video," *J. Visual Commun. Image Representat.*, vol. 9, no. 4, pp. 256–270, Dec. 1998.
[116] R. Chandramouli and N. D. Memon, "On sequential watermark detection," *IEEE Trans. Signal Process.*, vol. 51, pp. 1034–1044, Apr. 2003.
[117] W. Fumy and P. Landrock, "Principles of key management," *IEEE J. Sel. Areas Commun.*, vol. 11, pp. 785–793, Jun. 1993.

[118] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 644–654, Nov. 1976.
[119] R. M. Needham and M. D. Schroeder, "Using encryption for authentication in large networks of computers," *Commun. ACM*, vol. 21, no. 12, pp. 993–999, Dec. 1978.
[120] P. Judge and M. Ammar, "Security issues and solutions in multicast content distribution: A survey," *IEEE Network*, vol. 17, no. 1, pp. 30–36, Jan./Feb. 2003.
[121] W. Trappe, J. Song, R. Poovendran, and K. J. R. Liu, "Key management and distribution for secure multimedia multicast," *IEEE Trans. Multimedia*, vol. 5, pp. 544–557, Dec. 2003.
[122] R. Mukherjee and J. W. Atwood, "Proxy encryptions for secure multicast key management," in *Proc. 28th Annu. IEEE Int. Conf. Local, Computer Networks*, 2003, pp. 377–384.
[123] K.-C. Chan and S.-H. G. Chan, "Key management approaches to offer data confidentiality for secure multicast," *IEEE Network*, vol. 17, no. 5, pp. 30–39, Sep./Oct. 2003.
[124] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," *ACM Comput. Surveys*, vol. 35, no. 3, pp. 309–329, Sep. 2003.
[125] A. Wool, "Key management for encrypted broadcast," *ACM Trans. Inform. Syst. Security*, vol. 3, no. 2, pp. 107–134, May 2000.
[126] M. J. Moyer, J. R. Rao, and P. Rohatgi, "A survey of security issues in multicast communications," *IEEE Network*, vol. 13, no. 6, pp. 12–23, Nov./Dec. 1999.
[127] H. hua Chu, L. Qiao, and K. Nahrstedt, "A secure multicast protocol with copyright protection," *Proc. SPIE Security Watermarking of Multimedia Contents*, vol. 3657, pp. 460–471, Jan. 1999.
[128] I. Brown, C. Perkins, and J. Crowcroft, "Watercasting: Distributed watermarking of multicast media," in *Proc. Networked Group Communication '99*, pp. 286–300.
[129] P. Judge and M. Ammar, "WHIM: Watermarking multicast video with a hierarchy of intermediaries," presented at the 10th Int. Workshop Network Operation System Support Digital Audio Video, Chapel Hill, NC, 2000.
[130] G. Caronni and C. Schuba, "Enabling hierarchical and bulk-distribution for watermarked content," presented at the 17th Annu. Computer Security Applications Conf., New Orleans, LA, 2001.
[131] D. Kirovski and F. A. P. Petitcolas, "Blind pattern matching attack on watermarking systems," *IEEE Trans. Signal Process.*, vol. 51, pp. 1045–1053, Apr. 2003.
[132] S. Voloshynovskiy, S. Pereira, A. Herrigel, N. Baumgartner, and T. Pun, "Generalized watermarking attack based on watermark estimation and perceptual remodulation," *Proc. SPIE Security Watermarking Multimedia Contents II*, vol. 3971, pp. 358–370, Jan. 2000.
[133] E. T. Lin and E. J. Delp, "Temporal synchronization in video watermarking," *IEEE Trans. Signal Process.*, vol. 52, no. 10, pp. 3007–3022, Oct. 2004.
[134] H. Liu, N. Chen, J. Huang, X. Huang, and Y. Q. Shi, "A robust DWT-based video watermarking algorithm," in *Proc. IEEE Int. Symp. Circuits Systems*, vol. 3, 2002, pp. 631–634.
[135] C.-Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, and Y. M. Lui, "Rotation, scale, and translation resilient watermarking for images," *IEEE Trans. Image Process.*, vol. 10, pp. 767–782, May 2001.
[136] J. J. O'Ruanaidh and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Signal Process.*, vol. 66, no. 3, pp. 303–317, May 1998.
[137] X. Niu, M. Schmucker, and C. Busch, "Video watermarking resisting to rotation, scale, and translation," *Proc. SPIE Security Watermarking of Multimedia Contents IV*, vol. 4675, pp. 512–519, Jan. 2002.
[138] N. V. Boulgouris, F. D. Koravos, and M. G. Strintzis, "Self-synchronizing watermark detection for MPEG-4 objects," in *Proc. 8th IEEE Int. Conf. Electronics, Circuits, Systems 2001*, vol. 3, 2001, pp. 1371–1374.
[139] D. Delannay and B. Macq, "Generalized 2-D cyclic patterns for secret watermark generation," in *Proc. IEEE Int. Conf. Image Processing*, vol. 2, 2000, pp. 77–79.
[140] P. Bas, J.-M. Chassery, and B. Macq, "Geometrically invariant watermarking using feature points," *IEEE Trans. Image Process.*, vol. 11, pp. 1014–1028, Sep. 2002.
[141] G. Doërr and J.-L. Dugelay. (2003, Jul.) Switching between orthogonal watermarks for enhanced security against collusion in video. Eurécom Institute. [Online]. Available: http://www.eurecom.fr/~doerr
[142] M. U. Celik, G. Sharma, and A. M. Tekalp, "Collusion-resilient fingerprinting using random pre-warping," in *Proc. IEEE Int. Conf. Image Processing*, 2003, pp. 509–512.
[143] W. Trappe, M. Wu, and K. J. R. Liu, "Anti-collusion codes: Multiuser and multimedia perspectives," in *Proc. IEEE Int. Conf. Image Processing*, vol. 2, 2002, pp. 149–152.
[144] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Trans. Inf. Theory*, vol. 44, pp. 1897–1905, Sep. 1998.
[145] A. Adelsbach, S. Katzenbeisser, and H. Veith, "Watermarking schemes provably secure against copy and ambiguity attacks," in *Proc. ACM Workshop Digital Rights Management*, 2003, pp. 111–119.
[146] M. Barni, F. Bartolini, and T. Furon, "A general framework for robust watermark security," *Signal Process.*, vol. 83, no. 10, pp. 2069–2084, Oct. 2003.
[147] F. Deguillaume, S. Voloshynovskiy, and T. Pun, "Secure hybrid robust watermarking resistant against tampering and copy attack," *Signal Process.*, vol. 83, no. 10, pp. 2133–2170, Oct. 2003.
[148] C.-S. Lu, H.-Y. M. Liao, and M. Kutter, "Denoising and copy attacks resilient watermarking by exploiting prior knowledge at detector," *IEEE Trans. Image Process.*, vol. 11, pp. 280–292, Mar. 2002.
[149] M. Kutter, S. Voloshynovskiy, and A. Herrigel, "The watermark copy attack," *Proc. SPIE Security Watermarking Multimedia Contents II*, vol. 3971, pp. 371–380, Jan. 2000.
[150] M. Holliman and N. Memon, "Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes," *IEEE Trans. Image Process.*, vol. 9, pp. 432–441, Mar. 2000.
[151] B. Macq, J. Dittmann, and E. J. Delp, "Benchmarking of image watermarking algorithms for digital rights management," *Proc. IEEE*, vol. 92, no. 6, pp. 971–984, Jun. 2004.
[152] H. C. Kim, H. Ogunley, O. Guitart, and E. J. Delp, "The watermark evaluation testbed," presented at the SPIE Int. Conf. Security, Steganography, Watermarking VI, San Jose, CA, 2004.

Eugene T. Lin (Student Member, IEEE) was born in Stillwater, OK, in 1973. He received the B.S. degree in computer and electrical engineering and M.S. degree in electrical engineering from Purdue University, West Lafayette, IN, in 1994 and 1996, respectively. He is currently pursuing the Ph.D. degree in video watermarking techniques at the same university.

He was an Intern at Lucent Technologies in the summer of 2000. In 2001 and 2002, he was a summer Intern at Digimarc Corporation. His research interests include video watermarking and steganography, as well as video coding and image processing.

Mr. Lin is a Student Member of Eta Kappa Nu.

Ahmet M. Eskicioglu received the B.S. degree from the Middle East Technical University (METU), Ankara, Turkey, and the M.S. and Ph.D. degrees from the University of Manchester Institute of Science and Technology (UMIST), U.K.

He is with the Department of Computer and Information Science, Brooklyn College, City University of New York. He has actively participated in the development of several national and international standards for copy protection and conditional access in the U.S. and Europe. These include the content scramble system (CSS) for DVD players, the Advanced Television Systems Committee (ATSC) conditional access system architecture, the Electronics Industries Alliance (EIA) National Renewable Security Standard (NRSS), and the European Union's Digital Video Broadcasting (DVB) Content Protection and Copy Management (CPCM) System. He holds several patents on copy protection, conditional access, and digital interface protection. His teaching and research interests include data security, conditional access, digital rights management, copy protection, digital watermarking, and multimedia applications.

Reginald L. Lagendijk (Senior Member, IEEE) received the Ph.D. degree from Delft University of Technology, Delft, The Netherlands, in 1990.

He has been a Full Professor and Head of the Information and Communication Theory Group at Delft University of Technology since 1999. His research background is in stochastic signal processing and information theory. In particular, he is interested in the question of how visual information can be represented such that it is not only efficient in communication bandwidth or storage capacity, but that it is also easily accessible when stored in large volumes, that it is robust against errors when transmitted, that it can be used to embed secret information, and that it has a good visual quality. Research projects he is involved in cover subjects such as image and video compression, image quality measures, watermarking, image and video libraries, wireless media streaming, and image sequence restoration and enhancement. He has coauthored several books on imaging. In recent years, he has led or been involved in several research projects such as "Ubiquitous Communications," Freeband's "Context-Aware Communications, Terminal, and User," and European projects like CERTIMARK and STORit.

Dr. Lagendijk has served as Editor of the IEEE TRANSACTIONS ON SIGNAL PROCESSING AND IMAGE PROCESSING and Editor of SIGNAL PROCESSING: IMAGE COMMUNICATIONS, and the organization of the International Conference on Image Processing ICIP2001 (Thessaloniki, Greece) and ICIP2003 (Barcelona, Spain).

Edward J. Delp (Fellow, IEEE) was born in Cincinnati, OH. He received the B.S.E.E. (*cum laude*) and M.S. degrees from the University of Cincinnati and the Ph.D. degree from Purdue University, West Lafayette, IN. In May 2002, he received an Honorary Doctor of Technology from the Tampere University of Technology, Tampere, Finland.

From 1980 to 1984, he was with the Department of Electrical and Computer Engineering, The University of Michigan, Ann Arbor. Since August 1984, he has been with the School of Electrical and Computer Engineering and the Department of Biomedical Engineering at Purdue University. In 2002, he received a chaired professorship and currently is The Silicon Valley Professor of Electrical and Computer Engineering and a Professor of Biomedical Engineering. His research interests include image and video compression, multimedia security, medical imaging, multimedia systems, communication, and information theory.

Dr. Delp is a Fellow of the SPIE, the Society for Imaging Science and Technology (IS&T), and the American Institute of Medical and Biological Engineering. In 2000, he was selected a Distinguished Lecturer of the IEEE Signal Processing Society.