Secure Message Hiding System in Image using Modified Least Significant Bit Method

Aye Myat Thu, Tin Zar Nwe

Abstract— **Information Security is a major concern in today's modern area. Two methods are used for information security: Cryptography and Steganography. Cryptography is the science of using mathematics to encrypt and decrypt data. Steganography is the practice of concealing a file, message, image or video within another file, message, image or video. For effective security, steganography is combined with cryptography. Proposed system combines Rivest–Shamir–Adleman (RSA) cryptographic algorithm and stego color cycle least significant bit (SCC-LSB) steganographic algorithm to provide higher security. The paper provides modified SCC-LSB can hide using two steps, firstly: hiding first three bits using one-bit SCC-LSB and secondly: hiding remaining bits using two bits SCC-LSB. The system is implemented by using C # programming language.**

Index Terms— Steganography, cryptography, RSA, first LSB, second LSB, modified LSB.

1) INTRODUCTION

The internet has undoubtly become a huge part of our lives. Most communication channels are widely based on Internet. The security of information becomes essential to transmit data on the internet. Several properties concerning with information security: confidentiality, integrity, authenticity, secrecy and privacy. The two methods for these properties are Cryptography and Steganography.

Cryptography uses data encryption and decryption techniques to secure data. It is a well-established field, often thought of as an art strengthened with contributions of the skillful mathematicians. Cryptography concentrates on designing methods to map the original data to some random-looking data (encryption) and at the receiver side recovering the meaningful data (decryption). Encryption and decryption methods often make use of a key. At the encryption side this key is secret; at the decryption side, it may or may not be secret, forming the class of public-key and private-key cryptography system. The goal is that unauthorized parties should not be able to decrypt the message. Unfortunately, it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret.

Information hiding, on the other hand, steganography refers to a different class of problems where secure data transmission is carried out by hiding a message in cover data (also termed as host data). To send information embedded in cover file, steganography is an essential tool in order to prevent from the eavesdropper because it is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words stegos meaning cover and graphia meaning writing defining it as covered writing. In the Second World War, the Microdot technique was developed by the Germans. Today, steganography is mostly used on computers with digital data being the carriers and networks being the high-speed delivery channels.

The proposed system uses asymmetric algorithm for enhancing security. It provides not only security but also less embedding capacity. However modified LSB will give to enhance embedding capacity than original LSB.

The paper is organized as follows: Section 1 describes the introduction to the information security. Section 2 describes related works in steganographic and information hiding techniques that are pointed out from some papers. Section 3 describes the overview of cryptography and steganography. Section 4 describes proposed system design. Section 5 present implementation of proposed system. Test and results in Section 6. Finally, the conclusion for the paper is expressed in section 7.

2) RELATED WORKS

In today's communication, the security issues always been the top priority. Cryptography is the most common necessary elements for secure communication based on authentication, data confidentiality, data integrity and non-repudiation [1].

In Bharti and Soni, a novel data-hiding technique based on the LSB technique of digital images is presented. Data hiding is one of best topic in secret communication. A lossless data hiding technique using LSB in images is presented in this paper. LSB data hiding technique does not affect the visible properties of the image. The modern secure image steganography presents a challenging task of transferring the embedded information to the destination without being detected. This paper deals with hiding text in an image file using Least Significant Bit (LSB) technique. The LSB algorithm is implemented in spatial domain in which the payload bits are embedded into the least significant bits of cover image to derive the stego-image [2].

Then, Ramaiya, M.K., Hemrajani, N. and Saxena, A.K presented a unique technique for Image steganography based on the Data Encryption Standard (DES) using the strength of S-Box mapping & Secret key. Carried out the preprocessing of secret image by embedding function of the steganography

Manuscript received September, 2018.

Aye Myat Thu, *is with the Department of Information Technology in Pyay Technological University, Pyay, Myanmar (corresponding author to provide phone: 09975411402).*

Tin Zar New*, is with the Department of Information Technology in Pyay Technological University, Pyay, Myanmar (corresponding author to provide phone: 099737786382).*

algorithm using two unique S-boxes. Also proposed the scheme, capable of not just scrambling data but it also changes the intensity of the pixels which contributes to the safety of the encryption [3].

After that, Zhiwei *et al.* discussed image steganography combined with preprocessing of DES encryption. When transmitting the secret information, firstly, encrypt the information intended to hide by DES encryption was encrypted, and then was written in the image through the LSB steganography. Improved the Encryption algorithm lowest matching performance between the image and the secret information by changing the statistical characteristics of the secret information to enhance the anti-detection of the image steganography. Experimental results showed that the anti-detection robustness of image steganography combined with preprocessing of DES encryption was found much better than the way using LSB steganography algorithms directly [4].

Moreover, Gunda Sai Charan *et al.* presented a novel LSB based image steganography with multi-level encryption. In this investigation, a novel approach of encrypting the plain text into cipher text and embedding it into a color image is proposed. Encryption is done in two stages, during first stage it is encrypted by Ceaser cipher technique and in the second stage it is encrypted based on chaos theory. The cipher text obtained after encryption is embedded using 3, 3, 2 LSB replacement algorithm [5].

In paper, author combine the cryptography and information hiding. On the one hand, by using information hiding does not change the visual characteristic of cover image, we can embed secret information in another public image and transfer. On the other hand, by using digital signature and encryption technology of cryptography, we can make the unauthorized users can not know the location of the embedded secret information, so that the secret information cannot be extracted. The effective combination of the above two means further improves the security of information hiding [6].

3) Overview of Cryptography and Steganography

Cryptography is the art and science of achieving security by encoding messages to make them non-readable. In this, the structure of message is scrambled to make it meaningless and unintelligible unless the decryption key is available. Basically, cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it. Cryptography can also provide authentication for verifying the identity of something or someone. Cryptanalysis is the reverse engineering of cryptography.

i)RSA Algorithm

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. RSA stands for Ron **Rivest**, Adi **Shamir,** and Leonard **Adleman**, who first publicly described it in 1978. RSA algorithm is an asymmetric cryptographic system that utilizes two set of keys to encrypt and decrypt messages to ensure the security of quality information. In its performance, the keys are generated through a process of complex mathematical computation. The two keys generated are called public key and private key. The public key is distributed to the sender of a message to encrypt the message whiles the receiver of a message keeps the private key secretly to decrypt the public key encrypted message [8].

The steps below are the processes in generating public and private keys using RSA

1. Pick two large prime numbers p and q, p! =q;
2. Calculate n = p*q;
3. Calculate ϕ (n) = (p-1) (q-1);
4. Pick e, so that gcd (e, ϕ (n)) = 1,1<e< ϕ (n);
5. Calculate d, so that d*e mod ϕ (n) = 1, i.e. d is the Multiplicative inverse of e in mod ϕ (n);
6. Get public key as Ku= {e, n};
7. Get private key as Kr= {d, n};

Figure 1: RSA Algorithm

The public key is (n, e) and the private key is d. Encryption and decryption is of the following form, for some plaintext block M and cipher text block C.

For encryption,

$C = M^e \bmod n$

For decryption,

$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. The public key consists of n, the modulus, and e, the public exponent. The private key consists of n, the modulus, which is public and appears in the public key, and d, the private exponent, which must be kept secret. The key generation, encryption and decryption processes of RSA algorithm is illustrated with example.

The keys were generated as follow,

1. Select two prime numbers, p=17 and q=11.
2. Calculate n = p*q = 17 * 11 = 187.
3. Compute ϕ (n) = (p-1) (q-1) = 16 * 10 = 160.
4. Select e such that e is relatively prime to ϕ (n) = 160 and less than ϕ (n); so, choose e = 7.
5. Determine d such that e*d = 1 mod 160 and d < 160. The correct value is d = 23, because 23 * 7 = 161 = 10 * 160 + 1.

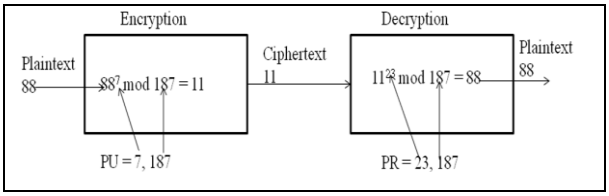

Figure 2: Example of RSA Algorithm

The resulting keys are public key PU = {7,187} and private key PR = {23,187}. The example shows the use of these keys for a plaintext input of M = 88.

For encryption process, calculate

$C = 88^7 \bmod 187 = 11$

For decryption process, he or she calculates:

$M = 11^{23} \bmod 187 = 88$

Steganography is the art of hiding information and an effort to conceal the existence of the embedded information. Most of steganography works have been carried out on image, video, audio and text.

ii)LSB Techniques

According to Katzenbeisser and Petitcolas [9], using least significant substitution for image steganography is able to optimize the capacity of the payload and not results in a perceptible amount of degradation to the human visual senses [7]. Since LSB appears at the lowest order bit in a binary value, therefore the altered bits can only be discovered with hex editor.

Images is the most wide-spread media in use [7] and when digital images are being utilized as cover in steganography, the cover-image is generally manipulated by changing one or more bits of a single or multiple byte in image pixels. The secret data can be stored in the LSB of one (e.g., blue colour) out of the three RGB colour bytes or in the parity of the entire RGB. Various bits for LSB-based steganography have currently been implemented in the existing tool.

a) Stego One Bit LSB

Stego one-bit LSB approach changes only notice the bit of the colour byte. Therefore, changing the LSB will only change the integer value of the byte by one. By manipulating the LSB of one of the RGB colour, the effect on the appearance of the image is indiscernible [7]. Fig 3 shows an example of using stego one bit in the blue colour byte.

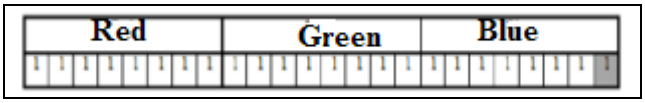

Figure 3. Example of stego one-bit LSB

b) Stego Two Bits LSB

Stego two bits LSB is an approach that manipulates two LSB of one of the colours in the RGB value of the pixels to store bits of secret data in the cover Please refer to Fig 4. The advantage of stego two bits is the amount of information embedded is twice that of stego one-bit LSB approach. Unlike stego bit, the degradation of stego-image quality using stego two bits LSB is slightly distinct [7].

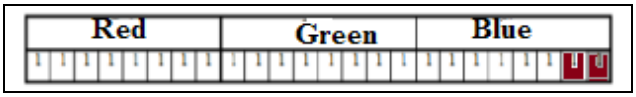

Figure 4. Example of stego two-bit LSBs

c)Stego Three Bits LSB

Fig 5 depicts the approach of using three LSBs one of the colours in the RGB value to hide secret data in the cover-image. The obvious advantage of using more LSBs is increased storage space for secret data. Stego three bits is capable of storing up to three times more secret data than stego one-bit LSB Unfortunately, the stego-image quality suffers more detectable degradation in this approach than stego two bits [7].

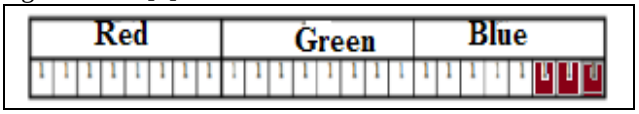

Figure 5. Example of stego three bits LSB

d)Stego Colour Cycle (SCC)

Using SCC, bits of secret data is embedded in rotating RGB colour values. Bailey and by using SCC, the presence of hidden data is more challenging to detect and need not subject a single colour to constant change. For instance, the first data bit could be hidden in the LSB of the blue colour byte, the LSB of the red colour by bit and subsequently the third data bit is embedded in the green value [7]. An example of SCC approach is shown in Fig 6.

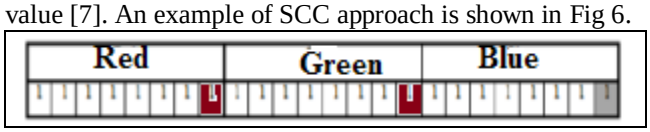

Figure 6. Example of SCC

4) PROPOSED SYSTEM DESIGN

The proposed system uses two methods. First is encrypting message that the user wants to hide using RSA algorithm for high security. Second is hiding encrypted message in a cover image. The block diagram of the whole system is shown in Fig 7 Selecting of cover images depends on the size of message.

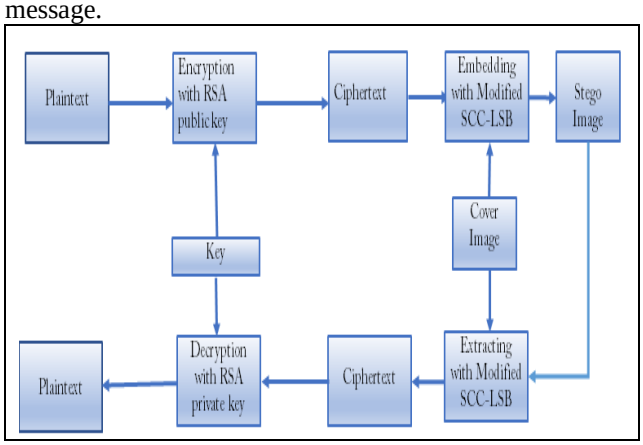

Figure 7. Block Diagram of Whole System

In hiding, the proposed system is enhanced combining popular one-bit SCC-LSB and two-bit SCC-LSB. When the user uses one-bit SCC-LSB, it only hides three binary bits in one pixel. Therefore, it can be said that it has less embedding capacity. Therefore, the proposed system uses two-bits SCC LSB. However, it will cause high mean square error. According to these facts, the proposed system firstly uses one-bit SCC-LSB. Only when length of binary form of message is greater than the embedding capacity of it, two-bit SCC-LSB is used to hide remaining message.

The main idea of proposed system is to reduce mean square error in two-bits LSB. To hide, two-bits LSB uses two least significant bits in each red, green, blue part in one pixel. Therefore, it has 6-bit changes in one pixel. It causes high mean square error. One-bit LSB has 3-bits changes in one pixel. Therefore, it has less mean square error. The proposed system firstly uses one-bit LSB by only hiding one least significant bit. However, when secret message size is larger than embedding capacity of one-bit LSB, proposed system will use second least significant bit to hide.

Step for proposed system is as below.

1. Input message to hide.
2. Firstly, encrypt using RSA algorithm.
3. Get ciphertext and convert to binary string.
4. Start index=0;
5. If index of binary string is less than length of the string, hide every character with this index using one-bit

SCC-LSB. And then remaining characters is hidden using two-bit SCC-LSB.

An example of two-bit SCC-LSB is shown in Fig 7.

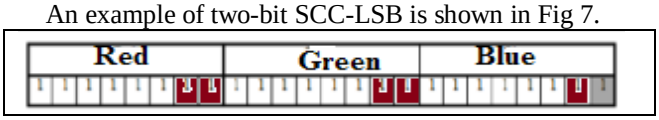

Figure 8. Example of two-bit SCC

Example of Modified SSC-LSB is as shown in Fig 8. To hide 1110 in one pixel, one-bit LSB cannot hide because the length of binary message is greater than embedding capacity of pixel. However modified SSC-LSB can hide using two steps, firstly hiding first three bits using one-bit SCC-LSB and secondly hiding remaining bits using two-bit SCC-LSB.

5) Implementation Of Proposed System

Firstly, plaintext message using RSA algorithm is encrypted as shown in Fig 9.

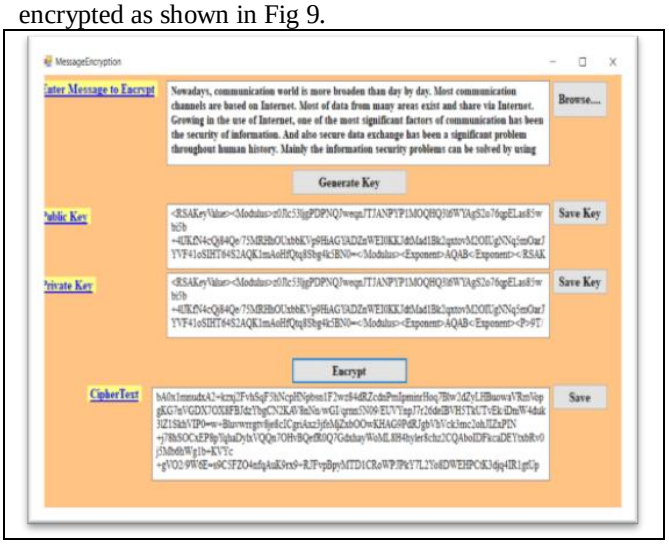

Figure 9. Encryption Process

Secondly encrypted message is hidden in cover image using Modified SCC-LSB shown in Fig 10.

Figure 11. Embedding Process

As shown in Fig 12, ciphertext is extracted from stego cover image.

Figure 12. Extracting Process

Finally, after decryption process in Fig 13, original message can be gotten.

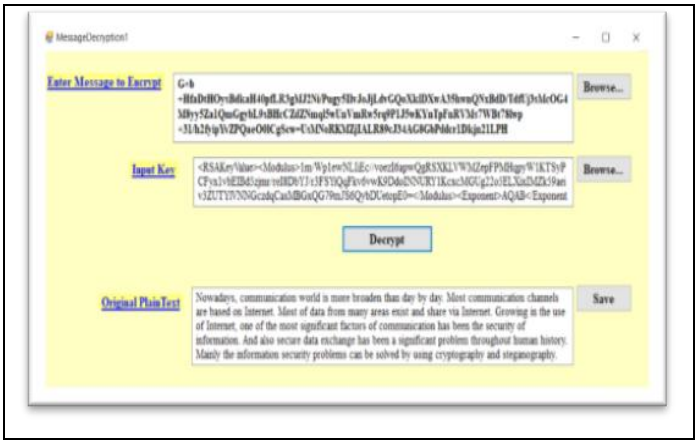

Figure 13. Decrypting Process

6) Tests And Results

i)Mean Square Error (MSE)

MSE in the recreated one is mean of the squared difference between original and recreated one. Suppose a 1x4 original array say [2 3 14 9] and a recreated array [2 4 16 8].

MSE = MEAN [(2-2) ^2 (4-3) ^2 (16-14) ^2 (8-9) ^2]

MSE = MEAN [0 1 4 1] = 6/4 = 1.5

Less mean square error it is, better the quality of image it has. Two-bit SCC-LSB and modified SCC-LSB gives different MSE value as shown in below.

When sample RGB value of one pixel is (00001110, 00011001, 01010111) and binary message is 0111. Two-bit LSB will hide as (00001**01,** 00011**01**, 01010111), ie. Bold letters are hiding message. MSE of two-bit SSC-LSB is ((1+4+0)/3=5/3).

Modified SSC-LSB will hide firstly three bits (011) in 0111 binary messages as (0000111**0,** 0001100**1**, and 0101011**1**) and then secondly remaining bit 1 is hidden second LSB bits of pixels as (0000111**0,** 0001100**1** and 0101011**1**). Therefore, MSE of modified SCC-LSB is ((2+1+1)/3=4/3).

It can easily be seen that modified SCC-LSB gives less MSE than original SCC-LSB.

ii) Embedding Capacity of modified SCC-LSB

Embedding capacity of original SCC-LSB is three by eight times of number of pixels in cover image. That of two-bit SCC-LSB is six by eight times of number of pixels in cover image. Modified SCC-LSB gives same embedding capacity. The result is shown table 1.

Table 1. Modified SCC-LSB

	Original LSB	Stego LSB	MSE	Embedding Capacity
Stego image for first LSB	3482*2321px	3482*2321px	444.69070659281110(exp-5)	3030KB
Stego image for second LSB	3482*2321px	3482*2321px	1037.03146433396*10(exp-5)	3030KB
Stego image for modified LSB	3482*2321px	3482*2321px	444.690706592811*10(exp-5)	3030KB

7) CONCLUSION

In the proposed system, the secure message hiding technique is enhanced by the modified methods are combining one-bit SCC-LSB and two-bit SCC-LSB.The proposed system gives higher security using RSA algorithm. It can give higher embedding capacity and less MSE. Further extension of proposed system is to test with Peak Signal to Noise Ratio (PSNR) and to add three bit and four-bit SSC-LSB.

ACKNOWLEDGMENT

First of all, the author really thanks to Chairmen and Co-chairmen of Organization Committee for International Journal of Science, Engineering and Technology Research (IJSETR). She also likes to express her supervisor, her Head of Department, and all of her teacher from Department of Information Technology, Pyay Technological University. She has provided not only helpful guidance but also a lot of inspiration, motivation and encouragement during my research work.

Finally, she is grateful to my parents and my family who specifically offered strong moral and physical support, care and kindness, during the year of my M.E study and anybody for overall supporting during my thesis.

REFERENCES

1) S. Inshi and A. Youssef, "Design and Implementation of an Online Feedback System," in communications, 2008 24th Bi-ennial Symposium on, 2008, pp.58-61
2) Bharti and Soni, "A New Approach of Data Hiding in Images using Cryptography and Steganography," Int. J. Compute. Appl., vol. 58, no. 18, pp. 1–4, 2012.
3) Ramaiya, M.K., Hemrajani, N. and Saxena, A.K.; "Security Improvisation in Image Steganography using DES", 3rd International Advance Computing Conference (IACC), pp.1094-1099, 2013.
4) Zhiwei, Z., Ren-er, Y., Shun, T. and Shilei, C.; "Image Steganography Combined with DES Encryption Pre-processing", Sixth International Conference on Measuring Technology and Mechatronics Automation, IEEE, 2014.
5) Charan, Gunda Sai, S. S. V. Nithin Kumar, B. Karthikeyan, V. Vaithiyanathan, and K. Divya Lakshmi, "A novel LSB based image steganography with multi-level encryption," International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015, pp. 1-5, IEEE, 201 5.
6) Xinyi Zhou, Wei Gong, WenLong Fu, LianJing Jin, "An Improved Method for LSB Based Color Image Steganography Combined with Cryptography", 2016 IEEE ICIS 2016, June 26-29, 2016, Okayama, Japan.
7) Lip Yee Por, Delina Beh, Tan Fong Ang, and Sim zing Ong, "An Enhanced Mechanism for Image steganography Using Sequential Colour Cycle Algorithm", The International Arab Journal of Information Technology, Vol. 10, No. 1, January 2013.
8) R.L. Rivest, A. Shamir, L. Adleman: "A method for obtaining digital signatures and Public-Key Cryptosystems", Communications of the ACM 21 (1978), 120-126.
9) Katzenbeisser S. and Petitcolas P., "i*nformation techniques for Steganography and Digital Watermarking"*, Artech House, London, 2000.
10) Ali Saleh AL Najjar* "Improved System to Conceal High Capacity of Data Based on RGB Color Image Using RSA Encryption and Proposed LSB Technique" volume 6, Issue10, 2016
11) Aarti Mehndiratta "Data Hiding System Using Cryptography & Steganography: A Comprehensive Modern Investigation" Volume: 02 Issue: 01 | Apr-2015
12) Varsha1, Dr. Rajender Singh Chhillar "Data Hiding Using Steganography and Cryptography" Vol. *4, Issue. 4, April 2015*
13) Pria Bharti and Roopali Soni "A New Approach of Data Hiding in Images using Cryptography and Steganography", Volume 58– No.18, November 2012

Aye Myat Thu received her BE (Information Technology) degree from Technological University (Pathein), Ayeyarwady, Myanmar. She is doing postgraduate research for master degree at Information Technology Department, Pyay Technological University. Her research is concerned Networking Security. She is also a lecturer at Technology University Pathein.

Daw Tin Zar Nwe (Lecturer), Department of Information Technology in Pyay Technological University, Pyay, Myanmar.