ISSN:2320-0790

An International Journal of Advanced Computer Technology

Separable Encrypted Data Embedding in Encrypted Image with Large Data Embedding Capacity

Supriya S. Sonawane[1], Prof. N. M. Shahane[2]

[1]Department of Computer Engineering, KKWIEER, Nasik, University of Pune, Maharashtra, India.
[2]Associate Professor, Dept. of Computer Engineering, KKWIEER, Nasik, University of Pune, Maharashtra, India.

Abstract: This paper proposes a novel scheme of separable encrypted data embedding in encrypted image with large data embedding capacity. An image encrypts using cryptography algorithm and secret data encrypts using hybrid cryptography. Then, the encrypted secret data can be successfully embedded in the encrypted cover image using Modified BPCS steganography. An encrypted image containing encrypted data is sent. At the receiver side, with an encrypted image containing embedded encrypted data, if a receiver has the data hiding key and data encryption key then he is only able to extract the encrypted and encrypted data is decrypted by data encryption key. If the receiver has an image encryption key then he can decrypt the image and get an image similar to the original one. If the receiver has the image encryption key also data-hiding key then he is able to recover the original image but extract the encrypted data. If the receiver has the image encryption key, data-hiding key, and data encryption key then he can recovered the image and extract the encrypted data after that encrypted data is decrypted to obtain a data similar to original data without any error. Separation activity is achieved according to available key/keys. A large data can embed data by using Modified BPCS steganography.

Keywords: BPCS (Bit Plane Complexity Segmentation); Data Embedding; Hybrid cryptography; Image recovery.

I. INTRODUCTION

In the current era, the internet is the prime medium to transfer information from one end to another across the world. The secret data can be stolen in many ways this is the main problem with sending information over the internet. It is very important to overcome the serious threats for secured data transmission.

Cryptography and data hiding are the most usually used techniques for improving the data security. In the cryptography, data encryption converts data into the encrypted form at sender side and data decryption converts encrypted data into original form of the data at receiver side. Data hiding is the technique in that secret information is hidden into another cover image. Image containing secret information seems same as cover image.

This paper introduced a new method of separable encrypted data hiding in encrypted images. At the sender side, first carrier image is encrypted by cryptography algorithm using image encryption key and secret data is encrypted by hybrid cryptography using data encryption key. Hybrid cryptography is taking advantages of RSA and AES algorithm. Then, encrypted data is embedding in the encrypted image using BPCS algorithm. An encrypted image containing encrypted data is sent. At receiver side there are different cases depending on available keys to obtain original data and recovered image.

II. RELATED WORK

A number of techniques are developed for compressing/decompressing encrypted data. Traditionally to transmit redundant data over bandwidth constrained channel then first compress it and then encrypt it. First encrypting a data and then compressing it with a lossless manner and the compressor does not have knowledge of the encryption key is developed in [1]. To compress encrypted images by resolution progressive compression with a lossless manner is presented in [2] and advantages are better coding efficiency also less computational complexity. The encrypted image is compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform using lossy compression method. The higher the compression ratio and the better the quality of the reconstructed image are developed in [3]. A buyer-seller watermarking protocol that is the concept of digital watermarking [4] are developed in data hiding in encrypted field. Several techniques are presented in field of reversible data hiding.

Least significant bit (LSB) insertion is a easy to embed data in a cover media [5] where the 8th bit of every byte of the original image can replace with by one bit of the secret data which we want to hide. The LSB is changed from 0 to 1 or vice versa. The file size is not usually increase in LSB method that is advantage. Disadvantage of LSB method is low data hiding capacity. A reversible data embedding using a difference expansion that is lossless data embedding is developed in [6]. The features of this method are the visual quality of embedded images along with a low computational complexity and the payload capacity limit. Encrypted data is embedded into the image in 6th, 7th, and 8th bit locations of the darkest and brightest pixels that is a hybrid approach of steganography is presented in [7]. The largest difference value between the other three pixels close to the target pixel is estimated how many secret bits will be embedded into the pixel are presented in pixel-value differencing [8].

A non-separable reversible data hiding in encrypted image is developed in [9]. A content owner encrypts the image using an image encryption key and a data-hider embeds additional data into the encrypted image using a data hiding key. Encrypted image containing data is sent. A receiver decrypts it by using an image encryption key and then extracts the hidden data and recovers the original image using the data-hiding key. A following Fig.1 shows non-separable reversible data hiding in encrypted image. In this method image decryption is not separable from data extraction. If receiver has the data hiding key but not the image encryption key then he cannot extract any information from the encrypted image containing additional.

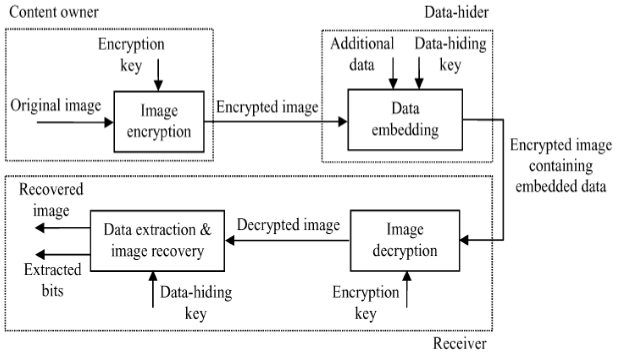


Fig.1. Non-separable reversible data hiding schema.

A separable reversible data hiding in encrypted image is introduced by Zhang [10]. Content owner encrypts the carrier image using an encryption key and a data hider embeds secret data into the encrypted image using a data hiding key. A data hider is compressed the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data.

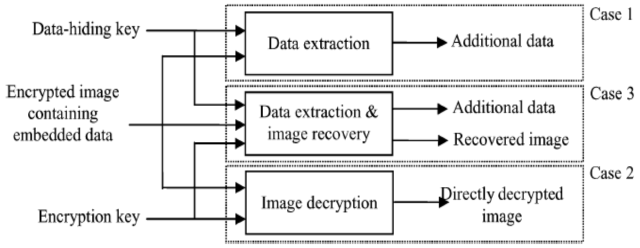


Fig. 2. Three cases at receiver side of the separable scheme

An encrypted image containing additional data is sent. The three cases at the receiver side are shown in Fig. 2. In first case, if the receiver has the data hiding key and encrypted image containing embedded additional data then he is able to extract the additional data but he does not get the recovered image. In second case, if receiver has the encryption key and encrypted image containing embedded additional data then he is able to decrypt the image which is similar to the original image but does not extract the embedded additional data. In third case, if the receiver has both the keys that are data-hiding key and encryption key also encrypted image containing additional data, he can extract the additional data and recover the original image without any error by exploiting the spatial correlation in natural image. But disadvantage of this method is the embedding capacity of additional data is not too large.

III. DETAILS OF DISSERTATION WORK

A. *Process Block Diagram*

A separable encrypted data hiding in encrypted image is proposed a novel approach. The separable activities are extraction of cover image and extraction of embedded data. This separation is done according to keys. Receiver side, there are different cases of separation to get data and image. Block diagram of the separable encrypted data embedding in encrypted image system is shown in Fig.3.

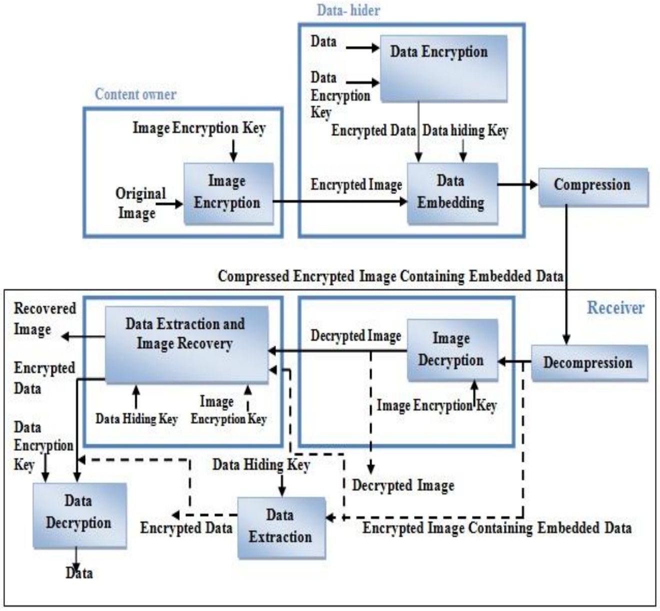


Fig. 3. Block diagram of separable data embedding in encrypted image system.

In this proposed system, at the sender side, first an original image is encrypted using an image encryption key by content owner. Then a secret data is encrypted using a data encryption key. After that the data hider embeds encrypted data into the encrypted image using a data-hiding key without knowledge of data. An encrypted image containing embedded encrypted data is compressed. Compressed encrypted image containing encrypted data is sent by sender to receiver. At the receiver side, first decompress the compressed encrypted image containing encrypted data. With encrypted image containing embedded encrypted data there are number of cases according to available keys to receiver.

- If he has only the image encryption key then he is able to decrypt the received image which is similar to the original image. But he cannot extract the embedded encrypted data.
- If the receiver has the data hiding key and data encryption key then he is able to extract the embedded encrypted data and encrypted data is decrypted by using data encryption key, so that he gets the data that is similar to original data embedded by sender successfully but he cannot know the original image.
- If the receiver has both the image encryption key and the data hiding key then he is able to recover the original image without any error and extract the encrypted data which was embedded but this data is in encrypted form.
- If the receiver has image encryption key, data encryption key and, data hiding key then he can recover the original image and extract the encrypted data after that the encrypted data is decrypted by using data encryption key so he will get the data which is similar to original data successfully.
- If the receiver has only the data hiding key then he is able to extract the embedded data but which is in encrypted form. So data cannot be in readable form also he does not know the image content. So that this case is not taken in consideration.

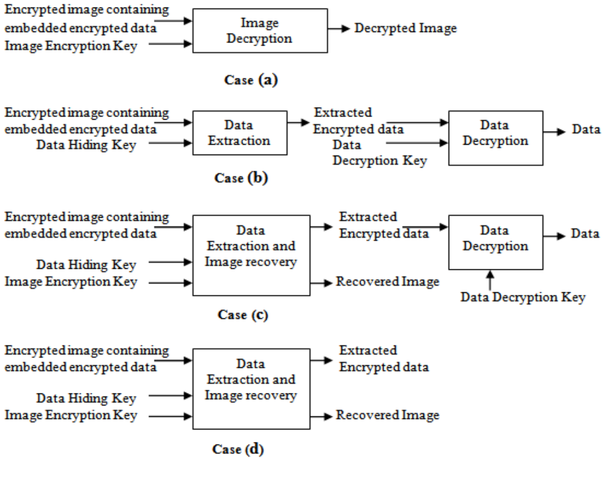


Fig.4. Four cases at receiver side of the separable scheme

Four of cases according to available key/keys at receiver side are shown in Fig. 4. If receiver has decrypted image containing encrypted data then he can extract the encrypted data using data hiding key and after that encrypted data is decrypted using data encryption key so get the original data which was embedded.

The proposed scheme is made up of different phases like image encryption, data encryption, image decryption, data embedding, data-extraction/image-recovery, data decryption, compression, and decompression. Original cover image is encrypted by using AES algorithm and data which we want to embed is encrypted by using RSA+AES algorithm. Encrypted data is embedded in an encrypted image using modified BPCS steganography.

1. Image Encryption/ Data Encryption: The sender encrypts the original uncompressed image using an AES image encryption key to get an encrypted image. Nowadays hybrid cryptography is new research area. Hybrid cryptography is getting by combining symmetric and asymmetric cryptography. Data which want to embed is encrypted by using hybrid cryptography. Sender encrypts data using AES data encryption key to get an encrypted data. Then AES data encryption key is encrypted by using RSA key and RSA algorithm. RSA is used public key for encryption and privet key for decryption of message because of RSA algorithm is the asymmetric key cryptography. This algorithm is quite simple. AES (Rijndeal) is symmetric key cryptography. Rijendeal supports the plain text block size 128 bits and key size should be 128bits. AES is used same key for both encryption and decryption of data/image. The minimum 10 rounds (when key size 128 bits and plain text block size 128 bits) in AES algorithm.

The speed of AES is faster than RSA when encrypting when data/image size is large. RSA is only suitable for encrypting a small amount of data. In RSA algorithm can distribute encryption key openly and keep the decryption keys secret but AES algorithm requires distributing a secret key before communication is more difficult. Also AES need to generate and keep a different key for different communication objects so RSA is better than AES. To give the advantages of both the algorithms by comparing AES algorithm and RSA algorithms form a new algorithm AES and RSA hybrid encryption algorithm. Hybrid encryption algorithm is produced more secure image/data. The entire hybrid encryption process is as: (assuming that the sender and receiver know RSA public key).

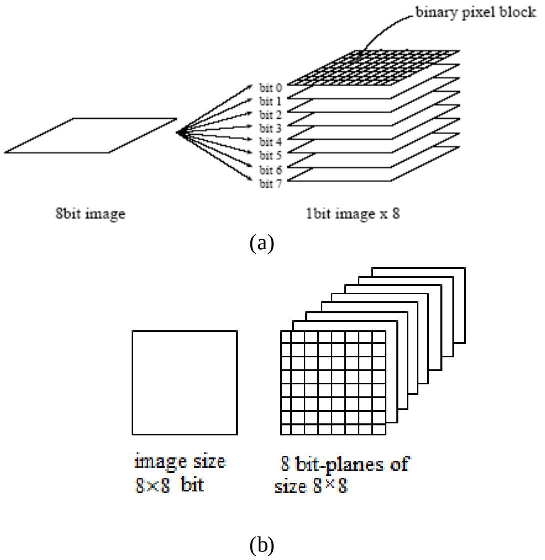
Image/data are encrypted with the help of a standard symmetric key AES algorithm and using 128-bit key which is one-time symmetric key means it is used once and then discarded. Output of this produces cipher text. Symmetric key of AES used for data encryption is encrypted by receiver’s public key using RSA algorithm. Encrypted image using AES algorithm and AES key is sent to the next block for data embedding. Encrypted AES key from RSA encryption algorithm and encrypted data from AES encryption algorithm together puts in digital envelope which is sent to next module of data embedding.

2. Image Decryption/ Data Decryption: After extracting data, receiver gets two things encrypted AES key from RSA algorithm and cipher text from AES encryption algorithm. Receiver first using its own private key and RSA decryption algorithm decrypts AES key. So now receiver gets one time symmetric key. Using this symmetric key and same AES symmetric key algorithm which was used by sender, receiver encrypts cipher text and gets original data. Under the data transmission will be more secure using dual protection of AES algorithm and RSA algorithm.

If receiver has AES image encryption key then he can decrypt the image by using AES algorithm and gets image similar to original one.

3. Data embedding: Modified BPCS (Bit Plane Complexity Segmentation) technique is used to embed encrypted data in encrypted image [11]. The goal of the system is to embed encrypted data as much as possible into an image also balance the quality of stego image. Therefore, this system is proposed an efficient hiding method to embed large number of encrypted data.

In BPCS, An image is consisting of bit-planes. Every bit-plane is divided into small square binary pixel blocks which are shown in Fig. 5(a). Encrypted data which is secret information is embedding in a binary pixel block if a binary pixel block has a complex black-and-white pattern which is noisy region.



(a)

(b)

Fig. 5. (a) Binary pixel blocks on bit-planes [11], (b) block of 8×8 bit image and its 8 planes

The flowchart of BPCS steganography is explained which is shown in Fig. 6.

1. The container image is divided into 24(8R, 8G, 8B) different Bit Planes. Bit-plane blocks are formed by dividing each bit-plane into small blocks of the same size as 8 × 8 bits. Fig 6(b) shows block of 8× 8 bit image and 8 bit-planes of size 8 × 8.

2. Calculate the complexity α of every binary pixel block. The complexity is calculated as the amount of all adjacent that get different values (one pixel is 0 and other is 1).

3. This method uses the more complex regions of an image to embed encrypted data. Assign the complexity threshold of the bit-plane block is max *minAlpha* (It is customize parameter).

α = (total length of black-and-white border in the image) /
(The max. possible B–W changes in the image) (1)

Where α is image complexity parameter. And range of α value is $0 \le \alpha \le 1$

Calculate image complexity α over the whole image. α can be used for a local image complexity of 8 × 8 pixel size area. If complexity of the bit-plane block is greater than *minAlpha* (threshold) then it is used to embed secret information. The more secret data can be embedded if the *minAlpha* is smaller. Bit-plane has a smaller complexity value than threshold is informative plane. Noisy plane is a plane which has bit-plane more complexity value than threshold.

4. Secret data is embedded into bit-plane blocks. If bit plane block's complexity is greater than *minAlpha* then the bit-plane block can replace the original one directly. But if the embedded block complexity is less than *minAlpha* then it wants to conjugate processing with the white checkerboard pattern block and take this conjugate processing block replaces the original image block.

5. Create a record of the conjugate processing blocks. This record information is also embedded into the carrier image.

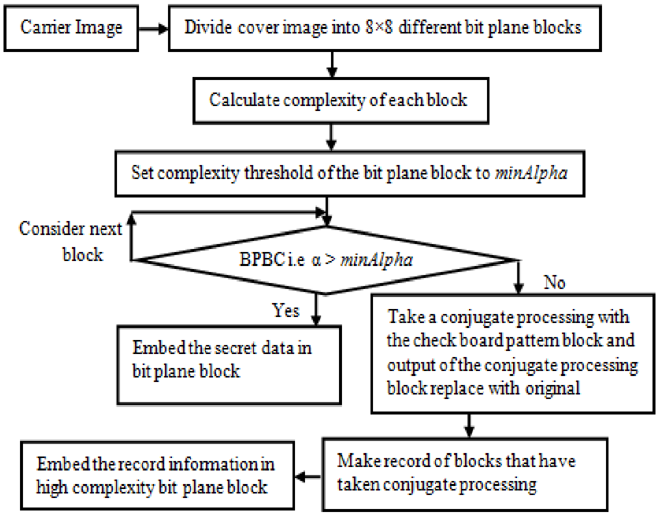

Carrier Image
Divide cover image into 8×8 different bit plane blocks
Calculate complexity of each block
Set complexity threshold of the bit plane block to minAlpha
Consider next block
BPBC i.e α > minAlpha
Yes
No
Embed the secret data in bit plane block
Take a conjugate processing with the check board pattern block and output of the conjugate processing block replace with original
Make record of blocks that have taken conjugate processing
Embed the record information in high complexity bit plane block

Fig. 6. Modified BPCS Steganography Flowchart.

The basic BPCS steganography is used bit 0th, 1st, 2nd, and 3rd. Modified BPCS method is used for bit 4, 5, 6, and 7. Consider a change in complexity from original 8×8 block of image to same stego image block indicates new value called as *gamma*. Calculate *alpha* for 4th, 5th, 6th, and 7th bit planes of image and if α is greater than *minAlpha* then generate the bit pattern to be embedded from secret data and recalculate α of the generated bit pattern. If *alpha* is smaller than *minAlpha* then take stego image and complex conjugate as par previous algorithm. Calculate change in bit pattern of modified image blocks from original image blocks that is *gamma* value. If this *gamma* value is less than *minGamma* then embed encrypted data in that calculated 8×8 blocks. If *gamma* value of the block is greater than *minGamma* then avoid that block for hiding purpose and consider next block. Use first two bits of block, which indicates whether the conjugated bit pattern or a hidden valid data. Apply this method for entire image and increase the size of image by embedding data. Therefore, the BPCS design has good visual imperceptibility and large data embedding capacity.

4. Compression/ Decompression: Encrypted image containing embedded encrypted data is compressed before transferring to receiver. Compression method is applied for reducing the redundancy of data due to this it's reduced the communication costs on conditional bandwidth. PNG method is used for the lossless image compression so that there is no loss of data after compression. The original data is to be perfectly reconstructed from the compressed data. The output of PNG compression is compressed encrypted image containing encrypted compressed data sent to receiver.

Decompression is exact inverses of compression. Receiver decompressed it and get encrypted image containing encrypted compressed data which is exactly similar to earlier one. Redundant data is added during decompression phase.

5. Data extraction/ Image Recovery: The secret data extraction is a simple process. Initially, take all the pieces of the original data whose complexity is greater than *minAlpha* and then take the extra-embedded data to confirm the blocks that have taken conjugate processing which mentioned in step (5) of data embedding phase. To get the recovery of conjugate processing block of data for that these blocks have to take XOR operation with white chessboard block.

B. Mathematical Model

Mathematical model of the proposed system -
Consider, S = {I, IEK, D, DEK, DHK, EI, ED, EID, CEID, DI, RI}
I: Original Image, IEK: Encryption Key, D: Data, DEK: Data Encryption Key, DHK: Data Hiding Key, EI: Encrypted Image, ED: Encrypted Data, EID: Encrypted image containing embedded encrypted data, CEID: Compressed encrypted image containing embedded data, DI: Decrypted image, RI: Recovered Image.
Functions:
F_1- It is a function is used to encrypt an image.
F_2- It is a function is used to encrypt a data.
F_3- This function will embed encrypted data into encrypted image.
F_4- It is a function is used for compression of encrypted image containing embedded encrypted data.
F_5- It is a function is used for decompression of encrypted image containing embedded encrypted data.
F_6- It is a function used to decrypt an image.
F_7- It is a function used to data extraction and Image recovery.
F_8- It is a function used to decrypt a data.
F_9- It is a function used for data extraction.
F_{10}- It is a function used to directly data extraction and image recovery.
This proposed system includes functions that are given below:
1. Function F1 returns an encrypted image.
F1 (I, IEK) → {EI}
2. Function F2 returns an encrypted data.
F2 (D, DEK) → {ED}
3. Function F3 returns an encrypted image containing embedded encrypted data.
F3 (EI, ED, DHK) → {EID}
4. Function 4 returns the compressed encrypted image containing embedded encrypted data.
F4 (EID) → {CEID}
5. Function 5 will decompress the compressed encrypted image containing embedded encrypted data and returns encrypted image containing embedded encrypted data.
F5 (CEID) → {EID}
6. Function 6 returns decrypted image.
F6 (EID, IEK) → {DI}
7. Function 7 returns the extracted encrypted data and recovered image.
F7 (DI, DHK, IEK) → {ED, RI}
8. Function 8 returns the data which is similar to original data.
F8 (ED, DEK) → {D}
9. Function 9 returns the encrypted data.
F9 (EID, DHK) → {ED}
10. Function 10 returns the extracted encrypted data and recovered image.
F10 (EID, DHK, IEK) → {ED, RI}
Fig.7 shows functional dependency between above functions.

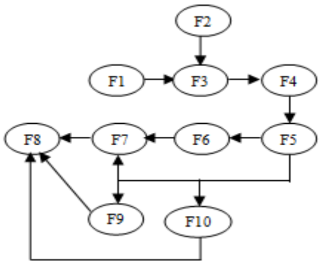


Fig. 7. Function dependency graph

IV. Result and Discussion

The proposed system will give us better results. In proposed system large data can be embedded using BPCS. Hybrid cryptography is stronger technique for encryption and decryption. Result at receiver side will get according to available key/keys. Data embedding capacity of BPCS steganography is too large. The data embedding capacity of image is 50% to 60% using BPCS steganography. Fig.8 (a) shows original image whereas Fig.8 (b) shows its encrypted version using AES algorithm and Fig.8(c) shows encrypted image containing embedded data. Result at receiver side retrieval of data and an image after decryption is shown in Fig.8 (d).

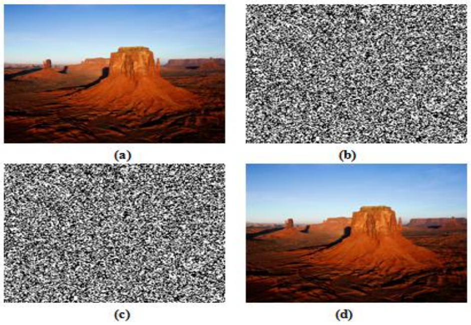


Fig.8. (a) original image, (b) its encrypted version, (c) encrypted image containing embedded data, and (d) after decryption

To check the quality of image to check the quality of image quality index is used [12]. Image Quality Assessment Techniques are also used to measure quality of image [13]. PSNR is used to compare reconstruction results of image. Here signal means original image and noise is error in reconstruction.

$$PSNR = 10 \times \log_{10}(\max_I^2 / MSE) db \qquad (2)$$

Where, $\max_I$ = 255 for grayscale images, the mean squared error (MSE) is difference between original to reconstructed image pixels and defined as:

$$MSE = (1/MN) \times \sum_M^{i=1} \sum_N^{j=1} (|C_I(i,j) - S_I(i,j)|) \qquad (3)$$

Where, M represents the number of horizontal pixels, N represents the number of vertical pixels, C is a cover image, and S is a stego image. The greater the PSNR and lower MSE is the better for image.

V. Conclusion and Future Scope

Hybrid Cryptography and Modified BPCS steganography are used which are more powerful techniques. AES algorithm is used for image encryption and decryption. AES is more secured algorithm. Hybrid cryptography is used RSA and AES algorithm for data which is more secured. Modified BPCS steganography is used to hide a data. The degradation in image quality is not visible to normal human eye. Sender can decide data hiding capacity as well as quality of the image because of the threshold of the bit-plane block is customized. Improved BPCS steganography has a large data embedding capacity. Intruder is not viable to steal the data because of these powerful security techniques.

A novel scheme for separable encrypted data hiding in encrypted image is proposed in this paper. Original image encrypted using an image encryption key. Data is encrypted using data encryption key. A data-hider is embedded an encrypted data in the encrypted image using a data-hiding key. Encrypted image containing encrypted data is compressed. At receiver side first decompressed it and get encrypted image containing encrypted data. Receiver will get the output according to available key/keys. Future scope of this system is hiding encrypted data in video.

References

[1] 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.

[2] 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.

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

[4] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," IEEE Trans. Image Process, vol. 10, no. 4, pp. 643–649, Apr. 2001.

[5] M. S. Sutaone, M.V. Khandare, "Image Based Steganography Using LSB Insertion Technique", Wireless, Mobile and Multimedia Networks, IET International Conference, pp-146 – 151, Jan-2008.

[6] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[7] Gandharba Swain, Saroj Kumar Lenka, "A Hybrid Approach to Steganography Embedding at Darkest and Brightest Pixels", Proceedings of the International Conference on Communication and Computational Intelligence – 2010, pp.529-534, Dec. 2010.

[8] Han-ling Zhange, Guang-zhi GENG, Cai-qiongXiong, "Image Steganography using Pixel-Value Differencing", Second International Symposium on Electronic Commerce and Security, pp-109 – 112,2009.

[9] X. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

[10] Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image," IEEE Trans. on Inform. Forensics and Security, vol. 7, no. 2, Apr. 2012.

[11] S. Bansod, V. Mane, L. Ragha, "Modified BPCS steganography using Hybrid Cryptography for Improving Data embedding Capacity," International Conference on Communication, Information & Computing Technology (ICCICT) Mumbai, India, Oct. 19-20, 2012.

[12] Z. Wang and A. C. Bovik, "A universal image quality index," IEEE Signal Process. Lett., vol. 9, no. 1, pp. 81–84, Jan. 2002.

[13] Nisha, S. Kumar, "Image Quality Assessment Techniques," IJARCSSE, Vol. 3, Issue 7, Jul 2013.