A Novel Secure Combination Technique of Steganography and Cryptography

Pye Pye Aung[1] and Tun Min Naing[2]

[1]University of Technology (Yatanarpon Cyber City), Pyin Oo Lwin, Myanmar
[2]Computer University (Pathein), Myanmar

ABSTRACT

A new technique proposed with the combination of cryptography and steganography enhanced with new secure feature for generating a new security system. Cryptography and Steganography are two popular ways for secure data transmission in which the former distorts a message so it cannot be understood and another hides a message so it cannot be seen. In cryptography, this system is used advanced encryption standard (AES) algorithm to encrypt secret message and then these are separated keys; one of which is used to hide in cover image. In steganography, a part of encrypted message as a key is used to hide in discrete cosine transform (DCT) of an image which is highly secured. This kind of system is to be introduced in applications such as transferring secret data that can be authentication of various fields.

KEYWORDS

Cryptography, DCT Coefficient, Hiding Text, Steganography, Stego- image

1. INTRODUCTION

In networking, cryptography can be specified as the security service for data and telecommunications. Cryptography is an important way to address message transmission security requirements. Encryption and decryptiong of messages are made for the technique of cryptography. A mechanism of hiding the original messages from the intruders and by making a suspect of the existence of the message only to the intended receiver is called steganography. Here the secret message is sent as image or text through the encryption of the message in which special keys are arranged for those intended receivers to get the original message. The receiver only makes actual procedure of the real message sent by the sender. Real message can be letters or digits which can be encrypted as hidden message in any form as audio or video or image [3]. Steganography must not be confused with cryptography, where the message is transformed so as to make its meaningless to malicious people who intercept it. The goal of steganography is to avoid drawing suspicion to the transmission of the secret message between sender and receiver. A secure data transmission is made using cryptography and steganography. Combination of both these two techniques results in appearing a highly secured method for data communication.

DOI : 10.5121/ijitmc.2014.2105

2. BACKGROUND THEORY

Cryptography can be specified as the security service including authentication, privacy and confidentially. In this paper we have used AES algorithm in cryptography. The three types of algorithms are described:

(i) Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption.
(ii)Public Key Cryptography (PKC): Uses one key for encryption and another for decryption.
(iii)Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information [6].

Steganography is a mechanism for hiding and retrieving the high sensitive information in data transmission. Steganography must not be confused with cryptography, where the message is converted its meaningless to malicious people who intercept it. The main goal of steganography techniques is that it is diffilcult to detect the image and so saved from attacks. The steganography approaches can be distinguished into three types: pure steganography, secret key steganography and public key steganography.

2.1. AES algorithm for Cryptography

Advanced Encryption Standard (AES) is a standard for the encryption of electronic data. The U.S. government held in 1997 and now use in worldwide. AES is a symmetric-key algorithm which means that the same key is used both of sender and receiver. This AES standard specifies the Rijndael algorithm [1], a symmetric block cipher that can process data blocks of 128 bits, using key size of 128, 192, and 256 bits. The input, the output and the cipher key are used in Rijndael. It takes an input and output of certain block size, only 128 bits.

2.1.1. Advantages of using AES algorithm

1. Very Secure.
2. Reasonable Cost.
3. Main Characteristics:

I. Flexibility, II. Simplicity.

2.2. DCT - frequency domain algorithm for Steganography

The hidden message is a stream of “1” and “0” giving a total number of 80 bits to insert the secret message into the DCT domain of the cover image. The color-based transformation converts the image (cover image) into 8x8 blocks of pixels. Next, at least 80 larger positive coefficients need to embed in the cover image in the low-mid frequency range. DCT can divide the image into high, middle and low frquency components. As the high frequency coefficients are vulnerable and less robust on the quality of image. The main issue of this work is robustness against with high quality of image, thus the low and mid frequency coefficients are the most appropriate. The selected coefficients *ci* are modified by the corresponding bit in the message stream. This K quantity represents the persistence factor. As soon as the ith term of message bit s(i) is “1”, the coefficient of the image is added with a quantity K; otherwise the same quantity is subtracted form it. Thus the replaced DCT coefficients are

DCT (new) = DCT+1*K for s(i)=1;
Else DCT (new) = DCT-1*K for s(i)=0.

2.2.1. Advantages of using frequency domain Steganography

1. Very secure, hard to detect
2. More flexible, different techniques for calculation of DCT coefficients values

3. PROPOSED COMBINING TECHNIQUE

In cryptography, this system is used AES algorithm with its symmetric key and the cipher text is converted into two extra keys for high security, then the steganography is implemented to the key (3) to get stego image. The system is designed with three creation steps to hide the text –

(a) For Cryptography – Crypto Creation Step
(b) For Steganography – Stego Creation Step
(c) For Extra Securtiy – Security Creation Step

3.1. Crypto Creation Step

For Crypto Module, the following steps are applied for encrypting the data (Refer Figure1):

(a) Insert text for encryption.
(b) Apply AES algorithm using 128 bit key.
(c) Convert cipher text into types of format Hexadecimal, based 64 string and ASCII code respectively.

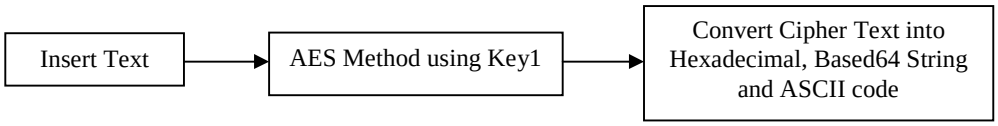

Figure 1. Crypto Creation Step

3.2. Security Creation Step

This security module works as follows: (Refer Figure2)

(a) Create array and allocate all the position points of digit (1) from the cipher text.
(b) Remove all the positions points of digit (1) from the cipher text and the remaining characters and digits are going to transform as modified cipher text.
(c) Remove the first ten allocated position of digit (1) among all digit (1) positions array and generate as a secret key (key 2).
(d) Take first ten allocated position points of digit (1) from all position points of digit (1) array and these ten digit(1) will be changed into the form of a secret key key(3).

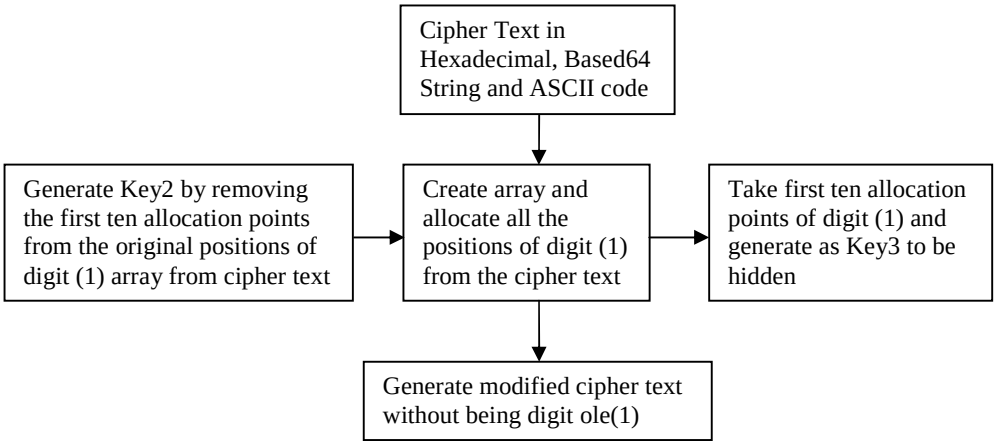

Figure 2. Security Creation Step

3.3. Stego Creation Step

For Stego Module, the following steps are discussed for hiding the above generated cipher text (Refer Figure3).

(a) Take the first ten allocated position points of digit (1) from the above discussed Security Module.
(b) Scramble the first ten allocated position points of digit (1) using a 64 bit key (Key 3).
(c) Take a Color Image.
(d) Find the DCT of the Image using color transformation.
(e) Hide the Cipher by altering DCTs.
(f) Apply Inverse DCT.
(g) Find the Stego Image.

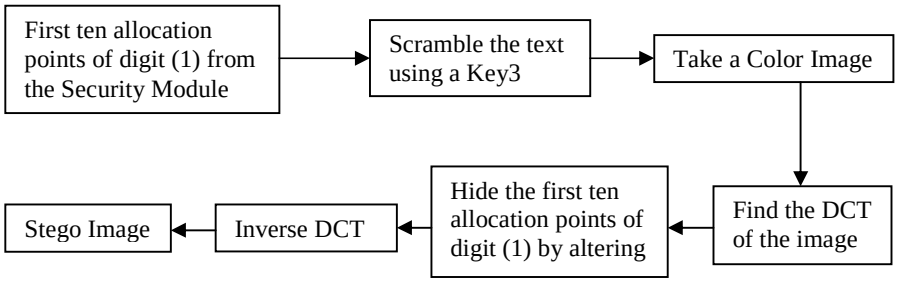

Figure 3. Stego Creation Step

4. PROPOSED SYSTEM IMPLEMENTATION

This system is developed in Visual Studio C# platform, mainly three creation steps involved –

(a) Crypto Creation Step – AES Implementation Step
(b) Security Creation Step – Newly Developed Technique
(c) Stego Creation Step – DCT Techniques Implementation Step

4.1. Algorithm for the proposed system

The steps of the algorithm for hiding text and retrieving text are discussed below (Refer Figure4 & Figure5).

4.1.1. Hiding Text

(a) Encrypt the original message into cipher text by using AES algorithm with symmetric key of key 1.
(b) Convert the cipher text into Hexadecimal format in the form of alphabets (A to F) and digits (0 to 9), Based 64 string format in the form of alphabets small letter (a to z), capital letter (A to Z), digits (0 to 9) and two arithmetic character (+/-) and ASCII code format of (256) characters respectively.
(c) Create array and allocate all the position points of digit (1) from converted cipher text and remove the first ten allocated points of all digit (1) positions and then generate the key (Key 2).
(d) Take the first ten allocated position points of digit (1) from array of cipher text and generate it as the third key (Key 3); this part will be hidden in the image.
(e) The cipher text without having digit (1) will be remained as modified cipher text.
(f) Hide the first ten allocated position points of digit (1) in the image and get Stego-Image.

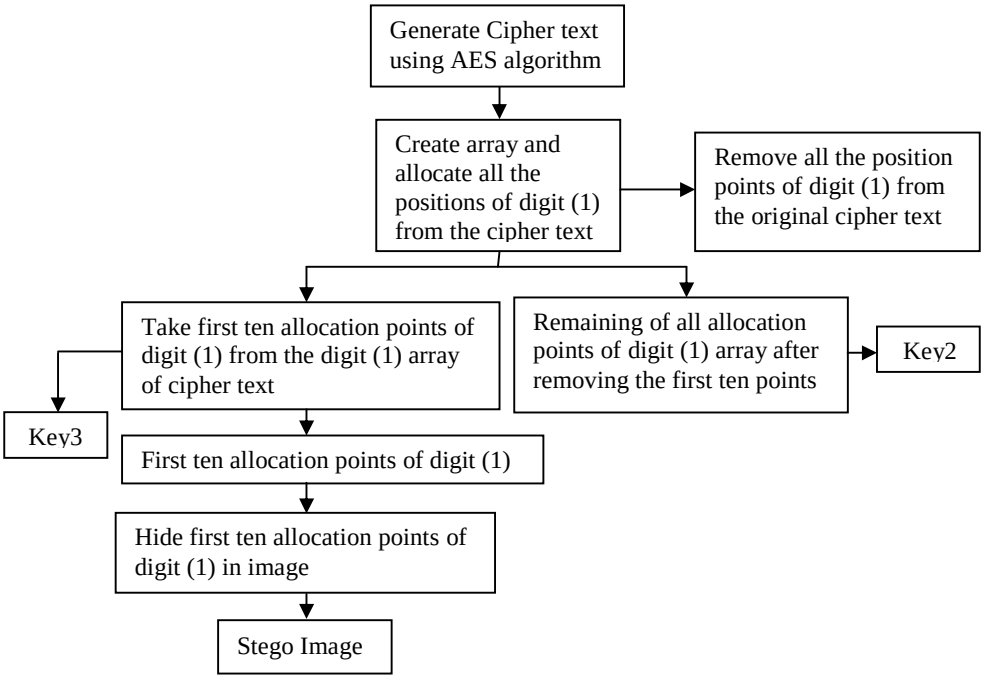

Figure 4. Proposed System for Hiding Text

4.1.2. Retrieving Text

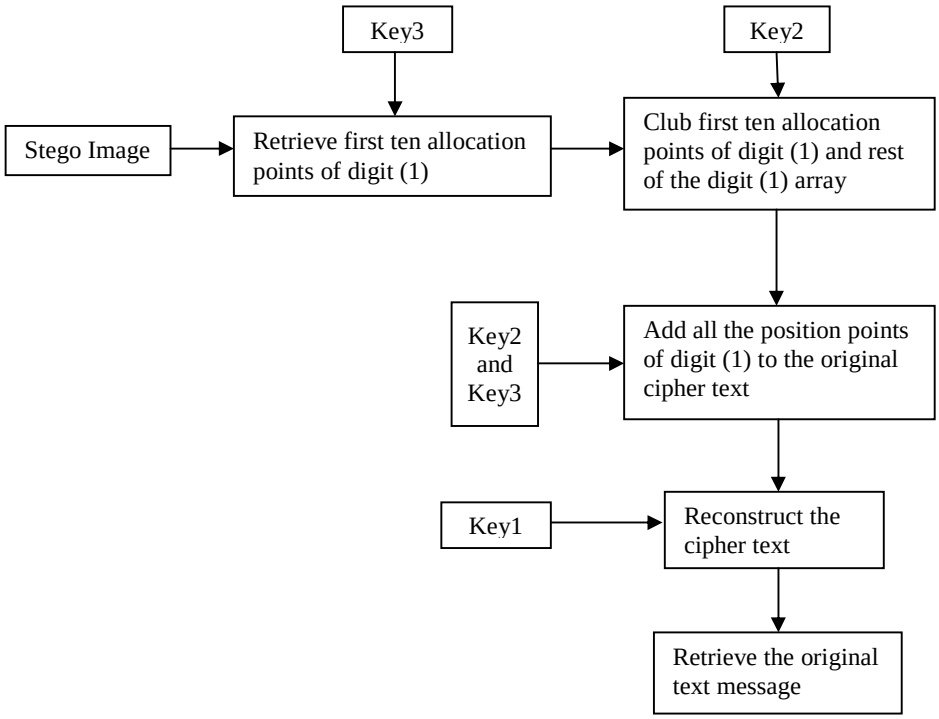

Figure 5. Proposed System for Retrieving Text

(a) Retrieve the first ten allocated position points of digit (1) from the image and unscramble it with Key 3.
(b) Add back the first ten position points of digit (1) into its all position points of digit (1) using Key 2.
(c) Add back all position points of digit (1) to the modified cipher text in order to get the original cipher text in Hexadecimal, Based 64 string and ASCII form.
(d) Reconstruct the original text message from the cipher text using AES algorithm and its key (Key 1).

4.1.3. Security Properties of Proposed System

The proposed system is highly secure because it is a combination of AES algorithm of encryption technique and DCT of message embedding technique. And also including two extra keys make the system highly secured. This system contains total 3 keys.

(a) One 128 bits symmetric key for AES algorithm
(b) Two 8 bits (1 byte) generated keys for scrambling the cipher text and retrieving the original message.

5. RESULTS

In this system, it can be compared our proposed system by using three kinds of encoding format type. They are Hexadecimal, Based-64 and ACSII code. Encryption time will be generated as different using three encoding format. Among them, ACSII encoding format is most efficient for large plaintext message to encrypt. But Hexadecimal encoding format will be taken more encryption time than any other format and so it can be used if the message size is small. As concerned with Based-64 encoding format is appropriate message size from below results. This paper shows the comparison of three encoding format in different messages in Figure6 and Figure7.

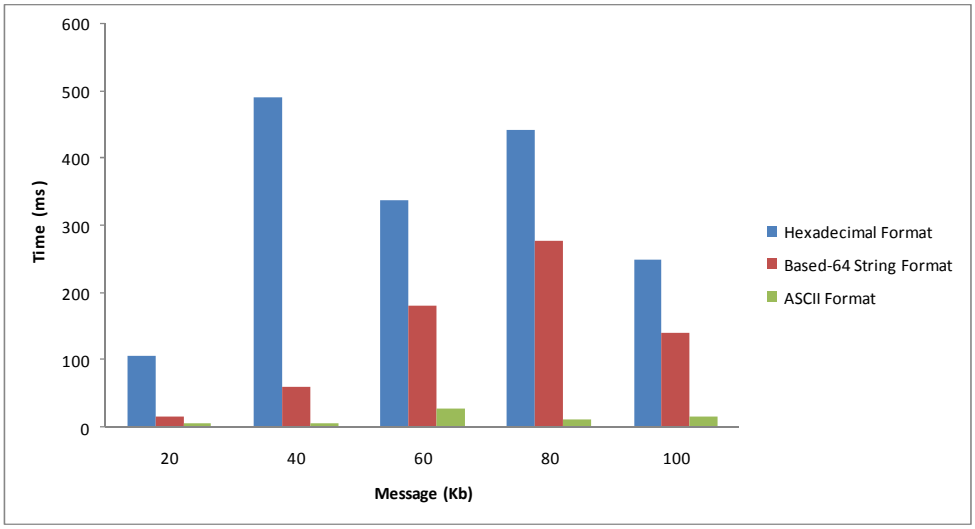

Figure 6. Key Separating time in Different Messages (20-100 Kb)

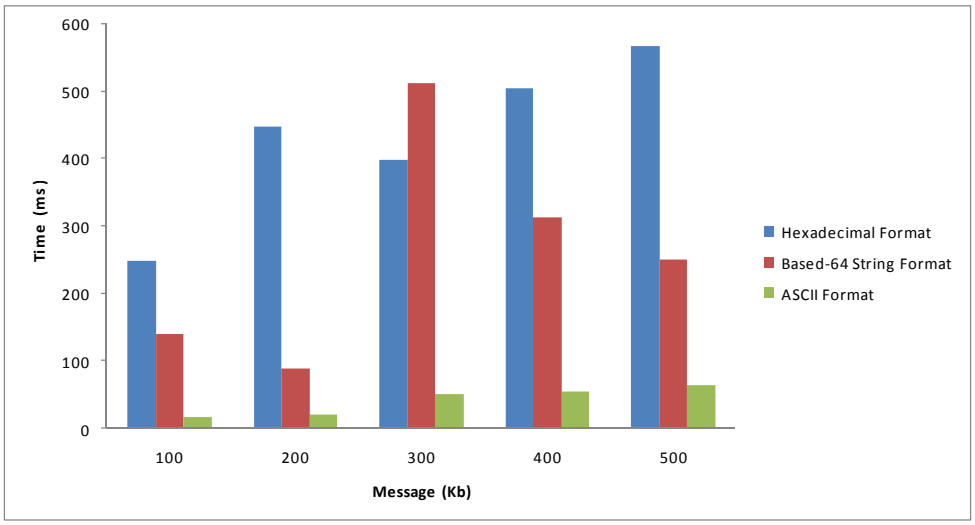

Figure 7. Key Separating time in Different Messages (100-500 Kb)

6. CONCLUSION

In this thesis, a new digital message hiding system is proposed for the combination of cryptography and steganography using three keys and modified cipher text. The combination of these two techniques satisfies the requirements such as highly security and robustness between sender and receiver. The proposed method ensures acceptable image quality with very little distortion in the image. The main advantage of this system is that the method used for AES algorithm which is very secure and the DCT transformation technique is very hard to detect in image steganography. It also produces efficient robustness of stego-image though it had been attacked by other techniques and additionally saved from attacks. Goal of this paper is to develop a new security system that messages cannot be retrieved easily from the image by any attackers or hackers in the communication process.

REFERENCES

[1] Secure Data Transmission using Stegnography and Encryption Technique, Shamim Ahmed Laskar and Kattamanchi Hemachandran, International Journal on Cryptography and Information Security (IJCIS),Vol.2, No.3, September 2012.

[2] Novel Security Scheme for Image Steganography using Cryptography Technique, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012.

[3] A Novel Information Security Scheme using Cryptic Steganography B. Raja Rao et. al. / Indian Journal of Computer Science and Engineering Vol. 1 No. 4 327-332.

[4] G. Ulutas, M. Ulutas and V. Nabiyev, "Distortion free geometry based secret image sharing", Elsevier Inc, Procedia Computer Science, Vol.3, pp.721–726, 2011.

[5] Proposed System for Data Hiding Using Cryptography And Setganography International Journal of Computer Applications (0975 – 8887) Volume 8– No.9, October 2010.

[6] B. E. Carvajal-Gámez , F. J. Gallegos-Funes and J. L. López-Bonilla, "Scaling Factor for RGB Images to Steganography Applications", Journal of Vectorial Relativity, Vol.4, No.3 pp.55-65, 2009.

[7] Domenico Daniele Bloisi, Luca Iocchi: Image based Steganography and cryptography, Computer Vision theory and applications volume 1, pp. 127-134.

[8] X. Li and J. Wang, "A steganographic method based upon JPEG and particle swarm optimization algorithm", Information Sciences 177 (15) (2007) 3099–31091.

[9] Domenico Daniele Bloisi, Luca Iocchi: Image based Steganography and cryptography, Computer Vision theory and applications volume 1, pp. 127-134.

[10] William Stallings, ―Cryptography and Network Security: Principles and practices‖ , Pearson education, Third Edit ion, ISBN 81-7808-902-5.