INTELLECTUAL PROPERTY PROTECTION FOR ELECTRONIC COMMERCE APPLICATIONS

S.H. Kwok
Department of Information and Systems Management
The Hong Kong University of Science and Technology
jkwok@ust.hk

C.C. Yang
Department of Systems Engineering and Engineering Management
The Chinese University of Hong Kong
yang@se.cuhk.edu.hk

K.Y. Tam
Department of Information and Systems Management
The Hong Kong University of Science and Technology
kytam@ust.hk

ABSTRACT

Online content distribution businesses require methods to protect the intellectual property of distributed content. Intellectual property protection is a mechanism to protect the rights of ownership of original work so that no one can use the rights-protected work in any way without seeking permission for the use and, if necessary, paying the rights owners a royalty for the use. Digital watermarking is the core technology in electronic rights protection. However, research addressing the concerns of businesses about intellectual property protection schemes through watermarking is scarce. In this paper, we address these concerns by first introducing watermark design patterns (WDPs) for electronic commerce applications, then presenting problems of copyright protection using watermarking, and finally presenting management concerns. A WDP is defined as the requirements of a digital watermark for a particular type of distributed media content under the protection of its intellectual property. This paper introduces four WDPs for four types of media data - video, image, audio, and text and they are denoted as WDP_{video}, WDP_{image}, WDP_{audio} and WDP_{text} respectively. The four WDPs are derived from the characteristics of watermarking techniques and the properties of a distributor's web site. In our study, the proposed WDPs are used to relate the digital watermarking techniques to electronic commerce applications, and their relationships are presented graphically. The relationship diagram can facilitate electronic commerce application developers to select appropriate digital watermarking techniques and off-the-shelf systems for intellectual property protection on their web sites.

Keywords: Intellectual property protection, copyright protection, digital watermarking, electronic commerce application, watermark design pattern.

1. Introduction

With advancements in Internet technologies and increasing demands on online multimedia businesses, digital copyright has become a major concern for businesses that engage in online content distribution through various business models, such as pay-per-view, subscription, trading, and so on. This is because a perfect copy of the distributed content can be reproduced at close-to-zero cost. Losses due to copyright infringement have increased dramatically. Intellectual property protection is a pressing concern for content owners who are exhibiting digital representations of photographs, rare books and manuscripts, and original artworks on the World Wide Web (WWW) [Dittmann, et al. 2002, Huang, et al. 2002, Kwok and Yang 2002]. Electronic commerce web sites or applications include electronic publishing and advertisement, real-time information delivery, product ordering, transaction processing, photograph galleries, digital libraries, web newspapers and magazines, network video and audio, personal communication and so on. In electronic commerce web sites or applications, digital contents can be categorized into four basic types of media data, and they are image, audio, video and text. Multimedia data will not be included in this paper, as this is considered to be a combination of these basic data types.

Watermarking [Dittmann, et al. 2002, Trowbridge 1995] is viewed as an enabling technology to protect these media data from re-use without giving adequate credit to the source or in an unauthorized way. In general, a watermarking [Memon and Wong 1998] enables ownership assertion, fingerprinting, authentication and integrity verification, content labeling, usage control and content protection. Hawkins [Hawkins 1998] addressed that many watermarking techniques have been proposed for intellectual property and copyright protection in the literature, but different media data apply different digital watermarking techniques. Moreover, technical requirements of different watermarking techniques also vary because of different functions and applications [Memon and Wong 1998].

Since intellectual property protection using digital watermarking is still at its infancy, this paper attempts to promote digital watermarking and introduces a mechanism for electronic business designers and developers to use watermarking in protecting their online media contents. In response to this need, this paper first introduces four watermark design patterns (WDPs) to describe the requirements of digital watermarks for various media contents. The proposal of these WDP is based on the characteristics of watermarking techniques addressed in the literature, and the properties of a distributor's web sites. The WDPs are then extended to relate the watermarking techniques to various electronic commerce applications. The graphical representation of the relation diagram could guide the developers to select appropriate watermarking for the protection of their distributed contents. Problems of copyright protection using watermarking and management issues are also presented.

The rest of the paper is organized as follows: Section 2 presents an overview of related literature. Section 3 presents the preliminary concepts of watermarking technique. Section 4 discusses the properties and copyright protection issues in electronic commerce applications and introduces common copyright protection schemes used in existing electronic commerce applications. Section 5 introduces a WDP to describe the characteristics of a digital watermark for a particular media data. After studying some representative distributors' web sites, WDPs for four different media data are derived. In Section 6, we apply our results of WDP to form the relationship between digital watermarking techniques and electronic commerce applications. Section 7 presents problems of copyright protection using watermarking. Section 8 presents management issues. Finally, Section 9 summarizes the contributions of our study and highlights the future research directions in this area.

2. Related Work

In this section, we briefly describe some related ideas and research areas published in the literature.

2.1 Copyright

The Recording Industry Association of America states "to all artists, 'copyright' is more than a term of intellectual property law that prohibits the unauthorized duplication, performance or distribution of a creative work. To them, 'copyright' means the chance to hone their craft, experiment, create, and thrive". Copyright law began with the "The Statute of Anne," the world's first copyright law passed by the British Parliament in 1709. Some of these basic copyright principles are likely to continue to endure: maintaining the intended purpose of copyright to fairly balance the rights of the public for access to information with the incentives for creation; providing authors with exclusive rights but limiting what copyright protects and the time period of copyright protection; and giving users certain rights, such as fair use, that restrict the owner's monopoly [Harper 2001]. Since 1709, copyright laws have been established in many countries. To address legal issues recently created by the development of the Internet and other new digital delivery services, the international legal framework for updating copyright laws for the digital era was laid down in two World Intellectual Property Organization (WIPO) Treaties [WIPO 2003] concluded in Geneva in December 1996. They were the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT). Signed by more than 100 countries, the treaties require ratification by 30 signatories in order to be enforced worldwide. At the start of 2000, 13 counties (states) had ratified the treaties and several other countries were working on implementing legislation. For example, Australia's Copyright Amendment (Digital Agenda) Act of 2000 amended its Copyright Act of 1968 to strengthen the rights of music copyright owners when music is used in "new" media - from Music-on-hold to Internet delivery services. The changes include an introduction of new enforcement measures over a wide range of services from digital encryption of music through watermarking to the pirating of pay television signals. In the United States, the congress passed the Digital Millennium Copyright Act (DMCA) in 1999, which addresses copyright issues for digital content. Digital content refers to digital music, video, images, documents and so on. This act makes it illegal to attempt to circumvent any technological measure, including digital watermarking, that effectively protects an owner's intellectual property rights of digital content. This move should act as a catalyst to advance the current state-of-the-art technology as well as to help define new applications for watermarking.

2.2 Copyright Protection

The entertainment industry has been testing a wide range of technologies that allow the multimedia industry to retain copyright controls provided by laws and to harness the power of the Internet to increase the size of the

industry and to enhance the experience of consumers. Foremost among these technologies are cryptographic-based and watermark-based copyright protection schemes. In cryptographic-based copyright protection, digital contents are always distributed in their encrypted forms. Given proper permission from the content provider or owner, clients are allowed to access the encrypted contents. However, when a piece of encrypted digital content is decrypted, it becomes ordinary digital content that is no longer protected and carries no copyright information. As a result, when the decrypted digital content is distributed to unauthorized consumers illegally, it is almost impossible for the cryptographic-based copyright management system to trace the person who has distributed the illegal copy of the digital content or to discover from where it actually came. To address this problem, many systems achieve copyright protection by attaching a code or a tag represented in a digital watermark that uniquely identifies both the creator and the consumer of the digital content. A digital watermark is digital data that can be embedded in digital contents and it allows one to establish ownership, identify a buyer, or add additional information about the digital content.

Sometimes cryptography and watermarking are utilized together, for example [Chen and Lee 2003], [Piva, et al. 2002] and [Anderson and Lotspiech 1995]. Chen and Lee [Chen and Lee 2003] presented a variance-based copyright protection method that takes advantages of both cryptographic tools and digital watermarking. It is lossless and robust to many malicious manipulations. Piva et al. [Piva, et al. 2002] proposed an open network electronic copyright management system (ECMS) that combines watermarking with cryptography to achieve reliable copyright protection while satisfying two contrasting requirements: actors in ECMS transactions must be able to verify that the watermark granting their rights is truly embedded in the multimedia document; and actors (other than the author) must not be able to remove the watermark. Anderson and Lotspiech [Anderson and Lotspiech 1995] proposed a rights enforcement system for an electronic library system that would control access and provide copyright protection. Access control is achieved through user authentication and session encryption, while copyright protection is enforced by visible and invisible watermarks. For instance, a user must provide a valid Lotus Notes password prior to accessing copyright-protected library materials. A bar code that acts as a visible watermark is attached to the front page of each digital article in the electronic library. A digital article is regarded as illegally printed if it contains no bar code on its front page. In addition, invisible watermarks are inserted into other spots in the digital document. Tracing these invisible watermarks can reveal any illegal act performed on the content.

2.3 Digital Watermarks and Watermarking

Copyright information usually refers to copyright or licensing information, such as the identity of the copyright holder, the creator of the material, or a link (URL) through which more related information is available. It may also contain a serial number that uniquely identifies material with particular registration entities. The copyright information together with product information, a customer profile, and company information can be represented by a key when digital watermarking is in use. The key is then converted into a digital watermark using a hashing function or a random generator for data embedding. Technically, a digital watermark consists of a sequence of numbers, also known as the watermark sequence. The watermark sequence consists of a set of watermark bits. From the signal processing perspective, a digital watermark is a digital signal. Subsequently, the original content (or the host signal) is embedded with the digital watermark and it becomes watermarked content or copyright-protected media.

Watermarking is a technique for media authentication and forgery prevention and it is viewed as an enabling technology to protect media from reuse without adequate credit or in an unauthorized way [Trowbridge 1995]. In general, watermarking enables ownership assertion, fingerprinting, authentication and integrity verification, content labeling, usage control and content protection [Memon and Wong 1998]. Digital watermarking offers copyright protection, ownership assertion, and integrity checks for various digital media, and it can provide evidence of copyright infringement after the event. Moreover, it may serve as a kind of deterrent to illicit copying and dissemination of copyrighted documents. Hawkins [Hawkins 1998] noted that many watermarking techniques have been proposed for intellectual property and copyright protection in the literature, but different media require different digital watermarking techniques. Moreover, the technical requirements of watermarking techniques also vary from application to application. Swanson et al. [Swanson, et al. 1998] identified the requirements for the application of copyright protection that watermarking must embed the ownership of the content when the content is being duplicated or abused.

Digital watermarking falls in the field of signal processing. The field of signal processing treats digital content as a digital signal. Digital signals include video signals and audio signals. Watermarking basically modulates one signal–the watermark signal-to another signal-the host signal. A perceptual watermarking technique uses adaptive watermarks that depend not only on the frequency response of the human eye and ear, but also on the properties of the host signal. A good perceptual watermarking technique should maximize the watermark strength (robustness) while satisfying the transparency requirement.

3. Analysis of Watermarking Processes

This section describes basic watermarking processes, including watermark insertion, detection and extraction. We take Cox's watermarking scheme [Cox, et al. 1997] as an example to explain watermarking concepts. We assume that the host digital content is a piece of digital music as it is easy to illustrate the operations.

3.1 Watermarking Process

Three basic watermarking processes are required in copyright protection management. They are watermark insertion, watermark detection and watermark extraction. In general, watermark insertion requires (i) digital content (or the host audio signal), (ii) a digital watermark, and (iii) and a private key that is held only by the owner of the digital content. After going through the watermarking insertion process, the process produces the watermarked music as shown in Figure 1a. The watermark can include information about ownership, the user's identity, and a description of the original data, etc. The watermark insertion process embeds a digital watermark into the digital content.

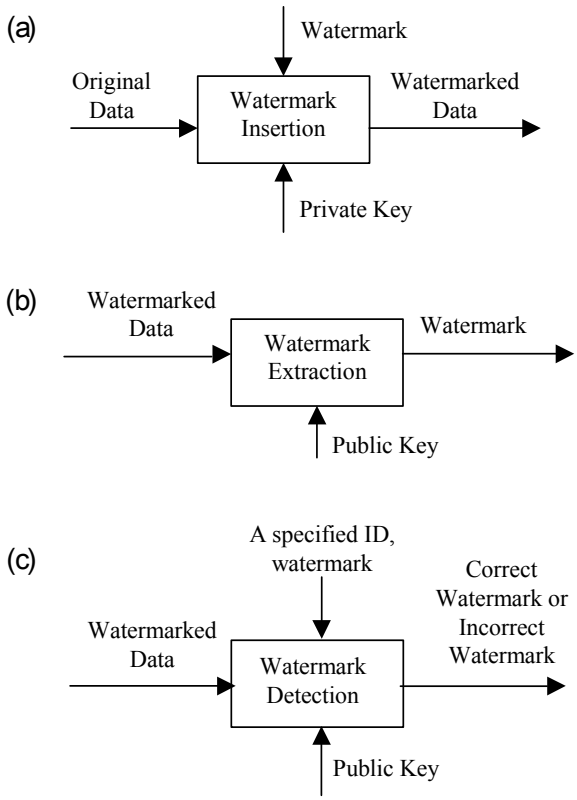


Figure 1: Watermark Procedures.

The watermark insertion process usually operates in the frequency domain of the host signal, which is known as the spread spectrum watermarking technique [Kirovski and Malvar 2003]. Cox's watermarking scheme [Cox, et al. 1997] is a typical example of this technique. Inserting the watermark sequence into the lower frequency components may result in highly robust watermarked music but it decreases the inaudibility of the watermark. On the other hand, inserting the watermark sequence into the higher frequency components of the music may render the watermark inaudible, but the robustness of the watermark decreases. There is always a trade-off between robustness and inaudibility. Therefore, some watermarking insertion processes choose the mid-band frequency for watermark embedding.

The generation of the watermark is usually a function of the information bits and a key. The key is needed for watermark detection and extraction. Some algorithms make the watermark generation dependent on the host audio signal, such that it is difficult for attackers to remove the watermark in the absence of the host audio signal.

Watermark extraction and detection processes as shown in Figures 1b and 1c are used to retrieve the embedded watermark from the watermarked music. In the process of watermark extraction, a public key, which is known to the general public, is used together with the watermarked music to retrieve the embedded creator's watermark.

Consumers have the right to know the creator of the distributed music and the watermark extraction process serves this purpose. In the watermark detection process, a public key and a specified ID or watermark are used together with the watermarked signal to determine whether the watermark is legitimate. When the copyright enforcement takes place (both online and offline) [Kwok and Lui 2002, Kwok and Tsang 2000], watermark detection will be used to verify the owners of the copyright-protected music. The owners include the distributor and the consumer.

4. Electronic Commerce Applications

When digital watermarks are used for intellectual property protection, many electronic commerce applications are benefited, and they include the online and offline distribution of multimedia content, broadcast services, document verification, ownership identification and so on. This technology also benefits content creators – artists, authors, and movie studios; content providers – photo stock archives, libraries, and professional photographers; electronic commerce and graphics software vendors; and manufacturers of digital still images, video cameras and digital video discs (DVDs).

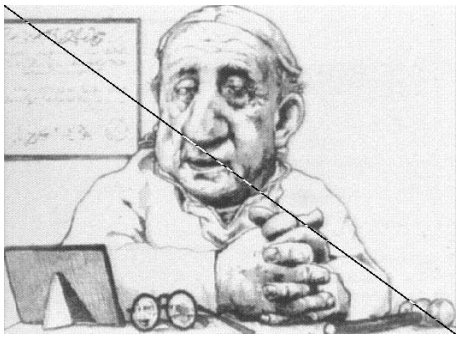
Numerous electronic commerce web sites are found in the Internet and nine general and typical web sites were chosen in our discussion. These nine representative distributor's web sites were chosen because (1) they distribute media content online; (2) they are representatives of web site in their businesses; (3) they have potentials to use digital watermarking; (4) they cover all four different media contents; and (5) they may have tried other methods to protect the distributed media contents. However, these web sites may not currently use digital watermarking for protection. The locations of the web site together with the media data types and types of associated digital contents are listed in Table 1. There are four basic data types of digital contents in these electronic commerce sites, namely image, video, audio and text. Common file formats for the four basic data types include JPEG and GIF for image; AVI, MOV and RA for video; MP3, WAV, and RA for audio, and PDF, PS and TIF for text.

Table 1: Nine representative electronic commerce web sites with their digital media data types and their digital contents.

Electronic Commerce Web Sites	Data Type	Digital Contents
NIST Image Gallery http://www.nist.gov/public_affairs/gallery/galindex.htm	Image	Scientific Graphic
Asian Painting Art Image Database http://wang.ist.psu.edu/cgi-bin/zwang/art/browse1.cgi	Image	Image Gallery
National Library of Medicine – OnLine Images from the History of Medicine http://www.nlm.nih.gov/	Image	Medicine Image
Apple Computer – Movie Trailer http://www.apple.com/trailers/	Video	Trailer and Music Video
ABC News http://abcnews.go.com/sections/us/video_index/video_index.html	Video	News Clip
MP3 http://www.mp3.com/	Audio	Music and Song
Live Radio on the Internet http://www.live-radio.net/	Audio	Music and Song
Truman Library http://www.trumanlibrary.org/photos/av-photo.htm	Text	Documentary Material
Delphion Research intellectual property network - international and US patent search database http://www.delphion.com/	Text	Patent Document

These web sites all offer digital contents for download, yet only a few appear to take any precautionary measures to prevent unauthorized or illegal further use of their digital contents. Some of these sites only include copyright statements and conditions of use which explained in explicit detail what kind of uses are, and are not, allowable for that particular assortment of digital contents. However, this appears not to be an aggressive approach for protecting their intellectual properties. A relatively interesting copyright protection attempt was found at the site of the National Library of Medicine – "OnLine Images from the History of Medicine". To prevent unauthorized re-use of the image files they provide, they have resorted to drawing diagonal lines through all the images known or

thought to be copyrighted and a sample image is given in Figure 2a. In the terminology of digital watermarking, this refers to a visible watermark. Use of a proper visible digital watermark was also found at the Asian Painting Art Image Database, which stamps the symbol of Copyright, "©" on all images in the database, to protect against unauthorized use. A sample image is shown in Figure 2b.



a. A sample image from National Library of Medicine – OnLine Images from the History of Medicine

b. A sample image from Asian Painting Art Image Database

Figure 2: Samples of perceptible watermark.

5. Watermark Design Patterns

As watermarking technology is still a relatively young research area and the past works were mainly devoted to specific applications and media data, it is difficult for developers who are new to the technology to select the appropriate watermarking technology to protect digital contents in their applications. To facilitate and encourage them to use the watermarking technology in a more convenient way, this paper proposes a mechanism or tool to relate off-the-shelf watermarking techniques and systems, and electronic commerce applications. Developers who are willing to use digital watermarking can easily identify appropriate techniques and commercial systems that best fit their applications by referring to the relationship diagram produced in Section 5.

A watermark design pattern (WDP) introduced in this paper describes the characteristics of a digital watermark for a particular media data. For instance, a watermark design pattern for image data can be invisible and fragile, whilst a watermark design pattern for audio data can be inaudible and robust. Different watermark design patterns are used in different applications due to their differences in digital contents and media data used in applications. A general WDP is described and presented in Figure 3.

The general watermark design pattern - $WDP_{media\ data}$ is a complete structure that covers all possible watermark design patterns that may be found in electronic commerce applications, regardless of the media data type of digital contents. The characteristics of a digital watermark, described in the general WDP, expresses that it can be either perceptible or imperceptible, and for either case, it can also be robust or fragile. For example, a watermark is perceptible and robust if it follows the left-most path, indicated by the thick arrow in Figure 3.

We studied nine typical electronic commerce web sites listed in Table 1 to investigate the relationship between watermark design pattern and media data. The focus of this paper is on copyright protection. Among the nine web sites, three sites are devoted to image data, and two sites are devoted to each video, audio, and text data. These web sites are typical media distribution sites, and we assume other media distribution web sites are of the same characteristics and requirements and therefore the results of this paper are applicable to them as well. After visiting and studying these sites and their media data, we learnt the characteristics of these sites, the properties of their digital contents and the characteristics of required watermarks. Applying the survey results to the general WDP, and incorporating the characteristics of existing watermarking technologies, we derived a set of four WDPs for various media data.

It is evident that although imperceptible watermarks dominate in most of these sites, perceptible watermarks are found to be useful for impressive samplings of digital image collections. Samples of perceptible watermark are already given in Figure 2.

It is noted that watermarks for audio and video data have to be inaudible and invisible respectively, as listeners and watchers like to enjoy these types of media in a noise-free and undisturbed environment. A perceptible watermark therefore could be a source of noise from the user's point of view. Watermarks for audio and video data

also have to be robust, in the sense that the watermarks can survive after undergoing various common attacks, such as cropping and filtering. It is necessary because fragments of video and music can be easily extracted for re-use without giving them proper credit or in an unauthorized way.

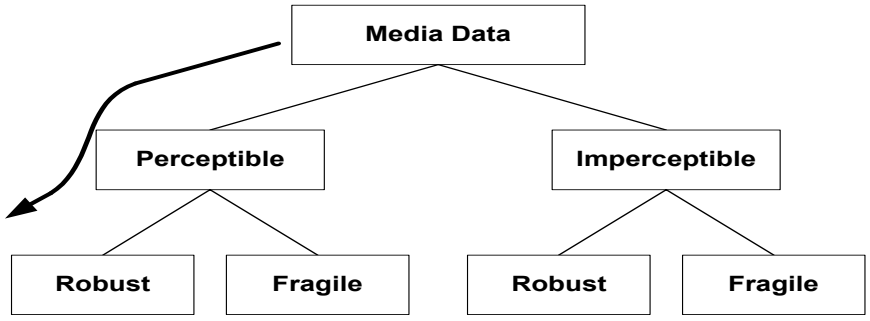


Figure 3: A general Watermark Design Pattern for Media Data.

Watermarks for rare documents and manuscripts, such as the Truman Library web site, have to be invisible, as these documents are already blurred after digitization. Any additional noise can likely turn the documents to be unreadable. Similarly, patent documents in IBM Intellectual Protection Network are also digitized documents; further distortion on the text and diagrams is not tolerable, and the attached bar-code requires a clear background for detection. Thus it is recommended that invisible watermarks are more appropriate for this type of document. In fact, text data in electronic commerce applications are usually produced by scanners and facsimiles and its readability has already been downgraded. Further degradation on the quality of the document is not encouraged. Besides, Acken [Acken 1998] suggested that an application used only to indicate modifications of the content needs only a fragile watermark. It is because fragile watermarks are easily corrupted by any form of signal processing procedures. Originality is the prime asset of important documents, such as rare and patent documents. Any changes or modifications must be noticeable to the viewers and owners. Thus, invisible and fragile watermarking is preferable to text data.

For image data, watermarks can be visible and invisible depending on the purposes of the application and digital contents. For promotion and demonstration purposes, a digital photograph may carry a visible watermark that can be a company trademark or a copyright mark, like Figure 2a, so that content distributors can easily identify their properties without performing any watermark extraction process. When perceptibility of digital contents is a concern, an invisible watermark is a better choice. All existing invisible image watermarking techniques and systems in the literature are robust, while all visible image watermark techniques and systems are fragile.

Basing on the above results, we conclude the characteristics of watermarks for the four different media data and their corresponding WDPs are shown in Figures 4, 5, 6 and 7.

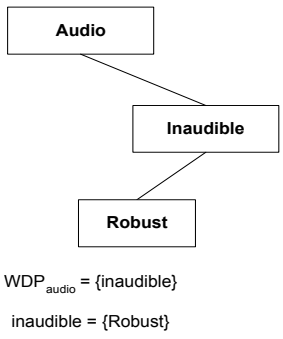


Figure 4: A WDP for Audio data.

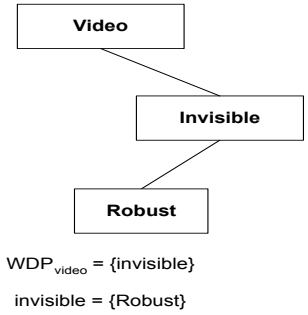


Figure 5: A WDP for Video data.

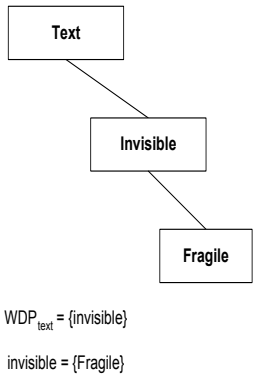


Figure 6: A WDP for Text data.

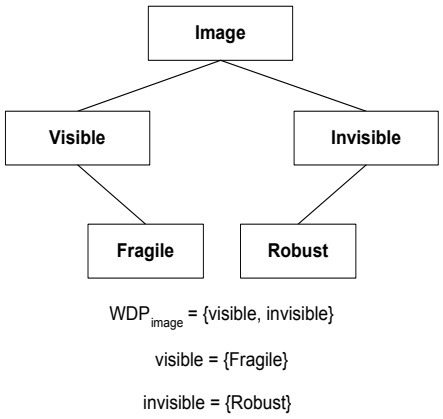


Figure 7: A WDP for Image Data.

These four WDPs are subsets of the general WDP, and they can be expressed as follows:
$WDP_{media\ data} = \{WDP_{image}, WDP_{video}, WDP_{audio}, WDP_{text}\}$

Our proposed WDPs can be summarized as follows:

- Watermark for audio data has to be inaudible and robust (Example: http://www.mp3.com/).
- Watermark for video data has to be invisible and robust (Example: http://www.apple.com/trailers/).
- Watermark for text data has to be invisible and fragile (Example: http://www.delphion.com/).
- Watermark for image data can be either: (1) visible and fragile (Example: http://www.nlm.nih.gov/), or (2) invisible and robust (Example: http://www.nist.gov/public_affairs/gallery/galindex.htm).

6. Relationship between Digital Watermarking Techniques and Electronic Commerce Applications

Using the four WDPs derived in Section 4, we introduce a selection scheme for electronic commerce application developers to select appropriate watermarking techniques and systems for different media data in their applications.

Zhao et al. [Zhao, et al. 1998] addressed that the watermarking technology's goals or functions can be classified into four application categories: copyright protection, hidden annotations; authentication; and secure and invisible communications. Each application category generally requires application-specific watermarking techniques. These categories are mapped to the electronic commerce domain. Incorporating the concept of WDP and the application categories, the basic relationship between digital watermarking techniques and electronic commerce applications can therefore be described as Figure 8.

In the diagram, there are four layers: category, digital contents, WDP and digital watermarking technique. At the category layer, four functions of the watermarking technology for electronic commerce applications are defined. For instance, for copyright protection, which is the focus of this paper, the application is enforced by a copyright protection scheme. Hence, the watermarking can provide ownership verification and identification. As discussed in Section 4, different media data of digital contents require different watermarking techniques. The characteristics of these digital watermarks are described by their associated WDPs, namely WDP_{video}, WDP_{image}, WDP_{audio} and WDP_{text} for video, image, audio and text data, respectively. Each WDP leads to a set of existing watermarking techniques and off-the-shelf watermarking systems.

The category of copyright protection in general can be formulated as follows:

$Cat_{copyright} = \{video_{copyright}, image_{copyright}, audio_{copyright}, text_{copyright}\}$

where

$video_{copyright} \Rightarrow WDP_{video}$,
$image_{copyright} \Rightarrow WDP_{image}$,
$audio_{copyright} \Rightarrow WDP_{audio}$, and
$text_{copyright} \Rightarrow WDP_{text}$.

And, therefore

$$Cat_{copyright} \Rightarrow \{WDP_{video}, WDP_{image}, WDP_{audio}, WDP_{text}\}$$

The above formulation can also be extendible to other categories. However, they are not covered in this paper because it is out of the scope of this paper.

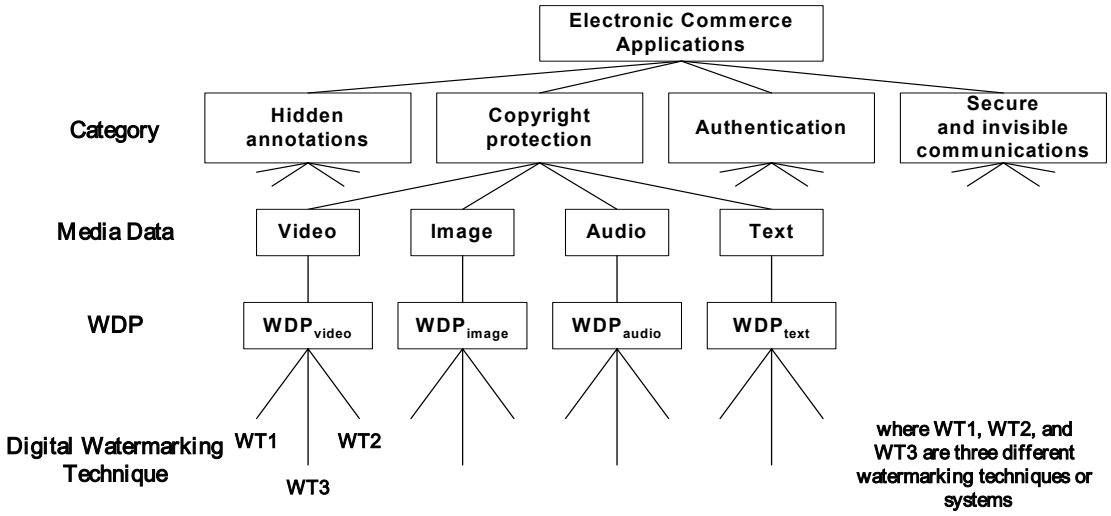


Figure 8: Relationships between digital watermarking techniques and electronic commerce applications.

The relationship diagram shown in Figure 8 is important for electronic commerce application developers to protect intellectual property of their distributed media, as it provides a look-up table for them to choose appropriate watermarking techniques and systems for their electronic commerce applications. For example, to design a web-based video distributing system, which supplies video trailers in MOV format to its subscribers, copyright protection should be a great concern to this form of electronic commerce. Referring to Figure 8, a digital watermark for its digital contents must be invisible and robust, and watermarking techniques, WT1, WT2, and WT3 are desirable for this case.

7. Problems of Copyright Protection using Watermarking

Copyright law gives the owner of the copyright the exclusive right to: (1) reproduce the work; record the work onto a CD, into a film soundtrack or onto a computer disk or reproduce the lyrics as sheet music or photocopy them (known as mechanical rights); (2) publish the work for sale or other transfer of ownership, or by rental, lease, or lending; (3) perform the work publicly, including performing the work live in pubs, clubs or at festivals or by through playing a recording of the work or showing a film containing the work. In the music industry, the right to perform a work in public is part of the performing rights; (4) make an adaptation of the work, for example, by arranging or transcribing the music or translating the lyrics. Consequently, a practical copyright protection scheme should allow the owner and should disallow unauthorized parties to execute these rights. As watermarking is the underlying technology for copyright protection, it is the responsibility of a watermarking scheme to facilitate the execution of these rights.

This section highlights the requirements of watermarks for copyright protection. Perceptual transparency and robustness are the most common requirements in a watermarking scheme. The requirements basically ensure that the quality of the original content is not degraded noticeably and the watermarked or copyright-protected digital content can resist attacks. Other requirements, such as security, unambiguous proof of ownership, and the capacity of the watermarking algorithm, are also required for copyright protection. Here we identify the above requirements and also point out challenges faced in meeting these requirements. Possible solutions to the problems are also given.

PERCEPTUAL TRANSPARENCY

Watermarks can be either perceptible or imperceptible. For the application of copyright protection, watermarks in content distribution are usually imperceptible. Perceptual transparency means that the embedded watermark is perceptually undetectable by humans. If humans cannot differentiate between the original content and the

watermarked content, the watermark is imperceptible. Blind tests are usually conducted to measure the perceptual transparency, where human subjects are randomly presented with data with or without watermarks and asked to determine the quality.

PROBLEMS

- Watermarks in digital music may not always be imperceptible if the human auditory system (HAS) model is not used in the watermarking scheme. Similarly, the model of the human visual system (HVS) is important for imperceptible image and video watermarks.
- Even though a watermarking technique claims that it can provide imperceptible watermarks, this may not always be true because watermark imperceptibility is also subject to the characteristics of the processing digital signal i.e., the processing frame. For example, the watermark performs very well in the first frame, but this may not be the case in the last frame as the characteristics of the two frames may be totally different.

SOLUTIONS

- Classify watermarking techniques for some specific digital content. For example, if Cox's watermarking is imperceptible in a high frequency audio signal, apply this watermarking technique to high frequency signals only. The imperceptibility of watermarking has to be extensively examined with experiments.

ROBUSTNESS

Signal processing operations, such as MP3, cropping, etc. are frequently applied to the watermarked content. Such operations can be considered as "attacks". After the attack, the watermarked content is modified or manipulated and the embedded watermark may have been destroyed. If the watermark is robust, it can ensure that the embedded watermark will not be destroyed and affected by the attack. As a result, unauthorized parties are not able to modify the watermarked content to thwart detection of the embedded watermark. An attacker usually performs many different kinds of operations (or attacks) on the watermarked content in an attempt to remove the embedded watermark. There is benchmarking software to ensure the robustness of the watermarking technique. Many benchmarking software packages are for image watermarking, including StirMark [Kuhn 2003].

PROBLEMS

- When the watermark insertion process performs on the same frame several times, the previous watermark may be altered accidentally, even though some watermarking algorithms claim to be very robust to attacks.
- There is no benchmarking software other than for image watermarking. It is risky not to use robust watermarking in business.
- If the copyright protection scheme employs a breakable watermarking technique, the protection of the copyright-protected content is not strong.

SOLUTIONS

- Avoid watermarking a frame more than once at the distribution site.
- All watermarking techniques in the copyright protection scheme must be evaluated before use.
- To improve the robustness of watermarking, classify watermarking techniques according to the characteristics of the signal.

SECURITY

In many applications, the embedding procedure must be secure so that an unauthorized user is not able to detect the presence of embedded data and to alter the embedded data. Security of watermarking can be interpreted in the same way as security of encryption techniques. Secure watermarking cannot be broken unless the unauthorized user has access to a secret key that controls the insertion of the data in the host signal. Thus, a watermarking scheme is truly secure if knowing the exact watermarking technique for embedding the data does not help an unauthorized party detect the presence of embedded data. An unauthorized user should not be able to extract the data in a reasonable amount of time even if he/she obtains the original host signal and is familiar with the exact watermarking algorithm.

PROBLEMS

If one can detect and extract the embedded watermark from digital content, all other digital contents from the same distributor are breakable. It is recommended that the distributors should utilize a complex watermarking scheme that requires various combinations of watermarking parameters in order to prevent this from happening and to discourage attackers from attacking the copyright protection scheme. Besides, the watermarking parameters, such as the secret key, the random generator algorithm, and the frame size, must be securely maintained.

SOLUTIONS

- Employ a sufficiently large number of parameters for watermarking.
- Apply more than one watermarking technique in the copyright protection scheme.

UNAMBIGUOUS PROOF OF OWNERSHIP

The proof of ownership is the application that requires the most attention in watermarking technologies.

PROBLEMS

No current watermarking technique is able to determine unambiguously the ownership of digital content if it does not use the original or copy in the detection process. Watermarks can be added to the watermarked content. In such cases, multiple ownerships may be claimed, which is also known as the deadlock problem.

SOLUTIONS

- The copyright protection scheme should only allow a small set of valid watermarks in the copyrighted material. Any watermark other than those from the small set is considered to be invalid.
- Employ a watermark clearance center to certify the copyright protection scheme. The clearance center is also responsible for issuing watermarks for all involved parties, registering the variable parameters and watermarking techniques in use, and making final judgments on the ownership of the distributed content.

THE CAPACITY OF THE WATERMARKING ALGORITHM

Knowing how much information can reliably be hidden in the host signal is very important to content distributors especially when the scheme gives them the ability to change this amount. Knowing the watermarking-access-unit (or granularity) is also very crucial; spreading the watermark over a full sound track prevents audio streaming, for instance. On the other hand, having the possibility of embedding a large number of watermark bits into a relatively short audio signal is also important to distributors, especially when multiple-bit watermarking is in use. The frame-to-watermark (FW) ratio of the number of frames to the total watermark length is a way to measure the number of watermark bits. The algorithm's capacity also determines how much side information can be embedded into the digital content together with the watermarks.

PROBLEMS

When multiple-bit watermarking is used, the capacity of the watermarking algorithm drops dramatically as each frame can at most contain only one bit of information. In the situation when the FW ratio is smaller than one, it is not possible to insert all watermark bits into the digital audio signal.

SOLUTIONS

- Based on many watermarking techniques using HAS, the watermarking scheme will insert a very weak watermark (or even no watermark) to the frame if the frame contains very few tonal components. For those frames containing excessive amounts of tonal components, an insufficiently strong watermark may be inserted into the digital content. This implies that the fixed-size framing approach is not efficient. A scheme with the flexible-size framing may improve the FW ratio.

8. Management Issues

There are many managerial issues related to the copyright protection of an online content distribution site.

BUSINESS MODEL: Distributors must first consider which business model to use for online content distribution. There are several options available, such as the pay-per-view model [Eolasia 2003], the subscription model [Napster 2003], the content sharing model [Gnutella 2003] and so on. The business model determines the choice of the copyright protection scheme. For example, under the pay-per-view model, the copyright-protected content can be delivered to customers through a streaming technology, for which a real-time copyright protection scheme is needed. In the case of a content sharing model in which consumers may share the purchased files with others (the laws in some countries do allow this), transfer of ownership becomes a need and thus the copyright-protection scheme should address this issue. Kwok and Lui [Kwok and Lui 2002] proposed a solution to this problem.

WATERMARK CLEARANCE CENTER: Distributors should employ a trustworthy watermark clearance center (WCC) to manage ownership identification and verification. The watermark clearance center could be a government authority or an entity representing the industry. The roles of the WCC are to (a) issue, renew, and revoke digital watermarks to creators, distributors, and individuals (consumers); (b) generate watermark revocation lists; and (c) publish watermarks through a directory server. In managing the ownership, the WCC acts as a judge to verify any suspected content files offline, indicating that there can be offline copyright enforcement as well. With the use of the WCC, the control of the valid range of watermark values can be achieved. However, there is no

official WCC being set up so far. As more online businesses realize the importance of copyright protection, such a clearance center will emerge. It is similar to the case of a CA issuing digital certificates.

MEMBERSHIP: A membership scheme allows the distributors to know their customers better keep records on all transactions made by the customers, know the credit histories of the customers, and obtain past credit records from other organizations and authorities, such as the WCC. Under a membership scheme, customers must be registered prior to ordering and purchasing from a distribution site and a unique identity is assigned to each customer. The IDs (or watermarks) are issued by the WCC.

WATERMARKING SCHEME: The watermarking scheme is closely related to the transaction model. In choosing the watermarking techniques in the copyright scheme, a sufficiently large number of watermarking techniques should be included. The chosen watermarking techniques must have been subjected to benchmarking tests for potential attacks. The proposed WDP can be useful in this case to identify the best watermarking techniques for particular digital content with specific characteristics.

COPYRIGHT ENFORCEMENT: There are two types of copyright enforcement, online and offline enforcement. Online copyright enforcement is administrated by the media player on the consumer side. The media player is able either to verify the copyright-protected content through the use of the copyright server at the watermark clearance center, or to verify the content using an internal watermark detection module [Kwok, et al. 2000, Kwok, et al. 2004 forthcoming]. Prior to taking action on illegal acts, the owners of the copyright-protected content must report the incident to a law enforcement agency. It would be more efficient if the owners (the creator and the distributor) could suggest a way to verify that the suspected digital content has infringed the copyright. Owners usually provide all variable parameters or an ownership verification software to claim the ownership of the distributed content. The latter is more secure than the former.

RELIABILITY OF THE WATERMARKING SCHEME: Breaking a watermark means one can (a) remove the embedded watermark(s) so that the copyright-protected content carries an incomplete set of watermarks; (b) modify the embedded watermark so that the ownership will be transferred to an unauthorized person; and (c) insert one or more watermarks using the same watermarking technique as the distributor to the copyright-protected content so that the rightful owners will fail to claim ownership [Kwok 2003].

9. Conclusions

Watermarking is undoubtedly important for protecting various forms of digital contents in the digital age. Electronic commerce applications require such protection to prevent the misuse of the material they mount for public consumption. However, only a few electronic commerce application developers apply efficient techniques to protect digital contents in their applications, mainly because they are unfamiliar with the technology. The objectives of this paper are to (1) develop a scheme that can facilitate electronic commerce application developers to choose adequate and appropriate digital watermarking techniques and off-the-shelf systems for their applications in an efficient way; (2) cover the problems of copyright protection using watermarking; and (3) discuss management issues. This paper proposed the watermark design pattern (WDP) to describe the characteristics of a digital watermark for specific media data. A study of nine representative distributor's web sites, which are exhibiting digital contents on the WWW, was conducted to investigate the relationship between watermark design patterns and media data, when copyright protection is a concern. Applying the study results to the general WDP and using characteristics of existing watermarking techniques, four watermark design patterns – WDP_{video}, WDP_{audio}, WDP_{image}, and WDP_{text} were derived for four different media data – video, audio, image and text, respectively. We extended and applied our findings and analysis to present the relationship between digital watermarking techniques and electronic commerce applications. The relationship diagram fulfills our objectives by closing the gap between developers' needs and digital watermarking technologies for copyright protection. Following the relationship diagram, the developers could (1) protect the intellectual property of distributed contents using digital watermarking by picking the corresponding watermarking techniques; (2) automatically apply appropriate digital watermarking techniques without knowing the details of watermarking techniques because the WDPs were developed based on their design guidelines; and (3) share experiences of other distributors while using the relationship diagram.

WDPs derived in this paper are an indispensable tool for protecting copyright when used by typical and general media distribution web sites. In special or extreme cases, WDPs may differ from those derived from the nine web sites. In order to strengthen the argument of our results, we will continue an extensive study on widespread electronic business web sites and applications. Future research will also focus on the issue of the applicability of versatile watermarking techniques to more than one type of media data, and how these techniques affect the structure of the relationship between watermarking techniques and electronic commerce applications.

Acknowledgements

The work described in this paper was partially supported by grants from the Research Grants Council of the Hong Kong Special Administrative Region, China (Project No. HKUST6256/03E), and the Sino Software Research Institute (SSRI) (Ref. SSRI01/02.BM01).

REFERENCES

Acken, J. M., "How Watermarking Adds Value to Digital Content," *Communications of ACM*, Vol. 41, pp. 75-77, 1998.

Anderson, L. C. and J. B. Lotspiech, "Rights Management and Security in the Electronic Library," *Bulletin of the American Society for Information Science*, Vol. 22, pp. 21-23, 1995.

Chen, T. H. and W. B. Lee, "A Variance-Based Public Verifiable Copyright Protection Scheme Surviving Intentional Attacks," *Imaging Science Journal*, Vol. 51, pp. 1-12, 2003.

Cox, I. J., J. Kilian, T. Leightont, and T. Shamoon, "Secure Spread Spectrum Watermarking for Images, Audio, and Video," *IEEE Transactions on Image Processing*, Vol. 6, pp. 1673-1687, 1997.

Dittmann, J., M. Steinebach, P. Wohlmacher, and R. Ackermann, "Digital Watermarks Enabling E-Commerce Strategies: Conditional and User Specific Access to Services and Resources," *Eurasip Journal on Applied Signal Processing*, Vol. 2002, pp. 174-184, 2002.

Eolasia, Eolasia.com, http://www.eolasia.com, accessed on 14 April 2003.

Gnutella, Gnutelliums - Gnutella Download, http://www.gnutelliums.com, accessed on 15 April 2003.

Harper, G. K., "Copyright Endurance and Change," *Journal of Electronic Publishing*, Vol. 7, 2001.

Hawkins, D. T., "Digital Watermarking: Intellectual Property Protection for the Internet?," *Online*, pp. 91-93, 1998.

Huang, F., H. M. Hosseini, H. C. Chua, and Y. L. Guan, "Watermarking of Streaming Video for Finger-Printing Applications," Proceedings of the IEEE International Symposium on Circuits and Systems, 2002.

Kirovski, D. and H. S. Malvar, "Spread-Spectrum Watermarking of Audio Signals," *IEEE Transactions on Signal Processing*, Vol. 51, pp. 1020-1033, 2003.

Kuhn, M., StirMark - Image Watermarking Robustness Test, http://www.cl.cam.ac.uk/~mgk25/stirmark.html, accessed on 14 April 2003.

Kwok, S. H., "Watermark-Based Copyright Protection System Security," *Communications of the ACM (CACM)*, Vol. 46, pp. 98-101, 2003.

Kwok, S. H. and S. M. Lui, "A License Management Model for Peer-to-Peer Music Sharing," *Special Issue on Virtual Organizations and E-Commerce Applications in the International Journal of Information Technology and Decision Making (IJITDM)*, Vol. 1, pp. 541-558, 2002.

Kwok, S. H. and K. F. Tsang, "Adaptive Audio Watermarking Scheme for Copyright Protection," Proceedings of the Pacific Asia Conference on Information Systems (PACIS 2000), 2000.

Kwok, S. H. and C. C. Yang, "Watermarking in Online Media E-Business," Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC-2002), 2002.

Kwok, S. H., C. C. Yang, K. Y. Tam, and J. S. W. Wong, "An SDMI-Based Rights Management System for Electronic Media Using Digital Watermarking," Proceedings of the International Conference on Electronic Commerce (ICEC 2000), 2000.

Kwok, S. H., C. C. Yang, K. Y. Tam, and J. S. W. Wong, "SDMI-Based Rights Management Systems," *Decision Support Systems (DSS)*, 2004 forthcoming.

Memon, N. and P. W. Wong, "Protecting Digital Media Content," *Communications of ACM*, Vol. 41, pp. 35-43, 1998.

Napster, Napster, http://www.napster.com, accessed on 15 April 2003.

Piva, A., F. Bartolini, and M. Barni, "Managing Copyright in Open Networks," *IEEE Internet Computing*, Vol. 6, pp. 18-26, 2002.

Swanson, M. D., M. Kobayashi, and A. H. Tewfik, "Multimedia Data-Embedding and Watermarking Technologies," Proceedings of the IEEE, 1998.

Trowbridge, C., Image Protection for Archives, Special Collection Libraries and Museums in the WWW Environment, http://sunsite.berkeley.edu/Imaging/Databases/Fall95papers/trowbridge.html, accessed on 11 March 2003.

WIPO, WIPO - World Intellectual Property Organization, http://www.wipo.int/, accessed on 14 April 2003.

Zhao, J., E. Koch, and C. Luo, "Digital Watermarking In Business Today and Tomorrow," *Communications of ACM*, Vol. 41, pp. 67-72, 1998.