Secure and Separable Data Hiding in Encrypted images with TCP Steganography

Prof.Minal Zope, Akash Aalane, Pooja Baviskar, Snehal Gaikwad, Punam Sarode

Department of Computer Engineering

AISSM"S Institute of Information Technology, Pune-01

Savitribai Phule Pune University

Abstract - All previous methods embed data by reversibly vacating room from the encrypted images, which may be result into some errors on data extraction and/or image restoration. In proposed project, We do Secure and Separable data hiding into encrypted images with TCP Steganography. The purpose of Separation is to transfer data and images without lossing of original cover of image Separately as per requirement. In order to this, we are following technique that is Reversible Data Hiding (RDH). RDH is mainly used for the medical imagery, military imagery and low forensics in that the original image should not distort. For this Purpose, We are going to implement the main two algorithms- Advanced Encryption Standard (AES) and Bit Plane Complexity Segmentation (BPCS). These Two algorithms requires TCP/IP Header for key passing and for transmission of respective data and image. AES is used for the data encryption and Image Encryption & BPCS is used to increase the payload capacity and embed encrypted data into the images also transmission of image. In the BPCS algorithm we used one more technique that is gamma for controlling Quality of Image, which helps to recover image near to 100%.By combining these modules, We are achieving the phenomenon result that user can extract the image and data separately which is transmitted over untrusted network with TCP Steganography.

Keywords: Encryption of Image and data; data hiding and Extraction of data and image; LSB technique, AES algorithm, BPCS Algorithm and TCP/IP header

I. INTRODUCTION

This paper introduces the separable reversible data hiding in encrypted images with the help of Advanced Encryption Standard(AES) Algorithm, BPCS(Bit Plane Complexity Segmentation) Algorithm and TCP/IP header. Reversibility is the characteristic that the method can recover exactly the original host signal (without any distortion) upon extraction of the embedded information. For that reason, reversible (lossless) data hiding is widely used on sensitive imagery. So In proposed method we implemented reversibility for extraction of image and data separately. Cryptography is used to convert the plain text data to cipher text to provide data security. The algorithms used for cryptography come under the Advanced Encryption Standard. To provide more security to the data, the concept of steganography is used, which helps to hide the encrypted data behind any image.

In proposed system, Sender transmit image and data when he is properly logged in to the system. The receiver on the other hand, authenticates himself and downloads these files, using the keys provided by the sender in TCP Packets and obtain Data and image present in email separately. If the user is not properly authenticated then he is not allowed to get the original data. Advanced security is provided by the system along with safe transmission of data over Untrusted Network. AES algorithm and LSB techniques are used in the system for data encryption and hiding data behind image respectively. For embedding data into image with high payload capacity, BPCS(Bit plane complexity segmentation) Algorithm is used. Gamma Technique is used for controlling quality of image.

This work also relates the areas of network protocols and security for data hiding in communication networks employing TCP/IP. There are different technique of key passing, also different attacks are present which is related to key passing technique. Attack is totally depend upon how the data is send over the network. Example man in the middle attack, dictionary attack etc, this attack is related to key passing concept. so we are use this technique i.e. key passing using TCP/IP header, which provide high security. This technique uses the generation of fourth-order chaotic system to generate chaos sequence which is used to encrypt secret message, and then embeds the encrypted message into IP identification field. It compared with Ahsa's scheme, this technique is providing higher security than previous technique.

II. SYSTEM MODEL

Figure 1. Shows System Model. In Proposed System Model, There is Sender and Receiver. Sender sends image and data in particular file. System applies bit plane separation on it and analysis of payload capacity is done. Data is encrypted using AES algorithm. Encrypted data is get embed into image by using Bit Plane Complexity Segmentation Algorithm. BPCS with gamma is used for LSB 0 and 1 for controlling quality of image. Then this Steganographed Image is encrypted using AES algorithm for achieving Image Encryption. And this embedded data is transferred through email on the TCP network. TCP network handles Keys for image, data in the form of TCP Packets providing high security for Keys. Receiver receives Encrypted Image and Decrypt image and data using AES algorithm separately.

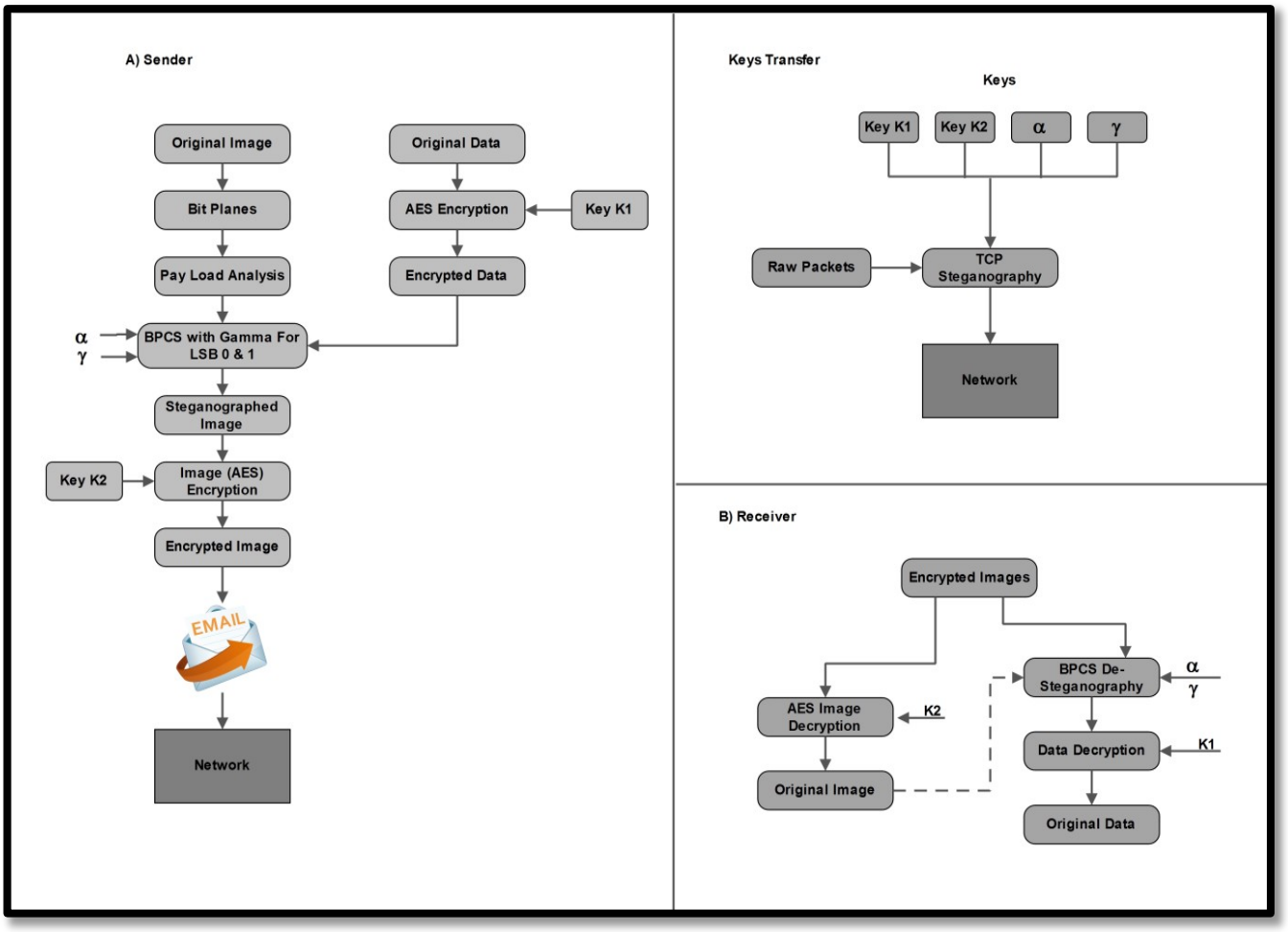


Figure 1. Proposed System Architecture

III. PREVIOUS WORK

In previous methods of RDH, Senders were doing image encryption by using image encryption key before reserving the room to hide data. Then after reserving room user can embed data into images. User reserve the room without any loss after encrypting the image. User then embed data in vacant space and send to the receiver by using Data hiding key. At receiver side user then extract data and image separately by using data hiding key and image encryption key. Since the user vacant some space without any loss from encrypted images. It is very hard and sometimes it is not able to work satisfactorily as referenced from [1].Following previous methods will give image with less quality. So we improves the previous method that we reserve some space before encrypting image so as RDH works efficient in nature and it's easier to embed data into images.

In theoretical point of view, kalker and willems [2]

developed a rate distortion model for RDH though which they proved the rate distortion bounds of RDH. In Practical point of view Rate distortion model is not efficient. So many techniques were developed. Hence J. Fredrich and M.Goljan [3] had developed general working model for RDH. The general working model was based on compression model. This techniques had drawbacks so more popular technique DE (Difference expansion)[4] had developed. In DE, difference between each pixel is expanded by adding or multiplying some value. Hence the LSBs of differences are all zero. and on that bits the data can embed. Another very popular technique to reserve the room is HS (i.e. Histogram shift) [5].In HS, Space in images reserved by shifting the bits of histogram of gray values.

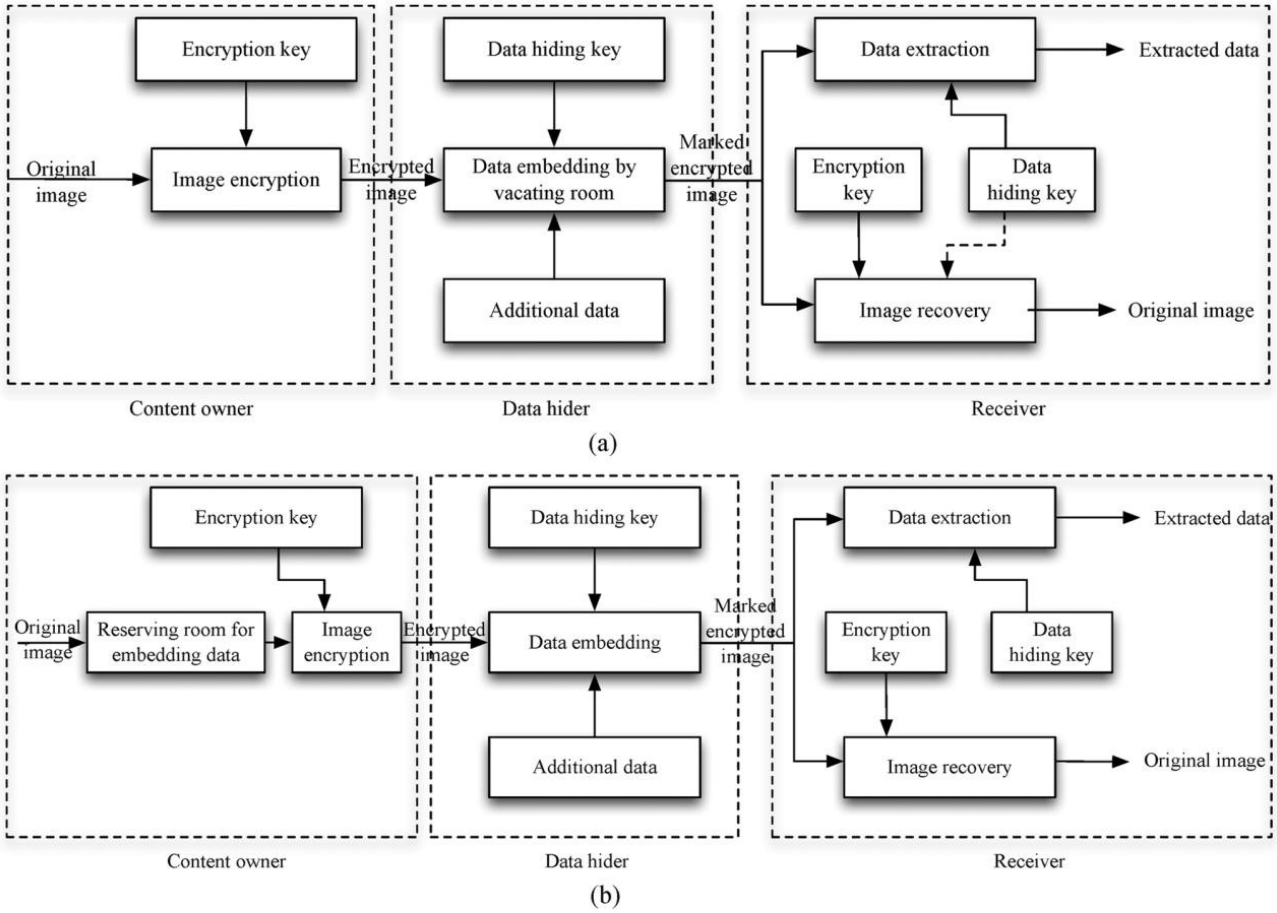


Figure. 2.Architecture: “vacating room after encryption (VRAE)” versus framework: “reserving room before encryption (RRBE).” (Dashed line in (a) states that the need of data hiding key in image recovery varies in different practical methods). Architecture VRAE. (b) Architecture RRBE.

The state of art methods[6]-[7] combines DE and HS to obtain better best performance. To provide privacy[8] encryption is very important .This will used for watermarking of images at that time. X. zhang in [9] divided the encrypted images into several blocks then flipping 3 LSBs of pixels in each block room can be vacated but this technique have some error rate.W.Hong[10] modified zhang‟s method by emerging special co-relation using different using different estimation. Thishong‟s method gives result of less error rate than zhang‟s method.

To obtaining separate data and image x. zhang [11] used a compression model. The method in [11] image obtain by using decompression technique. In previous methods VRAE have some drawbacks RRBE had developed[1] but also in RRBE data security is less and In [1] they are using LSB Technique which have minimum payload capacity to embed data. SoOur Proposed system we proposes the new system using AES(Advanced encryption standard) algorithm for providing high security to data and For embedding data into images BPCS(Bit plane Complexity segmentation algorithm) is used.

In BPCS, There are various techniques available such as listed below.1) Original BPCS 2) Modified BPCS 3) Improved BPCS[12].In our proposed system we are using combination modified and Improved BPCS to preserve the quality of image. Generally keys are transferred directly over untrusted network which is insecure to sender so that we are using TCP Steganography to embed keys and the data of BPCS into TCP Packet and transmit them over untrusted network.

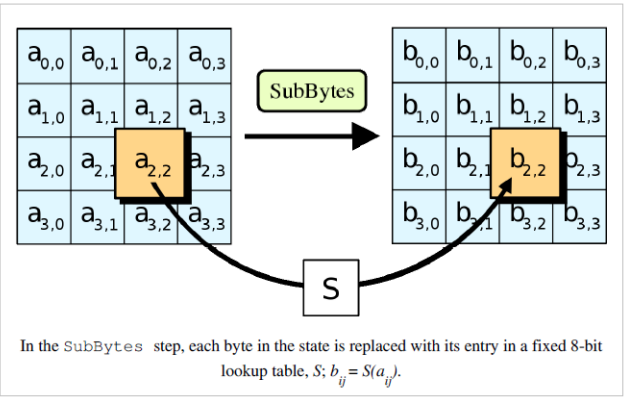
IV. PROPOSED METHODOLOGY

The proposed system implements two algorithms- 1)AES (Advanced Encryption Standard 2)BPCS(Bit plane Separation Segmentation) AES Algorithm-In our system we are using 128 bit key and in AES this is represented by Nb = 4, which reflects the number of 32-bit words (number of columns) in the State. The length of the Cipher Key K is 128. The key length is represented by Nk = 4, 6, or 8, which reflects the number of 32-bit words (number of columns) in the Cipher Key. The number of rounds to be performed during the execution of the algorithm is dependent on the key size. The number of iteration is represented by Nr, where Nr = 10 when Nk = 4, Nr = 12 when Nk = 6, and Nr = 14 when Nk = 8. For both its Cipher and Inverse Cipher, the AES algorithm uses a iteration function that is composed of four different byte-oriented transformations:

1. Substitution using a substitution table (S-box).
2. Shifting rows of the State array by different offsets
3. Mixing the data within each column of the State array
4. Adding a Round Key to the State.
5.

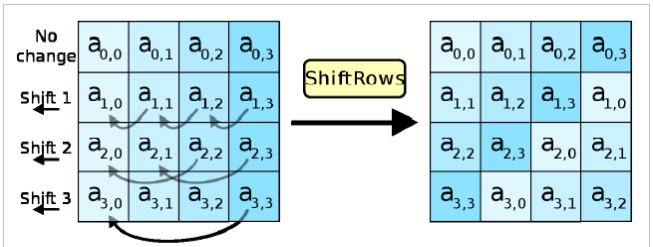
Description of AES functions are as follows:-

- SubBytes : Processing each byte through an S-Box.



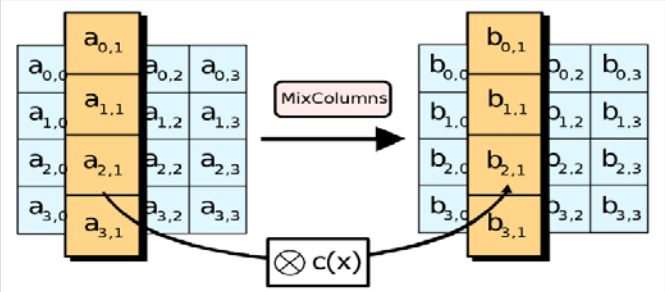
In the SubBytes step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, S; $b_{ij} = S(a_{ij})$.

- ShiftRows :The Shift Rows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset.



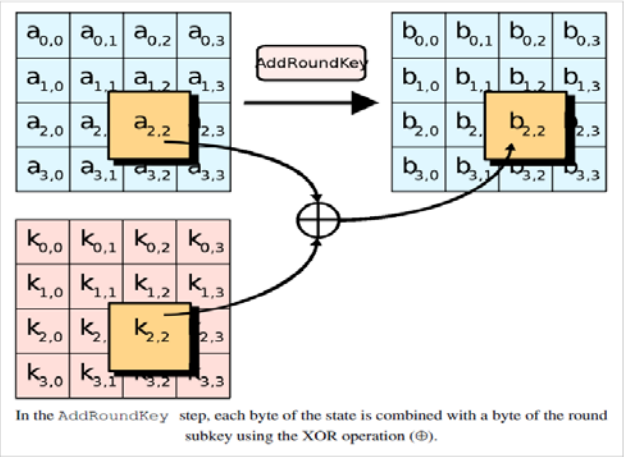
In the ShiftRows step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row.

Mix Columns: In the Mix Columns step, each column of the each state is multiplied with a fixed polynomial c(x). In the Mix Columns step, the four bytes of each Column of the state are combined using an invertible linear transformation.



In the MixColumns step, each column of the state is multiplied with a fixed polynomial $c(x)$.

- AddRoundKey : In this step, the subkey is combined with the each state. For each round, a subkey is derived from the main key using Rijndael's keys chedule; each subkey is the same size as the state.



In the AddRoundKey step, each byte of the state is combined with a byte of the round subkey using the XOR operation (⊕).

BPCS Algorithm- The BPCS is used for the image encryption for that 1st we divide the image into the bit planes. For that 1st we pick up the complex value of the every block which we divided in the 1st step. Then take a one threshold value where our image get changed that is set to the a Cmax. After that change the value of original image to the complex image. After that make a record of changed blocks which embed the extra information. In this algorithm we required one image that is more complex to hide more data into the image. Take value of complex block of image and also threshold value of complex block.

Description of BPCS functions are as follows:-

1. Divide the cover image into the 8 different small parts of same size that is bite planes.
2. Calculate the complexity of every block. Complexity means at which point the pixel value get change. The max value of complexity is denote as Cmax.
3. Set the value of complexity threshold as a c max and a is the parameter
4. Formed the secrete information into the different bit planes and replace original information with more complex image means bit planes.
5. Make the record of the blocks which are get changed and this information is embedded into the carrier it must be correctly picked up.

Figure 3 shows original Image and Figure 4. shows BPCS processing on Original Image.

Figure 3.Orginal Image

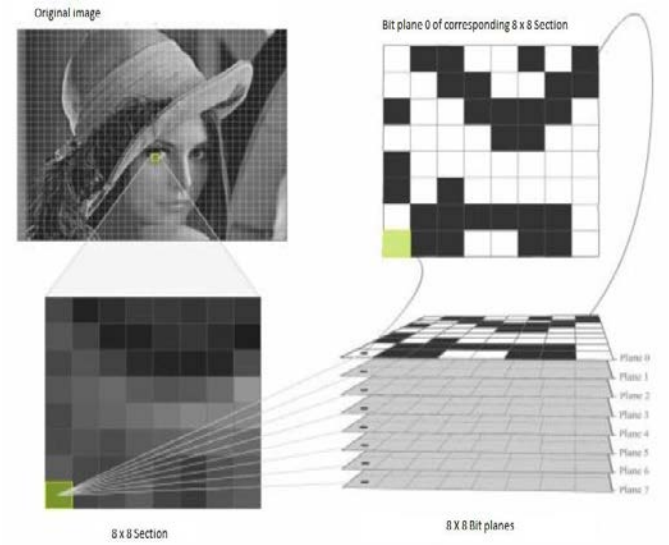


Figure 4. BPCS Processing

V. EXPERIMENTAL RESULTS

Overall, the result of steganographed image went fairly as expected. Increasing the threshold at which bit planes are determined to be complex decreased the embedding capacity, but also decreased the distortion. Embedding at full capacity (based upon the threshold) of the image including every bit plane proved to add distortion (although typically worse at lower thresholds) because the higher bit planes are visually much less tolerant to change. An interesting observation is that gray scale images had a slight advantage over the colour images in the sense that only gray scale

values could be changed as opposed to a combination of values for each colour plane. When pushed to higher limits, the gray scale images could look altered compared to the original, but still appear unaltered without comparison to the original. In colour images, when pushing the limits of threshold and capacity, noticeable colour distortions occurred that clearly indicated some kind of change to the original image.

According to simulation of AES algorithm, High speed and low RAM requirements were criteria of the AES selection process. Thus AES performs well operation on a Wide variety of hardware, from 8-bit smart cards to high-performance of computers. On a Pentium Pro, AES encryption process requires 18 clock cycles / byte, equivalent to a throughput of about 11 MiB/s for a 200 MHz processor. On a Pentium M 1.7 GHz output is about 60 MiB/s. On Intel i5/i7 CPUs supporting AES-NI instruction set extensions throughput is about 400MiB/s per thread.

VI. CONCLUSION

Our study of project concludes that RRBE (Reserving room before encryption) increased the performance data and image embedding. Also RDH recovers original cover and good visual imperceptibility. It also minimizes the PSNR which helps in enhancing security. In this paper, a novel scheme for separable reversible data hiding in encrypted image is proposed, which consists encryption of image, data embedding and data-extraction/image-recovery phases.

VII. FUTURE SCOPES

In future we can use audio, video in case of image as cover for hiding the data. In addition to this improvement, random data could be inserted in areas between valid data, especially because this technique has a higher embedding capacity. We can enhance the project by IDS (Intrusion Detection System) to detect leakage of data(for example University papers leakage).

REFERENCES

[1]. Kede Ma, Weiming Zhang, Xianfeng Zhao “Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption”, IEEE Transactions On Information Forensics And Security, Vol. 8, No. 3, March 2013

[2]. T. Kalker and F.M.Willems, “Capacity bounds and code constructions for reversible data-hiding,” in Proc. 14th Int. Conf. Digital Signal Processing(DSP2002), 2002, pp. 71–76.

[3]. J. Fridrich and M. Goljan, “Lossless data embedding for all image formats,” in Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.

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

[5]. Z. Ni, Y. Shi, N. Ansari, and S. Wei, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar.2006.

[6]. D.M. Thodi and J. J. Rodriguez, “Expansion embedding techniques for reversible watermarking,” IEEE Trans. Image Process., vol. 16, no. 3,pp. 721–730, Mar. 2007

[7]. V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, “Reversible watermarking algorithm using sorting and prediction,” IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009.

[8]. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC, 1996.

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

[10]. W. Hong, T. Chen, and H.Wu, “An improved reversible data hiding in encrypted images using side match,” IEEE Signal Process. Let., vol.19, no. 4, pp. 199–202, Apr. 2012.

[11]. X. Zhang, “Separable reversible data hiding in encrypted image,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[12]. Peipei Shi, Zhaohui Li, ”An improved BPCS Steganography based on Dynamic Threshold”2010 International Conference on Multimedia Information Networking and Security,2010.

[13]. Parag Kadam, Mangesh Navale, ”Separable Reversible Encrypted Data Hiding in Encrypted Image Using AES algorithm and Lossy Technique International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 21- 22.2014.

[14]. Miss D. D. DhobaJe,”Steganography By Hiding Data In Tcp/Ip Headers”, 20IO 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE).