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. 4, Issue. 3, March 2015, pg.396 – 405

RESEARCH ARTICLE

A Tactic for Encrypting Stego-Image Using AES and BPCS Algorithm

Shruti Gajare[1], Shiney Charles[2], Snehal Wagh[3], Vrunda Bhusari[4]

[1]Computer department & Pune University, India

[2]Computer department & Pune University, India

[3]Computer department & Pune University, India

[4]Computer department & Pune University, India

[1] shrutipgajare@gmail.com; [2] charles.shiney@gmail.com; [3] snehalwagh786@gmail.com; [4] vrundabhusari82@gmail.com

Abstract*— *In this paper, we are proposing a tactic to provide secure confidential data transmission through the internet which has revolutionized the mode of transmitting data. To achieve this we are using AES algorithm and BPCS steganography technique. The system which we are proposing will first encrypt the confidential data to be transmitted by using the AES algorithm and then this encrypted data is encapsulated into an image which acts as a cover image. For encapsulating the encrypted data into the image BPCS steganography is used which has the reputation of providing large data embedding capacity and preventing the degradation of the quality of the stego image. And now finally this stego image is encrypted by using AES algorithm thereby providing twofold protection to the confidential data and thus overcoming the shortcomings of the previous researchers. So at the sender side two keys are generated i.e. a data encryption key and an image encryption key. Now lastly at the sender side as an add-on feature the encrypted stego image is digital watermarked to protect the authenticity of the data. Now this final encrypted stego image is sent to the receiver and the receiver would be able to extort the encrypted data from the encrypted image and then would decrypt the encrypted stego image with the image encryption key. And then finally with the help of the data encryption key the receiver will decrypt the encrypted data. Hence same set of keys are used for encryption as well as for decryption and as two separate keys are used for encrypting the data and the image, the process of decryption is separable as well as reversible due to the use of AES algorithm.

Keywords*— *Cryptography, Steganography, BPCS (Bit Plane Complexity Segmentation), AES (Advanced Encryption Standard), alpha channel, Digital Watermarking , TGA(Truevision Graphics Adapter).

I. INTRODUCTION

Gaining access to internet has become the most essential part of today's digital world with the fast advancements and modifications in secure areas of research and technology. A usage of internet publically is precarious as there is no privacy. Transmission of confidential data over an internet is risky. Elucidating the complication of data security, a digital image is used to encapsulate the secret information. In today's rapidly changing digital world, the most important aspect of how to accomplish security and authentication of data and image is a very big challenge. The internet is the most crucial medium to transmit data from one point to another across the globe. The matter of concern is to overcome the drawbacks of greatly prevailing threats such as confidential data that can be stolen or hijacked by hackers leading to modification or extraction of secure information which results into misuse and unsecure confidential data transmission across the globe.

This paper acquaints us with a novel scheme of separable reversible encrypted data hiding into encrypted image using Advanced Encryption Standards (AES)[1] and Bit Plane Complexity segmentation [2].In our proposed system, on sender side we are encrypting confidential data using AES algorithm to obtain a final encrypted d1ata then we select an image which acts as a cover image in which confidential data is to be hidden[3]. After selecting the image, the next step is to extract the features from the image and then we apply the BPCS algorithm which has a reputation of having high payload capacity[4] to embed encrypted data into the carrier image[5].Then AES algorithm is applied on the stego image so as to obtain an encrypted stego-image. This stego encrypted image is watermarked to protect the integrity of confidential data. This entire mechanism takes place on sender side and then this encrypted stego-image is sent to the receiver. In this model, uses symmetric cryptography. After sending the encrypted image by email we send the keys to the receiver by means of sms or call. The sending of keys via sms or call on mobile results into separation of channel which is a merit of our system because this helps us to increase the security of the system and it results in making the system highly secure.

Now on receiver side, we receive the stego-encrypted image which is sent by the sender. Firstly we'll check whether there is any modification in the image, for this process we perform de-watermarking where we'll verify the image if it is modified or not. After successful de-watermarking, then this stego encrypted image is then split into two parts; one is data decryption and other is image decryption. The image and data are decrypted using the same AES keys which were used at the time of encryption. Hence, we get the original data as well as original image.

II. EXISTING SYSTEM

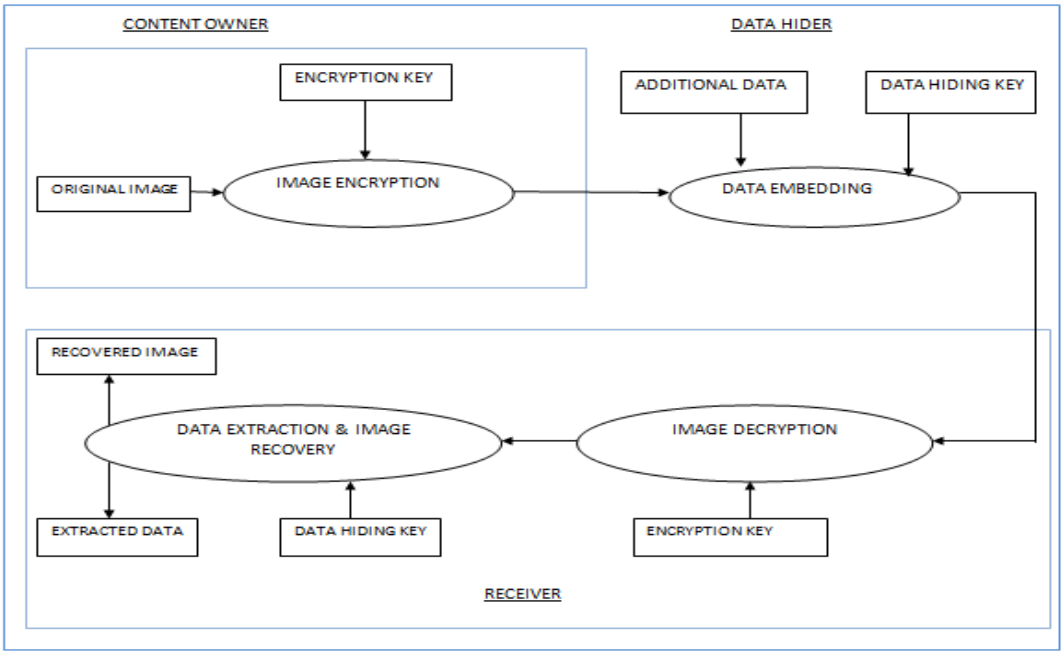

Fig. 1 Existing system

Providing safe and secure data transmission through Internet is a very vital matter and many researchers have been working on it since decades and have proposed many systems that offers secure confidential data. Various researches have proposed various techniques, one of which as illustrated in the above figure is to embed the confidential data to be securely transmitted into an image which is just an innocuous cover image and then to encrypt this stego image[6][7][8][9] . So here as the confidential data is not being encrypted this method poses a threat of losing this confidential data very easily. This limitation has led to another technique where both the confidential data as well as the cover image is encrypted. The encryption has been done with the help of AES algorithm and the confidential data has been embedded into the Least Significant Bits(LSB) of the cover image[3]. That is one bit of data is embedded into the 8th bit of each byte of the cover image. But as the data is embedded into the LSB of the cover image, it has very low data hiding capacity. So in order to increase the data hiding capacity ,in some of the system the LSB of the cover image is compressed in order to create an added space so as to embed additional data but this technique ends up distorting and degrading the quality of the cover image[3][10][11]. A very large number of works has been done in the field of non-separable data hiding in encrypted image where the process of extracting the data and decrypting the data is not separable from the process of decrypting the image[6]. There are also some systems where a digital watermark embedding protocol know as the buyer-seller watermarking protocol is used [12]. There is a reversible data hiding paper where the process of embedding or extracting the data to or from the image is done on plain spatial domain[13].

III. PROPOSED SYSTEM

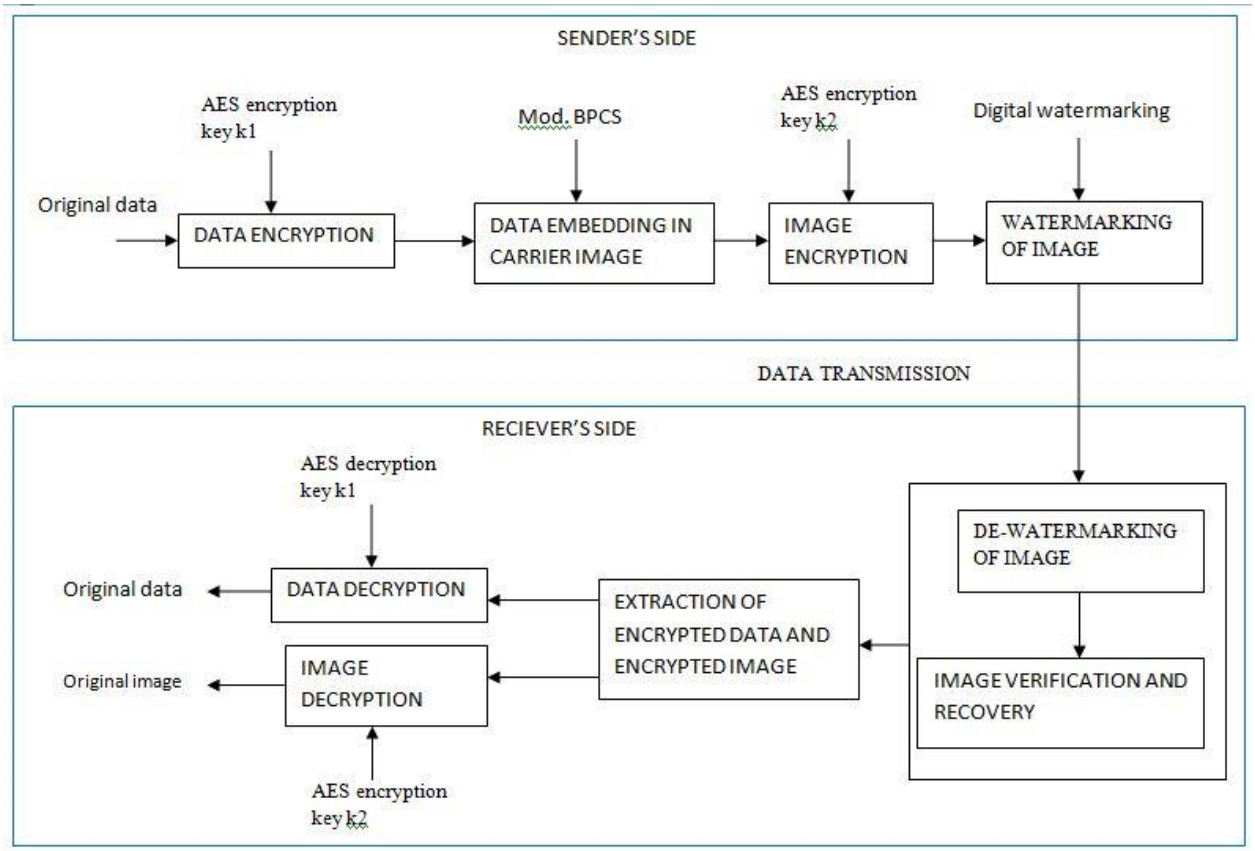

Fig. 2 System architectural diagram

This project provides us a more secure way for sending data over internet by proposing a novel scheme of separable reversible encrypted data hiding into encrypted image using Advanced Encryption Standards (AES) and Bit Plane Complexity segmentation In the proposed system on the sender side, we are encrypting image as well as the data simultaneously. On the sender side firstly we encrypt the image using AES algorithm and then we encrypt the data using AES algorithm Now this encrypted confidential data which we want to embed into the image is encapsulated using modified BPCS, as it has abundant data hiding capacity. So now we get the final stego image which is a combination of encrypted image and data. And the stego image contains confidential data which is to be transmitted over the internet. The process of embedding encrypted data into the encrypted image is known as data hiding. This final encrypted stego image is then transmitted over the internet to the receiver.

On the receiver side, the final stego image sent by the sender is then separated into encrypted image and encrypted data. The process of decryption of image and data is carried out in a reversible manner. The encrypted image obtained from the final stego image is then decrypted using AES algorithm which results in obtaining the original image. And then this original image is used for image recovery and data extraction. This extracted data is then decrypted using AES algorithm which gives us the original confidential data .

IV. IMPLEMENTATION MODULES

The implementation modules of our proposed system are as follows:

A. Data Encryption

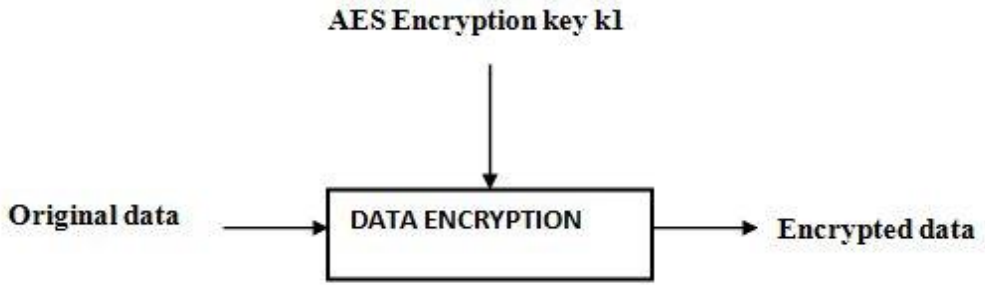

Fig. 3 Data Encryption

In this proposed system, the confidential data which we want to encapsulate is encrypted by means of cryptography. Sender firstly encrypts the data using AES algorithm which uses same key for encryption as well as decryption. AES algorithm uses 128 bits and 10 rounds to produce 128 bits cipher text. AES algorithm is ample of time faster than RSA in case of encrypting abundant amount of data and image.

B. Data Embedding

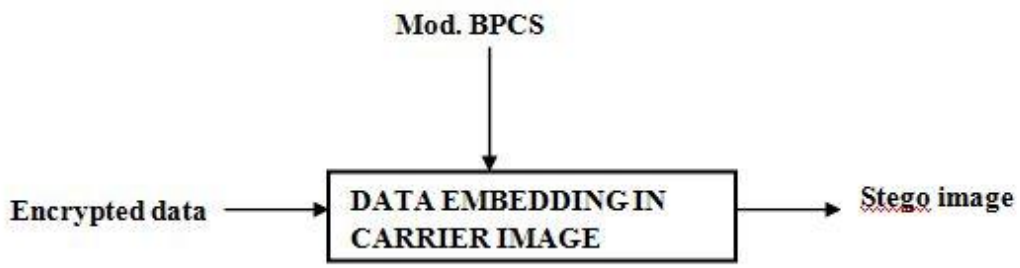

Fig. 4 Data embedding into carrier image

In order to encapsulate encrypted data in image the BPCS technique and alpha channel is used. It aims to encapsulate large encrypted data in carrier image without degrading the quality of image. The merit of using Modified BPCS is that its payload capacity of data embedding is high. The mechanism of data embedding using Modified BPCS and making use of alpha-channel to maintain and balance quality of image so as to obtain final steganography image is completely termed as Data hiding.Alpha channel is used to create the appearance of partial or full transparency by creating alpha composition which is mechanism of combining image with it background.

In Modified BPCS, An image is consisting of 24 planes which is again divided into 8R,8G,8B different bit planes. Every bit plane is divided into small square binary pixel blocks which are shown in figure below. The complexity α of each 8 bit plane is determined. The complexity is calculated by the amount of all adjacent pixels that has one black and one white pattern.

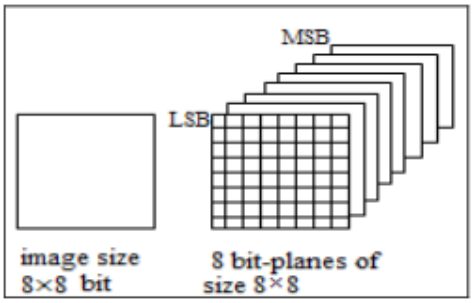

Fig. 5 Block of 8×8 bit image and its 8 planes

It uses the more complex regions of the carrier image to encapsulate encrypted data. The complexity of the bit plane is assigned to max *minalpha.*

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

The value of α range is $0 \leq \alpha \leq 1$.If the complexity of bit-plane block is greater than *minalpha* then the data is embedded into carrier image. Again the complexity of the stego image is computed to check whether it is less than or equal to the value that of *minalpha.* If it is less than it is conjugated with white chessboard pattern block and this information of each bit is recorded in 8 bit alpha plane.

C. Encryption of Image

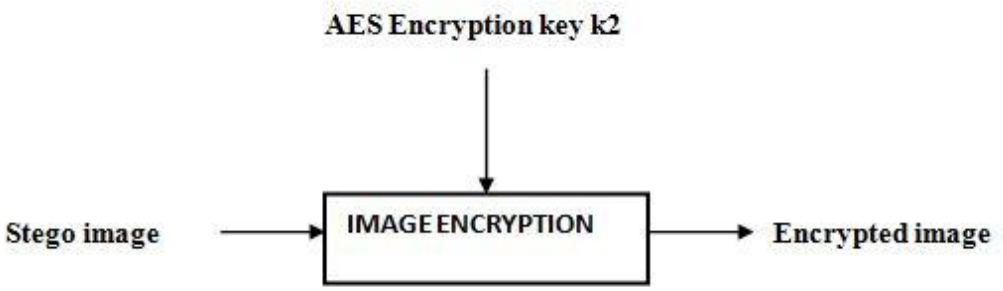

Fig. 6 Encryption of stego image

The sender encrypts the stego image using an AES algorithm and AES image encryption key to obtain encrypted image. This same key is used performing both encryption and decryption of image. The encrypted image key is then sent to data embedding block.

D. Watermarking

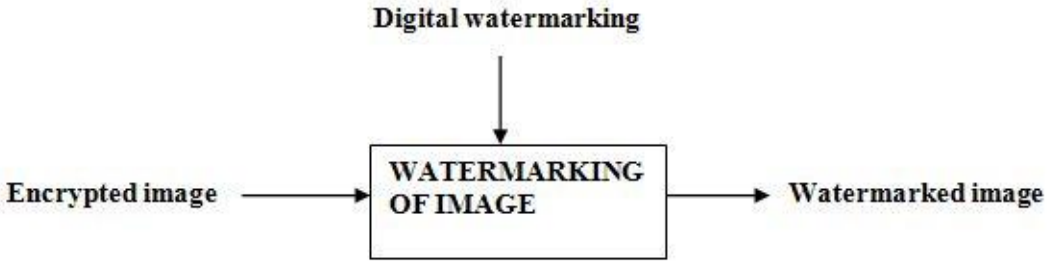

Fig. 7 Digital watermarking the stego image

In this model, digital watermarking technique is used. The major aim is to hide digital information in carrier signal. Generally, watermarking is used to crosscheck the integrity of the carrier signal. Input to this module is the stego encrypted image and the output is watermarked image which is finally sent to receiver.

E. De-watermarking

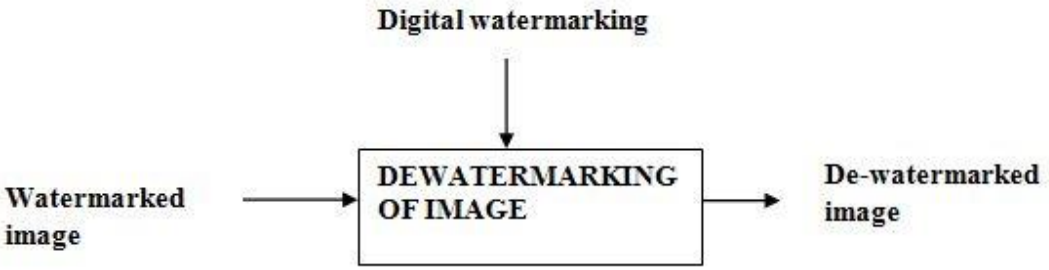

Fig. 8 De-watermarking the stego image

In this module, the water marked image is de-watermarked. It checks whether there are any changes in the watermarked image or not. If yes, then the recovery of image is performed.

F. De-steganography

Fig. 9 Extracting the encrypted data from the encrypted image

This module is used for separating the encrypted data and encrypted image from the final stego image.

G. Image decryption

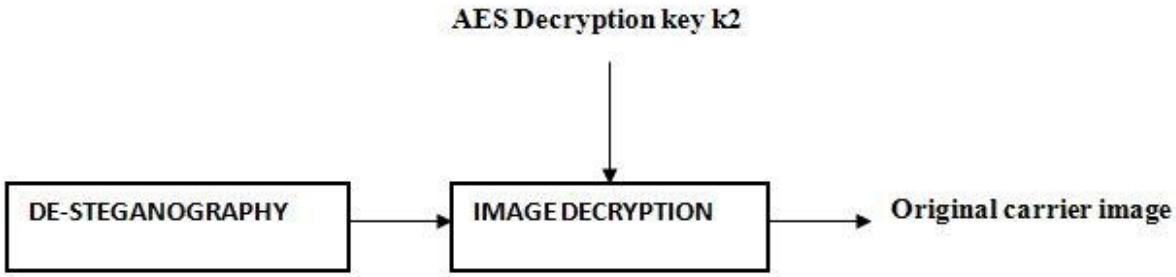

Fig. 10 Image decryption

After obtaining de- steganographic image, the receiver decrypts image by using the AES image encryption key which was used at the sender side. Finally, we obtain original image.

H. Data decryption

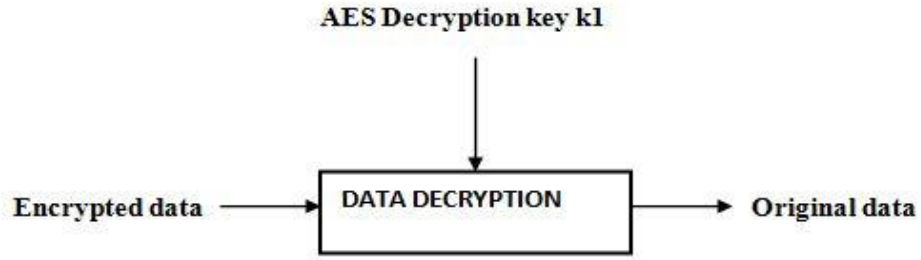

Fig. 11 Data decryption

After extracting confidential data, receiver gets two things encrypted AES key from AES algorithm and cipher text from AES encryption algorithm. Here we get encrypted data from data extraction this encrypted data then decrypted. 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 this data transmission will be more secure using protection of AES algorithm.

V. RESULT AND DISCUSSION

Modified BPCS technique is used for embedding large amount of data into image which has high payload capacity as compared to any other algorithm. As a result, large amount of data is embedded. Symmetric cryptography is used at both ends which is extremely fast method. So, the keys are distributed by another medium like by SMS or on call. Figures Fig (a) shows the original carrier image and Fig (b) shows the carrier image containing embedded data and Fig(c) shows the encrypted stego-image.

Fig (a): original carrier image

Fig (b): the carrier image containing embedded data

Fig(c): Encrypted stego- image

VI. CONCLUSION

A technique called modified BPCS algorithm and AES algorithm is used in the proposed project which takes all the advantage of the previously proposed system. In this project, modified BPCS technique allows the user to embed large amount of data in the colored image as its pay load capacity is high as compared to Gray scale image. Also, we are providing two-fold protection by encrypting data and the stego- image for secure transmission of data in the network. The colored image is taken as cover image for encapsulating encrypted data in it. In case of colored image, the various features of the image is extracted and the image is divided into three bit planes of 8R,8G and 8B planes and a total of 24 bit plane which allows us to embed 3-bits of data in one pixel of image. Using BPCS algorithm, the encrypted data is hided in the image. After encapsulation, the image is again encrypted using AES algorithm. In order to detect any modification in image, the image is watermarked and is sent to receiver. The receiver will use the exact reverse process as that used as sender side. And using the same keys that are used for encryption, the receiver will decrypt the data and image using separable reversible approach. We have implemented AES algorithm here, as this algorithm operates on block cipher, so its speed is faster and is having three different key sizes. For future implementation, we would be able to use videos in place images to embed large amount of data.

ACKNOWLEGEMENT

We would like to express our deepest appreciation to all those who provided us the possibility to complete this paper. We give a special gratitude to our final year project guide, Mrs. Vrunda Bhusari, whose contribution in stimulating suggestions and encouragement, helped us to coordinate our project especially in writing this paper.

REFERENCES

[1] Adam Berent, "Advanced Encryption Standard by Example" ,V.1.7.

[2] Eiji Kawaguchi and Richard O. Eason, "Principle and Applications of BPCS-Steganography", Kyushu Institute of Technology, Kitakyushu, Japan – University of Maine, Orono, Maine.

[3] 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.

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

[5] 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.

[6] X. Zhang, "Reversible Data Hiding in Encrypted Image," *IEEE signals processing letters*, vol. 18, no. 4, pp. 255-258, April 2011

[7] X.Zhang," Separable Reversible Data Hiding in Encrypted Image," *IEEE transactions on information Forensics and Security*, Vol.7,No.2,April 2012

[8] V.Santosh, J.Harish, R.V.K.Sumanth, N.Vijay and Dr.N.Sandhya," Separable Reversible Data Hiding In Encrypted Images," GRIET, Department of CSE,2013.

[9] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," *IEEE Trans. Inform. Forensics Security*, vol. 5, no. 1, pp. 180 187, Feb. 2010.

[10] Parag Kadam, Mangesh Nawale, Akash Kandhare and Mukesh Patil, "Separable Reversible Encrypted Data Hiding in Encrypted Image Using AES algorithm and Lossy Technique," 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME)

[11] Rini.J, " Study on Separable Reversible Data Hiding in Encrypted Images **,**" International Journal of Advancements in Research & Technology, Volume 2, Issue 12, December-2013 223 ISSN 2278-7763.

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

[13] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

