New Paradigms for Effective Multicasting and Fingerprinting of Entertainment Media

William Luh and Deepa Kundur, Texas A&M University

ABSTRACT

The large-scale adoption of network-centric entertainment systems rests on the ability to provide reliable, low-cost, and secure services for all parties in the entertainment distribution system. The use of modern data networks such as the Internet to communicate digital entertainment media is motivated, in part, by advancements in communication networking, signal processing, and storage technologies that facilitate more flexible and granular business models. This same technological progress can also be shown to equip potential "attackers" with the means to more easily violate system security. A broad class of system security issues for entertainment applications is addressed by the growing field of digital rights management. This article focuses on an aspect of DRM that involves multicast entertainment media distribution using digital encryption and digital fingerprinting technologies to prevent widespread piracy. The goal of DRM is to provide protection and facilitate equitable compensation for all parties in the entertainment distribution chain including content creators, aggregators, distributors, and consumers. Previous security proposals to protect entertainment media have sacrificed broadcast efficiency for security. This article collectively addresses security and broadcast efficiency for network-centric entertainment systems, an area of research seldom explored. We present the challenges, technological solutions, and future trends of this emerging field.

INTRODUCTION

To prevent piracy, practical digital rights management (DRM) requires persistent and economical methods of protection borrowing from fields including computer, network, and multimedia security. Commonly used primitives include encryption and digital fingerprinting functions. To effectively incorporate DRM into network-centric entertainment applications, networking issues such as effective bandwidth allocation and key management must be considered.

Encryption (which we call *level 1 security*), the most popular means of securing data while in storage and transmission, requires that a consumer, called a *user*, who wishes to purchase content from the *distributor* have previously exchanged an encryption key. Although the content is inaccessible while encryption is applied, once the data is decrypted for consumption it is possible for a user with access to this unprotected data to illegally distribute her copy in an underground entertainment network [1]. Such a user is called a *pirate* and such an attack is termed *piracy*.

Thus, a second level of security (which we call *level 2 security*) is required. One means of achieving this additional protection is to prevent the pirate from being able to unlawfully copy her decrypted media. This *active* form of security requires that any hardware capable of duplicating the entertainment content restrict action only to legitimate copying. One drawback, therefore, is that such hardware may have to be tamper-proofed, which is generally expensive (e.g., requiring users to purchase custom hardware) and sometimes unreliable [2]. In addition, a breach in one hardware console may have global consequences for all consoles, resulting in extensive system compromise; for example, the DRM system for DVD was hacked, and its secrets were made available on a Website in 1999 [3].

Another means to provide this additional level of post-decryption security (i.e., level 2 security) is by *deterring* instead of preventing piracy. This *passive* form of protection can be achieved by imperceptibly[1] embedding a unique buyer-dependent serial number, called the *fingerprint*, into the digital media, creating a slightly modified version of the entertainment media that is unnoticeable during consumption. A user is deterred from illegally copying and distributing her content because the hidden unique fingerprint can be used to trace her as the origin of the piracy within the entertainment network. The first challenge of this approach is that the differences among the fingerprinted copies of each user can be exploited by a coalition of pirates (colluders/attackers) to compare, detect, and remove these distinctions representing the fingerprint, or to create a fingerprint

---

[1] *Entertainment media such as audio media (music), and visual media (images and videos) have the property that data can be embedded into these media through application of subtle changes, and the resulting media will still have the same audio or visual qualities as perceived by a human.*

 77

belonging to an innocent user who is not part of the coalition (thus framing that user). This type of attack is known as *collusion*. The second challenge is the bandwidth inefficiency resulting from this approach; the unique fingerprints for each user result in unique copies of virtually the same content that must be sent individually to each user rather than more economically by exploiting the multicast protocol advantages of the Internet [1].

In this article we introduce the basic and related problems of digital fingerprinting and content distribution for passive security in entertainment networks. We present a novel fingerprinting approach for entertainment applications that allows the broadcasting of a single stream of data with size equal to that of the original enter-

tainment media to all users. Our concept also enables effective multicasting, in which *all* users receive an identical stream of data, and, in addition, *each* user receives a small unique stream of supplementary data that constitutes her fingerprint. We show that our method is not only more efficient at distribution, but also more secure against collusion attacks than traditional approaches.

PASSIVE SECURITY MODEL

In this article we focus on a broadcast distribution model in which a single content distributor provides the same digital entertainment to a group of predetermined subscribers. We assume that any secret keys required for security have
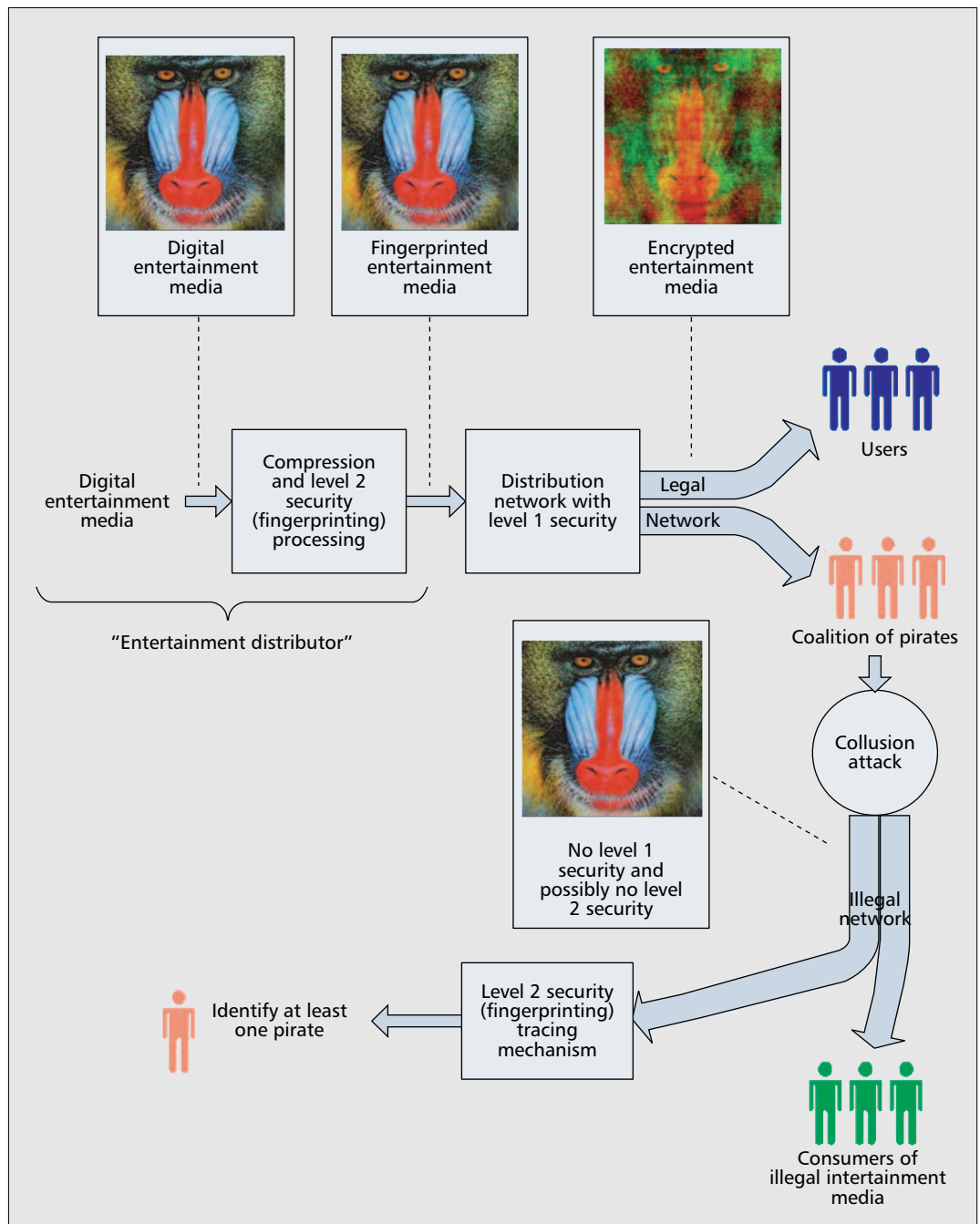
Figure 1. *The passive security entertainment network model.*
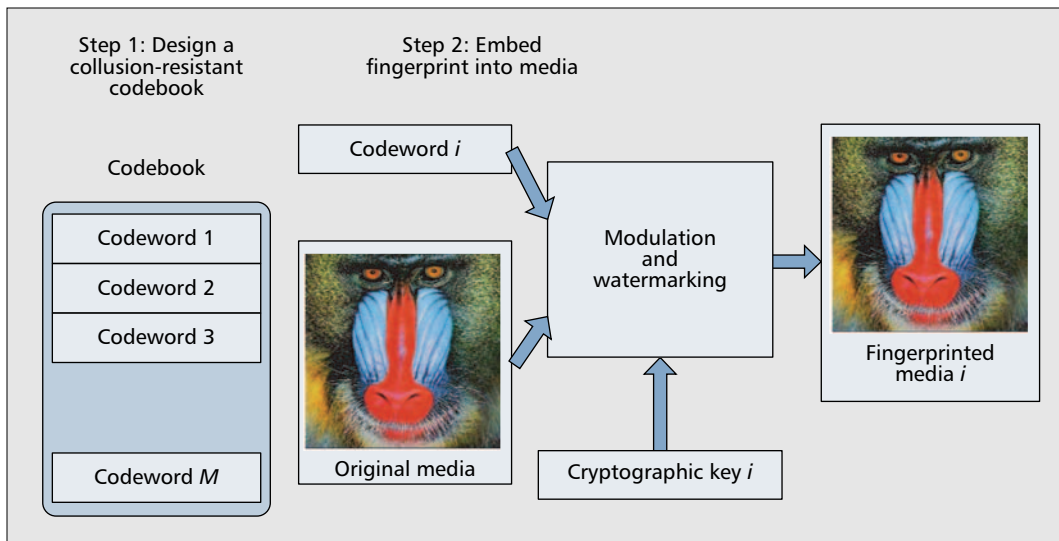
■ Figure 2. *Traditional 2-step "Codebook and Watermarking" level 2 fingerprinting security design.*

been previously exchanged between the distributor and users.

A popular model of passive security is depicted in Fig. 1. The goal of this security architecture is to deter piracy, while enabling bandwidth-efficient media distribution. We assume that the digital entertainment media (e.g., audio, images, and video) allow for certain signal processing to be applied without incurring any change in perceptual quality to the human user. The digital media first undergoes compression for bandwidth efficiency and level 2 security processing, such as fingerprinting, which is a passive means of security. The resulting fingerprinted content has the same perceptual quality as the original input digital media. This first step is generally performed by the *entertainment distributor*, who may be different than the content or the distribution rights holder.

The fingerprinted entertainment media is then transmitted to the users through the distribution network that applies encryption as a means to achieve level 1 security. In addition to achieving level 1 security, the goal of this network is to effectively transmit the fingerprinted entertainment to all legitimate users. Distribution efficiency, related to bandwidth efficiency, is a primary figure of merit.

Since the fingerprinted entertainment media is distributed to users who have legally purchased rights, the network associated with the distribution infrastructure is referred to as the *legal network*. As discussed earlier, the legal network is protected from piracy by level 1 security (i.e., encryption). Once the encrypted entertainment media is delivered through the legal network to the users, the users can decrypt the data with their previously established decryption keys. However, upon decryption, level 1 security is no longer valid, and a coalition of pirates are free to compare their uniquely fingerprinted entertainment media in hopes of removing all traces of their fingerprints, making it impossible to identify the origin of the piracy. At this point the entertainment media is said to have been "attacked," and the attacked entertainment

media can then be unlawfully sold through an underground entertainment network known as the *illegal network*.

In order for level 2 security to be effective against this attack, our model for passive protection includes a system that actively polls other networks (e.g., underground media distribution centers) to determine if they own the rights to circulate the content. We call this component the *tracing mechanism*, which searches for fingerprints in the digital entertainment media it polls. If detected fingerprints correspond to users who only have rights to personally consume but not redistribute or sell the entertainment, the tracing mechanism will identify such users as pirates. Subsequent prosecution of these pirates or other negative consequences may arise, thus creating a natural deterrent to piracy.

In the remainder of this article we present a popular class of fingerprinting approaches found in the literature to achieve level 2 security, and examine issues related to distribution efficiency. We also describe a novel paradigm to fingerprinting that has security features not found in previous approaches, and present a more efficient media distribution method that naturally arises from our new fingerprinting technique.

LEVEL 2 SECURITY: FINGERPRINTING VIA CODEBOOK AND WATERMARKING

Figure 2 depicts a popular approach to fingerprinting in which the design of the fingerprints is independent of the digital entertainment media. In step 1 a codebook with *collusion-resistant* properties is designed. Examples of collusion attacks include the *average* and *random attacks*. Details of collusion-resistant fingerprinting codes are found in [4, 5].

After the collusion-resistant fingerprinting codes are designed, each codeword (representing a unique fingerprint) is embedded into the digital entertainment media in question using digital watermarking techniques. In essence, watermarking imperceptibly hides the finger-
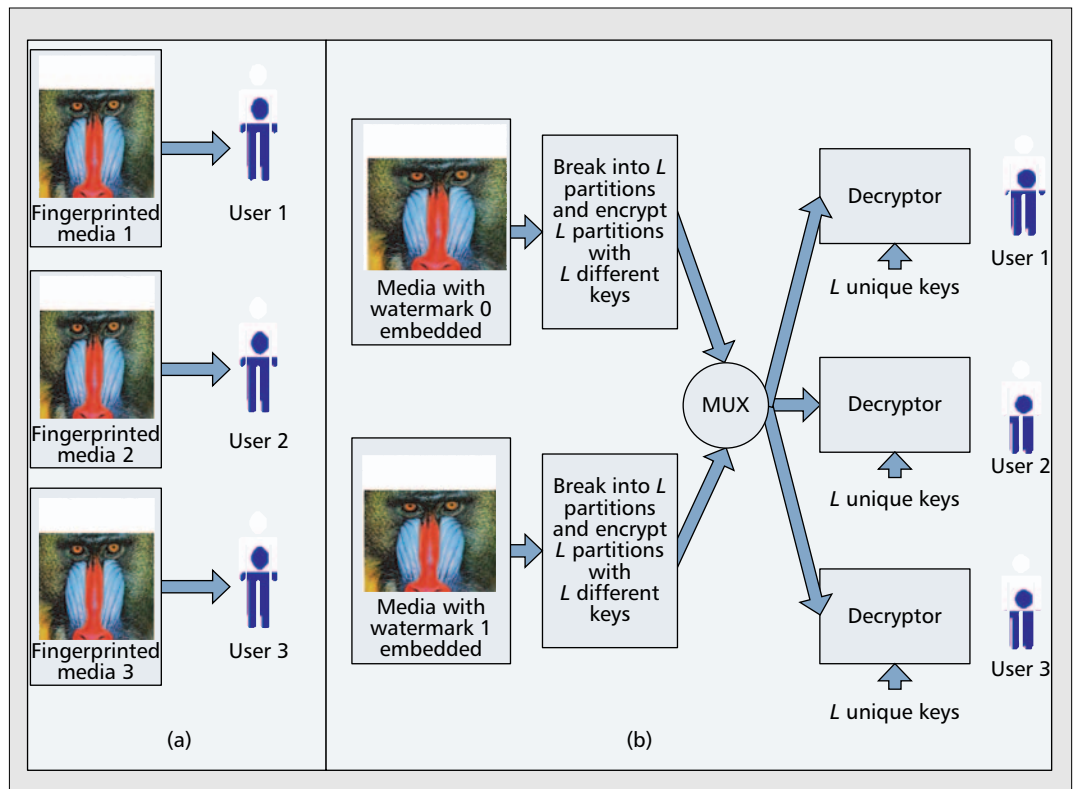
■ **Figure 3.** *a) Many-to-many distribution network in which each user receives a customized fingerprinted media; b) a better distribution network in which users receive 2 times the size of the original media, regardless of the number of users in the network.*

prints in the media so that the fingerprinted results appear perceptually identical to the original media. The fingerprints are hidden using unique secret keys unavailable to the users such that a fingerprint's exact whereabouts is unknown to each user, and a fingerprint cannot readily be removed by one user without causing perceptual distortion. An introduction to watermark design can be found in [6]. In addition to being obscured, the embedded fingerprints must also be robust to certain signal-processing-based collusion attacks to reinforce the collusion resistance initially developed during code design.

EFFICIENCY OF DISTRIBUTION NETWORKS

Once the entertainment media is fingerprinted, it is ready to be distributed to users. To investigate how efficiently distribution is carried out, we first look at a worst case naïve approach depicted in Fig. 3a. Here, each fingerprinted copy is uniquely sent to the corresponding user. Referring to Fig. 3a, we can think of this as each of the three users having her own *unique private channel* for transmission. If, however, there is only *one public channel* for use and there are three users, the channel must be *used three times*, thus overall sending three times the original size of the entertainment media. In this article we refer to the former channel as a *unicast channel* and the latter as a *broadcast channel*. We use the term *multicasting* for the

transmission of data using *both* the unicast and broadcast channels. Qualitatively, an entertainment network that adopts the passive security model is *efficient* if it incorporates both the broadcast and unicast channels such that the broadcast channel is used *M* times where *M* is small, while the unicast channel is seldom employed. We base this qualitative measurement of efficiency on the assumptions and studies of [7, 8] that show it is indeed cheaper to use the broadcast channel (termed *multicast* by these papers) than to use the unicast channel. As discussed, the distribution network in Fig. 3a can be interpreted as either solely using the broadcast channel (multiple times proportional to the number of users in the network) or only the unicast channel. Therefore, qualitatively this distribution network is not efficient.

Quantitatively, the efficiency of a distribution network *D* is measured relative to the purely naïve broadcasting scenario of Fig. 3a) and can be defined by the ratio given in Eq. 1 [7],

$$\eta_D \coloneqq \frac{m_D}{m_0}, \tag{1}$$

where m_D is a value proportional to the bandwidth used by network *D*, and m_0 is a value proportional to the bandwidth used in the broadcast channel case. In particular, m_0 is defined to be the number of times the broadcast channel is used when the distribution network is that in Fig. 3a, and m_D is the number of times the broadcast channel is used by the distribution network *D*. In Eq. 1 we assume that only the broadcast channel is available, and any data that

is to be sent through the unicast channel is sent once through the broadcast channel instead. Given that Fig. 3a corresponds to the worst case situation, we expect η_D to be between 0 and 1. In addition, we find that for a distribution network D_1 that is more efficient than a distribution network D_2, we have $\eta_{D1} < \eta_{D2}$.

PROPOSALS FOR PASSIVE SECURITY

One well-known approach combining fingerprinting and content distribution is proposed by Parvianen and Parnes [1, 4], and depicted in Figure 3b. In this distribution network two distinctly watermarked copies of the same entertainment media are partitioned into L pieces each, and each piece is then encrypted with a unique secret key. All $2L$ pieces are then broadcast to the users. Each user is given a set of L unique corresponding keys that can decrypt exactly L of the pieces such that when put together, each user ends up with a uniquely fingerprinted copy of the overall entertainment media. It can be shown that the fingerprinted copies are collusion-resistant when the set of L unique keys for each user is chosen to represent a binary collusion-resistant fingerprinting code.[2] To analyze the efficiency of this distribution network, we can think of this scenario as being equivalent to sending exactly two copies of the entertainment media across the broadcast channel. The efficiency of this scheme is therefore given by Eq. 2,

$$\eta_W = \frac{2}{m_0}. \qquad (2)$$

The reader should note that we focus on a security and distribution model for which the processes of fingerprinting and distribution are separated into the disjoint stages at the entertainment distributor and distribution network, respectively. Another possible approach, called *watercasting*, is to merge these two stages by allowing intermediaries in the network, such as trusted routers, to perform fingerprinting [9]. We point out that this method is vulnerable to attacks on the intermediaries, and may also be too costly for real-time entertainment applications due to the overhead of the routers having to perform fingerprinting.

We next present a novel fingerprinting paradigm for multimedia that offers additional security features as well as improved distribution network efficiency.

NOVEL FINGERPRINTING AND DISTRIBUTION PARADIGM

To motivate the need for a new fingerprinting paradigm, we first note that the distribution network described in Fig. 3b is not suitable for multicasting. As mentioned earlier, we wish to exploit the characteristics of both broadcast and unicast channels, and hence the novel paradigm will effectively enable this. In addition we point out some shortcomings in the security of the fingerprinting via codebook and watermarking method.

First, since the codebook is designed independent from the digital entertainment media, it can be shown that these codes are not appropriately specialized for digital entertainment media. For example, the attacks and attack assumptions against which these codebooks are robust may not be the actual signal-processing-based collusion attacks that can be applied directly to the digital entertainment media. An assumption often used in designing collusion-resistant codes is called the *marking assumption* [4], and if this assumption is violated, the security offered by fingerprinting is breached.

Second, common collusion attacks on uniquely fingerprinted copies using the codebook and watermarking design do not result in perceptual changes [10]. Ideally, pirates should be punished with a resulting perceptually degraded entertainment media when they apply collusion attacks. We assert that these shortcomings are a result of separating the design of the fingerprints from the media itself [10].

Therefore, we believe that fingerprints should be designed by making them judiciously dependent on the media in question. Therefore, we introduce a new paradigm termed *joint source fingerprinting* (JSF), which refers to the fact that the fingerprint design and media design are jointly achieved.

We define the *semantic class* of digital entertainment media to be a "coarse" representation of that media, having little commercial value. The *feature class* of a digital entertainment media is defined such that combining the feature class with the semantic class results in the original media. The semantic and feature classes are said to collectively represent the *semantic-feature representation* of digital entertainment media.

Given the semantic-feature representation of some digital entertainment media, fingerprints can be created from the feature class. In essence, the feature class is an effective alphabet from which strings or codewords are constructed. This dependence of the fingerprint on the feature class, and hence the media, effectively merges the fingerprint design process to the content itself. In addition, it is necessary that the semantic class combined with any fingerprint is perceptually similar to the original media.

NEW SECURITY FEATURE

We say that a fingerprint is *collusion-resistant* under the JSF paradigm when the following is true:

If a coalition of pirates creates a new fingerprint such that this new fingerprint cannot be used to identify any of the pirates, the pirates must introduce perceptual degradation.
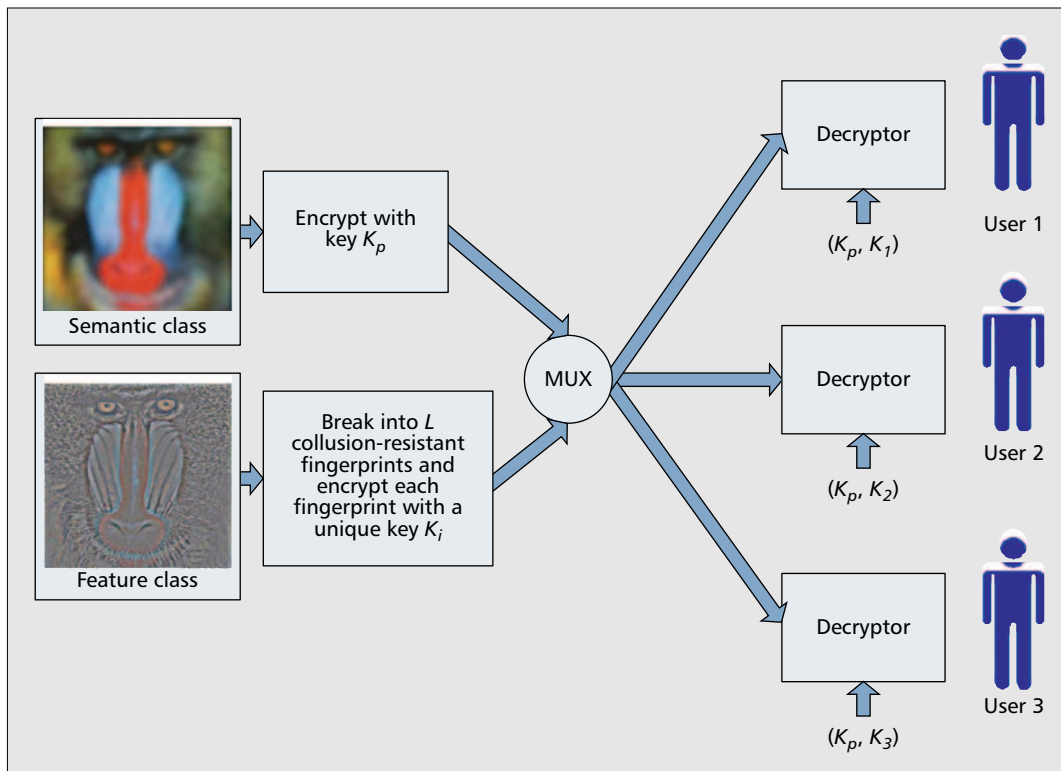
This requirement is fundamentally different from the traditional definition of collusion resistance, which requires that at least one pirate be identified [4]. In our paradigm, we trade off pirate identifiability with perceptual quality of the attacked media, such that if the pirates cannot be identified, they are at least left with a perceptually degraded colluded result that has no commercial value, and hence cannot be sold in underground entertainment networks.[3]

> We believe that fingerprints should be designed by making them judiciously dependent on the media in question. Therefore, we introduce a new paradigm termed *Joint Source Fingerprinting (JSF)*, which refers to the fact that the fingerprint design and media design are jointly achieved.

[2] *Since the L keys can be associated with watermarked media 0 or watermarked media 1, we can think of L keys as being a binary string of length L, and hence one can create 2^L binary strings of length L.*

[3] *The reader should note that one of the differences between digital watermarking and digital fingerprinting is that watermarking systems are designed with robustness to single-copy attacks in mind, whereas fingerprinting systems are also designed with robustness to multiple-copy attacks (i.e. collusion) in mind. Watermarking systems do have perceptual degradation as a counter to single-copy attacks; however fingerprinting systems have not been designed with this security feature against collusion, except for [10].*

■ **Figure 4.** *Joint source fingerprinting broadcasting, in which each user receives one uncompressed media; using two keys, users can decrypt and obtain the semantic class and their unique fingerprint.*

IMPROVED DISTRIBUTION NETWORK

Having described the novel JSF paradigm, we now show how the distribution network has improved efficiency. Figure 4 depicts the JSF method, as well as its distribution network. The main idea is that given the semantic class needs to be distributed to all users, we can simply broadcast this content class to all subscribers. On the other hand, the unique fingerprints based on the feature class are expected to be small in volume, and hence can be easily bundled and broadcast to all users. To facilitate this, each user shares a group key K_p that is used to decrypt the common semantic class data, and a unique secret key used to decrypt the unique fingerprints. If the JSF algorithm is collusion-resistant against a coalition of c pirates or less, where c is much smaller than the total number of users, and λ is the ratio of each fingerprint length to the size of the original media, it can be shown that Eq. 3 is the JSF distribution network efficiency:

$$\eta_{JSF} = \frac{1+(c-1)\lambda}{m_0}. \qquad (3)$$

Comparing Eq. 3 to Eq. 2, we see that our distribution network is more efficient than the method of Parvianen and Parnes if $(c - 1)\lambda < 1$.

We can also extend our distribution network to incorporate the unicast channel so that we have a multicast distribution network similar to [8]. In such a scenario, both broadcast and unicast channels are employed. For example, since the semantic class is common to all users, it can be broadcast through a public channel to all subscribers. In addition, the fingerprints that are unique to each user can be transmitted through individual private channels.

JSF VIDEO ALGORITHM

We illustrate the JSF paradigm by presenting a simple algorithm for video. Let the semantic class of a video sequence be a highly frame-decimated version of the original. The resulting frame-decimated video sequence will therefore have choppy motion, which implies that it is a coarse representation of the original video. We assume that the decimation rate is high enough to prevent interframe interpolation, so pirates cannot try to reconstruct the original video sequence from its semantic class; hence, the resulting semantic class has no commercial value. The decimated frames that are not part of the semantic class represent the feature class. In uncompressed video content, there is a great deal of frame redundancy due to motion the human visual system cannot perceive. Therefore, fingerprints can be constructed by partitioning the feature class such that each fingerprinted video will appear visually identical to the original video.

In our algorithm we compare the similarity of two frames by the *average motion* between two frames. Motion vectors from the video compression field are used to define average motion. Essentially every frame is partitioned into 8×8 or 16×16 blocks of contiguous nonoverlapping pixels. Given two consecutive frames, motion can be encoded by mapping blocks in the first frame to blocks in the second frame, such that the mapping results in pairs of blocks that are "close" to one another.[4] This mapping can also

[4] *The measure of "closeness" is usually the mean absolute deviation (MAD).*

■ Figure 5. *a) Original frame; b) random attacked frame from five colluders/attackers resulting in notable distortions around the eyes; c) original frame; d) random attacked frame from five colluders/attackers resulting in notable distortions on the plant, rock, and fence.*

be described by a vector that specifies the x and y pixel offsets of the block in the second frame to the block in the first frame. We then define *motion* between two blocks as the magnitude of this offset, and the average motion between two frames is then the average of the motion of all pairs of blocks between the two frames. Details of block mappings (commonly referred to as *block matching*) can be found in [11].

PERFORMANCE ANALYSIS

We demonstrate that the JSF distribution network is more efficient for certain pairs of c and λ. In our simulations, we used 8-s video clips consisting of 260 frames from the Video Quality Experts Group (VQEG). To ensure that the fingerprinted videos achieve the same video quality as the original video, we define a threshold such that the average motions (as defined in the previous section) between all frames in the fingerprinted videos are below this threshold. This threshold is dependent on the original video (derived empirically by trial and error for our experiments), and also dictates how many fingerprinted copies can be created.

We note that the proposed JSF distribution network is more efficient than the method by Parvianen and Parnes if the inequality $(c - 1)\lambda < 1$ is satisfied. We also observe that λ can be interpreted as the percentage of the fingerprint-

ed media that contains the fingerprint. Therefore, if we fix λ at 5 percent, for example, we can achieve collusion resistance against approximately 20 colluders/attackers, which is obtained by solving the inequality above. We assume that a pirate is constrained by cost, and therefore will be unlikely to obtain more than 20 copies of the same video. However, this assumption is not required because of JSF's new security feature, which results in perceptual degradation in the attacked media; this implies that sometimes we do not require collusion resistance for a large number of colluders/attackers. For example, Figs. 5b and 5d are the results of only five colluders/attackers applying random attacks; it is clear that with only five colluders/attackers, the perceptual quality is severely degraded.

Next, we compare the visual quality of the JSF video algorithm to traditional codebook and watermarking techniques on two types of collusion attacks: the average and random types. Figure 6 displays the peak signal-to-noise ratio (PSNR) of the attacked signals as a function of the number of colluders. This figure shows that when using the JSF video algorithm, visual degradation of the content is incurred when the two collusion attacks are applied, whereas for traditional codebook and watermarking techniques (based on DCT [6] and DWT [12]), the visual quality does not degrade. This means that the JSF paradigm is inherently more resistant to
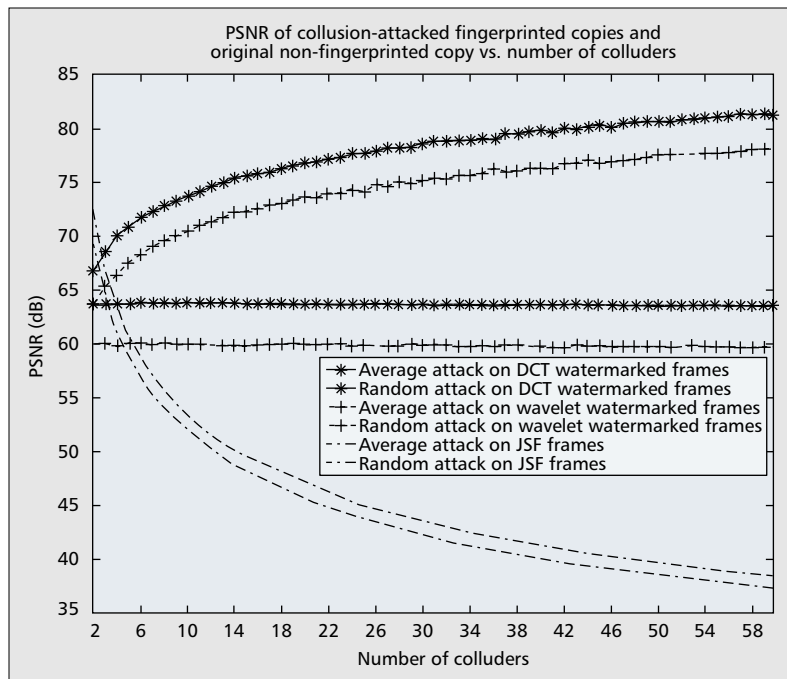
Figure 6. *PSNR of collusion attacked fingerprinted copies and original nonfingerprinted copies vs. number of colluders/attackers for the video of Fig. 5a–b.*

these two collusion attacks by degrading the commercial entertainment quality in comparison to the traditional approach. This is a new security feature only offered by the JSF paradigm.

CONCLUSIONS

This article introduces some challenges of establishing passive security in entertainment distribution networks. We present a metric for comparing the efficiency of such networks, and examine a novel paradigm called joint source fingerprinting. JSF offers a new form of security and exhibits greater distribution efficiency. To the best of the authors' knowledge, this is the first approach that offers perceptual degradation as a counter to collusion attacks. Our fingerprinting paradigm also merges the fingerprint design with the media, which is fundamentally different from the codebook and watermarking class of methods previously proposed.

REFERENCES

[1] R. Parviainen and P. Parnes, "Large Scale Distributed Watermarking of Multicast Media Through Encryption," IFIP TC6 and TC11, 2001, pp. 149–58.
[2] R. J. Anderson and M. Kuhn, "Tamper Resistance — A Cautionary Note," *Proc. USENIX Wksp. Electronic Commerce*, Rodos, Greece, Nov. 1996, pp. 1–11.
[3] R. Akalu and D. Kundur, "Technological Protection Measures in the Courts: Law, Engineering, and DRM Lessons Learned from the Failure of the Content Scrambling System," *IEEE Sig. Proc.*, Special Issue on Digital Rights: Management, Protection, Standardization, vol. 21, no. 2, Mar. 2004, pp. 109–17.
[4] D. Boneh and J. Shaw, "Collusion-Secure Fingerprinting for Digital Data," *IEEE Trans. Info. Theory*, vol. 44, Sept. 1998, pp. 1897–1905.
[5] W. Luh and D. Kundur, "Digital Media Fingerprinting: Techniques and Trends," *Handbook of Multimedia Security*, B. Furht and D. Kirovski, Eds. CRC Press, 2004.
[6] I. J. Cox *et al.*, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Trans. Image Proc.*, vol. 6, Dec. 1997, pp. 1673–87.
[7] J. C.-I. Chuang and M. A. Sirbu, "Pricing Multicast Communication: A Cost-based Approach," *Tellecommun. Sys.*, vol. 17, no. 3, 2001, pp. 281–97.
[8] H. Zhao and K. J. R. Liu, "Bandwidth Efficient Fingerprint Multicast for Video Streaming," *ICASSP 2004*, 2004.
[9] I. Brown, C. Perkins, and J. Crowcroft, "Watercasting: Distributed Watermarking of Multicast Media," *1st Int'l. Wksp. Networked Group Commun. '99*, L. Risa and S. Fdida, Eds., *LNCS*, vol. 1736, Springer-Verlag, 1999, p. 286.
[10] M. U. Celik, G. Sharma, and A. M. Tekalp, "Collusion-Resilient Fingerprinting Using Random Pre-Warping," *IEEE Sig. Proc. Lett.*, vol. 11, Oct. 2004, pp. 831–35.
[11] Y. Q. Shi and H. Sun, *Image and Video Compression for Multimedia Engineering — Fundamentals, Algorithms, and Standards*, CRC Press, 2003.
[12] C. Podilchuk and W. Zeng, "Image Adaptive Watermarking using Visual Models," *IEEE JSAC*, vol. 16, 1998, pp. 525–40.

BIOGRAPHIES

WILLIAM LUH (luh@ee.tamu.edu) received a B.A.Sc. degree in computer engineering in 2002 from the University of Toronto, Canada, and an M.S. degree in electrical engineering in 2004 from Texas A&M University. He is currently pursuing his Ph.D. degree in electrical engineering at Texas A&M University under Dr. Deepa Kundur. His research interests include multimedia and sensor network security, digital rights management, watermarking/fingerprinting, and steganography.

DEEPA KUNDUR (deepa@ee.tamu.edu) received her B.A.Sc., M.A.Sc., and Ph.D. degrees, all in electrical and computer engineering, in 1993, 1995, and 1999, respectively, from the University of Toronto, Canada. In January 2003 she joined the Electrical Engineering Department at Texas A&M University, College Station, where she is an assistant professor and a member of the Wireless Communications Laboratory. From September 1999 to December 2002 she was an assistant professor at the Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, where she held the Bell Canada Junior Chair in Multimedia. Her research interests include multimedia and network security for digital rights management, video cryptography, sensor network security, steganography, covert communications, and nonlinear and adaptive information processing algorithms. She has been on numerous technical program committees and has given tutorials at ICME 2003 and GLOBECOM 2003 in the area of digital rights management. She was a Guest Editor for *Proceedings of the IEEE* Special Issue on Enabling Security Technologies for Digital Rights Management.