International Conference on Advanced Computer Science & Software Engineering - (ICACSSE-2015)
December 20, 2015 - Hyderabad, India
www.ijmetmr.com/icacsse2015
Paper Publication in IJMETMR, A Peer Reviewed Open access International Journal.

Survey on Reversible Hiding Techniques

Peddinti Vamsi
M.Tech (CST)
Department of CSE
GITAM School of Technology,
Hyderabad.

Dr.S.PhaniKumar, M.Tech, Ph.D.
Professor & HoD
Department of CSE
GITAM School of Technology,
Hyderabad.

ABSTRACT:
With the increase in development of information technology nowadays, more and more images and data are available on the internet. So some kind of authentication is needed, for providing security to such important data. With the rapid increase in technology, the reversible data hiding (RDH) in encrypted images, has gain lots of importance. Reversible Data Hiding (RDH) in encrypted images is mainly focused with security and authentication and has an excellent property that the original image cover can be losslessly recovered after data embedded is extracted while protecting the image content's as confidential. In this survey paper different reversible data hiding methods are analyzed.

KEYWORDS: ***Reversible data hiding (RDH), Image encryption.***

INTRODUCTION

Data and information security have always been a vibrant area of research. In the area of data security various traditional approaches like Cryptography, Steganography, and Data Hiding can be used. Cryptography refers to the study of mathematical techniques and related aspects of Information Security like data confidentiality, data integrity, and of data authentication.

In cryptography a plain message is encrypted into cipher text and that might look like a meaningless jumble of character whereas in case of steganography, the plain message is hidden inside a medium that looks quite normal and does not provide any reason for suspecting the existence of a hidden message. Such an image is called as stego-image. Data hiding conceals the existence of secretinformation while cryptography protects the content of messages.More and more attention is paid to reversible data hiding in encrypted images. The hidden data in the cover image may be any text related to the image such as authentication data or author information [2]. Reversible data hiding represents a technique where the data is embedded in the host media and at the receiving end the secret data and also the host media will be recovered loss less

A. How we can define reversible data hiding

Reversible data hiding can be defined as an approach where the data is hidden in the host media that may be a cover image. A reversible data hiding is an algorithm, which can recover the original image losslessly after the data have been extracted.

The transmitter side of such systems involves a cover image, additional data, encryption key and data hiding key. The original image will be encrypted, data will be hidden and then image will be transmitted. The receiver thus needs to decrypt the image and extract the data. The reversibility means that not only the embedded secret data but also the encrypted cover image must be extracted lossless at the receiver side.

B. Major application areas of reversible data hiding

Reversible data hiding is technique to embed the additional message in the some distortion unacceptable cover media. This is the technique that is mainly used for the authentication of data like images, videos, electronic documents. As long as image is concerned the technique could be useful in area of protection and transmission of secret sensitive military and medical images.

In applications such as in law enforcement, medical images systems, it is desired to be able to reverse the stego media back to the original cover media for legal consideration. The remote sensing and military

imaging, high accuracy is required. In some scientific research, experimental data are expensive to be achieved. Under these circumstances, the reversibility of the original media isdesired [8]. The data hiding scheme satisfying these requirement can be referred as lossless

Let us consider an example, suppose a medical image database is stored in a data center, and server in the data center, and embed notations into an encrypted version of a medical image through a RDH technique. With the notations the server can manage the image or verify its integrity without having the knowledge of the original content, and thus the patient's privacy is protected. On the other hand, a doctor, having the cryptographic key, can decrypt hand, a doctor, having the cryptographic key, candecrypt and restore the image in a reversible manner for the purpose of further diagnosing.

Thus chief application area of reversible data hiding is in IPR protection, authentication, military, medical and law enforcement.

C. Two basic approaches for hiding data in the cover image

Some of the previous arts in the area of RDH are based on the concept of hiding data in the encrypted image.
In this method as shown in the fig 1 below, the content owner first encrypts the original image using a standard cipher with an encryption key employment. After producing the encrypted version of the image the space for storing the data is vacated from the image in a lossless manner [1].

The data hider can embed some secret data in the vacated space with the help of data hiding key. Then a receiver that may be the owner itself or any authenticated end user can extract the embedded data from encrypted image with the help of data hiding key as well as the original image can be recover with no loss of quality by using the encryption key [1].

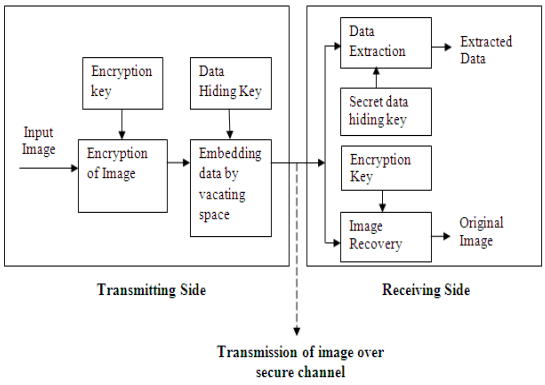

Fig. 1: Vacating Space after Encryption for RDH

This method of hiding data in the encrypted image is used in [2] & [3]. In [2] method of separable reversible data hiding in encrypted image with improved performance is proposed. Where the owner of image first encrypts the image by permutation, by making use of an encryption key. Since permutation only shuffles the pixels, the histogram of the image remains the same. The data hider without any knowledge about the original image contents hides the data into encrypted image by histogram modification method.

Since above specified approach require the lossless vacating the space from the encrypted image which can be sometimes difficult and inefficient. Thus Kede ma. Weiming Zhang, Xianfeng Zhao, Nenghai Yu, Fenghua Li, in [1] have proposed the approach of reserving the space for embedding the secret data prior to the image encryption. That is the reverse order is followed. The approach is explained in fig 2. Thus using this method the data hider gets extra space vacated out before encryption thus making data hiding process effortless.

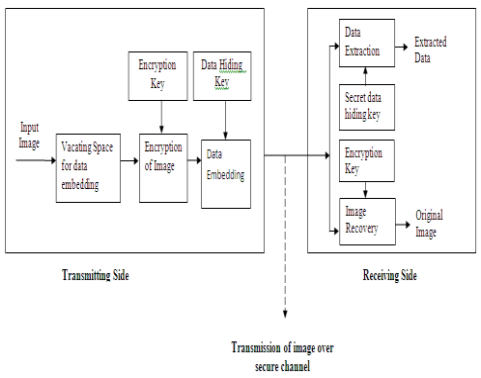

Fig. 2: Vacating Space before Encryption for RDH

D. Parameter to measure the performance of the RDH techniques

There are different methods used for reversibly hiding data in the image. All those methods if considered offers one or other benefit. The exciting feature of RDH methods ar algorithm is the reversibility itself. That retrieving the image lossless after then embedded secret data is extracted. There are different parameters on basis of which the performance of those techniques can be measured. The following parameters must be considered:

- Quantity of Data: This refers to the maximum amount of secret data that can be embedded in the cover image.
- Complexity of technique: Simplicity and complexity of these techniques is also important measure that affects the usability of the techniques.
- Quality of cover image: The quality degradation of the image after data is extracted will not be accepted in RDH. Thus quality of image is an important measure.

The RDH can become a promising secret communication channel since there is no visual discrimination between the embedded image and original image.

RELATED WORK

Lots of research has been done in the area of reversible data hiding. In last few years various efficient methods have been proposed for reversible data hiding and color image visual cryptography. Some noticeable work in area of reversible data hiding is as follows:

In [4] Jui Tian has introduced a difference expansion technique which discovers extra storage space by exploring the redundancy in the image content. Both the secret data holding capacity limit and the visual quality of embedded images of the DE method are among the best in the literature, along with a low computational complexity.

In [5] Wen-Chung Kuo, Po-Yu Lai, Lih-ChyauWuu has proposed a new method of adaptive reversible data hiding based on histogram. In order to enhance the data hiding capacity and embedding point adaptively anew proposed scheme was based on histogram and slope method. This method keeps the embedding capacity high and also maintains the high quality of stegno-image.

In [1] Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu and Fenghua Li has proposed a framework for reversible data hiding for embedding data in an image by reserving room before encryption. Since losslessly vacating room from the encrypted images is relatively difficult and sometimes inefficient.

In [6] Kuo-Ming, Wen-Kai Su, Ting-Wen Chen, Li-Ming Chen has proposed method that combines reversible data hiding, halftoning and vector quantization (VQ) technique to embed a grayscale image in other image. In embedding, first use halftoning to compress the image from grayscale to halftone. Next, compute th difference between original image and one which inversed by LIH. Employing the VQ compress the difference and embed it with secret data. Then the host image can be recovered better when extracting the secret data by the difference.

In the area of reversible data hiding José .R; Abraham .G, in [9] have proposed a novel scheme to reversibly hide data into encrypted greyscale image in a separable manner. Content owner encrypts the image by permuting pixels using encryption key. The data hider hides the data into the encrypted image by histogram modification based hiding by using data hiding key.

As our proposed scheme is combining two different approaches together that are reversible data hiding and colour visual cryptography. Visual cryptography was introduced by Naor [11]. In a k-out-of-n scheme of VC, a secret binary image is cryptographically encoded into n shares of random binary pattern. The n shares are Xeroxed onto n transparencies, respectively, and distributed amongst n participants. Any k or more participants can visually reveal the secret image by superimposing any k transparencies together. Let us have look at some commendable work in the area of visual cryptography.

Siddharth Malik, Anjali Sardana, Jaya in [10] has proposed another promising approach for color visual cryptography which involves three main steps that are Sieving, Division and Shuffling to generate random shares. This approach promises the minimal computation requirement for generation of the original secret image from the random shares without any loss of image quality.

In [12] InKoo Kang, Gonzalo R. Arce , Heung-Kyu Lee introduces a color visual cryptography encryption method that produce meaningful color shares via visual information pixel synchronization and error diffusion halftoning.

In [13] Wei Qiao, Hongdong Yin, Huaqing Liang has proposed a new secret visual cryptography scheme for color images bsed on halftone.Firstly a chrom,atic image is decomposed into three monochromatic images in tone cyan, magenta and yellow. Secondly, these three images are transmitted into binary images by halftone technique. Finally, the traditional binary to hide to get the sharing images.

Yi-Hui Chen, Ci-Wei lan and Chiaio-ChihHuang in [14] have proposed an authentication mechanism for visual cryptography. The proposed scheme consists of two procedures namely encryption procedures and decryption procedure. The secret image and the authenticated image can be decrypted by stacking the share using difference expansion.

Basic RDH Techniques

Following are different data embedding techniques that can be used in RDH algorithms:

- LSB Modification Technique
- Difference Expansion Based Technique
- Histogram Shifting Based Technique
- Prediction Error Based Technique
- Vector Quantization Based Technique

LSB Modification Technique

One of the earliest methods is the LSB (Least Significant Bit) modification. In this well known method, the LSB of each signal sample is replaced (over written) by a secret data bit. During extraction, these bits are read in the same scanning order, and secret data is reconstructed

Difference Expansion Based Technique

Difference expansion based techniques used in [16] was proposed by Tian]. The method of embedding is as follows. The two neighbor pixels (a,b) are considered the mean value and the difference is calculated first.

$$l = \lfloor (a+b)/2 \rfloor,\ y = a - b \text{----------(1)}$$

Where $\lfloor . \rfloor$ represents the floor operation which rounds the elements to the nearest integers towards minus infinity. To embed a binary data bit $x(x \in (0,1))$ into a difference, the expanded difference is calculated as:

$$y' = 2 \times y + x \text{----------(2)}$$

Finally, the new pixels (a', b') are computed as follows

$$a' = l + \lfloor (y'+1)/2 \rfloor, b' = l - \lfloor y'/2 \rfloor \text{----------(3)}$$

In extraction phase, the average and the difference of the pixels $(a', b')$are also calculated first:

$$l = \lfloor (a'+b')/2 \rfloor,\ y' = a' - b' \text{---------(4)}$$

The embedded data is least significant bit of h', and the original difference h is calculated by:

$$a = \text{LSB}(y').y = \lfloor y'/2 \rfloor \text{----------(5)}$$

And the original pixels can be restored by:

$$a = l + \lfloor (y+1)/2 \rfloor, b = l - \lfloor y/2 \rfloor \text{----------(6)}$$

In [10] Jui Tian has introduced a difference expansion technique which discovers extra storage space by exploring the redundancy in the image content. Both the secret data holding capacity limit and the visual quality of embedded images of the DE method are among the best in the literature, along with a low computational complexity.

Histogram Shifting Based Technique

The histogram shifting [16,17,18,19] based reversible data hiding scheme embed data by shifting the histogram into a fix direction. And there are two points which are important in these schemes, which are peak point and zero point. The peak point corresponds to the grayscale value, which corresponds to the maximum number of pixels in the histogram of the given image. Sand the zero point is usually the point that the number

is histogram is zero. And the minimum number of pixels is selected as the zero point to increase the embedded capacity.

In the histogram-shifting based algorithms, the pixel between the peak and zero pairs were modified in the embedding processing, the pixel in the peak point was used to carry a bit of the secret message, the others were modified and no secret data were embedded.
The basic procedure of histogram shift algorithm ia as follows:

- Create the histogram of image
- Find the peak points and zero points.
- We assume the peak point is 'a' and the zero point is 'b'. (a>b); shift the points between b+1 and a-1 by reducing 1.
- If the embedded bit is 1, the peak point is reserved; otherwise, change the peak point value by reducing 1.
- To achieve the reversibility requirements, the location of the pixels in the minimum point must be recorded and embedded. Then record the peak point, the zero points and some other auxiliary information.

Prediction Error Based Technique

Reversible data hiding [20,21] is based on prediction error use predicted system to embed data, there are many predictors which have been proposed. They are horizontal predictor, vertical predictor, Causal weighted average, Causal and SVF. One well known predictor is the median edge detection (MED) predictor.

There are different predictors that can be used, they are as follows:
The horizontal predictor is $p'(x,y) = p(x-1,y)$.

The vertical predictor is $p'(x,y) = p(x,y-1)$

The Causal weighted average is
$p'(x,y) = (p(x-1,y) + 2p(x,y-1) + 2p(x-1,y) + p(x-1,y+1))/6$.

Vector Quantization based Technique

This scheme is based on compression of image[22]. VQ is one of the efficient compression technique and it has widely used as it is easy for implementation and high efficiency. Vector Quantization is a method which is lossy compression. For fewer stores in images, video and transport obtains the lower data ratye and rebuild the signal that has some loss. Vector Quantization is proposed first time by Y Linde, A Buzo and M Gray in 1980. This method produces codebook that combining with each representative vectors which call code word symbolically by data training. The size and domain of codebook decide the rate that compress. The generating, optimization, encoding and decoding are included in codebook of VQ.

PROPOSED WORK

Image encryption

The use of computer networks for data transmissions has created the need of security. Many robust messageencryption techniques have been developed to supply this demand. The encryption process can be symmetric,asymmetric or hybrid and can be applied to blocks or streams.Several asymmetric algorithms use longkeys to ensure the confidentiality because a part of the key is known. These algorithms are not appropriateenough to be applied to images because they require a high computational complexity. In the case of block encryption methods applied to images, one can encounter three inconveniences. The first one is when we havehomogeneous zones (regions with the same color), all blocks in these zones are encrypted in the same manner.The second problem is that block encryption methods are not robust to noise. Indeed, because of the largesize of the blocks (which is at least of 128 bits) the encryption algorithms per block, symmetric or asymmetric,cannot be robust to noise. The third problem is data integrity. The combination of encryption and data-hiding[23]can solve these types of problems.The Advanced Encryption Standard (AES) algorithm consists of a set of processing steps repeated for anumber of iterations called rounds. The number of rounds depends on the size of the key and the size of thedata block. The number of rounds is 9 for example,

if both the block and the key are 128 bits long. Given asequence {X1,X2, ...,Xn} of bit plaintext blocks, each Xi is encrypted with the same secret key k producing theciphertext blocks {Y1, Y2, ..., Yn}.To encipher a data block Xi in AES you first perform an AddRoundKey step by XORing a subkey with theblock. The incoming data and the key are added together in the first AddRoundKey step. Afterwards, it followsthe round operation. Each regular round operation involves four steps. In the SubBytes step, each byte of theblock is replaced by its substitute in a substitution box (S-Box). In cryptography, an S-box is a basic componentof symmetric key algorithms used to obscure the relationship between the plaintext and the ciphertext. Thenext one is the ShiftRows step where the rows are cyclically shifted over different offsets. The next step is theMixColumns, where each column is multiplied with a matrix over the Gallois Field, denoted as GF. The last step of the round operation is another AddRoundKey. It is a simple XOR with the actual data and the subkeyfor the current round. Before producing the final ciphered data Yi, the AES performs an extra final routine thatis composed of (SubBytes, ShiftRows and AddRoundKey) steps.

The AES algorithm can support several cipher modes: ECB (Electronic Code Book), CBC (Cipher BlockChaining), OFB (Output Feedback), CFB (Cipher Feedback) and CTR (Counter) The ECB mode is actuallythe basic AES algorithm. With the ECB mode, each plaintext block Xi is encrypted with the same secret key k producing the ciphertext block Yi:

Yi = Ek(Xi) (1)

The CBC mode adds a feedback mechanism to a block cipher. Each cipher text block Yi is XORed with theincoming plaintext block Xi+1 before being encrypted with the key k. An initialization vector (IV) is used forthe first iteration. In fact, all modes (except the ECB mode) require the use of an IV. In CFB mode, Y0 issubstituted by the IV. The keystream element Ziis then generated and the ciphertext block Yi is produced Inthe OFB mode, Z0 is substituted by the IV and the input data is encrypted by XORing it with the outputZi. The CTR mode has very similar characteristics to OFB, but in addition it allows pseudo-random access fordecryption. It generates the next keystream block by encrypting successive values of a counter. Although AESis a block cipher, in the OFB, CFB and CTR modes it operates as a stream cipher. These modes do not requireany special measures to handle messages whose lengths are not multiples of the block size since they all work byXORing the plaintext with the output of the block cipher. Each mode has its advantages and disadvantages.

For example in ECB and OFB modes, any modification in the plaintext block Xi causes the corresponding cipheredblock Yi to be altered, but other ciphered blocks are not affected. On the other hand, if a plaintext block Xi ischanged in CBC and CFB modes, then Yi and all subsequent ciphered blocks will be affected. These propertiesmean that CBC and CFB modes are useful for the purpose of authentication while ECB and OFB modes treatseparately each block. Therefore, we can notice that OFB does not spread noise, while the CFB does exactlythat.

In this paper, for the proposed method, the ECB mode of AES algorithm has been chosen to encrypt theimages. The images are thus encrypted by blocks of 128 bits which correspond to 16 gray level pixels. We canfirst measure the image information content with the entropy H(X). If an image X has M gray levels αj, with0 _ j< M, and the probability of gray level αjis P(αj), the entropy H(X), without considering the correlationof gray levels, is defined as:

$$H(X) = -\sum_{j=0}^{M-1} P(\alpha_j) log_2(P(\alpha_j)). \quad (2)$$

If the encryption algorithm is efficient, the entropy H(Y) of an encrypted image Y must be maximal andthen greater than the entropy H(X) of the original image X:

H(Y) >=H(X) (3)

Encoding algorithm

The coding algorithm is composed of two steps which are the encryption and the data hiding step.For each

block Xi composed of n pixels pjof an image of N pixels, we apply the AES encryption algorithmby block:

$$Yi = Ek(Xi) \quad (4)$$

Where Ek() is the encryption function with the secret key k and Yi is the corresponding cipher-text to Xi. Onecan note that the sizes of Xi and Yi are identical.During the data hiding step, in each cipher-text we modify only one bit of one encrypted pixel of Yi:

$$Ywi= DHk(Yi) \quad (5)$$

Where DHk() is the data hiding function with the secret key k and Ywiis the marked cipher-text. We used bitsubstitution-based data hiding method in order to embed the bits of the hidden message. For each block Yi, thesecret key k is used as the seed of the pseudo-random number generator (PRNG) to substitute the bit of a pixelwith the bit to hidden. At the end of the coding process we get a marked encrypted image. Since we embed 1bit in each block of n pixels, the embedding factor is equal to 1/n bit per pixel

.

Decoding algorithm

The decoding algorithm is also composed of two steps which are the extraction of the message and the decryption-removing. The extraction of themessage is very simple: it is just enough to read the bits of the pixels we have marked by using the secret key kand the same PRNG. But after the extraction, each marked cipher-text is still marked. The problem is then todecrypt the marked encrypted image. The decryption removing is done by analyzing the local standard deviationduring the decryption of the marked encrypted images.To analyze the variation of the local standard deviation σ for each block Xi, taking account of its neighborsto calculate the local meanXi, we have:

$$\sigma(X_i) = \sqrt{\frac{1}{n}\sum_{j=1}^{n}(p_j - \overline{X_i})^2}, \quad (6)$$

With n the size of the pixel block to calculate the local mean and standard deviation, and 0 <=i<N/nif N is theimage size.For each marked cipher-text Ywiwe apply the decryption function Dk() for the two possible values of thehidden bit (0 or 1) and we analyze the local standard deviation of the two decrypted blocks X0i and X1i. Inthe encrypted image, the entropy must be maximal and greater than the original one as described in equation (3).Moreover, the local standard deviation of the encrypted image is higher than for an original image. From thisassumption we decided to compare for each block the local standard deviation of X0i with X1i and we selectthe bit value where the local standard deviation is the smaller:

Xi = Dk(Y 0i) if σ(Dk(Y 0i)) < σ(Dk(Y 1i))= Dk(Y 1i) else.

CONCLUSION

Reversible data hiding in encrypted images is a new topic drawing attention because of the privacy-protection requirements from large data management. Previously implementation of RDH in encrypted images by vacating room after encryption was as we did by reserving room before encryption. Here the data hider is benefited from the extra space emptied out in previous stage to make data hiding process easy. This proposed method gets advantage of all traditional RDH techniques for grayscale images and achieve excellent performance without loss of perfect data. Furthermore, this novel method achieves real reversibility, separate data extraction and improvement on the quality of marked decrypted images.

REFERENCES:

[1]Kede Ma. Weiming Zhang, Xianfeng Zhao, Nenghai Yu,Fenghua Li, “Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption”, IEEE Trans on Information Forensics and security, Vol. 8, No. 3, march 2013.

[2]Rintu Jose, Gincy Abraham, “A Separable Reversible Data Hiding in Encrypted Image with Improved Performance”, International Conference on Microelectronics, Communication and Renewable Energy, ICMiCR-2013.

[3]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

[4]M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in Proc. ECOC'00, 2000, paper 11.3.4, p. 109.

[5]Wen Chung Kuo, Po Yu Lai, LihChyauWuu, " Adaptive Reversible Data Hiding Based on Histogram", 10th International Conference on Intelligent Systems Design and Application, © IEEE 2010.

[6]Kuo-Ming Hung, Wen-Kai Su, Ting-Wen Chen, Li-Ming Chen, "Reversible Data Hiding Base on VQ and Halftoning Technique", International Conference on Microelectronics, Communication and Renewable Energy (ICMiCR-2013).

[7]Yun Q. Shi, "Reversible Data Hiding", I.J. Cox et al.: IWDW 2004, LNCS 3304, pp. 1-12 2005 © Springer-Verlag Berlin Heidelberg 2005 "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.

[8]A. Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.

[9]Jose, R.; Abraham, G, "A separable reversible data hiding in encrypted image with improved performance", Emerging Research Areas and 2013 International Conference on Microelectronics, Communications and Renewable Energy(AICERA/ICMiCR), 2013 Annual International Conference ©IEEE 2013.

[10]Siddharth Malik, Anjali Sardana, Jaya, "A Keyless Approach to Image Encryption",2012 international conference on Communication systems and Network Technologies ©2012 IEEE.

[11]Moni Naor, Adi Shamir," Visual Cryptography", in Proc. EUROCRYPT'94, Berlin, Germany, 1995, vol. 950, pp. 1-12,Springer-Verlag, LNCS.

[12]InKoo Kang, Gonzalo R. Arce , Heung-Kyu Lee, " Color Extended visual cryptography using error diffusion", ICASSP 2009 © IEEE 2009.

[13]Wei Qiao, HongdongHuaqing Liang, "A kind of Visual Cryptography Scheme For color Images based on halftone technique", International Conference on Measuring Technology and Mechatronics automation © 2009 IEEE.

[14]Yi-Hui Chen, Ci-Wei lan and ChiaoChih Huang, " A verifiable Visual Cryptography Scheme", Fifth International Conference and Evolutionary Computing © IEEE 2011.

[15]Jun Tian, "Reversible Data Embedding Using a difference Expansion", IEEE Transaction on circuits and systems for video technology, Vol.13, No. 8, Aug 2003.

[16]V Yu, Song Wei, "Study on Reversible Data Hiding Scheme for Digital Images", 2nd International Asia Conference on Informatics in Control, Automation and Robotics, (CAR) 2012.

[17]Wen Chung Kuo, Po Yu Lai, LihChyauWuu, " Adaptive Reversible Data Hiding Based on Histogram", 10th International Conference on Intelligent Systems Design and Application, © IEEE 2010.

[18]ZhenfeiZhaoa,b, HaoLuoc, Zhe-Ming Luc, Jeng-Shyang Pan, "Reversible data hiding based on multilevel histogram modification and sequential recovery", International Journal on Electronic and communication, Z. Zhao et al. / Int. J. Electron. Communications.(AEÜ) 65 (2011) 814–826.

[19]C. Vinoth Kumar, V. Nataranjan and DeepikaBhogadi, "High capacity Reversible Data hiding based on histogram shifting for medical image", International Conference on Communication and Signal Processing, April 3-5 2013, India © IEEE 2013.

[20]Che-Lun Pan, Wien Hong, Tung-Shou Chen, Jeanne Chen and Chih-Wei Shiu, "Multilevel Reversible Data Hiding using Modification of Prediction Errors", ICIC Vol 7,No. 9, Sept 2011.

[21]Xiaolong Li, Bin Yang and Tieyong Zeng, "Efficient Reversible Watermarking Based on Adaptive Prediction-Error Expansion and Pixel Selection", IEEE Transaction on Image Processing, Vol, 20, No. 12, Dec 2011.

[22]Kuo-Ming Hung, Wen-Kai Su, Ting-Wen Chen, Li-Ming Chen, "Reversible Data Hiding Base on VQ and Halftoning Technique", International Conference on Microelectronics, Communication and Renewable Energy (ICMiCR-2013).

[23]William Puech, Marc Chaumont, Olivier Strauss. A Reversible Data Hiding Method for Encrypted Images. IS&T/SPIE Electronic Imaging 2008 - Security, Forensics, Steganography, and Watermarking of Multimedia Contents, San Jose, CA, United States. SPIE/IS&T, 6819, ppN/A, 2008.