Secure Transmission of Data in Encrypted Image using Separable Reversible Technique with AES and BPCS Algorithm

Sneha Bhokare[1] Snehal Dighe[2] Pooja Lekawale[3] Shruti Patange[4] T.R.Patil[5]
[1,2,3,4,5]Department of Information and Technology
[1,2,3,4,5]NBNSSOE, Pune, India

Abstract— Steganography plays vital role for the secure communication between two parties, nevertheless communication is not guarantees for the security. In this paper we propose separable reversible data hiding technique in encrypted image using AES and BPCS algorithm. AES algorithm is used to encrypt data and image while BPCS algorithm is used to embed data into an encrypted image. To provide security to the embedded image we again encrypt the image using AES algorithm before sending to transmission medium. On the receiver end embedded image is decrypted by secured private key.

Key words: Image and data encryption; AES algorithm; BPCS Algorithm

I. Introduction

Due to untrusted medium secure communication is necessary. There is tremendous research going on to a solution for having secret communication between two parties and one area identified as a solution, which has also taken great stride since its inception in the history is Cryptography. Cryptography essentially deals with transforming the message and transmitting it .So that only the intended recipient can decipher what it means with the help of a key.

The aim in cryptography is to jumble the message with the help of a key so that the message becomes meaningless to the attacker, but can only be deciphered by either the same key or another key. Steganography does not allow us to change the message itself; rather we hide the message [11].

In Separable reversible data hiding technique data and image is separated and it is capable of returning to the original state without any loss. We use AES technology to resist two recent attacks, truncated differential attack and square attack. AES is the symmetric block cipher algorithm. It provides more security as compared to other used techniques. So that only the intended recipient can decipher what it means with the help of a key [22].

Another field is Steganography. Steganography is an art of embedding a message and the message will be hidden in a medium such as picture, audio file and video file [10]. Steganography provides more security as compare to cryptography in seemingly harmless messages like text, picture or other media. So in this case the attacker does not know if two parties are even exchanging messages [13].

II. Literature Survey

Currently available system provide separable data hiding in image but it has drawback like user must have all the keys to get original data and less security to data [3]. In other system of separable and reversible data hiding technique the data is embedded without encryption and provides less security for data as compared to image [2]. Least significant bit (LSB) is a simple approach to embedding information in an image. The least significant bit of some or all of the bytes inside an image is changed to a bit of the secret message. In LSB technique as it provide a less amount of space to embed a data [1]. Patchwork is a statistical technique that uses redundant pattern encoding to embed a message in an image.

To overcome this problem we are using BPCS steganography technique it allows to hide large amount of data in image. This technique makes use of the characteristics of the human vision system whereby a human cannot perceive any shape information in a very complicated binary pattern BPCS is the development of least significant bits (LSB) method, and it has better performance than the simple LSB method[1]. The major idea is that multiple bit-planes of the cover images are divided into fixed-size blocks. This technique is use to get high data hiding capacity and low perceptibility[5]. Although the LSB embedding methods hide data in such a way that the humans do not perceive it, such scheme can be easily destroyed, by a opponent such as using lossy compression algorithm or a filtering process.[14]

III. Proposed Methodology

In this system, we provide security tool based on steganographic technique in which data can be hidden in image without losing single bit of data. In this system, initially image and data will be encrypted by the AES algorithm.

The encrypted data stored with different extension to provide more security to the encrypted file. With the help of BPCS algorithm data is embedded with the encrypted image. Resulted image again encrypted by the AES algorithm. Now sender sends the resulted image and key to the receiver separately.

A. Sender Side:

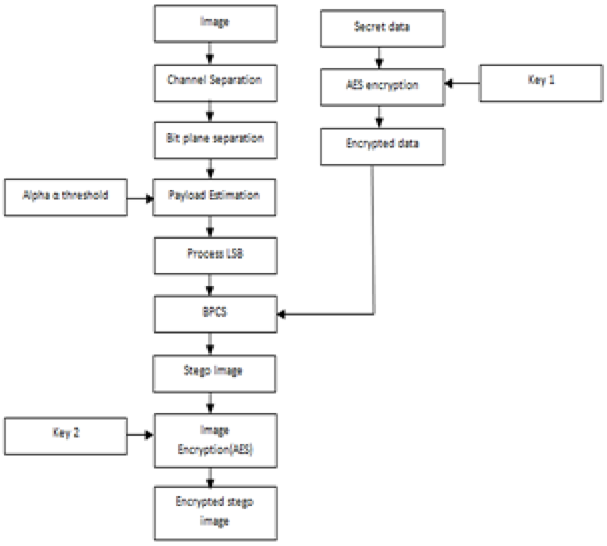


Fig. 1: Sender Side process

On the sender side:

1) *Channel Separation:*

The color data of an image is stored in the arrays known as channel typically the image will have at least 3 channels representing red, green and blue color value.

2) *Bit Plane Separation:*

Separating a color image into its bit planes is useful for analyzing the relative importance played by each bit of the image implying it determines the adequacy of number of bits used to quantize each pixel useful for image compression.

3) *Payload Estimation:*

Payload estimation is use to determine how block are available in the channel and channel are red green and blue.

4) *Processed LSBs:*

We can store large amount of data in LSB as compare to MSB plane because more number of block are present in LSB rather than MSB.

5) *Alpha Threshold α:*

Alpha is the threshold at which block are considered complex.

6) *Threshold:*

It is the simplest method of image segmentation from a grayscale image; threshold is also used for creating binary image.

7) *Image Encryption:*

The user will browse the image from computer and encrypt the image using AES algorithm and user also have to get a secret key.

8) *Encrypted Data:*

The user will browse data that he want send and encrypt the original data using AES algorithm and have to give a key.

9) *Secret data:*

Secret data is a confidential data which you want to send.

10) *Key:*

A piece of information used to encode or decode massage.

11) *Stego Image:*

After embedding a message into a cover image is known as a stego image.

12) *AES:*

AES is use for encryption and decryption of data and image.

13) *BPCS:*

BPCS is use to embed the confidential data into the image.

14) *Encrypted Stego Image:*

The process of hiding the message in the image, so that the presence of message itself is hidden in that image

B. *Receiver Side:*

The receiver first decrypts the image with the help of decryption key to extract encrypted data from the image. After words receiver has to perform destego operation to separate image and encrypted data after that receiver get the original data with the help of the decryption key.

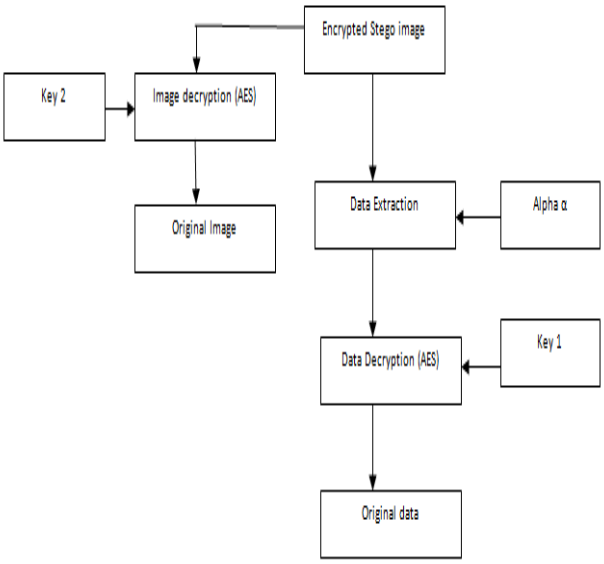


Fig. 2: Receiver Side process

On the receiver side:

1) *Key:*

A piece of information used to encode or decode massage.

2) *Image Decryption:*

The user will browse the image from computer and decrypt the image using AES algorithm and secret key.

3) *Data extraction:*

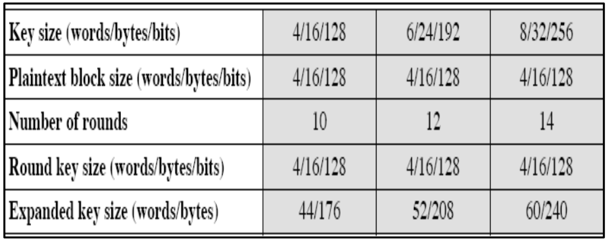
It is the act of retrieving data from image.

4) *Decrypted Data:*

The original data is retrieved using AES algorithm and to retrieve the data the user must know the decryption key.

C. *Encryption and Decryption Algorithm:*

AES is symmetric block cipher. Following figure shows overall construction of AES. The input for the encryption and decryption algorithm is 128. This block is depicted as a square matrix of bytes this block is copied into state array, which is modified at each stage of encryption or decryption. [22] After the last stage, state is copied to an output matrix. Similarly the 128 bit key is depicted as a square matrix of bytes. This key is then extended into an array of key schedule words, the total key schedule is 44 words and each word is four bytes for the 128 bit key.



Key size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext block size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of rounds	10	12	14
Round key size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded key size (words/bytes)	44/176	52/208	60/240

Following figure shows overall construction of AES. The input for the encryption and decryption algorithm is 128 bit block. This block is depicted as a square matrix of bytes this block is copied into state array, which is modified at each stage of encryption or decryption. After the last stage, state is copied to an output matrix.

Similarly the 128 bit key is depicted as a square matrix of bytes. This key is then extended into an array of key schedule words, the total key schedule is 44 words and each word is four bytes for the 128 bit key as shown in fig 3.2.

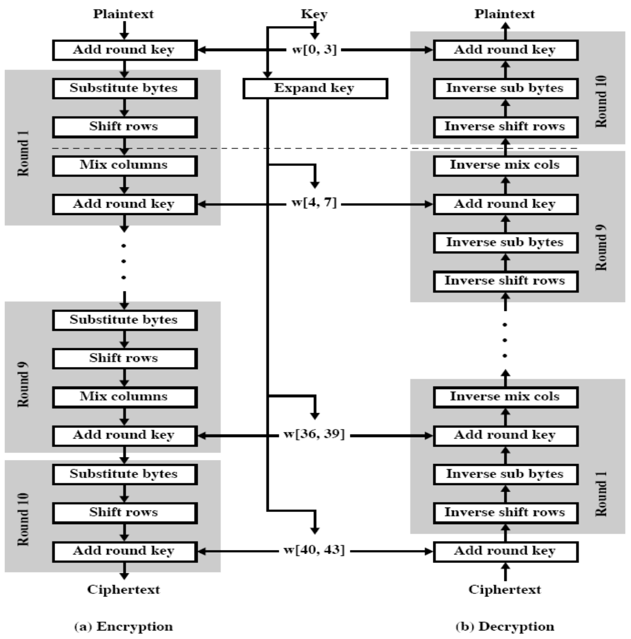


Fig. 3: AES encryption and decryption

Four different stages are used, one permutation and three of substitution

D. *The Main Loop of AES Performs Following Functions:*

- SubBytes()
- ShiftRows()
- MixColumns()
- AddRoundKey()

1) Substitute bytes:

It is a non-linear substitution step in which each byte is replaced with another according to a lookup table.

2) Shift Rows:

It is a transposition step in which the last three rows of the state are shifted cyclically in a certain number of steps.

3) MixColumns:

It is a mixing operation which operates on the columns then state combines the four bytes in each column.

4) AddRoundKey:

Each bytes of the state is combined with a block of the round key using the bitwise XOR.

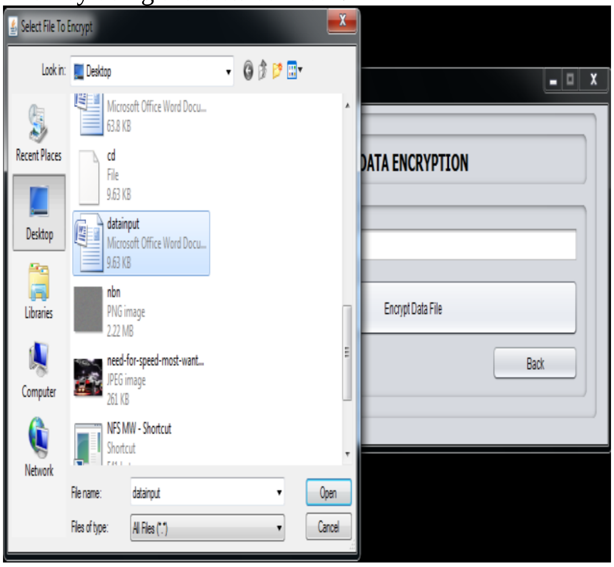


Fig. 4: AES Encryption Module

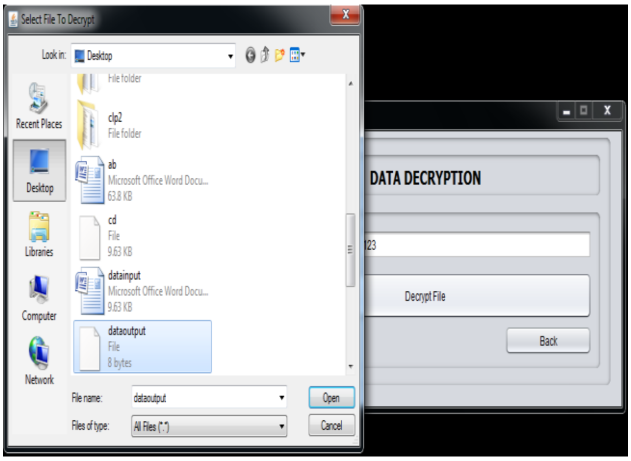


Fig. 5: AES Decryption Module.

E. *Embedding Algorithm:*

The BPCS (Bit Plane Complexity Segmentation) technique is to embed data into bitmap files. The ultimate goal is to embed as much data as possible into a image without detection by human observation statistical analysis [12]. BPCS has a large information hiding capacity. BPCS steganography addressed the embedding limit by working to mask the visual artifacts that are produced by the steganographic process. The human vision system is very good at spotting anomalies in areas of similar color, but less adept at seeing them in visually intricate areas. When an image is decomposed into bit-planes, the complexity of each region can be measured[16]. Areas of low complexity such as homogenous color or simple shapes appear as uniform areas with very few changes between the 1 and 0.complex areas such as a picture of a forest would appear as noise-like regions with many changes between 1 and 0.these random seeming regions in each bit-plane can then be replaced with hidden data, which is ideally also noise-like since it is difficult for the human eye to distinguish differences between the noise-like areas, we are able to mask the changes to the image[19].

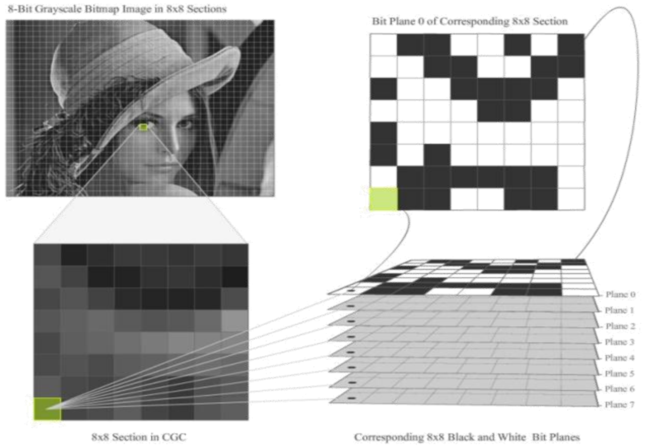

8-Bit Grayscale Bitmap Image in 8x8 Sections
Bit Plane 0 of Corresponding 8x8 Section
Plane 0
Plane 1
Plane 2
Plane 3
Plane 4
Plane 5
Plane 6
Plane 7
8x8 Section in CGC
Corresponding 8x8 Black and White Bit Planes

Fig. 6: Bit Plane Diagram.

A usual procedure for data hiding in BPCS steganography is summarized as follows

1) Segment each bit-plane of a dummy image into small size. for example 8*8, block. Then classify these blocks into informative and noise-like blocks using a threshold of complexity denoted by $\alpha_{0.}$A typical value of α_0 is $0.3_{\alpha\max,}$ where $\alpha_{\max}$ is the maximum possible complexity value.

2) Segment a secret block file into a series of block each containing 8 bytes of data. These blocks (which we call secret blocks) are regarded as 8*8 binary
3) If a secret block is less complex than the threshold α_0, conjugate it to make it more composite. Here the process called conjugation, which guarantees that any secret data can be embedded, is the exclusive OR operation with a check board pattern.
4) Replace each noise-like block in the bit planes with the block of secret data. If the block is conjugated, then record this fact in conjugation map.
5) Also embed the conjugation map in the same way as the secret block

The decoding procedure for extracting the embedded secret data is just the reverse of the embedding procedure.

In the decoding process, the complexity threshold α_0 and the amount of secret data need to be known. The amount of secret data can be embedded into a specific place in the dummy file.

F. Experimental Design/Implementation:

We have been implemented our system in NetBeans 7.4 software. The personal laptop used in all programs and experiments was Intel CORE i3 at 2.27GHz, with 4GB of RAM and 500 GB of hard disc capacity. The performance of this algorithm is evaluated based on parameters such as memory required and simulation time.

G. Evaluation Parameters:

Each of the encryption technique has their own pros and cons points. To apply an appropriate technique in a particular application we are required to know these pros and cons points.

H. Memory Required for Implementation:

Different techniques require different memory size for implementation. This memory requirement depends on the number of operations to be done by the algorithm. It is desirable that the memory required should be as small as possible.

I. Simulation Time:

The time required by the algorithm for processing completely a particular length of data is called the simulation time. It depends on the processor speed, complexity of the algorithm etc. The smallest value of simulation time is desired.

IV. RESULT

A. Comparison Of AES With Other Technique:

Factor	**AES**	**3DES**	**RC2**	**BLOWFISH**
Key	single	Single	Public	Public
Possible Keys	2^{128},2^{192}, 2^{256}	2^{112},2^{168}	2^{64},2^{128}	2^{32}
Security	secure	Inadequate	Vulunerable	Vulunerable
Developed in	2000	1978	1987	1993
Block size	128,192, 256 bits	64 bits	64 bits	64 bits
Key Length	128,192, 256 bits	168bits	64,128bits	448 bits
Cryptanalysis Resitance	Strong	Vulunerable	Vulunerable	Vulunerable

Table 1: Comparison of AES with other technique

V. CONCLUSION AND FUTURE SCOPE

This project helps to construct secure file preventing any unauthorized party access and security level of data is increased by encrypting data and by using BPCS algorithm we are able to hide large amount of data in small size image.

The experimental result shows that it is not possible to consistently detect the presence of secret message embedded in color image using BPCS technique. The reliability of inserting the message into the image depends on selection of threshold. In bit-plane, we can replace complex regions with secret information without changing image quality.

In future we can use audio and video instead of image to embed secret data.

REFERENCES

[1] Parag Kadam Mangesh Nawale, “Separable Reversible Encrypted Data Hiding in Encrypted Image Using AES algorithm an Lossy Technique” Proceedings of the 2013 International Conference on PRIME February 21-22.

[2] X. Zhang, “Separable Reversible Data Hiding in Encrypted Image”IEEE Trans. Inform. Forensics Security, vol. 7, no. 2, pp. 826-832, April 2012.

[3] X. Zhang, “Reversible Data Hiding Encrypted Image” IEEE signals processing letters, vol. 18, no. 4, pp. 255-258, April 2011.

[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] Eiji Kawaguchi and Richard O. EasonPrinciple andApplications of BPCS-SteganographyKyushu Institute of Technology, Kitakyushu, Japan – University of Maine,Orono, Maine.

[6] Lalit Dhande, Priya Khune, Vinod Deore, Dnyaneshwar Gawade,” Hide Inside-Separable Reversible Data Hiding in Encrypted Image” International Journal of Innovative Technology and Exploring Engineering IJITEE ISSN: 2278-3075, Volume-3, Issue-9, February 2014.

[7] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inform. Forensics Security, vol. 6, no.1, pp. 53-58, Feb. 2011.

[8] Hioki Hirohisa, A Data Embedding method using BPCS principle with new Complexity measures.

[9] Eiji Kawaguchi, Richard O. Eason: Principle and applications of BPCS – Steganography.

[10] R.PoornimaandR.J.Iswarya,”AnoverviewofDigitalimage steganography”International Journal of Computer Science & Engineering Survey IJCSES Vol.4, No.1, February 2013.

[11] Ms. Hemlata Sharma,Ms. MithleshArya, Mr. Dinesh Goyal Adnan M. Shihab, Raghad K. Mohammed, and Woud M. Abed,"Evaluating the perfomace of the secure block permutation image steganography algorithm "International Journal of Network Security & Its Applications IJNSA, Vol.5, No.5, September 2013.

[12] Samer Atawneh, Putra Sumari,"Imperceptible image-based steganographic scheme using Bit-Plane Complexity Segmentation BPCS" International Journal of Advances in Image Processing Techniques– IJIPT.

[13] Ms. Hemlata Sharma,Ms. MithleshArya, Mr. Dinesh Goyal,"Secure Image Hiding Algorithm using Cryptography and Steganography"IOSR Journal of Computer Engineering IOSR-JCE.

[14] Ms. Pradnya R. Rudramath, Prof. M. R. Madki,"High Capacity Data Embedding Technique Using Improved BPCS Steganography" International Journal of Scientific and Research Publications, Volume 2, Issue 7, July 2012.

[15] Jayeeta Majumder,Sweta Mangal,"An Overview of Image Steganography using LSB Technique"National Conference on Advances in Computer Science and Applications with International Journal of Computer Applications NCACSA 2012.

[16] Vinit K Agham, Tareek M Pattewar,"Separable reversible data hiding technique based on rgb-lsb method" International Journal of Research in Advent Technology IJRAT

[17] Deepthi Barbara Nickolasa, Sindhuja.Ba, Sivasankar. A," Enhancement of Data Hiding Process in Encrypted Image Using Advanced Encryption Standard" International Journal of Current Engineering and Technology2013.

[18] Pramendra Kumar, Vijay Kumar Sharma, "Information Security Based on Steganography & Cryptography Techniques: A Review",International Journal of Advanced Research in Computer Science and Software Engineering 2014.

[19] Pranita P. Khairnar, Prof. V. S. Ubale,"Steganography Using BPCS technology", Research Inventy: International Journal of Engineering and Science Vol.3, Issue 2 May 2013

[20] Suguna, Logesh Kumar, Lavanya,"Lossy Image Compression and Data Embedded In Compressed Encrypted Image"International Journal of Engineering and Advanced Technology IJEAT 2013.

[21] Debiprasad Bandyopadhyay, Kousik Dasgupta, J. K.Mandal,ParamarthaDutta,"AnovelsecureimageSteganographymethodbasedonChaostheoryinspatialdomain"International Journal of Security, Privacy and Trust Management IJSPTM Vol 3, No 1, February 2014.

[22] Divyani UdayKumar Singh, Kasturi Mohan Padwal, Madhura Pundlik Jadhav,"Separable Reversible Data Hiding in Image Using Advanced Encryption Standard with Fake Data Generation "Divyani UdayKumar Singh et al, / IJCSIT International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3469-3473.

[23] Atallah M. Al-Shatnawi,"A New Method in Image Steganography with Improved Image Quality" Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907 – 3915.

[24] Sarita, Kamlesh Lakhwani, shilpa choudhary, "An Improved BPCS Image Steganography In Integer Wavelet Transform Domain Using 4x4 Block Size "International Journal of Engineering Research & Technology IJERT2012.

[25] Harvinder Singh, Anuj kumar, Prateek Bansal,"Analysis and Implementation ofAlgorithm to Hide Secret Message"International Journal of Advanced Research in Computer Science and Software Engineering.2013

IJSRD