International Journal of Trend in Research and Development, Volume 3(2), ISSN: 2394-9333
www.ijtrd.com

A Survey of Watermarking Techniques

S.J.Basha,
Professor, Department of Electronics & Telecom Engineering,
Shree Rayeshwar Institute of Engineering & Information Technology, Goa, India

Abstract: Watermarks have been introduced in the 13th century in Italy. Initially watermarks were in the form of plain paper and paper bills. However, the digital watermarking field was developed only during the last 15 years and it is now being used for many different applications. Due to latest technology the watermarks are clearer and they are used in many areas such as most of the world's bank notes. Same as wax seal, a watermark was an emblem of prestige, and also guarded the security of personal correspondence. Today this watermarking technology becomes one of the research areas in many fields such as communication, signal processing and Image processing.

Many persons may be not willing to share their information over the net due to lack of security. Their information can be easily manipulated and shared without the consent of the owner. The Digital watermarking t3echnique gives the solution for this problem.

Keywords: *Watermarking, Authentication, copyright protection, Fragile, Robustness, Spatial Domain.*

I. INTRODUCTION

A. Reasons to choose Image Watermarking for Research:

There are many kinds of water marking such as audio and video. But Image watermarking becomes most popular due to the following reasons.

- Test images are readily available.
- It is easy to embed watermark due to much redundant information and
- Easy to upgrade video watermarking using any successful image watermarking algorithm [13].

B. Watermarking

Watermarking is a technique used to hide data or identifying information within digital multi media. Watermarking is a process of embedding information into the digital image, video or audio, to show the ownership or authentication. [11]

C. Digital watermarking

Digital watermarking is a field that refers to the process of embedding digital data directly onto multimedia objects such that it can be detected or extracted later to make an assertion about the object. Digital watermarking is a technology that embeds information, in machine-readable form, within the content of a digital media file (image, audio, or video). The information is encoded through subtle changes to the image, audio, or video.

D. Watermark

A watermark is A pattern of bits inserted into a digital image, audio or video file that identifies the file's copyright information (author, rights, etc.). Watermark can be defined as the data in the form of digits embedded in multimedia objects so that the watermark can be detected or extracted easily at later stages. It can be treated as a secondary image that is overlaid on the host image. It is a digital signature to show the authenticity or ownership. [2]

E. Digital Watermark

A Digital watermark is a digital signal or pattern of bits inserted into a digital image. Since this signal or pattern of bits is present in each unaltered copy of the original image.

II. WATERMARKING ELEMENTS

A watermarking system can be viewed as a communication system consisting of three main elements shown in figure 1

a. Watermark embedder.
b. Communication Channel
c. Watermark detector.

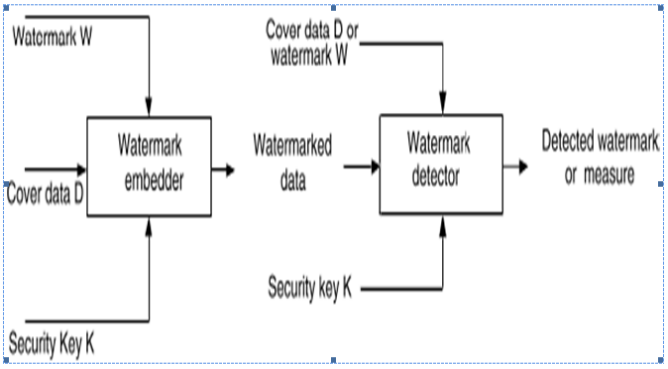


Figure 1: A typical watermarking system

The inputs to the watermark embedder are the watermark, the cover media data and the embedding security key. The watermark can be a number sequence, a binary bit sequence or may be an image. The key is used to enhance the security of the whole system .The output of the watermark embedder is the watermarked data.

Watermark information is embedded into the signal itself, instead of being placed in the header of a file so that it is extractable by the detector. [14][15]

III. WATERMARKING FEATURES

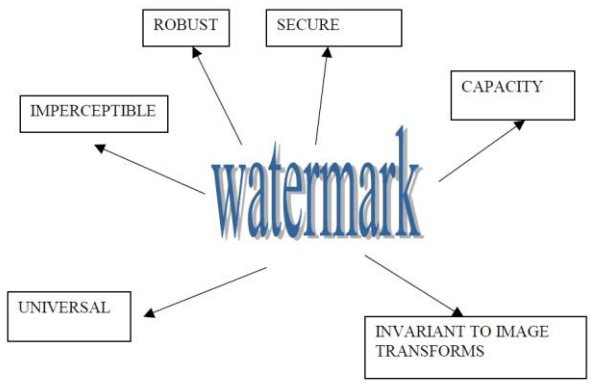


Figure 2: Watermarking Features

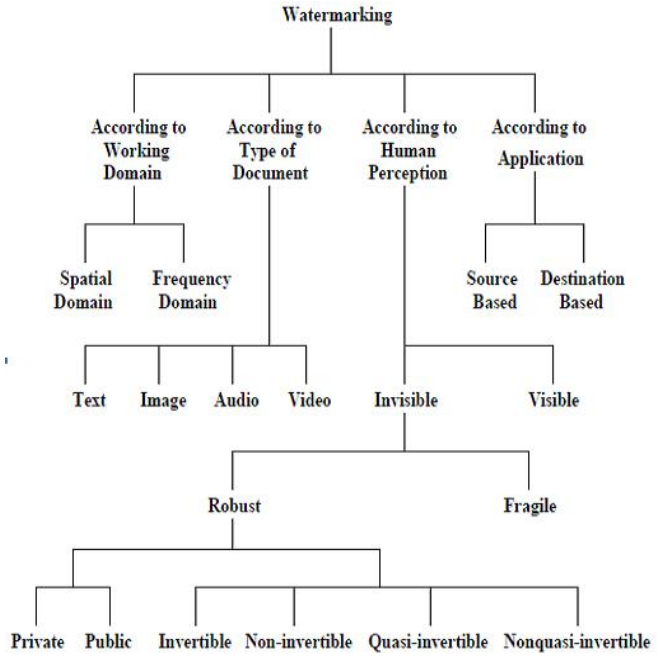
Ideal properties of a digital watermark are

- **Universality:** The water mark should be universal i.e. The same watermark or slightly modified watermark

algorithm should be applied for all considered digital multimedia data.[13]

- **Invisibility:** An embedded watermark is not visible. Invisible watermark is hidden in the content. It can be detected by an authorized agency only. [7]
- **C. Robustness:** Watermark must be difficult or impossible to remove. [9]
- **D. Security:** Should be secure
- **Capacity:** Should have high capacity. Watermarking capacity normally refers to the amount of information that can be embedded into a host signal. [7]
- Watermark extraction should be fairly simple. Otherwise, the detection process requires too much time or computation.
- Watermark detection should be accurate.
- Numerous watermarks can be produced. Otherwise, only a limited number of images may be marked.
- The watermark should be able to determine the true owner of the image.

IV. WATERMARKING CLASSIFICATION



Watermarking techniques are classified as follows [16]:

A. According to Working Domain: Watermarking techniques classified as

- Spatial domain,
- Frequency/transform domain.[11]

1. Spatial-domain techniques: embeds the watermarks by directly changing pixel values of host images. It is difficult for spatial-domain watermarks to survive under attacks such as lossy compression and low-pass filtering. Also the information can be embedded in spatial domain is very limited. Ex: spatial-domain algorithms include Least Significant Bit (LSB) Modification, Patchwork, Texture Block Coding, etc. The most serious drawback of spatial-domain technologies is limited robustness.

2. 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), the reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better.

Table 1: Comparison between working domain Watermarking Techniques [9]

Parameter	Spatial Domain	Frequency Domain
Cost of Computation	Low	High
Robustness	Fragile	More Robust
Perceptual Quality	High Control	Low Control
Capacity	High (Depend on the size of the image)	Low
Application ex	Authentication	Copy Rights

B. According to Type of document: Watermarking techniques classified as:

- Image Watermarking
- Video Watermarking
- Audio Watermarking
- Text Video Watermarking

C. According to the human perception, three categories are there:

Visible Watermarking, Invisible Robust Watermarking, Invisible Fragile Watermarking

1. Visible watermarking: Visible watermarks are an extension of the concept of logos. Such watermarks are applicable to images only. These logos are inlaid into the image but they are transparent. Such watermarks cannot be removed by cropping the centre part of the image. An example: a logo placed by TV networks.

2. Invisible watermarking: Invisible watermarks cannot be seen with the naked eye. Invisible watermark is hidden in the content. It can be detected by an owner only. They are used for content and author authentication [2]

Fragile watermark or Tamper-proof watermarks. Fragile watermark are also known as tamper-proof watermarks. Such watermark are destroyed by data manipulation or in other words it is a watermarks designed to be destroyed by any form of copying or encoding other than a bit-for-bit digital copy. Absence of the watermark indicates that a copy has been made. In fragile watermark, the watermark is hidden within the host signal and it is destroyed as soon as the watermarked signal undergoes any manipulation. When a fragile watermark is present in a signal, we can infer, with a high probability, that the signal has not been altered. [9]

D. According to type of application the watermarking technique is classified as

- Source-based and
- Application-based

E. According to Extractor:

- Blind
- Nonblind

Depends upon how the watermark is detected and extracted : Blind watermarking : watermark detection and extraction do not depend on the availability of original image. The drawback

is when the watermarked image is seriously destroyed; watermark detection will become very difficult.

Nonblind watermarking: Watermark detected only when there is a copy of original image. It guarantees better robustness but may lead to multiple claims of ownerships. [11]

V. WATERMARKING ATTACKS

Attack is any process that tampers or misleads the watermark detector A watermarked object may be subjected to certain manipulation processes before it reaches the receiver. The performance of a watermarking algorithm quality may be degraded due to these attacks reflects [2]
Basically there are five types of Attacks:

- Removal and interference Attacks
- Geometric Attacks
- Cryptographic Attacks
- Protocol Attacks.
- Estimation based Attacks.

A. Removal and interference attacks

Removal attacks may remove the watermark data from the watermarked object. Such attacks exploit the fact that the watermark is usually an additive noise signal present in the host signal. Interference attacks add additional noise to the watermarked object. Some of the examples of these attacks are Lossy compression, quantization, collusion, denoising,, averaging, and noise storm.

B. Geometric attacks

Geometric attacks manipulate the watermarked object in such a way that the detector cannot find the watermark data. They are specific to images and videos. Some of the examples includes affine transformations such as rotation, translation, and scaling. mosaic attack.

C. Cryptographic attacks

Cryptographic attacks deal with the cracking of the security. For example, finding the secret watermarking key using exhaustive brute force method. is a cryptographic attack, oracle attack . which creates a non-watermarked signal in case a watermark detector device is found available.

D. Protocol attacks

These attacks exploit the loopholes in the watermarking concept. Example of such attack is the IBM embeds one or several additional watermarks such that it is unclear which the watermark of the original owner was.

E. Estimation-Based Attacks

The concept of this attacks lies in the estimation of the embedded watermark, used with some prior knowledge of the signals‘ statistics. [12]

VI. WATERMARKING ADVANTAGES

Advantages of Watermarking over other techniques (such as cryptography) are

- It is invisible and does not affect the properties of the digital data.
- Watermarks become fused with the actual bits of the work, and they do not get removed when the work is displayed, copied or during format changes.
- They undergo the same transformation and sometimes the extracted mark can be used to learn about the history of transformations that the work has undergone.

VII. WATERMARKING APPLICATIONS

Classification of Digital Watermarking Applications

A. For Copyright Protection

The objective is to control access to and prevent illegal copying of copyrighted content. The metadata in this case contains information about the copyright owner. It is imperceptibly embedded as a watermark in the cover work to be protected. [1]

B. For Image and content authentication

The intent is to detect modifications to the data. The characteristics of the image, such as its edges, are embedded and compared with the current images for differences. [1] ,[19]

C. For Fingerprints

The fingerprint embeds information about the legal receiver in the image. This involves embedding a different watermark into each distributed image and allows the owner to locate and monitor pirated images that are illegally obtained. [1], [18].

D. For Broadcast Monitoring

The first applications for watermarking were broadcast monitoring. It is often crucially important that we are able to track when a specific video is being broadcast by a TV station. This is important to advertising agencies that want to ensure that their commercials are getting the air time they paid for. Watermarking can be used for this purpose. Information used to identify individual videos could be embedded in the videos themselves using watermarking, making broadcast monitoring easier. [2]

E. For System Enhancement

Digital watermarking can also be used to convey side-channel information with the purpose of enhancing functionality of the system or adding value to the content it is embedded in.[10]

F. For Medical applications

The medical reports play a very important role in the treatment offered to the patient. In medical field patient names can be printed on the X-ray reports and MRI scans using visible watermarking [1] ,

VIII. WATERMARKING CHALLENGES

Watermarking research has many technical challenges. The robustness and imperceptibility trade-off makes the research quite interesting. To attain imperceptibility, the watermark should be added to the high frequency components of the original signal. On the other hand, for robustness the watermark can be added to the low frequency components only. Thus, the watermarking scheme can be successful if the low frequency components of the original signal are used as the host for watermark insertion. In this section, we discuss the various technical issues related to watermarking, such as properties of the human visual system and spread-spectrum communication, which are commonly exploited for making watermarking schemes successful. [1], [17]

CONCLUSIONS

In this paper the survey of watermarking technique is given starting from its evolution to its challenges and limitations covering watermarking technique, types, attacks, advantages, and applications. This paper will help the researcher to start a research in this topic.

References

[1] http:// www.ijser.org
[2] http:// www.ijset.com
[3] http:// web.iiit.ac.in
[4] http:// ijsetr.org
[5] http:// www.ejournal.aessangli.in
[6] http:// www.euroasiapub.org
[7] http:// www.coursehero.com
[8] http:// www.cdt.info
[9] http:// Wob.iai.uni-bonn.de
[10] http:// www.cse.fau.edu
[11] http:// www.ee.sunysb.edu
[12] http:// www.thecho.in
[13] Gaurav Jain, Digital Image watermarking, Student, IIIT .Hyderabad.
[14] Mahmoud El-Gayyar, Watermarking Techniques, 06 Spatial Domain, Digital Rights Seminar, Media Informatics, University of Bonn, Germany. [15]Mahmoud El-Gayyar,Watermarking Techniques Spatial Domain ,Digital
[15] Saraju P. Mohanty,Digital Watermarking : A Tutorial Review: Digital Watermarking.
[16] Manpreet Kaur ,Sonika Jindal ,Sunny Behal,A Study Of Digital Image Watermarking,2012, IJREAS, Volume 2, Issue 2 (February), ISSN: 2249-3905.
[17] Conference on Industrial Informatics (INDIN 2005). Er-Hsien Fu, Literature Survey on Digital Image Watermarking,98, EE381K-Multidimensional Signal Processing. Rights Seminar.
[18] Yashu Pradhan ,Digital watermarking: Tool for Image Authenticity,Research Scholar, CMJ University, Shillong
[19] Mr. Gaurav N Mehta, Mr. Yash Kshirsagar, Mr. Amish Tankariya, 2012, Digital Image Watermarking: A Review, ijset, Volume No.1, Issue No.2 pg: 169-174.
[20] Kirtika Goel, Akhil Kaushik, Achal Agarwal, Sakshi Goel, 2012 ,IJSRET, Volume 1, Issue 5 pp, 120-123.
[21] Morgan Kaufmann Publisher ,Privacy Principles for Digital Watermarking 2008 – Version 1.0 , San Francisco, CA, USA.
[22] Vidyasagar M. Potdar, Song Han, Elizabeth Chang, "A Survey of Digital Image. Watermarking Techniques, 3rd International.
[23] Melinos Averkiou, Digital Watermarking Article © Neerav Bhatt .