DIGITAL IMAGE WATERMARKING

Brijesh kumar[1], Mahesh Gupta[2], Hitesh Kumar[3], M.R. Markam[4]
Department of MCA, G.H. Raisoni College of Engineering, Nagpur, India
bmguptadocs@gmail.com,hiteshmadgames@gmail.com

***Abstract*— In this paper we have attempted to presents the Digital Watermarking technology which is one of the data hiding technique that implants a message into an image or text or other digital form. Digital watermarking has several classifications such as visible & transparent watermarking, public & private watermarking, asymmetric & symmetric watermarking steganographic & non-steganographic watermarking etc. And techniques such as Least-Significant Bit (LSB),SSM-Modulation-Based Technique,Discrete Cosine Transformation (DCT),Discrete Wavelet Transformation (DWT) etc. The key applications of digital watermarking aresecurity, certification, authentication,conditionalaccess,copyrightprotection,copyprotection,telemedicine, criminal photograph authentication, Fraud and Tamper Detection, Fingerprinting which can be used to protect data.**

INTRODUCTION

Digital Watermarking describes methods and technologies that hide information, for example a number or text, in digital media, such as images, video or audio. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data. The hiding process has to be such that the modifications of the media are imperceptible. For images, this means that the modifications of the pixel values have to be invisible. Furthermore, the watermark must be either robust or fragile, depending on the application. By "robust", we mean the capability of the watermark to resist manipulations of the media, such as lossy compression (where compressing data and then decompressing it retrieves data that may well be different from the original, but is close enough to be useful in some way), scaling, and cropping, among others. In some cases, the watermark may need to be fragile. "Fragile" means that the watermark should not resist tampering, or would resist only up to a certain, predetermined extent.

The example below illustrates how digital watermarking can hide information in a totally invisible way. The original image is on the left; the watermarked image is on the right and contains the name of the author.[7]

WHAT IS WATERMARKING USED FOR?

The first applications that came to mind were related to copyright protection of digital media. In the past, duplicating artwork was quite complicated and required a high level of expertise for the counterfeit to look like the original. However, in the digital world, this is not true. Today, it is possible for almost anyone to duplicate or manipulate digital data, while not losing data quality. Similar to a painter's signature or monogram, today's artists can copyright their work by hiding their name within the image. Hence, the embedded watermark allows identification of the owner of the work. It is clear that this concept is also applicable to other media, such as digital video and audio. In this scenario, digital watermarking may be useful to set up controlled audio distribution and to provide efficient means for copyright protection, usually in collaboration with international registration bodies.[7]

INFORMATION HIDING TECHNIQUES

Techniques used to hide the information are:

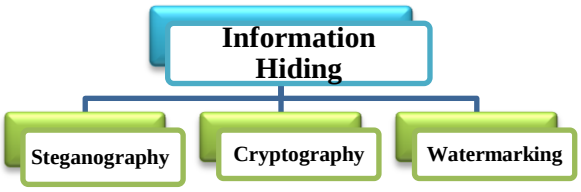

Fig: Classification of Information Hiding

STEGANOGRAPHY (ART OF HIDDEN WRITING)

A term derived from the Greek words “steganos” and

"graphia" (The two words mean "covered" and "writing", respectively).The art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message. The existence of information is secret.

CRYPTOGRAPHY

The conversion of data into a secret code for transmission over a public network. Today, most cryptography is digital, and the original text ("plaintext") is turned into a coded equivalent called "cipher text" via an encryption algorithm. The cipher text is decrypted at the receiving end and turned back into plaintext.

Fig : Cryptography

WATERMARKING

- A distinguishing mark impressed on paper during manufacture; visible when paper is held up to the light (e.g. $ Bill).
- Physical objects can be watermarked using special dyes and inks or during paper manufacturing.

Fig: Watermarked currency

HISTORY OF WATERMARKING

The term "watermark" was probably originated from the German term "wassermarke". Since watermark is of no importance in the creation of the mark, the name is probably given because the marks resemble the effects of water on paper. Papers are invented in China over a thousand years ago. However, the first paper watermark did not appear until 1282, in Italy. By the 18th century, watermarks on paper in Europe and America had been used as trademarks, to record the manufactured date, or to indicate the size of original sheets. Watermarks are commonly used on bills nowadays to avoid counterfeiting.

ADVANCING TO DIGITAL WATERMARKING

In recent times, due to great developments in computer and internet technology, multimedia data i.e. audio, images and video have found wide applications. Digital watermarking is one of the best solutions to prevent illegal copying, modifying and redistributing multimedia data. Encryption of multimedia products prevents an intruder from accessing the contents without a proper decryption key. But once the data is decrypted, it can be duplicated and distributed illegally. To enforce IP rights and to prevent illegal duplication, interpolation and distribution of multimedia data, Digital watermarking is an effective solution. Copyright protection, data authentication, covert communication and content identification can be achieved by Digital watermarking. Digital watermarking is a technique to embed copyright or other information into the underlying data. The embedded data should maintain the quality of the host signal. In order to achieve the copyright protection, the algorithm should meet few basic requirements.

i) Imperceptibility: The watermark should not affect the quality of the original signal, thus it should be invisible/ inaudible to human eyes/ ears.

ii) Robustness**:** The watermarked data should not be removed or eliminated by unauthorized distributors, thus it should be robust to resist common signal processing manipulations such as filtering, compression, filtering with compression.

iii) Capacity**:** the number of bits that can be embedded in one second of the host signal.

iv) Security: The watermark should only be detected by authorized person.

v) Watermark detection should be done without referencing the original signals.

vi) The watermark should be undetectable without prior knowledge of the embedded watermark sequence.

vii) The watermark is directly embedded in the signals, not in a header of the signal.

All these requirements are often contradictory with each other and we need to make a trade-off among them. For example increasing data rate in watermarking system results in quality

degradation of the watermarked signal and decreases the robustness against attacks. Imperceptibility and robustness are the most important properties for many applications. These conflicting requirements pose many challenges to design of robust watermarking.

WATERMARKING ON DIGITAL SIGNALS

Watermarking can also be applied to digital signals.

(a) Images (b) Video (c) Audio

A digital watermark is a pattern of bits inserted into a digitalimage, audio or video file that identifies the file's copyright information (author, rights, etc.). The name "watermark" is derived from the faintly visible marks imprinted on organisational stationery.

In addition, the bits representing the watermark must be scattered throughout the file in such a way that they cannot be identified and manipulated. And finally, a digital watermark must be robust enough to survive changes to the file its embedded in, such as being saved using a lossy compressionalgorithm eg: JPEG.

Satisfying all these requirements is no easy feat, but there are a number of companies offering competing technologies. All of them work by making the watermark appear as noise that is, random data that exists in most digital files anyway.

Digital Watermarking works by concealing information within digital data, such that it cannot be detected without special software with the purpose of making sure the concealed data is present in all copies of the data that are made whether legally or otherwise, regardless of attempts to damage/remove it.

The purpose of digital watermarks is to provide copyright protection for intellectual property that is in digital format.

As seen in above Fig, Alice creates an original image and watermarks it before passing it to Bob. If Bob claims the image and sells copies to other people Alice can extract her watermark from the image proving her copyright to it.

The caveat here is that Alice will only be able to prove her copyright of the image if Bob hasn't managed to modify the image such that the watermark is damaged enough to be undetectable or added his own watermark such that it is impossible to discover which watermark was embedded first.

CHARACTERISTICS OF DIGITAL WATERMARKING

- Invisibility**:** an embedded watermark is not visible.
- Robustness**:** piracy attack or image processing should not affect the embedded watermark.
- Readability**:** A watermark should convey as much information as possible. A watermark should be statistically undetectable. Moreover, retrieval of the digital watermark can be used to identify the ownership and copyright unambiguously.
- Security**:** A watermark should be secret and must be undetectable by an unauthorized user in general. A watermark should only be accessible by authorized parties. This requirement is regarded as a security and the watermark is usually achieved by the use of cryptographic keys. As information security techniques, the details of a digital watermark algorithm must be published to everyone. The owner of the intellectual property image is the only one who holds the private secret keys. A particular watermark signal is related with a special number used embedding and extracting. The special number is kept secretly and is used for confirming legal owners of digital products later. If we lay strong stress on robustness, and then invisibility may be weak. If we put emphasis on invisibility, then vice versa. Therefore, developing robustness watermark with invisibility is an important issue.

HISTORY OF DIGITAL WATERMARKING

- The first watermarking example similar to the digital methods nowadays appeared in 1954. The Muzak Corporation filed a patent for "watermarking" musical Work. An identification Work was inserted in music by intermittently applying a narrow notch filter centred

at 1KHz.

- About 1995, interest in digital watermarking began to mushroom.

WATERMARKING CLASSIFICATION

Digital Watermarking techniques can be classified in a number of ways depending on different parameters. Various types of watermarking techniques are enlisted below.

Robust & Fragile Watermarking:

Robust watermarking is a technique in which modification to the watermarked content will not affect the watermark. As opposed to this, fragile watermarking is a technique in which watermark gets destroyed when watermarked content is modified or tampered with.

Visible & Transparent Watermarking:

Visible watermarks are ones, which are embedded in visual content in such a way that they are visible when the content is viewed. Transparent watermarks are imperceptible and they cannot be detected by just viewing the digital content.

Public & Private Watermarking:

In public watermarking, users of the content are authorized to detect the watermark while in private watermarking the users are not authorized to detect the watermark.

Asymmetric & Symmetric Watermarking:

Asymmetric watermarking (also called asymmetric key watermarking) is a technique where different keys are used for embedding and detecting the watermark. In symmetric watermarking (or symmetric key watermarking) the same keys are used for embedding and detecting watermarks.

Steganographic & Non-Steganographic watermarking:

Steganographic watermarking is the technique where content users are unaware of the presence of a watermark. In nonsteganographic watermarking, the users are aware of the presence of a watermark.

Steganographic watermarking is used in fingerprinting applications while nonsteganographic watermarking techniques can be used to deter piracy.

WATERMARKING TECHNIQUES

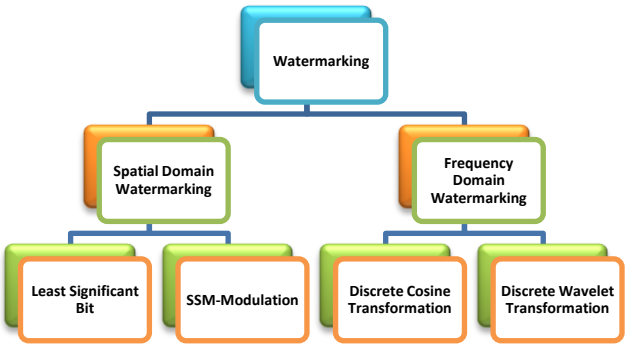

Fig: Watermark Techniques

SPATIAL DOMAIN TECHNIQUES

Some of the Spatial Techniques of watermarking are as follow.

Least-Significant Bit (LSB):

The earliest work of digital image watermarking schemes embeds watermarks in the LSB of the pixels. Given an image with pixels, and each pixel being represented by an 8-bit sequence, the watermarks are embedded in the last (i.e., least significant), bit, of selected pixels of the image. This method is easy to implement and does not generate serious distortion to the image; however, it is not very robust against attacks. For instance, an attacker could simply randomize all LSBs, which effectively destroys the hidden information.

SSM-Modulation-Based Technique:

Spread-spectrum techniques are methods in which energy generated at one or more discrete frequencies is deliberately spread or distributed in time or frequency domains. This is done for a variety of reasons, including the establishment of secure communications, increasing resistance to natural interference and jamming, and to prevent detection. When applied to the context of image watermarking, SSM based watermarking algorithms embed information by linearly combining the host image with a small pseudo noise signal that is modulated by the embedded watermark.

Frequency Domain Techniques:

Compared to spatial-domain methods, frequency-domain methods are more widely applied. The aim is to embed the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Discrete Laguerre Transform (DLT) and the Discrete Hadamard Transform (DHT). The reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients. For example, the HVS is more sensitive to low-frequency coefficients, and less

sensitive to high-frequency coefficients. In other words, low-frequency coefficients are perceptually significant, which means alterations to those components might cause severe distortion to the original image. On the other hand, high-frequency coefficients are considered insignificant; thus, processing techniques, such as compression, tend to remove high-frequency coefficients aggressively. To obtain a balance between imperceptibility and robustness, most algorithms embed watermarks in the midrange frequencies.

Discrete Cosine Transformation (DCT):

DCT like a Fourier Transform, it represents data in terms of frequency space rather than an amplitude space. This is useful because that corresponds more to the way humans perceive light, so that the part that are not perceived can be identified and thrown away. DCT based watermarking techniques are robust compared to spatial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc. DCT domain watermarking can be classified into Global DCT watermarking and Block based DCT watermarking. Embedding in the perceptually significant portion of the image has its own advantages because most compression schemes remove the perceptually insignificant portion of the image.

Discrete Wavelet Transformation (DWT):

The Discrete Wavelet Transform (DWT) is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelets have their energy concentrated in time and are well suited for the analysis of transient, time-varying signals. Since most of the real life signals encountered are time varying in nature, the Wavelet Transform suits many applications very well.

ANALYSIS OF ROBUSTNESS

The similarity measurement between original watermark and extracted watermark is obtained through Normalized Correlation (NC) coefficient and Accuracy Rate (AR).

Normalized Correlation (NC):

The Normalized correlation Coordinate (NCC) computes the similarity measurement of original watermark and extracted watermark, which is defined as

$$NC = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} W(i,j) * W'(i,j)}{\sum_{i=1}^{N}\sum_{j=1}^{N} W^2(i,j)}$$

Where N×N is the size of watermark, W(i,j) and W'(i,j) represents the watermark and recovered watermark images respectively.

Accuracy Rate (AR):

The Accuracy Rate (AR) is used to measure the difference between the original watermark and the recovered one. *AR* is computes as follows:

AR= CP/ NP

Where *NP* is the number of pixels in the original watermark and *CP* is the number of correct pixels obtained by comparing the pixels of the original watermark to the corresponding ones of the recovered watermark.

APPLICATIONS OF WATERMARKING

Security:

In the field of data security, watermarks may be used for certification, authentication, and conditional access.

Certification:

It is an important issue for official documents, such as identity cards or passports. Digital watermarking allows to mutually link information on the documents. That means some information is written twice on the document, for instance, the name of a passport owner is normally printed in clear text and is also hidden as an invisible watermark in the photo of the owner. If anyone would intend to duplicate the passport by replacing the photo, it would be possible to detect the change by scanning the passport and verifying the name hidden in the photo does not match any more the name printed on the passport.

Authentication:

The goal of this application is to detect alterations and modifications in an image. Suppose we have picture of a car that has been protected with a watermarking technology. And if, the same picture is shown but with a small modification, say, the numbers on the license plate has been changed. Then after running the watermark detection program on the tampered photo, the tampered areas will be indicated in different colour and we can clearly say that the detected area corresponds to the modifications applied to the original photo.

Conditional access:

For example conditional access to confidential data on CD-ROMs may be provided using digital watermarking technology. The concept consists of inserting a watermark into the CD label. In order to read and decrypt the data stored on the CD, the watermark has to be read since it contains information needed for decryption. If someone copies the CD, he will not be able to read the data in clear-text since he does not have the required watermark.

Copyright Protection:

Copyright protection inserts copyright information into the digital object without the loss of quality. Whenever the copyright of a digital object is in question, this information is

extracted to identify the rightful owner. It is also possible to encode the identity of the original buyer along with the identity of the copyright holder, which allows tracing of any unauthorized copies.

Copy protection:

Copy protection attempts to find ways, which limits the access to copyrighted material and/or inhibit the copy process itself. Examples of copy protection include encrypted digital TV broadcast, access controls to copyrighted software through the use of license servers and technical copy protection mechanisms on the media. A recent example is the copy protection mechanism on DVDs. However, copy protection is very difficult to achieve in open systems, as recent incidents (like the DVD hack) show.

Other applications:

Digital watermarks can also serve as invisible labels and content links. For example, photo development laboratories may insert a watermark into the picture to link the print to its negative. This way is very simple to find the negative for a given print. All one has to do is scan the print and extracted the information about the negative. In order to distinguish between different copies, different watermarks are embedded into different copies of the same document. These marks are also called "digital fingerprints".

Fingerprinting :

In applications where multimedia content is electronically distributed over a network, the content owner would like to discourage unauthorized duplication and distribution by embedding a distinct watermark (or a fingerprint) in each copy of the data.

Fraud and Tamper Detection:

When multimedia content is used for legal purposes, medical applications, news reporting, and commercial transactions, it is important to ensure that the content was originated from a specific source and that it had not been changed, manipulated.

CONCLUSION

Thus we conclude that digital watermarking can have many applications in the range of security, certification, authentication,conditional access,copyright protection, copy protection, telemedicine,criminal photograph authentication, Fraud and Tamper Detection, Fingerprinting etc. So that digital watermarking can be good asset to be used in the mentioned area effectively and efficiently to portrait data protection.

REFERENCES

[1] M.Swanson, B. Zhu, A. Tewfik, and L. Boney, "Robust Audio watermarking using perceptual masking" Signal Process., Special Issue on Watermaking, 1997, pp. 337-3555.

[2] L. Boney, A. Tewfik, and K. Hamdy, "Digital watermarks For audio signals," in IEEE Proc. Multimedia, 1996, pp-473-480.

[3] M. Swanson, M. Kobayashi, and A. Tewfik, "Multimedia Data-embedding and watermarking strategies," Proc. IEEE Vol. 86, pp. 1064-1087, June 1998.

[4] Christine I. Podilchuk and Edward J. Delp, "Digital Watermarking: Algorithms and Applications", IEEE SIGNAL PROCESSING MAGAZINE.

[5] Keshav S Rawat, Dheerendra S Tomar, "Digital Watermarking schemes for authorization Against copying Or piracy of color images" in IEEE, Vol. 1 No. 4 295-300

[6] Anthony T.S.Ho, Jun Shen, Soon Hie Tan "A Robust Digital Image-in-Image Watermarking Algorithm Using The Fast Hadamard Transform" proceedings of SPIE Vol. 4793(2003)© 2003 SPIE · 0277-786X/03/$15.00

[7] http://www.alpvision.com/watermarking.html.