A Review of Digital Watermarking, Applications and its Techniques

Er. Sanjeev Kumar[1], Dr. Tanu Preet Singh[2]
[1]Assistant prof., Department CSE, PTU Jalandhar, India
[2]Prof. and Head, Department ECE, PTU Jalandhar, India

Abstract- 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, spatial domain, frequency domain, LSB, DCT, DWT.

I. INTRODUCTION

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 [1]. 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 [3].

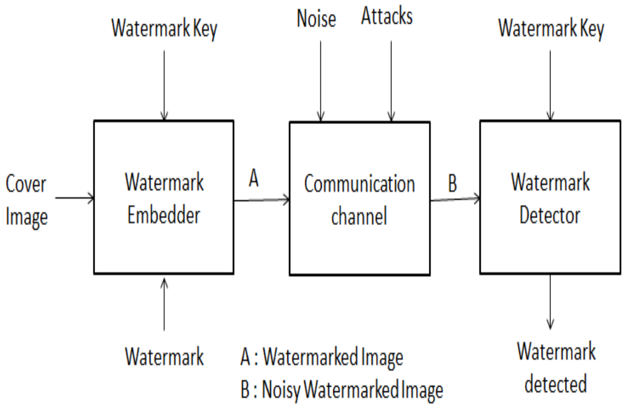

Fig 1.1 Digital Watermarking System

II. APPLICATIONS OF DIGITAL WATERMARKING

There are various applications of watermarking which are listed below [3].

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.

E. Content Description

This watermark can contain some detailed information of the host image such as labeling and captioning. For this kind of application, capacity of watermark should be relatively large and there is no strict requirement of robustness.

F. Covert Communication

It includes exchange of messages secretly embedded within images. In this case, the main requirement is that hidden data should not raise any suspicion that a secret message is being communicated.

III. WATERMARKING TECHNIQUES

Watermarking techniques can be classified into two domains:

a. Spatial domain watermarking
b. Frequency domain watermarking

IV. SPATIAL DOMAIN WATERMARKING TECHNIQUES

In spatial domain technique the watermark embedding is achieved by directly modifying the pixel values of the host image. The most commonly used method in the spatial domain technique is the least significant bit (LSB). In the least significant bit (LSB) of each pixel in the host image was modified to embed the secret message [5].

A. LSB Technique

The most straightforward method of watermark embedding would be to embed the watermark into the least significant bits of the cover object. Fig. 3.1 shows an example of modifying LSB [1], [6].

Image: 11001010 00110101 00011010 00000000
Watermark: 1 1 1 0
Watermarked image 11001011 00110101 00011011 00000000

B. Correlation-Based Techniques

Another technique for watermark embedding is the correlation properties of additive pseudo-random noise patterns as applied to an image. A pseudo-random noise (PN) pattern W(x,y) is added to the cover image I(x,y), according to the equation shown below.

$$I_w\,x,y = I\,x,y + k * W(x,y) \qquad (1)$$

In above equation, *k* denotes a gain factor, and IW the resulting watermarked image. To retrieve the watermark, the same pseudo-random noise generator algorithm is seeded with the same key, and the correlation between the noise pattern and possibly watermarked image computed. If the correlation exceeds a certain threshold T, the watermark is detected, and a single bit is set. This method can easily be extended to a multiple-bit watermark by dividing the image up into blocks, and performing the above procedure independently on each block.

V. Frequency Domain Watermarking

This technique is also known as Transform domain. In this technique values of certain frequencies are changed from there original values. There are various methods which are used in transform technique such as DWT, DCT and DFT [2].

A. Discrete Wavelet Technique

Discrete Wavelet transform (DWT) is a mathematical tool for decomposing the image. The transform is based on small waves called wavelet of varying frequency. The wavelet transforms decomposing the image into three directions i.e. horizontal, vertical and diagonal. Fig 5.1 shows the decomposition of image [3] [8].

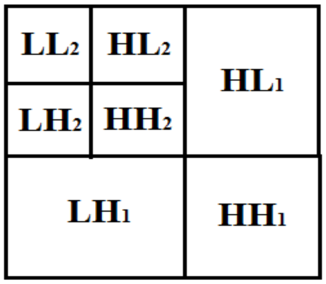

Fig 5.1 2-level DWT

Hence magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH and HL). The DWT is used in a signal processing applications such as audio and video compression and simulation of wireless antenna distribution.DWT is preferred because it provide both a simultaneous spatial and frequency spread of watermark within the host image [9].

B. *Discrete Cosine Transform*

DCT represents data in the form of frequency rather than an amplitude space. DCT watermarking techniques are robust compared to spatial domain techniques. DCT domain watermarking can be classified into Global DCT and Block based DCT watermarking [2].

$$X_k = \sum_{n=0}^{N-1} x_n \cos\left[\frac{\pi}{N}\,(n+n/2)k\right] \qquad (1)$$

K=0, 1, 2…………N-1

Where X_k is discrete cosine transform. DCT is used for lossy data compression because it has a strong energy compaction property [9].

C. *Discrete Fourier Transform*

DFT transforms a continuous function into its frequency components. It has robustness against geometric attacks such as rotation, scaling, cropping etc. DFT show translation invariance [2]. DFT is rotation, scaling and translation (RST) invariant. It can be used to recover from geometric distortions where as the spatial domain, DCT and DWT are not rotation, scaling and translation invariant and it is difficult to overcome from geometric distortions [10].

VI. COMPARSIONS OF DIFFERENT WATERMARKING TECHNIQUES[2]

Algorithm	Advantages	Disadvantages
LSB	➢ Easy to implement and understand. ➢ Low degradation of image quality. ➢ High perceptual transparency.	➢ It lacks robustness ➢ Susceptible to noise. ➢ Vulnerable to cropping and scaling.
Correlation	➢ Gain factor can be increased resulting in increased robustness	➢ Image quality gets decreased due to increased in gain factor
DCT	➢ The watermark is embedded into the coefficients of middle frequency, so the visibility of image will not affected and watermark will not be removed by any kind of attack.	➢ This block wise DCT destroys the invariance properties of the system. ➢ Certain higher frequency components tends to be suppressed during the quantization step.
DWT	➢ Allow good localization both in time and spatial frequency domain ➢ Higher compression ratio which is relevant to human perception.	➢ Cost of computing can be higher. ➢ Longer compression time. ➢ Noise near edges of images or video frames.
DFT	➢ DFT is rotation, scaling and translation invariant. It can be used to recover from geometric distortions.	➢ Complex implementation ➢ Cost of computing may be higher.

VII. PERFORMANCE EVALUATION MATRICS

For the measurement Mean Square Error and Peak Signal to noise ratio

a. MSE is defined as in the equation:

$$\text{MSE}=1/XY\left[\sum_{i=1}^{X}\sum_{j=1}^{Y}(c(i,j)-e(i,j))^2\right] \qquad (1)$$

Where X and Y are height and width of the image. The c(i,j) is the pixel value of the image and e(i,j) is the pixel value of the embed image[11].

b. PSNR is used to determine the degradation in the embedded image with respect to original image. PSNR is defined by the following formula as:

$$\text{PSNR} = 10* \log10\,(255)^2\,/\text{MSE} \qquad (2)$$

VIII. 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.

REFERENCES

[1] 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.

[2] 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.

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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

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

[9] 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.

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

[11] LI Hui-fang1, “A study on image digital watermarking based on wavelet transform”, pp 122-126.2010.