Editor: Nevenka Dimitrova
*Phillips Research*

# Spies, Thieves, and Lies: The Battle for Multimedia in the Digital Era

**Hong Heather Yu**
*Panasonic*

**Deepa Kundur**
*University of Toronto*

**Ching-Yung Lin**
*IBM*

Multimedia security has become an immediate concern for content providers, artists, and the entertainment industry. The apparent panic over the need for an effective mechanism for digital media rights protection echoes in many of today's news stories. The fundamental cause for this frenzy is the leakage problem.

The leakage problem involves the illegal duplication, unlawful tampering, and wrongful distribution of media. Because of the popularity of handheld digital cameras, online news magazines, and movies on digital versatile disk (DVD), traditional forms of analog media are being replaced with new digital counterparts. Advances in digital media storage, duplication, editing, and transmission technologies have made this alternative more flexible, scalable, and cost effective for emerging applications. Ironically, however, these same appealing conveniences have facilitated large-scale piracy of and unlawful tampering with digital content. Because of analog media's media, high-quality duplication is expensive and therefore inaccessible to the average consumer.

Although people can duplicate VHS tapes and audiocassettes, the quality of these copies is noticeably inferior to the original. As people generate copies from copies, the continual reduction of signal fidelity destroys the content's commercial value. Thus, analog media is inherently resistant to large-scale duplication, which is the reason media piracy hasn't been a significant issue in the past.

In contrast, we can easily produce perfect bit-by-bit copies of digital media, making it impossible to distinguish between an original and its duplicate. The wide availability of digital copying tools further aggravates the piracy problem. For instance, equipped with a CD rewriteable drive (available for approximately $150) and Adaptec Easy CD Creator software (available for free), the average consumer can copy a CD album or collection of songs downloaded from the Internet onto a $0.50 CD-R disk in approximately one hour.

## The battle begins

Despite new legislation by governments and the ongoing efforts of the entertainment and high-tech industries, there's been little progress in preventing multimedia theft and tampering. One example involves the CSS (Content Scrambling System, http://www.dvdcca.org/dvdcca/css) v. the De-Content Scrambling System (DeCSS) legal battle. (You can find more information about DeCSS at http://decss.robinlionheart.com/). In November 1999, a small group of Norwegian hackers cracked the CSS, the officially licensed DVD-video digital encryption scheme used for copy protection. The hackers called it DeCSS and made it available for widespread download on the Internet. DeCSS made it possible to save DVD movies—normally stored in encrypted form to prevent unlawful access of the copyrighted video without a legitimate decryption chip—in unscrambled form on the hard disks of computers. This made the content vulnerable to large-scale duplication and tampering. As a result, in December 1999, the DVD CCA (Content Control Association) sued over 500 people in at least 11 nations related to the incident, claiming misappropriation of trade secrets. Legal cases related to DeCSS are still pending in court (visit http://www.lemuria.org/DeCSS/press.html for related news).

Because of the social, economic, and scientific nature of media piracy, the multimedia security problem involves multidisciplinary collaboration among scientists and the entertainment, information technology, and consumer electronics industries. The number of established and emerging standards bodies working on digital content protection issues demonstrates the significance of the issue. Well-known working groups include the



1070-986X/01/$10.00 © 2001 IEEE

DVD Copy Protection Technical Working Group (CPTWG) and the Secure Digital Music Initiative (SDMI). Many standards forums also have ad-hoc groups working on digital rights management and content protection (see the "Copyright Protection Forums" sidebar).

### Traditional and emerging technologies for multimedia security

Multimedia security has three main objectives:

- authentication to assure the credibility of multimedia information;
- confidentiality to secure content transmission privacy; and
- copy control to protect multimedia data from illegal distribution and theft.

Traditionally, we use cryptographic tool sets to address data authentication and confidentiality. We commonly use encryption and hash functions to establish the integrity and privacy of data. However, because of multimedia data's diversity, perceptual nature, and volume, these conventional approaches are somewhat insufficient for today's applications. The high sensitivity of conventional hash functions makes them impractical for verifying media subsequently compressed or converted into another format. Furthermore, the varying data sizes and high volume of multimedia make it too complex and cumbersome to use standard encryption algorithms optimized for traditional data.

More importantly, traditional authentication and encryption algorithms don't address leakage. Cryptographic functions applied to multimedia can detect information tampering and protect the communication channel used for transmission from eavesdropping. Without a secret key, an attacker can't successfully view, modify, or fabricate information without detection. However, after we decrypt information, no mechanism exists to protect against unauthorized media duplication. This problem is known as leakage—that is, once encryption is inactive and the content is available for viewing, it's susceptible to piracy. DeCSS, for example, essentially decrypts DVD movies and facilitates free storage and circulation without requiring royalty payments to the motion picture industry.

To solve these problems, a few years ago scientists and researchers proposed a new technology known as *digital watermarking*. Adopting digital watermarking for DVD video, DVD audio, and digital music—among many others—is currently under investigation. Numerous conferences and workshops demonstrate the effort, such as the Information Hiding Workshop sponsored by the International Federation for Information Processing (IFIP), Multimedia Security Workshop at ACM

## Copyright Protection Forums

This list of forums demonstrates the intensity of the war between the content industry and hackers.

- The Copyright Protection Technical Working Group (CPTWG, http://cptwg.org/) concentrates on standardizing copy protection tools for digital interfaces and watermarking for DVD video and audio content.
- The Intellectual Property Management and Protection group of the Moving Picture Experts Group (ISO/IEC JTC1/SC/29/WG11, see http://www.cselt.it/mpeg/ and http://www.mpeg.org/) focuses on extended interfaces to associate IPMP to MPEG-4 applications.
- TV Anytime Forum (http://www.tv-anytime.org/) aims to include transparent and user-friendly security elements to maintain the integrity of copyright material and to ensure that illicit duplication doesn't occur.
- The Digital Versatile Disk Forum (http://www.dvdforum.org/) is working to standardize DVDs with its working group 9/ad-hoc group 1 (WG-9/AH-1). They also focus on standardizing copy protection for DVD system architectures. The working group 6/ad-hoc group 8 (WG-6/AH-8) is standardizing copy protection for DVD-Rs.
- The Secure Digital Music Initiative's charter (http://www.sdmi.org/) is to develop open technology specifications that protect legitimate playing, storing, and distribution of digital music to boost a new market. SDMI's open technology specifications provide consumers with convenient access to music in any emerging digital distribution system, enable copyright protection for artists' works, and promote the development of new music-related business and technologies.
- One theme of the Open Platform Initiative for Multimedia Access (http://www.cselt.it/ufv/leonardo/opima/) is standardizing an open generic framework for access control and content management and protection (CMP) tools on downloadable and/or replaceable security for Internet and pay TV applications. The OPIMA platform targets value-chain participants and provides the ability to acquire, supply, process, and consume multimedia services worldwide in accordance with the rights associated with these services. OPIMA specifically addresses intellectual-property management and protection.
- The Digital Audio–Visual Council (http://www.davic.org/) has produced a general copy-protection framework baseline document in their line of work on the standardization of digital TV and interactive applications.

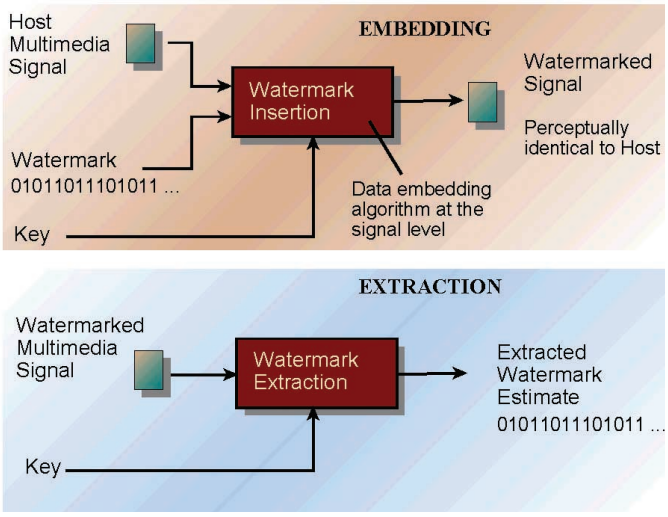


*Figure 1. Watermark embedding and extraction.*

Multimedia, and sessions at the IEEE International Conference on Information Technology: Coding and Computing (ITCC) and IEEE International Conference on Multimedia and Expo (ICME).

Digital watermarking is the process by which we imperceptibly embed a discreet data stream (possibly a security code or signal tag) into a digital media file using steganographic (data hiding) principles. The original media is the *host*, the hidden signal is the *watermark*, and the overall composite signal is the *watermarked signal*. In addition, we can use a secret key to embed and extract a watermark, resisting unwanted parties extracting and manipulating a watermark. It should be possible to extract or detect the embedded watermark (depending on the application) without any reference to the host signal. Figure 1 shows a description of digital watermarking.

We categorize digital watermarking into two broad classes: fragile and robust. As the name implies, a fragile watermark is one that can't survive most kinds of modifications on the watermarked media. A robust watermark, on the other hand, can endure common signal processing and some level of intentional modifications of the marked signal. For multimedia security, we use fragile watermarks for media authentication and tamper proofing. We detect any modification of the embedded watermark to assess tampering. Scientists in the computer, communications, and signal processing research communities have proposed robust watermarks to address the leakage problem. Embedding a stamp or access control code can actively or passively control digital rights management using a compliant media player.

We can also use hybrid, semifragile watermarks (which survive some acceptable manipulations while rejecting malicious manipulations) for media authentication and recovery. Figure 2 is an example of a self-authentication-and-recovery image (SARI, http://www.ctr.columbia.edu/sari) based on a semifragile watermark. The SARI system, developed by researchers at Columbia University, can detect malicious manipulations, retrieve the manipulated positions, and recover an approximation of the discarded area. This prototype system shows how watermarking helps reconstruct multimedia's trustworthiness in the digital era.

The design of an effective digital watermarking system involves developing an application-specific technique that exhibits an appropriate compromise to the watermark's imperceptibility, the embedded mark's robustness or fragility after media manipulation, portability to different media, computational complexity, and statistical measures of false watermark extraction or detection. In addition, it's interesting to evaluate the maximum number of bits reliably tagged in and later extracted from the media, known as data-hiding capacity (DHC). Effective watermarking often borrows ideas from established tool sets in the areas of data communications, human perception or psychology, traditional security, data fusion, and subliminal channels. Modeling the watermarking problem using any one or more of these analogies provides insight into general design principles.

Different DHC requirements exist for different applications. For instance, if we need watermarking to specify a media-access level, then we need a control number that requires a DHC of only a few bits-per-medium. Multilayer data-hiding schemes that involve a number of different types of embedded data for various objectives—such as error correction control, authentication, and synchronization information—may require a higher DHC.

Security and robustness of any hidden data must be based on Kerchoff's assumption—that is, the strength of the watermarking system must not be based on the fact that an attacker doesn't know the algorithmic details. The lack of knowledge of a secret key should keep the watermark secure from unwanted extraction, forgery, or elimination. This requirement has proven challenging so far. In the last several months, a group of nine scientists from Princeton University, Rice University, and Xerox Palo Alto Research Center claimed they broke audio watermarking algorithms for copy protection that SDMI selected for a public challenge (see http://news.zdnet.co.uk/story/0,,s2082137,00.html).

## Multimedia security: present and future challenges

The evolution of digital content has disrupted traditional media distribution and business models. For instance, the unlawful MP3 circulation through Napster, the infamous online content-swapping program, shifted media circulation control from several large players in the recording industry to smaller, more versatile players. Furthermore, the ability to adapt and suit the needs of individual consumers is an emerging measure of business success. This movement toward empowering the individual also influences the requirements for security. In turn, we must make security more personal by tying it to the media or a specific consumer using variations of conventional security algorithms or novel solutions such as digital watermarking.

There are many degrees of security. Because of the nature of the applications, multimedia security isn't concerned with a holy grail of system protection. Instead, it involves developing a suite of practical services that increase the pain threshold of breaking a system for the average consumer without sacrificing user convenience. We can't incorporate media security solutions into a single technology. For protection against diverse forms of attacks for a variety of media in a constantly changing environment, security is an evolving process that's as strong as its weakest component.

So where do we go from here? A number of specific technical issues still remain unresolved.

- *Layered protection systems*. Scrambling systems, such as CSS, are designed for transmission privacy from the content provider to legitimate consumers. They weren't designed to provide copy control functionality. Whenever someone descrambles multimedia content, encryption doesn't prevent illegal distribution. That's why layered protection including both encryption and watermarking are necessary.

  Encryption, hash functions, and digital watermarking technologies are building blocks for an overall media-protection scenario. These tools must be effectively incorporated in hardware and software within different layers of a communication network to enforce and adapt media-access privileges. This type of layered security is appealing, especially for media digital rights management (DRM) applications. DRM, considered extensively in standards bodies, refers to mechanisms for describing and enforcing copyrights associated with networked digital data distribution.

- *Scalability*. Multimedia content protection methods including DRM approaches must adapt to the media's value, the content's lifespan, evolving threats, and consumer preferences. Future work should focus on developing multimedia security schemes that stand the test of time. For example, the longer opponents have to break a system, the more likely it is that they will succeed, especially with improved processor speeds.

- *Renewability*. The ability of a security system to recover from a successful attack by replacing one of its components, such as a secret key, with a newly generated or more secure component, is an important aspect of scalability. For example, in the case of DeCSS, if the CSS was renewable, a simple modification in one or more of the components would render DeCSS useless for future movies encrypted with the CSS. Effective schemes also make it possible to completely invalidate the compromised key and prevent it from being used to unlawfully decrypt information. Future research should investigate the scalability of such a system for different situations and applications.

- *Interoperability*. Interoperability refers to the ability of heterogeneous security systems to cooperate and ensure mutual security and

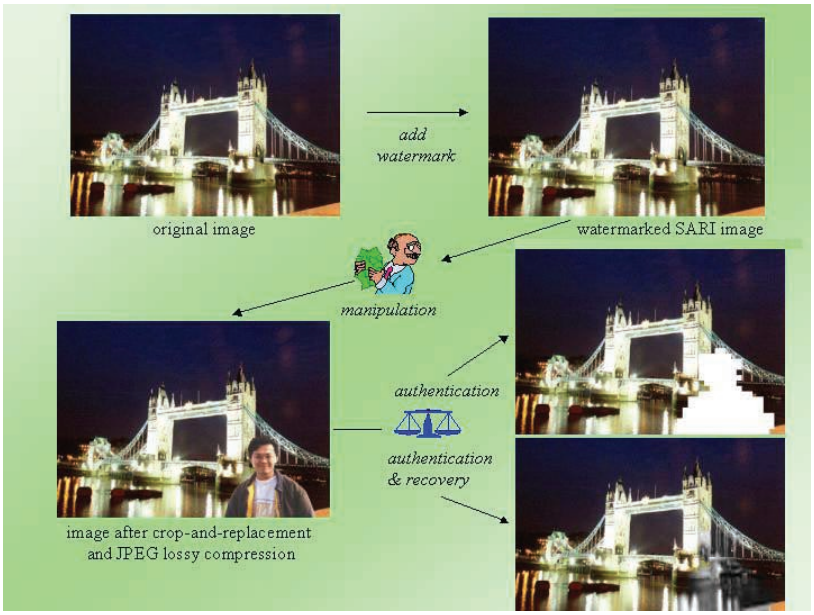


***Figure 2. An example of using semifragile watermarks to generate self-authentication-and-recovery images.***

compatibility of key security components in related systems. This problem becomes more important while multimedia content distribution is shifting from a centralized channel to network-based channels. Investigating and promoting content protection system interoperability with other related systems is a focal point in recent studies. The extent to which scalability advances interoperability and interoperability encourages scalability of the overall media protection system needs further investigation.

- *Active protection.* Recently, interest has increased in active security that initiates actions to defend or protect content. Passive forms of security such as encryption detect or prevent threats, but they don't react or attempt to recover after an attack. We expect active protection to improve the interactivity of security, facilitate traceability and audits, and allow more control over reaction to security breaches. An interesting possibility is the role of digital watermarking technology as a means of allowing implementation of such active protection capabilities. The SARI watermarking system is an example of active protection. Although traditional cryptography methods only tell whether the image is manipulated, the SARI images actively resist and recover from malicious changes.

- *The potential and role of digital watermarking.* There are still many unanswered questions to address concerning this slowly maturing technology. Is it feasible to make a watermark robust enough to aid against piracy? Digital watermarking uses human visual and auditory masking principles also employed in perceptual coding. However, digital watermarking tries to hide additional information while compression attempts to remove it. Hence, it's important to ask how digital watermarking and compression can combine to help instead of hinder the other's objectives. Perhaps we may never have a watermark robust enough to prevent its removal. Future use of watermarking may be limited to authentication or function switch flagging. We must assess the limits of the technology comprehensively to understand its potential and role for multimedia security.

- *Multimedia encryption tomorrow.* In 50 years, a computer might be $10^{xx}$ faster than currently available processors. To ensure security, will the key lengths grow to the order of $10^{xxx}$ bits? It's interesting to consider whether secure content scrambling of multimedia using long keys will still be practical for use in consumer electronics and electronic content distribution or if a new theory development will provide us an upper bound of the key length needed. Will generic encryption remain an important tool for content protection, or will more content-based application-specific approaches displace it?

## The battle shall continue

The constantly transforming needs of multimedia industries will provide challenges for multimedia security and the digital-media industry. In such a highly evolving and integrated environment where intellectual property isn't intended to be copied and modified freely, multimedia protection will be necessary. Perhaps industry will develop more complete and effective security solutions. No matter where the future leads us, the cycle of improving and then breaking improved security shall continue. We expect that no single technological improvement, lawsuit, government legislation, or international initiative will completely curb this cycle, and there won't be a single winner in this game to control or manipulate media distribution. We can hope for the speedy development of business, distribution, and protection models that benefit all parties, such as content users, creators, owners, and distributors. However, only joint efforts by content creators, owners, distributors, consumer electronic and IT industries, and scientific communities will solve the media battle quickly. **MM**

Readers may contact Yu at heathery@research.panasonic.com.