Implementation and Comparative Analysis of Variants of LSB Steganographic Method

Conference Paper · January 2022

DOI: 10.1109/SAUPEC55179.2022.9730643

Temitayo Olutimi Ejidokun
Afe Babalola University
18 PUBLICATIONS **51** CITATIONS

Olusegun O. Omitola
Afe Babalola University
33 PUBLICATIONS **138** CITATIONS

Implementation and Comparative Analysis of Variants of LSB Steganographic Method

Temitayo Ejidokun
Department of Electrical, Electronics and Computer Engineering
Afe Babalola University,
Ado-Ekiti, Nigeria
engrtayo@gmail.com

Olusegun O. Omitola
Department of Electrical, Electronics and Computer Engineering
Afe Babalola University,
Ado-Ekiti, Nigeria
omitolasegun@gmail.com

Ifeoma Nnamah
Department of Electrical, Electronics and Computer Engineering
Afe Babalola University,
Ado-Ekiti, Nigeria
ifeomannamah@yahoo.com

Kehinde Adeniji
Department of Electrical, Electronics and Computer Engineering
Afe Babalola University,
Ado-Ekiti, Nigeria
Kehindeadeniji@ymail.com

2022 30th Southern African Universities Power Engineering Conference (SAUPEC) | 978-1-6654-6887-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/SAUPEC55179.2022.9730643

***Abstract*— In this 21st century, the inability to securely transmit information over a digital medium has been a major problem because the information stands a chance of being intercepted by hackers before it reaches its destination. Therefore Stenography was introduced to prevent sensitive information from been accessed by unauthorized persons. Stenography is a method of encrypting data as related to cryptography but hides a message in plain sight thereby making it a more secure method of sending across secret information. In this study variants of the least significant bit (LSB) method was implemented and performance comparative analysis was carried out across three image format. The result obtained from that the mean square error (MSE) and peak signal to noise ratio PSNR analysis, indicate that PNG and Bitmap image performed better than GIF images**

Keywords—Stegobit, Steganography, Stego-image, LSB, PSNR, MSR

I. INTRODUCTION

The recent advancement in multimedia technologies has aided the seamless and faster exchange of information, over the network. Also, the global internet revolution through digitalization has boasted data sharing and usage, via cloud-based infrastructures [1]-[4]. However, securing such information from unauthorized persons or organizations is a major concern of modern societies, which is a difficult task to achieve. In an attempt to solve this problem, techniques based on cryptography and steganography are considered the main mechanisms for data security [5]-[6].

The use of cryptographic techniques to encrypt information results in the rearrangement of information to be secured so that it is can not be easily detected and intercepted by intruders. The basic authentication approach includes the use of hashing, digital signatures, or also setting up threshold values for embedding secret bits. Oftentimes cryptography method does not adequately guarantee that the secret information is completely secured. Therefore, there was an increased need, to introduce steganography [7]-[8]. For this reason, experts often recommend that both steganography and cryptography constitute multiple layers of security.

Image steganography protects sensitive information by hiding it in images, which should not be detected by the human sense of vision. Image steganography has been applied in various fields such as communications and mobile computing. It has also been implemented in online voting systems, surveillance systems as well as medical applications for securing medical records [9]-[10]. Several image steganography techniques have been developed and implemented over the years. The LSB method; the simplest method under the spatial domain category, is based on encoding secret information into the least significant bits of each pixel of an image. The technique provides some levels of confidentiality whenever information is transmitted over the internet. The advantages of the LSB methods are the low values of mean square error (MSE), and the high values of peak signal to noise ratio (PSNR), which make it tough for the human eye to recognize. Because of these advantages, the LSB method is commonly used in the development of image steganography applications.

A k-LSB-based method for hiding an image inside another image using k least bits was implemented in [11]. A local entropy filter was used for the identification of the bit containing the concealed image. The outcome of the proposed study revealed that images can be concealed with very minimal distortion and loss of information. An enhanced LSB substitution technique of image-based steganography was implemented in [12]. This technique was used to provide double security by initially encrypting the message to be embedded before its conversion into stego-image. The method was able to achieve a significant increase in embedding capacity with good PSNR.

In [13], an automated method to secure a secret message using a dual level of security was developed. The secret message was encrypted with an encryption method developed in Java, named Character Bit Shuffler (CBS) for the first level. For the second level, the encrypted secret message bits were then inserted inside an image using the least significant bit (LSB) technique. The method was adopted for its simplicity and ability to retain the image quality. An improved LSB Steganography approach based on the use of modulus function for data hiding information was proposed in [14]. A method for hiding the secret message bits in the pixels of an RGB true colour image using a secret key was developed in [15]. Furthermore capacity of the image to be transmitted was increased by reducing the secret data that have seven bits in ASCII to five-bit streams.

978-1-6654-6887-9/22/$31.00 ©2022 IEEE

The concluded result showed the capacity of the image can be increased up to 30% and the PSNR (Peak Signal to Noise Ratio) improved up to 27% when compared to other existing techniques. Therefore, this study aims to implement a variant of the LSB substitution method (i.e. Stego 1, 2, 3, and 4) in three image formats (GIF, Bitmap and PNG) and also carry out its comparative analysis.

II. METHODOLOGY

A. *Overview of the images-based steganography*

Fig. 1 gives a diagrammatic illustration of the process of hiding secret messages in a given media. It also highlights the components of a typical steganographic system. The two main processes are based on the embedding and extraction of text-based messages at the sender and receiver's side respectively. The embedding process involves the hiding of secret messages in a cover image using a stego-key, thereby producing a stego-image. Afterward, the embedded image is sent over a transmission medium to the receiving party.

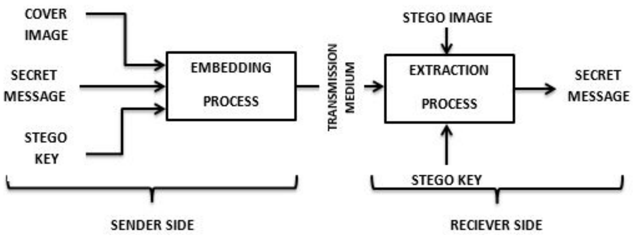


Fig. 1. A typical steganographic system

At the receiver's end, the retrieval of the secret message from the stego-image with the aid of a stego-key is carried out. Subsequently, after successful extraction, the secret message appears in text format.

B. *The mathematical formulation for the LSB steganographic Techniques*

In this study, the LSB substitution method was used to embed text in 8-bit grayscale cover images (GIF) and 24-bit color images (bitmap and PNG). For an 8-bit grayscale image denoted as $I_{grayscale}$ of size, $P_{I_{gray}} \times Q_{I_{gray}}$, the pixel is represented in equation 1 as follows:

$$I_{gray} = \left\{ x_{ij} \middle| 0 \le i \le P_{I_{gray}}, 0 \le i \le Q_{I_{gray}}, x_{ij} \in \{0,1,2.....,255\} \right\} \quad (1)$$

Also, for a 24 –bit color cover image denoted as I_{color} of size $P_{I_{color}} \times Q_{I_{color}} \times 3$, the pixel represention for the three color components red, green, and blue is given in equation 2 as follows:

$$I_{color\ \ red} = x^{red}_{ij} \left| \begin{matrix} 0 \le i \le P_{I_{color\ \ red}}, \\ 0 \le i \le Q_{I_{color\ \ red}}, x^{red}_{ij} \end{matrix} \right. \in \{0,1,2.....,255\}$$

$$I_{color\ \ green} = x_{ij}^{\ green} \left| \begin{matrix} 0 \le i \le P_{I_{color\ \ green}}, \\ 0 \le i \le Q_{I_{color\ \ green}}, x_{ij}^{\ green} \end{matrix} \right. \in \{0,1,2.....,255\} \quad (2)$$

$$I_{color-blue} = \left\{ x_{ij}^{\ blue} \left| \begin{matrix} 0 \le i \le P_{I_{color-blue}}, \\ 0 \le i \le Q_{I_{color-blue}}, x_{ij}^{\ blue} \end{matrix} \right. \in \{0,1,2.....,255\} \right\}$$

Given that S is the n-bit of the secret message to be embedded into the 8-bit grayscale and 24-bit color image is defined in equation 3.

$$S = \left\{ s_i \middle| 0 \le i \le n, s_i \in \{0,1\} \right\} \quad (3)$$

Furthermore, the secret message is re-arranged to form a k-bit virtual message S' given in equation 4.

$$S' = \left\{ s'_i \middle| 0 \le i \le n', s_i \in \{0,1,......2^{k-1}\} \right\} \quad (4)$$

Where $n' = P_{I_{gray}} \times Q_{I_{gray}}$ and $n = P_{I_{color}} \times Q_{I_{color}}$

Also a mapping between the secret message (S) and embedded message (S') resulted into equation 5.

$$s'_i = \sum_{j=0}^{k\ \ 1} s_i \times k + j \times 2^{k\ \ 1\ \ j} \quad (5)$$

Hence, the embedding process is completed for k (k =1, 2, 3, 4) of each pixel by S'. Therefore each pixel storing the k-bit message for a stego-pixel based on equation 6.

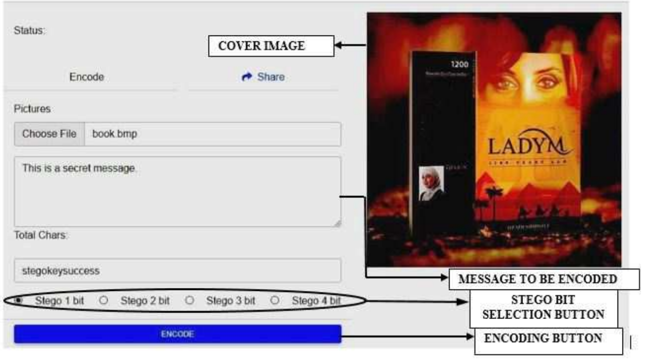
$$x'_i = x_i \bmod 2^k + s'_i \quad (6)$$

Lastly, the embedded image is extracted from the stego-image using equation 7.

$$s'_i = x_i \bmod 2^k \quad (7)$$

C. *Web-based Implementation*

The LSB technique was implemented on a web-based interface using python programming language connected to the Mysql database as shown in Fig. 2 and 3. On the sender's side, the system allows the user to select a suitable cover image, enter the message to be embedded into the cover image, input the stego-key and choose the desired mode of encryption as shown in Fig. 2.


Pictures: Choose File book.bmp

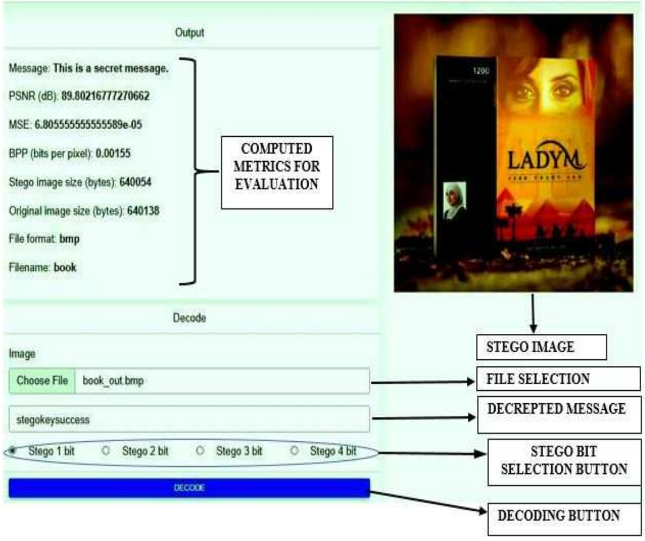
This is a secret message.

stegokeysuccess

● Stego 1 bit ○ Stego 2 bit ○ Stego 3 bit ○ Stego 4 bit

Fig. 2. Simple GUI at the sender's side

After all the required inputs have been entered, the user clicks the Encode button to start the embedding process. On completion, the system would display a confirmation text indicating that the message has been embedded successfully. At the receiver's end the embedded can be retrieved, after selecting the appropriate input variable on the GUI interface as shown in Fig. 3. Also for the purpose of this study the computed metrics of evaluation can be visualized on the receiver's side.



Output

Message: This is a secret message.

PSNR (dB): 89.80216777270662

MSE: 6.805555555555589e-05

BPP (bits per pixel): 0.00155

Stego image size (bytes): 640054

Original image size (bytes): 640138

File format: bmp

Filename: book

Decode

Image

Choose File book_out.bmp

stegokeysuccess

● Stego 1 bit ○ Stego 2 bit ○ Stego 3 bit ○ Stego 4 bit

Fig. 3. Simple GUI at the receiver's side

D. Modalities of Data Collection and Criteria for Evaluation

Ten images for each of the formats namely; GIF, BITMAP, and PNG were obtained from the internet and used for the evaluation of the technique. The considered evaluation metrics are; Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE)

Mean Square Error gives an estimate of the resultant error in the cover image due to the embedded data. It can be computed mathematically using equation 8.

$$MSE = \sum_{I=1}^{N} (C_i - C_i')^2 \qquad (8)$$

Where C_i denotes the size of stego image, C_i^I is the size of the cover image, N = size of the original image. PSNR is used to measure the degree of distortion caused by the embedded data. Mathematically, the PSNR can be calculated using equation 9.

$$PSNR(decibel) = 10\log_{10}(\frac{255}{MSE}) \qquad (9)$$

A high computed value of PNSR indicates the image is less distorted by the data and vice versa.

III. RESULTS AND DISCUSSION

A. Computation of peak signal to noise ratio (PSNR)

Figure 4 shows a bar graph of the computed average PSNR for the considered variants (stego 1, 2, 3, and 4), tested with PNG, BMP, and GIF images. It can be observed that as the stego bits used to embed the secret message bits increase, the average value of the peak signal to noise ratio for each stego bit decreases. This is an indication that, as more stego-bit is replaced by the message bit, the stego-image becomes distorted, thereby exposing the secret message to a security threat. Furthermore, the PSNR for the PNG image is relatively higher for stego 1-3 bit, while the PSNR for the GIF image is relatively low compared to other image formats.

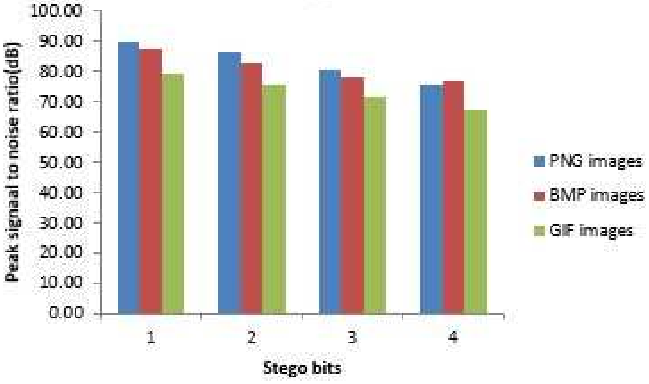


Fig. 4. Bar chart showing the PSNR computation

B. Analysis for mean square error (MSE) and stego bits

The line plot in Fig. 5, gives the computed average MSE value across the considered image formats for stego 1-4 bit. It was observed that the error for the three image formats was very minimal at stego 1 bit. Consequently, the errors becomes more significant as the replacing stego bit increases. As the stego bit increases the errors in GIF images become very significant when compared with other image formats(PNG and Bitmap).

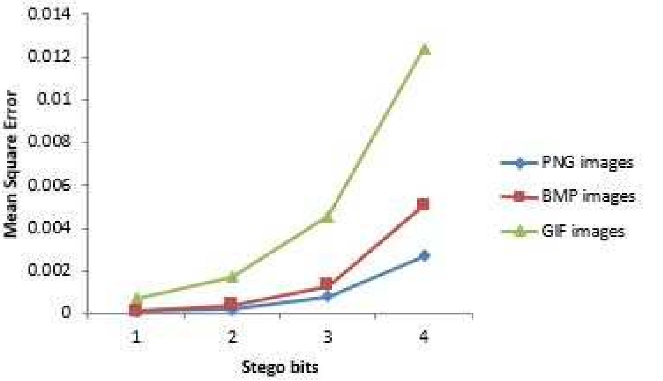


Fig. 5. MSE computation across all image formats

CONCLUSION

This study has carried out a comparative study on the performance of the variant of the LSB substitution method on three different image formats. In the course of the evaluation, it was observed that as the replacing stego-bit increases there is always a relative drop in the PSNR while the MSE increases, leading to the distortion of the image used for hiding the secret message. However, the security of the embedded message largely depends on the degree of perceptibility of the image. Because steganographic methods are not 100% safe, it is crucial to use caution while concealing sensitive information.

Based on the results obtained, it is suggested that the cover picture should be large enough to hold the secret data, with the data containing no more than 20% of the cover image on average. Also, the amount of data to be hidden should be as small as possible to avoid using up too many pixels.

REFERENCES

[1] R. L, Ambika, Biradar, and V. Burkpalli. Encryption-based steganography of images by multiobjective whale optimal pixel selection. International Journal of Computers and Applications, 1-10., 2019

[2] K., Bailey, & K. Curran. An evaluation of image based steganography methods. Multimedia Tools and Applications, 30(1), 55-88, 2006

[3] R., Bhardwaj, & V. Sharma. Image steganography based on complemented message and inverted bit LSB substitution. Procedia Computer Science, 93, 832-838, 2016

[4] Danny Adiyan, Z., Purboyo, T. W., & Nugrahaeni, R. A. (2018). Implementation of secure steganography on jpeg image using LSB method. International Journal of Applied Engineering Research, 13(1), 442-448.

[5] X. Li, and J. Wang, A steganographic method based upon JPEG and particle swarm optimization algorithm. Information Sciences, 177(15), 3099-3109. 2007

[6] J. D Teja,. A. C. S., Rao, & S. Dara, A new image steganography technique for hiding the data in multilayers of the PNG images. Int J Ad Hoc Ubiquitous Comput., 2(7), 104-112, 2017.

[7] A. F., Tukiwala, and Degadwala, S. D. (2014). Data Hiding in Image using Multilevel 2-D DWT and ASCII Conversion and Cyclic Mathematical Function based Cryptography. International Journal of Computer Applications, 105(7).

[8] F. A., Rafrastara, R., Prahasiwi, E. H., Rachmawanto, & C. A. Sari, Image Steganography using Inverted LSB based on 2 nd, 3 rd and 4 th LSB pattern. In *2019 International Conference on Information and Communications Technology (ICOIACT)* (pp. 179-184). 2019.

[9] M., Jain, and A. Kumar., RGB channel based decision tree grey-alpha medical image steganography with RSA cryptosystem. International Journal of Machine Learning and Cybernetics, 8(5), 1695-1705. 2017

[10] S., Rustad, A., Syukur, & P. N. Andono. Inverted LSB image steganography using adaptive pattern to improve imperceptibility. Journal of King Saud University-Computer and Information Sciences, 2019

[11] O., Elharrouss, N., Almaadeed, & S. Al-Maadeed,. An image steganography approach based on k-least significant bits (k-LSB). In 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT) (pp. 131-135), 2021

[12] A., Arora, M. P., Singh, P., Thakral, & N. Jarwal, Image steganography using enhanced LSB substitution technique. In 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC) (pp. 386-389). 2016.

[13] A., AlWatyan, W., Mater, O., Almutairi, M., Almutairi, & A. Al-Noori, Security approach for LSB steganography based FPGA implementation. In 2017 7th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), pp. 1-5, 2017

[14] N., Akhtar, V., Ahamad, & , H. Javed A compressed LSB steganography method. In 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT) (pp. 1-7)., 2017.

[15] A., AlWatyan, W., Mater, O., Almutairi, M., Almutairi, & A. Al-Noori. Security approach for LSB steganography based FPGA implementation. In 2017 7th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO) (pp. 1-5), 2017.