Implementation and Analysis of Three Steganographic Approaches

Wai Wai Zin
University of Computer Studies, Mandalay
Mandalay, Myanmar
waiwaizin.ucsmmdy@gmail.com

Than Naing Soe
University of Computer Studies, Mandalay
Mandalay, Myanmar
Konaing2006@gamail.com

Abstract— **Due to increasing the technologies security systems are very popular in many areas. The security of information can be achieved by using encryption and steganography. In cryptography, encrypted data is transmitted after transforming the other form instead of the original data. Contrast cryptography, information hiding process can be extended for protecting from the interesting of any attacker. This paper proposes the enhance security system by combining these two techniques. In this system, the encrypted message is embedded in a BMP image file. In proposed system, three LSB steganographic techniques have been implemented and analyzed. This proposed system intends for data confidentiality, data authentication and data integrity. This system not only enhances the security of data but also becomes more powerful mechanism. This system intends to support effective ways for protecting data. The primary goal of our system is to enhance the security of data and then to compare three steganographic techniques. Then we will use the optimized method for embedding. In this paper, we just present three steganographic approaches. In this system, data is encrypted with RC4 encryption algorithm and then embedded the encrypted text in the BMP image file using three steganogrpaphic methods.**

Keywords: encryption, steganography, LSB techniques, RC4 algorithm

I. INTRODUCTION

The network security is becoming more important as the amount of data being exchanged on the Internet is increasing [1]. Encryption and steganography are the preferred techniques for protecting the transmitted data [2]. In this paper, the proposed system combines and takes advantages the efficiency of the two methods. In this system, data is encrypted with encryption algorithm (RC4) and then embedded the encrypted text in an image file with LSB steganographic method. To enhance the security of the data, we propose three encrypto-stego techniques. This paper is organized as follows. Section 2 is our related works related to our system. Section 3 gives a background about the encryption technique. In this technique, we use the hash function RIPEMD-160 for encryption key. In section 4, background concept of Blum Blum Shub Pseudo Random Number Generator is discussed. In section 5, we present three LSB steganogrpahic methods. Section 6 presents future plan and finally, section 7 concludes the paper.

978-1-61284-840-2/11/$26.00 ©2011 IEEE

II. RELATED WORKS

Nowadays security has become one of the most significant problems for information technology. Many users want to use their information to be secure. Cryptography and steganography can solve this issue. H.Al-Barhmtoshy, E.Osman and M.Ezzat implemented a secured package in [3]. This package is integrated under the hash function to protect multimedia information while communicated over insecure channels. Hash functions are supported for data integrity and authentication. In [4], Chiu-Wah Ng, Tung-Sang Ng and Kun-Wah Yip presented a unified architecture of MD5 and RIPEMD-160. This designed intended to obtain a resource efficient implementation. Their proposed hardware design is suitable for applications that require low to medium throughput such as Ethernet networks. H.MIchai, V.Thanasoulis, D.Schinianakis, G.Panagiotakopoulos, C.Goutis applied a novel technique for RIPEMD-160 in [5]. In [6] M.Knezevic, K.nezevic, K.Sakiyama, Y.K.Lee and I.Verbauwhede presented two new architecture on the high throughput implementation of RIPEMD-160 Algorithm. Their approach can be used in other popular hash algoritms for a high-throughput implementation. Allam Mousa and Ahmad Hamad predicted the performance of the RC4 algorithm in [1]. To predict the performance they used various encryption key length and file size. Alfred J.Menezes, Paul C.Van Oarschot and Scott A. Vanstone said modern stream cipher in [7]. They said that stream ciphers are faster than the block cipher. To produce keystrings, LFSR (Linear Feedback Shift Register) can be used. In RC4, LFSR is not used to produce keystrings. For RC4, stream combinations are done on byte-length strings of plaintext. Mr.Nabarun Bagchi proposed a secure method using dual security model and Max-Bit Algorithm in [8]. In his system, secure BMP image steganography was used by using I.D.E.A image intensity and Bit Randomization. His proposed method was intended for hiding the maximum data in each pixel. His paper is a very good for strongest stegano operation. H.B.Kekre, Archana Athawale and Pallavi N.Halarnakar proposed a new improved version of LSB method in [9]. Their proposed method used gray scale image as cover image. The proposed method was also implemented on color image. In [10], Mamta Juneja and Parvinder Singh Sandhu presented a technique that combined steganography and encryption technique. The goal of this application was to help users maintain their data's confidentiality. They described steganography tools based on LSB algorithms. These tools supported BMP, GIF, PNG images and WAV

audio files as the carriers. But their application only supported hiding data in BMP images.

III. BACKGROUND OF CRYPTOGRAPHY

In cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available. It makes no attempt to disguise or hide the encoded message. 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 someone or something [11]. There are several ways of classifying cryptographic algorithms. The three types of algorithms are:

(1) Secret Key Cryptography: Uses a single key for both encryption and decryption.

(2) Public Key Cryptography: Uses one key for encryption and another for decryption.

(3) Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information.

A. RC4 Encryption Algorithm

In this paper, we use RC4 encryption algorithm. It is a variable key size cipher and symmetric key algorithm. Variable key size is from 1 to 256 bit to initialize a 256 bit state table. State table is used for subsequent generation of pseudo-random bits and then to generate a pseudo-random stream. The algorithm has two stages: initialization and operation.

The steps for RC4 encryption algorithm is as follows: [12].

1. Get the data to be encrypted and the selected key.
2. Create tow string arrays.
3. Initiate one array with the numbers from 0 to 255.
4. Fill the other array with the selected key.
5. Randomize the first array depending on the array of the key.
6. Randomize the first array within itself to generate the final key stream.
7. XOR the final key stream with the data to be encrypted to give cipher text.

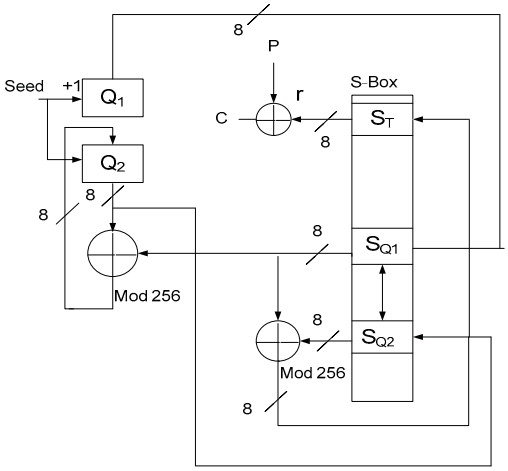


Figure 1. Model of RC4 encryption

B. RIPEMD-160 hashing function

Hash algorithms are important components in many cryptographic applications and security protocol suites [4]. Hah functions, also called message digests and one way encryption, use no key. They are also employed by many operating systems to encrypt passwords. Therefore, it provides a measure of the integrity of a file.

In this paper, we use RIPEMD-160 hash algorithms to provide higher protection. RIPEMD-160 has been designed by Hans Dobbertin, Antoon Bosselaers and Bart Preneel and produces a 160 bit output after performing five independent rounds. Each round is composed of 16 iterations resulting in 80 iterations in total. RIPEMD-160 operates on 512-bit message blocks which are composed of sixteen 32-bit words. The compression function consists of two parallel data paths as shown in Fig. 2. F_i and F_i' are non-linear functions and K_i and K_i'are fixed constants. Temporary variables A, B, C, D and E for the left and A', B', C', D' and E' for the right data path, are initialized with the five 32-bit chaining variables, h_0, h_1, h_2, h_3 and h_4 respectively. Chaining variables are either initialized with the fixed values to hash the first 512-bit message block or updated with the intermediate hash values for the following message blocks. Each step of the algorithm uses a different message word Xi for the left and X_i' for the right data path. All the 16 message words are reused for each round but in a different order [6].

RIPEMD-160 Algorithm

$T = \mathrm{rol}_s(A \oplus F_i(B, C, D) \oplus X_s \oplus K_i) \oplus E$

$E = D$

$D = \mathrm{rol}_{10}(C)$

$C = B$

$B = T$

$A = E$

$T' = \mathrm{rol}_{s'} A' \oplus F_s'(B', C', D') \oplus X_i' \oplus K_i') \oplus E'$

$E' = D'$

$D' = \mathrm{rol}_{10}(C'')$

$C'' = B'$

$B' = T'$

$A' = E'$

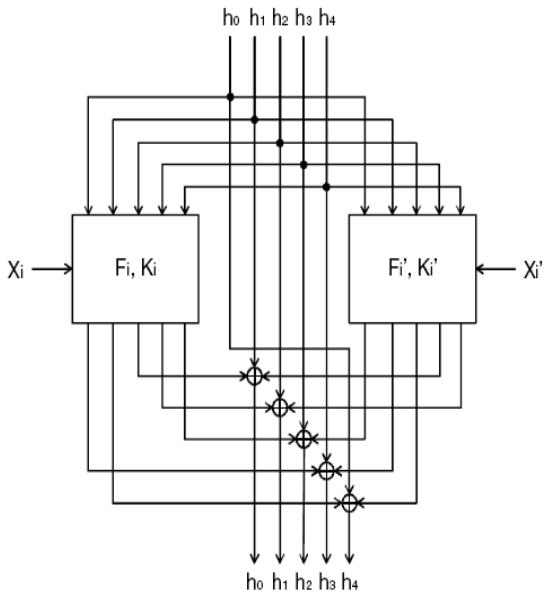


Figure 2. Comparison function of RIPEMD-160 algorithm

IV. BLUM BLUM SHUB PSEUDO RANDOM NUMBER GENERATOR

Random numbers play an important role in the use of encryption for various network security applications. One of well-known generators for generating secure pseudorandom number is known as Blum Blum Shub (BBS) generator. It has perhaps the strongest public proof of its cryptographic strength. The procedure is as follows.

Choose two large numbers, p and q.

These numbers have a remainder of 3 when divided by 4.

$p \equiv q \equiv 3 \pmod 4$

Let n = p x q

Next, choose a random number s, such that s is relatively prime to n.

Then BBS generator produces a sequence of bits B_i according to the following algorithm [13].

$X_0 = s^2 \bmod n$

For i = 1 to α

$X_i = (X_{i-1})^2 \bmod n$

$B_i = X_i \bmod 2$

In this paper, the encryption key from RIPEMD-160 hash function is an input of BBS random number generator and to generate random key stream for stego key.

V. THREE LSB STEGANOGRAPHIC METHODS

Steganography becomes more important as more people join the cyberspace revolution. Steganography is the art of concealing information in ways that prevent the detection of hidden messages. Some of the techniques used in steganography are domain tools of simple system such as least significant bit (LSB) insertion and noise manipulation, and transform domain that involve manipulation algorithms and image transformation such as discrete cosine transformation and wavelet transformation [11]. In this system, we use three LSB steganographic methods. It is the most well-known image steganography technique. In our system, after producing cipher text, random key stream and cipher text are embedded by using LSB steganographic technique. In this case, there are 3 LSB steganographic methods: (1) Simple LSB method after encryption (2) Hide using Pseudo Random Number Generator (3) Hide using Scattered LSB method.

A. Simple LSB Method after encryption

First method is simple LSB method after encryption. Before hiding the secret data (cipher text), header field is added to the encrypted message. Stego-key and file extension are included with these modified messages together. In our proposed system, BMP image file is used as the container image. In BMP file container, 54 bytes are BMP file header. Next bytes are RGB color values. In this method, message must be encrypted before inserting the secret data to the LSB of container image.

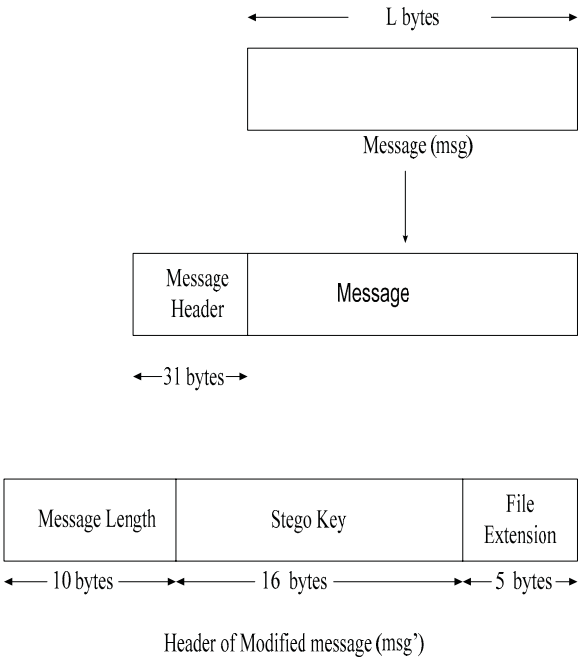
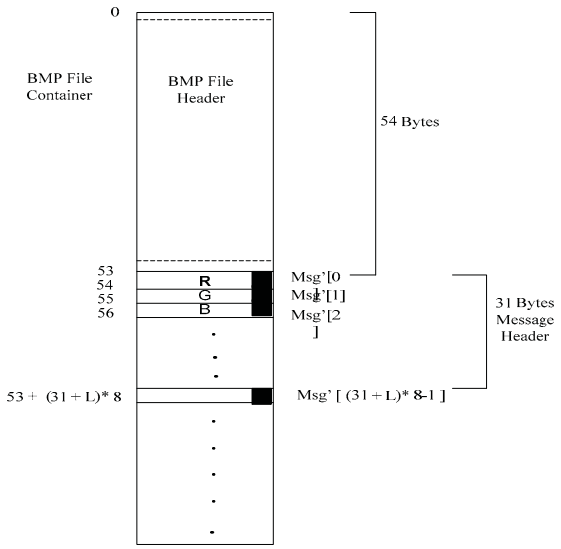


Figure 3. Pre Processing for Modified of Message

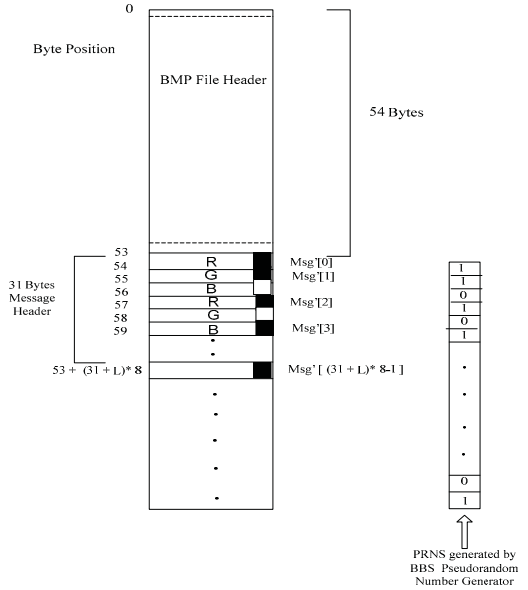


Msg' = Modified message
Msg'[j] = Bit value of position ' j ' (of modified message)
L = Length of Message

Figure 4. Simple LSB Method after encryption

B. *Hide Using Pseudo Random Number Generator*

Hiding using PRNG is the second method. This method depends on the pseudo-random number sequences. Random sequences may be strings of 1 and 0.These random sequences can be generated by using any type of PRNG. In proposed system, BBS generator is used to generate random sequence. If BBS (Blum Blum Shub) generates "1"as PRNS, the secret message may be inserted to LSB of container image. In contrast, the message can't be inserted to LSB.

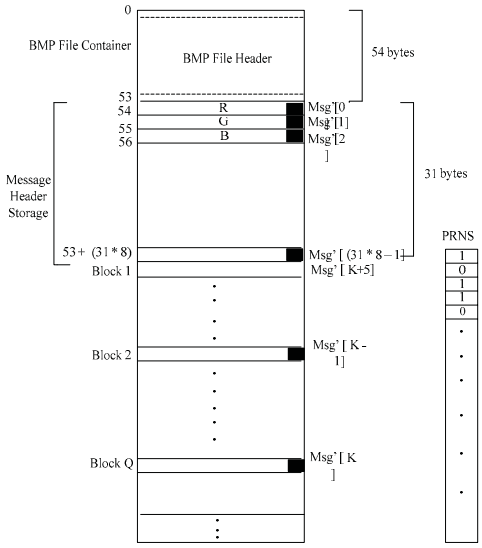


Msg' = Modified message
Msg'[j] = Bit value of position ' j ' (of modified message)
L = Length of Message

Figure 5. Message Hiding used BBS PRNG

C. *Hide Using Scattered LSB Method*

Last method is Scattered LSB method using BBS Generator. In this method, BMP file is divided into number of blocks. In each block, the encrypted messages may be embedded in LSB of container image which depends on the PRNS (Pseudo-random number sequence). This last method is similar to the insertion process of second method.



Msg' = Modified message
Msg'[j] = Bit value of position ' j ' (of modified message)
L = Length of Message
Q = Block Count
L/Q = Length of one Block

Figure 6. Simple LSB Method after encryption

VI. LIMITATION FOR THREE METHODS AND FUTURE PLAN

In this paper, this system uses the steganography method for embedding the encrypted data into image. But this system intend to use only bitmap file (*.bmp). The data size depends on the size of the cover image. The drawback is that if the stego-image is transformed (rotation, masking, etc) by some image processing software the data cannot be extracted. In this paper, the first method is very simple. If the attacker knows the stego key, the attacker can get the secret data. The second method depends on pseudo random sequences. As a consequence of these sequences, the secret message may be more secure than the first method. Last method is similar to the second method. But the last method is more secure than the second method because it is divided into several blocks. The secret messages can be embedded in each block. So, the attacker can't know easily what data

exists in which block. In proposed system, we just proposed three steganographic methods. So, our assumption on the last method cannot correct clearly. Firstly, we need to compare and analyze three steganographic methods and then the optimized method will use for data hiding. Finally, stego-image can be produced after inserting cipher text file into stego medium (container image). It is important to ensure that the size of the image can support the message to be embedded. This system uses cryptography and steganography to enhance the security. By combining these two techniques, it can enhance confidentiality and integrity of information. The following figure is the proposed system.

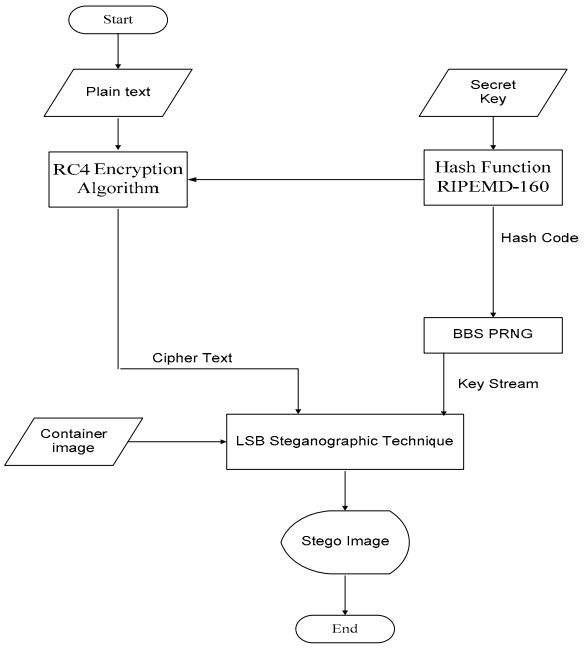


Figure 7. Proposed system

VII. CONCLUSION

Our proposed system uses cryptography and steganography to enhance the security. By combining these two techniques, it can enhance confidentiality and integrity of information. In this paper, we just present the three steganographic approaches for secure encrypto-stego technique. This system not only enhances the security of data but also becomes more powerful mechanism. Next, we will prove that.

REFERENCES

[1] Neha Sharma, Mr.J.S.Bhatia, Dr (Mrs) Neena Gupta, "An Encrypto-Stego Technique based secure data transmission system", 2004.

[2] H.El-din H.Ahmed, M.K.Hamdy, and O.S.Farag Allah, "Encryption quality analysis of the RC5 blok cipher algorithm for digital images", Optical Engineering, vol-45, Issue 10107003, 2006, (7 pages).

[3] H.Al.Barhmtoshy, M.Ezzat, E.Osman, "A Novel Security Model Combning Cryptography and Steganography"

[4] Chiu-Wah Ng, Tung-Sang Ng and Kun-Wah Yip, "A Unified Architecture of MD5 and Ripemd-160 Hash Algorithms", 2004, IEEE.

[5] H.Michail, V.Thanasoulis, D.Schinianakis, G.Panagotakopoulos, C.Goutis, "Application of Novel Techniques In RIPEMD-160 Hash Function Aiming At High Throughput"

[6] M.Knezevic, K.Sakiyama, Y.K.Lee, I.Verbauwhede, "On the High-Throughput Implementation of RIPEMD-160 Hash Algorithm", 2006.

[7] Erik Zenner, Crypto Als, "Stream Cipher Criteria", 2006, eStream paper no. 2006/032.

[8] Mr.Nabarun Bagchi, "Secure BMP Image Steganography Using Dual Security Model (I.D.E.A image intensity and Bit Randomization) and max-Bit Algorithm.

[9] H.B.Kekre, Archana Athawalse, Pallavi N.Halamkar, "Increased capacity of Information Hiding in LSB's Method for Text and Image".

[10] Mamta Juneja, Parvinder Singh Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Inssertion and Encryption", 2009 IEEE.

[11] Muhalim Mohamed Amin, Subariah Ibrahim, Mazleena Salleh, Mohd Rozi Katmin, " Information Hiding Using Steganography", Department of Computer System & Communication Faculty of Computer Science and Information System, 2003.

[12] Allam Mousa and Ahmad Hamad, "Evaluation of RC4 Algorithm for Data Encryption", International Journal of Computer Science & Applications, vol-3, No.2, June 2006.

[13] William Stallings, "Cryptography and Network Security", Principles and Practices, Fourth Edition.