Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 7, July 2014, pg.195 – 199

RESEARCH ARTICLE

A Novel Approach for Multilevel Steganography

M.Ananathavalli[1], K. Kuppusamy[2]

[1]M.Phil Research Scholar
Department of Computer Science and Engineering
Alagappa University
Karaikudi, India

[2]Professor
Department of Computer Science and Engineering
Alagappa University
Karaikudi, India

[1] ananthavalli1991@gmail.com; [2] kkdiksamy@yahoo.com

Abstract*— The proposed scheme is a multi level steganography in which steganography is done at two places. The cover image is divided into fixed size blocks and then Discrete Cosine Transformation is applied into each block of cover image. The resulting DCT coefficients are quantized using quantization process. In the quantized DCT coefficient, the encrypted data file is embedded by using Least Significant bit technique. The resultant stego image is encrypted by Hill cipher algorithm. The encrypted image is hiding into another image. In the second level steganography the cover image is divided into equal sized blocks and then Discrete Wavelet Transformation is applied on each block. In the DWT coefficients the encrypted image is hidden by applying Least significant bit technique. Finally the performance parameters are evaluated.

***Keywords*— Steganography, DCT, DWT, Quantization, Huffman coding, AES Rijndael, Hill Cipher Algorithm**

I. INTRODUCTION

Data security is more important in the telecommunication sector. Cryptography and Steganography are two important techniques for communication over a network in secure manner. Steganography is the process of communicating information in a secret and hidden way. The data will be hided inside the text or an image or may be in the audio or video file. Steganography consists of cover image, data to be hide and algorithm for embedding.

The approach of combining cryptography and steganography gives more secure data transmission. This approach prevents the data from the crackers do not break the security of data. The steganography could be classified into two categories such as spatial domain steganography and frequency domain steganography. In spatial domain steganography the

data will be hiding directly inside the cover object by modifying its bit position. The well known spatial domain steganography algorithm is LSB. In frequency domain steganography the spatial domain of the image will be transferred into frequency domain.

For encryption the AES Rijndael algorithm is used to encrypt and decrypt the text as well as the image, because it is considered as a better solution for image encryption. The AES Rijndael algorithm is used, because of its simplicity, efficient working syntax. Since, AES Rijndael algorithm is precise, substitution ciphers are used to encrypt the given data. In this proposed methodology symmetric transmission is used for data encryption. Hence at both ends, same key is used to encrypt and decrypt information. The quality of the encrypted images is tested with different quality factors [3].

The AES Rijndael algorithm is the advanced encryption standard algorithm, used most widely for encryption because of its simplicity and efficient working syntax. Rijndael is an iterated block cipher with a variable block length and a variable key length. The block length and key length can be independently specified to 128,192 or 256 bits.

DCT technique is applied to perform first level steganography process. It is used to fetch the DCT coefficients for the process. DCT separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components. In low frequency sub-band, much of the signal energy lies at low frequency which contains most important visual parts of the image while in high frequency sub-band, high frequency components of the image are usually removed through compression and noise attacks. So the secret message is embedded by modifying the coefficients of the middle frequency sub-band, so that the visibility of the image will not be affected [4].

DWT technique is applied to perform second level steganography process. A 2-dimensional DWT consists of two operations: One is the horizontal operation and the other is the vertical one. Detailed procedures of a 2-D DWT are described as follows: At first, scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right. Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part while the pixel differences represent the high frequency part of the original image [1].

Hill cipher is a polygraphic substitution cipher introduced by Lester S.Hill in 1929 which is the first polygraphic cipher. In the hill cipher encryption, the message is divided into block of n size. The matrix is used as a cipher key. Each block is multiplied by an invertible n x n matrix. The Hill cipher algorithm is used to encrypt the image in the proposed work.

II. LITERATURE REVIEW

Cryptography and steganography are important in transferring the images through communication networks to protect data, against malicious attacks. Neil F. Johnson and Sushil Jajodia et al. have provided several Characteristics in information hiding methods to identify the existence of hidden messages and also identify the hidden information [12].

Lisa M.Marel and Charles T. Retter [11] have presented a method of embedding information within digital images. A hidden message can be recovered by using appropriate keys without any knowledge of the original image. Giuseppe Mastronardi et al.,[13] have studied the effects of steganography in different images formats (BMP, GIF, JPEG).

Mohammed Ali Bani younes and Aman Jantan [5] have proposed a steganographic approach for data hiding. This approach uses the LSB insertion to hide data within encrypted data. Bhattacharrya et al. proposed a security model which imposes the concept of secrecy over privacy for text messages. The proposed model combines the steganographic techniques with cryptography.

In the paper proposed by Nawal El-Fishaway and osama M.Abu Zaid quality of the encryption algorithms based on specific parameters is discussed [6]. H.Elkam Chouchi and M.A.Markar proposed the measurement of the quality of the bitmap images using the Rijndael and kamkar block cipher algorithms [14].

M.Van Droogenbroeck and R. Benedett, have proposed the techniques and methods used for the encryption of compressed and uncompressed images. In their work, the data is partly encrypted, as image content in order to be visualizing the encrypted images, although not with full precision. The principle of selective encryption is first applied to uncompressed images. A scheme called multiple selective encryptions is proposed in their paper [9].

I.Ozturk and I.Sogukpmar have proposed the comparative study on various encryption algorithms and their analysis for the image encryption techniques [7]. V.Potdar and E.Chang proposes the differentiation of the text encryption and the Image encryption techniques and their results [8].

J.Mahalakshmi and K.Kuppusamy [3] have proposed a novel technique for the image encryption using the AES Rijndael algorithm. Also, some performance metrics are discussed.

Gopala Lakshmi et al presents the paper "Optimal Huffman coding Of DCT Blocks" [4] in which a minor modification to the Huffman coding of the JPEG baseline compression algorithm to exploit steganography.

III. **PROPOSED WORK**

In this proposed work, multilevel data hiding scheme is developed. The proposed work involves double encryption and double steganography.

A. DCT based steganography

Discrete cosine transform (DCT)-based steganography algorithm have been proposed for image steganography. The bitmap image taken as input for DCT based steganography. In this system, the bitmap image is divided into 8 x8 blocks and then DCT is applied on each block. Next, DCT coefficients are quantized using quantization and, finally, the quantized DC coefficients are Huffman encoded. Finally LSB is applied on DC coefficients.

1) Steps to embed text message

Step 1: Read cover image.
Step 2: Read secret message and convert it in binary.
Step 3: The cover image is broken into 8×8 block of pixels.
Step 4: Working from left to right, top to bottom divide each block of pixels by 3.
Step 5: DCT is applied to each block.
Step 6: Each block is compressed through quantization table.
Step 7: Apply Huffman coding for each block.
Step 8: Calculate LSB of each DC coefficient and replace with each bit of secret message.

B.DWT based Steganography

Discrete wavelet transform DWT based steganography algorithm have been proposed for image steganography. The bitmap image taken as input. In this system, the bitmap image is divided into 8 x8 blocks and then DWT is applied on each block. Next, DWT coefficients are quantized using quantization and, finally, the quantized DWT coefficients are Huffman encoded. Finally LSB is applied on DWT coefficients. The following steps are applied for DWT based steganography.

1) Steps to embed data

Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step 2: Convert the text message into binary.
Step 3: The cover image is broken into 8×8 block of pixels. Divide each block of pixels by 3.Apply 2D DWT transform on each block.
Step 4: Obtain the horizontal and vertical filtering coefficients of the cover image. Cover image is added with data bits for DWT coefficients.

Step 5: Each block is compressed through quantization table.
Step 6: Apply Huffman coding for each block.
Step 7: Calculate LSB of each DWT coefficient and replace with each bit of secret message.

C.Combined Approach

In this paper encryption process is done by two times for text security and for cover object such as image. And also steganography employs at two places. As, a first step the encryption of text is done using the AES Rijndael algorithm and covers inside the Bitmap image. After that, the Covered image is encrypted using the Hill cipher Algorithm and encrypted image covered inside another image. Hence, multilevel security for the data is imposed. It will provide the high secure data transmission.

1) Steps for Proposed Methodology

Step 1: Get text from user
Step 2: Apply AES Rijndael on text. Display Encrypted Text.
Step 3: Get the cover image (1) from the user
Step 4: hide encrypted text inside the cover image using DCT based Steganography. Display stego image.
Step 5: Encrypt stego image using Hill Cipher. Display the Encrypted image.
Step 6: Get the cover image (2) from the user. Hide encrypted image inside the cover image using DWT based Steganography.

2) Structure of Proposed Methodology

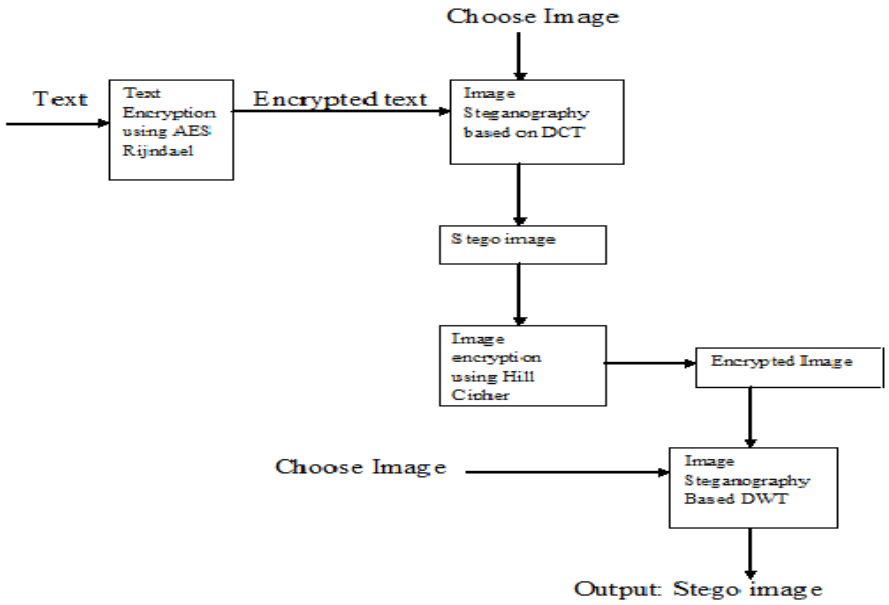

Fig. 1. Structure of Proposed Methodology

IV.**CONCLUSIONS**

In the network communication, data security is more considerable issue. The proposed work provides security to data provided by the user through multilevel steganography combined with cryptographic techniques. This multilevel encryption of data within images will significantly improves the security of the data and encryption ratio is increased. Moreover, various parametric measures are described so as to prove the proposed algorithm provides considerable security to the data.

The proposed work is applied on bitmap image. This combined work provides considerable better result for bitmap images.

For the first level steganography MOON and SEA SHORE image are taken to experimental test. The proposed steganography scheme for these bitmap images gives better performance values.

TABLE I
FIRST LEVEL STEGANOGRAPHY

IMAGE	PSNR	Embedding Efficiency
MOON	54.302	2.4077
SEA SHORE	52.456	2.0452

The second level steganography is applied on multilevel image and Blue image. The Syndrome coding and Huffman coding based DWT based steganography scheme provide better results. The performance results are list in the following table.

TABLE II
SECOND LEVEL STEGANOGRAPHY

IMAGE	PSNR	Embedding Efficiency
BLUE IMAGE	47.010	2.7037
MULTILEVEL IMAGE	45.853	2.3240

REFERENCES

[1] Po-Yueh Chen and Hung-Ju Lin, A DWT Based Approach for Image Steganography, *International Journal of Applied Science and Engineering 2006.*

[2] Stuti Goel, Arun Rana and Manpreet Kaur, A Review of Comparison Techniques of Image Steganography, IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 6, Issue 1 (May. - Jun. 2013), PP 41-48

[3] J.Mahalakshmi and K.kuppusamy, A New Technique for Image Encryption using AES Rijndael Block Cipher Algorithms, *International journal of computer Applications, vol 45, Number 11, pp. -7-10, May 2012.*

[4] Gopal Lakhani ,Senior Member, IEEE, Optimal Huff,man Coding Of DCT Blocks, IEEE Transactions On Circuits And Systems For Video Technology, Vol. 14, No. 4, April 2004.

[5] Mohammed Ali Bani Younes and Aman Jantan, A New Steganography Approach for Images Encryption Exchange by Using the Least Significant Bit Insertion, *International Journal of Computer Science and Network Security, vol. 8, no. 6, pp.247-257, 2008.*

[6] Nawal El –Fishaway, And Osama M.Abu Zaid, Nov 2007, Quality of Encryption Measurement of Bitmap Images with RC6, MRC6 and Rijndael Block Cipher Algorithms, *International Journal of Network Security, Vol.5, No.3, PP.241-251,. Nov 2007.*

[7] I.Ozturk and I.Sogukpmar, Analysis and Comparision of Image encryption Algorithms, *Transactions on Engineering, Computing and Technology, Vol.3, PP.1305-1313, 2004.*

[8] V.Potdar and E.chang, Disguising text cryptography using Image cryptography, *International Network Conference in plumouth , UK, 6-9, July, 2004.*

[9] M.Van Droogenbroeck and R.Benedett, Techniques for a Selective encryption of uncompressed and compressed images, *Proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS)* Ghent, Belgium, September 9-11, 2002, PP.90-97.

[10] I.Venkata and Saj Manoj , Cryptography and Steganography, *International Journal of Computer Applications* (0095 – 8887), Volume 1- No.12.

[11] Lisa M.Marvel and Charles T. Retter, "A Methodlogy for Data Hiding using Images," *IEEE conference on Military communication*, vol. 3, Issue. 18-21, pp. 1044-1047, 1998.

[12] Neil F. Johnson and Sushil Jajodia,1998,, "Steganalysis: The Investigation of Hidden Information," *IEEE conference on Information Technology*, pp. 113-116, 1998.

[13] H.Elkam Chouchi and M.A.Makar, 2005. "Measuring Encryption Quality of Bitmap Images Encrypted with Rijndael and Kamkar block ciphers", Twenty Second *National Radio Science Conference* CNRS (2005), PP.C11, Cairo, Egypt, 2005.

[14] Giuseppe Mastronardi, Marcello Castellano, Francescomaria Marino, "Steganography Effects in Various Formats of Images. A Preliminary Study," *International Workshop on Intelligent dataAcquisition and Advanced Computing Systems: Technology and Applications*, pp. 116-119, 2001.

