A Secure Image Steganography using LSB and Double XOR Operations

Ali Ahmed[†] **and Abdelmotalib Ahmed**[††]
aabdelrahim@kau.edu.sa alikarary@gmail.com talab_ahmed@yahoo.com
[†]Faculty of Computing and Information Technology, King Abdulaziz University-Rabigh, Rabigh 21589, Saudi Arabia
[††]Faculty of Engineering, Karary University, Omderman 12304, Sudan

Summary
Least Significant Bit (LSB) is a common and popular technique for steganographic images, especially when the spatial domain of an image is considered. Because of its high quality of stego-image produced, this method is currently widely used and continues to be developed to date. The limitations of the LSB method are its simplicity and high predictability of inside secrets, so researchers try to improve the security of hidden messages in this way. This study proposes two layers of encryption and hiding stages. Here, first the message is encrypted by using a Secret key (extract from MSB) and double XOR operations using binary representation, and then an encrypted stream of bits is hidden into the cover image using the LSB technique. To ensure the quality of our proposed method, a well-known evaluation measure, such as MSE, PSNR, Entropy and histogram distribution, was calculated. Our experimental results show that our proposed method has acceptable results and it preserves the security of hidden text messages. Our best results achieved for PSNR and MSE are 55.67 dB and 0.18 respectively.

Key words:
Steganography, Cryptography, Least significant bit method, Hybrid security method, PSNR, MSE

1. Introduction

Information and communication technology has evolved rapidly and exponentially due to the growth of the internet, but both sender and receiver parts face the crucial problem of data security during the exchange of messages, such as data transmission, copyright control and regulation, etc. [1]. Two main techniques were used to safeguard data security over unsecure channels of communication: steganography and cryptography. Cryptography actually scrambles the plain text of secret or private messages to make them unreadable by an unauthorized user. However, steganography deals with hiding secret text data or other media on other media. The latter is named cover media. In fact, it masks the presence of a hidden message to avoid spoofing results. It was derived from the Greek words “steganos” and “graptos”, which mean covered and writing, respectively [2]. Cover media can be one of the four types of multimedia, but the most frequently used covers are image, audio [3, 4] and video [5, 6]. When images are used as cover media there will be two options for using either its spatial domain [7, 8], or its frequency domain [9, 10]. The spatial domain approaches are straightforward as well as simple to build. The least significant bit is one of the leading and well-known strategies in spatial domain image steganography [11]. Steganographic and cryptographic techniques are both efficient, reliable, and robust; numerous ways have been developed and identified to combine steganographic and cryptographic techniques to achieve a hybrid system [12]. The combination of several steganographic techniques with various cryptography algorithms, such as Advance Encryption Standard AES algorithm, random key generation, alteration components and key-based security algorithms, have been reviewed [13, 14]. In this study a combination method of cryptography and steganography is proposed, and the encryption process proposed here is very simple and considered as being very efficient since it is achieved by performing a double XOR operation on a stream of message text stream of bits with stream of MSB bits that represent the random key. The main contributions of our proposed scheme are summarized as:

(i) Strongest symmetric algorithm based on double XOR operation with automatic random key extracted from MSB of cover image pixel values.

(ii) Improvement and enhancement of the traditional LSB steganography method since the content of hidden secret text is encrypted.

(iii) Improvement and enhancement of capacity of the amount of hidden secret text messages since our proposed method could apply on different sizes of grey images.

The rest of the parts of this paper are arranged as follows: Section 2 presents the related works; Section 3 describes the fundamentals behind the proposed combination schemes. In Section 4, simulation results and discussions are demonstrated. Finally, Section 5 provides the conclusion of the paper.

2. Related Works

Steganography and cryptography have been reported to be individually insufficient for complete or effective information security; therefore, a more reliable and strong mechanism can be achieved by combining both techniques, in this section various studies for improving and enhancing

Manuscript received May 5, 2020
Manuscript revised May 20, 2020

Secret messages and hidden into cover image files will be discussed.

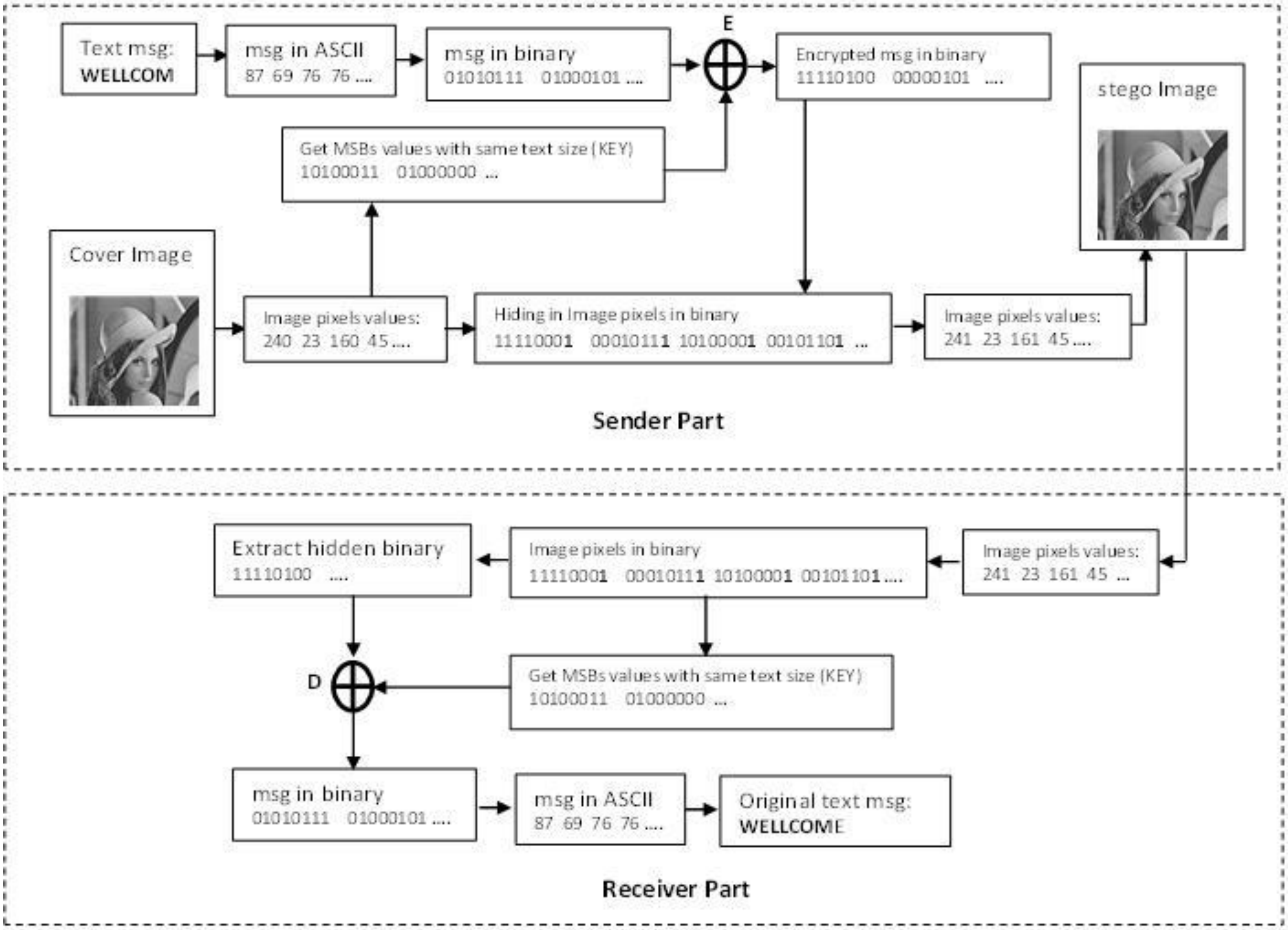

Fig. 1 Workflow of Proposed Security Method for Hiding Encrypted Text Messages

A combination of Cat Map (ACM) with RSA and subsequently embedding the encrypted result in a cover image using two-bit LSB steganography method was successfully implemented and achieved better results [15]. Sofyane et al. [16] improved image steganography by first reducing the length of the message, then by using AES algorithm. De Rosal et al. [17] used divide and modulus function and improve message security since the messages are split into two parts and sent separately. A simple XOR binary based process used by Arindam et al. [18] is implemented. In their study, some modification of LSB algorithms was done by adding a sequence algorithm for pixel selection. Yani et al. [19] proposed a three-time XOR operation on text messages and used three bits of MSB as a key in the encryption process. In this study, a simple and effective way of a double XOR operation with a truly random key is performed before embedding text using the LSB technique, and a random key was extracted from all MSB bits with the same length of text message in binary representation.

3. Proposed Method

A combination of steganography and cryptography strategies can ensure better secrecy of information and will meet the security and robustness requirements for the transmission of important information. Figure 1 presents our proposed method for the combination of both techniques. A one-time pad (OTP) symmetric encryption algorithm with double XOR operation is used; this algorithm is noted to be very fast and unbreakable since it performs a single operation on a stream of bits of both plain text and random key. There are further good and powerful features of this method in the concept of key generation, and neither a need for generation of a key nor sending it to the receiver part. A key used by both the sender and receiver part will extract automatically from most significant bits (MSB) of image pixels of cover and stego-image; the only information we need to send is length of user plain text message. For this purpose we proposed to preserve a few first bytes (always first 32 bytes) of the cover image to send the length of user text message in binary and it will locate on the second LSBs to avoid the overlapping of secret text messages, the following algorithm shows steps in both sender and receiver parts:

Encryption and Hiding Algorithm:
Input: a cover image C and a message m
Output: a stego-image S

```
Start
Key1 ← Extract string of bits from MSBs of C as same length of m
m-in-bits=convert message m to string of bits
EMtemp = m-in-bits XOR Key1
Key2 = flip (Key1)// turns over all bits
EM = EMtemp XOR Key2 // EM is encrypted user message
for i = 1 to length (m) do
    Si ← LSB1(Ci) = EMi      // hiding encrypted message in first LSB
end for
Lkey=dec2bin(length (m))
for i = 1 to length Lkey (in bits)
    Si ← LSB2(Ci) = Lkey // hiding length of message in second LSB
end for
end
```

Extraction and Decryption Algorithm:
Input: a stego-image S
Output: a message m

Fig. 2 Pseudocode of Hiding and Encryption

```
Start
for i = 1 to first 32 bytes of S do //always length of m is first 32 bytes
    Lkey ← Extract string of bits for message length from LSB2(Si)
end for
length (m)=bin2dec(Lkey)
for i = 1 to length (m) do
    key1 ← Extract string of bits from MSBs of S
end for
for i = 1 to length (m) do
    EM ← Extract string of bits from LSB1(Si)
end for
EMtemp = EM m-in-bits XOR Key1
Key2 = flip (Key1)
m-in-bits = EMtemp XOR Key2 // user message m
End
```

Fig. 3 Pseudocode of Extraction and Decryption

4. Experimental Results and Discussion

In order to evaluate our proposed method, three different experiments were conducted. For each of the experiments the same cover image was used with different text message sizes. Three different text messages were used as a plain text and they were converted into cipher text using double XOR operations, as explained in the algorithms shown in Figure 2. For each cover file a certain capacity is permitted according to the size of the cover image, Table 1 below shows the three cover images used, along with their capacity or allowable text size. Extraction and decryption were performed on a receiver according to the algorithms shown in Figure 3.

Table 1: Cover image samples and total text capacity

Image Name	Image sample	size	Total pixels	Maximum capacity
Lena		255 × 255	65025	8128 bytes
Barbara		512 × 512	262144	32768 bytes
Man		1024 ×1024	1048576	131072 byte

For performance and evaluation measures two common well-known metrics were used with mean square error MSE and peak signal to noise ratio PSNR. MSE is the expected value of the squared error loss or quadratic loss, MSE is between two images A(x,y) and B(x,y), where A and B are stego-images and cover images respectively, as given by the following equation:

$$MSE = \sum_{i=1}^{x}\sum_{j=1}^{y}\frac{(|A_{ij} - B_{ij}|)^2}{x * y} \qquad (1)$$

Where, x and y are width and height of image

PSNR is a well-known performance measure for image distortion, which is always applied to stego-image and computed as the following equation:

$$PSNR = 10log_{10}\frac{C^2_{max}}{MSE} \qquad (2)$$

Where C^2_{max} is the maximum value in the image such as:

$$C^2_{max} \le \begin{cases} 1 \text{ in double precision intensity images} \\ 255 - 8 \text{ bit unsigned integer intensity images} \end{cases}$$

These two metrics were early found by Ahmet et al. [20] and they were widely used in this area of image steganography as well as image compression. The experiments are validated on MatLab2019b with 64-bit Microsoft Windows 10 OS, platform Intel core i5 with 1.65 processor and 8 GB random access memory. Our results of PSNR and MSE for hiding three different text messages sizes with each of the different three cover images were illustrated in Table 2 and Figure 4.

Table 2: PSNR and MSE of Proposed Method for different text size

Cover image	200 Byte Message Size		500 Byte Message Size		1000 Byte Message Size	
	PSNR	MSE	PSNR	MSE	PSNR	MSE
1	40.74	5.52	36.90	13.38	33.95	26.36
2	49.23	0.78	45.23	1.96	41.99	4.14
3	55.67	0.18	51.95	0.42	48.86	0.85

Additionally, both cover and stego-images with their histogram distribution for Barbara and Man images are presented in Figure 5, 6, 7 and Figure 8, respectively. Inspection and reading from Table 2 and Figure 4 give good results for both MSE and PSNR values. Most values of PSNR are greater than 40 dB, which is considered as being an acceptable performance, as reported by Nolkha et al. [1]. In addition, Figures 5 and 7 show that our proposed method has good visual results for both stego-images and histograms.

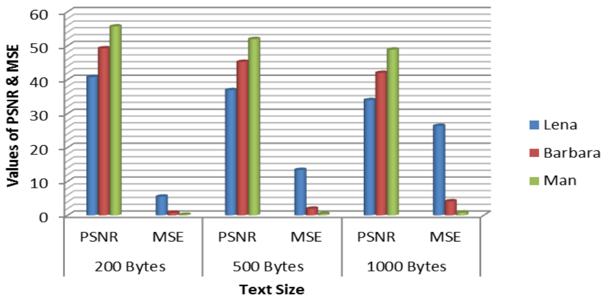

Fig. 4 PSNR and MSE of Proposed Method for different text size

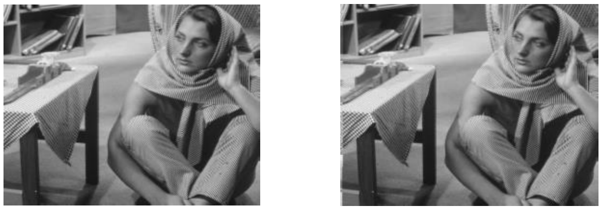

Fig. 5 a) Barbara cover image b) Barbara stego-image

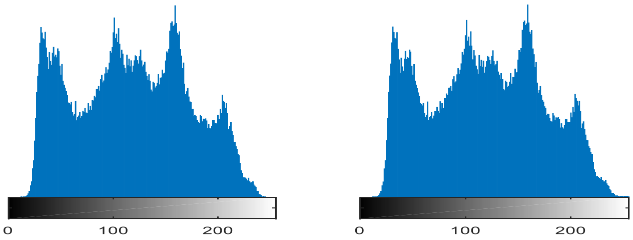

Fig. 6 a) Histogram for Fig 5 a b) Histogram for Fig 5 b

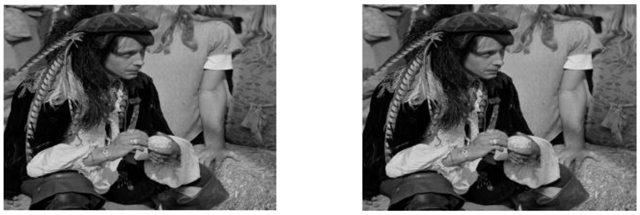

Fig. 7 a) Man cover image b) Man stego-image

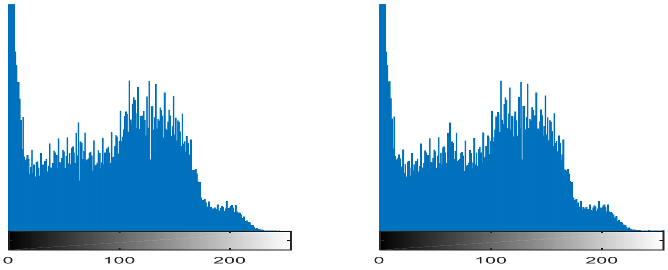

Fig. 8 a) Histogram for Fig 7 a b) Histogram for Fig 7 b

Another measure, known as the Entropy (Average content of the information) parameter is also used for the analysis of cover image and stego-image. This test measures the proportions of the details and it is usually represented as bits in units. The equation for the entropy calculation is shown below:

$$E(P) = \sum_{i=0}^{G-1} P(i) \log P(i) \qquad (3)$$

where, P(i) is probability density function of a given image at intensity level, l and G is total number of grey levels in the image, highest value of entropy means good quality and informative about an image.

Table 3: Entropy for cover images and stego-images

Image	Entropy of cover image	Entropy of stego-image
Lena	6.4498	6.5710
Barbara	7.6321	7.6413
Man	7.5237	7.5299

The obtained entropy results in Table 3 of images shows that the entropy of stego-image is slightly greater than the cover image with less than 0.01, and this is because the more hidden information is added to the cover image without a significant change in pixels values. Finally, the low performance results of the first image (Lena) in terms of MSE and PSNR are due to bad histogram distribution of the image itself even before the hiding process was performed, as shown in Figure 9 below.

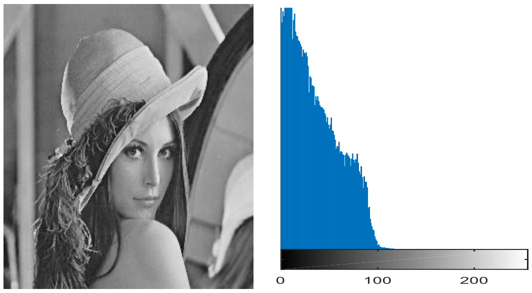

Fig. 9 a) Lena cover image b) Lena Histogram distribution

5. Conclusion

In this paper, an improvement model for securing and hiding text messages into grey scale images was developed; two-stage processes for encrypted text messages using double XOR binary based operation were performed. Hiding encrypted text was made on LSB of each image pixel byte. Our proposed method has been evaluated using the well-known evaluation measures of MSE, PSNR and entropy and it shows acceptable results of all metrics. Other type of colour image could be used in future to increase the text capacity.

Acknowledgment

This research was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, Saudi Arabia. The authors, therefore, gratefully acknowledge the DSR for their technical and financial support.

References

[1] Nolkha, A., S. Kumar, and V. Dhaka, Image Steganography Using LSB Substitution: A Comparative Analysis on Different Color Models, in Smart Systems and IoT: Innovations in Computing. 2020, Springer. p. 711-718.

[2] Morkel, T., J.H. Eloff, and M.S. Olivier. An overview of image steganography. in ISSA. 2005.

[3] Atoum, M. S., S. Ibrahim, G. Sulong and M. Ali. MP3 steganography. International Journal of Computer Science Issues (IJCSI), 2012. 9(6): p. 236.

[4] Atoum, M., S. Ibrahim, G. Sulong and A. Ahmed. New Secure Scheme in Audio Steganography (SSAS). Australian Journal of Basic and Applied Sciences, 2013. 7(6): p. 250-256.

[5] Ratna, S. R., J. S. Loret, D. M. Gethsy, P. P. Krishnan and P. A. Prabu. A Review on Various Approaches in Video Steganography. in Intelligent Communication Technologies and Virtual Mobile Networks. 2019. Springer.

[6] Gupta, H. and S. Chaturvedi, Video steganography through LSB based hybrid approach. International Journal of Computer Science and Network Security (IJCSNS), 2014. 14(3): p. 99.

[7] Abdulwahedand, M.N., S. Mustafa, and M.S.M. Rahim. Image Spatial Domain Steganography: A study of Performance Evaluation Parameters. in 2019 IEEE 9th International Conference on System Engineering and Technology (ICSET). 2019. IEEE.

[8] Nisha, C. and T. Monoth, Analysis of Spatial Domain Image Steganography Based on Pixel-Value Differencing Method, in Soft Computing for Problem Solving. 2020, Springer. p. 385-397.

[9] Chatterjee, A. and N. Barik, A New Data Hiding Scheme Using Laplace Transformation in Frequency Domain Steganography. International Journal of Hyperconnectivity and the Internet of Things (IJHIoT), 2020. 4(1): p. 1-12.

[10] Bikku, T. and R. Paturi, Frequency Domain Steganography with Reversible Texture Combination. Traitement du Signal, 2019. 36(1): p. 109-117.

[11] Islam, M. R., A. Siddiqa, M. P. Uddin, A. K. Mandal and M. D. Hossain. An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography. in 2014 International Conference on Informatics, Electronics & Vision (ICIEV). 2014. IEEE.

[12] Taha, M. S., M. S. M. Rahim, S. A. Lafta, M. M. Hashim and H. M. Alzuabidi. Combination of Steganography and Cryptography: A short Survey. in IOP Conference Series: Materials Science and Engineering. 2019. IOP Publishing.

[13] Sharma, H., K.K. Sharma, and S. Chauhan, Steganography Techniques Using Cryptography-A Review Paper. 2014.

[14] Aung, P.P. and T.M. Naing, A novel secure combination technique of steganography and cryptography. International Journal of Information Technology, Modeling and Computing (IJITMC), 2014. 2(1): p. 55-62.

[15] Kusuma, E.J., C.A. Sari, and E.H. Rachmawanto, A Combination of Inverted LSB, RSA, and Arnold Transformation to get Secure and Imperceptible Image Steganography. Journal of ICT Research and Applications, 2018. 12(2): p. 103-122.

[16] Chikouche, S.L. and N. Chikouche. An improved approach for lsb-based image steganography using AES algorithm. in 2017 5th International Conference on Electrical Engineering-Boumerdes (ICEE-B). 2017. IEEE.

[17] Santoso, H.A., E.H. Rachmawanto, and C.A. Sari. An improved message capacity and security using divide and modulus function in spatial domain steganography. in 2018 International Conference on Information and Communications Technology (ICOIACT). 2018. IEEE.

[18] Roy, A., J. Bhattacharya, S. Kundu, S. Sahana and D. Singh. Block Steganography Based Secure Key Encryption to Improve Data Security. in International Conference on Innovation in Modern Science and Technology. 2019. Springer.

[19] Astuti, Y.P., E.H. Rachmawanto, and C.A. Sari. Simple and secure image steganography using LSB and triple XOR operation on MSB. in 2018 International Conference on Information and Communications Technology (ICOIACT). 2018. IEEE.

[20] Eskicioglu, A.M. and P.S. Fisher, Image quality measures and their performance. IEEE Transactions on communications, 1995. 43(12): p. 2959-2965.

Ali Ahmed received his B.Sc. from Karary University (Sudan) in computer engineering and his M.Sc. degree in computer science, from Khartoum University (Sudan). He received his PhD and post-doctoral in computer science from UTM University (Malaysia). He worked as an assistant professor in Sudan (2014-2018). Now he is an associate professor in the Faculty of Computing and Information Technology at King Abdulaziz University in KSA. His research interests include machine learning, data mining, information retrieval, image processing and medical image retrieval. He is a member of IEEE, ACM and SEA Sudan.

Abdelmotalib Ahmed received his B.Sc. from Karary University (Sudan) in computer engineering and his M.Sc. degree in computer engineering, from Khartoum University (Sudan). He received his PhD in computer architecture from Harbin institute of technology (Harbin -China). [illegible] t professor in the Faculty of Engineering, Karary University, Sudan. His research interests include image processing, parallel architectures and information security.