http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 5 (3): 471-475, 2006
ISSN 1812-5638

A Comprehensive Analysis of Digital Watermarking

[1,2]Muhammad Aamir Qureshi and [1]Ran Tao
[1]Department of Electronics Engineering, Beijing Institute of Technology, Beijing-100081, China
[2]Department of Electrical Engineering, NED University of Engineering and Technology, Karachi, Pakistan

Abstract: Copyright protection of digital contents has become more and more important in accordance with the development of digital technology. As a solution of this predicament, digital watermark technology is drawing attention and various watermarking methods have been presented and studied. Digital watermarking provides protection of intellectual property in the digital world. Just as plagiarism runs rampant in the physical world, unauthorized copying of data whether it be audio, visual, or video exists in the digital world. Digital watermarking attempts to copyright the digital data that is freely available on the World Wide Web to protect owner's rights. As opposed to traditional, printed watermarks, digital watermarks are transparent signatures. They are integrated within digital files as noise, or random information that already exists in the file. Thus, detection and removal of the watermark becomes more difficult. Typically, watermarks are dispersed throughout the entire digital file such that manipulation of one portion of the file does not alter the underlying watermark. However, it is difficult to decide which method is better than others, because the measure for evaluating their performance has not been established yet. Recently, digital contents can be easily accessed by using computer networks and the problem of protecting multimedia information becomes more and more important. To resolve various problems occurring in these upcoming areas and future emerging disciplines, digital watermark technology is now drawing attention as a new method and technique of protecting copyrights for digital data. Digital watermark is realized by embedding information data with an insensible form for human audio/visual systems. It must be difficult for an attacker to remove watermark purposely. In this paper an outline of watermarking and analysis of the various techniques used in the area of image watermarking is presented.

Key words: Watermarking

INTRODUCTION

The past decade has seen an explosion in the use and distribution of digital multimedia data. PCs with Internet connections have made the distribution of digital data and applications much easier and faster. However, this has also had a serious effect on copyright encroachment, thereby creating a new demand for copyright protection of digital data. To provide copyright protection for digital data, two complementary techniques have been developed: encryption and watermarking. Encryption can be used to protect digital data during the transmission process from sender to the receiver. However, after the receiver has received and decrypted the data, it becomes identical to the original data and is no longer protected. Watermarking can compliment encryption by embedding a secret imperceptible signal, a watermark, into the original data in such a way that it always remains present.

Digital watermarking is the unique solution that can be used for protecting all the digital multi media data from any illegal use. Digital watermarking comes to the front as new application to give the protection needed in the world of digital multi media. Digital watermarking is the process of embedding particular information (watermark message) into or onto the digital media and retrieving it from other digital data.

A digital watermark is a distinguishing piece of information that is adhered to the data that it is intended to protect, this meaning that it should be very difficult to extract or remove the watermark from the watermarked object. Since watermarking can be applied to various types of data, the imperceptibility constraint will take different forms, depending on the properties of the recipient (i.e., the human senses in most practical cases).

WATERMARKING PROCESS

The successive stages of watermarking process are described as follows:
In general, any watermarking scheme (algorithm) consists of three parts (Bloom *et al*., 1999):

Corresponding Author: Muhammad Aamir Qureshi, Department of Electronics Engineering, Beijing Institute of Technology, Beijing-100081, China Tel: 86-10-68914646

- The watermark
- The encoder (marking insertion algorithm)
- The decoder and comparator (verification or extraction or detection algorithm)

Each owner has a unique watermark or an owner can also put different watermarks in different objects and the marking algorithm incorporates the watermark into the object. The verification algorithm authenticates the object determining both the owner and the integrity of the object.

Decoder: If an image is denoted by I, a signature by $S = \{s_1, s_2, ...\}$ the watermarked image by I'. E is an comparator encoder function, it takes an image I and a signature S and it generates a new image which is called watermarked image I', i.e.,

$$E (I, S) = I'$$

It should be noted that the signature S may be dependent on image I. In such cases, the encoding process described by the above equation holds.

A decoder function D takes an image J (J can be a watermarked or an un-watermarked image and possibly corrupted) whose ownership is to be determined and recovers a signature S' from the image. In this process, an additional image I can also be included which is often the original and un-watermarked version of J. This is due to the fact that some encoding schemes may make use of original images in the watermarking process to provide extra robustness against intentional and unintentional corruption of pixels. Mathematically,

$$D (J, I) = S'$$

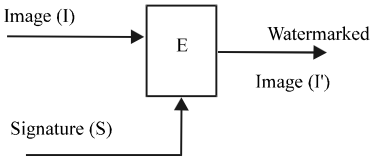
The extracted signature S' will then be compared with the owner signature sequence by a comparator function C_δ and a binary output decision generated. It is 1 if there is a match and 0 otherwise.

$$C_\delta(S', S) = \{1, c >= \delta \quad 0, \text{otherwise}\}$$

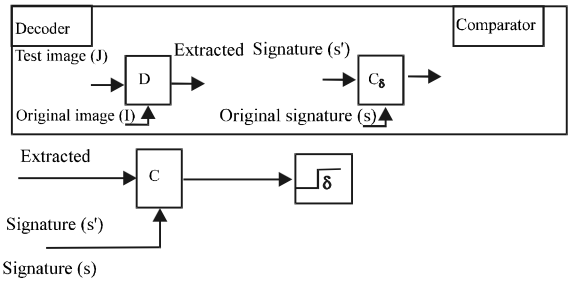
Here, c is the correlation of two signatures and δ is certain threshold. Figure below shows the comparator.

Where, C is the correlator and $x = C \delta S, S'$. Without loss of generality, watermarking scheme can be treated as a three-tuple (E, D, C_δ).

A watermark must be detectable or extractable to be useful (Cox *et al*., 1999). Depending on the way a watermark is inserted and depending on the nature of the watermarking algorithm, the method used can involve



Encoder



Comparator

very distinct approaches. In some watermarking schemes, a watermark can be extracted in its exact form, a procedure we call watermark extraction. In other cases, we can detect only whether a specific given watermarking signal is present in an image, a procedure we call watermark detection. It should be noted that watermark extraction can prove ownership whereas watermark detection can only verify ownership (Dugelay, 1999)

WATERMARKING PROPERTIES

A watermark is designed to permanently reside in the host data. When the ownership of data is in question, the information can be extracted to completely characterize the owner. To achieve maximum protection of intellectual property with watermarked media, several requirements must be satisfied.

Ideal properties of a digital watermark have been stated in many articles and papers (Gonzalez, 2002; Hernandez *et al*., 2000; Johnson and Katezenbeisser, 1999). Properties depend on application such as fragile watermarking is needed for authenticity.

Among the desirable properties which a watermark should have are:

Perceptual transparency: A digital watermark should not be noticeable to the viewer nor it should degrade the quality of content. The watermark should be imperceptible so as not to affect the viewing experience of the image or the quality of the audio or a video signal.

Undetectable: The watermark must be difficult or even impossible to remove by malicious cracker or an attacker, at least without obviously degrading the host signal.

Robustness: A watermark must be difficult to remove. The attempt to destroy the mark by adding a noise should result in the degradation of the perceptual quality of the host data so as to render it unusable. The mark should resist to: - Common signal processing: for instance, color alterations for a picture or lossy compression; - Geometric transformations: for images, rotation, scaling, translation, mosaicing, cropping.

Security: This is a description of how easy it is to intentionally remove a watermark example by deletion, modification or buying of the watermark in another illicit one.

Data capacity: Refers to the amount of information that can be stored within the content. For example, when transmitting medical images, the personal data and the diagnosis can be embedded into the same picture.

WATERMARKING TECHNIQUES

In general, the embedding techniques can be classified into two categories: spatial domain approach (Katzrnbeisser, 1999; Kutter and Hartung, 1999) or frequency domain approach (Langelaar *et al*., 2000). Spatial domain watermarking technique slightly modifies the pixels of one or two randomly selected subsets of an image. Modifications might include flipping the lower-order bit of each pixel. The inserted information may be easily detected using computer analysis.

Many frequency domain sometimes called the transform domain approaches have been proposed including the discrete cosine transform, discrete wavelet transform and discrete Fourier transform. Many scholars have found that the frequency domain approach has some advantages because most of the signal processing operations can be well characterized in the frequency domain. In frequency domain, values of certain frequencies are altered from their original. The watermark is inserted into the coefficients of the transformed image. Typically, these frequency alterations are done in the mid-frequency components since the low frequency components are very sensitive to distortion and the high frequency components can be removed without significantly affecting the original image quality. The frequency domain watermarking methods are relatively robust to noise, image processing and compression compared with the spatial domain methods (Langelaar *et al*., 2000).

Unfortunately, not too much data can be embedded in the frequency domain because the quality of the host image will be distorted significantly. Shih *et al*. (1999) suggested combination of spatial and frequency domain in order to provide more watermark data and to minimize the distortion of the watermarked image.

Currently watermark techniques based on the transfer domain are more popular and effective as compared to those of the spatial domain. DCT-based methods have been most widely used in a lot of research works among the transform based methods. However, recently wavelet-based watermark techniques are becoming main research topic. With wide as well as expanding use of the internet, effective audio and video watermarking researches are also required.

CLASSIFICATION OF DIGITAL WATERMARKING APPLICATIONS

There are a number of different watermarking application scenarios and they can be classified in a number of different ways. The following classification is based on the type of information conveyed by the watermark (Meerwald, 2001).

Watermarking (data hiding) (Meerwald, 2001) is the process of embedding data into a multimedia element such as an image, audio or video file. This embedded data can later be extracted from, or detected in, the multimedia for security purposes. A watermarking algorithm consists of the watermark structure, an embedding algorithm and an extraction, or a detection algorithm. Watermarks can be embedded in the pixel domain or a transform domain. In multimedia applications, embedded watermarks should be invisible, robust and have a high capacity. The approaches used in watermarking still images include least-significant bit encoding, basic M-sequence, transform techniques and image-adaptive techniques.

In image watermarking, two distinct approaches have been used to represent the watermark. In the first approach, the watermark is generally represented as a sequence of randomly generated real numbers having a normal distribution with zero mean and unity variance. This type of watermark allows the detector to statistically check the presence or absence of the embedded watermark. In the second approach, a picture representing a company logo or other copyright information is embedded in the cover image. The detector actually reconstructs the watermark, and computes its visual quality using an appropriate measure (Table 1).

Digital watermarking is an effective technique for protecting Intellectual Property (IP) rights by embedding information in digital multimedia data. It bears a huge commercial potential as it is widely deployed in consumer electronic devices. Digital watermark technology can be used in consumer electronic devices such as digital still

Table 1: Classes of watermarking applications

Application class	Purpose of the embedded watermark	Application scenarios
Protection of intellectual property rights	Conveys information about content ownership and intellectual property rights	Copyright protection, copy protection, Fingerprinting
Content verification	Ensures that the original multimedia content has not been altered and/or helps determine the type and location of alteration	Authentication integrity checking
Information hiding	Represents side-channel used to carry additional information	Broadcast monitoring system enhancement

cameras, digital video cameras, Set Top Boxes (STB), Digital Versatile Disc (DVD) players and MPEG-1 Audio Layer-3 (MP3) players. As a result, it can protect information in controlled access (pay-per-view broadcasts) preventing illegal replication and embedding ownership information in images captured in digital, still or video cameras.

An exhaustive list of watermarking applications is of course impossible. However, it is interesting to note the increasing interest in fragile watermarking technologies. Especially applications related to copy protection of printed media are very promising. Examples here include the protection of bills with digital watermarks. In addition to technological developments, marketing and business issues are extremely important and require in-depth analysis and strategic planning. It is very important to prepare the industry to the usage of digital watermarks and to convince them of the added value their products can gain, if they employ digital watermarking technologies.

CONCLUSIONS

The recent expansion of the internet medium and usage in communications engineering besides in the daily life of human beings, corporations, organizations, establishments, governments, military, etc and the networked multi media systems has necessitated the need for protection of digital media. This is especially critical for the protection and enforcement of intellectual property rights. Copyright protection involves the authentication of object (text/image/video) ownership and the identification of illegal copies of a (possibly forged/fake) object.

This study has introduced the background information, requirements and evaluation techniques required for the implementation and evaluation of watermarking techniques. The paper gives a brief but comprehensive overview of the watermarking area with reference to image watermarking.

Techniques are needed to prevent the copying, forgery and unauthorized distribution of images and video. In the absence of above, playing images or video sequences on a public network puts them at risk of theft and alteration. The need for watermarking emanates from the following: A designer has created an image and wants to make it available on the network. When unauthorized copies or forgeries of the image appear elsewhere on the network, the designer needs to prove his/her ownership of the image. One also needs to determine if and by how much the image has been modified from the original. This way a person can prove ownership by illustrating the difference between the forged image and the original.

Digital watermarking is becoming a popular technology for the information security engineering and communications, the speed of its utility is rapidly increasing. In the early days, encryption and control access techniques were used to protect the ownership of media. Recently, the watermark techniques are utilized to keep the copyright of media.

For the foreseeable future digital watermarking technology will complement information and data security in information hiding environments. The primary reason is that the digital watermarking technology is more secure, reliable, robust and accurate in many aspects than previously used techniques and methods for this purpose.

REFERENCES

Bloom, J.A., I.J. Cox, T. Kalker, J.M.G. Linnartz, M.L. Miller and C.B.S. Traw, 1999. Copy Protection for DVD Video. In Proceedings of the IEEE, 87: 1267, 1272-1275.

Cox, I.J., M.L. Miller, J.M.G. Linnartz and T. Kalker, 1999. A Review of Watermarking Principles and Practices. In Digital Signal Processing for Multimedia Systems, Parhi K.K. and T. Nishitani (Eds.), New York, New York, Marcel Dekker, Inc., pp: 461-482.

Dugelay, J. and S. Roche, 1999. A Survey of Current Watermarking Techniques. In: Information Techniques for Steganography and Digital Watermarking, Katzenbeisser, S.C. *et al.* (Eds.). Northwood, MA: Artec House, pp: 121-145.

Gonzalez, R.C. and R.E. Woods, 2002. Digital Image Processing. Upper Saddle River, New Jersey, Prentice Hall, Inc.

Hernandez, J.R., M.Amado and F. Perez-Gonzalez, 2000. DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis And a New Structure, in IEEE Trans. Image Processing, 9: 55-68.

Johnson, N.F. and S.C. Katezenbeisser, 1999. A Survey of Steganographic Techniques. In: Information Techniques for Steganography and Digital Watermarking, Katzenbeisser, S.C. *et al.* (Eds.). Northwood, MA: Artec House, pp: 43-75.

Katzenbeisser, S.C., 1999. Principles of Steganography. In Information Techniques for Steganography and Digital Watermarking, Katzenbeisser, S.C. *et al.* (Eds.). Northwood, MA: Artec House, pp: 2-40.

Kutter, M. and F. Hartung, 1999. Introduction to Watermarking Techniques. In: Information Techniques for Steganography and Digital Watermarking, Katzenbeisser, S.C. *et al.* (Eds.). Northwood, MA: Artec House, pp: 97-119.

Langelaar, G., I. Setyawan and R.L. Lagendijk, 2000. Watermarking Digital Image and Video Data. In: IEEE Signal Processing Magazine, 17: 20-43.

Meel, J., 1999. Spead Spectrum. De Nayer Institute, October 6th, 1999.

Meerwald, P. and A. Uhl, 2001. Watermark Security Via Wavelet Filter Parameterization. Internation Conference on Image Processing, Thessaloniki, Greece.

Meerwald, P. and A. Uhl, 2001. A Survey of Wavelet-Domain Watermarking Algorithms. EI San Jose, CA, USA.