ISSN 2395-1621

Data Hiding in Color Image for Secure Data Transmission with RDHbyRRBE

Komal Khandale [#1], Mrunal Patil [#2], Rohini Tale [#3] , Hemavati Tanpure [#4]

[1]Komalkhandale@gmail.com
[2]mrunalpatil15@gmail.com
[3] talerohini@gmail.com
[4]madhuritanpure1993@gmail.com

[#1234]Department of Computer Engineering ,
Navsahyadri Education Society's Group of Institutions,
University of Pune, India

ABSTRACT

The reversible data hiding plays very important, vital role in the proposed system. The proposed method provides integrity and confidentiality for both the image as well as data. The system involves the technique called Reversible data hiding (RDH). RDH in encrypted image ensures the original image which is used to hide the message that can be recovered without loss of quality of the image which is used as cover. There cause errors on the data extraction and image extraction resulted due to previous methods. In this scheme, the reserving room before encryption with a RDH algorithm results in easiness for the data hider to reversibly embed data in the encrypted images. By RRBE method the real reversibility can be achieved, that is data extraction and image recovery are without any error. Experiments show that this novel method can embed more than 10 times lager payloads (i.e.) efficiency for the embedding data and extracting data with same image quality as the previous methods like peak sound to noise ratio dB. It is easier to modify and misuse the valuable information through hacking because of availability of such huge network. Cryptography and steganography are the two ways to sending data securely without modifications by unauthorized person. The proposed methodology deals with the image steganography with the different security aspects and about the steganographic algorithms like Least Significant Bit (LSB) algorithm, RLSB algorithm. Those algorithms are used by means of speed, correctness, accuracy and security. All previous methods only support for gray scale image so in this scheme, instead of gray scale image color image is used to hide data.

Keywords— Reversible data hiding (RDH), LSB Algorithm, Visual cryptography algorithm, encryption, privacy protection.

ARTICLE INFO

Article History

Received : 16th April, 2015

Received in revised form :

18th April, 2015

Accepted : 22nd April 2015

Published online :

14th May 2015

I. INTRODUCTION

Basically Data security means protection of data from unauthorized, illegal users or hackers and providing high level security to particular system without any modification. Now a day, the data security domain requires more and more attention due to the increase in data transfer rate over the internet. Focusing to improve the security features over the internet there are various techniques have been developed like: Steganography, Cryptography. Steganography provides more security by hiding the cipher text into apparently invisible image or any other formats, While the cryptography technique involves conversion of plain text to "cipher texts" and transmitting it to the intended receiver using an secrete key. Reversible data hiding (RDH) in images is a technique, by which the original image quality can be recovered when the embedded message is extracted. And hence the quality of original image can be maintained. Data hiding technique aims to embed some secret information into an image. In the Reversible Data Hiding technique as the name indicates, the data is embedding in reversible manner without knowing the various contents of referring image. The large error-rate found in previous method, in the process of data extraction. But In this paper, in order to decrease the error rate an improved method is presented and hence we can preserve the quality of encrypted image. The LSB is one of the well-known and best methods of steganography in which the least significant bits of each pixels of selected image are used to hide the information. The various digital evidences can be embedded by various general stenographic techniques in Least Significant Bit embedding. The

resulting cover is contrast or similar to original one as the changes are made at only least significant bit of considering pixels. And hence the hackers or unauthorized persons cannot predict that image carries the message also. Many techniques use the LSB embedding technique due to its simplicity. High level transparency is also allows in LSB technique. In this scheme encryption of image as well as data is carried out separately. In the first phase, sender encrypts the original uncompressed image by using encryption key. Then the least significant bits of the encrypted image are compressed by the content owner. So we can have the reserved space to accommodate some additional data.

II. RELATED WORK

In this framework, at sender side the content owner encrypt the original image using a standard cipher with an encryption key. The data hiding process is followed after producing the encrypted image, and hence the content owner can easily embed data in encrypted image with data hiding key. Then at the receiver end, the data which is embedded in encrypted image can be extracted by the receiver. The receiver itself maybe the data owner or an authorized third party who can extract data with the data hiding key, later original image is recovered from the encrypted version with the help of the encryption key.

The "emptying room after encryption" technique is about vacating the rooms after encryption for data embedding or hiding [2] used in existing system, one of the encryption key is used image encryption for data hiding that is embedding process. According to Advanced Encryption standard, the secret key allows the receiver to retrieve the embedded data and further recover the original image from the encrypted version. All previous schemes are known to be disadvantageous due to more error-rate on data extraction and image recovery and the data hiding process became effort full because of Emptying Room After Encryption [2]. As the previous system uses only gray scale image for data hiding, it results in restriction on image selection by user and scope of the system. The method "Emptying Room After Encryption" [2] was referred in previously implemented scheme, in this technique the compression of image takes place first and encryption performed by using the encryption key. Using the data hiding key, the data of content owner is embedded in to the image. There is a sequential process that is followed by system in which at the receiver side first receiver will extract the image using the data hiding key in order to extract the data [2]. Hence it is not a separable process.

III. PROPOSED METHOS

In the present paper, we are using the "reserve room before encryption" with RDH instead of using "reserving the room after encryption" that is RRAE. In this scheme, changing the Least Significant Bits of some pixels and then adding that into other pixels referring the basic RDH algorithm the room will be emptied out. After that the image will be encrypted, so the locations of the LSBs which are used to embed data in the same encrypted image. The excellent performance can be achieved as the proposed method does separate data extraction from image decryption. At sender side, reserving room before image encryption method is applied the RDH process in encrypted images would be much easier and more natural which leads us to the extreme framework, "reserving room before encryption (RRBE)" [1].

The emptying room after the encryption of image which used previously is not so efficient also hard and time consuming, so why we still use it. If the order of emptying room mechanism and encryption technique is reversed, that is, let reserving room done first at sender side then image encryption and then the following the process of RDH in encrypted images would be much, easier very natural which leads in new framework, i.e. "Reserving Room Before Encryption (RRBE)"[13]. The sender first reserves much space, additional space in original image and then referring encryption key image will be encrypted. The scheme involves various phases such as 1.Encryption of image, 2.data embedding, 3.data extraction and 4.image-recovery [1] [13]. To produce an encrypted image the sender encrypts the unreduced, original image with the help of an encryption key. Then, the content owner reduces only the least significant bits (LSB) of the encrypted image taking data-hiding key and the small vacant space is created to absorb the valuable data over that area. Considering the data hiding key the stored data can be extracted in vacant space from encrypted image. The data stored only at the LSB of image which can affect the original image in small proportion.

IV. METHODOLOGY

SYSTEM STRUCTURE

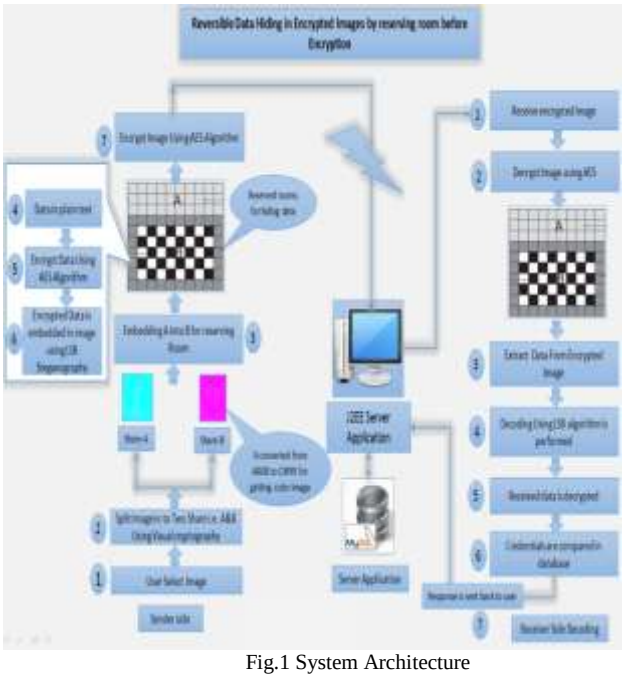

Fig.1 System Architecture

As shown in figure 1, First user have to select one image from given set of images or can browse another one. Then using visual cryptography algorithm image will be divided into two shares to reserve room for data embedding. The data is encrypted first and then embedded into desired or selected image. So the data- hider is ready to hide their data at the reserved space in image. In this way we separate the process of data encryption as well as the image encryption. It will result, to preserve and maintain the original image quality as well. The original image

quality helps for assurance of the systems reliability. the image encryption is carried out by the AES algorithm and that encrypted image is ready to transmit. At receiver side the same steps mentioned above will be followed in reverse order.

System implementation

The RRBE can be classified into three stages:

a) Generation of an encrypted image

b) Hiding the data in encrypted image

c) Data extraction and image recovery.

a. Generation of an Encrypted Image

The content owner acquires the encrypted image, he can embed data but he does not get the access to the image. Content owner first locate the encrypted version of A. after knowing how many bit-planes and pixels have to change, the data hider substitute the available bit-planes with additional data M with LSB replacement. Finally, the content owner sets the label to point out the end position of the embedding process.

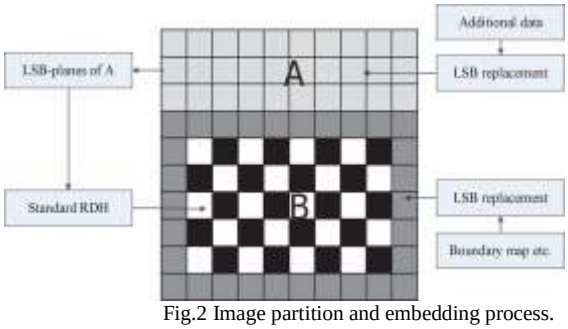

Fig.2 Image partition and embedding process.

1) Image Partition*:*

The user selected image is partitioned into two shares A and B. The visual cryptography algorithm (VCA) is used [6] to maintain color image quality , which results in a image partition.Then we have to encrypt the re-arranged image to generate its final version.

Fig.3 image partition.

Fig. 3 shows partition of original image into two parts by applying visual cryptography algorithm to maintain the image quality. Fig 4 shows the mathematical formulae to calculate the CMYK values which are needed and used for image partitioning of original image. These formulae's are used at both side sender side as well as receiver side. The range of ARGB is between 0-255 while CMYK values are in between 0 to 1.

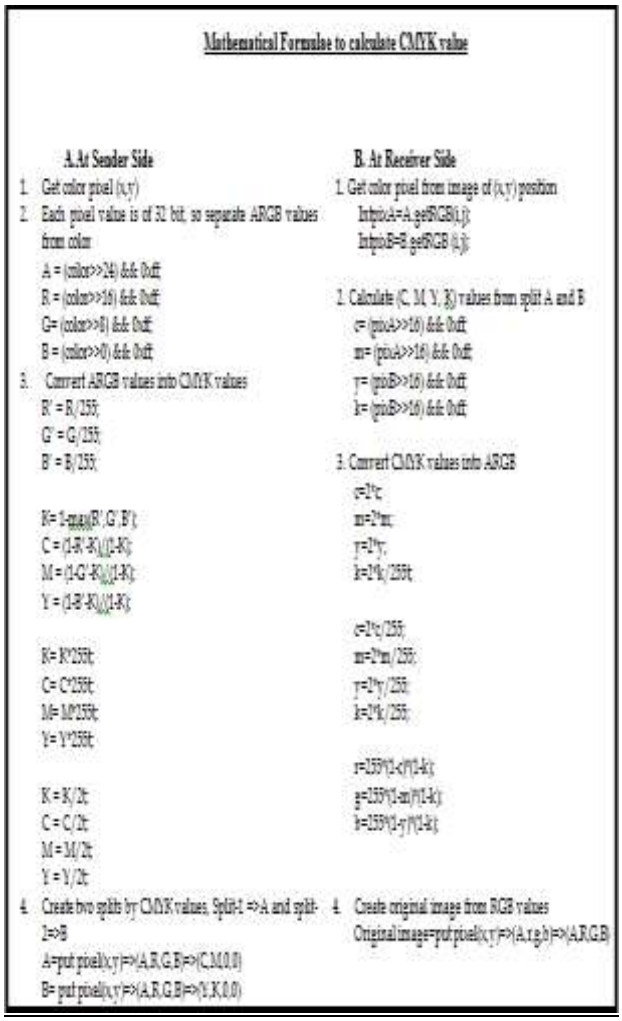

Fig.4. mathematical formulae

2) Self-Reversible Embedding*:*

T he main Moto of self-reversible embedding is to embed the LSB-planes of split A into split B by employing Reversible Data Hiding technique. In this each pixel is divided into two sets such as S1 and S2 with extra additional bits. If additional bit is 0 then three LSB's of set S1 flipped otherwise, three LSB's of set S2 will flip. To reduce replication of value 0 and 1 the boundary map comes in picture. Boundary map is used for checking pseudo boundary and natural pixels. In proposed approach Boundary map is used because its size is very critical to identify the practical applicability. For sometimes there is no need to use boundary map concept.

Fig.5 RDH by RRBE

Fig. 5 shows the image with embeding data and also encrypted form. In this scheme we are reserving room before encryption for secure data hiding while it is not possible previous system.Using this technique possiblity of image selection is increased. As the rooms are reserved before encryption the system becomes more reliable because we avoid the wastage of pixels of image.

3) Image Encryption:

After embedding data into image, the Advanced Encryption Algorithm (AES) is used to encrypt that image.

AES Encryption Algorithm:

The figure 6 shows the AES block which is used in encryption. In AES algorithm the Symmetric key are used at both side sender as well as receiver for encryption and decryption. The plain text is converted into cipher text through the cipher engine.

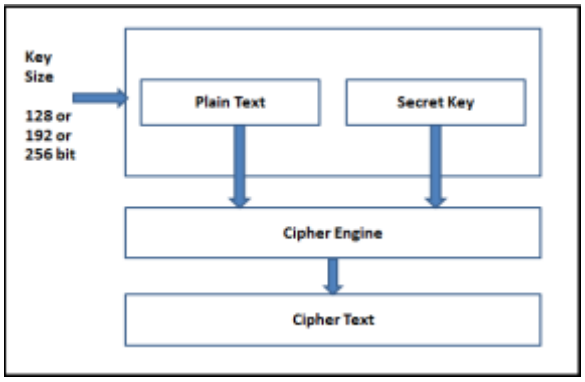

Fig 6.AES Blocks

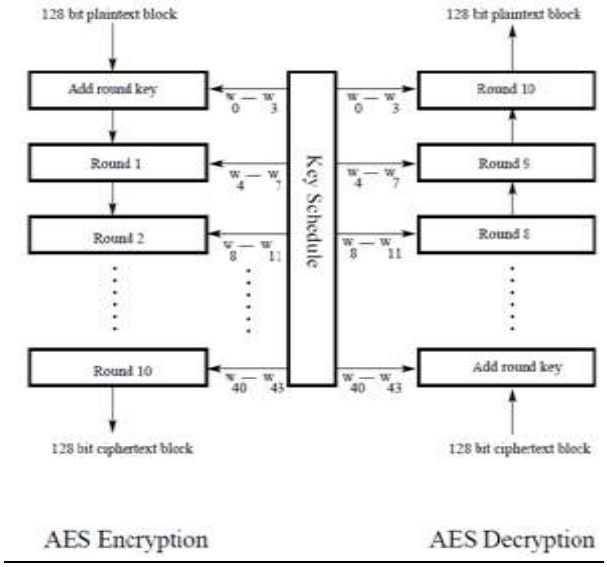

Fig. 7 AES Algorithm

The AES algorithm used for encryption and decryption of important information, for that three different key sizes are used. Also It consist into four steps such as Substitution of bytes, Shifting rows, Mixing columns, and Adding round key which is used in encryption. The XORing is done at last step. For each round above four steps are used. The number of repetitions of transformation depends on the key size used for an AES cipher and also no of rounds that modifies input specified. Hence the modified input called cipher text. At opposite side set of inverse of that rounds are carried out to transform that cipher text into the original plaintext using the same encryption key.

In Table No.1 shows the AES parameters. The AES is also called as Symmetric Encryption Algorithm. This algorithm uses a 128 bit data block and may use three different key sizes 128,192 and 256 bits. The 128 bit data block is divided into 16 bytes and is mapped into a 4*4 array called State. It is an Iterative algorithm. The total Number of rounds Nr is depends on key length Nk. Here the length is specified in "words".

Algorithm	Key Length(Nk)	Block Size(Nb)	No.of rounds Nr=Nk+6
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Table 1.Parameters of AES

AES operates on the Binary Finite Field, GF(2^8).Each byte will be represented as a polynomial of at most degree 7:

$$b_7X^7+b_6X^6+b_5X^5+b_4X^4+b_3X^3+b_2X^2+b_1X^1+b_0$$

b. Data Hiding in Encrypted Image

At sender side when sender has the encrypted image, he is able to embed useful and valuable data. Still he does not get access to the original image. Also the sender is able to modify or change how much bit-planes and rows of pixels are present there, the sender simply make replacement of LSB bit planes with additional data.

Least Significant Bit (LSB) based steganography

The common and simplest type of steganography is LSB (least significant bit) ever. Here, there is the use of only the one bit of byte for the purpose of data embedding. Let's say, we have to encode the letter A (ASCII 65 or binary 01000001) in the following block shows the 8 bytes of a carrier file.

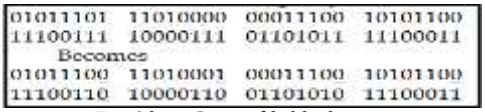

Fig. 8 byte Carrier file block

c. Data Extraction and Image Recovery

The process of data extraction is totally independent from the process of image decryption; this involves two cases for data extraction as well as image recovery.

1) Case 1: Data Retrieval From Encrypted Images:

In this case the the main task is extraction of data from encrypted image is carried out. It is necessary to consider this case on situation. First of all the data is retrieved and then image is decrypted. To update and manage the information of images which are used for encrypting the clients privacy, the data hiding key is only the way to manipulate data in encrypted domain as well[11]. Both the data embedding and data extraction are manipulated in same the domain of encryption.

2) Case 2: Data Retrieval From Decrypted Images:

In this case the data hidden in encrypted image is retrieved from original image. I.e. firstly image is decrypted and then only the data is extracted. On the other side, there is another situation that the user or the receiver has to decrypt the image first and after extracts the data from the decrypted image.

V. ADVANTAGES & APPLICATION

The system is more advantageous in order to maintain the perfect secrecy without leakage of data. This method ensures the confidential data hiding with security. In this scheme quality of image as well as data recovery is achieved. The process of data hiding becomes easier than as there is use of RRBE technique. The main Moto is to ensure user privacy by keeping the information hidden from others. The proposed system used in medical imagery, military imagery, government sector, banking sectors. This system is applicable for all applications and fields where there is a requirement of higher level of security.

VI. EXPERIMENTS & COMPARISIONS

The standard image of Lena is used to demonstrate the feasibility of proposed method as shown in Fig. 9(a). Figure 9(b) is the desired encrypted image which contains embedded messages and in fig. 9(c) illustrates the decrypted version with messages. Also the last one i.e., Fig. 9(d) represents the recovery version which is exactly similar to original image. We have compared the various methods of reversible data hiding. There may be errors introduce on data extraction or image restoration, where the proposed scheme is free of any error for all types of images. The quality of resultant decrypted images is compared in the terms of PSNR. (Peak Noise Sound Ratio).Introducing an error-correcting codes, the pure payload is maintained with error rate. The results considered with perfectly high scale of successful data extraction and significant image recovery. For all situations, from the Fig. 10, it can be observed that using any range of embedding rate, our scheme performs state of the art RDH algorithms in encrypted images. The approaches in [2],[9] can achieve comparatively low PSNR at high embedding rate, that is the gain in terms of PSNR is significantly high at embedding rate range. In addition, one more advantage of our scheme is the much wider range of embedding rate can be acceptable for PSNRs. In fact, this scheme can hide more than 10 times large payload for the same PSNR (e.g., dB), like the approaches in [2], [9], which results a very good potential for practical applications.

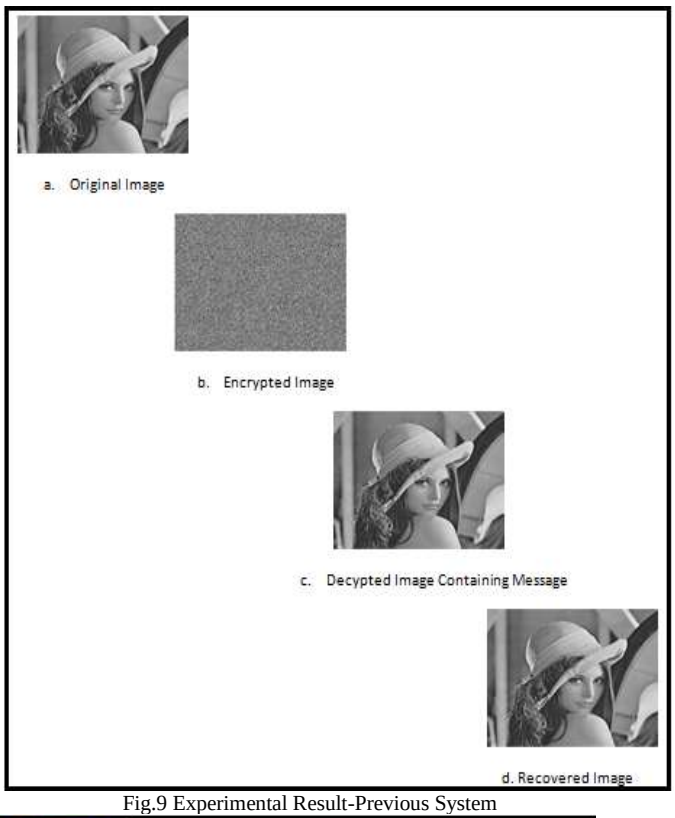

Fig.9 Experimental Result-Previous System

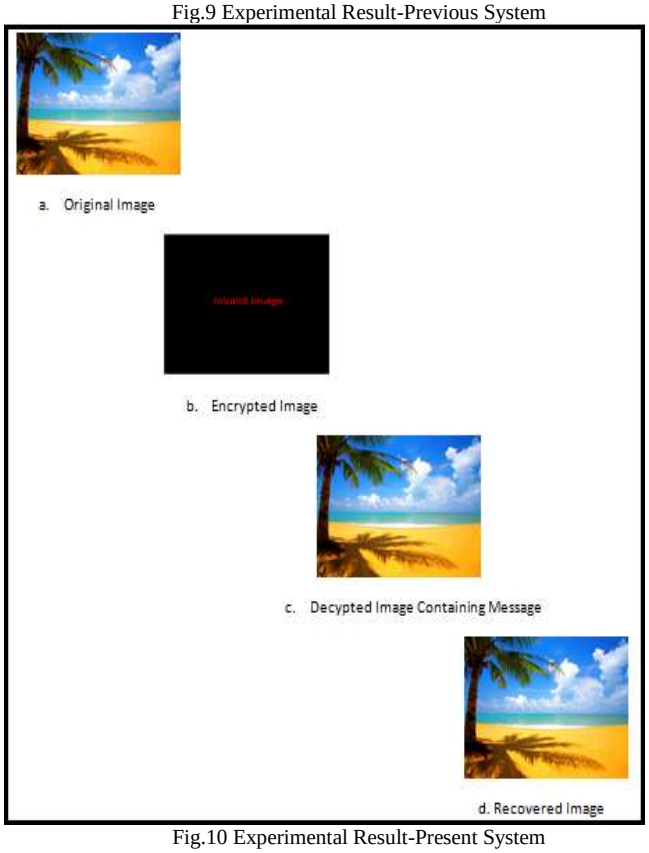

Fig.10 Experimental Result-Present System

The Figure 11 shows graphical analysis of 4 schemes, in which 3 schemes are from [9]-[11] and remained is present scheme.

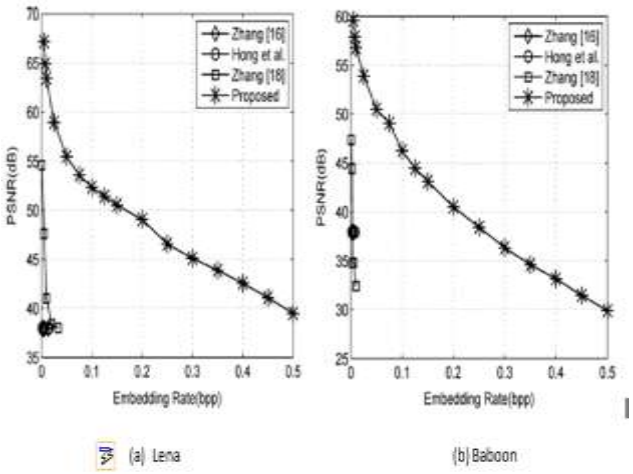

Fig. 11 PSNR comparison with the methods of Zhang [9], Hong [10], Zhang [12] and proposed system for (a) Lena and (b) Baboon

VII.CONCLUSION

Now a days due to the functionality and scalability the more trends is toward the use of web services. So that preservation of privacy becomes major issue. This scheme facilitates the requirement of privacy preservation that is security. In this scheme the space is occupied in advance before doing the encryption so the data embedding process becomes efficient and easier. The mechanism helps for private communications known as steganography. The conversion of data from original or readable form to some unreadable form or not understandable by unauthorized Person is called Encryption. This scheme is provides advantages of basic RDH technique for all color images and achieve the standard or benchmark with perfect secrecy. Further the system enables the separation of data extraction and greatly maintains the quality of image used as cover. If the receiver knows both the encryption and data hiding key, then he is capable to get the hidden data and decrypt the encrypted information, error free and get selected image with its original quality.

VIII.FUTURE SCOPE

a The method which is used for encrypted image having embedded data is lossless compression, the useful data can be still extracted and the original content can be also recovered. Since no change in the content of the encrypted image having embedded data is ensured by the lossless compression technique. Bit XOR operation is used for encryption, the lossy compression scheme is not suitable here even this method is compatible with encrypted images generated by pixel permutation. The lossy compression deserves further research in the future as it ensures a compressive combination of image encryption and data hiding. The reversible approach which is implemented can be enhanced in future by using the following provisions,

- In case of lot of change in the pixel to retain nearest to the original value, the MLSB technique can also be applied after embedding data.

- As the keys are send and received securely, and applicable in networking domain.

REFRENCES

[1] "Reversible data hiding in Encrypted Images by reserving room before Encryption", by Kede Ma, Weiming Zhang, Xianfeng Zhao, *Member, IEEE, Nenghai Yu, and Fenghua Li*, IEEE transactions on Information Forensics and Security,vol. 8,no. 3,March 2013.

[2] 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.

[3] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Signal Process, vol.* 89, pp. 1129–1143, 2009.

[4] 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.

[5] L. Luo *et al.*, "Reversible image watermarking using interpolation technique," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 187–193, Mar. 2010.

[6] Sozan Abdulla "New Visual Cryptography Algorithm For Colored Image" *JOURNAL OF COMPUTING*, vol. 2, ISSUE 4, APRIL 2010, ISSN 2151-9617.

[7] 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.

[8] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," *IEEE Internet Comput.*, vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.

[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. Lett.*, 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] T. Margaret PG Student [Embedded System], Dept of ECE, Sathyabama University, Chennai, Tamil Nadu, India "Reversible data hiding in encrypted images b XOR Ciphering techniques" IJAREEIE vol. 3, issue 2, February 2014.

[13] Komal Khandale, Mrunal Patil, Rohini Tale, and Hemavati Tanpure,"Data Hiding in Color Image for Secure Data Transmission with RDHbyRRBE", Volume 1, Issue 6, February-2015 **.**

