JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 10(3), SEPTEMBER, 2022
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com

Development of an Improved Pairwise Least Significant Bit Steganography using Immune Programming Approach

Stephen Nwachukwu, Habib Rabi'u
Department of Electrical Engineering
Bayero University, Kano.

ABSTRACT
Steganography is the science of secret communication i.e., hiding a secret message in a carrier file such as image, video or text. The goal of steganography is to conceal the presence of a message from unauthorized party. The challenge of modern image steganography is to transfer the embedded information to the destination without being detected and decoded by an attacker. Many different carrier file formats can be used, but digital images are the most popular because of their prevalence on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have their respective strengths and weaknesses. In this work, the conventional pairwise Least Significant Bit (lsb) algorithm is modified and merged with an Immune Programming Strategy to find a near optimal solution for masking the message thus, making it imperceptible and secured. The result obtained revealed a low Mean Square Error (MSE) which implies minimal pixel differences between the original and stego images. In addition, the result also demonstrated a high Peak Signal to Noise Ratio (PSNR) which suggest sustenance of the image quality, thus less prone to hackers

ARTICLE INFO
Article History
Received: June, 2022
Received in revised form: July, 2022
Accepted: September, 2022
Published online: September, 2022

KEYWORDS
Information hiding, Steganography, LSB matching, Immune Programming

.

INTRODUCTION

Throughout time security is a prominent issue. With the advent of internet as a convenient and efficient medium for communication, the challenge has multiplied many folds. Using internet, messages can be transferred in a fast and cheaper way. The internet is used globally, it finds application in fields such as military, schools and medical institutions [1]. Similarly, its application is evident in financial institutions such as banks, insurance etc. However, messages transferred over the internet are prone to attack by hackers. This significantly erode the confidentiality of the transmitted message. To ensure messages are transferred securely and safely over the network, a suitable method that can keep the message secured is required. To achieve this, Steganography is one of the trustable methods that provide secured means of messages transfer. In steganography, the data are hidden in the cover media which can be in the form of image file, text file, video file, or audio file. Generally, steganography is defined as a science or art of hiding message inside some cover medium known as carrier as highlighted by [2], [3]. To further enhance the security architecture of the steganography, the secret message is first encrypted using cryptography technique before embedding it onto the cover image, the image that contain the secret message is known as stego image or payload, which is mathematically expressed as:

$$Stego - medium = Cover\ medium + \cdots message + secret\ key \quad (1)$$

The encrypted text generally known as cipher text can then be sent over the network safely. To recover the message at the receiver end, a decrypting algorithm that uses the generated private key during encryption is required [4]. Therefore, a combination of cryptography and steganography helps to improve security level of the data being transmitted. If

Corresponding author: Rabiu. H. ✉ rabiuhabib@gmail.com *Department of Electrical Engineering, Bayero University, Kano.*

image is used as a cover medium, the security of the message can be increased by embedding the data into the red plane of the image as it is less perceptible to human eye [5].

Quality of steganography is measured using minimum error difference between the pixel values of the stego image and those of the original image. Imperceptibility is a crucial key requirement of a good steganography system, without which it can attract attention and get compromised easily. Steganography often takes advantage of the limited capabilities of the human biological system. For instance, image steganography is drawn upon the visual limited capabilities of the Human Visual System (HVS) which cannot detect the slight intensity variation of pixels of an image especially the red plane of the image. As a result, hiding the secret data into the LSBs of the original image would only marginally change the colour intensities of the carrier image so much that it would be unnoticeable by a human naked eye. Thus, an unauthorized observer cannot distinguish between the original carrier image and the stego image [6].

REVIEW OF RELATED WORKS

In research conducted by [7], in which a robust approach of information security was proposed. It presents two components based LSB steganography methods for embedding secret data in the least significant bits of blue components and partial green components of random pixel locations in the edges of images. They further, employed adaptive LSB based steganography for embedding data based on data available in Most Significant Bits (MSB's) of red, green, and blue components of randomly selected pixels across smooth areas. The new method proved to be more defiance to steganalysis attacks like visual analysis, histogram analysis, chi-square,

In another account [8] employed a novel steganographic method, in which immune programming (IP) algorithm was used to find a near-optimal solution for the pairwise least significant bit (LSB) matching scheme. This strategy was inspired from human immune systems. The immune system of living beings is composed of a great variety of molecules, cells and organs in the body which can distinguish between self-cells and non-self-cells, and can also learn and memorize the types of cells. This way, the immune system performs several functions to maintain a stable state of vital functions, protect the body against attack by diseases and eliminate malfunctioning cells. The developmental stages of immune system include; clonal selection, negative selection and affinity maturation. The mechanism of identification, memory and learning in the immune system is facilitated by pattern recognition expert which leads to the discovery of Immune Programming (IP). The stages in IP consist of crossover, mutation, vaccination and annealing selection. The IP strategy is used in the LSB matching to find a nearly optimal adjustment list.

[9], developed a method to embed a series of ternary secret data into a cover image based on an improved LSB scheme using the modulo three strategies. The new method can hide two ternary numbers into each grayscale pixel, normally only the two LSBs of the pixel are modified, while it may cause overflow/underflow and a carry/borrow. This problem is solved by adding 1 to the pixel or subtracting 1 from the pixel before embedding. The embedding capacity of this method is high. At the same time, the quality of the stego image of this method is better than traditional LSB scheme when embedding capacity is greater than 3 bpp (bits per pixel) with a PSNR greater than 37 dB. Experimental results indicated that the new method is capable of getting a higher PSNR than traditional LSB scheme when the embedding capacity is greater than 3 bpp, and it has higher resistance ability against the chosen steganalysis algorithm when embedding capacity is low.

In the work of [10], the authors proposed an adaptive LSB substitution method using uncorrelated colour space, this increases the attribute of imperceptibility while minimizing the chances of detection by the human vision system. In this scheme, the input image is passed through an image scrambler, resulting in an encrypted image, preserving the privacy of image contents, and then converted to HSV (Heu, Saturation, Value) colour space for further processing. The secret contents are encrypted using an iterative magic matrix encryption algorithm (IMMEA), which subsequently produce the cipher contents. Finaly,

Corresponding author: Rabiu. H. ✉ rabiuhabib@gmail.com Department of Electrical Engineering, Bayero University, Kano.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 10(3), SEPTEMBER, 2022
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com

an adaptive LSB substitution method is then used to embed the encrypted data inside the V-plane of HSV colour model based on secret key-directed block magic LSB mechanism. The results from this method and its application for addressing the security and privacy of visual contents in online social networks (OSNs) confirm its effectiveness in contrast to traditional LSB. However, this method is not very robust as the embedded data can still easily be decoded.

In a recent work published by [11], a new approach using least significant bit steganography to improve on the 1 byte least significance technique combined with cryptography was reported. They presented detail description of image steganography using LSB to reduce the possibility of a message being intercepted and uncovered.

[12] Introduced picture steganography algorithm based on the Artificial Immune System in which a congregation picture is used as the cover image. The host picture is then partitioned into blocks, where the artificial immune system finds the proper locations for inserting message bits within the cover picture's pixels. This way, faster embedding of the secret message is achieved.

PROPOSED METHOD

The purpose of applying Immune Programming is to adjust the order of the secrete bits in such manner that guarantees minimal variation with the cover image bits. If the matching order is properly adjusted, the output image will generally have fewer changes in its pixel values, thus becomes less attractive to steganalysis attack. Figure1 illustrates the general frame work of the proposed method.

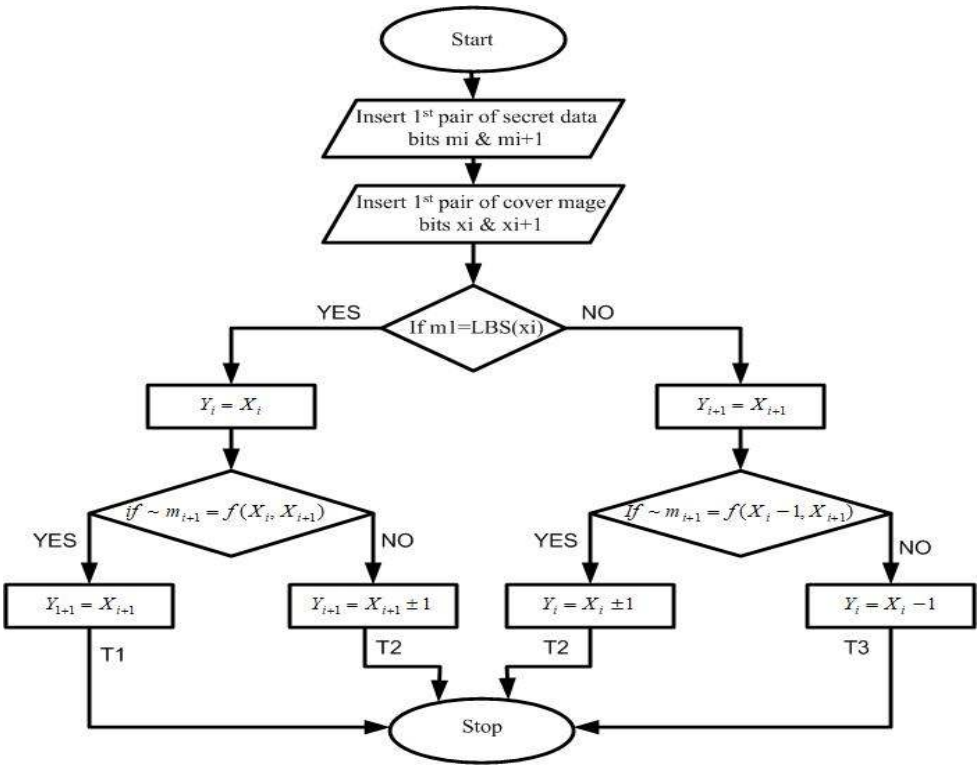

Figure 1: General flow chart of the proposed Algorithm

Corresponding author: Rabiu. H. rabiuhabib@gmail.com *Department of Electrical Engineering, Bayero University, Kano.*

Note that; the $f(xi, xi+1)$ is represented as the lsb of $(xi/2 + xi + 1)$. Note also in the process of computing $f(xi, xi + 1)$ any result that yields fraction is always rounded downwards. The Ti, T2 and T3 are weights used in generating tier score matrix and are assigned based on their relevance. Where T1=10, T2=5 and T3=0

To illustrate how the new algorithm work, let's the cover image be matrix "H" and the secrete message be "S"

$$H = \begin{bmatrix} 181 & 168 & 245 & 192 \\ 193 & 42 & 87 & 66 \\ 71 & 31 & 150 & 130 \\ 174 & 128 & 58 & 179 \end{bmatrix}$$

$$S = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

To transform the matrices into streams, simply write them out row-wise as illustrated below.

H' = [181 168 245 192 193 42 87 66 71 31... 150 130 174 128 58 179] (2)

S' = [1 0 0 1 0 1 1 1 0 0 0 0 0 1 1 0] (3)

Next, we need to generate a score matrix using the algorithm in Figure 1. To do that lets; $M_i \; and \; M_{i+1}$ represent the first pair of the secret message bits and $X_i \; and \; X_{i+1}$ represent the first pair of the cover image bits.

That is, the first pair of cover pixel values [181,168] and secret data values [1,0] in this example;

$$X_i = 181\,, \qquad X_{i+1} = 168$$
$$M_i = 1\,, \qquad M_{i+1} = 0$$

At this stage we test to see if

$$M_i = \; lsb(X_i)$$

as dictated by Figure 1. But in this case, ($M_i = 1 \; and \; X_i = 181$) which satisfy the condition. Therefore, we set the output pixel to be $Y_i = X_i$ else, $Y_{i+1} = X_{i+1}$.

Next, we move down the algorithm to test for $M_{i+1} = \; f(X_i \; , \; X_{i+1})$
That is in this example, $M_{i+1} = f[(181/2) + (168)]$, rounding off downward
$M_{i+1} = lsb(258.5)$
Since the $m_i + 1 = M_{i+1} = lsb(258) = 0$. and thus, this expression is true. Therefore, using the flow chart we arrived at $T_1 = 10$

Similarly, using the same procedure above which landed us to T1, the scores of each cover pixel pairs and secrete data pairs, can be determined as given by matrix M.

Corresponding author: Rabiu. H. rabiuhabib@gmail.com Department of Electrical Engineering, Bayero University, Kano.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 10(3), SEPTEMBER, 2022
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com

$$M = \begin{bmatrix} 10 & 10 & 5 & 5 & 10 & 5 & 5 & 0 \\ 0 & 0 & 0 & 5 & 0 & 10 & 10 & 5 \\ 0 & 0 & 0 & 5 & 0 & 10 & 10 & 5 \\ 5 & 5 & 5 & 10 & 0 & 0 & 0 & 5 \\ 5 & 5 & 5 & 0 & 5 & 0 & 5 & 10 \\ 5 & 5 & 5 & 0 & 5 & 0 & 5 & 10 \\ 0 & 0 & 0 & 5 & 0 & 10 & 10 & 5 \\ 10 & 10 & 5 & 5 & 10 & 5 & 5 & 0 \end{bmatrix} \quad (4)$$

Once the score matrix M is determined, an adjustment list J which also serve as the encryption key can be generated by visiting at the columns and selecting the maximum entries from each column without repeating a row position which was earlier selected. This leads to getting a highest score value. In this case the J matrix is derive from elements in the following positions: (1,1), (8,2), (6,3), (4,4), (5,5), (7,6), (2,7) and (3,8) are selected with a total sum of 65, which also produced an adjustment list of;

$$J = [1,8,6,4,5,7,2,3] \quad (5)$$

$$f(J) = \frac{1}{f^M} \Sigma \, \mathrm{m(i,j)} J,$$

$$f^M = Ls.T1$$

where;

f^M is the maximum score for the adjustment list and Ls is number of rows in the score matrix. T_1 = 10, $m(i,j) =$ element of a score matrix at a particular position

To get the optimal matching order that minimizes the distortion of the stego image, the adjustment list F(J) needs to have the highest score.

Therefore,

f^M = Ls. T_1

L_s = 8

T_1 = 10

f^m = 8 x 10 = 80

$\sum m(i,j) =$ (10 + 10 + 0 + 10 + 5 + 10 + 10 + 10) = 65

$$F(J) = \frac{65}{80} = 0.8125$$

Encryption

Now having generated the secret key, we are in a position to start encrypting the message. Remember that our original message was given as equation 3. To start the encryption proper, we reorder the pairs of bits belonging to the original message entries using the matrix J as follows:

$$J = [1,8,6,4,5,7,2,3]$$

Corresponding author: Rabiu. H. rabiuhabib@gmail.com *Department of Electrical Engineering, Bayero University, Kano.*

The first number 1 in the J matrix means that the first pair of the message should remain unchanged, the second number which is 8 in J matrix means that the eighth pair of the message should replace as the second pair. This continues until all entries of the message are rearrange according to J matrix. Finally.

S' = [1 0 0 1 0 1 1 1 0 0 0 0 0 1 1 0], now becomes;

S'' = [1 0 1 0 0 1 1 1 0 0 0 1 0 1 0 0] (6)

Now, the new re-ordered secrete data streams can be embedded into the cover image to form a stego image with fewer pixel changes.
The cover image H' equation (2) and the re-ordered secrete bits S'' equation (6) are; combine together using the embedding algorithm as;

$M_i \; and \; M_{i+1}$ represent the first pair of the secret message bits.

X_i , X_{i+1} represent the first pair of the cover image bits.

Y_i , Y_{i+1} will therefore represent the pair of the stego image.

For the first pair of cover pixel values [181,168] and secret data values [1,0];

$$X_i = 181\,, \qquad X_{i+1} = 168$$

$$M_i = 1\,,\; M_{i+1} = 0$$

Since $M_i = lsb(X_i) = M_i = 1$; Therefore, $Y_i = X_i = 181.$

Elseif

$$M_{i+1} = f(X_i\,, \qquad X_{i+1}) \ldots = f[(181/2) + (168)]$$

$M_{i+1} = lsb(258.5)$ rounding off downward

M_{i+1} = lsb (258) this expression is true. Therefore, $Yi + 1 = Xi + 1 = 168$

Hence, the first pair of the stego pixels Y_i and Y_{i+1} are 181 and 168 respectively.
This procedure is repeated for all pairs to generate other stego pixel values which yield the stego stream as in equation (7).

$$St' = [181\ 168\ 245\ 192\ 194\ 42\ 87\ 66\ 70\ 31 \ldots$$
$$150\ 130\ 174\ 128\ 58\ 179] \qquad (7)$$

Reshaping the stego streams into its corresponding matrix, it results as;

$$St = \begin{bmatrix} 181 & 168 & 245 & 192 \\ 194 & 42 & 87 & 66 \\ 70 & 31 & 150 & 130 \\ 174 & 128 & 58 & 179 \end{bmatrix} \qquad (8)$$

By comparing the cover image matrix with the stego image matrix, the MSE and PSNR can be calculated.

Corresponding author: Rabiu. H. rabiuhabib@gmail.com Department of Electrical Engineering, Bayero University, Kano.

$$H = \begin{bmatrix} 181 & 168 & 245 & 192 \\ 193 & 42 & 87 & 66 \\ 71 & 31 & 150 & 130 \\ 174 & 128 & 58 & 179 \end{bmatrix} \quad St = \begin{bmatrix} 181 & 168 & 245 & 192 \\ 194 & 42 & 87 & 66 \\ 70 & 31 & 150 & 130 \\ 174 & 128 & 58 & 179 \end{bmatrix}$$

Noticed some slight variations at entries corresponding to positions (2,1) and (3,1). To compute the MSE of the stego, equation (9) is used.

$$MSE = \frac{1}{mn}\sum_0^{m-1}\sum_0^{n-1}\|f(i,j) - g(i,j)\|^2 \quad (9)$$

$$= \frac{(193-194)^2+(71-70)^2}{4\times4}$$

$$= \frac{2}{16} = 0.125$$

Also, the PSNR can be computed using equation (10) thus;

$$PSNR = 10log_{10}\frac{255}{0.125} = 57.1617\text{dB}$$

RESULTS AND DISCUSSION

The performance metrics used in this work are MSE and PSNR. Table 4.1 presented the indices where different cover messages are used.

Table 4.1. Results of MSE and PNSR

Stego Image	Message Size	Proposed Method (dB)	Proposed Method MSE
Girl	8kb	52.3161	0.3815
Baboon	8kb	52.4560	0.3694
Lena	8kb	52.4070	0.3736
Clock	8kb	53.0095	0.3762

From the results presented in Table 1, it can be seen clearly that, the modified LSB pairwise using immune programming technique have yielded low Mean Square Error across different image covers used. The new method also re-orders the sequence of the secret message bits in a manner that guarantees minimum changes of pixel between the cover image and the stego image.

It can also be seen that the proposed method has a good PSNR values across all cover images used. This means that the quality of the generated images using this method is preserved.

CONCLUSION

This article presented a new steganographic method that used modified LSB pairwise manipulation technique using IP approach. The result obtained have demonstrated a significant improvement in terms of MSE and PSNR as compared with other similar methods. The lower MSE suggests the new method has very low pixels variations as compared with the original image, this also implies that the output image will be less suspicious and unattractive to hackers. In addition, the higher PSNR implies good preservation of the image quality. Further works should focus on improving the secret key technique, to make it a multi-level encryption method.

Corresponding author: Rabiu. H. rabiuhabib@gmail.com *Department of Electrical Engineering, Bayero University, Kano.*

REFERENCES

[1] V. M. Potdar and E. Chang, "Grey level modification steganography for secret communication," in *2nd IEEE International Conference on Industrial Informatics, 2004. INDIN'04. 2004*, 2004, pp. 223–228.

[2] S. Atawneh, A. Almomani, and P. Sumari, "Steganography in digital images: Common approaches and tools," *IETE Tech. Rev.*, vol. 30, no. 4, pp. 344–358, 2013.

[3] K.-H. Jung, "Dual image based reversible data hiding method using neighbouring pixel value differencing," *Imaging Sci. J.*, vol. 63, no. 7, pp. 398–407, 2015.

[4] H. C. Stenbaek-Nielsen, T. J. Hallinan, and L. Peticolas, "Why do auroras look the way they do?," *Eos Trans. Am. Geophys. Union*, vol. 80, no. 17, pp. 193–199, 1999.

[5] S. A. Laskar and K. Hemachandran, "Steganography based on random pixel selection for efficient data hiding," *Int. J. Comput. Eng. Technol.*, vol. 4, no. 2, pp. 31–44, 2013.

[6] N. F. Johnson, Z. Duric, and S. Jajodia, *Information hiding: steganography and watermarking-attacks and countermeasures: steganography and watermarking: attacks and countermeasures*, vol. 1. Springer Science & Business Media, 2001.

[7] M. Juneja and P. S. Sandhu, "A new approach for information security using an improved steganography technique," *J. Inf. Process. Syst.*, vol. 9, no. 3, pp. 405–424, 2013.

[8] H. Xu, J. Wang, and H. J. Kim, "Near-optimal solution to pair-wise LSB matching via an immune programming strategy," *Inf. Sci.*, vol. 180, no. 8, pp. 1201–1217, 2010.

[9] W.-L. Xu, C.-C. Chang, T.-S. Chen, and L.-M. Wang, "An improved least-significant-bit substitution method using the modulo three strategy," *Displays*, vol. 42, pp. 36–42, 2016.

[10] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, "Image steganography using uncorrelated color space and its application for security of visual contents in online social networks," *Future Gener. Comput. Syst.*, vol. 86, pp. 951–960, 2018.

[11] O. Rachael, S. Misra, R. Ahuja, A. Adewumi, F. Ayeni, and R. Mmaskeliunas, "Image steganography and steganalysis based on least significant bit (LSB)," in *Proceedings of ICETIT 2019*, Springer, 2020, pp. 1100–1111.

[12] P. Navya, "High secured steganography using artificial Immune system," *Turk. J. Comput. Math. Educ. TURCOMAT*, vol. 12, no. 13, pp. 1411–1424, 2021.

Corresponding author: Rabiu. H. ✉ rabiuhabib@gmail.com *Department of Electrical Engineering, Bayero University, Kano.*