Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 93 (2016) 832 – 838

Procedia Computer Science

6th International Conference On Advances In Computing & Communications, ICACC 2016, 6-8 September 2016, Cochin, India

Image Steganography Based on Complemented Message and Inverted bit LSB Substitution

Rupali Bhardwaj*[a], Vaishali Sharma[b]

[a]AP, CSED, Thapar University, Patiala,Punjab,India 147004
[b]M.Tech Schlar,CSED,Thapar University,Patiala,Punjab,147004

Abstract

Steganography is the art of encoding/embedding secret information in cover media in such a way so as not to provoke an eavesdropper's suspicion. The primary purpose of this paper is to provide three levels of security, first is provided by complementing the secret message, second by hiding complemented secret message in cover image pixels that are selected randomly by using pseudo random number generator, third by using inverted bit LSB method[2] as stegnographic technique rather than simple LSB, thus, reduces the chance of the hidden message being detected. MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) are two common quality measurements to measure the difference between the cover-image and the stego-image. Results showed that the proposed method gives better results than simple LSB and inverted LSB with higher PSNR and lower MSE.

Peer-review under responsibility of the Organizing Committee of ICACC 2016

Keywords: Image Steganography, LSB, Pseudo Random Number, PSNR.

1. Introduction

With rapid advancement in Multimedia technologies during the recent years, communication and information exchange have become much easier and faster but at the same time the issues related to data security and confidentiality have become a major concern of today's era. To cater to this need of information security, a number of hidden and secret communication techniques have been developed.

Steganography refers to the art of hidden communications[1], encoding/embedding secret information in cover media in such a way that it is a difficult job for a unauthorized person to see that there is something hidden in the cover media. The output is an image called stego-image that is similar to the cover media. This stego image is then sent to the receiver where the receiver retrieves the hidden message by implementing de-steganography process. A stego-key is used for embedding or encoding process to restrict decoding or extraction of the embedded data in cover media.

rupalibhardwaj09@gmail.com

Peer-review under responsibility of the Organizing Committee of ICACC 2016
doi:10.1016/j.procs.2016.07.245

The modern age steganography is usually implemented computationally, where multimedia files are used as cover media. A good Steganographic mehods has three features, good hiding capacity, good imperceptibility and the last is robustness.
In this paper, three levels of security is used to secure the embedded information and to add more complexity for steganalysis. This is a three step process, rather than embedding the message bits directly in cover image, pixels are generated randomly through pseudo random number generator after that complemented secret data is embedded in cover image using inverted bit LSB method.

In section 2 literature survey is conferred .After a brief discussion of LSB and inverted bit LSB in Section 3, Section 4 describes the proposed method. Section 5 demonstrates experiments and results. Section 6 concludes the paper.

2. Literature Survey

Steganography is classified into two domains spatial domain and transform domain. This paper emphasize towards spatial domain technologies with its literature survey where two methodologies are discussed LSB based and EDGE based.
In LSB based LSB'S of cover image are affected. In LSB Matching less modification to cover image pixels are performed by adding or subtracting one from cover pixel if secret message is not similar but LSB embedding can be analysed by steganalysis attacks[3]. Jarno *et. al.* proposes LSBMR, it uses two pixels for embedding bits of secret information one bit is embedded in first LSB and a function of two pixels is used to carry another bit of information This technique spreads the message uniformly thus providing good security level compare to LSBM.
EDGE based methods use the difference of pixels and their nearby pixels. D. Wu *et al.*[4], their technique aids a large capacity for embedding message bits where as their number is calculated by difference between pixel and its nearby pixel. This technique does not hold well against statistical analysis. X. zhang *et al.*[5] proposes that PVD are vulnerable to steganalysis due to atypical steps in its histogram. An analyst can determine the size of the embedded message. Thus he proposes a modified pixel value differencing scheme. Luo *et. al.*[6] put forward that edge-based schemes are not better than the LSB-based approaches.

3. Preliminaries

3.1. Inverted Bit LSB Substitution

Nadeem Akhtar *et. al.* proposed a scheme in which PSNR of the stego image has increased and also security is maintained by selecting pixels randomly.In this technique message bits are embedded in the cover image pixels randomly and a count with respect to the combination of bits at 2nd and 3rd bits of the pixel is maintained. Suppose 2nd and 3rd bits of a pixel are 01 so if the LSB of image matches this counter is incremented for not changed pixel else counter is incremented for changed bits, same is performed for all the combinations (00, 01, 10, and 11).
Example: Four message bits 1 0 0 0 are to be hidden into four cover image pixels
10000100
00101101
11101101
11101111
After plain LSB steganography, stego-image pixels are
1000010**1**
0010110**0**
1110110**0**
1110111**0**
No. of changed pixels is four. According to algorithm check the 2nd and 3rd Least significant bit of the stego- image.For example let 2nd pixel=0 and 3rd pixel=1.Now if the 2nd and 3rd bit of pixel matches the required combination than invert the LSB else it will remain the same.Thus if we applied this case to above example than the pixels in the stego image will be:
1000010**0**

00101101
11101101
11101110
No. of changed pixel is one, so by employing this technique there will be increment in the PSNR as there will be pixel benefit. Same process will be performed for all the bit combination. The bit inversion is performed only if the changed bits count is greater than unchanged bits count thus leading to less distortion of the cover image and leading to increased PSNR.

4. Proposed Methodology

In this technique a random seed is used to choose the pixels randomly and embed the message bits in least significant bit of this randomly chosen pixel. In the given scheme along with message p bits are also embedded that determine whether the bits are inverted or not, here we require 4 bits to determine. First bits represent '00' combination if inverted than one else it will be complemented , second bit represent '01' combination, third bit represent '10' combination and last bit represent '11' combination.

4.1 Data Embedding Algorithm

INPUT: Cover Image C of size I x I, Secret Data, M of size J x J, p=4 bits(initially all are zero).
OUTPUT: Stego-image, Key
STEP 1: Embed the M to the LSB planes of C to get the stego-image S. The embedding procedure is given as below

1. Complement the message bits.
2. Generate the set of random pixels using secret key
3. For i = 1 to J
4. For j = 1 to J
5. k1=get the 2nd bit of C(i,j)
6. k2= get the 3rd bit of C(i,j)
7. m1=get the 1st bit of C(i,j)
8. check k1 and k2 belongs to which combination(00,01,10,11)
9. if m1==M(i,j) then increment the respective counter for unchanged LSB
10. else
11. set the LSB of cover image as m1
12. increment the respective counter for changed LSB
13. End;End;End
14. if counCt00>countNc00 then invert the LSB of all the pixels with 2nd and 3rd bit as 00
15. else if counCt10>countN10 then invert the LSB of all the pixels with 2nd and 3rd bit as 01
16. else if counCt01>countNc01 then invert the LSB of all the pixels with 2nd and 3rd bit as 10
17. Else if counCt11>countNc11 then invert the LSB of all the pixels with 2nd and 3rd bit as 11.
18. Make changes into p bits according to counter values and embed in the image.

Where C (i,j), S (i,j), M (i,j) means pixel value at position (i,j) in cover image, stego image and message bits.

4.2 Data Extraction Algorithm

Extracting the message from the stego-image includes inverse comparison to that used in embedding.
Input: Stego-Image, Key Matrix.
Output: Secret Data.
The steps of the extraction phase are as follows:

1. Generate the random pixel using key.
2. Extract p bits
3. if first bit of p is 1 then invert the LSB of all the pixels with 2nd and 3rd bit as 00.

4. Else if second bit of p is 1 then invert the LSB of all the pixels with 2nd and 3rd bit as 01
5. Else if third bit of p is 1 then invert the LSB of all the pixels with 2nd and 3rd bit as 10
6. Else if forth bit of p is 1 then invert the LSB of all the pixels with 2nd and 3rd bit as 11
7. For i = 1 to N
8. For j = 1 to N
9. If s(i,j)==even then M(i,j)=1
10. Else M(i,j)=0
11. End;End;End;

where S(i,j), means pixel value at position (i,j) in stego image and M (i,j) means message bits value at position (i,j) .

5. Result and Analysis

In this section, some experiments are carried out to prove the efficiency of the proposed method where simulation is done on Matlab 14. A set of 8- bit greyscale image of size 512 × 512 is used as the cover image to hide binary and grey image of size 128 × 128 to form the stego-image. With the experimental study, we noticed that the visual differences between the original cover-images and stego images with the complemented message and inverted LSB technique is hardly detected with naked eyes.

5.1 PSNR Analysis

MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) are two common quality measurements to measure the difference between the cover-image and the stego-image.
MSE is the averaged pixel-by-pixel squared difference between the cover-image and the stego-image.

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} [C(i, j) - S(i, j)]^2 \quad (1)$$

where, M and N are the rows and columns of the cover image respectively, and C(i, j) and S(i, j) means the pixel value at position (i, j) in the cover-image and the corresponding stego-image, respectively.
The PSNR is expressed in dB's and can be calculated using MSE as

$$PSNR = 10 \times \log\left(\frac{P^2}{MSE}\right) \quad (2)$$

Where, P is the peak signal value of the cover- image, and

$$P = \max(C(i, j), S(i, j)) \quad (3)$$

Table 2(figure 2), table 3(figure 3), table 4(figure 4) and table 5(figure 5) give the measured values of MSE and PSNR of different types of cover images of size 512×512 respectively for simple LSB, random LSB, inverted LSB, complemented inverted LSB. It is observed that when the payload increases the MSE increases and this affects the PSNR inversely and for all cover- images PSNR is greater than 50, this indicates good performance of the proposed system. As can be seen in figure 2, the reduction in PSNR is very slight as compared with the increases in the size of embedded message and this suggests that the quality of the image remains almost constant when the message size increases. It means that the stego-images created with proposed system can survive the common -cover-carrier attack. Table 1(figure 1) gives the measured values of MSE and PSNR of cover images of size 512×512 and hidden message size is 128× 128 respectively. It is observed that PSNR value of proposed method is better than other techniques.

Table 1Comparison of proposed scheme with other schemes

Cover Image	Message Imaage	Simple LSB		Random LSB		Invert LSB		Complemented Random Invert LSB	
Lena	Cameraman	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
512x512	4225 bits	59.6578	0.0649	59.6958	0.0644	59.7138	0.2494	59.7275	0.0645
512x512	16384 bits	53.7982	0.2499	53.8054	0.3806	53.8149	0.2486	53.8174	0.2492
512x512	24964 bits	51.9777	0.3807	51.9788	0.3806	51.9841	0.3801	51.9979	0.3809

Table 2 Image Steganography through Simple LSB

Simple LSB						
Cover Image	Msg1(4225bits)		Msg2(16384 bits)		Msg3(24964 bits)	
512X512	PSNR	MSE	PSNR	MSE	PSNR	MSE
Pepper	59.0700	0.0650	53.2174	0.2500	51.3902	0.3808
Lena	59.6578	0.0649	53.7982	0.2503	51.9777	0.3807
Baboon	59.1370	0.0645	53.2761	0.2488	51.4320	0.3804

Table 3 Image Steganography through Random LSB

Random LSB						
Cover Image	Msg1(4225 bits)		Msg2(16384 bits)		Msg3(24964 bits)	
512X512	PSNR	MSE	PSNR	MSE	PSNR	MSE
Pepper	59.0840	0.0648	53.2117	0.2503	51.3672	0.3828
Lena	59.6958	0.0644	53.8054	0.2499	51.9788	0.3806
Baboon	59.0912	0.0646	53.2297	0.2493	51.3986	0.3800

Table 4 Image Steganography through Inverted LSB

Invert LSB						
Cover Image	Msg1(4225Bits)		Msg2(16384Bits)		Msg3(24964Bits)	
512X512	PSNR	MSE	PSNR	MSE	PSNR	MSE
Pepper	59.1391	0.0639	53.227	0.2497	51.3583	0.3836
Lena	59.7138	0.0641	53.8149	0.2486	51.9841	0.3801
Baboon	59.1025	0.0650	53.2495	0.2503	51.4332	0.3803

Table 5 Image Steganography through Complemented Inverted LSB

Invert LSB						
Cover Image	Msg1(4225Bits)		Msg2(16384Bits)		Msg3(24964Bits)	
512X512	PSNR	MSE	PSNR	MSE	PSNR	MSE
Pepper	59.0945	0.0647	53.2341	0.2490	51.3912	0.3807
Lena	59.7275	0.0645	53.8174	0.3810	51.9979	0.3789
Baboon	59.1234	0.0647	53.2779	0.2487	51.4310	0.3805

Figure 1 Comparison of proposed scheme with simple, random, inverted LSB

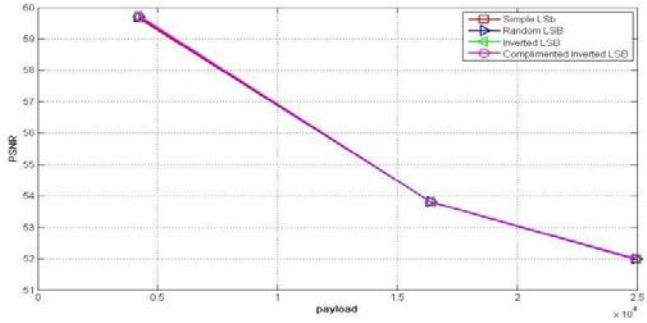


Figure 2 Complemented inverted LSB PSNR comparison

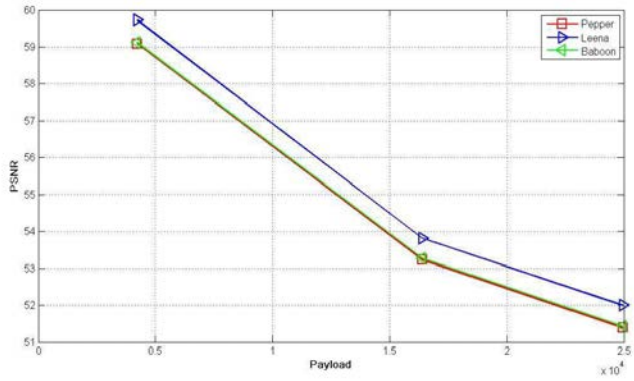


Figure 3 Simple LSB PSNR comparison

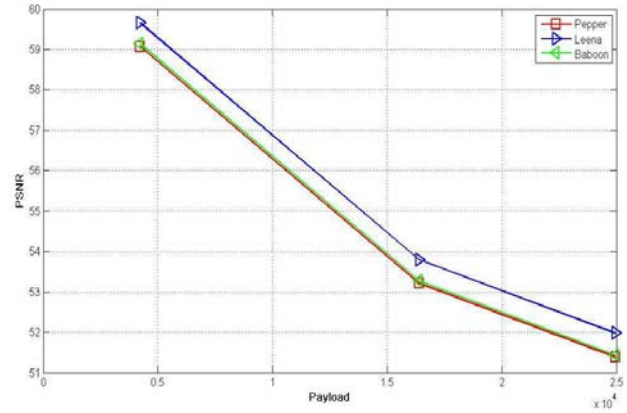


Figure 4 : Random LSB PSNR comparison

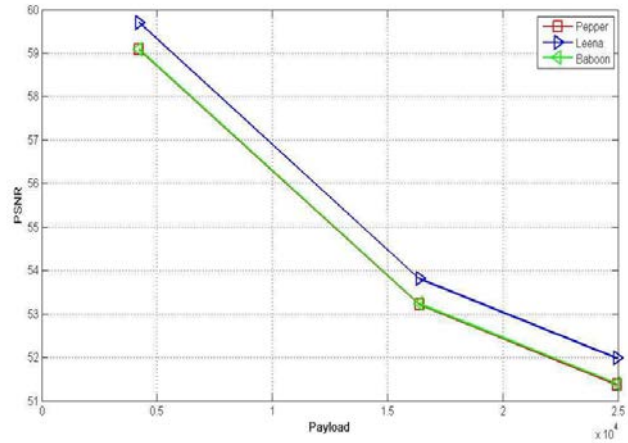
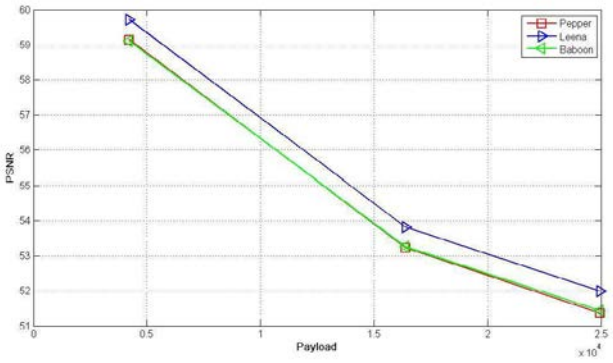


Figure 5 Inverted LSB PSNR comparison



6. Conclusion

The primary purpose of this paper is to provide three levels of security, rather than hiding the message bits directly in cover image, pixels are generated randomly through pseudo random number generator after that secret data is hidden behind a cover image using inverted LSB method.

Experimental study points out that the proposed system is better than basic LSB method in terms of higher visual quality as indicated by the high PSNR values of hiding secrete message bits in the image thus reduces the chance of the confidential message being detected and enables secret communication. For future work we will generate random number through cellular automata as further securing system and use other type of cover-object for hiding the data.

References

1. Oorschot P, Vanstone, and Menezes AJ. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, FL, 1997.
2. Akhtar N, Khan S, Johri P. *An improved inverted LSB image steganography*. In Issues and Challenges in Intelligent Computing Techniques (ICICT), International Conference on.IEEE, 2014; p. 749-755.
3. Ker A. *Improved detection of LSB steganography in grayscale images*. In Proc. Information Hiding Workshop Springer LNCS 2014; 3200: 97–115.
4. Wu D, Tsai W. *A steganographic method for images by pixel value differencing*. Pattern Recognit. Lett. 2003; 24:1613–1626.
5. Zhang X, Wang S. *Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security*. Pattern Recognit. Lett. 2004; 25: 331–339.
6. Yang HC, Weng CY, Wang SJ, Sun HM. *Adaptive data hiding in edge areas of images with spatial LSB domain systems*. IEEE Trans. Inf. Forensics Security 2008; 3: 488–497.
7. Li B, He J, Huang J, Shi YQ. *A Survey on Image Steganography and Steganalysis*. Journal of Information Hiding and Multimedia Signal Processing 2011; 2:142-172.