Image Watermarking Technique for Authenticity

Rajni Bala[1], Suraj Pal[2]
[1]*M. Tech, GCET, Gurdaspur*
[2]*AP. CSE department, GCET Gurdaspur*

Abstract **- Image Watermarking is the way of inserting essential information/logo under an image that can be used to validate its authenticity or the identity of its owners. The straightforward manipulation of data constitutes a real threat for information creators, and copyright owners want to be compensated every time their work is used. Diverse Image watermarking schemes have been proposed in literature. This paper explains the basic idea of spatial domain image watermarking for inserting the message/logo under the image. The performance of the developed watermarking system is assessed in this paper.**

Index Terms **- Watermarking, Spatial Domain, LSB, DCT.**

I.INTRODUCTION

Digital multimedia files like audio, images and videos are easily available to the public user by the boon of internet. Obviously, it leads to unauthorized replication problem. Watermarking is the process of embedding data called a watermark into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. Digital watermarking emerged as a tool for protecting the multimedia data from copyright infringement. In digital watermarking an imperceptible signal ‘‘mark’’ is embedded into the host image, which uniquely identifies the ownership. After embedding the watermark, there should be no perceptual degradation. These watermarks should not be removable by unauthorized person and should be robust against intentional and unintentional attacks. Different watermarking techniques have already been published in the literature [1, 2].

Broadly there are two ways of watermarking that is visible and invisible. Example of visible watermarking is the logo visible superimposed on the corner of television channel in a television picture. On the other hand, invisible watermark is hidden in the object which can be detected by an authorized person. Such watermarks are used for suit the author authentication and detecting unauthorized copying. Digital watermarking is described as one of the possibilities to close the gap between copyright issues and digital distribution of data. It acts as a very good medium for copyright issues as it embeds a symbol or a logo in the form of a watermark, which cannot be altered manually. The digital watermarking technique essentially consists of a watermark inserter and a watermark detector. The watermark inserter inserts a watermark onto the cover image and the watermark detector detects the presence of watermark information/logo. Sometime a watermark key is also used during the process of embedding and detecting watermarks [3]. The watermark key has a one-to-one correspondence with watermark information. The watermark key is private and known to only authorized parties and it ensures that only authorized parties can detect the watermark. The digital image watermarking system is shown in figure 1.

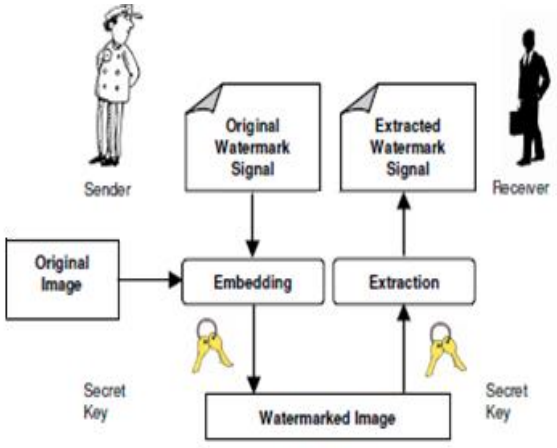

Fig. 1: Digital Image Watermarking

II.SPATIAL DOMAIN WATERMARKING

Image watermarking schemes is classified into spatial domain and transform domain [4]. The spatial domain is the simplest approach to hide data within an image and is called least significant bit (LSB) insertion. The

main strength of pixel domain methods is that they are conceptually simple and have very low computational complexities. However, they also exhibit a major drawback: The need for absolute spatial synchronization leads to high susceptibility to de-synchronization attacks. Here, the secret messages are embedded directly therefore easy to be attacked. It reserves the image quality, increases embedding capacity but is not robust against attack. Potdar used a spatial domain technique in producing a fingerprinted secret sharing steganography for robustness against image cropping attacks. Their paper addressed the issue of image cropping effects rather than proposing an embedding technique. Based on the same embedding capacity, the proposed method improves both image quality and security [5, 6]. In Computer-Based Watermarking, several forms of digital media may be used as "cover" for hidden information. Photos, documents, web pages, and even MP3 music files may all serve as innocuous-looking hosts for secret messages. In covert communications through the Internet, digital images are possibly the most practical type of Watermarking medium primarily due to their sheer abundance in the Web. However, one common problem with using digital images is use of insufficient hiding capacities. Most watermarking software hide information by replacing only least-significant bits of an image with bits from the file that is to be hidden. This technique is generally called LSB encoding.

➢ *Least Significant Bit Insertion*

The LSB is the simplest spatial domain watermarking technique to embed a watermark in the least significant bits of some randomly selected pixels of the cover image. Example of least significant bit watermarking is shown in figure 2.

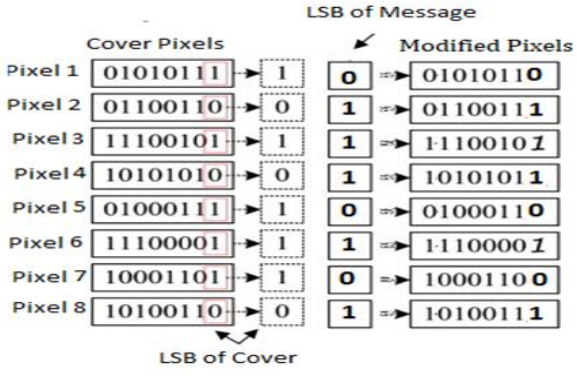

Fig. 2: LSB Image Watermarking

The main advantage of this method is that it is easily performed on images. And it provides high perceptual transparency. When we embed the watermark by using LSB the quality of the image will not degrade. The spatial domain watermarking is simple as compared to the transform domain watermarking. The robustness is the main limitation of the spatial domain watermarking [7].

III.RELATED WORK

Cheng-Hsing Yang [8] proposes a new LSB-based method, called the inverted pattern (IP) LSB substitution approach to improve the quality of the stego-image. Each section of secret images is determined to be inverted or not inverted before it is embedded. The decisions are recorded by an IP for the purpose of extracting data and the pattern can be seen as a secret key or an extra data to be re-embedded.

Chien-Chang Chen and Yao-Hong Tsai [9] presents an adaptive block sized reversible image watermarking scheme. A reversible watermarking approach recovers the original image from a watermarked image after extracting the embedded watermarks. Experimental results show that the proposed adaptive block size scheme has higher capacity than conventional fixed block sized method.

Han-Min Tsai, Long-Wen Chang [10] proposes a secure reversible visible watermarking approach. The proposed pixel mapping function superposes a binary watermark image on a host image to create an intermediate visible watermarked image.

R. Bangaleea and H.C.S. Rughooputh [11] has proposed an algorithm, where a small number of bits are embedded onto an image in the spatial domain using a method similar to the direct sequence spread spectrum. The message bits are modulated with a PN sequence by Spread Spectrum modulation so that the watermark is tamper proof and has anti-jam properties in the transmission channel.

Dipti Prasad Mukherjee [12] have presented an invisible spatial domain watermark insertion algorithm for which we show that the watermark can be recovered, even if the attacker tries to manipulate the watermark with the knowledge of the watermarking process.

Liu and Tan [13] have proposed the use of SVD in watermarking. In their technique, authors find the singular values of the host image and then modify

them by adding the watermark. SVD transform is again applied on the resultant matrix to find the modified singular values. These singular values are combined with the known component for getting watermarked image. This technique shows better robustness against geometric attacks when compared to wavelet based techniques.

IV.RESULTS

LSB algorithms were implemented in MATLAB and performance of the developed system is evaluated.
The Result shown below reveals that the watermarked and original image is perceptually same. This means that minimum degradation occurs when we use LSB watermarking technique. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower the error.

$$MSE = \frac{\sum_{M,N} \quad [I_1(m,n) - I_2(m,n)]^2}{M * N}$$

Where M and *N* are the number of rows and columns in the input images, respectively and $I_1(m, n)$ is the original image, I_2 (m, n) is the watermarked image. The PSNR is calculated using the following equation:

$$PSNR = 10 \left[\frac{R^2}{MSE}\right]$$

Where R represents maximum fluctuation or value in the image, its value is 255 for 8 bit unsigned number. Figure 3 shows the result of LSB scheme.

(a) (b) (c) (d)

Figure.3: LSB Method (a) Original Image (b) Logo (c) Watermarked Image (d) Extracted Watermark

(a) (b) (c) (d)

Figure.4 : LSB Method (a) Original Image (b) Logo (c) Watermarked Image (d) Extracted Watermark

TABLE 1: PSNR & MSE FOR DIFFERENT BIT SUBSITUTION

Method	PSNR	MSE	Embed Time
LSB or 1st Bit	55.9192	0.1664	0.8281
2nd Bit Substitution	50.0900	0.6369	0.8281
3rd Bit Substitution	43.7996	2.7109	0.8281
4th Bit Substitution	38.2486	9.7324	0.8125
5th Bit Substitution	32.4342	37.1247	0.7813
6th Bit Substitution	25.5523	181.0713	0.8750
7th Bit Substitution	20.8188	538.5146	0.7969
MSB or 8th Bit	15.4374	1.8593e+03	0.8594

Table 1 shows the Quality evaluation of developed system with Least significant bit (LSB) to Most significant bit (MSB) insertion. The quality of the watermark image degrades when we go towards MSB insertion. Table 2 and Table 3 shows the quality assessment of developed system for various images.

Table 2: Various Quality Measures of image using LSB Method

Image	PSNR	MSE	Average Difference	Maximum Difference
Lena	58.4	0.0960	-0.1487	0
Pepper	58.1	0.0968	-0.1267	0
Cameraman	58.7	0.0910	-0.1487	0

Table 3: Various Quality Measures of noisy images using LSB Method

Image	PSNR	MSE	Average Difference	Maximum Difference
Lena	18.1	1.01×10^3	-1.6128	191
Pepper	17.6	1.098×10^3	-2.2045	226
Cameraman	18.2	1.03×10^3	-0.7614	170

V.CONCLUSIONS

This paper assessed the developed spatial watermarking scheme. The quality assessment of

developed watermarking system with different bit substitution from LSB to MSB is measured. It is concluded that LSB insertion of watermark create least degradation and watermarked image seem to be same as original image. Similarly the watermark image degrade when we insert the watermark in the consequent bits i.e second towards last (MSB) bit. The quality of watermark image is assessed with various images.

REFERENCES

[1] A. Nikolaidis, S. Tsekeridou, A. Tefas, V Solachidis, "A Survey on Watermarking Application Scenarios and Related Attacks", IEEE international Conference on Image Processing, Vol. 3, pp. 991 – 993, Oct. 2001.

[2] Niu, X., Sun, S., Xiang, W., Multiresolution watermarking for video based on gray-level digital watermark. IEEE Trans. Consumer Electron. 46 (May 2000), 375–384.

[3] E. Vellasques, E. Granger, R. Sabourin, "Intelligent watermarking systems:" a survey, 4th ed., Handbook of Pattern Recognition and Computer Vision, World Scientific Review, 2010, pp. 687–724.

[4] C.S. Lu, S.K. Huang, C.J. Sze, H.Y.M. Liao, Cocktail watermarking for digital image protection, IEEE Trans. Multimedia 2 (4) (2000) 209–224.

[5] C. Rey and JL. Dugelay. A survey of watermarking algorithms for image authentication. *EURASIP Journal on Applied Signal Processing*, 6:613–621, 2002.

[6] C.C. Chang, J.C. Chuang, Y.P. Lai, Hiding data in multitone images for data communications, IEE Proc. Vision Images Signal Process. 151 (2) (2004) 137–145.

[7] Brigitte Jellinek, "Invisible Watermarking of Digital Images for Copyright Protection" submitted at University Salzburg, pp. 9 – 17, Jan 2000.

[8] Cheng-HsingYang , "Inverted pattern approach to improve image quality of information hiding by LSB substitution", Elsevier , Pattern Recognition vol 41 pp 2674 – 2683, 2008.

[9] Chien-Chang Chen and Yao-Hong Tsai, "Adaptive reversible image watermarking scheme", Elsevier, The Journal of Systems and Software vol. 84 pp 428–434, 2011.

[10] Han-Min Tsai, Long-Wen Chang, "Secure reversible visible image watermarking with authentication", Elsevier, Signal Processing: Image Communication vol. 25 pp 10–17, 2010.

[11] R. Bangaleea and H.C.S. Rughoopth, "Performance improvement of spread Spectrum Spatial Domain Watermarking Scheme Through Diversity and Attack Characterization", in IEEE conference Africon , pp 293-298 ,2002.

[12] Dipti Prasad Mukherjee, Subhamoy Maitra and Scott T. Acton, "Spatial Domain Digital Watermarking of Multimedia Objects for Buyer Authentication", in IEEE transactions on multimedia, Vol 6. No. 1, Feb. 2004.

[13] Liu R, Tan T. An SVD-based watermarking scheme for protecting rightful ownership. IEEE Transactions on Multimedia 2002; 4(1):121-8.