ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

Quality Evaluation for LSB Replacement Watermarking of Grayscale Images

Deepshikha Chopra[1], Rajesh Purohit[2], Gaur Sanjay B.C.[3]

M.Tech Scholar, CSE, Jodhpur Institute of Engineering & Technology, Jodhpur, India [1]

HOD, CSE, MBM Engineering College, Jodhpur, India [2]

HOD, ECE, Jodhpur Institute of Engineering & Technology, Jodhpur, India [3]

Abstract: The recent progress in the digital multimedia technologies has offered many facilities in the transmission, reproduction and manipulation of the data. However, these advancements have also brought the problems such as content protection for content providers. Digital watermarking is one of the proposed solution techniques for copyright protection of multimedia. This paper presents the general overview of LSB image watermarking. Distortions introduced due to various attacks and measures robustness of the watermark are evaluated. Comparisons are made by quality determining factors known as MSE and PSNR. This work has been implemented in MATLAB R2008a.

Keywords: Digital Watermarking, JPEG, MSE, PSNR, LSB, HVS

I. INTRODUCTION

The application of digital media has grown immensely in past few years. Many inexpensive methods are readily available for synthesizing and editing digital images very easily. Unlike analog information the reproduction of digital images is simple and robust [1]. The copying of digital images which are identical to original ones can be easily made (piracy). Unfortunately, the very same properties that make a digital media element attractive for use and distribution also facilitate the unauthorized use, misappropriation and misrepresentation [2]. Thus, there is a great interest in developing technology that will help to protect the integrity of a digital image and intellectual property rights of its owner [3].

Digital watermarking is embedding the signal (known as watermark) into the original image or base image to ensure protection against various attacks [4]. The problem with the traditional way of printing logos or names is that they may be easily tampered or duplicated [5]. In digital watermarking actual bits are scattered in the image in such a way that they cannot be identified and show resilience against attempts to remove the hidden data. Digital watermarking is a very active and interesting area [6].

II. RELATED WORK

In Spatial Domain, LSB substitution techniques [7,8] can be used to embed the secret data in cover image. in LSB technique 1 bit of secret message can be inserted replacing the least significant bit of cover image pixels. LSB technique is relatively simpler and has low computational complexity [9].

Syndel *et. al* proposed a technique in which watermark is generated using m-sequence generator. The watermark was embedded to Least Significant Bits (LSB) of the original image to produce the watermarked image. The watermark was extracted from a suspected image by taking least significant bits at proper locations. Detection was performed by cross- correlation of the original and extracted watermark. They showed that resulting image contained an invisible watermark with simple extraction procedures. But the watermark was not robust to additive noise [10]. Hajiaji *et. al* proposed watermarking of medical images, in which set of data is inserted into medical image. This method is based on LSB to check integrity and confidentiality of medical information of the patient and hospital data. Puneet Sharma *et. al* proposed image watermarking and its security issues. To hide the logo (secret image) into cover image they used LSB algorithm. LSB of each of the pixel of the cover image is replaced by the bits of secret image [11]. One of the earliest proposed technique was Image Downgrading given by Kurak and McHughes [12] to embed LSB.

III. WATERMARKING SCHEME

The scheme aims to replace the bits of original image with the bits of watermark image. As the number of bits replaced increases watermark becomes visible from invisible. This scheme is based on Steganographic technique proposed by N.F. Jhonson *et. al* [13]. In simplest case, the sender uses all base image bits for inserting the watermark bits, starting at the first element. The substitution is performed between base image and watermark image elements. One could also imagine a substitution operation which changes more than one bit of the base image, for instance two least significant bits of base image replaced by two most significant bits of watermark image. The extraction process is exactly reverse of substitution operation. The LSB of the selected base image are extracted and lined up to reconstruct the watermark. The basic scheme is shown in algorithm below used for embedding and extraction.

Algorithm

1. Read Base Image and Watermark Image.
2. Convert Images to Grayscale Images.
3. Get the Size of Base Image and Watermark Image.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

4. n ← Size of Base Image / Size of Watermark Image
5. if n<=0
    Watermark not in position
6. else if n>=1
    (a) Current bit of watermark ← 1
    (b) LSB (Current bit of Base Image) ←
    (current bit of watermark)
    (c) Embed the Watermark into Base Image
    (d) Current bit of Watermark+1
      Current bit of Base Image +1
    (e) n—
7. Stop

IV. EXPERIMENTAL ANALYSIS

In our Experimental analysis, we have 256*256 grayscale BMP image which is shown in figure 1 used as base image. We have tested watermark image insertion of different sizes. The watermarks used are of same size as that of base image and smaller size than base image as shown in figure 1. Table 1 shows the size of base image, watermarks used and the obtained sizes of watermarked images. The *capacity* of the algorithm is tested by increasing or decreasing the sizes of watermarks used. The maximum capacity is same as that of size of base image and the minimum capacity obtained is 30 bytes.

(a) (b) (c)

Fig. 1(a) Base Image (b) Small Watermark (c) Large Watermark

TABLE I
The Size of Base Image and Watermark Images

Size of Base Image	Base Image in bytes	Size of Watermark	Watermark in bytes	Size of Watermarked Image	Watermarked Image in bytes
256*256	65536	256*256	65536	256*256	65536
256*256	65536	150*150	22500	256*256	65536

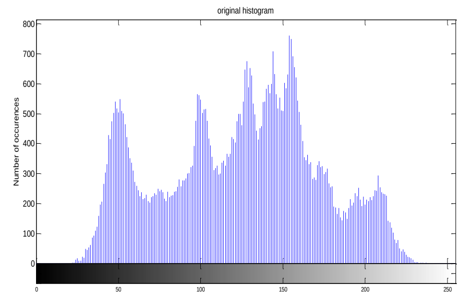
The watermark recovered is of size 524288 bytes and of 256*256.

The visibly watermarked images of small and large watermark are shown in figure 2 below. The results obtained vary largely. On increasing the number of bits substituted of watermark from base image the watermark turned visible from invisible. But the best results are obtained for invisible watermarking. At first bit substitution the watermark remains invisible, at second bit also watermark remains visually unnoticeable, similarly at third bit substitution also no changes are seen. At fourth bit substitution the watermark becomes noticeable by HVS (Human Visual System).

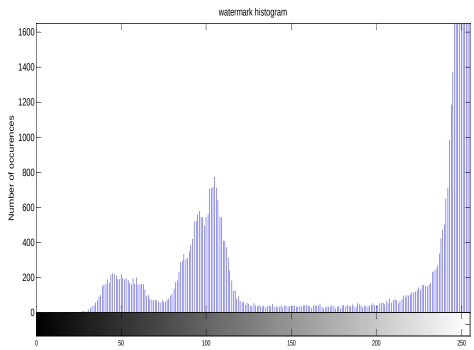
(a) (b)

Fig. 2 Watermarked Image at Bit = 7 Substitution (a) With Small Watermark (b) With Large Watermark

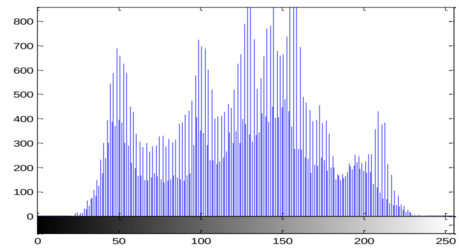
The histogram plots are made to obtain the pixel intensity variations. Histogram plots for watermarked images as compared to original image and recovered watermark images as compared to watermark inserted are shown in figures. Fig. 3 indicates bitwise pixel intensity changes due to bit replacement increment large Watermark Insertion. From histograms it can be evaluated that pixel intensity level is decreased on increasing the number of bits replaced of watermark. Fig. 4 shows the histogram plot of the recovered large watermark, it has plots on boundaries only because the recovered watermark has only black and white colours, middle range values for different intensity is not present in recovered watermark. Hence the recovered watermark is not of very good quality.



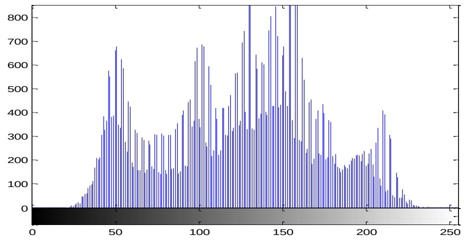
(a)Base Image



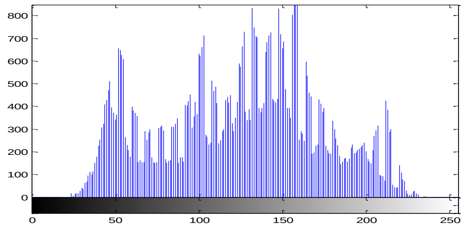
(b)Watermark (Large Sized)



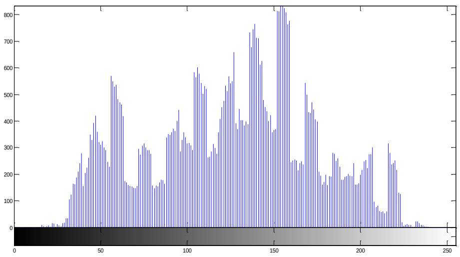
(c) Bit=1



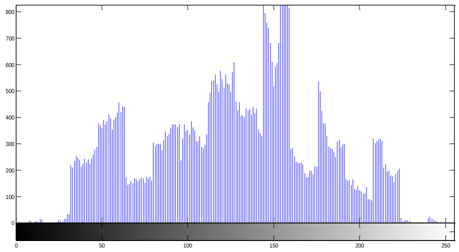
(d) Bit=2



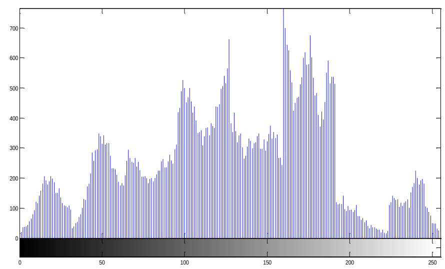
(e) Bit=3



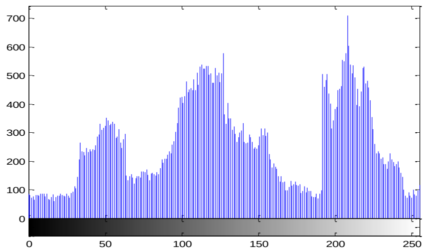
(f) Bit=4



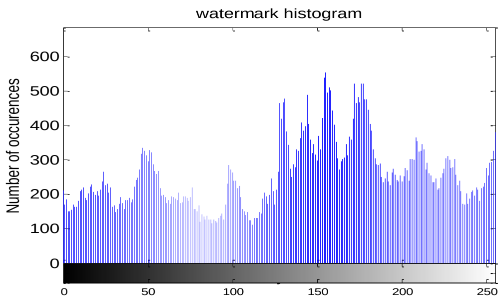
(g) Bit=5



(h) Bit=6



(i) B=7



(j) Bit=8

Fig. 3 Histogram Plot to show the Pixel Intensity Variations on Bitwise Substitution for Watermarked Image with Large Watermark

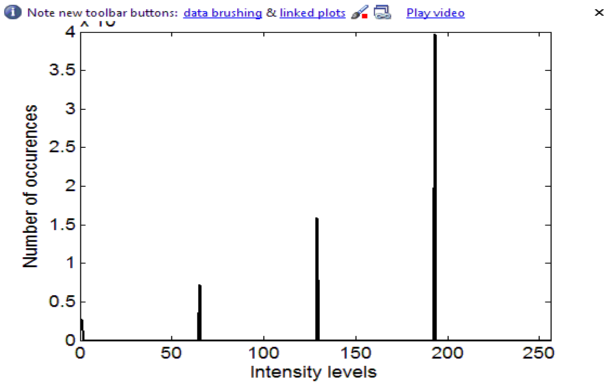
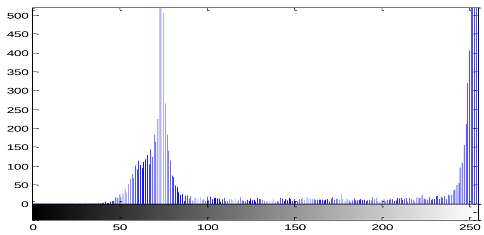
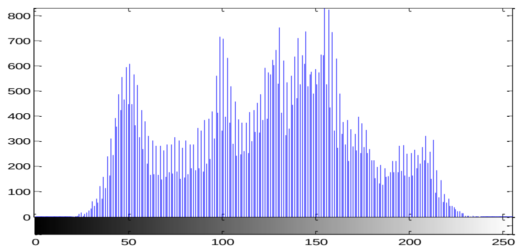


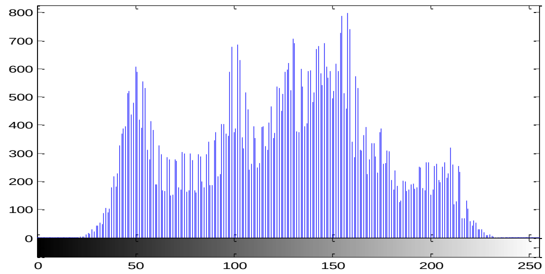
Fig. 4 Histogram Plot For Recovered Large Watermark



(a) Small Watermark



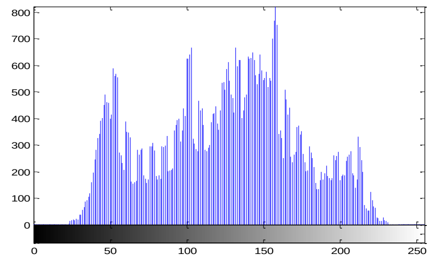
(b) Bit=1



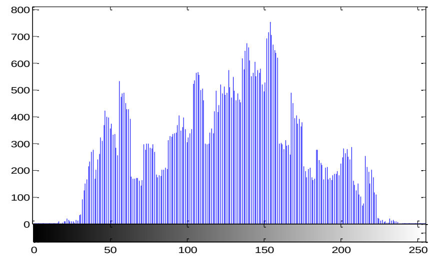
(c) Bit=2

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

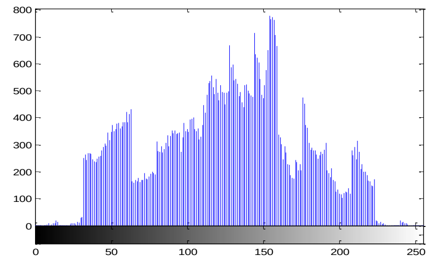
ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940



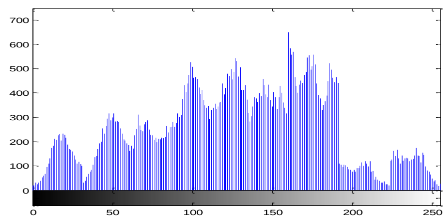
(d) Bit=3



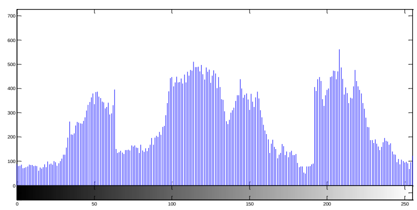
(e) Bit=4



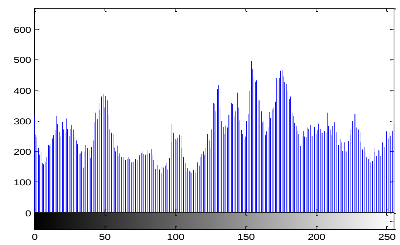
(f) Bit=5



(g) Bit=6



(h) Bit=7



(i) Bit=8

Fig. 5 Histogram Plot for Watermarked Images with Small Watermark with Bitwise Substitution Variation

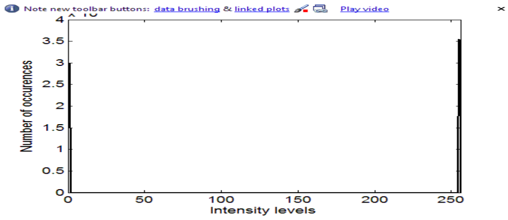


Fig 6 Histogram Plot for Recovered Small Watermark

Fig. 5 shows the histogram plots for watermarked images with small watermark. Fig. 6 shows the histogram plot for recovered watermark for small watermark. The watermark recovered has only black and white pixels therefore the plot is at the boundary only for all bits being replaced (varying).

Imperceptibility of watermark is tested by comparing the watermarked images with original one. Embedded watermark is imperceptible if it does not alter the watermarked image contents. The visible watermark is not imperceptible. Imperceptibility is analysed by MSE and PSNR values. In the MSE, we will often refer to the error signal e_i,= $x_i - y_i$, which is the difference between the original and distorted signals. the MSE may also be regarded as a measure of signal quality. The PSNR is useful if images having different dynamic ranges are being compared, but otherwise contains no new information relative to the MSE.

$$MSE(\mathbf{x},\mathbf{y}) = \frac{1}{N}\sum_{i=1}^{N}(x_i - y_i)^2 \qquad (1)$$

$$PSNR = 10\log_{10}\frac{L^2}{MSE} \qquad (2)$$

TABLE II
MSE and PSNR Values for Large Watermark Embedded

Bit Substitution	Large Watermark embedded	
	MSE	PSNR
1	0.49	50.24
2	1.96	45.24
3	8.03	39.12
4	30.45	33.33
5	120.3	27.36
6	180.34	20.34
7	200.75	15.15
8	250.14	10.12

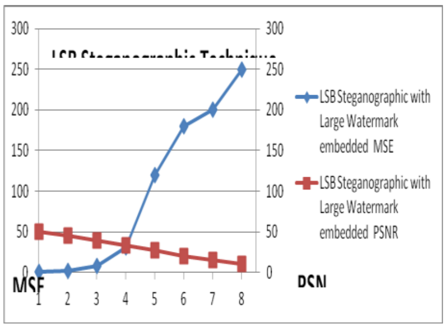


Fig. 7 MSE and PSNR values Plot to determine the Optimal Point with Large Watermarked Image

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

TABLE III
MSE and PSNR Values for Small Watermark Embedded

Bit Substitution	Small Watermark Embedded	
	MSE	PSNR
1	0.3	51.11
2	1.81	45.19
3	7.9	39.06
4	30.28	34.34
5	127.9	26.97
6	179.56	19.59
7	199.69	11.17
8	249.98	9.29

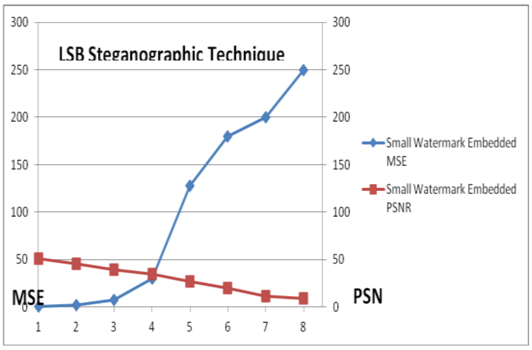


Fig. 8 MSE and PSNR values Plot to determine the Optimal Point with Small Watermarked Image

The algorithm is proved optimal on a point at which it has maximum performance. *Optimality* of algorithm is obtained on the basis of its performance measures made by MSE and PSNR values. The bit replacement at which MSE and PSNR values obtained are same is optimal point. The optimal point is obtained at bit four replacement at which signal noise ratio and difference between base image and watermarked image are obtained same. As shown in Fig. 7 and Fig. 8 plotted on the basis of Table II and Table III.

V. CONCLUSION

The ongrowing Internet era has mande it very easy to modify and transmit the images. Watermark is the method to provide robustness, authentication, copyright against such attacks. This Paper Evaluates the Capacity of Watermarking scheme. The Bitwise Replacement effect is analysed by histogram plots. The small and large watermark usage is evaluated. The imperceptibility is analysed by using traditional MSE and PSNR method. The optimal point of algorithm is determined when the performance of the algorithm is most optimal. The tool used for execution is MATLAB R 2008a.

REFERENCES

[1] Deepshikha Chopra, and Preeti Gupta, "LSB Based Digital Image Watermarking for Grayscale Images", IOSRJCE, vol. 3, issue 6, pp. 9-30, Sept-Oct 2012.

[2] Deepshikha Chopra, Rajesh Purohit, and Gaur Sanjay, "Evaluation of LSB Watermarking Scheme for Grayscale Images", IJRIT, vol. 2, issue 4, pp. 114-121, April 2014.

[3] R.B. Wolfgang, C.I. Podichulk, and E.J. Delp, "Perceptual Watermarks for Digital Images and Video", proc. Of IEEE, vol. 87, no. 7, pp. 1108-1126, July1999.

[4] Mandhani., "Watermarking using Decimal Seuences", Master Thesis submitted to the Graduate Faculty of Louisiana State University, India, 2003.

[5] Katzenbeisser, and Petitcolas, "Information Hiding Techniques for Steganography and Digital Image /watermarking", Artech House Publishers, 2000.

[6] Nagra, Thomson, and Collberg, "A Functional Taxonomy for Software Watermarking", in proc. Of 25th Australian Computer Science Conference, ACS, pp. 177-186, 2002.

[7] C.K. Chan, and Cheng, "Hiding Data in Images by Simple LSB substitution", Pattern Recognition, pp. 469-474, 2004.

[8] N. Nikoliads, and I. Pitas, "Robust image Watermarking in Spatial Domain", Signal Proc., vol. 666, no. 3, pp. 385-403, May 1998.

[9] Vidysagar M. Potdar, Somg Han, and Elizabeth Chang, "A Survey of Digital Image Watermarking Techniques", 3rd IEEE International Conference on Industrial Informatics (INDIN), pp. 709-716, 2005.

[10] R. Schyndel, A. Tirkel, and Osborne, "A Digital Watermark", proc. IEEE Int. Conf. on Image Processing, vol. II, pp. 86-90, Nov. 1994.

[11] M. A. Hajijai, A. Mtibba, and E. Bourennane, "A Watermarking Of Medical Image Based LSB", Journal of Engg. Trends in Computing and Information Sciencees, vol. 2 , No. 12, pp. 714-721, Dec. 2011.

[12] Kurak, and Mchughes, "A Cautionary Note on Image Downgrading", in proc. Of IEEE Computer Society Applications Conference, vol. 2 IEEE Computer Society Press, CA, 153-159, 1992.

[13] N.F. Jhonson, and S.C. Katezenbeisser, "A Survey of Steganographic Techniques" in Information Techniques for Steganography and Digital Watermarking, MA: Artec House, Dec. 1999, pp. 43-75.