AES Algorithm based Separable Information Steganography

Mr. Sagar Y. Kumbhar[1] Dr. S. A. Patil[2] Miss Ashwini C. Kumbhar[3]
[1]PG Student [2]Head of Dept. [3]Assistant Professor
[1,2]Department of Electronics & Telecommunication Engineering [3]Department of Electrical Engineering
[1,2]DKTE, Ichalkarnji, India [3]AMGOI, Wathar Tarf Vadgaon

Abstract— As the internet is the prime medium to transfer information from one end to another across over the world. The secret data can steal in many ways this is the problem with sending information over the internet. Cryptography and data hiding are the most usually used techniques for improving the data security. Using Cryptography secret data can encrypt then by data hiding techniques sending encrypted data to a sender. Data hiding is the technique in that secret information was concealed into another cover image. An image containing secret information seems same as the cover image. In this paper, we analyze AES algorithm with different modes of operation (block cipher) regarding PSNR, MSE & Histogram, etc.

Key words: AES Algorithm, Information Steganography

I. INTRODUCTION

For to make unreadable data like text, image, audio and video during transmission scramble it using data Cryptography. So its goal is to keep the data secure from unauthorized access [1]. The method of concealing plaintext in such a way as to hide its data is called encryption. Encrypting plaintext results in unreadable data called cipher text. The process of reverting ciphertext to its original plaintext is called decryption. This is called cryptosystem. The complexity of encryption process depends on the encryption algorithm, key & the software used to encrypt or decrypt the data. Cryptographic algorithms are classified as asymmetric algorithms (public key) and symmetric algorithms (secret key), depending upon the number of keys used. In the Symmetric-key system a single key is used on both side of the sender and recipient. And, in the Asymmetric-key system two keys are used, a public key known to everyone and a private key that only the recipient of messages uses. So the symmetric key algorithms are further classified as block cipher (AES) and stream cipher (RC4). Block Ciphers operate with a fixed transformation on large blocks of plain text data while stream ciphers with the time-varying transformation on individual plain text bits. There are various benefits for stream cipher over block cipher like faster in operation, no or limited error propagation, low hardware complexity etc.

II. RELATED WORK

Some techniques are developed for compressing/ decompressing encrypted data. Traditionally to transmit redundant data over bandwidth-constrained channel first compress it and then encrypt it. Encrypting a data first and then compressing it without losing it & with the compressor does not have a knowledge of the encryption key was developed in [2]. Compress encrypted images by proper resolution, by progressive compression with a lossless manner is presented in [3]. The encrypted image was compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform using lossy compression method. With the higher compression ratio for better quality of the reconstructed images were developed in [4]. In [5], to cover data in higher and lower bit-planes of transform domains were respectively encrypted and watermarked. In [6], the content owner encrypts the signs of host DCT coefficients, for that each content-user uses a different key to decrypt only a subset of the coefficients, so that a series of versions containing different fingerprints were generated for the users. In these joint schemes, however, only a partial encryption is involved, in leading to a leakage of partial information of the cover.

III. AES ALGORITHM

The algorithm is flexible in supporting any combination of data and the key size of 128, 192, and 256 bits. However, AES only allows a 128-bit data length that can be divided into four basic operation blocks. These blocks operate on an array of bytes and organized as a 4×4 matrix which is called the state. For full encryption, the data is passed through rounds (Nr = 10, 12, 14) [4, 6]. Such rounds were implemented by the following transformations:

A. Bytesub Transformation

It is a nonlinear byte Substitution, using a substation table (s-box), which was constructed by multiplicative inverse and affine transformation.

B. Shiftrows Transformation

It is a next step of byte transposition, where the bytes in the last three rows of the state are cyclically shifted and the offset of the left shift varies from one to three bytes.

C. Mixcolumns Transformation

It is similar to a matrix multiplication of columns of the states. In which, column vector is multiplied by a fixed matrix. For that the bytes are treated as polynomials rather than numbers.

D. Addroundkey transformation

It is a simple XOR between the working state and the roundkey. This transformation is its inverse.

IV. DATA EMBEDDING

The secret message's LSB bit i.e. least significant bit of some or all of the bytes of an image are changed as per encryption strategy. Digital images are mainly of two types (i) 8-bit images(For Gray Scale Image) and (ii) 24-bit images(For RGB i.e. color image) In 8 bit images, one or two bit of information can be hidden [7][8][9]. So increasing or decreasing the value by changing the LSB does not change the appearance of the image much so the resultant stego image looks almost same as the cover image. But if we going to increase the number of bit greater than 3 bit, then there is a chance of loss of information of stego image.

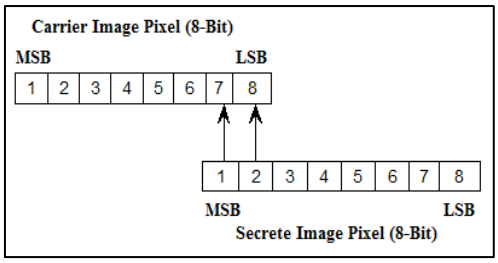

Fig. 1: LSB Embedding Technique

V. THE PROPOSED SYSTEM

Here in this system, a sender encrypts the data which going to hide can be any form of audio, video, text, document, etc. and the original image by using AES algorithm [10] and then after encrypting data and image system will auto-generate the data encryption and image encryption keys. Then Data embedding is done by using least significant bits i.e. LSB Embedding Technique means hiding of the encrypted data into encrypted image and then system will auto generate data-hiding key during the data hiding process. Then the sender will send such encrypted file with newly generated extension to the receiver via email but keys will be sending privately.

Then the receiver will receive an encrypted image containing additional data which is also encrypted. But if the receiver has data extraction and image decryption keys then he will decrypt an image similar to the original one up to 80%, but without getting the additional data. If the receiver has all three i.e. the data-hiding key, the data decryption key and the image decryption key, then he will extracts the additional data to its original form and recover the original natural image when the amount of data is not too large.

In proposed algorithm, an original image is encrypted using AES algorithm & then hiding of original encrypted image into host/carrier image by LSB embedding technique. Following shows the block diagram of proposed method.

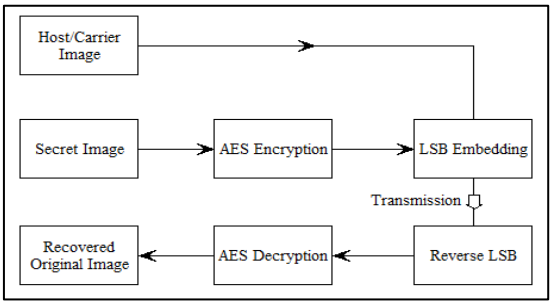

Fig. 2: Block Diagram of Proposed Method

VI. METHODOLOGY OF IMPLEMENTATION

A. AES Algorithm Steps

1) In our system, we are using 128 bit data block, and in AES it can be represented by Nb = 4, which given the number of 32-bit words (number of columns) used in the State array.
2) The Cipher Key length in AES (i.e. K) has given as 128-bit. Which is represented by Nk = 4, gives the number of 32-bit words (number of columns) in the Cipher Key.
3) So the number of rounds to be performed during the execution process of the algorithm is dependent on the key size. If the number of rounds is represented by Nr, then Nr = 10 when Nk = 4, Nr = 12 when Nk = 6, and Nr = 14 when Nk = 8.

B. Algorithm Steps for LSB Embedding

Inputs: Secret image, & the host image
Output: Encrypted image

1) Take the pixels of the AES Encrypted Secret image
2) Then take the pixels of the host image
3) Convert pixels to binary and replace the last 2 bits of host image with first two bits of secret image
4) Continue step 3 till secret image pixels finished and obtain stego image.
5) Following Fig.3 shows the 2 Bit LSB embedding process:

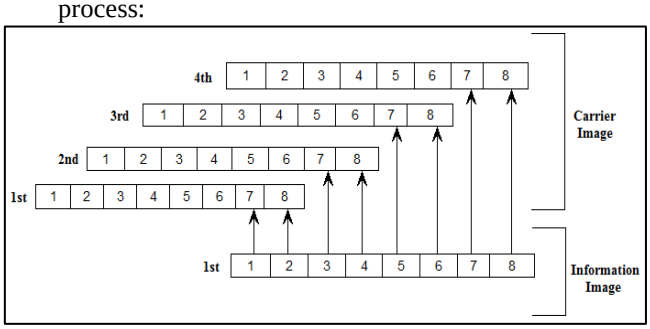

Fig. 3: 2-Bit LSB Embedding

C. Algorithm Steps for LSB Extraction

Inputs: stego-image
Output: Encrypted image

1) Take each pixel of stego image at a time.
2) Form temporary matrix with all zeros.
3) Convert stego pixel into binary and extract last two bits and replace at first of temporary matrix.
4) Continue step 3 until the size of encrypted image is achieved.

Following Fig.4 shows the 2 Bit LSB extracting process:

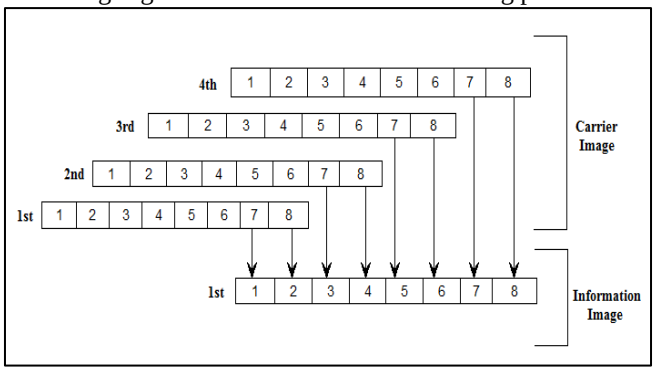

Fig. 4: 2-Bit LSB Extraction

D. Algorithm Steps for AES Decryption

1) Take input image obtained from LSB extraction.
2) Use the secret key same as that of used at the time of encryption and decrypt the image.
3) Continue step 2 until all the image is decrypts & obtain the final original information image.

VII. RESULTS & DISCUSSIONS

Here, the AES image encryption algorithm is tested & evaluated based on MATLAB software for simulating, analysis & visualization of experimental data. In this proposed method Secret image is encrypted

Using AES, then encrypted image hide into cover image by LSB embedding technique. For analysis purpose choose secret image having size 64x64 & cover image having size 260x270. Following Fig.5 shows MATLAB experimental results:

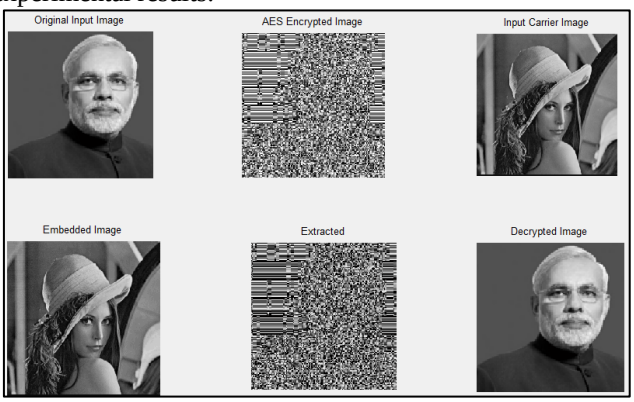

Fig. 5: Proposed Method Results using AES

VIII. PERFORMANCE EVALUATION

To compare the obtained secret image from final AES decryption & RC4 algorithm to that of original information image we use Peak signal to noise ratio (PSNR), Mean square (MSE) and Histogram as the parameter of comparison. PSNR and MSE were calculated as indicated the equations 1 and 2.

A. Peak Signal to Noise Ratio (PSNR)

It is defined as the ratio of peak square value of pixels by MSE. It is expressed in decibel. It measures the statistical difference between cover and stego images, is calculated using following equation

$$PSNR=10 \log 10 (255/RMSE) \quad (1.1)$$

B. MSE (Mean Square Error)

It is defined as the square of the error in between stego image and cover image. The distortion in the image can be measured using MSE & calculated using following equation

$$MSE=\sum ([f(i, j)-F(i, j)])^2 /N^2 \quad (1.2)$$

In this equation cover image f (i, j) that contains N by N pixels & stego image F (i, j), where F is nothing but decoded image of the encoded version of f (i, j).So that root mean square error (RMSE) is the square root of MSE.

$$RMSE= SQRT (MSE) \quad (1.3)$$

Cover image	Secret image	MSE	PSNR	Embedding time	Extract-ion time
Lena. bmp	Modi. bmp	2.8306e+004	3.6121	8 Seconds	9.5 seconds
Modi. bmp	Secret.bmp	960.9338	18.3039	8.03 seconds	10.05 Seconds

Table 1: Result using AES algorithm

C. Histogram Analysis

The Histogram analysis is employed to illustrate its original secret image & recovered decrypted the secret image. The histogram of the original image is shown below. By comparing these two histograms, we find that histogram of encrypted image is fairly uniform & is significant that from original one as shown in Fig.6

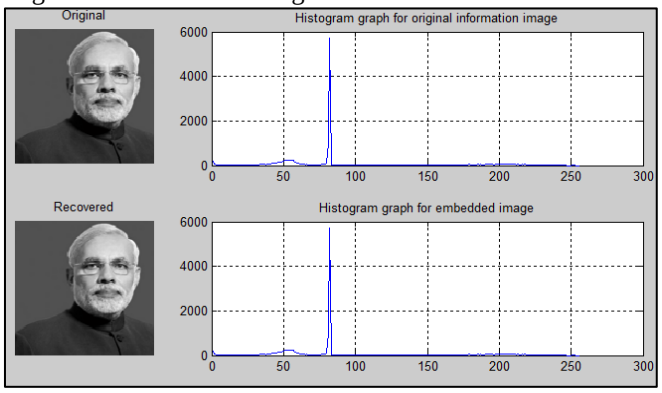

Fig. 6: Proposed Method Histogram

IX. CONCLUSION

In this paper, we have introduced AES Algorithm Based Separable Information Steganography. As we seen cryptography and steganography are two methods mainly used for of data security. In this proposed system cryptography and steganography methods are combined to give better security to secret data. In this proposed scheme secret message is encrypted before hiding it into the cover/carrier image which gives high security to secret data. So here AES is used for encryption of secret image, and 2-Bit LSB embedding technique is used to hide encrypted secret message into the host image. The present technique is implemented to combine the features of both cryptography and steganography, which will gives a higher level of security. The main thing of this system is that, the method used for encryption is AES, it is very secure, and the 2-Bit LSB embedding technique is used for steganography are very byzantine to detect.

ACKNOWLEDGMENT

It gives me immeasurable pleasure to express my lots of thanks with deep sense of gratitude to Prof. Dr. S. A. Patil HOD, Department of Electronics & Telecommunication Engineering, DKTE, Ichalkarnji as well as Miss Ashwini C. Kumbhar, Assistant Professor, Department Of Electrical Engg., AMGOI, Wathar tarf Vadgaon for their valuable guidance, encouragement and keen personal interest during the course of this project work, I thank him hearty for his unstinting co-operation and guidance.

REFERENCES

[1] Alanazi Hamdan.O., Zaidan B.B., Zaidan A.A., Jalab Hamid.A., Shabbir .M and Al-Nabhani.Y, "New Comparative Study Between DES, 3DES and AES within Nine Factors" Journal of Computing, Volume 2, Issue 3, March 2010, ISSN 2151-9617, pp.152-157.

[2] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[3] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[4] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inform. Forensics Security, vol. 6, no. 1, pp. 53–58, Feb. 2011.
[5] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inform. Forensics Security, vol. 4, no. 1, pp. 86–97, Feb. 2009.
[6] William Stallings, Cryptography and network security: Principles and Practice, Prentice Hall, Upper Saddle River, New Jersey, 2003
[7] "Detecting LSB Steganography in Color and Gray-Scale Images" Jessica Fridrich, Miroslav Goljan and Rui Du State University of New York, Binghamton.
[8] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, "Hiding data in images by optimal moderately significant-bit replacement" IEE Electron. Letter.36 (25)(2000) 20692070.
[9] "Hiding data in images by simple LSB substitution" by Chi-Kwong Chan, L.M. Cheng Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong Received 17 May 2002.
[10] Akash Kumar Mandal, Chandra Prakash, Mrs. Archana Tiwari "Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE Trans. on Electrical, Electronics and Computer Science, 2012.

