PERFORMANCE EVALUATION OF IMAGE STEGANOGRAPHIC TECHNIQUES BASED ON HYBRID CRYPTOGRAPHIC SYSTEM

Zin May Zaw[1], Thet Thet Aye[2]

Department of Computer Engineering and Information Technology, Mandalay Technological University, Mandalay, Myanmar

Abstract

Information security plays an important task in protecting data resources that are shared through insecure channels. Information security has two main approaches: Cryptography and Steganography, which help to ensure efficient and adequate level of security. Cryptography is the science of using mathematics to encrypt and decrypt data in which the data are converted into some other gibberish form. While Steganography is the art and science of hiding communication, a stenographic system, thus embeds hidden content in the unremarkable cover media so as not to provoke an eavesdropper's suspicion. The combination of steganographic and cryptographic technique can give the higher security than using stand-alone technique. Therefore, in this proposed system, AES and RSA cryptographic algorithms are effectively combined with a new steganographic algorithm, namely modified Cyclic Steganographic Technique (CST).Firstly, the secret message is encrypted with AES encryption technique and then the key of AES is encrypted with RSA algorithm to obtain the better security of the system. The performance of proposed method is evaluated by comparing LSB method, original CST and modified CST in terms of embedding capacity, Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE).

Keyword: Cyclic Steganographic Technique (CST), AES, RSA, LSB, MSE, PSNR.

1.INTRODUCTION

Nowadays, Information security has grown to be a colossal factor, especially with modern communication networks, leaving loopholes that could be leveraged to devastating effects. With the advent of technology, the illegal users can access and attack the data. All of the communicating bodies want confidentiality, integrity and authenticity of their secret information [5]. Steganography and Cryptography are well-known and widely used techniques to achieve the data security against various attacks but these two techniques have different in nature.

Cryptography is a method of protecting information and communication through the use of codes so that only those for whom the information is intended can read and process it. Encryption is a key concept in cryptography .It is a process whereby a message is encoded in a format that cannot be read or understood by an eavesdropper. A plain text from a user can be encrypted to a ciphertext, then send through a communication channel and no eavesdropper can interfere with the plain text. When it reaches the receiver end, the ciphertext is decrypted to the original plain text. Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data. In steganography the secret message embeds in a harmless looking cover such as text, image, audio or video. Among them, images are the most popular cover objects used for steganography. Moreover, in image steganography, color image steganography finds more importance than grey scale image steganography because color images have large space for information hiding.

Thus, this work implements an information security system based on hybrid cryptography and modified cyclic steganographic technique by using color image cover. According to the experimental results, the modified CST method is capable to hide more data in cover image and provides better security than original CST [1] and LSB substitution method.

2.RELATED WORKS

All In this modern era, information security is becoming the most important in data storage and transmission due to the rapid growth of digital communication and electronic data exchange. Therefore, new proposed algorithms to enhance the security are developed in order to get efficient reliability in many research areas.

In [1], K. Muhammad proposed the Cyclic Steganographic Technique (CST) method. The secret bits are embedded in the LSBs of cover image pixels' planes: RED, GREEN, BLUE, RED, GREEN, BLUE and so on. In addition, the binary value of secret bits can embed in one channel of LSB for one pixel. Therefore, the embedded data may be loss so that enough space needs for data embedding.

Moreover, in 2013, Por, L. Y. et al. proposed the LSB substitution algorithm which is known as Sequential Colour Cycle (SCC) algorithm that is used for data hiding in color image. This proposed algorithm can give high embedding capacity because secret data can be embedded in four LSBs of each RGB pixel. Then, PSNR is used to measure the quality of stego image. According to the PSNR values of this method, the image quality is fairly low because the average PSNR value is 31.49dB. Nevertheless, human visual senses cannot distinguish it. In addition to this, the data can be embedded in half of the cover image size. Therefore, this technique provides high embedding capacity [2].

According to the literature and concepts of the security enhancement approaches which are pointed out from the previous researches, image steganographic technique is modified and used with hybrid cryptographic algorithms in this proposed system.

3.BACKGROUND THEORY

This system is implemented based on the integration of two cryptographic algorithms such as AES and Rivest Shamir Adleman (RSA) algorithms and modified Cyclic Steganographic Technique (CST). But, for performance analysis and security consideration, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) of image are calculated on LSB, original CST [1] and modified CST methods.

3.1. AES Algorithm

AES is a symmetric block cipher that can process data blocks of 128 bits, using key sizes of 128, 192, and 256 bits. The number of rounds is relied on the length of the key. The key sizes decide to the number of rounds such as AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys[3].

The main loop of AES performs the following methods

1. Convert to State Array
2. Transformations (and Their Inverse)
   i. AddRoundKey
   ii. SubBytes
   iii. ShiftRows
   iv. MixColumns
3. Key Expansion

The matrix of 4x4 consisting of 128 bytes input block is known as the state array. The process of encryption revolves around four stages namely mix columns, sub bytes, add round key and shift rows.

Sub Bytes – It is defined as substitution step. It is non-linear. Each byte is restored with another according to S-box. The operation gives an indirect proportion in cipher. The resultant matrix consists of four columns and four rows.

Shift Rows – It is stage where each row is rotated repetitively a definite number of times. It is also known as permutation. The four rows in the matrix are rotated as accordingly. The rows are shifted to the left. Shift is carried out as Row1 is not rotated. Row2 is shifted one byte place to the left. Row3 is shifted two places to the left. Row4 is shifted three places to the left. The resultant matrix consists of the 16 bytes but rotated with respect to each other.

Mix Columns –In this step, each column is changed using matrix multiplication. Each column consists of four bytes. The resultant matrix consists of 16 bytes. The input is taken for each column. It takes four bytes. The output produces four bytes which is entirely different from the four bytes given as input.

Add Round Key – The round key is bounded to each byte of state. In this particular step, the matrix is XORed with the round key. A 4x4 matrix represents the original key. It contains 128bits. This 4 words key where each word is of 4 bytes, is converted to a 43 words key. The first four words represent W[0], W[1], W[2], and W[3].

3.2. RSA Algorithm

RSA involves a public key and private key. The public key can be known to everyone; it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key. The keys for the RSA algorithm are generated the following way[4]:
Step 1: Choose two distinct random prime numbers p and q: ($p \neq q$)
Step 2: Compute modulus: $p \times q$.
Step 3: Compute the totient: $\phi(n) = (p-1)(q-1)$ where $\phi(n)$ stands for
Step 4: Choose the public exponent e with gcd ($\phi(n)$, e); $1 < e < \phi(n)$.
Step 5: Calculate the private key d such that $d \equiv e^{-1}$ (mod $\phi(n)$).

For the data encryption, plaintext (M) must be in the range $0 < M < n$. Then, message (M) is encrypted by raising it to the e^{th} power modulo n to obtain the ciphertext (C) as shown in Figure 1. Decryption is the reverse form of encryption. Ciphertext (C) is decrypted by raising it to the d^{th} power modulo n to get back the plaintext (M) as depicted in Figure 2.

Plaintext: $0 < M < n$

Ciphertext: $C = M^e \bmod n$

Figure 1. Encryption Process of RSA Algorithm

Ciphertext: C

Plaintext: $M = C^d \bmod n$

Figure 2. Decryption Process of RSA Algorithm

3.3. Modified Cyclic Steganographic Technique (CST) method

Modified CST method is based on the existing CST method. In this method, the secret data are hidden in LSBs two channels of each pixel. In one pixel of cover image, the two secret bits are embedded. Therefore, the embedding capacity of proposed method is higher than the original method. The example calculation of embedding process and extraction process of modified CST method is shown in Figure 3 and Figure 4, respectively. The order of pixel colour is shown in TABLE I.

TABLE I

RANDOM MAPPING TABLE

Count	Pixels	Order of Pixels Color	
1	Pixel 1	RED	GREEN
2	Pixel 2	GREEN	BLUE
3	Pixel 3	BLUE	RED

Procedure for Message Embedding:

1. Take the colour image and secret data
2. Separate the RED, GREEN and BLUE channels from the cover image.
3. Convert the secret data into 1-D array of bits.
4. Set the count is initial 1.
5. If the count is 1, replace the LSB of RED and GREEN channels.
   Else if count is 2, replace the LSB of GREEN and BLUE channels.
   Else if count is 3, replace the LSB of BLUE and RED channels.
6. Increment the count by 1.
7. Set the count value by 1, if the count value is 3.
8. Step 5 to Step 7 is working until all secret data bits are embedded.
9. Combine all three channel planes to form stego image.

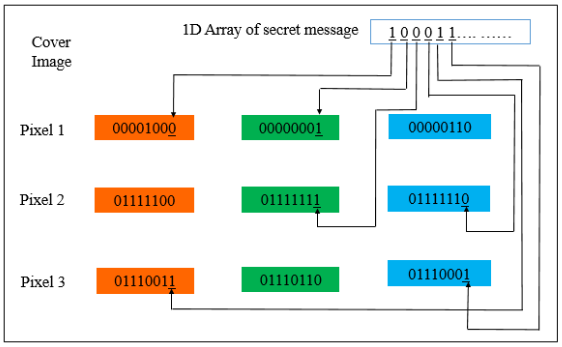

Figure 3. Example Embedding of Modified CST Method

Procedure for Message Extracting:

1. Take the stego image and separate the RED, GREEN and BLUE channels from it.
2. Set the initial count value is 1.
3. If the count is 1, extract the LSB of RED and GREEN channel.
   Else if count is 2, extract the LSB of GREEN and BLUE channel.
   Else if count is 3, extract the LSB of BLUE and RED channel.
4. Increment the count value by 1.
5. Set the count value is 1 when the count is 3.
6. Repeat step 3 to 7 until all secret bits are extracted.
7. Convert the extracted secret bits into its original secret data format.

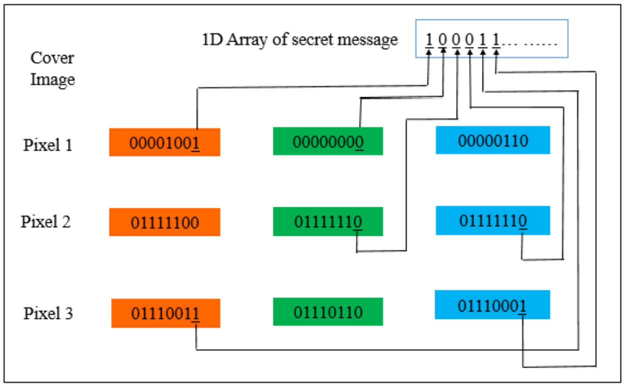

Figure 4. Example Extraction of Modified CST Method

3.4. Least Significant Bit (LSB)

Least significant bit (LSB) insertion is a common, simple approach for embedding information in a cover file where the binary representation of the data that to be hidden is written into the LSB of the bytes of the carrier. Firstly, the image data and secret message are accessed as a series of bits. Then, the bits of the secret message are inserted into the LSB of the bytes of the encrypted cover image by using XOR operation. On average, only half the bits in an image will need to be modified to hide a secret message using the maximum cover size [6].

3.5. Mean Square Error (MSE)

Mean Square Error (MSE) is the measure of error between the original image and the reconstructed image. It can be estimated in one of many ways to quantify the difference between the values implied by an estimate and the true quality being certificated. MSE is a risk function corresponding to the expected value of squared error. Given a noise-free m×n monochrome image I and its noisy approximation K, MSE is defined as shown in Equation (1):

$$\mathrm{MSE} = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[\mathrm{I}(i,j)-\mathrm{K}(i,j)]^{2}$$

,where I is original image, K is reconstructed image, m and n are height and width of the images respectively. The higher MSE indicates a greater difference between the original and processed image. On the other hand, the lower the value of MSE, the higher the quality of image.

3.6. Peak Signal to Noise Ratio (PSNR)

Peak Signal-to-Noise Ratio (PSNR) is the ratio between the modified image and original cover image. It is used for calculating the observable deformation that occurs in stego images after intentionally embedding secret data. The PSNR is calculated in terms of decibels (dB). The higher the value of PSNR, the more the stego image is correlated with original cover image and vice versa. Stego images with PSNR less than 30dB represent low quality. PSNR must strive for 40dB or higher values in order to fulfil the favorable demands of modern steganographic systems [7].

The PSNR is computed by using Equation (2).

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\mathrm{MAX}_{\mathrm{I}}^{2}}{\mathrm{MSE}}\right)$$

,where $\mathrm{MAX}_{\mathrm{I}}$ is the maximum possible pixel value of the image and MSE is the mean squared error.

4. PROPOSED SYSTEM ARCHITECTURE

The design of proposed system is organized with two portions: sender side and receiver side which are illustrated in Figure 5.

At the sender side, the secret message is initially encrypted by using AES algorithm with the secret key to obtain ciphertext. Then, the secret key is also encrypted by using RSA algorithm with receiver's public key to obtain cipher key. The resulting two ciphers are concatenated. Next, the concatenated ciphertext is embedded into the cover image by using modified CST which is based on the ideas of original CST [1]. Finally, stego image is sent to the receiver.

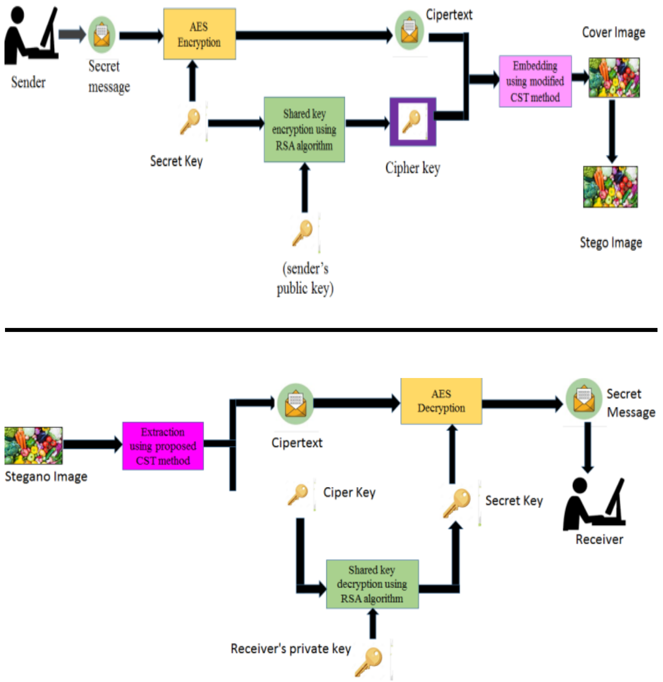

Figure 5. Proposed System Design

When the receiver has received the stego image from the sender, the concatenated ciphertext is extracted from the stego image by using modified CST. Then, ciphertext and cipher key are divided from the concatenated ciphertext. After that, cipher key is decrypted by using RSA decryption algorithm with the receiver's private key to obtain the secret key. At last, the original message is decrypted from the ciphertext by using the AES algorithm with the help of secret key.

5.PERFORMANCE ANALYSIS

In this section, the performance of LSB embedding method, original CST and modified CST are compared by evaluating Peak-Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE) values.

To comparative the performance of LSB, the original CST and modified CST, the experiments were evaluated based on the same image dimension to embed different amount of data. Figure 6 and Figure 7 show the comparison of MSE and PSNR results respectively.

According to the background theory and literature review, the lower the MSE, the better the stego image quality. As the experimental results, it can be found that in Figure 6, the MSE values of modified CST are lower than that of original CST which means that the stego image quality of modified CST is better than that of original CST. Furthermore, according to the experimental results, it can be found that the PSNR values of modified CST are higher than that of original CST as shown in Figure 7. The higher the PSNR values, the better the stego image quality.

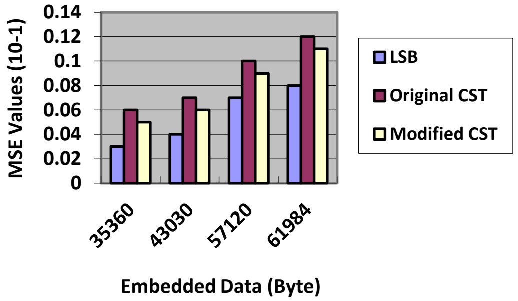

Figure6 .Comparison Results of MSE Values (Same Image Dimension with Different Amount of Data)

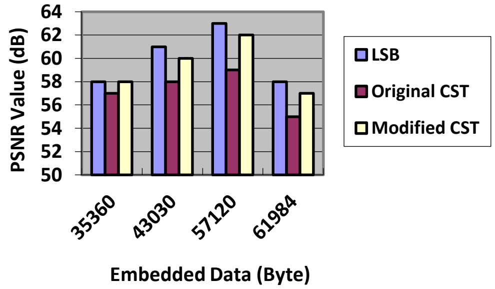

Figure 7.Comparison Results of PSNR Values (Same Image Dimension with Different Amount of Data)

6. CONCLUSION

This system proposed a secure image steganography system based on the integration of cryptography and steganography. From the security point of view, AES algorithm can give the data confidentiality but to prevent the breakable of AES key which is also called brute force attack, RSA algorithm can solve this attack by using separate keys for encryption and decryption. From the steganography point of view, in the original CST, secret message is embedded in the sequential color channel of RGB image. Therefore, the steganalyzer can extract easily the secret message. However, in the modified CST, cover image of channels are randomly selected according to random seed number. As a result, it makes difficulty for message extraction process compared to that of original CST. In addition, although the different amount of secret message was embedded in color images by using modified CST, the PSNR value is above 51dB. Therefore, it can be said that the modified CST can produce better image quality and embed very large amount of data in cover image.

REFERENCES

[1] N. U. R. Jamil Ahmad, Zahoor Jan, Khan Muhammad, "A Secure Cyclic Steganographic Technique for Color Images using Randomization," Technical Journal, University of Engineering and Technology Taxila, Pakistan, vol. 19, pp. 57-64, 2014.

[2] [13Por] Por, L. Y. et.al. : An Enhanced Mechanism for Image Steganography Using Sequential Colour Cycle Algorithm, International Technology, 10(1), January 2013.

[3] [01Ano] Annoymous: *Announcing the Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publications (FIPS PUBS), National Institute of Standards and Technology (NIST), American, (2001).

[4] [08Beh] Behrous A. Forouzan: "*Cryptography and Network Security*", International Ed., McGraw Hill Co., (2008).

[5] A.Kaur et al, "Review Paper on Image Steganography", *International Journal of Advance Research in Computer Science and Software Engineering"*, vol. 6, June 2016.

[6] Nilar Shein Lwin: "New Embedding Method Based on Stego-key Length", *The 4th International Conference on Science and Engineering (ICSE)*, Yangon, Myanmar, December, 2013.

[7] [07Xia] Xiangjun, L., and Jianfei, C.: Robust Transmission of JPEG2000 Encoded Images over Packet Loss Channels, ICME, (2007) 947-950.