Chapter XXVII
Digital Watermarking for Digital Rights Management

Farid Ahmed
The Catholic University of America, USA

Cecilia Gomes
The Catholic University of America, USA

ABSTRACT

With the remarkable growth of Internet and multimedia applications, production and distribution of digital media has become exceedingly easy and affordable. Applications such as distance education, e-commerce, telemedicine, digital library, and live audio/video broadcast activities require distribution and sharing of digital multimedia contents. Consequently, maintaining the quality of service of the applications and the rights of the content owner as well as enforcing a viable business model among the producer, consumer, and distributor of digital contents has become an increasingly challenging task, leading to a contentious area called digital rights management (DRM). This chapter presents how digital watermarking (DWM) technology can addresses part of this DRM problem of secure distribution of digital contents.

INTRODUCTION

The spectacular development in communication and network infrastructures coupled with exponential growth on digital contents and applications have placed enormous challenges on the storage, distribution, and use of these contents. The dissemination and sharing of information in this digital age consequently gives rise to a number of legal, ethical, and economic questions that need to be appropriately addressed by policy makers, consumers, developers, and technologists. We particularly address the technological aspect of the rights management of this digital distribution scenario in this chapter.

An analysis of the threat model, risks, and vulnerabilities associated with the storage and distribution of digital multimedia is first provided. Then we identify the requirements of enforcing the digital rights of different players, like the owner, distributor, and users involved in the transaction management of the digital contents. This leads to the design issues of different digital rights management (DRM) applications. Next, we specifically present a paradigm of technological solutions using the digital...
Digital Watermarking for Digital Rights Management

watermarking (DWM) technology. A fairly moderate technical know-how of the digital watermarking technology will be presented to show how it can address the DRM problems in terms of copyright protection, copy protection, owner identification, content authentication, and transaction tracking. The effectiveness of the technology will be analyzed by defining a set of metrics derived from the requirements of multimedia distribution. Finally the limitations of DWM and interoperability with other technological solutions will be presented.

THE PROBLEM: THREATS AND VULNERABILITIES OF DIGITAL MULTIMEDIA DISTRIBUTION

Digital multimedia data are easy to share and copy. Most importantly the sharing and copying can be done without any distortion done to the contents. If some distortions occur, data can be reconstructed by various algorithms well-studied in the areas of digital communications and signal processing. Interestingly, this property of digital data that facilitates the easy distribution is also responsible for its misuse.

Digital representation of text, audio, speech, image, video, graphics, and animation fall in the general umbrella of digital multimedia. The continuation of the chapter will primarily focus on the rights management of digital images. Figure 1 shows the typical distribution of digital images. Data acquisition is performed using imaging sensors such as camera, radiography, ultrasonogram, electron microscope, and so forth.

Depending upon the use of the image, it can be processed thereafter for enhancement or filtering out sensor noises. It may then be consumed for its intended use, or it may leave the digital world to enter into the analog/print world. The image may go through some wear and tear processes in the print media, and after that it may be scanned back to digital form and eventually reconstructed back to its original quality. While in the digital form the images may be copied, shared, or distributed through digital media, networks, or Internet. In this life-cycle of a digital image, different players such as the creator, owner, distributor, buyer, seller, consumer, and user have different models of ownership rights. The ease of distribution coupled with different attack models has made the rights enforcement of digital data vulnerable. The vulnerabilities are manifested through copyright thefts, identity thefts, data piracy, unauthorized access, and counterfeiting (Stallings, 2003). In a networked environment, the threats and vulnerabilities to data are even more evident. Essentially, all sorts of digital data are at risk.

The Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) have jointly been conducting an annual survey of cyber-crimes for the last couple of years (CSI/FBI, 2007). It is

Figure 1. Life cycle of digital images
interesting to see that one of the leading financial losses is done by digital proprietary theft. It is to be noted that U.S. Copyright Industry is more than $700 billion, which is more than 5% of US GDP. According to the Federal Trade Commission (FTC) more than an estimated 10 million Americans are victims of identity theft each year. Many leading companies, such as Citigroup, ChoicePoint, Bank of America, and Lexis Nexis have experienced different forms of data/identity theft over last couple of years (http://www.consumer.gov/idtheft/). Recording Industry Association of America (RIAA) reports Piracy problems in more than 60 countries (http://www.riaa.com/default.asp). Motion Picture Association of America (MPAA) estimates that the U.S. motion picture industry loses more than $3 billion annually in potential worldwide revenue due to piracy; for example, copies of prerelease versions of The Last Samurai were illegally distributed. Hollywood traced the pirated version and the distribution chain back to one of the screeners (http://msnbc.msn.com/id/4037016/).

THE SOLUTION: DIGITAL RIGHTS MANAGEMENT (DRM)

Requirement Analysis of DRM

Simply said, DRM is about “digital” information, it is about “rights,” and finally it is about “management.” Digital asset management is sometimes used interchangeably with digital rights management. So, what is digital asset? There are some born digital and most of the others are converted digital. Born digitals are produced in a digital incubator using digital hatching. We see examples of converted digitals when large archives of analog or print media are transferred to their digital counterparts. Another form of digital data is called induced digital. The recent research and deployment of sensor networks effectively result in huge induced digital data. Question is: Do these different types of digital data need to be treated differently? Do they imply different sorts of associated “rights”? Or do they require different types of “management”?

While some rights are intrinsic (governed by law of physics) most other rights are governed by laws and policies adopted by policymakers. Can policy law dictate the law of physics of bits? This has long been a debate in the digital world. The question, “Who owns the right?” is also very confusing because of the fuzzy nature of ownership. “Born,” “converted,” and “induced” entities may have different catalysts resulting in different sorts of ownership models.

The third word “management” is even more subtle. The term “management” in this context has mostly been used in a regulatory sense to imply limiting or controlling rights. But recent use of digital assets has pointed to many other implications of “management,” like “facilitation of use,” “enhancement of rights,” and “classification of use.”

Example Requirements of Content Owner/Provider

- Protection of intellectual property. The content owner has the right to exchange/disavow the ownership within the framework of an adopted business model. Technological solutions should be able to enforce this.
- Integrity and authenticity of dissemination of digital contents.
  - Is the multimedia authentic or has it been tampered with?
  - Can tampering be prevented?
  - Can the tampering be detected/localized?
  - Can the tampered part be recovered?
  - How well the traitor tracing can be done?
- Access control of digital contents: Only duly registered clients can access the data.
Example Requirements of End-User/Consumer

- Anonymity/privacy of communication
- Nonrepudiation in information exchange: The sender may not repudiate the sending, or the receiver may not deny the reception of the information.
- Access control: The buyer/consumer should have due access to the contents.

DRM TECHNOLOGIES

The primary technologies used for digital rights management are the following:

- Cryptography: Cryptographic techniques and protocols are by far the most widely used mechanisms to implement DRM systems. Both the network level and the data level solutions are provided by a host of protocols based on the public-key cryptography and the symmetric key cryptography. Pretty good privacy (PGP), secure socket layer (SSL)/TLS, IPsec, and Kerberos are just a few of the example protocols.
- Digital watermarking/steganographic solutions. The next details this technology.
- Hybrid solutions employing cryptography, watermark, and biometric technology.

DIGITAL WATERMARKING

Digital watermarking is the process of embedding a digital code (watermark) into a digital content such as image, audio, or video (Cox et al., 2001). The embedded information, sometimes called watermark, is dependent on the DRM requirements mentioned above. For example, if it is a copyright application, the embedded information could be the copyright notice. Figure 2 shows a block diagram of such a digital watermarking process.

To embed a message $m$ in an image $I_o$ (referred to as original image), the message is first encoded using source coding and optionally with the help of error correction and detection coding, represented in the figure as $e(m)$, where $W_m = e(m)$.

The encoded message $W_m$ is then combined with the key-based reference pattern $W_K$ in addition to the scaling factor $\alpha$, to result in $W_a$ which is the signal that is actually added to the original image.

$$W_a = \alpha (I_o)[W_m \otimes W_K]$$

$$I_w = I_o + W_a$$

The result of this process is the watermarked image $I_w$. When the scaling factor is dependent on the original image, informed embedding is possible which may result in more perceptually adaptive watermarking (Cox et al., 2001).

Figure 3 shows the original image, watermarked image, and the difference image using a correlation-based watermarking algorithm (Ahmed & Moskowitz, 2004). As evident from Figure 3(b), the hidden message is imperceptible as well as the change in the original image. This is one of the primary criteria of digital watermarking.

In addition to imperceptibility, DWM must make a trade off among a number of different criteria. It can thus be considered as a multidimensional problem optimizing among the criteria of imperceptibility, unobtrusiveness, capacity, robustness, security, and detectability. The message being hidden should be imperceptible as well as the changes made in the original image. This also implies that the inserted watermark should not be obtrusive to the intended use of the original image. For example, while watermarking a medical image for patient privacy or security, it should not degrade the diagnostic quality of the image. Since the watermarking process does not increase the size of the original image, it may be desirable to add as much information as possible. Generally the increase in information will severely impact on the perceptual quality of the image. From the detection point of view, a watermark should be...
robust enough to tolerate a range of image postprocessing and degradation. In addition, the embedded watermark must be secure to prevent its removal. Finally, delectability of the embedded watermark is an important criterion that places some constraints on the embedding algorithm.

**DWM FOR DRM: FINDING THE NATURAL MATCH**

With this brief introduction to watermarking technology, let us turn our attention to its applicability towards DRM. In this regard, following is a list of DRM applications that the watermarking technology can help in managing (Hartun, 2000; Wu, 2002).

A. Security Enhancement
   a. Copyright Protection
   b. Copy Control
   c. Access Control

B. Enabling Technologies
   a. Bridging the Print and Digital World
   b. Device Control
   c. Intelligent Multimedia

**Figure 3. (a) Original image $I_o$ (b) watermarked image $I_w$ and (c) the difference image, $W_a$ (enhanced for visual discernment)**
Digital Watermarking for Digital Rights Management

C. Identification
   a. Annotation
   b. Data Mining
   c. Digital Preservation

D. Forensic Analysis
   a. Transaction Tracking/Fingerprinting
   b. Tamper Detection

Digital watermarking has demonstrated significant potential in implementing copyright protection and access control (Arnold, 2003). Copy control technology allows the media owner to monitor and control copies made, that is, DVD “copy once,” “copy twice,” and “no copy” mechanism. Digital watermarking can enforce this dynamic control of digital media usage.

The second category of techniques pertains to enabling digital medium. Digital libraries and archives are increasingly being populated by “converted” digital from their analog counterpart. One of the amazing features of digital watermarking is authentication or integrity verification across this boundary of print and digital medium. Digimarc Corporation (Digimarc Corp.) has deployed a product called MediaBridge, which effectively bridges the print and digital world. A similar application, intelligent multimedia, embeds “intelligence” information into a digital multimedia content, which can then be used for many device control applications. A third category is identification, which is becoming increasingly challenging due to the exponential growth of digital data on networks and Internet. Identification and recognition of patterns are key operations required in data mining applications in digital archives and libraries. Digital watermarking technology can hide imperceptible digital identification inside a digital content that can be used for searching through a database and data mining applications (Wu, 2002). This identification tag may be generated from the features or signatures of the media concerned. This can facilitate indexing in the digital preservation application. A variant of this application, named Marc Spider from Digimarc Corporation, searches like a Web crawler to find registered copies of digital media content.

The fourth category relates to digital forensic analysis (Naumovich, 2003; Chai, 2001). In the continuous (re)distribution of digital content through the Internet and other digital media (e.g., CD, camera, etc.), it is important to track the distribution points to detect possible illegal distribution of contents. Tracking the usage of digital media is important to implement any legal and economic model of digital rights management as well as to track down forged and unlawful usage of digital data. A related application is tamper detection or integrity verification. This is particularly relevant in digital archival applications where data will sometimes need to be transferred from one storage medium to another and replicated in a number of places. Integrity of the digital content and authentication of the source and destination of the distribution chain is therefore of utmost importance. Tamper detection applications embed some hash of the original content into the digital media using watermarking technology. The detector then extracts this embedded hash and compares with the computed hash. If there is a discrepancy then, it is said to have been tampered with.

DWM FOR DRM: DESIGN AND IMPLEMENTATION ISSUES

While different DRM problems can be addressed by using different classes of watermarking technique, the primary design issue revolves around making an optimization in each case of the perceptuality, capacity, detectability, robustness, and security of the systems. Some of the key design questions then are:

a. What type of DWM is used for a specific DRM problem?
b. Which specific DRM requirements are met by a class of DWM?
c. What type of error does the watermarking process introduce in embedding the informa-
tion? What is the impact on the quality of the media due to the embedding error? How to enhance quality by minimizing the embedding error?

d. How to increase robustness of the system, which is useful for applications like copyright protection?

e. How much information can be embedded in a digital media? How to increase the embedding capacity?

f. How to increase detectability?

g. Is there a way to prevent and/or identify any sort of tampering done to the digital multimedia?

Based on these questions, we hereby elaborate on the following four DWM-based DRM design issues:

- Determination of a specific watermarking technique
- Minimization of embedding error for better perceptual quality
- Robustness, capacity, and detectability tradeoffs
- Authentication/tamper detection issues
- Integration with encryption and compression

### Determination of Specific Watermarking Technique

In order to fully appreciate the use of watermarking for secure digital rights management, it is instructive to look at different classes of watermark (Cox et al., 2001; Petitcolas, 2000; Hartung, 1999), which is (delineated) depicted in Figure 4.

Figure 4 shows watermark classifications based on different criteria. For example, depending on the robustness criteria of watermarking, they can be classified into three categories: robust, fragile, and semifragile. While the robustness of a watermark is important, it is not always equally desirable in all applications. Let us take the authentication as an example. If an owner of a digital content embeds some authentication information into the content using watermarking. The owner might want to see the authentication fail, if the image is stolen. This a type of nonrobust watermark where the fragility of the embedded watermark is required to detect any forging done on the original digital content.

The cover document is the unwatermarked digital media in which it embeds or hides the watermark; for example, of such digital media are hardware/software, video, image, text, and audio. Based on the use of key in detection, watermarking can be public or private. In public watermarking applications, the watermark can be detected by everyone and they would not have access to the original work. In private applications, the watermark can be detected only by a selected group of people who have access to the original unwatermarked work. If the fact that “some information is hidden” in a media is kept secret, the application is steganographic, otherwise it is nonsteganographic.

The watermark detector might either have access to the original media or not have it. In the blind detector, the original media is not needed for the extraction or detection of the watermark. For the nonblind detector, the original content is needed for extraction, also called informed detector.

Invertible or reversible watermark is a distortion free data embedding scheme, used for applications which cannot tolerate the slightest amount of degradation done to the host images. For example, medical images require invertible or semiinvertible watermark. In the noninvertible case, the watermark cannot be extracted without possible alteration of the original.

The actual signal which is embedded during watermarking could be another image like a logo, or it could be a spread spectrum noise signal of a bit sequence.

A watermark signal can be embedded either directly in the spatial domain or in the transform domain. Spatial domain is useful for embedding a fragile watermark where the selected pixel values are modified by the watermark bits thereby chang-
Digital Watermarking for Digital Rights Management

Figure 4. Watermark classifications

- Robust
- Fragile
- Semi-fragile
- Robustness
- Recognition
- Readable
- Detectable
- Visible
- Invisible
- Spatial Domain
- Transform domain
- Noise
- Image Format
- Transform domain
- Message
- Invertibility
- Invertible
- Non-Invertible
- Extractable
- Non-Extractable
- Video
- Video
- Image
- Text
- Audio
- Public
- Private
- Non-Steganographic
- Steganographic
- Blind
- Non-Blind
- Hardware Software
- Video
- Image
- Text
- Audio
- Visible
- Invisble
- Recognition
- Detection
- Existence of Message
- Watermarking

ing some of the color information of the original image. Although the embedding method is relatively easy, there is trade off in the way the embedding locations are selected. If a less significant location is selected, the watermark would be invisible but not robust because they are removed by compression. To make it robust it has to embed in the more significant locations, but that would degrade the visible quality of the image.

Transform domain, a frequency domain watermarking method, is usually more robust to attacks and compression. Discrete cosine transform (DCT), discrete fourier transform (DFT), and wavelet domain transform (DWT) are some of the domains.

The types of watermarking we are interested in are invisible watermarking, since they are imperceptible and are not intrusive to the host image. However, visible watermark that can be seen with bare eyes may also be used, which is outside the scope of this chapter.

Finally, based on the recognition of a watermark signal, in some applications such as copyright, the embedded information needs to be readable. However in an authentication application, it may only suffice to know whether some information is hidden or not.

With this understanding, as an example, let us look at a rapidly emerging application, which is the digital rights management of wireless multimedia networking (Hartung, 2000). This typically includes video streaming, teleconferencing, voice over IP, and so forth. The following considerations should be made for watermarking digital contents for these applications.

- A progressive watermark is required so that receiver can make a progressive decision about the authenticity of a received streaming multimedia, just from a handful of packets, instead of waiting for the whole stream of
Digital Watermarking for Digital Rights Management

packets. This requires a watermark whose energy is distributed throughout the content and across the entire spectrum.

- A transform domain watermark, like a DWT domain watermark (Meerwald, 2001) may be better suited due to its better robustness against compression, which multimedia data inevitably go through while in transmission.
- Robustness of the watermark against random packet loss is desirable. Alternatively, a forward error correction mechanism may be necessary to reconstruct the watermark from packet loss.
- A fast watermarking algorithm is required for real-time communication.
- For authentication application, a semifragile or semirobust watermark is a necessity, so that its authentication decision can be made on degradation levels.

As for a second example, we turn to the electronic health record (EHR) to be used in telemedicine applications. Figure 5 shows how a specific patient clinical image, like the X-ray, can be accessed by different players with different access privileges.

This also shows that multiple different watermarks are required to enforce all the rights management of all the players, as shown in Figure 6. For example, the patient ID or demographic information can be embedded for the purpose of identification. Since the information is always attached to the image, it will result in less error in processing the data. To find out whether there has been any tampering done on a medical image, we may use an authentication watermark based on image signatures. A physician’s notes on a specific image, which may be revisited later, can be embedded. Generally speaking any form of watermark used in this case should be invertible, not to degrade the diagnostic quality of the image.

Minimizing Embedding Error for Better Perceptual Quality

The additional information that a watermarking system embeds in a host image essentially leads to a distortion of the host image, as evident from Equation (2). At the same time, because of the finite depth of image pixel values there may be rounding error, clamping error, and clipping error (Cox et al.,

Figure 5. User community accessing patient data

![Figure 5. User community accessing patient data](image-url)
Digital Watermarking for Digital Rights Management

2001). Rounding error occurs because the pixel values are represented by 8-bit integer numbers, while the watermarked signal $I_w$ could be real-valued. Any value of $I_w$ greater than 255, is truncated to 255, resulting in a clamping error, while any value of $I_w$ smaller than 0, is truncated to 0, resulting in clipping error. As a result of these three types of errors, the embedding efficiency may not be completely accurate and consequently the embedded signal, $W_a$, may not be reconstructed perfectly by the detector. Therefore one of the design aspects of the watermarking is to reduce this error. A number of ways to achieve this are as follows:

a. Reversible watermarking (Fridrich, 2002) to ensure that the distortions done during embedding can be retrieved
b. Avoiding clipping and clamping error by selective embedding
c. Encrypting the embedded signal

The following example depicts an authentication watermark for the analysis of embedding error and ways to mitigate this.

Figure 7 shows the use of a watermark for image authentication, which has some similarities with the cryptographic authentication using digital signature (Stallings, 2003). Unlike cryptography though, watermarking gives both in-storage and in-transit authentication. Watermarking is also faster compared to encryption, which is very important in Internet-based image distribution. By comparing a watermark against a known reference, it might be possible to infer not just that an alteration occurred, but what, when, and where changes happened. As shown in Figure 7, first some features are identified from the digital content, next the digital signature is computed, which is then embedded into the content. The detector takes a test data, computes the signature and extracts the embedded signature, and then compares the two. If they match, the image is authenticated. If they do not then the image may have gone through some forging/tampering effects and the algorithm may optionally detect the tamper area as well.

As an example of an authentication watermark, let us look at the Fourier transform-based method reported in (Ahmed & Moskowitz, 2004). The original image is transformed from the spatial domain to the frequency domain via the DFT. Consider an MxN host image $h(m,n)$, where $(m,n)$ are the spatial indices (pixel locations). The DFT of $h(m,n)$ is written as $H(u,v)$ where $(u,v)$ represent the frequency coordinates.

Figure 6. Different types of watermark needed in telemedicine applications
Digital Watermarking for Digital Rights Management

Figure 7. Image authentication using watermark

\[ H(u, v) = \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} h(m, n) \exp(-j2\pi(\frac{um}{M} + \frac{vn}{N})) \]  

(3)

Switching to polar coordinates, the Fourier transform of the image can equivalently be expressed as:

\[ H(u, v) = X(u, v) \exp(j\phi(u, v)) \]  

(4)

where, \( X(u,v) \) is the magnitude \( |H(u,v)| \) of the frequency component, and \( \phi(u,v) \) is the phase part of the \((u,v)\) frequency given by:

\[ \phi(u,v) = \arg\left(\frac{\text{Re}(H(u,v))}{\text{Im}(H(u,v))}\right) \]  

(5)

We then compute a signature, which is (nothing but) simply the binary phase-only filter of the image and given by:

\[ S(u, v) = +1, \text{if } \cos(\phi(u, v)) \geq 0 \]

\[ = 0, \text{ otherwise} \]  

(6)

In the embedding process, the phase is kept unchanged and the magnitude \( X(u,v) \) is modulated. The real-valued \( X(u,v) \) is first transformed to integer-valued as follows.

\[ R(u,v) = \text{round}[X(u,v)] \]  

(7)

where the \( \text{round}() \) function rounds the operand to the nearest integer value. That makes it able to be represented by a fixed number of \( q \) bit planes. Hence we have \( R=R_{q-1}, R_{q-2}, \ldots, R_1, R_0 \) where \( R_i \) is the \( i \)-th bit-plane of the rounded magnitude.

After the bit-plane embedding, where the \( i \)-th bit-plane is substituted by the signature, the Fourier spectrum becomes

\[ \tilde{H}(u,v) = \tilde{R}(u,v) \exp(j\phi(u,v)) \]  

(8)

To the above we apply the inverse DFT. The watermarked image (in the spatial domain) is then given by:

\[ \tilde{h}(m,n) = \frac{1}{MN} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} \tilde{H}(u,v) \exp(j2\pi(\frac{um}{M} + \frac{vn}{N})) \]  

(9)
This will result in a real-valued image which is converted to an actual grayscale bitmap in the spatial domain, by the clamping and clipping operator `uint8` (converts to 8-bit unsigned integer to represent 0 to 255).

\[
\tilde{h}_w(m, n) = uint8(\tilde{h}(m, n))
\]

(10)

Now let us look at how much error is introduced because of the watermarking process itself. Keep in mind that the values of \( \tilde{h}(m, n) \) have not been clipped, clamped, or rounded into integers between 0 and 255.

\[
e(m, n) = \tilde{h}(m, n) - h(m, n)
\]

\[
= \frac{1}{MN} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \left( \hat{H}(u, v) - H(u, v) \right) \exp(j2\pi \frac{um}{M} + j\frac{vn}{N})
\]

\[
= \frac{1}{MN} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \left( \hat{R}(u, v) - R(u, v) \right) \exp(j\pi \frac{um}{M} + j\frac{vn}{N})
\]

\[
= 2^{-i} \frac{1}{MN} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \left( \hat{R}(u, v) - R(u, v) \right) \exp(j2\pi \frac{um}{M} + j\frac{vn}{N})
\]

(11)

The total difference between is given by:

\[
\sum_{m=0}^{M-1} \sum_{n=0}^{N-1} e(m, n) = 2^{-i} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \left( \hat{R}(u, v) - R(u, v) \right) \exp(j\pi \frac{um}{M} + j\frac{vn}{N})
\]

which is shown [20] to be equal to

\[
\sum_{m=0}^{M-1} \sum_{n=0}^{N-1} e(m, n) = 2^{-i} \left( \hat{R}(0, 0) - R(0, 0) \right)
\]

(12)

This is a very obvious result. In order to minimize the error, \( i \) should be small which indicates a low significant bit-plane is needed to be selected in the Fourier magnitude domain. But this error minimization comes at a cost (Farid, 2007), which is shown in Figure 8. In the following chart watermark strength is given by the value of \( i \). The detectability decreases with the decrease in the strength of the watermark, but sure quality increases.

For a good trade-off between the detectability and perceptuality in this bit-plane embedding method, redistributing the embedded information in different bit planes is found to improve the quality of the image for a given bit error rate (Ahmed & Moskowitz, 2006).

In the pursuit of further improvement on minimizing the embedding error, one can have a disjoint space for embedding and signature. If the signature space and the embedding space are not disjointed, it has the undesirable effect of changing the signature domain, so that even in absence of any kind of degradation, the computed signature and the extracted signature will not be the same. In Farid (2007) that problem is partly eliminated by using wavelet decomposition for utilizing different subbands for the signature and embedding space.

Increasing the Robustness and Security of Watermarking Algorithm

Robustness is a desirable feature of a watermarking system which describes how well the embedded information can survive different sort of distortions such as compression, signal processing, and so forth. On the other hand, security is a measure of the resilience of a watermarking system against some attacks, such as tampering, forging, and so forth. There are some measures that can be taken to improve both the robustness and security of a system. Of course robustness alone does not mean much unless it is associated with something to describe against what the system has to be robust against. For example, in a video streaming of copyrighted materials the embedded copyright watermark should be robust against compression.

Figure 9 shows the authentication value and the bit error rate as a function of compression of the watermark detector of the authentication system described in the previous section. This shows that with higher strength both the compression tolerance and the authentication value improve.

Each of the different algorithms will have its built-in robustness against a specific processing.
The following are a few general approaches that can be taken to enhance the robustness and security of a system. They include (Cox et al., 2001)

- Redundant embedding
- Spread spectrum coding of messages
- Embedding in a perceptually significant coefficients
- Embedding in coefficients of known robustness
- Inverting distortions in the detector
- Using error correction coding
  - repetition code
  - block code
  - convolution code

**Integration with Encryption and Compression**

One of the practical concerns in DRM applications is the interoperability of watermarking with already existing protocols of encryption and compression (Mehrav, 2006; Lian et al. 2007; Dittman et al., 2001), which are prevalent in multimedia communication. One design issue is the relative order of encryption, watermarking, and compression. There are a number of schemes where watermarking is performed in compressed domain using the modulation of bits in the JPEG bit streams. The robustness of these algorithms is not very good. On the other hand, if compression is to be done after the image is watermarked, the watermarking algorithm must be robust against compression. Generally, watermarking performed in a frequency domain have better leverage in this regard. Liang, Liu, Ren, and Wang (2007) propose a commutative watermark with encryption where the order of operations can commutate. Watermarking the encrypted information has some advantages and disadvantages. On one hand, it can hide any sort of existence of hidden data; on the other hand, the capacity of the watermark may be limited due to the noisy nature of encrypted image. The success of this of course depends on an emerging area of “signal processing in the encrypted domain.” An example of the interoperability of these three technologies is discussed by Mehrav (2006), where the author studies the problem of joint coding for three objectives: information embedding, compression, and encryption.

**PERFORMANCE ANALYSIS OF DWM ALGORITHMS**

Without a proper validation suite, the performance of the watermark-based DRM systems cannot be
trusted. There are a number of metrics used by researchers to evaluate the perceptual quality, detectability, robustness, and the capacity of a watermarking system. A widely used objective metric to discern the perceptual quality in image processing is the Peak-signal-to-noise-ratio, defined as follows:

\[
PSNR = 10 \log_{10} \left( \frac{255^2}{\frac{1}{MN} \sum_{m=1}^{M} \sum_{n=1}^{N} (h(m,n) - \hat{h}_n(m,n))^2} \right)
\]

Robustness of the embedded message is often represented by the ratio of the number of bits correctly detected by the total number of bits embedded, which is called bit error rate (BER). Most of the watermarking detectors use a correlation-based detection strategy. The performance of correlation is often given by a normalized correlation coefficient.

The performance of a watermarking algorithm against a possible attack is even more important for digital rights management under different types of attacks and vulnerabilities.

Taxonomy of attacks can be summarized as follows:

- **Removal Attacks** – removes the mark
  - Denoising
  - Quantization/compression attack
  - Remodulation/rewatermarking
  - Collusion attacks
  - Signal processing attack
- **Filtering, cropping, print/scan**
- **Geometric attack** - distorts the mark
  - Rotation, scale, translation, shear
- **Cryptographic attacks**
  - Brute force search for embedded information
  - Oracle attack (possible if detector is available)
- **Protocol attacks**
  - Invertibility of watermark
  - Copy attack
  - Forgery

Based on these different types of attacks and the different evaluation metrics, a number of evaluation suites have been developed, including the Stirmark, CheckMark, Optimark (Macq et al., 2004; CERTIMARK; StirMark). Finally, in order to facilitate the Web-based evaluation of DRM management capability an open watermarking open source community has also been developed (OpenWatermark).
CONCLUSION

We reported a design and analysis approach of digital watermarking technique for the enforcement of digital rights management. The design issues should always be factored in carefully for a successful DWM-based DRM application. In addition, just like cryptographic measures are subject to different types of attacks and vulnerabilities, digital watermarking is also subject to a number of attacks. In an ill-designed watermark, attackers can tamper with the mark, forge, and even remove the watermark. Cryptographic attacks on key-based watermarking systems are also possible. Another major limitation is that the watermarking process cannot be made sufficiently robust to arbitrary types of different attacks. Some watermarking algorithms are more resistant to these attacks than others. It is possible to make it more robust in the cat-and-mouse game between the attackers and designers of the watermark.

The quality degradation of media after the watermarking may be a reason of concern. With technology one can always make a tradeoff among different parameters like quality, security, and robustness. Another limitation is that the watermarking technology is not yet widely deployed, and nor is the protocol satisfactorily standardized. Therefore, the hybrid combination of cryptography and watermarking is expected to improve the secure distribution of digital content across the unreliable Internet.

REFERENCES


**KEY TERMS**

**Authentication**: The process of verifying the digital identity of the sender and receiver of a communication. Usually a cryptographic hash is used for this purpose. Content authentication is used for verification of the content.

**Cryptography**: The technique of concealing the intended meaning of information. And it does so by encrypting a plain text into an unintelligible format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text.

**Data Compression**: The technique of representing the data in a format that requires fewer storage locations. Typically, lossy compression employs quantization and some sort of entropy coding, whereas lossless compression does not need quantization.

**Digital Rights Management (DRM)**: An umbrella term that refers to access control or management technologies used by publishers and other copyright holders to limit or facilitate the usage of digital content or devices.

**Digital Watermark**: The process of embedding a digital code into a digital content like image, audio, or video. As an example, the digital code representing the creator/owner of a digital image can be embedded into the image for copyright protection. The embedded information, sometimes called watermark, is dependent on the intended application.

**Fingerprinting**: Fingerprinting is used for distribution and piracy detection of various types of digital content. It embeds in the delivered data some unique information related to the transaction, so that if any copy of this data is found later on the Internet, the leak can be traced back to the person who obtained it first.

**Multimedia**: Deals with multiple forms of information content and processing for example,
Digital Watermarking for Digital Rights Management

text, audio, graphics, animation, image, and video. It can also extend to analog domain such as print media.

**Reversible Watermarking:** Reversible watermarking, or invertible watermark, is a distortion-free data embedding scheme, where the embedded information can be totally extracted without any distortion done to the host media. This is used for applications which cannot tolerate any degradation done to the host data, such as medical image protection.