Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Review Paper on Digital Image Watermarking Technique for Robustness

Manpreet Kaur[1]
Computer Science and Engineering
[1]SGGSWU, Fatehgarh Sahib, India

Sheenam Malhotra [2]
Computer Science and Engineering
[2]Assistant Professor, SGGSWU, Fatehgarh Sahib, India

Abstract- The protection and illegal redistribution of digital media has become an important issue because of popularity and accessibility of the internet now days by people. Digital watermarking is used to protect the information against the illegal distribution in the form of images, videos and audios. Digital image watermarking technique is the process of embedding watermark in the form of image that contain the special information and then it detect and extract that special information. The robustness, copyright protection, fidelity, capacity and some more are essential requirements of watermarking schemes so that they can handle several types of image processing attacks. This paper reviews different aspects and techniques of digital image watermarking for protecting digital contents.

Keywords- Digital Watermarking, Discrete Cosine Transform, Discrete Wavelet Transform, Discrete Fourier Transform, Singular Value Decomposition, Least Significant Bit.

I. Introduction

Recent advancements in computer technologies offer many facilities for duplication, distribution, creation and manipulation of digital contents. Due to rapid development of network technology, multimedia such as text, image, video and audio has now been widely used. Humans can easily access or distribute any multimedia data from networks. The development of communication networks and the trivialization of image processing tools have given rise to content security problems underscoring the need to secure digital images from illegal modification, protect their economic interest and ensure intellectual property [1]. Various techniques of watermarking are used to insert data about ownership of contents, which help to keep the integrity of data. Watermarking is the process of embedding data into a multimedia element such as an image, audio or video file for the purpose of authentication. This embedded data can be later extracted or detected the multimedia data for security purposes. A watermark is information about origin, ownership and copy control. This information is embedded in multimedia content with take care of imperceptibility and robustness. General block diagram of watermarking is shown in Fig.1.

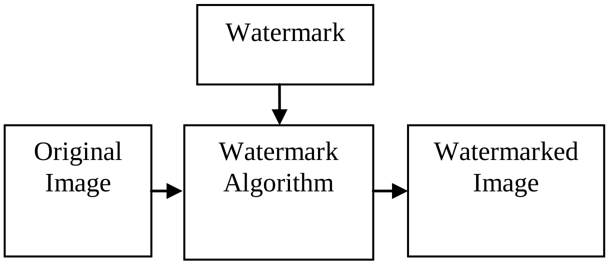

Fig. Diagram of a watermarking algorithm

Digital Image watermarking technique consists in embedding a permanent watermark in a cover image in such a way that the watermarked image remains accessible to everyone and the embedded watermark can be decoded with low much accuracy after the watermarked image have undergone several attacks[1].

Watermarking techniques given in the literature can be classified into numerous categories based on different sets of criteria. One of them is the domain in which the watermark is inserted; spatial domain techniques and frequency domain techniques [3]. In Special domain, watermark is added by modifying pixel values of the host image. Generally, it is easy to implement from a computational point of view, but too fragile to resist numerous attacks. In Frequency domain, watermark is not added to the image intensities, but to the values of its transform coefficients. Then to get the watermarked image, one should perform the transform inversely. It includes DCT (Digital Cosine Transform), DFT (Digital Fourier Transform), and DWT (Digital Wavelet Transform).

This paper is organized into five sections. Section I explains the basic introduction for watermark. Section II explains the background for Image Watermarking. Section III focuses on aspects of image watermarking and Section IV explains the review of image watermarking techniques.

II. Background

The security level of digital images over network has attracted much attention recently, and many different image watermarking methods have been proposed to enhance the security of these images [2]. Some previous researches are briefly described in the following.

Hana et al. [1] proposed a multiple non-blind watermarking scheme based on the discrete wavelet transform. This scheme consists of applying the DWT (Discrete Wavelet Transform) to the gray scale cover image and modifying the LL and HH sub-band coefficients in order to insert the binary watermarking. Experimental results indicate good fidelity and robustness against a large range of attacks.

Scholar et al. [2] proposed a robust and secure image watermarking algorithm that embeds watermark in the deinterlace images using wavelet transform. This scheme provides very high payloads and imperceptibility when compared to similar transform domain techniques and achieves excellent robustness against attacks such as noise addition.

Ali et al. [3] proposed an optimized image watermarking technique employing Differential Evolution (DE) in DWT-SVD domain. Experimental results have shown that the proposed scheme maintains a satisfactory image quality and watermark is resilient to various attacks even though the watermarked image is seriously distorted.

Chaturvedi et al. [4] this paper compares the digital image watermarking methods DWT and DWT-DCT on the basis of PSNR and concluded that DWT-DCT method is best technique for level one watermark embedding.

Pratap et al. [5] have done watermark insertion and extraction using the DWT and IDWT, and used alpha blending technique. The results obtained for the recovered images and the watermark are identical to the original image.

Gurpreet et al. [6] proposed a special domain method LSB for security of images, which is easy, simple and more effective.

III. Aspects of Image Watermarking

Digital watermarking has many applications according to the type of the watermark and the used technique. Watermarking systems can be divided by number of properties that are fidelity, data payload, blind detection, false positive rate, capacity, robustness, security, watermark keys, cost, sensitivity and scalability. Some of them are common to more practical applications. These properties are discussed due to their importance in watermarking applications. Some properties are:

a) **Fidelity:** The watermarking process should not distort the original image to ensure its commercial value.
b) **Transparency:** Transparency is perceptual similarity between the original and the watermarked versions of the cover work. The digital watermark should not affect the quality of the original image after it is watermarked.
c) **Robustness:** Robustness is the ability to detect the watermark after common signal processing operations. Watermark should be robust against variety of geometrical and non-geometrical attacks.
d) **Capacity:** This property describes how much data should be embedded as a watermark to successfully detect during extraction.

IV. Review of Image Watermarking Techniques

1. **Spacial Domain watermarking:** In Spacial domain the watermark is inserted into the intensity values. It embed the watermark by modify the pixel value of the host image. Low computational complexity and simplicity are the main strengths of the special domain methods. The best widely known algorithm is LSB techniques.

2. **Least Significant Bit:** This is the simplest approach. Given an image with pixels, and each pixel is represented by 8-bit sequence. The watermark is embedded in the last bit that is Least Significant Bit of the selected pixels of the image. This method is easy to implement and does not generate serious distortion to the image and it is not very robust against attacks[6].

3. **Frequency Domain watermarking:** In most of the watermarking techniques, the watermark will be embedded into frequency domain instead of the Spacial domain for the robustness of the watermarking. Discrete Cosine Transformation (DCT), Discrete Fourier Transform(DFT), and Discrete Wavelet Transform(DWT) are the three main methods of data transformation in this domain. The strength for the transform domain techniques is that they can take advantage of special properties of alternate domain to address the limitations of pixel– based methods or to support additional features.

4. **Discrete Cosine Transform (DCT):** The discrete cosine transforms is a technique for converting a signal into frequency components. It represents data in terms of frequency space rather than an amplitude space. DCT based watermarking techniques are robust compared to spacial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness, contrast adjustment and blurring. They are

difficult to implement and are computationally more expensive. At the same time they are weak against geometrical attacks like rotation, scaling, cropping etc.

The discrete cosine transform is a technique for converting a signal into frequency components. It represents an image as a sum of sinusoids of varying magnitudes and frequencies. From eq.1, the input image, x, and the DCT coefficients for the output image, y, are computed. In the equation, x is the input image having N*M pixels, x (m,n) is the intensity of the pixel of the image and y(u,v) is the DCT coefficient of the DCT matrix[4].

$$y(u,v) = \sqrt{\frac{2}{M}\sqrt{\frac{2}{N}}\,a_u a_v \sum_{u=0}^{M-1}\sum_{v-0}^{N-1} \quad x(m,n)}$$

$$\cos\frac{(2m+1)u\pi}{2M}\cos\frac{(2n+1)v\pi}{2N} \qquad (1)$$

Where alpha u and alpha v are given by:

$$a_u = \begin{cases} \frac{1}{\sqrt{2}}\ u = 0, u = 1,2,..,N-1 \\ 1 \end{cases}$$

$$a_v = \begin{cases} \frac{1}{\sqrt{2}}\, v = 0, v = 1,2,..,N-1 \\ 1 \end{cases}$$

The results from these giving three frequency sub-bands: low frequency sub-band, mid frequency sub-band and high frequency sub-band. DCT based watermarking is based on two facts. The first fact is that how much of the signal energy lies at low-frequencies sub-band which contains visual parts of the image. The second fact is that high frequency components of the image are usually removed through compression and noise attacks [4].

5. **Digital Fourier Transform (DFT):** Fourier Transform (FT) is an operation that transforms a continuous function into its frequency components. The equivalent transform for discrete valued function requires the Discrete Fourier Transform (DFT) [7]. The discrete Fourier transform of an image is generally complex valued and leads to a magnitude and phase representation for the image [8]. It is robust to the usual image processing as linear or non-linear filtering, sharpening, JPEG compression and resist to geometric transformations as scaling, rotation and cropping.

6. **Digital Wavelet Transform (DWT):** Discrete Wavelet transform (DWT) is a mathematical tool for hierarchically decomposing an image [4]. It is useful for processing of non-stationary signals. The transform is based on small waves, called wavelets. Wavelet transform provides both frequency and spatial domain of an image. Unlike conventional Fourier transform, temporal information is retained in this transformation process. Wavelets are created by translations and dilations of a fixed function called mother wavelet. This section analyses suitability of DWT for image watermarking and gives advantages of using DWT as against other transforms. For 2-D images, applying DWT corresponds to processing the image by 2-D filters in each dimension. The filters divide the input image into four sub-bands LL1, LH1, HL1 and HH1. The sub-band LL1 represents the coarse-scale DWT coefficients while the sub-bands LH1, HL1and HH1 represent the fine-scale of DWT coefficients. To obtain the next scale of wavelet coefficients, the 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 until N. Due to its excellent spatiofrequency localization properties, the DWT is very suitable to identify the areas in the host image where a watermark can be embedded effectively[4].

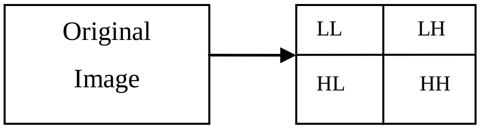

Fig. 1 DWT Decomposition of Image Using 1-Level Pyramid

7. **Other Watermarking Techniques:** The watermark can either be directly inserted into the image or by using some other techniques or methods.

Singular Value Decomposition (SVD) [3] 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. It can be seen as a method for transforming correlated variables into a set of uncorrelated ones that better expose the various relationships among the original data. Let A be a square matrix of order n. then according to SVD it can be represented mathematically as:

$$A = U\,S\,V^T \qquad (2)$$

Parameters used in Image watermarking:

- **PSNR** (Peak Signal to Noise Ratio):
  To measure the quality of a watermarked image, the peak signal to noise ratio is used.

$$PSNR = 10.\log_{10}\frac{MAX_1^2}{MSE} \qquad (3)$$

- **MSE** (Mean Squared Error) :
  Mean Squared error between original and distorted image is calculated using following formula.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - k(i,j)]2 \qquad (4)$$

- **NC** (Normalized Correlation) :
  We measure the similarity between the original watermark and the watermark extracted from the attacked image using the Normalized Correlation factor.

$$NC = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M} w(i,j) * w'(i,j)}{\sum_{i=1}^{N}\sum_{j=1}^{M} w^2(i,j)} \qquad (5)$$

- **SNR** (Signal to Noise Ratio) :
  It measures the sensitivity of the images. It measures the signal strength relative to the background noise.

$$SNR_{db} = 10\log_{10}\frac{P_{signal}}{P_{noise}} \qquad (6)$$

- **BER** (Bit Error Rate) :
  It is the ratio that describes how many bits received in error over the number of the total bits received.

$$BER = \frac{P}{H*W} \qquad (7)$$

Where H= Height
W= Width

V. Conclusion

This study discusses a number of techniques for the watermarking of digital images, also focus on the limitations and promises of each. LSB substitution does not provide robustness therefore it is not very efficient approach for digital watermarking. DCT domain watermarking proved to be highly considerable amounts of random noise. The wavelet domain as well proved to be highly resistant to both compression and noise, with minimal amounts of visual degradation. Typically these techniques are highly robust and unpredictable computationally.

References

[1] Hana Ouazzane, Hela Mahersia, Kamel Hamrouni, "*A Robust Multiple Watermarking Scheme based on the DWT*," 10th IEEE International Multi-Conference on Systems, Signals and Devices(SSD), pp. 18-21, 2013.

[2] Sridhar B and Arun Dr.C, "On *Secure Multiple Image Watermarking Techniques using DWT*," IEEE-20180, 26th - 28th July 2012.

[3] 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.

[4] Chaturvedi Navnidhi and Basha S.J, "*Comparison of Digital Image watermarking methods DWT and DWT-DCT on the basis of PSNR*," International Journal of Innovative Research in Science, Engineering and Technology(IJIRSET), ISSN: 2319-8753, Vol. 1, Issue 2, December 2012.

[5] Singh Akhil Pratap and Mishra Agya, "*Wavelet Based Watermarking on Digital image,"* Indian Journal of Computer Science and Engineering, ISSN : 0976-5166, Vol 1, No. 2, pp. 86-91.

[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] 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.

[8] http://books.google.co.in/books?id=6eeLBtO3cb4C&pg=PA101&1pg=PA101&dq=dft+in+watermarking &source=b1&ots=Hz821K-w9Y&sig=24Yt8JTLy99pcxii6uPdEL_6ju0&hl=en&sa=X&ei=jvg0U7D4 DIqtrAfbn4GIAQ&ved=0CDoQ6AEwAzgK#v=onepage&q=dft%20in%20watermarking&f=false