International Journal For Technological Research In Engineering
Volume 1, Issue 7, March-2014 *ISSN (Online): 2347 - 4718*

A BRIEF SURVEY ON DIGITAL IMAGE WATERMARKING TECHNIQUES

Ms.Jalpa M.Patel[1], Mr.Prayag Patel[2]
[1]M.E. Student, [2] Asst. Professor
Department of Computer Science and Engineering
SPB College of Engineering, Linch, Gujarat, India.

***Abstract*: Due to the recent progress in internet, digital contents e.g. video, audio, images are widely used. Protection of digital contents must require. So, it has become a tough task to protect copyright of an individual's creation. The purpose of Digital Image Watermarking is to ensure and facilitate data authentication, security and copyright protection of digital images. This paper elaborates watermarking overview, embedding techniques, watermarking attacks, performance analysis. It will be useful for researchers to implement effective image watermarking technique.**

***Keywords:* Digital image watermarking, DCT, DWT, DFT, Attacks, Performance.**

I. INTRODUCTION

With widespread use of Internet multimedia content e.g. video, voice, and images are widely used and acquired in our daily life from the internet. Due to this, original digital multimedia contents suffer from infringement of their copyrights, easy modification and fast content transfer over the Internet. As a result, data piracy and copyright protection has become a serious issue in order to protect one's ownership rights. To secure the multimedia content various techniques are used e.g. cryptography, steganography, and watermarking. Each technique is used for its purpose. Cryptographic techniques are used to change the meaning of the documents. Steganographic techniques are used to hide the existence of the important content. Watermarking schemes are used for protection and or authentication of multimedia content [1]. Digital image watermarking is modification of the original image data by embedding a watermark containing key information such as authentication or copyright codes [2]. 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 scaleimage. The examples of this type of watermark include date, serial number, logo or any other kind of identification mark [3].
Digital image watermarking is used for Copyright Protection, Broadcast Monitoring, Tamper detection, Fingerprinting , Authentication and Integrity Verification, Content description, Covert communication etc.

The remaining sections of the paper are as follows. In section 2 we discuss an overview of Watermarking, section 3 describes watermarking techniques, and section 4 presents attacks on watermarked image and section 5 includes various performance analysis measures.

II. DIGITAL WATERMARKING OVERVIEW

Watermarking uses the concept of data hiding and can be considered as a signature that reveals the owner of the multimedia object. Information hiding means communication of information by hiding in and retrieving from any digital media [5]. The hiding process has been illustrated in Figure.1. Generation & Embedding of Watermark, attacks and retrieval/detection of embedded Watermark, these are the main steps of a Watermarking Algorithm [4]. Digital watermarking hides the copyright information into the digital data through certain algorithm. The secret information to be embedded can be some text, author‘s serial number, company logo, images with some special importance. This secret information is embedded to the digital data (images, audio, and video) to ensure the security, data authentication, identification of owner and copyright protection. The watermark can be hidden in the digital data either visibly or invisibly. A Visible Watermark [6] allows the primary image to be viewed, but still marks it clearly as the property of the owning organization. An Invisible Watermark [6], on the other hand, is an image overlaid on another image which cannot be seen, but can be detected algorithmically. For a strong watermark embedding, a good watermarking technique is needed to be applied. Watermark can be embedded either in spatial or frequency domain.

III. DIGITAL IMAGE WATERMARKING TECHNIQUES

Digital image watermarking techniques can be broadly classified into two major categories:
i). Spatial Domain Watermarking
ii). Frequency Domain Watermarking

i) Spatial Domain Watermarking
Early watermarking schemes were introduced in the spatial

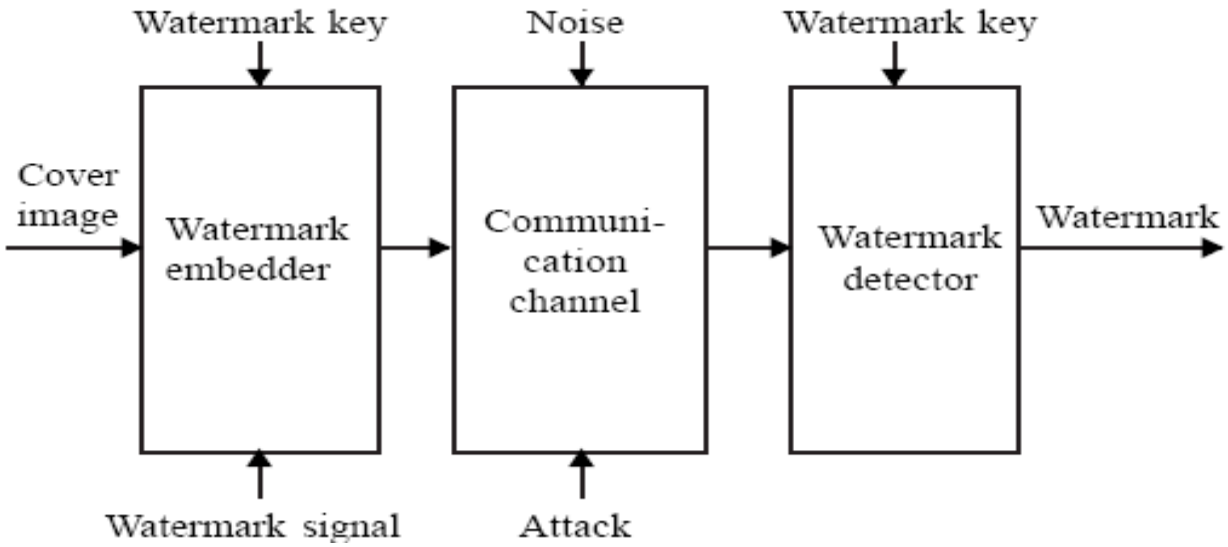

Fig.1. Generic Watermarking Scheme [4].

domain, where copyrighted information is added by changing pixel values of host image. Least Significant Bit insertion is one of the examples of this category. But such algorithms have low payload, they can be easily discovered and quality of image after embedding the copyright information and extracted watermark is not acceptable as pixel strengths are directly changed in these algorithms [9]

ii) Frequency Domain Watermarking

In the Frequency domain the watermark is embedding into frequency coefficients of host image. Frequency domain watermarking provides more information hiding capacity and high robustness against various geometrical attacks. Frequency domain watermarking is more robust than spatial domain watermarking due to the embedding of watermark into the altered frequency coefficients of the transformed image [9]. Some well-known watermarking transform domain are Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT).

A. Discrete Fourier Transform (DFT)

Transforms a continuous function into its frequency components. It has robustness against geometric attacks like rotation, scaling, cropping, translation etc. DFT shows translation invariance. Spatial shifts in the image affects the phase representation of the image but not the magnitude representation, or circular shifts in the spatial domain don't affect the magnitude of the Fourier transform.

B. Discrete Cosine Transform (DCT)

DCT like a Fourier Transform, it represents data in terms of frequency space rather than an amplitude space. 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.

The first efficient watermarking scheme was introduced by Koch et al. In their method, the image is first divided into square blocks of size 8x8 for DCT computation [15] as shown in the figure 2.

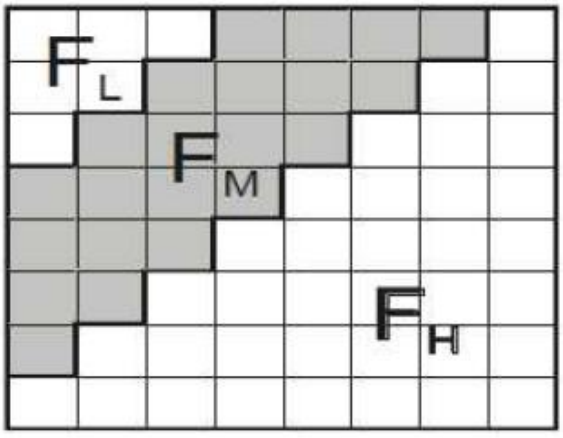

Fig.2. DCT Coefficients

In general, the DCT coefficients are divided into three bands (sets), namely low frequencies, middle frequencies and high frequencies. Fig. 2 visualizes these bands. Low frequencies (FL) are correlated with the illumination conditions and high frequencies (FH) represent noise and small variations (details). Middle frequencies (FM) coefficients contain useful information and construct

the basic structure of the image. Middle frequencies FM is chosen to embed the watermark as the embedding of watermark in a middle frequency band does not scatter the watermark information to most visual important parts of the image i.e. the low frequencies. It does not overexpose them to removal through compression and noise attacks where high frequency components are targeted [10]-[11]. Other reason for inserting watermarks in high frequency band is that they tend to have less influence on the quality of original image, while watermarks in low band will achieve a better robustness (since a large portion of high frequency components may be quantized to zero under JPEG compression).

The steps involved in any technique which is based on DCT [12] are as follows:

Step 1: Divide the entire image into 8x8 sized non-overlapping blocks.
Step 2: Take the DCT of each block of size 8x8.
Step 3: Apply a block selection criterion based on the knowledge of Human Visual System
(HVS).
Step 4: Use some coefficient selection criteria for embedding.
Step 5: Embed the watermark by modifying the selected coefficients.
Step 6: Take the inverse DCT of each block.

Almost all the algorithms for digital watermarking based on DCT are classified on the basis of step 3 and 4 i.e. the main differentiation between these algorithms is on the basis of block selection criteria or coefficient selection criteria.

C. Discrete Wavelet Transform (DWT)

Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial directions, i.e horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely. 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).

DWT is the multiresolution description of an image the decoding can be processed sequentially from a low resolution to the higher resolution [7]. The DWT splits the signal into high and low frequency parts. The high frequency part contains information about the edge components, while the low frequency part is split again into high and low frequency parts. The high frequency components are usually used for watermarking since the human eye is less sensitive to changes in edges [8].In two dimensional applications, for each level of decomposition, we first perform the DWT in the vertical direction, followed by the DWT in the horizontal direction. After the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1. For each successive level of decomposition, the LL subband of the previous level is used as the input. To perform second level decomposition, the DWT is applied to LL1 band which decomposes the LL1 band into the four sub- bands LL2, LH2, HL2, and HH2. To perform third level decomposition, the DWT is applied to LL2 band which decompose this band into the four sub-bands – LL3, LH3, HL3, HH3. This results in 10 sub-bands per component. LH1, HL1, and HH1 contain the highest frequency bands present in the image tile, while LL3 contains the lowest frequency band. The three-level DWT decomposition is shown in Fig.3.

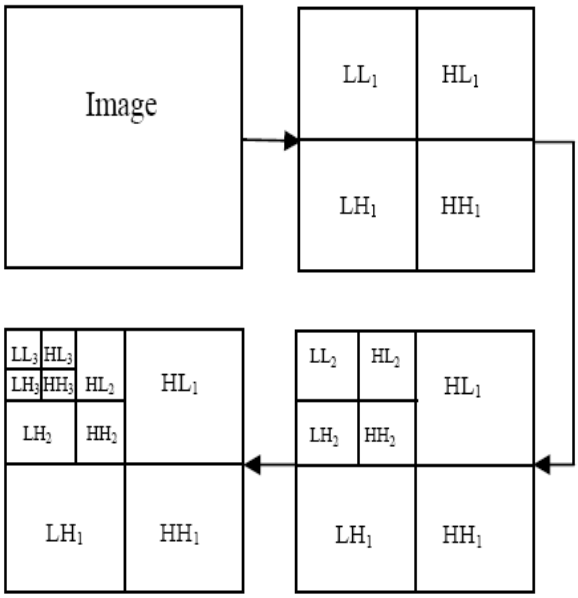

Fig.3. 3-level discrete wavelet decomposition

IV. ATTACKS ON WATERMARKED IMAGE

Attacks on watermarked image are distortions in watermarked image. These attacks may be intentional or un-intentional. An image watermarking method can be judged against such relevant attacks. The attacks are broadly classified as signal processing attacks and geometric attacks [8].

- ***Signal Processing Attacks***

Signal processing attacks are also called as image processing attacks or non-geometric attacks. These common signal processing attacks may include compression of image, addition of noise like Gaussian or salt and pepper noise, gamma correction, filtering, brightness, sharpening, histogram equalization, averaging, collusion, printing, scanning etc.

- ***Geometric Attacks***

Geometric attacks include basic geometric transformations in an image. These include geometrical distortions like rotation, scaling, translation, cropping, row-column blanking, warping etc. Geometric attacks attempt to destroy

synchronization of detection thus making the detection process difficult and even impossible.

V. PERFORMANCE ANALYSIS

The performance analysis for watermarked image and extracted watermark is done using different statistical measures. The watermark robustness depends directly on the embedding strength, which in turn influences visual degradation of the image. For benchmarking and performance evaluation, visual degradation due to embedding is important. Since there is no universal metric, we review in this section the most popular pixel based distortion criteria [14].

A. Watermark Imperceptibility Analysis

The imperceptibility of watermarked image is qualitatively decided by visual artefacts in watermarked image. Different literatures have reported different metrics. As a quantitative measure, following metrics are used. The notations used are listed below.

X (i, j): Original image,
X' (i, j): Watermarked image,
Nt: Size of image

a. Mean Square Error (MSE)

Mean Square Error between original image and watermarked image is calculated as follows:

$$MSE=\frac{1}{Nt}\sum_{i,j}(X(i,j)-X'(i,j))^2 \quad \text{.....eq. (1)}$$

b. Peak Signal to Noise Ratio (PSNR)

PSNR is used to compare difference between the original and the watermarked image [13]. Larger the PSNR value, more similar is watermarked image to the original image. This image quality metric is defined in decibels as:

$$PSNR=10\ log10\ \frac{(255\times255)}{MSE} \quad \text{.....eq. (2)}$$

If the PSNR value is greater than 30dB then the perceptual quality is acceptable.

c. Image Fidelity (IF)

Image fidelity is a measure of imperceptibility or transparency of watermarked image and is calculated as follows:

$$IF=1-\frac{\sum_{i,j}(X(i,j)-X'(i,j))^2}{\sum_{i,j}(X(i,j))^2} \quad \text{.....eq. (3)}$$

High value of image fidelity is desirable.

B. Watermark Robustness Analysis

The robustness of watermarked image is qualitatively analysed by visual artefacts in extracted watermark in case of visually meaningful logo watermark. As a quantitative measure, following metrics are used in case of logo or binary sequence watermark. These indicate reliability and readability of extracted watermark. The notations used are listed below.
W (i, j): Original Watermark
W' (i, j): Extracted Watermark

a. Correlation Coefficient (CRC)

This metric is used to analyze compatibility of original watermark and extracted watermark. The value ranges from 0 to 1.

$$CRC=\frac{\sum_{i,j}\sum_{i,j}W(i,j)W'(i,j)}{\sqrt{\sum_{i,j}\sum_{j,j}W(i,j)^2\times\sum_{i,j}\sum_{i,j}W(i,j)^2}} \quad \text{..... eq. (4)}$$

b. Similarity Measure (SIM) /Normalized Correlation (NC)

A similarity measure also called as similarity coefficient (SC) between extracted watermark and embedded watermark is used for objective judgment of the extraction fidelity.

$$SIM\ (W,\ W') = \frac{\sum_{i,j}\sum_{i,j}(W(i,j)W'(i,j)}{\sum_{i,j}\sum_{i,j}(W(i,j))^2} \quad \text{.....eq. (5)}$$

c. Bit Error Rate (BER)

This performance metric is suitable for random binary sequence watermark. The parameter is defined as ratio between number of incorrectly decoded bits and length of the binary sequence. BER indicates probability of incorrectly decoded binary patterns. It is defined as follows.

$$BER = \frac{DB}{NB} \quad \text{.....eq. (6)}$$

Where,
DB: No. of incorrectly decoded bits
NB: Total no. of bits

d. Accuracy Ratio (AR)

It is used to evaluate similarity between the original watermark and extracted one. It is defined as ratio of number of correct bits between original watermark and extracted watermark and number of original watermark bits. It is defined by following equation.

$$AR = \frac{CB}{NB} \quad \text{.....eq. (7)}$$

Where,
CB: No. of correct bits
NB: Total no. of bits

VI. CONCLUSION

The watermarking research is progressing very fast and various researchers from various fields are focusing to develop robust watermarking schemes. For that reason, we have presented brief knowledge of digital image watermarking in terms of overview, watermarking techniques, attacks, applications, performance analysis. Here, we tried to elaborate watermarking techniques with their importance in watermark embedding. Also In this paper we tried to give the complete information about the digital watermarking which will help the new researchers to get the maximum knowledge in this domain.

REFERENCES

[1] Riaz, Sang-Woong Lee," Image Authentication and Restoration by Multiple Watermarking Techniques with Advance Encryption Standard in Digital Photography" IEEE, ICACT 2013.

[2] Mr. Manjunatha Prasad. R, Dr.Shivaprakash Koliwad "A Comprehensive Survey of Contemporary Researches in Watermarking for Copyright Protection of Digital Images", International Journal of Computer Science and Network Security (IJCSNS), Vol.9 No.4, April 2009, pp.91-102.

[3] Wan Adnan, W.A.; Hitam, S.; Abdul-Karim, S., Tamjis, M.R., "A review of image watermarking", Research and Development, SCORED, 2003, pp. 381-384.

[4] DP Kaur, J Kaur, K Deep," Digital Image Watermarking: Challanges and Approach for a Robust Alorithm", International Journal of Electronics Engineering, 1(1), 2009, pp. 95-97.

[5] Preeti Gupta, "Cryptography based digital image watermarking algorithm to increase security of watermark data", IJSER, Volume 3, Issue 9, September 2012, ISSN 2229-5518.

[6] Jung S Cho, Seung W. Shin, Won H. Lee, M Jong U. Choi,Enhancement of Robustness of Image Watermarks Image Watermark into Coloured Image, based on WT & DCT,ITCC Las Vegas, (2000).

[7] Xiao Jun Kang Li Jun Dong, "Study of the Robustness of Watermarking Based on Image Segmentation and DFT", IEEE International Conference on Information Engineering and Computer Science, ICIECS, 2009, pp1-4.

[8] Vaishali S. Jabadeand and Dr. Sachin R. Gengaje, "Literature Review of Wavelet Based Digital Image Watermarking Techniques", International Journal of Computer Applications, vol. 31–No.1, October 2011.

[9] Chirag Sharma, Deepak Prashar, " DWT based robust technique of watermarking applied on igital Images", International Journal of Soft Computing and Engineering (IJSCE),Volume-2,Issue-2,May 2012

[10] Liwei Chen, Mingfu Li,"An Effective Blind Watermark Algorithm Based on the DCT", IEEE, Proceedings of the 7th World Congress Intelligent Control and Automation, June 2008, Chongquing, China.

[11] A. Hanaa , M. hadhoud, and A. Shaalan, "A Blind Spread Spectrum Wavelet Based Image Watermarking Algorithm" International Conference on Computer Engineering &Systems, pp. 251-256, 2009.

[12] Mehmet Utku Celik, Gaurav Sharma, Ahmet Murat Tekalp. " Lossless Generalized – LSB Data Embedding", IEEE Transactions on Image Processing, vol. 14, No.2, February2005.

[13] Huming Gao , Liyuan Jia, Meiling Liu, ". A Digital Watermarking Algorithm for Color Image Based on DWT", TELKOMNIKA, Vol. 11, No. 6, June 2013, pp. 3271 - 3278.

[14] F. Kumgollu, A Bouridane, M A Roula and S Boussaktd, "Comparison of Different Wavelet Transforms for Fusion Based Watermarking Applications", IEEE Transactions, Vol.3, 2003, pp. 1188-1191.

[15] Lin Liu, "A Survey on Digital Watermarking Techniques"

