International Journal of Computer and Communication Technology

Volume 6 | Issue 1 Article 2

January 2015

Modified LSB Watermarking for Image Authentication

R. AARTHI
Department of Information Technology, Velammal College of Engineering and Technology, Madurai, India, aarthiramasami@gmail.com

V. JAGANYA
Department of Information Technology, Velammal College of Engineering and Technology, Madurai, India, jaganyavijayan@gmail.com

S. POONKUNTRAN
Department of Information Technology, Velammal College of Engineering and Technology, Madurai, India, s.poonkuntran@gmail.com

Modified LSB Watermarking for Image Authentication

[1]R.AARTHI, [2]V. JAGANYA, & [3]S.POONKUNTRAN

Department of Information Technology, Velammal College of Engineering and Technology, Madurai, India
E-Mail - aarthiramasami@gmail.com, jaganyavijayan@gmail.com, s.poonkuntran@gmail.com

Abstract - This paper mainly aims at developing an authentication scheme for digital images. The LSB scheme is chosen base for our proposed work. Through literature survey it is found that conventional LSB scheme provides low embedding rat low distortion and is irreversible. Because of its irreversibility, the conventional LSB scheme cannot be used for critic applications where reversibility is mandatory. Through this literature survey, we learnt that this conventional LSB scheme us only one bit in every pixel for embedding. Our proposed scheme presents a modified LSB embedding strategy that satisfies tl reversibility and improves the embedding rate by using two bits in every pixel for embedding.

***Key words**: LSB, reversibility, watermarking, authentication, selection strategy, secret data, PSNR*

I.INTRODUCTION

[1] is a method of embedding useful information into a digital work (especially, thus, audio, image, or video) for the purpose of copy control, content authentication, broadcast monitoring, etc. The distortion introduced by embedding the watermark is often constrained so that the host and the watermarked work are perceptually equivalent. However, in some applications, especially in the medical, military, and legal domains, even the imperceptible distortion introduced in the watermarking process is unacceptable. This has led to an interest in *reversible* watermarking [2]-[6], where the embedding is done in such a way that the information content of the host is preserved.

This enables the decoder to not only extract the watermark, but also perfectly reconstruct the original host signal from the watermarked work.

II. TRADITIONAL LEAST SIGNIFICANT BIT

The least significant bit (LSB) technique is used to embed information in a cover image. The LSB technique is that inside of a cover image, pixels are changed by bits of the secret message. These changes cannot be perceived by the human visibility system. However, a passive attacker can easily extract the changed bits, since it has performed very simple operation.

For example, Figure 1 shows the 1-bit LSB. In Figure 1, LSB can store 1-bit in each pixel. If the cover image size is 256 x 256 pixel image, it can thus store a total amount of 65,536 bits or 8,192 bytes of embedded data.

Digital watermarking

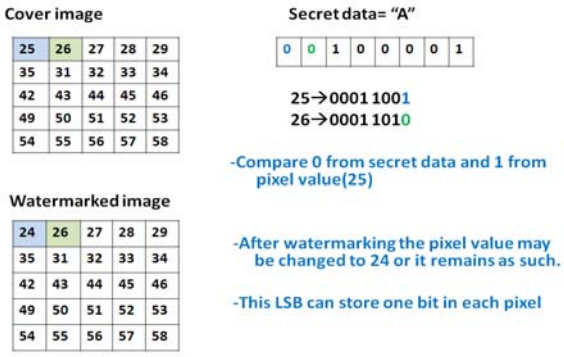

Figure 1 An example of 1 bit LSB.

III. MODIFIED LEAST SIGNIFICANT BIT

A. Reversibility

After the secret data gets embedded or hidden in the cover image, the original cover image will get modification to some extent with respect to the length of the secret data. At the receiving end we are not able to get back the original cover image since our traditional LSB is not providing reversibility. Reversible feature is a process of getting back the cover image from the watermarked or embedded image at the extraction phase. After getting the watermarked image, we need to create a matrix initialized with zeros, whose dimension is equal to the watermarked image. By XOR-ing each and every pixel of both the original and watermarked image, the result will be stored in the corresponding positions in the newly created matrix. This matrix will also be sent to the extraction phase along with the watermarked image. During extraction the value of the newly created matrix will be checked. If it is 1, then watermarked image's s LSB of each pixel

must be changed, else vice versa. Finally we could get back the original cover image.

B. Boosting the capacity of the scheme

Most of researchers have proposed the first LSB scheme but our proposed watermarking algorithm is using the third and fourth LSB for hiding the data. Our algorithm can store 2-bits in each pixel. If the cover image size is 256 x 256 pixels image, it can thus store a total amount of 1, 31,072 bits secret data which is double the number of bits stored by traditional LSB. First, we select the image as shown in figure 2 and then we will convert the data to binary value as shown in the figure 3. Then, we hide the data in the image using the proposed algorithm. Then, we will get the watermarked image as shown in the figure 4. Then, the receiver will retrieve the data back from watermarked image by extraction.

B=

25	26	27	28	29
35	31	32	33	34
42	43	44	45	46
49	50	51	52	53
54	55	56	57	58

Figure 2 An example for cover image matrix.

w=

0	1	0	1	0	0	1	1	(S)
0	1	1	1	0	1	0	0	(t)
0	1	1	0	0	0	0	1	(a)
0	1	1	1	0	0	1	0	(r)
0	1	1	1	0	1	0	0	(t)

Figure 3 An example for secret data matrix

17	18	19	20	21
39	23	32	45	38
46	38	32	37	42
49	54	55	60	49
58	55	60	53	50

Figure 4 An example for watermarked image.

To implement reversibility in our proposed algorithm, we can simply create two matrices, to record the modifications made in the 3rd and 4th LSBs of the cover image. As previously said we need to send these matrices to the extraction phase to get back the original cover image.

C. *Selection Strategy*

After the modification done on the traditional LSB, we could realize the changes in the pixel values in the cover image and the watermarked image by comparing the figure 5 and figure 6 and that may reduce imperceptibility. If all the altered pixels are clustered in a location, it may lead to robustness but in our paper we are providing fragility. To solve the above two problems we are implementing selection strategy. For that we are randomly selecting the pixels and after that we are embedding the secret data in the cover image. Our modified algorithm failed in providing imperceptibility, it is shown in the figure 5. Since reversibility is implemented we could get the extracted image which same as that of cover image as shown in the figure 6.

After applying selection strategy in our modified algorithm imperceptibility is also achieved as shown in the figure 7.

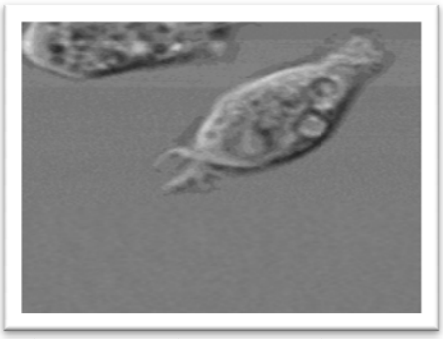

Figure 5 Watermarked image after applying LSB34_rev.

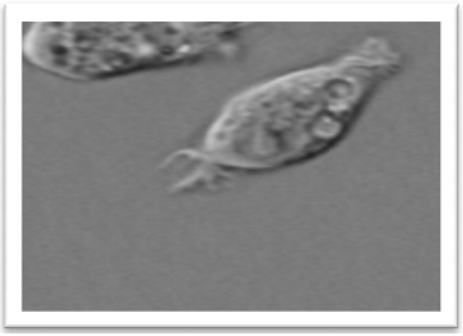

Figure 6 Extracted image after applying LSB34_rev.

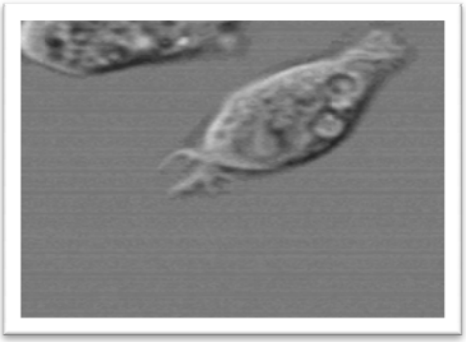

Figure 7 Watermarked image after LSB34_REV_SEL.

IV. QUANTITATIVE ANALYSIS

A. Imperceptibility and Reversibility

The PSNR value was used to evaluate the quality of the watermarked images. It is most easily defined via the Mean Squared Error (MSE) which is for two M x N images I and K where one of the images is considered as a noisy approximation of the other. MSE is defined as the following equation (2) and the PSNR is defined in equation (1).

$$PSNR = 10 \cdot log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20 \cdot log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \quad (1)$$

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

where I is the original image and K is the watermarked image. Based on equations (1) and (2), we calculate the PSNR for our proposed algorithm to see the quality of the watermarked images.

SCHEME NAME: LEAST SIGNIFICANT BIT

TYPE: PNG File

Table 1 A sample table for LSB algorithm analysis.

SIZE OF WATERMARI	IMPERCEPTIBILIT (PSNR values)	REVERSIBILITY (PSNR values)
50	78.2565	78.2565
100	74.8137	74.8137
500	68.0870	68.0870
1000	64.9475	64.9475
2000	62.0506	62.0506
10000	55.0951	55.0951
100000	Not Applicable	Not Applicable

The above Table 1 is to show the result of the PSNR for two combinations,

1) Original image and embedded image (imperceptibility)
2) Original image and extracted image (reversibility)

Since the PSNR value for both above mentioned combination of input are same, it is understood that embedded and extracted images are also same and the reversibility is not achieved. After applying reversibility we could get the Table 2 as follows,

SCHEME NAME: LEAST SIGNIFICANT BIT WITH REVERSIBILITY

TYPE: TIF File

Table 2 A sample table for LSB with reversibility.

SIZE OF WATERMARI	IMPERCEPTIBILIT (PSNR values)	REVERSIBILITY (PSNR values)
50	73.1359	100
100	70.2103	100
500	63.2421	100
1000	60.2253	100
2000	57.2827	100
10000	Not Applicable	Not Applicable
100000	Not Applicable	Not Applicable

Since the original image and the extracted image are same the PSNR value is 100. Hence the reversibility is now achieved. After boosting up the capacity of the scheme, we got the Table 3 and Table 4 as follows.

By comparing Table 2 and Table 4, we could say that our scheme has boosted the capacity of traditional LSB.

SCHEME NAME: LEAST SIGNIFICANT BIT34

TYPE: PNG File, Table 3 A sample table for LSB34.

SIZE OF WATERMARI	IMPERCEPTIBILIT (PSNR values)	REVERSIBILITY (PSNR values)
50	61.6457	61.6457
100	57.9029	57.9029
500	50.7422	50.7422
1000	47.7507	47.7507
2000	45.1578	45.1578
10000	38.0822	38.0822
100000	Not Applicable	Not Applicable

SCHEME NAME: LEAST SIGNIFICANT BIT34 WITH REVERSIBILITY

TYPE: TIF File

Table 4 A sample table for LSB34 with reversibility.

SIZE OF WATERMARK	IMPERCEPTIBILITY (PSNR values)	REVERSIBILITY (PSNR values)
50	56.6351	100
100	53.5651	100
500	46.6396	100
1000	43.8361	100
2000	40.7374	100
10000	33.9417	100
100000	Not Applicable	Not Applicable

Higher the PSNR values better the quality of the image. Since we embedded the secret data in 3rd and 4th LSB bits of each pixel, we got some changes with the value of the pixels. Because of this, our

algorithm's imperceptibility went down as shown in the Figure 8.

By consolidating all the values from 20 tables (i.e. 10 images*2 shemes) we got the following graph for representing imperceptibility.

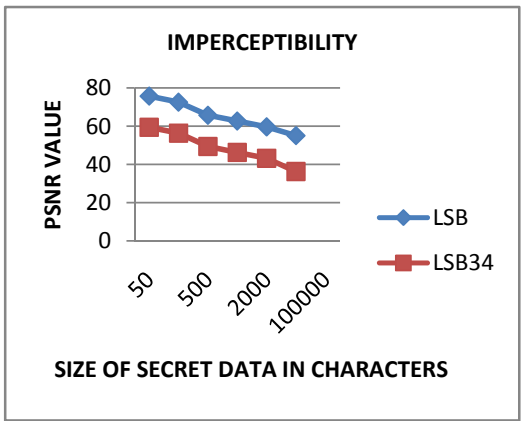

Figure 8 Imperceptibility Analysis.

Since imperceptibility is very important feature in information hiding, we overcame this problem by implementing the pixel selection strategy.

B. Fragility

To check the fragility in our modified LSB algorithm, we are attacking [7] the watermarked image and that must modify our hidden data in it.

SCHEME NAME: LEAST SIGNIFICANT BIT34 (LSB_34)
NAME OF THE ATTACK: JITTER
TYPE: TIF File
Percentage of attack: 70

Table 5 An example to show the attacked percentage.

SIZE OF WATERMARK(bits)	ATTACKED SECRET DATA (%)
400	13.25
800	8.12
4000	6.80
8000	11.45
16000	10.31
80000	8.40
800000	Not Applicable

Table 5 is an example to prove that our algorithm is fragile [5] because it shows how much percentage of secret data got attacked. Figure 9 is to represent all the tables in the form of graph.

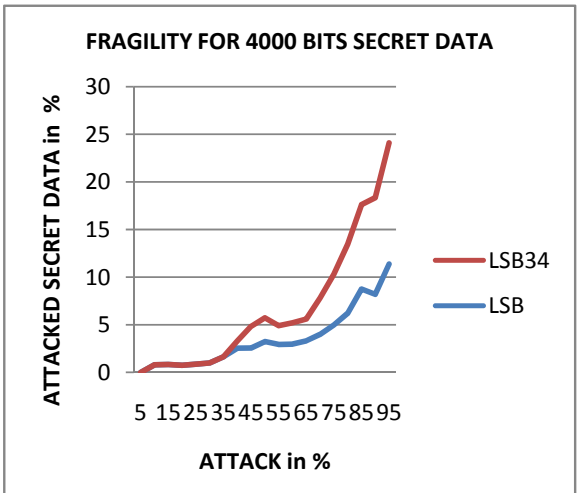

Figure 9 Fragility Analysis.

V. CONCLUSIONS

Thus the result of our quantitative analysis helps us to prove that our proposed algorithm will boost the capacity of the scheme and provide reversibility, fragility for the transmitting secret data.

REFERENCES

[1] Techniques and applications of digital watermarking and content protection by Michael Konrad Arnold, Martin Schmucker, Stephen D. Wolthusen

[2] "Reversible Zero-Bit Watermark Based on Chaotic Encryption "in Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference, Sept. 2010.

[3 "Digital watermarking algorithm using LSB" in Computer Applications and Industrial Electronics (ICCAIE), 2010 International Conference, Dec. 2010.

[4] "Block-based digital image watermarking using Genetic Algorithm" in Emerging Technologies (ICET), 2010 6th International Conference, Oct. 2010

[5] "Cheating resistance and reversibility-oriented secret sharing mechanism " in Information Security, IET, June 2011.

[6] "Robust LSB watermarking optimized for local structural similarity" in Electrical Engineering (ICEE), 2011 19th Iranian Conference, May 2011.

[7] "A steganographic scheme for colour image authentication (SSCIA) " in Recent Trends in Information Technology (ICRTIT), 2011 International Conference, June 2011.

[8] "A watermarking e-note technique against geometric attacks" in Mechanical and Electronics Engineering (ICMEE), 2010 2nd International Conference, Aug. 2010.

◈◈◈