JOURNAL OF INFORMATION, KNOWLEDGE AND RESEARCH IN ELECTRONICS AND COMMUNICATION ENGINEERING

A REVIEW ON IMAGE WATERMARKING TECHNIQUES AND PERFORMANCE MEASURES

[1]*D.M.GAIKWAD,* [2]*Dr. A. R. KARWANKAR*

[1]M.E. (EC), Government College of Engineering Aurangabad, India
[2] Associate Professor, Government College of Engineering Aurangabad, India

[1]*dnyangaik@gmail.comn,* [2]*karwankar@yahoo.com*

ABSTRACT *: With popularity and ease access of the internet, the multimedia data such as images, audios and videos are easily created, copied and transmitted in every fraction of second by people. This imposes an important matter of protection, authentication and illegal redistribution of digital media. A technique known as digital watermarking is used against all such misuse of data. Digital image watermarking technique is the process of embedding secret information in digital media. A watermark is secret information which is embedded in digital media that can be detected and extracted by the authentic user only thereby providing the copyright protection and ownership to digital media. This paper reviews different aspects and techniques of digital image watermarking.*

KEY WORDS: Digital Watermarking, Watermark, Copyright Protection.

1. Introduction

Due to rapid development of computer technologies, smart hand held devices and communication field the multimedia such as text, images, audio and videos has now been widely used which offer many facilities for duplication, distribution, creation and manipulation of digital data. Now a day, majority of transactions like railway reservation, airplane reservations, shopping, banking, efiling the income tax return are done online. A group of people can illegally access, distribute and misuse data over the internet without owner's consent. Therefore, there is need to secure and protect the digital media from illegal modification. The idea of communicating secretly is as an older technique found in the Indian literature in which secret writing/steganography have been used. Watermarking technique has been evolved from steganography in which person communicates a message secretly [1].

In digital image watermarking, the original image data is modified by embedding a watermark. This watermark contains key information such as authentication or copyright codes [2]. Digital watermarking technology is the process of embedding coded information called as watermark, tag or label into a multimedia object such as image, audio or video. This watermark can be detected or extracted later to authenticate and prove the ownership.

1.1 Need of Digital Watermarking:

The idea behind digital watermarks is to provide copyright
protection for intellectual property that is in digital format, such that nobody can tamper the data without consent of the owner.

1.2 Objectives of Digital Watermarking:

Traditional information security technology has deficiencies of the security and protection which can be removed by using digital watermarking. In this method, by hiding certain information in the original data provides an effective solution to compensate issues of the of traditional information security. Digital watermarking prevents illegal duplication, distribution the digital media [1].

This paper is organized into five sections. Section I explains the basic introduction for watermark. Section II elaborates Digital Image Watermarking technique. Section III focuses on properties of image watermarking and Section IV explains performance measures. Section V explains conclusion and section IV gives an acknowledgement.

2. DIGITAL WATERMARKING TECHNOLOGY

Digital watermarking is one of such popular technique of copyright protection. It hides certain details of digital data. These details can be hidden in the form of digital image, text, an audio or video signal which determines the nature of digital watermarking. General block diagram of watermarking is shown in Fig.1.

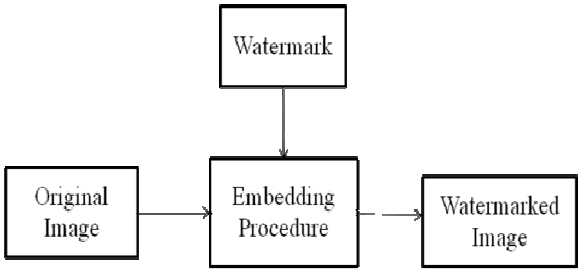

Fig. 1 Block diagram of a watermarking

Digital watermarks are messages embedded in a multimedia such as an image or text or other digital videos.

A watermark is information about origin, ownership and copy control. This information is embedded in multimedia which will take care of imperceptibility and robustness. General block diagram for watermark extraction is shown in fig. 2

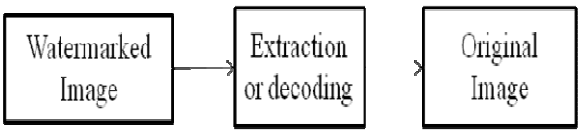

Fig. 2 Digital watermark extraction

2.1 Classification of Digital Watermarking

The digital watermarking can be categorized depending on its characteristics, attached media, detection process and copyright protection as follows

1) According to characteristics: Digital watermarking can be divided as robust watermarking and fragile watermarking.

i) Robust watermarking: This is used to sign copyright information of the digital media. This watermark can resist the common image processing, edit processing, and lossy compression. The watermark remains intact even after some attack and can still be detected to provide certification.

ii) Fragile watermarking: It is mainly used for protection of integrity, which is very sensitive to the changes of signal. We can check whether the data has been tampered or not.

2) According to attached media: It can be categorized as text watermarking, image watermarking, audio watermarking, video watermarking, and graphic watermarking. Image watermarking refers to watermark embedding in still image. In video watermarking, a watermark is embedded in video stream to control video applications. In text watermarking, a watermark is added to PDF, DOC and other text file to prevent changes occurring in text. In graphic watermarking, a watermark is embedded to 2-D or 3-D computer-generated graphics to indicate the copyright.

3) According to detection process: It can be divided into visual watermarking and blind watermarking. In the testing of visual watermarking, original data is required. It has stronger robustness, but has limited application. Whereas blind watermarking doesn't need original data, which has wide applications

4) According to copyright protection: In this, if the owners want others to see the mark of the image watermark then the watermark is visible after adding the watermark to the image, and the watermark still remain even if it is attacked.

Fig. 3. Shows (a) Lena image (b) Cameraman image to be Watermarked (c) visible watermarked Image and (d) the recovered cameraman image.

2.2. Properties of Image Watermarking

Watermarking technique can be divided into number of properties that are fidelity, data payload, security, robustness, capacity, false positive rate. We have to consider these requirements while designing the watermarking system. The properties of image watermarking are as follows

a) Fidelity or Transparency: After embedding the watermark, the quality of the image should remain intact. In other words, human visual system will not be disturbed by embedded watermark.

b) Robustness: Robustness is the ability to remain intact when undergoes common image operations like rotation, filtering, scaling, cropping and compression. Watermark should be strong and robust against geometrical and non-geometrical attacks.

c) Capacity or Payload: It describes how much data should be embedded as a watermark which will be successfully detected during extraction. Watermark should to carry enough information to represent the uniqueness of the image. Payload requirement varies as per the application [3].

3. REVIEW OF IMAGE WATERMARKING TECHNIQUES

In the literature, watermarking techniques are classified in two types as spatial domain and frequency domain techniques [4]. In Spatial domain, watermark is added by modifying pixel values of the original image. It is easy to implement from a computational point of view, but prone to numerous attacks. In Frequency domain, first image is transformed into a set of frequency domain coefficients by using transforms. The transform domain techniques used are DCT (Discrete Cosine Transform), DFT (Discrete Fourier Transform), and DWT (Discrete Wavelet Transform) and then watermark is added to its transformed coefficients. To

obtain the watermark, one should perform the transform inversely.

1. Spatial Domain watermarking:

The spatial domain techniques works directly on pixel values. The spatial-domain techniques directly modify the pixel values or color values of selected pixels and the frequency-domain techniques changes the values of some transformed coefficients [5].

The advantages of this method are: It is easy and simple method. It has low computational complexity and less time consuming. Though, computational speed is higher than transform domain but it is less robust against attacks. The most important method of spatial domain is Least Significant Bit (LSB). This is the simplest technique. With given image, each pixel is represented by 8-bit sequence. Out of 8-bit sequence, watermark is embedded in the Least Significant Bit (LSB) of the selected pixels of the image. It is easy to implement and does not have much distortion in the image. The main advantage is that it is simple to implement and provides high perceptual transparency. It is simple as compared to the transform domain but has low robustness. It can resist simple operations like cropping and addition of noise [6].

2. Frequency/Transform Domain watermarking:

To increase robustness of the watermarking, the watermark is embedded into frequency domain instead of the spatial domain. Here, first an image is transformed into a set of frequency domain coefficients [7]. The transforms like Discrete Cosine Transformation (DCT) Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT) methods are used. The transform domain has special properties of alternate domain to address the limitations of pixel based methods and support additional features.

3. Discrete Cosine Transform (DCT):

This technique converts a signal into frequency components. It converts data in terms of frequency rather than an amplitude space. The image is equally represented as a sum of sinusoid signals of different magnitude and frequencies. [8] The popular block based DCT transform results in giving three frequency coefficients: low frequency, mid frequency and high frequency sub-band. To retain the image quality, watermark is embedded in mid frequency sub-band [9]. DCT watermarking techniques are more robust than spatial domain techniques. It is robust against operations like low pass filtering, blurring, brightness and contrast adjustment but weak against geometrical attacks like rotation, scaling, cropping etc. They are difficult to implement and are computationally more expensive.

4. Digital Fourier Transform (DFT):

Fourier Transform (FT) is operation carried on signal that transforms a continuous function into its frequency components. The digitized discrete samples are equivalently represented in discrete valued function i.e. DFT [10]. The DFT of an image is generally complex value signal and used to represent magnitude and phase of the image. It is robust to usual image processing as linear or non-linear filtering, sharpening, JPEG compression. It is resistant to geometric transformations as scaling, rotation and cropping.

5. Digital Wavelet Transform (DWT):

It is a mathematical tool for hierarchically decomposing an image [8]. It is useful for processing of non-stationary signals. DWT transform is based on small waves know as wavelets. Wavelet transform provides information of both frequency and spatial domain of an image. Unlike conventional FT, temporal information is retained in this transformation. Wavelets are created by translations and dilations of a fixed function called mother wavelet. The wavelet transform is an excellent time-frequency analysis method, which can be used for extracting the information content of the image. A brief introduction to wavelet is as follows [11]. It decompose an image in basically three parts i.e, horizontally, vertically and diagonally such that the image is separated into four different parts namely LL, LH, HL and HH. Here first letter refers to applying either low pass or high pass frequency operation to the rows and the second letter refers to the filter applied to the columns of the cover image [12].

• LL level is the lowest resolution level which consists of the maximum information of the cover image,

• Remaining three levels i.e., LH, HL, HH give the detailed information of the cover image.

Applying a 1-D wavelet transform to all the rows of the Image and then repeating on all of the columns can compute the 2-D wavelet transform. For 2-D images, applying DWT corresponds to processing the image by 2-D filters in each dimension. This filter divides the input image into four sub-bands LL1, LH1, HL1 and HH1. The sub-band LL1 represents the coarse-scale while the sub-bands LH1, HL1and HH1 represent the fine-scale of DWT coefficients. For obtaining, the next scale of wavelet coefficients, sub-band LL1 is further processed until some final scale N is reached. When N is reached, we will have 3N+1 sub-bands consisting of the multi-resolution sub-bands LLN and LHx, HLx and HHx where x ranges from 1 to N. DWT excellent spatio-frequency localization properties suitable to identify the areas in the host image where a watermark can be embedded effectively. The following figure 4 and figure 5 shows the 1-level and 2-level decomposition of an image respectively.

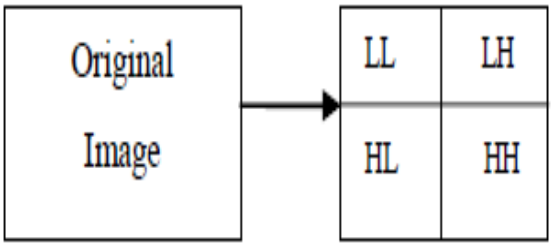

Fig. 4 One level DWT decomposition of image

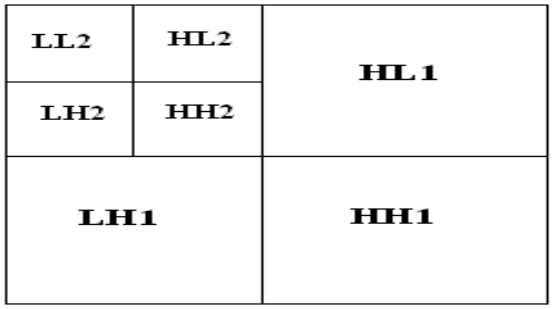

Fig. 5 Two level DWT decomposition of image

6. Singular Value Decomposition (SVD):

SVD transform is a linear algebra transform which is used for factorization of a real or complex matrix with various applications in image processing [13]. A digital image can be represented in a matrix, with its entries giving the intensity value of each pixel in the image, SVD has an matrix A which has singular value decomposition into product of an orthogonal matrix U, an diagonal matrix of singular values S and transpose of an orthogonal square matrix V. Let A be a square matrix of order n. then according to SVD it can be represented mathematically as:

$$A = U\,S\,V^{T} \quad (1)$$

$$U * U^{T} = I$$

$$V * V^{T} = I \quad (2)$$

Where, I represents an Identity matrix and S is the diagonal matrix of order m x n having elements Si (i=1, 2, 3, n). The singular values of A are represented by the diagonal elements of S. The columns of U matrix are known as the left singular values of A, and the columns of V are known as the right singular values of A. Factorization is called the singular value decomposition of A.

In recent years, lot of work has been carried out in transform domain watermarking using DCT, DWT, SVD and DWT-SVD and it is still going on.

4. PERFORMANCE MEASURES OF WATERMARKING

The performance analysis is done using different statistical measures for watermarked image and extracted watermark. The embedding strength of watermark decides its robustness, which influences visual degradation of the image. For benchmarking and performance evaluation, visual degradation is important due to embedding. In this section, we review the most popular pixel based distortion criteria [14][15].

4.1 Watermark Imperceptibility Analysis:

This is qualitative measure decided by visual artifacts in watermarked image. Different literatures have reported different metrics. As a quantitative measure, following metrics are used. The notations used are given below.

Xi: Original image,

X'i : Watermarked image, and

Nt : Size of image

4.2 Mean Square Error (MSE):

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

$$\mathrm{MSE} = \frac{1}{\mathrm{Nt}} + \sum_{i,j}\left((\mathrm{X}_{i,j} - \mathrm{X}'_{i,j}\right)^{2} \quad (3)$$

4.3 Peak Signal to Noise Ratio (PSNR):

PSNR is calculated between the original and the watermarked image. Larger the PSNR value, both watermarked image to the original image will be more similar. This image quality metric is defined in decibels as:

$$\mathrm{PSNR} = 10 * \log_{10}\frac{255 * 255}{\mathrm{MSE}} \quad (4)$$

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

4.4 Image Fidelity (IF):

Image fidelity is a measure of imperceptibility or transparency of watermarked image. High value of image fidelity is desirable.

4.5 SNR (Signal to Noise Ratio):

It measures the sensitivity of the images. It measures the signal strength relative to the background noise.

$$SNRdb = 10 * \log 10\ \frac{\mathrm{Psignal}}{\mathrm{Pnoise}} \quad (5)$$

4.6 BER (Bit Error Rate):

It is the ratio that describes how many bits received in error over the number of the total bits received [16].

$$BER = P * \mathrm{H/W} \quad (6)$$

Where H= Height W= Width

5. CONCLUSION

The literature survey shows that watermark may be of visible or invisible type and each method has its own strengths and weaknesses. The quality of watermarked images is measured in terms of PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error). Ideally, the value of PSNR & MSE should be infinite and zero respectively. But practically large PSNR and small MSE are desirable.

6. ACKNOWLEDGEMENT

I am very much thankful to my guide Dr. A. R. Karwankar, Associate Professor in Electronics and Telecommunication Engineering for his consistent

motivation, valuable guidance and support. I am grateful to all my department lab technicians for their technical support.

REFERENCES:

[1] Shraddha S. Katariya (Patni), "Digital Watermarking: Review", International Journal of Engineering and Innovative Technology (IJEIT), Volume 1, Issue 2, February 2012.

[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] Cox, IJ, Miller, ML & Bloom, JA 2002, Digital Watermarking, Morgan Kaufmann Publisher, San Francisco, CA, USA 2002.

[4] Ali Musrat, Ahn Chang Wook, Pant Millie, "An Optimized watermarking Technique based on DE in DWT-SVD Domain", IEEE Symposium on Differential Evolution, pp. 99-104, 2013.

[5] Ibrahim Nasir, Ying Weng, Jianmin Jiang, "A New Robust Watermarking Scheme for Color Image in Spatial Domain".

[6] Kaur Gurpreet and Kaur Kamaljeet, "Image Watermarking Using LSB (Least Significant Bit)", International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE), ISSN : 2277 128X, Vol. 3, Issue. 4, April 2013.

[7] Arvind Kumar, Parthasarathy and Subhash Kak, "An Improved Method of Content Based Image Watermarking", IEEE Transaction on broadcasting, Vol. 53, No. 2, June 2007, PP 468- 479.

[8] A. Sharma and A. Ganguly (20 12). Image Watermarking in DCT-DWT Domain. IRNet Trans on Electrical and Electronics Engineering, 1, 1-5.

[9] R. Dubolia and R. Gupta (201 1). Digital Image Watermarking by using DWT and DCT and Comparison based on PSNR. IEEE Communication Systems and Network Technologies, 593-596

[10] Ram Bhupendra, "Digital Image Watermarking technique using Discrete Wavelet Transform and Discrete Cosine Transform", International Journal for Advancements in Research and Technology, ISSN: 2278-7763, Vol. 2, Issue 4, April 2013.

[11] Vallabha V Hampiholi, " Multiresolution Watermark Based on Wavelet Transform for Digital images"

[12] M. MohamedSathik, S. S. Sujatha, "A Novel DWT Based Invisible Watermarking Technique for Digital Images", International Arab Journal of e-Technology, Vol 2, no. 3, pp. 167-173, January 2012.

[13] Manjunath. M, Prof. Siddappaji, "A New Robust Semi blind Watermarking Using Block DCT and SVD", IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), pp. 193- 197, 2012.

[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] Vaishali S. Jabade, Dr. Sachin R. Gengaje, "Literature Review of Wavelet Based Digital Image Watermarking Techniques", IJCA, Volume 31– No.1, October 2011.

[16] Manpreet Kaur, Sheenam Malhotra, "Review Paper on Digital Image Watermarking Technique for Robustness", IJARCSSE, Volume 4, Issue 5, May 2014.