American Journal of Engineering Research (AJER)
E-ISSN: 2320-0847 p-ISSN: 2320-0936
Volume-8, Issue-2, pp-39-44
www.ajer.org
Research Paper Open Access

A Robust and Secured Image Steganography using LSB and Random Bit Substitution

U. A. Md. Ehasn Ali[1], Md. Sohrawordi[1], Md. Palash Uddin[1]
[1](Department of Computer Science and Engineering, Hajee Mohammad Danesh Science and Technology University, Dinajpur-5200, Bangladesh)
Corresponding Author: U. A. Md. Ehasn Ali

ABSTRACT :*In the era of information, secret communication is one of the most important issues in today's communication systems. The development of digital communication with data secrecy becomes one of the main purposes of the researchers. Among the data security techniques, steganography is an approach to hide the existence of secret message in a carrier without being apprehended by the intruders. At present, it is important to hide data as well as develop mechanisms by transporting them in such a way that the intruders cannot understand the message. There are various data hiding methods that use different digital media. Digital images are the most popular among the carrier formats because of their frequency on the Internet. In this paper, a new approach of image steganography with least significant bit substitution is proposed where the information embedded in the random bit position of a pixel. The experimental result signifies the importance of the proposed method.*

KEYWORDS: *steganography, LSB substitution, data hiding, embedded message, retrieved message.*

Date of Submission: 22-01-2019 Date of acceptance: 07-02-2019

I. INTRODUCTION

Communication in secret ways with others has always been one of the well-known glitches from the ancient times. Nowadays, although cryptography and steganography are used for secured communication but they are different in nature [1]-[6]. As cryptography reforms a message, it cannot be understood whereas steganography hides the message so that it cannot be seen. The aim of steganography is to embed the communication content in a public cover media [2], [3], [6]. As a result, the presence of concealed message can be hidden. Digital steganography is the science of transferring information with secret message embedded in it. Thus, steganography is a form of security technique where the existence of a message is kept hidden between the sender and the intended recipient. Steganography is classified into 3 categories [2], [8]-[10],

- Pure steganography with no stego key. Here, the communicating parties assume that no other party is aware of the communication.
- Secret key steganography with the stego key. Here, the communicating parties exchange the key prior to communication. This is most susceptible to interruption.
- Public key steganography with a public key and a private key. Here, the both keys are used for secure communication.

In general, Steganography focuses on hiding the secret messages in carriers with unnoticed and less attractive way. Almost all digital file formats can be used as a carrier, but the suitable formats are those which have a high degree of redundancy. There are various methods and algorithms of hiding data in different types of digital file formats. There are many suitable steganographic techniques which are being used to obtain security depending on the type of the carrier [2], [8]-[10].

- Image Steganography: When an image used as a cover object in steganography, it is known as image steganography. Generally, pixel intensities of the image are used to hide the information in these techniques.
- Network Steganography: Taking network protocol, such as TCP, UDP, ICMP, IP etc. as cover object, is known as network protocol steganography. Here, steganography can be achieved by using unused header bits of network protocols.

- Video Steganography: In video Steganography, the carrier for hidden information is video (combination of pictures). To hide the information in each of the images in the video, normally, discrete cosine transforms (DCT) technique is used. Various video formats such as H.264, Mp4, MPEG, AVI etc. are used in video steganography.
- Audio Steganography: While using audio as a carrier for hiding information, it is called audio steganography. Because of popularity of voice over IP (VOIP), it has become very important medium. Digital audio formats such as WAVE, MIDI, AVI MPEG or etc. are used for this steganography.
- Text Steganography: To achieve information hiding in text steganography, different techniques such as capital letters, white spaces, number of tabs, just like Morse code and etc. is used.

II. IMAGE STEGANOGRAPHY

In today's world, almost in every page on the internet, digital images can be found due to the easiest distribution. Therefore, image files are the most commonly used environments for steganography applications, although they vary according to the formats used [2], [8]-[10]. The human visual system has a weakness that is; it has a low sensitivity towards random pattern changes and luminance. The human eye cannot detect the small changes in color or patterns and due to this weakness, text or graphic files can be inserted into the carrier image without being detected. For example, an image file with an encoded text stored in it results another image file, called "stego image", that is physically and visually not the same from the original. Hence, an eavesdropper only sees a picture that is transferred between the two parties when a communication take place between them, but they are unaware of the hidden messaging actually takes place by this picture. However, an image is a collection of individual points, referred to as pixels that constitute different light intensities in different areas of the image. In an image, the pixels are presented horizontally row by row. Different color schemes use different number of bits for each pixel, called the bit depth. The smallest bit depth in current color schemes is 8, that is, to represent the color of each pixel 8 bits are used (corresponding to 2^8 = 256 colors). 8 bits are used in monochrome and grayscale images for each pixel and are able to display 256 different shades of gray. Digital color images use 24-bit for each pixel and use the RGB color model, also known as true color. Different methods can be used to hide information in images. These methods can be categorized under two headings, considering the data they use during embedding.

1. Spatial / Image Domain Technique
2. Frequency / Transform Domain Technique

In Spatial Domain or Image Domain, the pixels of the image file are directly changed for embedding secret data in it. An example of this technique is the Least Significant Bit Insertion (LSB) method, which is commonly used. In Frequency Domain or Transform Domain, the cover image is transformed in frequency domain from spatial domain and then its frequencies are used to hide the secret data. After hiding, the object is again transformed into spatial domain. An example of the Transform Domain technique is the discrete wavelet transform (DWT) implementation that uses a discrete set of the wavelet scales and translations. To evaluate the quality of the method used for information hiding, this research takes on a number of Standard parameters for the purpose of measuring the quality of images. The most common measures used to determine the quality of image are Peak Signal to Noise Ratio (PSNR) and Mean Squared Error (MSE) metrics. MSE is to estimate the mean of the squares of the error between stego image and the original image [11].

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(X_{ij} - X'_{ij})$$

PSNR is often used a s a quality measurement to determine the degradation in the embedding image with respect to the cover image, that is, the difference between the original and the stego image [11].

$$PSNR = 10log_{10}\frac{I^2}{MSE}$$

Where X_{ij} is the pixel in the original image (cover image) in i^{th} row and j^{th} column, X'_{ij} is the pixel in the stego image in i^{th} row and j^{th} column, MN is the size of the image where M is the height and N is the width and I is the range pixel value. For 8-bit images, I=255.

III. RELATED WORK

Due to its plainness and non-detectability, Least Significant Bit (LSB) steganography has been commonly used to hide information within image. Different authors used the simple LSB techniques to hide data by replacing the pixels with secret data bits. Zhou, Gong, Fu and Jin proposed a method that was built up by combining Rivest-Shamir-Adleman (RSA) cryptology and LSB steganography. Compared to the standard LSB substitution technique, this method achieved a 5.8% increase in PSNR value [12]. Akhtar, Khan and Johri introduced a method with two different LSB methods were suggested based on bit inversion. In this paper, 3 different images were used to hide 6 different messages. As a result of the experiments carried out, the PSNR

value was improved by 5.92% and 15.8% in first and second proposed method respectively [13]. A. Singh and H. Singh proposed a new LSB steganography method where 2-2-4 message bits are embedded in the R-G-B channels, respectively. In the study, applying the method on 2 different images, PSNR value was improved by 36.44% and 64.54%, respectively [14]. To hide information in grayscale and color images, Goyal, Ramaiya and Dubey proposed 1-2-4 LSB method with the RSA algorithm to encrypt the message. 4 different images were used to test the method and up to 41.48% improved PSNR value was achieved [15]. Sugathan proposed a new LSB steganography algorithm where different embedding direction of message bits was used. Implementing the method on 10 different images, a 1.32% improvement in PSNR value has been achieved compared to the classical LSB method [16]. On the other hand, Kaur and Kochhar introduced two different LSB and DCT techniques were used to perform steganography. Comparing the PSNR values with previous works the method showed a good result and the security was improved by using DCT [17].

IV. THE PROPOSED METHOD

Sometimes an image with an embedded file inside can be wide-open to many threats that pose a risk to the files to be hidden. A new method is proposed to preserve the secrecy of this information and prevent it from being exposed to any threat that may lead to its revelation. The 24-bit color images with RGB color model use 8 bits each for red, green and blue value to represent a pixel. The proposed method uses a modified LSB technique where the random position of the RGB binary representation of the color image is used to hide message bits. The overall method is shown in Figure 1.

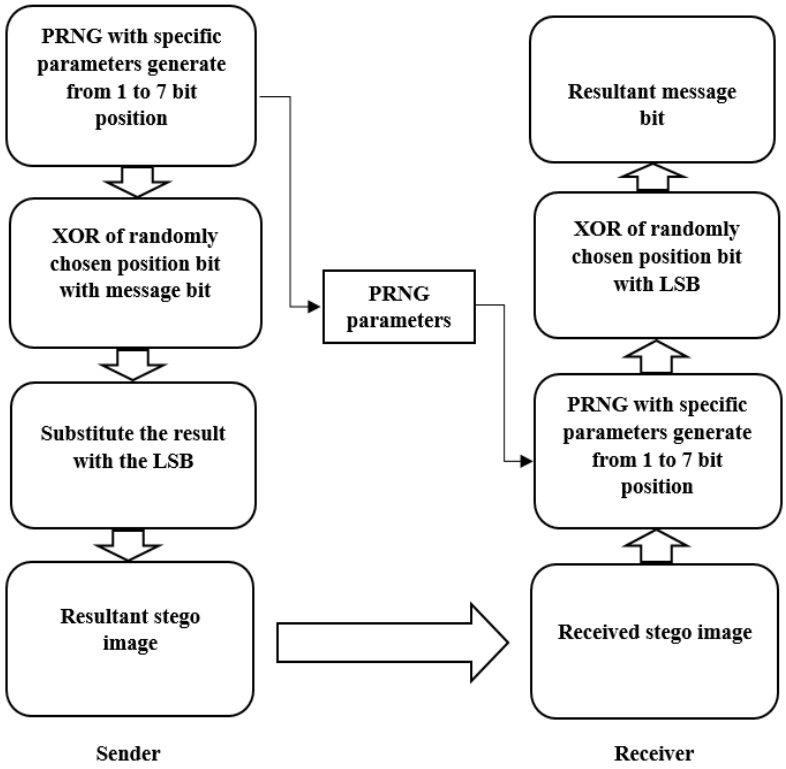

Figure 1: Proposed method

The embedding process of the proposed method is as follows:

1. Convert the message into binary form.
2. Generate random bit position from bit 1 to 7 for each R, G and B values of each pixel of the image.
3. Perform XOR operation of randomly chosen position bit with message bit.
4. Substitute the result with the LSB of the R, G or B values.

In this method, the secret message is converted into binary form to embed it in the image. A Pseudo Random Number Generator (PRNG) is used to generate random bit position from 7 most significant bits for each R, G and B values of each pixel of the image. The 1st message bit and the randomly chosen position bit of R value are used for Exclusive-OR operation and the result is substituted with the least significant bit. The process follows with the 2nd message bit and the randomly chosen position bit of G value in next and the 3rd message bit and the randomly chosen position bit of B value in next and so on. For example, if the message is

01000101 and the randomly chosen position is 5, 2, 6, 4, 5, 1, 7 and 4 then the encoding process is illustrated in Table 1.

Table 1: Embedding process

Pixel values	Binary with randomly chosen position from 1 to 7 bit	Message bits	XOR of randomly chosen position bit with message bit	Substitute the result with the LSB position
R	1100***1***001	0	1 ⊕ 0 = 1	11001001
G	0***1***111110	1	1 ⊕ 1 = 0	01111110
B	00100***1***00	0	1 ⊕ 0 = 1	00100101
R	111***1***0111	0	1 ⊕ 0 = 1	11110111
G	1001***0***100	0	0 ⊕ 0 = 0	10010100
B	***0***0011110	1	0 ⊕ 1 = 1	00011111
R	1111011***1***	0	1 ⊕ 0 = 1	11110111
G	100***1***0100	1	1 ⊕ 1 = 0	10010100

The extraction process of the proposed method is as follows:

1. Generate random bit position from bit 1 to 7 for each R, G and B values of each pixel of the image.
2. Perform XOR operation of randomly chosen position bit with LSB.
3. Collect the result as that is the message bit.
4. Retrieve the message from the result by converting.

To retrieve the message from the image, first we need to use the same Pseudo Random Number Generator to generate random bit position. Then Exclusive-OR operation is performed in randomly chosen position bit of R value and least significant bit of R value to extract the 1st message bit and the process goes on. Finally, with all the message bits, the secret message is retrieved by converting them. The process is illustrated in Table 2 to extract the message of the example considered.

Table 2: Message retrieving process

Pixel values	Binary with randomly chosen position from 1 to 7 bit	XOR of randomly chosen position bit with LSB	Message bits
R	1100***1***001	1 ⊕ 1 = 0	0
G	0***1***111110	1 ⊕ 0 = 1	1
B	00100***1***00	1 ⊕ 1 = 0	0
R	111***1***0111	1 ⊕ 1 = 0	0
G	1001***0***100	0 ⊕ 0 = 0	0
B	***0***0011110	0 ⊕ 1 = 1	1
R	1111011***1***	1 ⊕ 1 = 0	0
G	100***1***0100	1 ⊕ 0 = 1	1

V. EXPERIMENTAL RESULT

The proposed steganography method has been implemented in MATLAB (R2014a) using the mostly available three 24-bit images (Lena, pepper and baboon) with size 512×512as shown in Figure 2and the MSE, SNR and PSNR have been measured. The message to embed in the entire experiment is "HelloWorld".

Lena | Peppers | Baboon

Figure 2: Cover images used in the experiment

The results of the implemented method are illustrated in Table 3:

Table 3: The measures of MSE, SNR and PSNR

Cover Image	MSE	SNR	PSNR
Lena	0.00004196	85.0479	90.1855
Peppers	0.00002670	84.1735	90.0977
Baboon	0.02022934	56.1544	61.4840

The result shows that the proposed method have the same PSNR value as the standard LSB method, but the secret message is hidden in the random bit position of the pixel value in the proposed method whereas the message is hidden in least significant bit of the pixel value in standard LSB. Due to this random bit substitution, the attackers cannot retrieve the message although they detect the presence of the secret message in the image. In addition, to enhance the security we can add an encryption technique for the text. Hence, the proposed method provides a robust image steganography for secured communication.

VI. CONCLUSION

To communicate digitally with each other, and to share and exchange electronic documents among them, computer-based communications are main and essential in modern life. In order to secured and protected communication over Internet, the proposed method of image steganography hides the message bit in random position of the pixel bits and hides a reference like standard LSB technique. Thus, it hides the reference not the real data. The experimental measures PSNR and MSE for the proposed technique show that the method provides good performance compared with the standard LSB in regards to invisibility and robustness.

REFERENCES

[1]. Uddin,M.P., Marjan, M.A.,Sadia, N.B.,Islam, M.R.: Developing an Efficient Algorithm to Combine Cryptography and Steganography Based on ASCII Conversions and Cyclic Mathematical Function, 3rd IEEE International Conference on Informatics, Electronics & Vision, Dhaka, Bangladesh,May 23-24(2014).

[2]. Islam, M.R.,Siddiqa, A., Uddin,M.P., Mandal, A.K., Hossain, M.D.: An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography, 3rd IEEE International Conference on Informatics, Electronics & Vision, Dhaka, Bangladesh, May 23-24(2014).

[3]. Uddin,M.P.,Saha, M.,Ferdousi, S.J., Afjal, M.I., Marjan, M.A.: Developing an Efficient Solution to Information Hiding through Text Steganography along with Cryptography, 9th IEEE International Forum on Strategic Technology, CUET, Bangladesh, October 21-23, (2014).

[4]. Uddin,M.P., Afjal, M.I., Nitu, A.M., Islam, M.M., Marjan, M.A.: Development of a Symmetric-key Cryptographic Algorithm based on ASCII and Radix Conversions, Institutional Engineering and Technology (IET), 5(1):19-24, April, (2015).

[5]. Basak, P., Arjuman, L., Nitu, A.M., Afjal, M.I., Uddin,M.P., Rabbi, M.F., Islam, M.R.: A Modified Blind Steganalysis Method Based on the Moments of Characteristic Function, HBRP Advancement in Software Engineering and Testing, Volume 1 Issue 2, pp. 1-9 (2018).

[6]. Sultana, S., Khanam, A., Islam, M.R., Nitu, A.M., Uddin,M.P., Afjal, M.I., Rabbi, M.F.: A Modified Filtering Approach of LSB Image Steganography Using Stream Builder along with AES Encryption, HBRP Recent Trends in Information Technology and its Applications, Volume 1 Issue 2, pp. 1-10 (2018).

[7]. Morkel, T.,Eloff, J.H.P., Olivier,M.S.: An Overview of Image Steganography, Proceedings of the Fifth Annual Information Security South Africa Conference,Sandton, South Africa (2005).

[8]. Saha,A.,Halder, S., Kollya, S.: Image steganography using 24-bit bitmap images, 14th International Conference on Computer and Information Technology, 56-60, (2011).

[9]. Karim,S.M.M., Rahman,M.S., Hossain, M.I.: A New Approach for LSB Based Image Steganography using Secret Key, Proceedings of 14th IEEE International Conference on Computer and Information Technology, 286 – 291 (2011).

[10]. Wayner, P.: Disappearing Cryptography: Information Hiding: Steganography & Watermarking, *ELSEVIER*, 3rd Edition(2008).

[11]. Sumathi, C.P., Santanam, T., Umamaheswari, G.: A Study of Various Steganographic Techniques Used for Information Hiding", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6 (2013).

[12]. Zhou, X., Gong, W., Fu, W., Jin, L.: An Improved Method for LSB Based Color Image steganography Combined with Cryptography, ICIS 2016, Okayama, Japan, IEEE June 26-29 (2016).

[13]. Akhtar, N., Khan, S., Johri, P.: An Improved Inverted LSB Image Steganography, IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT) (2014).

[14]. Singh, A., Singh, H.: An Improved LSB based Image Steganography Technique for RGB Images, IEEEInternational Conference on Electrical, Computer and Communication Technologies (ICECCT) (2015).

[15]. Goyal, S., Ramaiya, M., Dubey, D.: Improved Detection of 1-2-4 LSB Steganography and RSA Cryptography in Color and Grayscale Images, IEEE International Conference on Computational Intelligence and Communication Networks (2015).

[16]. Sugathan, S.: An Improved LSB Embedding Technique for Image Steganography, IEEE International Conference on Applied and Theoretical Computing and Communication Technology (2016).

[17]. Kaur, G., Kochhar, A.: A steganography implementation based on LSB & DCT. International Journal for Science and Emerging Technologies with Latest Trends, 4(1), pp.35-41 (2012).

U. A. Md. Ehasn Ali (ehsan_cse@hstu.ac.bd) received his B. Sc. degree in Computer Science and Engineering from Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh in 2013. His main working interest is based on Image Processing, Expanding the Applications of Artificial Intelligence, Machine Learning, Data Mining, Data Security etc. Currently, he is working as a lecturer in Dept. of Computer Science and Engineering in Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh. He has several scientific research publications in various aspects of Computer Science and Engineering.

Md. Sohrawordi (mdsohrawordicse@gmail.com) is working as a lecturer in Dept. of Computer Science and Engineering in Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh. He received his B. Sc. degree in Computer Science and Engineering from Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh in 2013. Now, he is pursuing M. Sc. degree in Computer Science and Engineering from Rajshahi University of Engineering & Technology (RUET), Rajshahi, Bangladesh. His main working interest is based on Image Processing, Artificial Intelligence, Data Mining, Mobile Networks,cryptographyetc.He has several scientific research publications in various aspects of Computer Science and Engineering.

Md. Palash Uddin (palash_cse@hstu.ac.bd), a member of IEEE, is presently serving as an Assistant Professor in department of Computer Science and Engineering in Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh. Previously, he was a lecturer in the same university and in department of Computer Science and Engineering at Central Women's University, Dhaka, Bangladesh. He has completed his M. Sc. degree from department of Computer Science & Engineering, Rajshahi University of Engineering & Technology (RUET), Rajshahi, Bangladesh in 2018. He received his B. Sc. degree in Computer Science and Engineering from Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh in 2011. His focal research interest is based on the remote sensing image analysis, artificial intelligence based application development and machine learning algorithms for data mining. He has several national and international journal and conference publications in various fields of Computer Science and Technology. In 2017, he received the "**best paper award**" on the paper tilted as "Feature Extraction for Hyperspectral Image Classification" in the prestigious IEEE 5th Region 10 Humanitarian Technology Conference (R10HTC) hosted by Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh. In 2018, he as a co-author of the paper entitled "Weighted-Correlation based Band Reordering Heuristics for Lossless Compression of Remote Sensing Hyperspectral Sounder Data" received "**best paper award**" in IEEE International Conference on Advancement in Electrical and Electronic Engineering-(ICAEEE 2018) organized by Dhaka University of Engineering and Technology (DUET), Gazipur, Bangladesh.

U. A. Md. Ehasn Ali" A Robust and Secured Image Steganography using LSB and Random Bit Substitution " American Journal of Engineering Research (AJER), vol.8, no.02, 2019, pp.39-44