RESEARCH ARTICLE OPEN ACCESS

Relative Analysis of Indiscernible Text Digital Watermarking

Lakshman JI [1], Smeer Awasthi [2]
M.Tech [1], Assistant Professor [2]
Department of Computer Science and Engineering
Bansal Institute Of Engineering & Technology Lucknow
India

ABSTRACT

Multimedia security is extremely significant concern for the internet technology because of the ease of the duplication, distribution and manipulation of the multimedia data. The digital watermarking is a field of information hiding which hide the crucial information in the original data for protection illegal duplication and distribution of multimedia data. The image watermarking techniques may divide on the basis of domain. Today, in the market, the protection of copyrighted material has become a new challenge, as the importance of the internet is increasing day by day in information acquisition. For protection of copyright material watermarking is introduced. Digital Watermarking is the process to authenticate user files by embedding and hiding digital code behind an image, text, audio and video file With the rapid development and wide use of Internet, information transmission faces a big challenge of security. Digital watermarking is a technique of data hiding, which provide security of data. The process of embedding additional data along with the digital audio, images and video is called digital watermarking. This paper classified various watermarking techniques and there comparisons. It starts with overview, classification, features, techniques, application and performance measuring of watermarking and a comparative analysis of watermarking techniques.

Keywords:- Digital watermarking

I. INTRODUCTION

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should,[1] 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 authentication.

Watermarking is a technique used to hide data or identifying information within digital multimedia. Our discussion will focus primarily on the watermarking of digital images, though digital video, audio, and documents are also routinely watermarked. Digital watermarking is becoming popular, especially for adding undetectable identifying marks, such as author or copyright information. The digital watermarking process embeds a signal into the media without significantly degrading its visual quality. Digital watermarking is a process to embed some information called watermark into different kinds of media called Cover Work. Digital watermarking is used to hide the information inside a signal, which cannot be easily extracted by the third party. Its widely used application is copyright protection of digital information. Watermark is perceptible or imperceptible identification code which uniquely identifies ownership of an image . It is permanently embedded into the host image. The embedded watermark may be pseudo-random binary sequence, chaotic sequence, spread spectrum sequence or binary/gray scale image. Such watermarks are used for objective detection using correlation measures. Binary or gray image is meaningful and is used for subjective detection. The examples of this type of watermark include date, serial number, logo or any other kind of identification mark

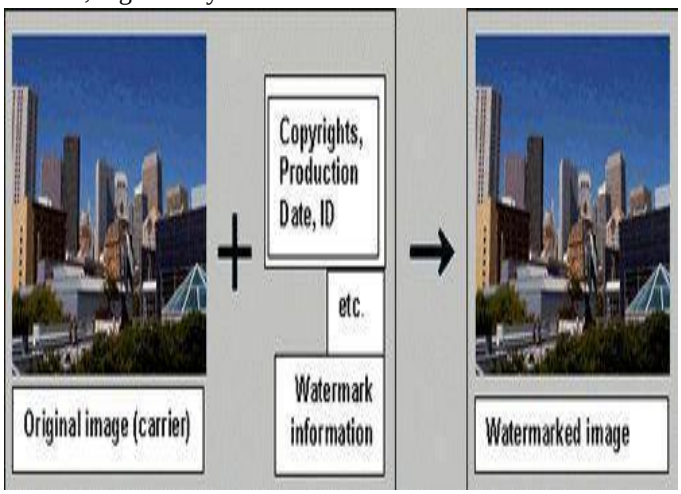


Figure 1: Original image with watermarked image

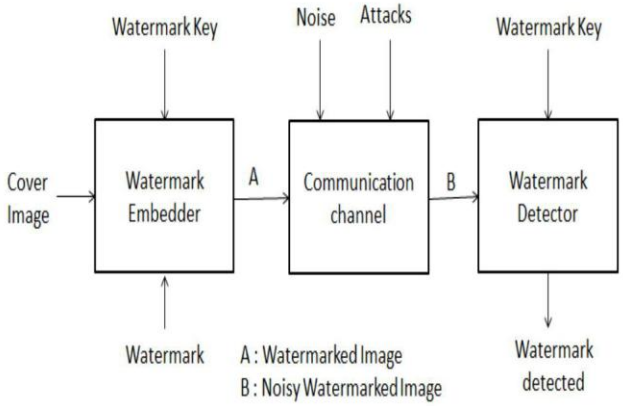


Fig 1.2 Digital Watermarking System History

The term "Digital Watermark" was coined by Andrew Tirkel and Charles Osborne in December 1992. The first successful embedding and extraction of a steganographic spread spectrum watermark was demonstrated in 1993 by Andrew Tirkel, Charles Osborne and Gerard Rankin. Watermarks are identification marks produced during the paper making process. The first watermarks appeared in Italy during the 13th century, but their use rapidly spread across Europe. They were used as a means to identify the papermaker or the trade guild that manufactured the paper. The marks often were created by a wire sewn onto the paper

Applications.

There are various applications of watermarking which are listed below

A. Copyright Protection

When a new work is produced, copyright information can be inserted as a watermark. In case of dispute of ownership, this watermark can provide evidence.

B. Broadcast Monitoring

This application is used to monitor unauthorized broadcast station. It can verify whether the content is really broadcasted or not.

C. Authentication and Integrity Verification

Content authentication is able to detect any change in digital content. This can be achieved through the use of fragile or semi-fragile watermark which has low robustness to modification in an image.

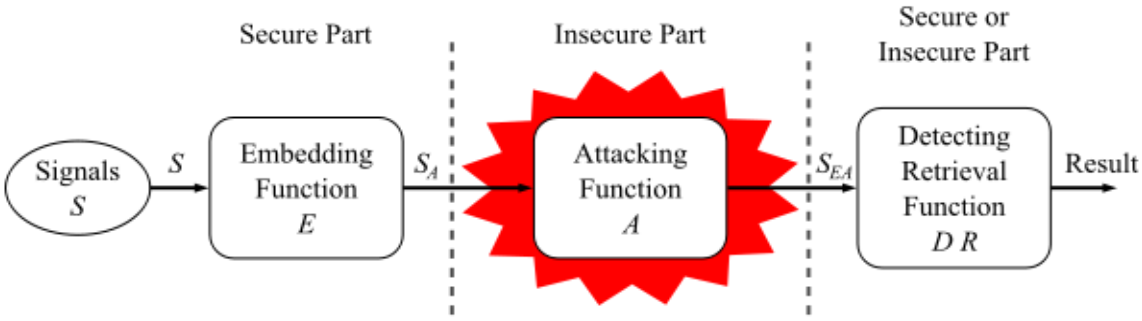
D. Fingerprinting

Fingerprints are unique to the owner of digital content and used to tell when an illegal copy appeared

Digital 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 steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.

General digital watermark life-cycle phases with embedding-, attacking-, and detection and retrieval functions



II. DIGITAL WATERMARKING

Digital watermarking is that technology which is used for protection of digital media such as video, audio and image In this technique, watermark i.e. secret information is embedded in digital media using some algorithms and the watermarked media is processed. After that, watermark i.e. secret information is extracted using the particular algorithm. This technique, i.e. digital watermarking is used for authentication of data and protection of . Here two phases are used which are embedding of the watermark and detection and extraction of watermark

Qualities of Digital Watermarking

There are some basic qualities, a digital watermark must possess:

- *Robustness:* It simply means ability to survive. When we transmit a watermarked data, then there are various attacks on that and that information may undergo different types of operations. So in these conditions, watermark must not degrade its quality

- *Imperceptibility:* This simply means that watermark must be such that it cannot be observed by human eyes. It must be such that it can only be accessed by particular operations on watermarked data.

- *Security:* It means that, the watermark must be such that only authorized users can access it. If any user has no embedding information, he must be unable to detect the watermark. This is termed as security of watermark.

- *Capacity:* It simply means that how much amount of information we are able to embed in the original image. Watermark capacity simply refers the secret information amount present in watermarked image.

- *Computational Cost:* It depends on the method which is used for watermarking. If the watermarking method is more complex, then it contains complex algorithm, requirement of more software and hardware, so computational cost increases and vice versa.

- software and hardware, so computational cost increases and vice versa.

III. WATERMARKING TECHNIQUES

Digital watermarking is very much popular now a days because it is easily available and it protects our data from illegal use. It has two major areas i.e. spatial domain watermarking and frequency domain watermarking In the spatial domain techniques, we embed the watermark by modifying the pixel values. On the other hand, in transform domain watermarking, the watermark is embedded into the coefficients of transform domain. Various types of transform domain techniques are DCT, DWT and DFT. From robustness and imperceptibility point of view, transform domain techniques are better than spatial domain techniques.

A. Spatial Domain Watermarking

We know that the image is made up of pixels. In this method of watermarking, we embed the watermark in some specific pixels of image . In the extraction phase, we extract the watermark from these specific pixels. This technique is very much easy to use, less complex and also takes less time. But on the other hand, it is not robust for various types of attacks.

B. Transform Domain Watermarking

The transform domain watermarking is better as compared to the spatial domain watermarking. The image is represented in the form of frequency in the transform domain watermarking. In the transform domain watermarking techniques, firstly conversion of the original image is done by a predefined transformation. Then we embed the watermark in the transform image or in the transformation coefficients. Finally, we take the inverse transform to get the watermarked image Commonly used transform domain methods are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT).

1) Discrete Cosine Transform

It is generally used for the signal processing. In this we transform the image into the frequency domain. It is applied in many areas like pattern recognition, data compression, and image processing. This technique is more robust than spatial domain watermarking techniques. The main steps used in DCT are:

- Firstly, take the image and divide it into nonoverlapping 8*8 blocks.

- Calculate forward DCT of each of the non-overlapping blocks.

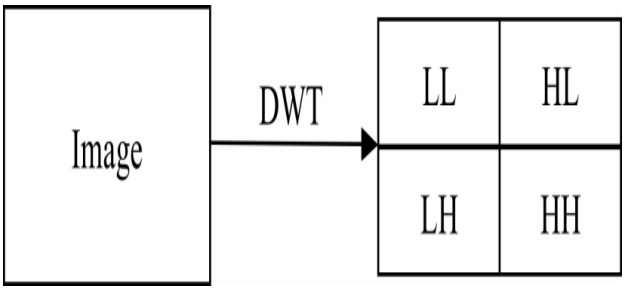
- Calculate forward DCT of each of the non-overlapping blocks.
- Use HVS blocks selection criteria.
- Now use highest coefficient selection criteria.
- Then embed watermark in the selected coefficient.
- Now take inverse DCT transform of each block.

2) Discrete Wavelet Transform

Discrete Wavelet Transform (DWT) gives a multi resolution representation of the image. This representation provides a simple framework for interpreting the image formation. The DWT analyses the signal at multiple resolution. When we apply the DWT to an image, it divides the image into two quadrants, i.e. high frequency quadrant and low frequency quadrant. This process repeats until the signal has been entirely decomposed. If we apply 1-level DWT on two dimensional image, it divides it into four parts, i.e.

- *LL:* It consists the low frequency details of the original image. We can say that approximation of the image lies in this part.
- *LH:* It consists vertical details of the original image. *HL:* It consists the horizontal details of the original image.
- *HH:* It consists high frequency details of the original image.

Since we know that the detail of original image lies in low frequency coefficients, so we embed the watermark into low frequency coefficients If we apply IDWT, we can reconstruct the original image from the decomposed image



3) Discrete Fourier Transform

Discrete Fourier Transform (DFT) offers more robustness against geometric attacks like scaling, cropping, translation, rotation, etc. It decomposes an image in sine and cosine form. In this, embedding may be done in two ways: direct embedding and the template based embedding.

In the direct embedding technique we modifying DFT magnitude and phase coefficients and then the watermark is embedded. The template based embedding technique introduces the concept of templates. In DFT domain, during embedding process, we embed the template, which is used to find the transformation factor. When the image is transformed, firstly this template is searched and it is then used to resynchronize the image. After this, detector is used to extract the embedded spread spectrum watermark

IV. WATERMARKING ATTACKS

When the watermarked media is transmitted, several attacks take place on that watermarked media. These attacks may be given as:

- *Removal Attack:* In this, the unauthorized user tries to remove the watermark i.e. secret information from the watermarked data.
- *Interference Attack:* In these types of attacks, the noise is inserted to the watermarked media. Some examples of this category are averaging, quantization, compression etc.
- *Geometric Attack:* These types of attacks can change the geometry of the image. The examples of this category are cropping, rotation etc.
- *Low Pass Filtering Attack:* This type of attack takes place when we pass the watermarked data from a low pass filter.

- *Active Attack: It* is the most important attack. Here the unauthorized user tries to extract the watermark or simply makes the watermark such that it cannot be detected by any operation.

- *Passive Attacks:* In this type of attack, unauthorized user simply tries to find out that the particular data contain the watermark or not.

- *Image Degradation:* In these types of attacks, the parts of the image are removed, resulting in damage of robust watermarks. Examples of these attacks are partial cropping, row removal and column removal, insertion of Gaussian noise

V. CONCLUSION

In this paper it have represented various aspects related to digital watermarking. The paper defines the meaning of digital watermarking, its applications and various watermarking techniques which help the new researchers in the field of digital watermarking. It also give the comparisons of various watermarking techniques with their advantages and disadvantages and also defined the performance measurement of images.

As we can see that digital watermarking is very useful method for digital data authentication. It ensures the protection of copyright and authentication. This paper gives an overall analysis of various types of digital watermarking methods. In this paper we have discussed different methods such as spatial domain methods and transform domain method which consists DCT, DWT and DFT. We have discussed the pros and cons of these methods. From a research point of view, this technology is an interesting field because many techniques are emerging for protection of data and many still have to come.

REFERENCES

[1] A. A. Hood and Prof. N. J. Janwe, "Robust Video Watermarking Techniques and Attacks on Watermark – A Review", International Journal of Computer Trends and Technology, vol. 4, Issue No. 1, pp. 30-34, 2013.

[2] Gurpreet Kaur, Kamaljeet Kaur, "Image watermarking Using LSB", international journal of Advanced Research in Computer science and Software Engineering,Volume 3, Issue 4, April 2013.

[3] Prabhishek Singh, R S Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013.

[4] Vaishali S. Jabade, Dr. Sachin R. Gengaje "Literature Review of Wavelet Based Digital Image Watermarking Tchniques ", International Journal of Computer Applications (0975 – 8887) Volume 31– No.1, October 2011.

[5] Meenu Singh, Abhishek Singhal and Ankur Chaudhary, "Digital Image Watermarking Techniques: A Survey", International Journal of Computer Science and Telecommunications Volume 4, Issue 6, June 2013.

[6] Alankrita Aggarwal Monika Singla, "Image Watermarking Techniques in Spatial Domain: A Review", Int. J. Comp. Tech. Appl., Vol 2 (5), 1357-1363, IJCTA | Sept-Oct 2011.

[7] Ankita Sengar1, Preeti verma2, Prof. Shreeja Nair3, Sanjay Sharma4, "A Comparative Study On Lsb Based Watermarking and Vss Based Watermarking",International Journal Of Research In Computer Applications And Robotics Issn 2320-7345, Vol. 1 Issue2 April 2013.

[8] Pallavi Patil, D.S. Bormane , "DWT Based Invisible Watermarking Technique for Digital Images" ,International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013.

[9] A. Adhipathi Reddy, "A new wavelet based logo-watermarking scheme", Pattern Recognition Letters vol 26 pp 1019–1027, 2004.

[10] Anand Bora, Nikhil Dalshania, Aditya Bhongle, "Competitive Analysis of Digital Image Watermarking Techniques", International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, Volume-1, Issue-2, June 2012.

[11] Vidya sagar M. Potdar, Song Han, "A survey of digital image watermarking techniques", 2005 3rd IEEE international conference on industrial informatics (INDIN).

[12] LI Hui-fang1, "A study on image digital watermarking based