Image Steganography using Complemented Random Inverted Least Significant Bit Substitution

S.Tamil Selvan[1], R.Rajkumar*[2],
R. Thalapathi Rajasekaran[3],V.Manjula[4]

[1]Professor, Department of CSE, Saveetha, School of Engineering, Chennai
*[*2]Associate Professor, Department of ECE, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai*
[3]Assocaite Professor, School of CSE, Saveetha, School of Engineering, Chennai
[4]Associate Professor, Department of CSE, Vellore Institute of Technology, Chennai
[1]tmlslvn@gmail.com,[2]rajkumarramasami@gmail.com,[3]r.rajthalapathi@gmail.com,
[4]manjula.v@vit.ac.in

Abstract

Steganography is the technique of concealing private information in cover media so that an eavesdropper does not suspect it. The primary objective of this research is to provide three levels of security: the first by complementing the secret message, the second by hiding the complemented secret message in cover image pixels that are chosen at random via a pseudo random number generator, and the third by using inverted bit LSB as a Steganography technique rather than simple LSB, which 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 used to compare the cover-image and stego-image. Results showed that the proposed method gives improved results than simple LSB and inverted LSB with higher PSNR and lower MSE.

Keywords: *Image Steganography, LSB, Pseudo Random Number, PSNR, MSE*

Corresponding Author
[*] *R.Rajkumar, Associate Professor, Department of ECE, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai*

1. Introduction

Communication and information transmission have become much easier and faster because of the recent rapid advancements in multimedia technologies. However, concerns about data security and confidentiality have grown significantly in importance in the modern era. Many covert and secret communication methods have been created to meet this demand for information security.

Steganography is the art of hidden communications. This involves encoding or embedding secret information in a cover medium in a way that makes it difficult for a third party to detect that something is concealed there. The result is a cover media image known as a stego-image. The receiver receives the Steganography image and uses a de-Steganography technique to recover the encrypted message. To prevent the decoding or extraction of the embedded data from cover media, a stego-key is utilized throughout the embedding procedure.

Steganography in the present day is typically computationally implemented, and multimedia files are utilized as the cover medium. An excellent Steganography method has three characteristics: secrecy, encryption techniques, and robustness.In order to protect the embedded data and increase the complexity of Steganography, three levels of protection are applied in this study. It involves three steps: first, random pixels are generated using a pseudo-random number generator; next, complemented secret data is inserted in the cover image using the inverted bit LSB approach; and finally, the process is completed.

[1]Steganography can be divided into two categories, which are the spatial domain and the transform domain. There will be a discussion of two methodologies in this article, LSB-based and EDGE-based, with an emphasis on spatial domain technology in the literature review. The LSBs in cover images are affected by LSB-based. A smaller amount of alteration will be made to the cover image pixels if the secret message is not comparable. In this case, LSB Matching will add or

remove one pixel from the cover image pixel. As a result, LSB embedding can be subject to stego-analysis attacks in some cases.

2. Literature Survey

According to Jarno et al. As a result of. The LSBMR is a proposal that utilizes two pixels to transport two bits of secret information - one bit is contained in the first LSB, and the second bit is carried by the functions of the two pixels. It is critical to note that this method provides a high level of security and consistency when compared to LSBM, which consistently distributes the message.

It is the difference between pixels and the pixels close to them that is used in EDGE-based approaches. A lot of message bits can be embedded according to the technique proposed by Wu et al.4's research. This allows for a large number of message bits to be embedded. It is determined by the difference between a pixel and its neighboring pixels which determines the quantity of these pixels. In terms of statistical analysis, this method does not seem to be very well supported. In the paper by Zhang et al.5, it is suggested that the unusual stages in the PVD histogram make them susceptible to a stego-analysis since they have unusual stages. It is possible for an analyst to determine the size of the embedded message by calculating its length.As a result of this, the author proposes a modified approach for pixel value differencing as a result. Steganography is divided into two domains, namely the spatial domain and the transform domain. With its literature review, this paper focuses on spatial domain technologies and discusses two methodologies: LSB-based and EDGE-based.

LSB-based LSB's affect the LSB's of the cover image. If the secret message is not similar, LSB Matching performs less modification to the cover image pixels by adding or subtracting one, but LSB embedding can be analyzed by stego-analysis attacks. Jarno et al. This paper proposes a mechanism for encrypting bits of secret information using two pixels, a system known as LSBMR. This is one bit in the first LSB and a function of two pixels to carry another bit of information.

In comparison to LSBM, this technique spreads the message uniformly, providing a higher level of security.There are a number of EDGE-based methods that are used in order to determine the edge between pixels and their neighbors. D. Wu et al.4 developed a technique that allows for a large capacity for embedding message bits. This capacity is determined by the difference between a pixel and its neighboring pixel. This technique does not stand up to statistical scrutiny. PVD are vulnerable to stego-analysis, according to X. zhang et al., due to atypical steps in their histogram. The size of the embedded message can be determined by an analyst.As a result, the authors suggests a modified pixel value differencing scheme. According to Luo et al., edge-based schemes are not superior to LSB-based approaches.

3. Inverted Bit LSB Substitution

A scheme in which the PSNR of the stego image is increased while maintaining safetywas discussed. This scheme involves generating random pixels in order to increase the PSNR of the stego image. Message bits are randomly embedded in the pixels of the cover image in this technique. A count is kept with respect to the combination of bits in the pixel's second and third bits. Assume the second and third bits of a pixel are 01, so if the LSB of the image matches, this counter is incremented for not changed pixels; otherwise, this counter is incremented for changed bits; this is repeated for all combinations (00, 01, 10, and 11).

For Example:

Four message bits 1 0 0 0 are to be hidden within four cover image pixels.

10000100
00101101
11101101
11101111

After plain LSB Steganography, stego-image pixels are
10000101
00101100
11101100
11101110

There are four pixels that are different in this image. It is imperative to check the second and third least significant bits of the stego-image using the algorithm. Assume the second pixel in the image is 0 and the third pixel in the image is 1. It is recommended to invert the LSB of the pixel if the second and third bits of the pixel match the required combination, otherwise the LSB will remain unchanged. In order to calculate the pixels in the stego image, we can use the example of the preceding example as an example:

10000100
00101101
11101101
11101110

The number of changed pixels in this technique is one, so using this technique will result in an increase in PSNR as a result of the pixel benefit. Each bit combination will be the same as the previous one. A bit inversion can only occur if the changed bit counts is higher than the unchanged bit count. Therefore, the cover image appears better and the PSNR is higher when bit inversion occurs.

4. Proposed Methodology

The message bits are embedded in the least significant bit of the randomly chosen pixel using a random seed in this technique. Along with the message, p bits are embedded in the scheme to determine whether the bits are inverted or not, which requires 4 bits in this case. The first bits represent the '00' combination. This combination will be complemented, the second bit represents the '01' combination, the third bit indicates the '10' combination, and the last bit indicates the '11' combination.

4.1 Data Embedding Algorithm

Input: A cover image with a size of A x A, a secret data with a size of Z x Z, and a precision of p=4 bits. (Initially all are zero).
Output: Stego-image with key,

Embed the M to the LSB planes of P in order to get the stego-image S. Below is the procedure for embedding the M to the LSB planes of P.

- The message bits should be complemented.
- The secret key will be used to generate the randomly selected pixels.

```
For i = 1 to Z
For j = 1 to Z
k1=get the 2nd bit of P(i,j)
```

k2= get the 3rd bit of P(i,j)
m1=get the 1st bit of P(i,j)

- check k1 and k2 belong to which combination (00,01,10,11)
- The respective counter will be incremented if m1 = M(i,j), which means that the LSB will remain unchanged
- else
- set the LSB of the cover image as m1
- Counters for each changed LSB should be incremented
- End; End; End
- It is recommended to invert the LSB of all pixels if countPt00 > countNc00, so that the second and third bit of each pixel will be 00
- If countPt10 is greater than countN10, then invert the LSB of all pixels by setting the 2nd and 3rd bits as 0.
- Other than that, if countPt01 > countNc01, then invert the LSB of all pixels by assigning the 2nd and 3rd bits as 10 if countPt01 > countNc01
- Otherwise, if countPt11>countNc11, the LSBs of all pixels should be inverted with the third bit as 11 and the second bit as 11.
- Change the p bits according to the counter values and embed the result in the image.
- The pixel values at position (i, j) in the cover image, stego image, and message bits can be represented by P (i, j), S (i, j), or M (i, j).

4.2 Data Extraction Algorithm

Input: Stego-Image, Key Matrix.
Output: Secret Data.

The steps of the extraction phase are as follows:

- The random pixel will be generated by using the key as input.
- Extract p bits
- The first bit of P will be 1, so invert the LSB of all the pixels with the second and third bits as 00 if the first bit of P is 1.
- If the second bit of p is 1, then it is necessary to invert the LSB of all pixels with the 2nd and 3rd bits set to 01 if the second bit of p is 1
- As an alternative, if the third bit of p is 1, then invert the LSB of all pixels so that the 2nd and 3rd bits are 10 if p is 1.
- The second alternative is to invert all the LSB of all the pixels that have the 2nd and 3rd bit as 11 if the fourth bit of p is 1.

```
For i = 1 to N
For j = 1 to N
If s(i,j)==even then M(i,j)=1
Else M(i,j)=0
End;
End;
End;
```

It is important to note that S(i,j) represents the pixel value at position (i,j) in the Stego image and M(i,j) represents the message bit value at position (i,j).

5. Results and Discussions

Using MATLAB 14, some experiments are conducted to demonstrate the efficacy of the proposed method. To hide binary, an 8-bit grayscale image of size 512×512 is included as the cover image, and a grayscale image of size 128×128 is used as the stego-image. With the inverted LSB technique and complemented message, we found that it was difficult to detect visual differences between the original cover-images and stego images.

Cover-image and stego-image quality measurements include MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio). Between cover-image and the stego-image, the MSE is the averaged pixel-by-pixel squared difference.

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

There are M rows and N columns in the cover image, and C(i, j) and S(i, j) are the pixel values corresponding to the positions (i, j) of the cover image and the corresponding stego image.

In order to calculate PSNR in dB, MSE can be used

$$\mathrm{PSNR} = 10 \times \log \frac{\mathrm{P}^2}{\mathrm{MSE}}$$

Where, P is the peak signal value of the cover- image, and P=max (C (i,j),S(i,j))

Table.1 PSNR& MSE Comparison of the Proposed Method with other Techniques

No of Secret Message Bits	Cover Image	Simple LSB		Random LSB		Invert LSB		Complemented Random Invert LSB	
		PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
4225	Pepper	59.696	0.063	59.102	0.065	59.153	0.229	59.108	0.064
	Lena	59.696	0.065	59.714	0.065	59.728	0.229	59.741	0.063
	Baboon	59.137	0.065	59.091	0.065	59.116	0.230	59.137	0.064

16384	Pepper	53.798	0.275	53.221	0.341	53.230	0.229	53.237	0.097
	Lena	53.805	0.275	53.815	0.340	53.817	0.228	53.820	0.229
	Baboon	52.747	0.273	53.239	0.341	53.252	0.230	53.280	0.097
24964	Pepper	51.391	0.381	51.373	0.383	51.372	0.384	51.405	0.383
	Lena	51.979	0.381	51.984	0.381	51.998	0.381	52.012	0.381
	Baboon	51.433	0.381	51.399	0.380	51.447	0.381	51.445	0.383

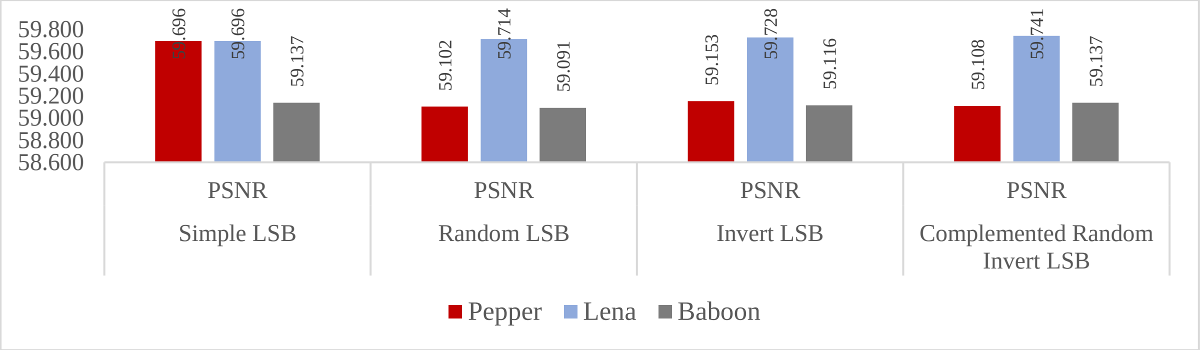

Figure.1. PSNR Comparison of Images with 4225 Embedded bits

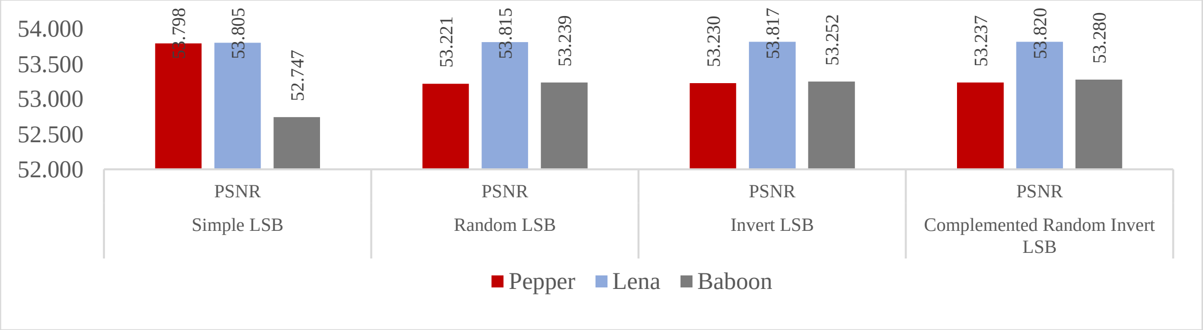

Figure.2. PSNR Comparison of Images with 16384 Embedded bits

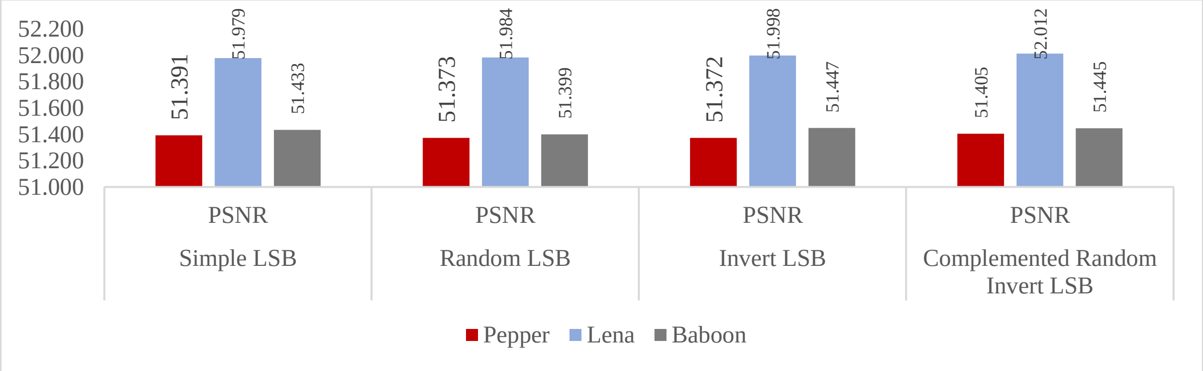

Figure.3.PSNR Comparison of Images with 24964 Embedded bits

Table.1 shows the performance comparison PSNR and MSE for various methods for image size of 512 x 512. In that the proposed Complement random invert LSB embedding technique shows the better performance. The Figure.(1-3) shows the graphical comparison of PSNR values for different level of embed bits i.e 4225 bits, 16384 bits, 24964 bits for simple LSB, random LSB, inverted LSB, complemented inverted LSB. PSNR is greater than 50 for all cover-images when the MSE is high, indicating high performance for the proposed system. Increased payload increases MSE, which affects PSNR inversely. As can be seen in figures, the reduction in PSNR is very slight as compared with the increases in the size of the embedded message. This suggests that the quality of the image remains almost constant when the message size increases. This means that the stego-images created with the proposed system are resistant to the common cover-carrier attack. The PSNR value of the proposed method is better than other methods.

6. Conclusion

In this paper, three levels of security are provided, rather than encrypting message bits directly in the cover image. By using a pseudo random number generator, pixels are generated randomly, and then secret data is concealed behind a cover image using an inverted LSB algorithm. According to the experimental results, the proposed system has a higher visual quality than the basic LSB method. This is due to its high PSNR values for hiding secret message bits in the image. This reduces the chance of detection of the confidential message and enables secure communication. In the future, we will generate random numbers using cellular automata's as an additional secure system and hide the data with other kinds of cover-objects.

References:

[1] *P. Oorschot , Vanstone, and A.J. Menezes, "Handbook of Applied Cryptography",. CRC Press, Boca Raton, FL, **(1997)***

[2] *N. Akhtar ,S. Khan S, P. Johri, "An improved inverted LSB image steganography" Issues and Challenges in Intelligent Computing Techniques (ICICT), International Conference on.IEEE, **(2014**); pp. 749-755.*

[3] *A. KeR, "Improved detection of LSB steganography in grayscale images" Proceedings. Information Hiding Workshop Springer LNCS**(2014)**, pp. 97–115*

[4] *D. Du , W. Tsai, "A steganographic method for images by pixel value differencing" Pattern Recognition. Letters, vol.24 **(2003),** pp.1613–1626.*

[5] *S.Tamilselvan, P. Dhavachelvan, "An Image Security System", International Journal of Engineering, Applied and Management Sciences Paradigms, vol.54,no.3,(**2019)**,*

[6] *X.Zhang , S.Wang, "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security" Pattern Recognition. Letters, vol.25,**(2004**), pp. 331–339.*

[7] *H.C. Yang, C.Y. Weng, S.J. Wang, and H.M.Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems" IEEE Transactions on. Information Forensics Security, vol.3,**(2008)**, pp. 488–497.*

[8] *B.Li , J. He, J. Huan and, Y.Q. Shi, "A Survey on Image Steganography and Steganalysi", Journal of Information Hiding and Multimedia Signal Processing, vol.2**,(2011),** pp.142-172.*

[9] *Er. Priya Tiwari, Dr. Naveen Dhillon and Er. Kuldeep Sharma, "Analysis of Image Restoration Techniques for Developing Better Restoration Method" Multimedia Signal Processing,vol.3, no. 4,**(2013),** pp.1142-1158.*

[10] *Mathri thakur, Shilpa Chadur, "Image Restoration Based on Deconvolution by Richardson Lucy Algorithm" International Journal of Engineering Trends and Technology (IJETT), vol.14,no.4, **(2014),**pp.455-467.*

[11] *R.Pushpavalli1 and G.Sivarajde "A hybrid filtering technique for eliminating uniform noise and impulse noise in digital image" Signal & Image Processing: An International Journal (SIPIJ) vol.4, no.4**,(2013),** pp.198-208.*

[12] *Giacomo Boracchi and Alessandro Foi, "Modelingthe Performance of Image Restoration from Motion Blur". IEEE Transactions on image processing, v ol. 21, no. 8, **(2012)** ,pp.*

[13] *Ryo Nakagaki,, and Aggelos K. Katsaggelos, "A VQ-Based Blind Image Restoration Algorithm" IEEE transaction on image processing. vol 9, **(2003),** pp. 1044-1053.*

[14] *Dr.P.Subashini, ".Image Deblurring Using Back Propagation Neural Network. World of Computer Science and Information Technology Journal (WCSIT)" vol. 1, no. 6,**(2011)**,pp.277-282.*

[15] *Neeraj Kumar, Rahul Nallamothu, Amit Sethi.september, "Neural Network Based Image Deblurring" Neural network application in electrical engineering**(2013),** pp.219-222.*

[16] *S.K. Satpathy, S.K. Nayak, K. K. Nagwanshi, S. Panda, C. Ardil. "An Adaptive Model for Blind Image Restoration using Bayesian Approach". International Journal of Electrical, Robotics, Electronics and Communications Engineering, vol:4, no:1,**(2010)**. pp.29-36*