International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 13 (2014), pp. 1237-1244

http://www. irphouse.com

Performance Evaluation of LSB Technique for Digital Watermarking

Neha Bansal[1], Vinay. K. Deolia[2], Atul Bansal[3] and Pooja Pathak[4]

[1, 2, 3, 4]GLA University, Mathura, India

Abstract

Watermarking of digital content is an imperative and interactive method for identification and protection of digital data. It allows veritable watermarks to be hidden in digital data for example image, audio, and video. Procedure of embedding and extracting of watermark from original image and watermarked image is complex. These include randomization of the watermark and selection of locations to embed and extract it from the specific locations. Proposed work gives a robust digital watermarking algorithm that follows Least Significant Bit Technique. Embedding of watermark is done at the least significant bit of each pixel value of the cover image. Watermarked image is used to extract the watermark without any help of the original image. Parameters used to evaluate the performance watermarking technique are Peak Signal to Noise Ratio, Mean Square Error and Normalized Cross Correlation for Gaussian noise, Poisson noise, Salt and Pepper noise and Speckle noise.

***Index Terms*--** Digital Watermarking, Least Significant Bit (LSB) technique, Mean Square Error (MSE), Normalized Cross Correlation (NC), Peak Signal to Noise Ratio (PSNR).

INTRODUCTION

Digital content, with the appearance of Internet and swift evolution of information technologies, has become a fundamental part of one's day to day life. As it is easy to make an exact copy of the digital contents, illegitimate sharing and replication of digital contents has become major concern for authors, publishers and legitimate owners of the contents [1]. It has become imperative to maintain the intellectual characteristics of digital content of a given media. In the beginning, ciphering and control access methods were used to save from harm the authenticity of digital content of a given media [4]. But this avoids free sharing and transmission of the content through the network, which is most of the time not preferable to the author of

the content. To deal with the crisis, digital watermark has been proposed [1]. Watermarking is the procedure of adding concealed information by modifying the pixel values of an image with least amount of perceptual interruption. A recent survey of major techniques appears in [2]. Some preferable features of valuable watermarking methods include robustness, imperceptibility and security. Imperceptibility is the measure of perceptual resemblance between the cover and watermarked signals. The watermark can be made imperceptible under untailored observation by embedding the watermark in a discreet, self-effacing manner. The strength of the watermark against manipulations is that it is robust to linear and nonlinear filtering, lossy compression, cropping and scaling. The capability of the watermark to oppose antagonistic attacks is known as Security. Attacks are not restricted to elimination of the watermark content, but they also comprise watermark falsification or estimation, collusion, and uncertainty attacks. Obviously, it is preferable to have a robust, imperceptible and secure watermarking technique [4] [10].

Visible and invisible are the broader classification of Watermarks. Visible watermark is seen with the content of the image and unauthorized removal of the same, causes' damage to the image. Example of such scheme is the IBM digital watermarking scheme for the Vatican library. Invisible watermarking is required for copyright protection specially in multimedia products. Though the Watermark modifies an image, it should not degrade the image as seen by human eye. Some of the basic requirements of a good watermark are given in [5]. Firstly, the watermark must not corrupt the image as seen by human, although the watermark has customized the digital image. Secondly, the message embedded in the watermark must not be accessible by unauthorized persons, while at the same time authoritative persons should be capable to reconstruct the watermark for ownership identification from the watermarked image. Thirdly, the watermark data embedded in the image must remain same in the digital content even when the image is subjected to various processing operations for example linear transformation and compression [14].

Invisible watermark has a broader and general application when compared to visible watermark which is generally applied for image ownership identification. The exploitation of the human psycho-visual characteristics for example visibility threshold, visual masking, and brightness adaptation defines the success of invisible data embedding in images. These imperfections of the human visual system (HVS) have been fully exploited in image bandwidth (or data rate) reductions, i. e., details of the image which cannot be seen by the human eye are not included in the encoded image for transmission and viewing. The insertion of watermark to the image data will surely damage the image, but if the embedded data has energy in the region of 30 dB or more below the peak signal energy of the image, the signature can be encoded and concealed in the image without causing perceptible interruption to the viewer [18]. If the embedding algorithm or key is made available to the computer, it can of course totally recognize the embedded data. The prime aim of data embedding can be summarized as being authenticity protection. It is unavoidable to remove the embedded data by pirates of the images. Using these data embedding schemes it is difficult to remove the embedded data by plagiarizes of the images without leaving

some damage on the reproduced copies. This requires that the embedding schemes should be robust against interruption. An outstanding review of this feature and other issues of ownership protection can be found in [6] [7].

A robust watermarking algorithm based on LSB is used in this paper. In this method pixel values of cover image and watermark image are processed. Values of cover image pixels and watermark image pixels are converted into binary. After conversion, LSB of each pixel of cover image is replaced by each bit of watermark image. Experimental result shows the performance of the LSB watermarking technique for various attacks as Gaussian noise, Poisson noise, Salt and Pepper noise and Speckle noise in terms of Peak Signal to Noise Ratio, Mean Square Error and Normalized Cross Correlation.

This paper is organized as follows: Section II introduces the proposed approach for digital watermarking; the watermarking using LSB is shown in Section III, the simulation results are shown in Section IV, the conclusion is given in Section V.

PROPOSED APPROACH FOR DIGITAL WATERMARKING

Various data embedding schemes are used for watermarking, many of which are simple to implement while others are more difficult. Embedding schemes can be freely classified into two domains; one of them works in the spatial domain and the other one works in the frequency (or transform) domain. In the spatial domain, the pixel values in arbitrarily chosen sections of the image are customized based on the watermark preferred by the author of the product [7]. In the spatial domain, during watermark embedding, host signal is not transformed. The main potencies of pixel domain methods are that they are theoretically simple and have very low computational complexities. The block diagram of a spatial-domain digital watermarking system is shown in Fig. 1 [8].

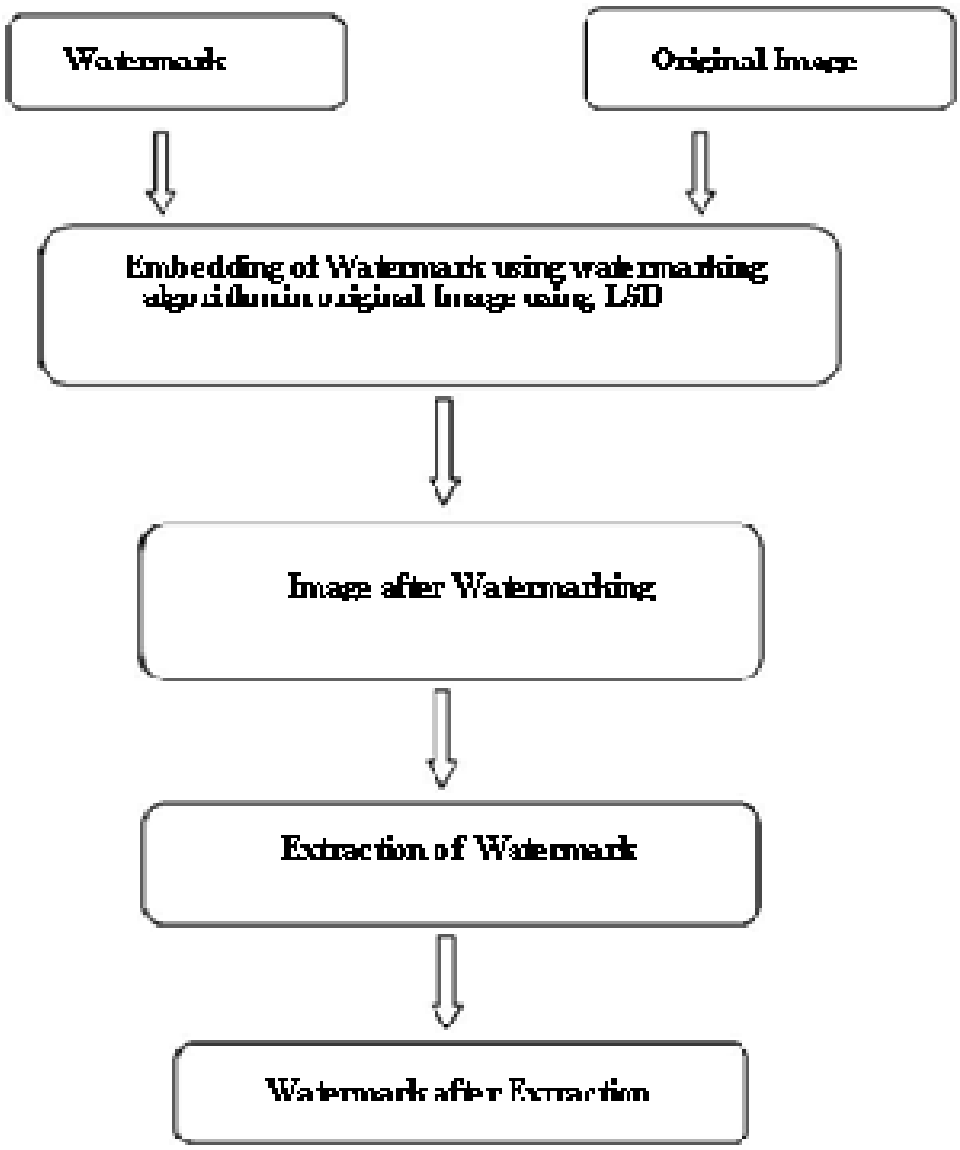

Fig. 1. Block diagram of a spatial domain watermarking system

WATERMARKING USING LSB

In the proposed method, pixel values of cover image and watermark are converted into binary. The cover image is of size m x n and the watermark image is of size (m x n)/8. The least significant bit of each pixel of cover image is replaced by the each bit of watermark image. In this way watermark is embedded and watermarked image is obtained. The process is shown in Fig. 2.

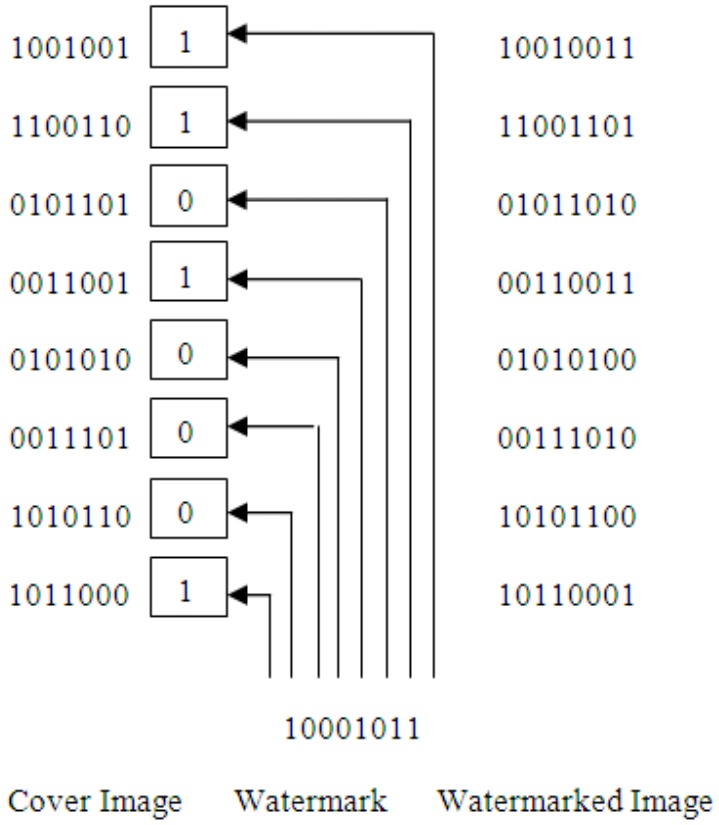

Fig. 2. Process of LSB watermarking using 8th bit

At extractor end, the watermark is extracted by replacing the least significant bit of the watermarked image by a zero matrix which is of equal size to the watermark.

There will be no distortion for the watermarked images because of no deviation between the images after watermarking and before watermarking. We got the result after we calculated the Normalized Cross correlation (NC) and Peak signal-to-noise ratio (PSNR). PSNR values are used to examine the excellence of the images after watermarking. The degree of excellence of regeneration in compression of image can be used as Peak signal-to-noise ratio. The PSNR values of two images K and I of size m x n is most commonly defined by the Mean Squared Error where one image is considered as a noisy approximation of the other image (Also known as, I is the cover image and K is the image after watermarking) [8]. MSE is defined as the following [9]:

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

The PSNR is defined as:

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

and the NC is defined as:

$$NC = \frac{P.Q}{R} \quad P = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[M(i,j)M'(i,j)]$$

$$Q = \sqrt{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}M(i,j)^2} \quad R = \sqrt{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}M'(i,j)^2}$$

Where $M(i,j)$ is the actual watermark, $M'(i,j)$ is the watermark after extraction and the size of the watermark is m x n.

Typical values for the PSNR are between 30dB and 40dB. If the watermarked image has PSNR deviation more than 30, it is difficult to detect the deviation between the cover image and image after watermarking by the human eyes [8] [9]. In this paper performance is evaluated for four attacks which are Gaussian noise, Poisson noise, Salt and Pepper noise and Speckle noise.

SIMULATION RESULTS

In this section, the simulation results are shown for images before watermarking, after watermarking and watermark after extraction by calculating the values of MSE, PSNR and NC parameters. Image quality can be compared by using the values of MSE and PSNR. This parameter is used to examine the superiority between the Images before watermarking and after watermarking.

Cover Image

Watermark Image

Watermarked Image without noise

With Gaussian Noise

With Poisson Noise

With Salt and Pepper Noise

With Speckle Noise

Fig. 3. Watermarking results using 8th bit

TABLE I MSE, PSNR AND NC VALUES FOR VARIOUS ATTACKS

Attacks/ Parameters	Without any attack	Gaussian attack	Poisson attack	Salt & Pepper attack	Speckle attack
MSE	0. 0041	638. 1393	107. 5751	962. 566	553. 9072
PSNR (db)	165. 8081	46. 2397	64. 0434	42. 1292	47. 6553
NC	1	0. 6696	0. 7796	0. 9891	0. 733

CONCLUSION

LSB based digital watermarking scheme is used in this work. The simulation result illustrates that the proposed watermarking algorithm preserves the superiority of the image after watermarking for Gaussian attack, Poisson attack, Salt and Pepper attack and Speckle attack. The values of Peak signal-to-noise ratio (PSNR) and Normalized Cross correlation (NC) are used to evaluate the proposed watermarking algorithm. Therefore, watermark can be inserted inside the image by using this digital watermarking algorithm. In the proposed algorithm, the size of watermark is very small. Large images can be taken as a watermark for future work.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the support of Prof. T. N. Sharma, Head ECE Department, Prof. A. S. Jalal, Head CEA Department and Dr. Sanjay Maurya, Associate Professor, EN Department, GLA University Mathura for their contribution in this work.

REFERENCES

[1] C. Y. Chang and S. J. Su, “The Application of a Full Counterpropagation Neural Network to Image Watermarking”, IEEE (2005), pp. 993-998.

[2] Wai C. Chu, “DCT-Based ImageWatermarking Using Subsampling”, IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 5, NO. 1, MARCH 2003, pp. 34-38.

[3] Chih-Wei Tang and Hsueh-Ming Hang, “A Feature-Based Robust Digital Image Watermarking Scheme”, IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL. 51, NO. 4, APRIL 2003, pp. 950-959.

[4] Maher EL’ARBI, Chokri BEN AMAR and Henri NICOLAS, “Video Watermarking Based On Neural Networks”, IEEE(2006), pp. 1577-1580.

[5] J. J. K. O’Ruanaidh et al., “Watermarking digital images for copyright protection”, IEEE Proc. Vis. Image Signal Process., Vol. 143, 1996, pp. 250-256.

[6] M. D. Swanson, M. Kobayashi and A. H. Tewfik, “Multimedia data-embedding and watermarking techniques”, IEEE Proc., Vol. 86, 1998, pp.

1064-1087.

[7] W. N. Cheung. "Digital image watermarking in spatial and transform domains", 2000 TENCON Proceedings Intelligent Systems and Technologies for the New Millennium (Cat No00CH37119), 2000

[8] Zhang Zhi-Ming, Li Rang-Yan, Wang Lei, "Adaptive Watermark Scheme with RBF Neural Networks, " in Proc. 2003 International Con$ Neyral Networks and Signal Processing, 2003, vol. 2, pp. 1517-1520

[9] J. W Bae, S. H. Lee and J. S. Yoo "an efficient wavelet based motion estimation algorithm", IEICE transaction INF & SYST Vol E88-D, NO1, January 2005.

[10] Puneet Kr Sharma and Rajni, "Information security through Image Watermarking using Least Significant Bit Algorithm, " Computer Science & Information Technology, vol. 2, no. 2, May 2012.

[11] Malihe Soleimani, Faezeh Sanaei Nezhad, Hadi Mahdipour and Morteza Khademi, "A Robust Digital Blind Image Watermarking Based on Spread Spectrum in DCT Domain, " Science Academy Transactions on Computer and Communication Network, vol. 2, no. 2, June 2012, pp. 122-126.

[12] Mrs. Rekha Chaturvedi, Mr. Abhay Sharma, Mr. Naveen Hemrajani, Mr. Dinesh Goyal, "Analysis of Robust Watermarking Technique using Mid-band DCT domain For different image formats, " International Journal of Scientific and Research Publications, vol. 2, no. 3, March 2012.

[13] Thanuja T C, P Nagaraju, Vinay J, Kavya N Bhushan and Naren S Vasanad, "Hardware Implementation of a Robust Modulo Watermarking Algorithm, " MES Journal of Technology and Management, vol. 2, no. 1, 2011, pp. 51-56.

[14] S. Craver, N. Memon, "Resolving Rightful Ownership with Invisible Watermarking Techniques: Limitations, Attacks and Implications", IEEE Trans., vol 16, No. 4, 1998, pp. 573-586.

[15] M. Alghoniemy and A. H. Tewfik, "Image watermarking by Moment invariants, " in Proc. IEEE Int. Conf. Image Process., vol. 2, Jan. 2001, pp. 73–76.

[16] M. Shiang Hwang, C. Chang and K. Hwang "Digital watermarking of images using neural networks", Journal of Electronic Imaging Volume 9, Issue 4, October 2000, pp. 548-555.

[17] F. C. Mintzer et al., "Toward on-line world wide access To Vatican library materials", IBM J. Research and Development, Vol. 40, 1996, pp. 139-162.

[18] Mohamed Ali HAJJAJI Abdellatif MTIBAA El-bey BOURENNANE, "A Watermarking of Medical Image: Method Based "LSB"", Journal of Emerging Trends in Computing and Information Sciences, VOL. 2, NO. 12, December 2011, ISSN 2079-8407, pp. 714-721.