A SURVEY OF WATERMARKING PROCESS

S.Dhanalakshmi[#1] , Dr.T.Ravichandran[*2]
[#] *Department of Computer Science & Engineering, SNS College of Technology, Coimbatore-641 035, India* [1]
[*] *Department of Computer Science & Engineering, Hindusthan Institute of Technology, Coimbatore-641 042, India* [2]
[1]dhana261978@yahoo.com

Abstract

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of computer-aided information hiding in a carrier signal; the hidden information should, but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote and for authentication. A digital image is a representation of a two-dimensional image as a finite set of digital values, called picture elements or pixels Pixel values typically represent gray levels, colours, heights, opacities etc. Selection for histograms with multimodal feature.

Keywords: ***Information hiding, Digital watermarking, Digital Image Processing, Attacking process***

I. INTRODUCTION

1. INFORMATION HIDING

This technique is used to hide the information, and then the information hiding is classified into Steganography, cryptography and watermarking.

(a) 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.

(b) 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.
Encryption Decryption
Plaintext → cipher text → Plaintext

(c) Watermarking is embedding a hidden message within the original data “host image”. Watermarking is used for Proof of Ownership (copyrights and IP protection), Copying Prevention, Broadcast Monitoring, Authentication, and Data Hiding. A hidden watermark message is inserted into a host image such that the hidden message will survive intended or Unintended attacks. Fig.1. shows the process of adding the watermarked message. Watermark message M(x,y) Is the Random or pseudo random signal, then the binary value is represented by {-1, +1} or {-1, 0, +1} and other signals are used. Then the Watermark message is added linearly as $W(x, y) = I(x, y) + kM(x, y)$

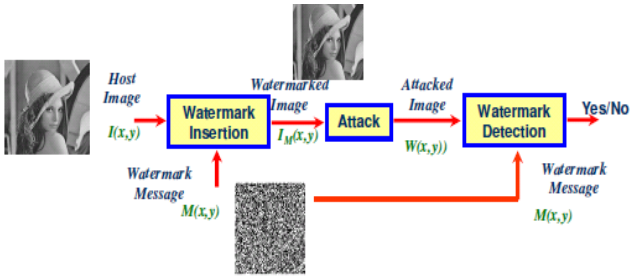

Fig.1. Watermarked message

It is based on the concept of 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.

2. DIGITAL WATERMARKING

Watermarking can also be applied to digital signals! Digital watermark, a pattern of bits inserted into a digital image, audio, video or text file that identifies the file's copyright information (author, rights, etc.). Fig.2. shows the representation of watermarked digital signals. The name comes from the faintly visible watermarks imprinted on stationary that identify the manufacturer of the stationery. The purpose of digital watermarks is to provide copyright protection for intellectual property that's in digital format. 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 embed of information should be such that it should not create any visible effect in the image by changing the value of the pixels [10].The example below shows that digital watermarking allows hiding information in a totally invisible manner. The real image is on the left; the watermarked image is on the right and contains the name of the writer a watermark is a

clear image in paper that can be seen in many shades of lightness/darkness when viewed by transmitted light affected by thickness variations in the paper.

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

Fig.2. Representation of digital signals

A watermark well-established in a data file ensures a method of authentication of data which combines aspects of data hashing and digital watermarking. Both are useful for fiddle detection, though each has its own advantages and disadvantages. Digital watermarking is the process of possibly irreversibly embedding information. A subscriber, with knowledge of the watermark and how it is recovered, can determine changes in a file, lossy compression.

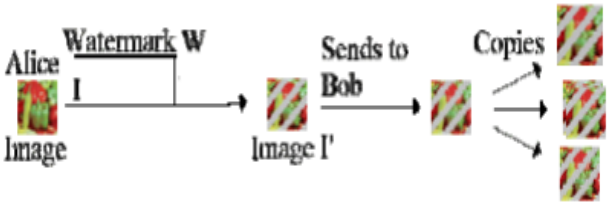

Fig.3. Copyright Protection

A disadvantage of digital watermarking is that a subscriber cannot significantly alter some files without sacrificing the quality or utility of the data. Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where pirates attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video or intentionally adding noise. Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In robust digital watermarking able to produce the watermark correctly, even the modifications were strong. Fig.3. shows the 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.

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.

3. WATERMARKING LIFE-CYCLE PHASES

The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital

watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the *host* signal. A watermarking system is usually divided into three distinct

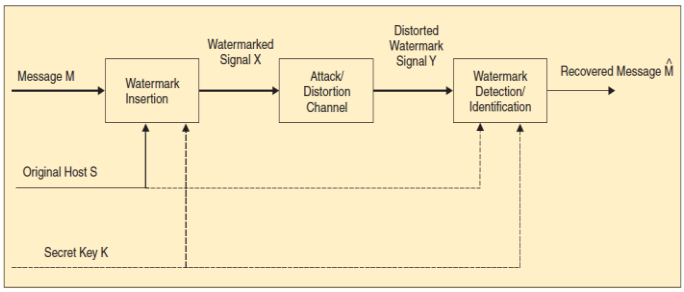

Fig.4. Block Diagram of Watermarking System

Steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and Produces a watermarked signal. Fig.5. shows the embedding system. Inputs to the scheme are the watermark, the cover data and an optional public or secret key. The outputs are watermarked data. The key is used to enforce security.

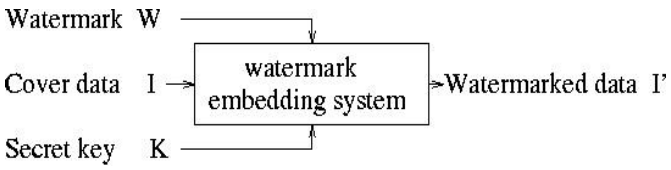

Fig.5. Embedding

Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an *attack.* While the modification may not be malicious, the term attack arises from copyright protection application, where third parties may attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video or intentionally adding noise. Few possible attacks in the life cycle process.*Robustnes*s *attacks*: Which are intended to remove the watermark such as…JPEG compression, cropping, etc.*Presentation Attacks:* Under watermark detection failure they come into play. Geometric transformation, rotation, scaling, translation, and change aspect ratio, affine transformation etc.*Counterfeiting attacks:* Rendering the original image, generate fake original. Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In *robust* digital watermarking applications, the extraction algorithm should be able to produce the watermark

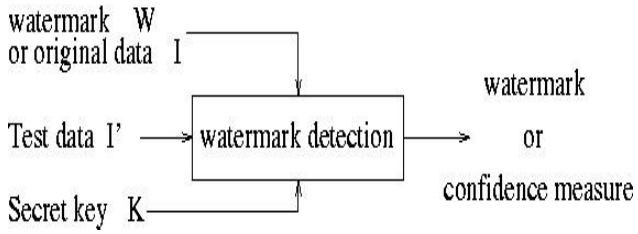

Fig.6. Extraction

Correctly, even if the modifications were strong. In fragile digital watermarking, the extraction algorithm should fail if any change is made to the signal. Fig.6. shows the Extraction process. Inputs to the scheme are the watermarked data, the secret or public key and, depending on the method, the original data and/or the original watermark. The output is the recovered watermarked W or some kind of confidence measure indicating how likely it is for the given watermark at the input to be present in the data under inspection.

4. WATERMARKING CLASSIFICATION

A digital watermark is called robust with respect to transformations if the embedded information may be detected reliably from the marked signal, even if degraded by any number of transformations. Typical image degradations are JPEG compression, rotation, cropping, additive noise, and quantization. For video content, temporal modifications and MPEG compression often are added to this list. A digital watermark is called imperceptible if the watermarked content is perceptually equivalent to the original, unwatermarked content. In general, it is easy to create robust watermarks or imperceptible watermarks, but the creation of robust and imperceptible watermarks has proven to be quite challenging. Robust imperceptible watermarks have been proposed as tool for the protection of digital content, for example as an embedded no-copy-allowed flag in professional video content.

Digital watermarking techniques may be classified in several ways.

(i) Robustness - A digital watermark is called fragile if it fails to be detectable after the slightest modification. Fragile watermarks are commonly used for tamper detection (integrity proof). Modifications to an original work that clearly are notice able, commonly are not referred to as watermarks, but as generalized barcodes. A digital watermark is called semi-fragile if it resists benign transformations, but

fails detection after malignant transformations. Semi-fragile watermarks commonly are used to detect malignant transformations. A digital watermark is called *robust* if it resists a designated class of transformations. Robust watermarks may be used in copy protection applications to carry copy and no access control information.

(ii) Perceptibility - A digital watermark is called imperceptible if the original cover signal and the marked signal are perceptually indistinguishable. A digital watermark is called perceptible if its presence in the marked signal is noticeable. NB. A digital watermark that is perceptual, on the other hand, is imperceptible. It works context-sensitive/adaptive.

(iii) Capacity - The length of the embedded message determines two different main classes of digital watermarking schemes:

- The message is conceptually zero-bit long and the system is designed in order to detect the presence or the absence of the watermark in the marked object. This kind of watermarking scheme is usually referred to as zero-bit or presence watermarking schemes. Sometimes, this type of watermarking scheme is called 1-bit watermark, because a 1 denotes the presence (and a 0 the absence) of a watermark.
- The message is a n-bit-long stream ($m = m_1 \dots m_n,\ n \in \mathbb{N}$,with $n = |m|$) or $M = \{0,1\}^n$ and is modulated in the watermark. These kinds of schemes usually are referred to as multiple-bit watermarking or non-zero bit watermarking scheme.

4.1 Characteristics of Digital Watermarking

*1) Invisibility***:** an embedded watermark is not visible.

2) Robustness: piracy attack or image processing should not affect the embedded watermark.

3) 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.

4) 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.

5. CLASSIFICATION OF DIGITAL WATERMARKING

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
- Visible & Invisible Watermarking
- Asymmetric & Symmetric Watermarking
- Public & Private Watermarking
- Steganographic & Non-steganographic Watermarking

1) 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.

2) Visible & Invisible Watermarking
Visible watermarks are ones, which are embedded in visual content in such a way that they are visible when the content is viewed. Visible watermarking is used to indicate ownership and for copyright protection. Invisible watermarks are imperceptible and they cannot be detected by just viewing the digital content. . It is used as evidence of ownership and to detect misappropriated images.

Dual watermarking is the combination of visible and invisible watermark. An invisible watermark is used as a backup for the visible watermark.

3) 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.

4) 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.

5) Steganographic &Non-Steganographic watermarking
Steganographic watermarking is the technique where content users are unaware of the presence of a watermark. In non steganographic watermarking, the users are aware of the presence of a watermark. Steganographic watermarking is used in fingerprinting applications while non Steganographic watermarking techniques can be used to deter piracy.

6. TECHNIQUES IN DIGITAL WATERMARKING

Watermarking Techniques can be classified into spatial domain and frequency (transform) domain watermarking.

1) Spatial Domain watermarking - The spatial domain is the normal image space, in which a change in position in I directly projects to a change in position in space. Distances in I (in pixels) correspond to real distances (*e.g.* in meters) in space. This concept is used most often when discussing the frequency with which image values change, that is, over how many pixels does a cycle of periodically repeating intensity variations occur[4]. One would refer to the number of pixels over which a pattern repeats (its periodicity) in the spatial domain. Here we use Least Significant bit (LSB) method and SSM modulation techniques.

1.1) 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. One of the simplest technique in digital watermarking is in spatial domain using the two dimensional array of pixels in the container image to hold hidden data using the least significant bits (LSB) method. Note that the human eyes are not very attuned to small variance in color and therefore processing of small difference in the LSB will not noticeable.
The steps to embed watermark image are given below.
Steps of Least Significant bit

1) Convert RGB image to gray scale image.
2) Make double precision for image.
3) Shift most significant bits to low significant bits of watermark image.
4) Make least significant bits of host image to zero
5) Add shifted version (step 3) of watermarked image to modified (step 4) host image.

1.2)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.

2) Frequency-domain Techniques- 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.

2.1) 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.

2.2 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.

7. APPLICATIONS OF WATERMARKING

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

2) 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.

3) 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.

4) 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".

8. CONCLUSION

Digital Image Watermarking can protect image, video, audio from unauthorized person, noise; copyright etc. the technology of information hiding has been widely applied to fields of copyright protection (digital watermarking), communication, and so forth. Digital watermarking has rapidly advanced from theory to practice. This report focuses on how watermarking techniques are advantageous over stenography, cryptography and also focuses on different types and domains of digital watermarking techniques. A common application requirement for the watermarks is that they resist attacks that would remove it.

REFERENCES

[1] 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.

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

[3] M. Swanson, B. Zhu, A. Tewfik, and L. Boney, "Robust audio watermarking using perceptual masking, "Signal Process., Special Issue on Watermarking, 1997, pp. 337-355.

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

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

[6] Christine I. Podilchuk and Edward J. Delp, "Digital Watermarking: Algorithms and Applications",IEEE SIGNAL PROCESSING MAGAZINE, 1053-5888/01/$10.00©2001IEEE.

[7] 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.

[8] 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.

[9] M. Swanson, B. Zhu, A. Tewfik, and L. Boney, "Robust audio watermarking using perceptual masking," Signal Process., Special Issue on Watermarking, 1997, pp. 337-355.

[10] 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 .

[11] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, and M. Miller, "Rotation, scale, and translation resilient public watermarking for images," IEEE Trans. Image Process., vol. 10, no. 5, pp. 767-782, May 2001.

[12] Xiang-Gen Xia, Charles G. Boncelet and Gonzalo R. Arce. "Wavelet Transform based watermark for digital images."Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 1971.

