Enhancing Image Security in Spread-Spectrum watermarking: A review

1Rajkumari Hatkar, 2Dr.Ritu Shrivastava, 3Dr.Manish Manoria
1Student, 2Professor, 3Professor
1Computer Science & Engineering,
1 Sagar Institute of Research and Technology & Science, Bhopal, India

ABSTRACT

Digital Watermarking is a way of protecting the digital media from unauthorized usage. Digital watermark is digital signal carrying information of the creator of the media. Digital watermark is inserted into digital media in such a way that it is imperceptible to the human eye, but it is visible to a computer. To protect the images from misuse and illegal use watermarking is used as a secure technique for the protection of images In my work i have proposed a novel approach for digital watermarking, where I will use the simulation tools like MATLAB and the outcomes will be measured in standard parameters PSNR, MSE, NC etc.

Keywords: Multimedia, Digital Watermarking, MATLAB

I. INTRODUCTION

The expanding quantities of web clients wherever on the planet have forced numerous threats on the assurance of the reachable advanced information. Analysts and researchers in the range of digital security are tested to make new procedures to square such a hazard. Henceforth, this exploration performs advanced watermarking as a path for protecting various types of data like writings, pictures, sounds or recordings. It is fundamentally done by covering specific measures of visual pictures by setting undetectable checks, for example, copyright data to control any unlawful utilization of these pictures. In the field of computerized sight and sound correspondence, a few systems have helped a great deal for putting away, altering and getting to of these items [1]. However, security amid the exchanging correspondence is extremely pivotal. As lack of security prompt the misfortune in property rights. So to tackle this issue, advanced watermarking is great [2].

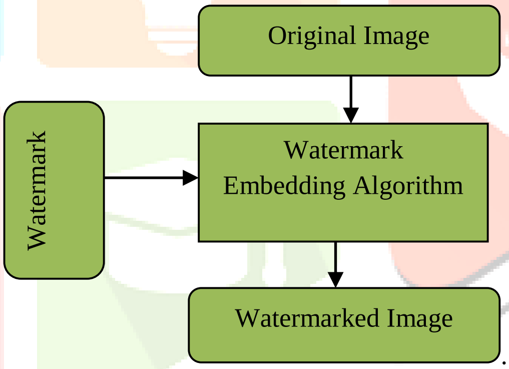

Figure 1: Watermark embedding process

Fig. 1 demonstrates the progression of watermark implanting. Digital watermarking is the process of embedding an image with secret data for the communication. The embedded image can only be extracted by person who has authentication which is shown through fig.2.

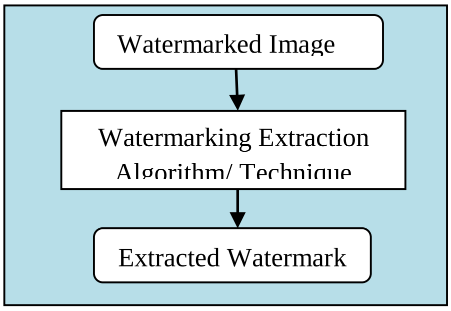

Figure 2: Image extracted watermark

Basically there are two methods for watermarking .i.e. spatial and transform domain. Every method has its own particular favorable circumstances and additionally inconveniences. However, the primary favorable position of change space technique is that it is more robust. Watermark implanting techniques are usually connected in spatial domain [3, 4] or in frequency domain [5, 6]. Though the first is prestigious for its shortcoming in the regular picture dangers, for example, (JPEG) pressure, the last (the frequency domain), has better quality with regards to picture watermarking by modifying their coefficients. This changed area watermarking strategy must need to experience certain strides: 1) the picture must be changed; 2) how to implant the watermark and 3) watermark recuperation plan. Heartiness prerequisites of advanced watermarking calculations worked in recurrence area are much better off than spatial domain systems. To have a productive watermarking method, it ought to be disguised; it can be utilized together with the first picture and ought to give right information [4]. To check whether it is powerful, reproduction (utilizing MATLAB) was utilized for testing different image handling strategies (to embed and extricate watermarks). There are two sorts of image watermarking, one is visually impaired and the other one is non-blind. In visually impaired picture watermarking, there is no prerequisite of unique substance and it is likewise called as open image watermarking. In non-blind image watermarking, there is prerequisite of unique substance and it is otherwise called private image watermarking.

The organization of the remaining section of the paper is done as follows: Section 2 talks about watermarking strategy. Section 3 presents the literature work in the field of watermark by different researchers/ author. In section 4 delineates our proposed methodology for digital watermarking. Section 5 demonstrates the exploratory results and examination of the proposed approach and last section gives overall conclusion of the paper.

II. DIGITAL WATERMARKING TECHNIQUES

2.1 Discrete Wavelet Transform

Discrete Wavelet Transform (DWT) is any wavelet change for which the wavelets are discretely examined [7]. It is helpful for preparing of non-stationary signs. In transform little waves which are called wavelets of shifting recurrence and restricted span are utilized as mother wavelet. Wavelets are made by interpretations and enlargements of a settled capacity called mother wavelet. Wavelet change gives both recurrence and spatial depiction of a picture DWT is the multi determination portrayal of an image the unraveling can be handled consecutively from a low determination to the higher determination The DWT parts the sign into high and low recurrence parts. The high recurrence part contains data about the edge segments, while the low recurrence part is part again into high and low recurrence parts. The high recurrence segments are normally utilized for watermarking since the human eye is less perceptive to changes in edges [9]. In two dimensional applications, for every level of decay, we first play out the DWT in the vertical bearing, trailed by the DWT in the even course. After the principal level of decay, there are 4 sub-groups: LL1, LH1, HL1, and HH1. For each progressive level of deterioration, the LL sub-band of the past level is utilized as the information. To perform second level decay, the DWT is connected to LL1. To perform third level decay, the DWT is connected to LL2 band which break down this band into the four sub-groups – LL3, LH3, HL3, HH3. This outcome in 10 sub-groups per parts. LH1, HL1, and HH1 contain the most elevated recurrence groups present in the picture tile, while LL3 contains the most reduced recurrence band and the estimated image [8]. Following figure demonstrates a 3-level DWT transform of an image.

2.2 Spread Spectrum Transform (SS)-Domain

Another well-known transform-domain scheme is the spread spectrum method proposed by Cox [10],[11]. The term “spread spectrum” is used to name this approach because the watermark is spread throughout the spectrum of an image. The marks are added to the significant DCT components not to the lower magnitude components, which are less visible. The authors argue that because the insignificant components can be attacked with little loss in image quality, they are insecure. Figure 4 shows the basic steps of the embedding process. We first take the transform DCT or DWT of the entire image. Then, select the significant transform components. The zero mean, unit variance Gaussian mark, W, is added to these significant components, X, by the following formula according to the multiplicative embedding rule.

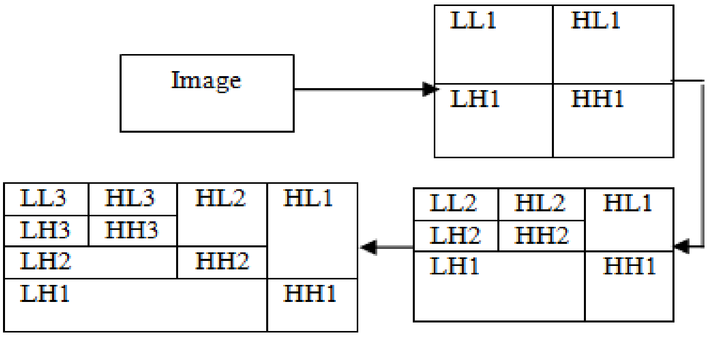

Figure 3: level DWT of IMAGE

$$X'(i, j) = X(i, j)\,(1 + c.\ W(i, j))$$

Where c is a properly chosen value. In their example, the value of c is 0.1. It is clear that a large c would distort the marked image quality.

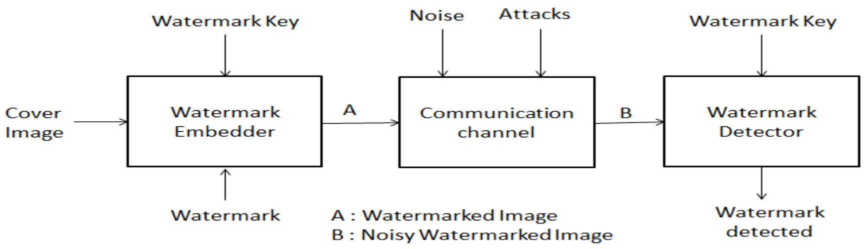

Fig.1:

Figure 4: Watermark Embedding Process

The watermark extracting process is shown in Figure 5. The original image DCT components are needed to retrieve the mark. A correlation can be used to detect the existence of the embedded mark. The standard detection theory can be used to analyze its performance, including error rate, etc. It is reported that this scheme works well under image size scaling, cropping and JPEG compression [10],[11].

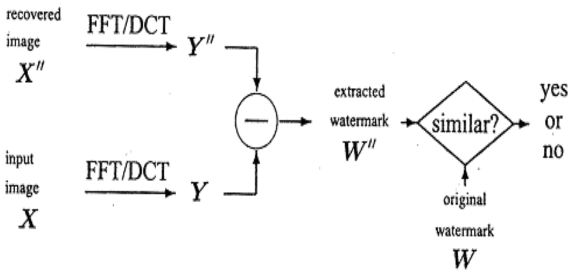

Figure 5: Decoding process of spread spectrum algorithm

2.3 Discrete Fourier Transform (DFT)

Transforms a continuous function into its frequency components [12]. It provides robustness against geometric attacks like scaling, cropping, rotation, translation etc. DFT of an original image is generally complex valued, which results in the magnitude and phase representation of an image. 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. DFT is resistant to cropping because effect of cropping leads to the blurring of spectrum. If the watermarks are embedded in the magnitude, these are normalized coordinates, there is no synchronization are needed. The advantages of this are that it is very helpful in geometric distortions. Drawback is that it is complex to implement and require much computing time.

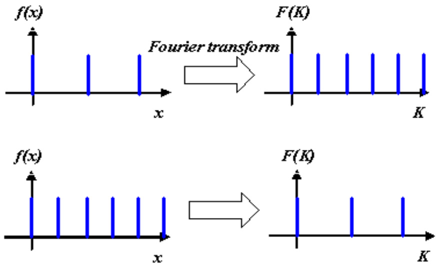

Figure 6: Fourier Transform activity

2.4 Least Significant Bit

The earliest work of digital image watermarking schemes embeds watermarks in the LSB of the pi pixels. Given an image with pixels, and each pixel being represented by an 8-bit sequence, the watermarks are embedded in the last (i.e., least significant) bit, of selected pixels of the image. This method is easy to implement and does not generate serious distortion to the image; however, it is not very robust against attacks. For instance, an attacker could simply randomize all LSBs, which effectively destroys the hidden information. Such an approach is very sensitive to noise and common signal processing and cannot be used in practical applications [13].

III. REQUIREMENTS AND APPLICATIONS OF WATERMATKING

A good watermarking technique is used in various field of security and also has some requirements for implementing it which is describing below [13]:

1. Transparency: The watermark embedded should minimize the quality of images to a minimum rate.
2. Robustness. Embedded watermark should pass through common image processing for example cropping, filtering, rotation, re-sampling, and compression along with interceded attacks.
3. Security: The scheme of watermarking must be secured and protected even if the algorithm of embedding is contrived publically.
4. Appropriate complexity: The additional computation and memory requirements should be concerned for the processes of compression and decompression, primarily for real-time applications.

Digital Image Watermarking is used in many applications. They are as follows:

1. **Digital Rights Management:** It concerns the management of digital rights and the enforcement of rights digitally.
2. **Copyright Protection:** Copyright protection is an important application of digital watermarking. It enables the identification of the copyright owner and thus protects his or her right in content distribution.
3. **Tamper Detection:** Temper detection is used to disclose alterations made into an image. It is closely related to authentication. If tampering is detected in an image, then the image is considered inauthentic.
4. **Broadcast Monitoring:** Over the last few years, the number of television and radio channels delivering content has notably expanded. And the amount of content flowing through these media vehicles continues to grow exponentially. In this highly fragmented and fast changing market, knowing the real broadcast reality has become critical for content owners, copyright holders, distributors and broadcasters [15].
5. **Fingerprinting:** The fingerprint embeds information about the legal receiver in the image. This involves embedding a different watermark into each distributed image and allows the owner to locate and monitor pirated images that are illegally obtained [16].
6. **Medical Application:** Patients Information can be printed on the X-ray reports and MRI scans using techniques of visible watermarking.

IV. PROPOSED METHODOLOGY

4.1 Methodology

The proposed methodology implemented here for the information hiding using a hybrid combinatorial method of applying geometrical attacks to the image and then encryption is done on the attacked image so that the information hide is made secure. Finally the encrypted image is watermarked with the cover image using Spread Spectrum based watermarking.

The proposed methodology implemented here works in the following stages:

1. Initiate steps
2. Take an input image and a secrete image
3. Apply geometric attacks (rotation, translation, cropping etc.) into cover image.
4. Then apply Block Cipher into the attacked cover image to encrypt the data.
5. Apply embedding process on to the cover image with secret data
6. Now for the retrieval of information from the watermarked image, it needs to apply reverse procedure to recover both secret and cover image separately.
7. The received watermarked image and apply to decrypted using the same Block Cipher technique.
8. Now check the geometric attacked cover image and apply same procedure to the remove attack, so that the cover image will get original form as previous.
9. Finally Information retrieval is done using spread spectrum watermarking.
10. To measurement of outcomes:
11. Apply standard MSE formula.
12. Apply standard PSNR formula
13. Apply NC formula
14. Finally compare with previous existing methodology.
15. Finished.

4.2 Performance Metrics

There are various parameters available for measuring the performance of the watermarking but the implementation of the proposed methodology is done using PSNR, MSE and CPU Time parameter. The description about these parameters is given below:

MSE: MSE is the cumulative squared error between the compressed and the original image. Mean square error is substantially a signal fidelity measure. The purpose of a signal fidelity measure is to compare two signals. Consistently, it is pretended that one of the signals is an immaculate original, while other signal is distorted or corrupted by errors. The MSE is given by formula:

Where, *M***N* is the size of image, f(x,y) is the original image and F(x,y) is the reconstructed image.

$$MSE = \frac{1}{m * n} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [(f(x,y) - F(x,y)]$$

PSNR: PSNR is most commonly used to measure the quality of for image confining. The signal in this case is the original data, and the noise is the error received by compression. When analyze compression, PSNR is a human perception of reorganization quality. The PSNR is determined based on colour texture based image segmentation. The PSNR range between [0, 1], the higher is better. PSNR calculate by using formula:-

$$PSNR = 10log_{10}L * \frac{L}{MSE}$$

PSNR is most commonly used to measure the quality of reorganization. The signal in this case is the initial data, and the noise is the error received by confining. Although a higher PSNR mostly illustrate that the reconstruction of the superior quality, in some cases it may not give the superior quality.

Execution Time

It is one of the important parameter to compute the working and performance of the watermarking algorithms in relation with time. It evaluates the amount of time required in embedding process and extraction process of watermark. To measure of execution time CPU cycles are used. General formulae can be used as:

$$Initial\_Time = CPUtime$$
$$Time\_Taken = CPUtime - Initial\_Time$$

REFERENCE

[1] J.L. Liu, D.C. Lou, M.C. Chang, H.K. Tso, ―A Robust Watermarking Scheme Using Self-Reference Image‖, Computer standards and interfaces, vol. 28, issue 3, Jan 2006, pp. 356-367, doi:10.1016/j.csi.2005.07.001.

[2] V. Gupta, A. Barve, ―A Review on Image Watermarking and Its Techniques‖, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), vol. 4, issue 1, January 2014, pp. 92-97.

[3] Z. Tang. and X. Zhang, "Secure Image Encryption without Size Limitation Using Arnold Transform and Random Strategies", Journal of Multimedia, vol. 6, no. 2, (2011).

[4] G.S. Kalra, R. Talwar and H. Sadawarti, "Blind Digital Image Watermarking Robust Against Histogram Equalization", Journal of Computer Science, vol. 8, no.8, (2012), pp. 1272- 1280.

[5] M.F.L. Abdullah, A. A. M. Ukasha and M.F. Mohammed Elbireki, "Image Compression Technique using DCT, FFT Transform", Presentation in National Conference on Electrical and Electronic Engineering (NCEEE) (2012).

[6] G Yuxi and W Yanmin, "DWT Image Watermarking Algorithm Based on Scrambling Algorithm", IEEE Proceedings, World Automation Congress, (2012), pp.1-4.

[7] W. Hong and M. Hang, "Robust Digital Watermarking Scheme for Copy Right Protection", IEEE Trans. Signal Process, 2006.

[8] Deepshikha Chopra, Preeti Gupta, Gaur Sanjay B.C., Anil Gupta, "LSB Based Digital Image Watermarking For Gray Scale Image", IOSR Journal of Computer Engineering (IOSRJCE), ISSN: 2278-0661, ISBN: 2278-8727 Volume 6, Issue 1 (Sep-Oct. 2012), PP 36-41.

[9] Qing Liu, Jun Ying (2012),"Gray scale Image Digital Watermarking Technology Based on Wavelet Analysis"

[10] I. Cox,, M. Miller, et al. "Digital watermarking and Steganography", Morgan Kaufmann, 2008.

[11] N. Cvejic, "Algorithms for Audio Watermarking and Steganography", University of Oulu, Oulu, 2004.

[12] Jalpa M. Patel, "A brief survey on digital image watermarking techniques", International Journal for Technological Research in Engineering Volume 1, Issue 7, March-2014.

[13] Manpreet Kaur, "A study of digital image watermarking", IJREAS Volume 2, Issue 2, Feb. 2012, ISSN: 2249-3905.

[14] G. C. Langelaar, I. Setywan, and R. L. Lagendijk, "Watermarking digital image and video data," IEEE Signal Process. Mag., vol. 17, no. 5, pp. 20-46, Sep. 2000.

[15] Kusuma Kumari B. M, "A Survey of Digital Watermarking Techniques and its Applications", International Journal of Science and Research (IJSR), Volume 2, Issue 12, December 2013.

[16] Vandana Tehlani, "A New Fragile Approach for Optimization in Invisible Image Watermarking by Using Symmetric Key Algorithms", International Journal of Advanced Research in Computer Engineering & Technology, Volume 1, Issue 5, July 2012.

[17] Swati Barwal, Ranjit Kumar, "Adaptive Watermarking Based On DWT with Set Partitioning in Hierarchical Trees", International Journal of Engineering Science and Computing, March 2016.