ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

An Efficient Data Security System by Combining Reversible and Lossless Data Hiding Schemes

Krishna Priya S*, Minu Lalitha Madhavu#

PG Scholar, Dept. of CSE, Sree Buddha College of Engineering, Pattoor, Alappuzha, Kerala, India*

Assistant Professor, Dept. of CSE, Sree Buddha College of Engineering, Pattoor, Alappuzha, Kerala, India#

ABSTRACT: The security of the data being transmitted is coming to a serious issue in today's fast moving world. Hence for providing data security, we can use any type of lossless or reversible data hiding techniques.Due to the compatibility between the lossless and reversible schemes, the data embedding operations in the two manners can be simultaneously performed in an encrypted image. So here we use a combined lossless and reversible data hiding technique so that one part of data can be extracted before image encryption and another confidential part can be extracted after encryption. In the combined scheme we use visual cryptography for image encryption to improve the efficiency of the system by reducing the time consumption. Then we use hash encryption method for lossless hiding of one part of secret data and difference expansion method for reversible hiding of next part of secret data. Thus we can embed two parts of data in a single encrypted image which provides more security to our data.

KEYWORDS: Data Hiding, Reversible Data Hiding, Lossless Data Hiding, Visual Cryptography Image encryption, Image decryption.

I. INTRODUCTION

Nowadays the data that is to be secured is transmitted by embedding it in encrypted images. This way improves the security of the data. This type of data hiding where we can achieve reversibility is called as Reversible Data Hiding. Hence the security of the cover image can be ensured. We can use this technique in situations where the security of both the transmitted data and the cover image are confidential.

The Reversible Data Hiding is a technique which is established based on both steganography & security. That is the data to be secured is embedded in an encrypted image. In the first step, the image is encrypted using any encryption technique. Then the data to be secured is embedded in that encrypted image by the sender. With an encrypted image containing the additional data, the receiver can extract the additional data if he knows the data-hiding key even though he does not know the image content. He can also decrypt the received encrypted image to recover an image similar to the original image if he knows the encryption key. If the receiver has both the data hiding and encryption keyshe can extract the additional data and also he can recover the original content which is an errorless process.

We can do the data hiding schemes in a lossless or reversible manner. The terms lossless and reversible can be distinguished differently. The data hiding method is said to be lossless if the display of cover image containing embedded data is same as that of original cover image even though the cover image have been modified for the data embedding process. On the other hand, the data hiding method is reversible if the original image content can be perfectly recovered from the encrypted image containing the embedded data even though a small distortion has been brought in the data embedding procedure.

In this paper, we combined both lossless and reversible data hiding schemes together to get a more secure and error free data hiding scheme .The process of data embedding can be done in an encrypted image using both of the schemes. But the data extraction processes in the two schemes are different. Hence by combining these two schemes we can embed two parts of data into a single coverimage. That means the different types of data for various purposes

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

may be embedded into an encrypted image, and a part of the data can be extracted before decrypting the cover image and another part can be extracted after decrypting the cover image.

II. RELATED WORKS

Reversible data hiding technique focuses on the data embedding or extraction. The main aim of this technique is the error free and separable data extraction and image recovery. Lossless data hiding focuses on the display of cover image containing embedded data which will be same as that of original cover even though the cover image have been modified for data embedding. A combination of both lossless and reversible schemes will provide security to highly confidential data so that one part of data can be extracted before encrypting the cover image and other highly confidential part can be extracted after encrypting the cover image.

A. Reversible data hiding schemes

There are a number of techniques for reversible data hiding. In all reversible data hiding techniques data embedding is performed in an encrypted domain. The reversible data hiding can be done in Encrypted JPEG Bitstream [1]. The secret message is embedded into the encrypted bitstream by slightly modifying the JPEG stream. The system identifies the usable bits for data hiding so that the encrypted bitstream carrying secret data can be correctly decoded. The encryption and embedding are based on the encryption and embedding keys respectively. Hence if a receiver has both the keys, the secret data can be extracted by analysing the blocking artifacts of the neighbouring blocks and the original bitstream can be perfectly recovered. In the case if the receiver has only the encryption key he/she can still decode the bitstream to obtain the good quality image without extracting the hidden data.

The technique of image interpolation and the detection of smooth and complex regions in the cover images provides an improved reversible data hiding scheme [2]. A binary image that represents the locations of reference pixels is constructed based on the local image activity. In complex regions, more reference pixels are chosen and thus some pixels are used for embedding the data which reduces the image degradation. In the smooth regions, less reference pixels are chosen, which increases embedding capacity. Pixels are interpolated according to the constructed binary image, and the interpolation errors obtained are then used to embed data through histogram shifting. The pixel values in the cover image are modified one gray scale unit at most to ensure that a high quality stego image can be produced.

Histogram Shifting is another technique which can be used for reversible data hiding [3]. Here the input image is divided into some number of blocks and then histogram shifting is performed on each block which enhances the data hiding capacity and visual quality. This technique mainly consists of three stages: 1) Dividing image into two blocks 2) Processing Stage and 3) Data Embedding Stage. The first stage includes dividing the image into two main blocks. Processing stage includes histogramgeneration of each block and the difference of histogram are taken after histogram modification. The proposed approach shows a binary tree structure which overcomes the drawback of communicating the multiple peak points to the receiver. Also the data embedding is done after dividing the image into blocks.

B. Lossless Data Hiding Schemes

Lossless data hiding techniques provides the cover image containing embedded data to be same as that of the original cover. There are some lossless data hiding techniques. There is a method of lossless data hiding in which a lossless compression technique for encrypted gray scale image using a method called progressive decomposition and rate-compatible punctured turbo codes [4] are used. In this method they developed resolution progressive compression, which has been shown to have much better coding capacity and less computational complexity than that of the existing approaches. This lossless compression of encrypted sources can be obtained through Slepian-Wolf coding. For the encrypted real-world sources such as images, they are trying to improve the compression efficiency. There is a resolution progressive compression scheme which compresses an encrypted image progressively in resolution, so that the decoder can be able to observe a low-resolution version of the image, study local statistics based on it, and use the statistics obtained to decode the next resolution level.

There is another lossless generalized LSB data embedding method [5], which enables the exact recovery of the original host signal upon extraction of the embedded information. A generalization of the LSB modification is proposed as the data embedding method, which introduces additional operating points on the capacity distortion curve.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Lossless recovery of the original image is achieved by compressing portions of the signal that are susceptible to embedding distortion and transmitting these compressed descriptions as a part of the embedded payload. A prediction based conditional entropy coder which utilizes unaltered portions of the host signal as side information improves the compression efficiency and thus the lossless data embedding capacity.

A high capacity lossless data embedding techniques for palette images can be done based on histogram analysis [6]. The histograms are analysed to identify the embedding capacity of different image types. Histogram maxima and minima are used in embedding capacity estimation. The data embedding and extraction is performed using simple processing operations that can save power consumptions for wireless devices. The proposed algorithm uses the indices corresponding to zero values in the histogram to repeat the most used colours. After repeating colours, the indices of the repeated colours are used to map data bits according to a predefined mapping scheme.

C. *Combined Lossless and Reversible Data Hiding Scheme*

The above two separate data hiding schemes can be incorporated to form a single scheme which can be used for embedding two parts of data in a single encrypted image. A combined lossless and reversible data hiding schemes for public key encrypted images [7] is the advanced existing scheme.In both of the two data hiding techniques in the combined scheme, the data embedding operations are performed in encrypted domain. On the other hand, the data extraction procedures of the two schemes are very different. With the lossless scheme, data embedding does not affect the plaintext content and data extraction is also performed in encrypted domain. With the reversible scheme, there is slight distortion in directly decrypted image caused by data embedding, and data extraction and image recovery must be performed in plaintext domain. That implies, on receiver side, the additional data embedded by the lossless scheme cannot be extracted after decryption, while the additional data embedded by the reversible scheme cannot be extracted before decryption. The combined lossless and reversible schemes can be used to construct a new scheme, in which data extraction in either of the two domains is feasible. That means the additional data for various purposes may be embedded into an encrypted image, and a part of the additional data can be extracted before decryption and another part can be extracted after decryption.In the combined scheme, the image provider initially performs histogram shrink and image encryption on the original image.When having the encrypted image, the data-hider may embed the first part of additional data using the method reversible data hiding. Then he can embed the second part of additional data using a lossless data hiding scheme.On receiver side, the receiver firstly extracts the second part of additional data from the LSB-planes of encrypted domain. Then, after decryption with his private key, he extracts the first part of additional data and recovers the original plaintext image from the directly decrypted image.

III. A COMBINED LOSSLESS AND REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES USING VISUAL CRYPTOGRAPHY

To overcome the problems of data missing and degradation of image quality and to reduce the computational complexity of public key cryptosystems and also to ensure complete security, we proposes a new combined lossless and reversible data hiding in encrypted images with visual cryptography.Visual cryptography overcomes both the complexity as well as security problems associated with public-key cryptosystems.Also the data extraction and image recovery are much easier as there is no need of any key exchange and also it is less time consuming.The main stages of the new scheme are Histogram Shifting, Image Encryption, Data Embedding, Data Extraction and Image Recovery. The framework of the proposed scheme is shown in figure 1.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

A. *Histogram Shiftin*

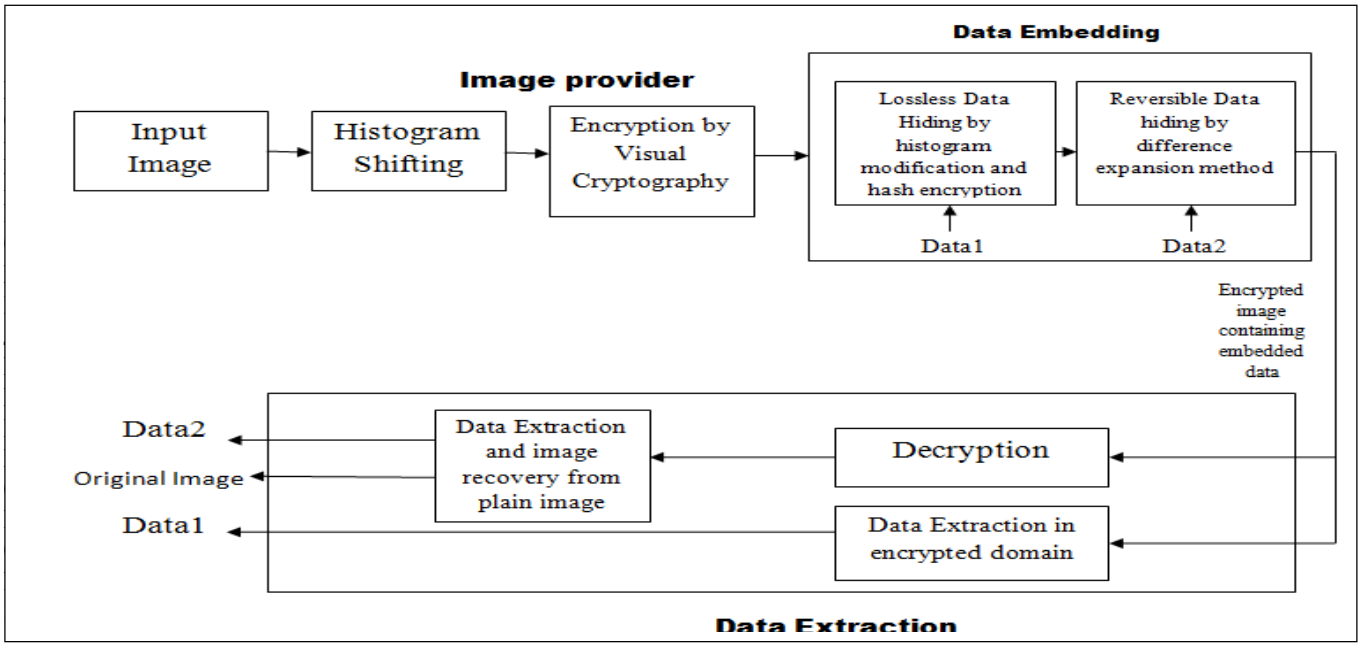

Fig 1. Combined Reversible and Lossless Data Hiding Scheme

In this phase the histogram of the input image is obtained and performs histogram shifting on it. In histogram shifting, it shifts slightly the part of the histogram between the maximum point and the minimum point to the right side by one pixel value to create an empty bin besides the maximum point for hiding an input message. Advantages of this method include yielding superior hiding capacities and providing higher qualities in stegoimages.

In this Histogram Shifting process [7] a small integer shared by the sender and the receiver is used. Then the sender side collect the pixels with gray values in[0,lamda+1], and represent their values as a binary stream BS1 and also collects the pixels with gray values in [255- lamda , 255] and represent their values as binary stream BS2. Then the gray values are enforced into [lamda +1, 255- lamda],

$$m_s(i,j) = \begin{cases} 255\text{- lamda, if } m(i,j) >= 255\text{-lamda} \\ m(i,j) \text{ , if lamda+1} < m(i,j) < 255\text{-lamda} \\ \text{lamda +1 , if } m(i,j) <= \text{ lamda +1} \end{cases}$$

Then denoting the new histogram as *h'v*where h_v denotes the number of pixels in the original plaintext image with gray value v, there must be

1. If v<=lamda, then h'v = 0.
2. If v=lamda+1, then h'v = hv.
3. If lamda+1<v<255-lamda, then h'v = hv.
4. If v>255-lamda, then h'v = 0.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Then the image provider finds the peak of the new histogram,

V = arg max *h'v*

Then a histogram shift operation is made on the received pixels.The figure 2 shows the histogram shrinked image and the original image.

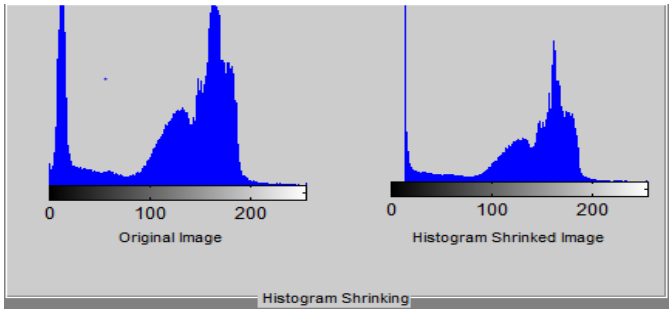

Fig.2. Histogram Shrinking

T. *Image Encryption using Visual Cryptography*

The input image is taken and it is divided into seven bit planes using bit planeslicing and of that the last bit plane is selected. Then we performs visual encryption on that seventh bit plane. In the visual encryption process, the image is split into two shares. Each share has a pair of pixels for every pixel in the original image. These pixels are shaded black or white according to the following rule:

- If the original image pixel was black, the pixel pairs in the shares mustbe complementary; randomly shade one pixel black and white and theother white and black.When these complementary pairs are overlapped,they will appear dark gray.
- If the original image pixel was white, the pixel pairs in the shares mustmatch both white and black or both black and white. When these matchingpairs are overlapped, they will appear light gray. Then the six bitplanes and the two shares are send to the receiver so that he can getthe message as well as the original image back. The figure 3 shows theshare.

Fig. 3. Shares generated using visual cryptography

U. *Lossless Data Embedding*

The lossless data embedding technique takes the encrypted share, the message that we entered and the length of the message asinput. Then the share received is reshaped to a single row of pixels where rowsize is equal to row x column of the share. Then we obtained the minimumpixel location is obtained and the pixels are grouped from minimum pixel valueto minimum pixel value added with the length.

Then we can hide the message into the share after converting the message into bits. If the first bit in the message is 1, then the pixel in the share is setto 1 otherwise it is set to 0. Thus we can embed the whole message bits intothe input share. This step provides the share with first part of data embeddedas the output.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

V. *Reversible Data Embedding*

The reversible data embedding technique takes the encrypted share, the messageto be hidden and the message length as input. Then the horizontal and vertical produce of the share are created and HaarWavelet transform is applied to both produces. The next step is the data embedding process using difference expansion scheme[8]. The Difference Expansion data embedding algorithm consists of six steps:-

1. Calculate the difference values.
2. Partitioning difference values into four sets.
3. Creating a location map.
4. Collecting original LSB values.
5. Data embedding by replacement.
6. Inverse integer transform.

In a digital image, one can select some expandable difference values of pixels, and embed one bit into each of them. To extract the embedded data and restore the original values, the decoder needs to know which difference values have been selected for the DE. To facilitate it, we need to embed such location information, such that the decoder could access and employ it for decoding. For this purpose, we will create and embed a location map, which contains the location information of all selected expandable difference values.

The difference values are denoted as h and order them into a one dimensional list h1, h2, h3 … hn.Next we create four disjoint sets of difference values,

EZ, EN, CN, and NC:

1. EZ: contains all expandable h=0 and expandable h=-1
2. EN: contains all expandable h! =EZ.
3. CN: contains all changeable h! = (EZ U EN).
4. NC: contains all non-changeable h.

Each difference value will fall into one and only one of the above four sets.Next we create a location map of selected expandable difference values. For every difference value h in EZ, it will be selected for the DE. For EN, depending on the payload size, some difference values will be selected for theDE. Then the original LSBs of difference values are collected and after thatthe location map, original LSB and payload p (includes hash of original image) is embedded into the share. Finally all bits are embedded and apply, inverseinteger transform to obtain embedded image.

W. *Lossless Data De-embedding*

In the lossless data decoding technique the size of the new message embeddedimage is obtained. The message embedded share, its size and the minimum pixel location are the input taken here. Then the embedded share is reshapedinto a single row and after that the data is taken from it in the form of bits. The original message embedded is extracted by converting the bits extractedinto character message.

X. *Reversible Data De-embedding*

We can retrieve the embedded bit stream by collecting LSBs of all changeabledifference values. From the bit stream, we can decode location map andoriginal LSB. After all changeable difference values have restored their originalvalues, we can restore the original image exactly. The reversible datade-embedding includes 5 steps:-

1. Calculate the difference values(apply transform).
2. Create two sets(CH-changeable h) and (NC-Non changeable h).
3. Collect LSBs of all difference values in CH and form bit stream.
4. We decode the location map.
5. Restore the original values of differences.
6. Inverse transform to reconstruct a restored image.

Y. *Image Decryption and Image Recovery*

At the receiver side, the two shares of the seventh bit plane and the other six bit planes are XORed together to obtain the original image. This step is performed after data extraction and so the share received here doesn't have any data. At first the two shares are XORed to get the seventh bit plane. After that the seven bit planes joined together to get the original input image.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

IV. EXPERIMENTAL RESULTS

The proposed scheme is evaluated by obtaining the PSNR values, embedding capacity of the stego image and the time complexity. For embedding efficiency also called embedding quality or visual quality of the stego image, in order to avoid a subjective evaluation by human naked eyes, a well-known measurement called peak-signal-to-noise ratio(PSNR) is used to obtain the similarity between original image and stego image.

PSNR is defined as

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \text{ dB}$$

Where MSE is the mean square error represents the difference between stego image and original image sized H X W pixels. The MSE is defined as

$$MSE = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} (Iij - I'ij)2$$

According to the visual quality evaluation, a high value of PSNR means that a stego image is much similar to its original image and the embedding efficiency is high. The figures 4 and 5 represents the graphs that comparing the embedding capacity and PSNR values of existing system and proposed system respectively

Different image are taken and different data are embedded into it each times so as to evaluate its PSNR and embedding capacity in each cases. In each of the cases it is obtained that the PSNR and Embedding capacity are higher than the existing combined scheme.

The time complexities of both existing and proposed systems are calculated and compared to obtain the result that the proposed work has less time complexity. Thus it overcomes the problem of high computational complexity.

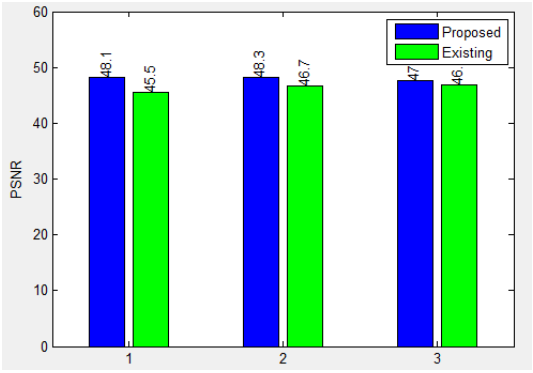

Fig 4. PSNR of Existing vs Proposed

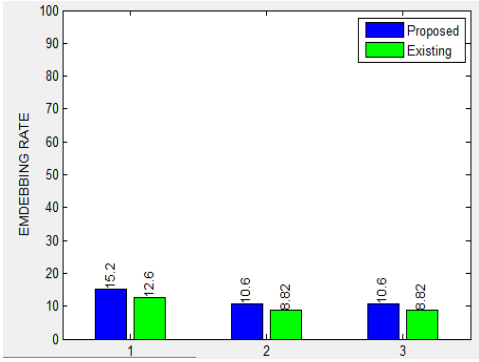

Fig 5. Embedding Rate of Existing vs Proposed

V. CONCLUSION

This work proposes a combined reversible and lossless data hiding scheme for providing security to highly confidential data. The combined scheme performs data embedding in an encrypted image using both of the data hiding schemes. Here the image is encrypted using visual cryptography as it requires no key exchange. The highest time consumption and complexity which are the problems of existing combined data hiding schemes overcomes here. Also

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

the efficiency and security of the system is improved. Thus we can use this system for the transmission of highly confidential data as we can embed two parts of data into a single cover image so that one part can be extracted after the decryption of the cover image and other part before the decryption of the image.

REFERENCES

1. Z Qian, X Zhang and S Wang, "Reversible Data Hiding in Encrypted JPEG Bitstream", IEEE Transactions on Multimedia(2014).
2. Weing Hong and Tung-Shou Chen, "Reversible Data Embedding for High Quality Images using Interpolation and Reference Pixel Distribution Mechanism", J.Vis Commun.Image R22,Elsevier(2011).
3. W .Hong and T.S.Chen, "Histogram Shifting based Reversible Data hiding", International Journal of Engineering Trends and Technology(2014).
4. Wei Liu, Wenjun Zeng, Lina Dong, and Qiuming Yao "Efficient Compression of Encrypted Grayscale Images", Image Processing, IEEE Transactions Vol: 19, April 2010, pp. 1097 –1102.
5. Mehmet Utku Celik, Gaurav Sharma, Ahmet Murat Tekalp, Eli Saber, "Lossless Generalized-LSB Data Embedding", IEEE Transactions on Image Processing.
6. Noura A Saleh and Hoda N boghdady, "High Capacity Lossless Data Embedding Techniques for Palette Images based on Histogram Analysis", Digital Signal Processing(Elsevier 2010).
7. Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng, "Lossless and reversible Data Hiding in Encrypted Images with Public key Cryptography", IEEE Transactions on Circuits and Systems for Video Technology" , 2015.
8. Yongjian Hu, *Member, IEEE*, Heung-Kyu Lee, Kaiying Chen, and Jianwei Li, "Difference Expansion based Reversible Data Hiding using Two Embedding directions",IEEE Transactions on Multimedia, 2008.
9. X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255258, Apr. 2011.
10. 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.
11. J. Tian, "Reversible data embedding using a difference expansion" Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890 2003.
12. 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.
13. W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary covers" vol. 21, no. 6, pp. 2991–3003, June. 2012.
14. 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.
15. Wei Liu, Wenjun Zeng, Lina Dong, and Qiuming Yao "Efficient Compression of Encrypted Grayscale Images", Image Processing, IEEE Transactions Vol: 19, April 2010, pp. 1097 –1102
16. Vinit K Agham and Tareek M Patterwar, "Seperable Reversible Data Hiding Technique Based on RGB-LSB Method", International Journal of Research in Advent Technology(2013).
17. Kede Ma, Wei. Zhang, Xianfeng Zhao, "Reversible data Hiding in Encrypted Images by reserving Room before encryption", IEEE trans. On information forensics and security, vol,8 No.3 , march 2013.
18. J Jagadersan Balika and Nikhila Nyapathy ,"Reversible Data Hiding in Encrypted Images using AES Data Encryption Technique", International Journal of Emerging Research in Management and Technology(2014).
19. M. Johnson, P. Ishwar, V.M. Prabhakaran, D. Schonbergand K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992-3006, Oct. 2004.
20. Sukhdeep Kaur and Manshi Shukla, "Reversible Data Hiding in Images using Circular Hough Transform", International Journal of Computer Science and Information Technologies(2014).
21. Jiantao Zhou,Weiwei Sun, Li Dong,Xianming Liu, Oscar C. Au,and Yuan Yan Tang, "Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation", IEEE transactions on circuits and systems for video technology,2015.
22. Kede Ma, Wei. Zhang, Xianfeng Zhao, "Reversible data Hiding in Encrypted Images by reserving Room before encryption", IEEE trans. On information forensics and security, vol, 8 No.3, march 2013.