ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

A Novel and Improved Technique for Reversible Data Hiding using Visual Cryptography

Shruti M. Rakhunde[1], Archana A. Nikose[2]

M.Tech Student, CSE, Priyadarshini Bhagwati College of Engineering, Nagpur, India [1]

Assistant Professor, CSE, Priyadarshini Bhagwati College of Engineering, Nagpur, India [2]

Abstract: This paper presents a detail description of novel scheme for reversible data hiding which can recover the original image after hidden data have been extracted. Scheme applies a method for hiding data in an image before encryption and utilizes a novel method for encrypting the image using visual cryptography. A modified algorithm for reversible data hiding using difference expansion technique is used in this scheme. The proposed scheme thus increases the amount of data that can be hidden in the image which also guarantees the lossless recovery of an image after the extraction phase.

Keywords: Reversible Data Hiding, Difference Expansion technique, SDS, RDH

I. INTRODUCTION

Data hiding is referred to as a process to embed useful data (representing some information) into a cover media. In certain application, the embedded data are closely related to the cover media, such as authentication. In this type of application, invisibility is the major requirement. In most cases, the cover media will experience some distortion due to data hiding and cannot be inverted back riginal image. That is, some permanent distortion exists even after the hidden data have been extracted. In some applications, such as medical diagnosis and law enforcement, it is desired to reverse the marked media back to the original cover media after the hidden data are retrieved. The marking technique satisfying these requirements is referred to as reversible or lossless data hiding techniques.

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 stegno 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 is desired. 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, can decrypt 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.

A. Fundamentals of RDH

Two basic approaches can be used in RDH that are:

-Vacating the room for hiding the data after the image encryption

-Vacating the room in the original image for hiding the data and then the image is encrypted

In the first approach sometimes vacating the room for hiding the data becomes inefficient and difficult as encryption process affects the entropy of an image. That is not the case with the second approach as reserving the room in the original image is sufficiently effortless.

B. 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 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.

C. Existing Methods

There are various methods which has been proposed for reversibly embedding the data in the cover image Hwang in [2] has proposed the method for reversibly hiding the data in the image using histogram shift method

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

The histogram shifting 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.

In enhanced the embedded capacity Yeh proposed an efficient data hiding scheme based on predict error method [3]. It include dividing the cover image into blocks(e.g. 3x3) the block center point as the base point and obtain the prediction error value between it and the surrounding pixel. Do predict error value histogram and find out the peak point. Embed the secret data into two side region of peak point.

J. Tian in [4] has proposed the simple scheme with improved capacity of hiding data. Tian has introduced a Difference Expansion technique which discovers extra storage space by exploring the redundancy in the image content. Here the difference between the neighboring pixel values is calculated and some differences value is selected for difference expansion. Both the payload capacity limit and the visual quality of embedded images of the DE method is among the best in the literature.

All above method gives a method for hiding a data into an image in a reversible manner that in the extraction phase the image will be restored lossless but while the image is holding a data the secrecy of an image is also a major concern especially in transmission. And when the image and the data hidden into an image have a relation in that case both the data and image should not be revealed to the unintended user. Thus image can be protected by applying various kinds of encryption techniques onto it. A number of image encryption techniques have also been developed over years. Encryption algorithms falls under two general categories: substitutions and transpositions. Some algorithm performs both to enhance security. In a substitution based image encryption makes changes to the pixel values to make the content unrevealed. In permutation based encryption algorithm the pixels are shuffled and no change is made to the pixel values.

In the proposed scheme after applying RDH for hiding data, the image is encrypted using an novel scheme of visual cryptography which involves dividing the image into random shares.

D. Our contributions

Proposed scheme combines two different approaches that are reversible data hiding and visual cryptography. It uses the modified algorithm for data hiding which uses difference expansion technique. In [4] Tian has proposed the scheme of difference expansion for grayscale images. In our approach we have modified the scheme for color images by reversibly embedding data in each color component individually, which also increases the capacity of data to be hidden. The common approach for high capacity reversible data embedding is to select an embedding area (for example, least significant bit of some pixel) in an image, and embed both the payload and the original values in this area. We have employed the method to extract the smoother area in an image so that the RDH techniques can be employed comfortably on it. It includes dividing the image logically into smoother and complex block by defining a function to measure its first order smoothness (f value). The block whose f value is below the average value of first order smoothness function is considered for data hiding. Standard PSNR ratio can be used to compare the quality of cover image.

II. PROPOSED SCHEME

The proposed scheme combines two different approaches together that are reversible data hiding and visual cryptography which gives an efficient technique to overcome the limitations of existing schemes in the area of reversible data hiding. The proposed scheme suggests the novel approach for data hiding and image encryption. Different Reversible Data Hiding schemes studied in literature deals with finding the room for hiding the data in an encrypted image where image is encrypted first and then data is hidden into it by reserving the room. Since lossless vacating the room from the encrypted image is relatively difficult and sometimes inefficient thus proposed scheme apply a method of finding the room for data prior to the image encryption thus founded room can be used to hide the secret data. By reversing the order of encryption and data hiding we overcome the difficulty of finding the room for data from already encrypted image. In addition many schemes proposed in literature uses the standard ciphers for encrypting the image as after hiding the data the security of the cover image is also matter of concern. The scheme makes the use of color visual cryptography algorithm. The proposed scheme makes the use of enhanced Seiving-Division-Shuffling algorithm [10] for encrypting the image in lossless fashion.

Following figure gives the framework for proposed scheme. It involves five main steps; Reserving room for embedding data, Data Embedding in reserved room, Image Encryption using keyless SDS algorithm, and Original image recovery and Data extraction.

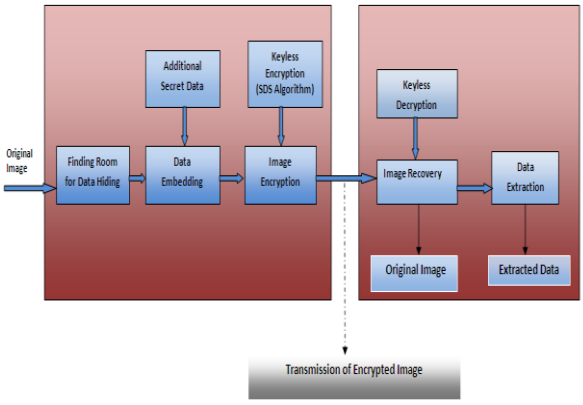

Fig: 1. Framework for proposed scheme

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

III. IMPLEMENTATION

Details of the algorithm involved in the proposed scheme are as follows:

A. Finding Room for Data Embedding
B. Improved High Capacity Data Embedding using Difference Expansion.
C. Image Encryption by dividing the image into Shares (using SDS)
D. Image Decryption (Image Retrieval)
E. Data Extraction

All the above stated steps can be implemented with the help of any programming language like Java, C# etc. Methods to be implemented are explained in the details of steps below:

A. Finding Room for Data Embedding

The common approach for high capacity data embedding is to find the room for embedding data. The scheme involves partitioning the image logically into the, the goal of image partition is to construct a smoother area B, on which RDH algorithm can achieve better performance. Let us consider there is original image C is a 32 bit color image with sized $M \times N$ and pixel $C_{i,j} \in [0,255]$, $1 \le i \le M$, $1 \le j \le N$. First, the content owner finds several blocks from the original image, along the rows, several blocks whose number is determined by the size of to-be embedded messages, denoted by *l*. Image will be divided into number of blocks evary block will be consisting of m rows, where $m = \left\lceil \frac{l}{N} \right\rceil$, and the number of blocks can be computed from $No\_Of\_Blocks = \lceil M/m \rceil$. For every block we define a function to measure its first order smoothness with the help of following function,

$$f = \sum_{u=2}^{m} \sum_{v=2}^{N-1} \left| C_{u,v} - \frac{C_{u-1,v} + C_{u+1,v} + C_{u+1,v} + C_{u,v+1}}{4} \right| \quad \text{----------(1)}$$

Higher f relates to blocks which contain relatively more complex textures. The content owner thus selects the blocks with relatively lower f value to be B which is logical smoother area to hide the data. For deciding over the smoother area the average value of f-value of all the blocks is considered and the blocks with f-value below average is considered to be relatively smoother

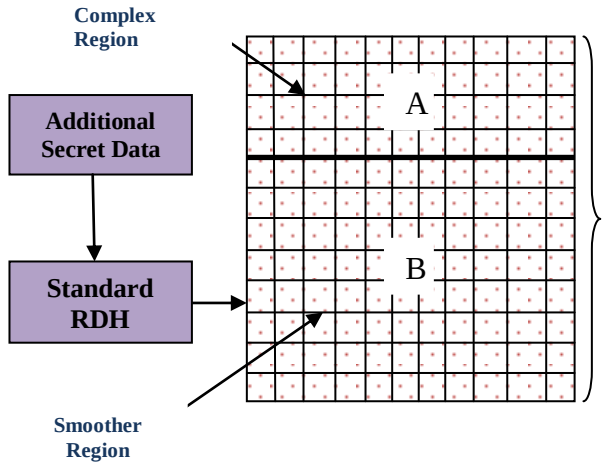

Fig: 2. General view of Logical partition of Image

$if (f - value_{i-block} < f - value_{avg})$ $then$

$block_{index}[i] = 1$
$else$
$block_{index}[i] = 0$

Thus blocks with index value 1 will be used for data hiding in the data embedding phase.

B. Improved High Capacity Data Embedding using Difference Expansion

Difference expansion is high capacity reversible data hiding technique introduced by Tian in [2] where it maintains the high visual quality of digital images which are used. We calculate some difference values for difference expansion. The technique discovers the extra storage space by exploring the redundancy in the image content. This technique was introduced by Tian[2] for the grayscale images where the payload capacity limit and the visual quality of embedded images of the DE method is one amongst the best in literature.

In proposed algorithm the data is embedded in each color components individually as the inputted image is a color image. Thus improved algorithm for reversible data hiding using difference expansion technique for color images is used here for embedding the data. In our implementation the blocks whose f-value < $fvalue_{avg}$ are considered for data hiding.

This data hiding scheme involves separating the Red Green and blue component of the image then considering each component of the color separately to hide the data into it. This increases the data embedding capacity of an image then the available schemes. The method of embedding is as follows:

Algorithm: Improved Difference Expansion Technique:
Input: Color Image
Process:

1. Find separate R, G, B components of an image, it will form three different matrices of three different color components like R-Matrix, G-Matrix, B-matrix.

2. Now apply the process of difference expansion for hiding data bits. Here pixel from only those blocks are used whose *f-value* lies below *f-avg*. These blocks are smoother than others. After using all possible pixels of R-component of a block, G-component is considered then B-component is used.

3. Convert the text into binary then considering bits from the binary data one by one hide using Difference expansion based technique 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

Original Image ted first

$+ b)/2], y = a - b$

where $\lfloor . \rfloor$ represents the floor operation which rounds 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:

$$y' = 2 \times y + x$$

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

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

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

Output: Image with hidden data.

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.
3. If certain block is completely used then the other block is taken under consideration. Likewise complete data file is hidden in the image blocks.

C. Image Encryption by dividing the image into Shares (using SDS)

Existing reversible data hiding schemes the design of an encryption algorithm must provide security against unauthorized attacks. Key oriented algorithms are very efficient but they were very bulky to manage as key handling must be done. To improved quality of existing system, keyless random hiding techniques can be used. Techniques of keyless encryption of images allow secure transmission of image. Random hiding is a technique that embeds the important text into a cover image such that the important images are imperceptible and can be securely transmitted to the receiver.

In the proposed scheme we are using the novel visual cryptography algorithm for image encryption. Visual cryptography involves secret sharing of image by dividing it into multiple shares. Then those shares are transmitted or stored on different places in the storage server for security; the original image could not be reconstructed unless we have all the shares with us to combines. Thus the method provides the security to the image in the sense that image so divided into shares is protected and for regeneration all the shares are required.

This scheme does not involve use of keys for encryption, has low storage and bandwidth requirements, while also keeping the computation cost during encryption/ decryption low, the proposed technique is implemented with the SDS algorithm and involves three steps[10].

In step one i.e. sieving, the secret image is split into primary colors. In step two i.e. Division, these split images are randomly divided. In step three i.e. Shuffling, these divided shares are then shuffled each within itself. Finally these shuffled shares are combined to generate the desired random shares[10].

The scheme implemented using the SDS (Sieve, Division, Shuffle) algorithm involves the following three steps:

Sieving: Sieving as the name suggests involves filtering the combined RGB components into individual R, G and B components (as shown in Figure 3). The granularity of the sieve depends the range of values that R/G/B component may take individually. To make the process computationally inexpensive, sieving uses the XOR operator.

Division: Having filtered the original image into the R, G and B components, the next step involves dividing the R, G and B components into D parts or shares each.

R (R_A, R_B, R_C, R_D)

G (G_A, G_B, G_C, G_D)

B (B_A, B_B, B_C, B_D)

While dividing it is ensured that each element in $R_{A\text{-}D}$, $G_{A\text{-}D}$ and $B_{A\text{-}D}$ is assigned values randomly, such that the entire domain is available for randomized selection; in case x = 8, then individual elements should be randomly assigned a value varying from 0- 255. The shares so generated should be such that (R_A, R_B, R_C, R_D) should regenerate R and similarly for G/B components. The shares so generated should be such that (R_A,---------- R_D) should regenerate R and similarly for G/B components.

Shuffling: Though experimental results have shown that the random shares created by division in no way exhibit any resemblance to the original image, but as a second step towards randomizing the generated shares i.e. $R_{A\text{-}D}$, $G_{A\text{-}D}$ and $B_{A\text{-}D}$, we perform the shuffle operation. This involves shuffling the elements in the individual shares.

Having carried out the above three operations the generated shares are combined to generate the final z random shares (RS).

$RandomShare_A \rightarrow (R_{A\text{-}shuffle}, G_{A\text{-}shuffle}, \text{and } B_{A\text{-}shuffle})$

$RandomShare_B \rightarrow (R_{B\text{-}shuffle}, G_{B\text{-}shuffle}, \text{and } B_{B\text{-}shuffle})$

--- --- --- --- --- --- --- --- --- --- --- --- -- --- --

$RandomShare_D \rightarrow (R_{D\text{-}shuffle}, G_{D\text{-}shuffle}, \text{and } B_{D\text{-}shuffle})$

The random shares so generated individually convey no information about the secret image, however to recover the original image all the random shares would be required. In our proposed scheme there are no keys involved and hence there is no key management. All that is required is to transmit one of the random shares on a secret channel while transmitting the rest on an unsecure channel.

D. Image Decryption (Image Retrieval)

Image retrieval involves the reverse of operation that we have performed in the image encryption process. That involves sieving the random shares and retrieving $R/G/B_{(A\text{-}Shuffle)}$, $R/G/B_{(B\text{-}Shuffle)}$, $R/G/B_{(C\text{-}Shuffle)}$, $R/G/B_{(D\text{-}Shuffle)}$ then from individual shuffle shares the original $R_A G_A B_A$, $R_B G_B B_B$, $R_C G_C B_C$ and $R_D G_D B_D$ are generated. And using this original image can be generated. The retrieved image is same as original and no loss of picture quality occurs. Thus this scheme involves no use of keys while encryption and decryption and keeps computation cost during encryption and decryption low.

E. Data Extraction

After we get all the shares of the image the image can be reconstructed and from the reconstructed image the data can be retrieved. In the data retrieval process the new pixel value are considered and difference is calculated. The LSB of the difference is the bit which was hided. For this the 'data retrieval method' require the index position of those blocks which were considered in hiding process and the pixel pairs position where the data is hidden as the input.

Algorithm:

Data_Extraction(image,blocks_index_pos[],pos_pixel_pairs[])

Input:

Image after the reconstruction phase which has data hidden in selected blocks

Parameters:

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

-Index position of blocks that are used for hiding data.
-Position of pixel pairs whose difference is expanded satisfying the overflow and underflow condition.
Process:
1. Again separate the R-G-B component matrix of the image blocks.
2. Apply the following process on considered pixel pairs. In extraction phase, the average and the difference of the pixels (a', b') are also calculated first

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

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

$$a = LSB(y'), y = \lfloor y'/2 \rfloor$$

And the original pixels can be restored by:

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

4. By above process the one by one bit will be extracted from the pixel pairs.
3. Then applying the proper encoding technique generates the characters for the extracted binary data bits to get the hidden text.

IV. CONCLUSION

Proposed scheme gives a completely new framework for reversible data hiding. Partitioning the image logically into smoother and complex region improves the performance and efficiency of RDH algorithm. Reserving room from encrypted image is relatively difficult and sometimes inefficient; the proposed scheme reserves the room before encryption. Then for hiding data improved Difference expansion technique is used which increases the data hiding capacity by hiding data in separate color component. In the proposed scheme the .txt file of huge size can be hidden by maintaining the quality of retrieved image.
Providing the security to the image is also a major area of concern when its storage or transmission is considered. For image encryption after hiding a data instead of using any standard cipher, a method of visual cryptography is used. For retrieving the complete image, all the random shares will be required. Image so retrieved will be same as original image. Proposed scheme guarantees the lossless retrieval of the image so as data. After retrieving the image hidden data will be extracted lossless.
In our proposed technique both during encryption and decryption the computation cost is low since the majority operations involved use logical XOR, OR and AND. There are no keys involved in the proposed scheme for encryption/decryption hence there is no key management. The scheme is robust to withstand the brute force attacks. The scheme is suitable for authentication based application or where trust cannot be reposed in any one participant for decision making and collective support is required to proceed, in such situation the important authentication related data like any password string or code can be hidden into the image and image can be divided into random shares then those shares are distributed to the trusted partners whenever the code has to be retrieved all the shares from all partners will be required no partner can individually take any decision.

V. FUTURE WORK

In our previous paper we have given the detail survey of various reversible data hiding schemes and also presented the comparative analysis of those schemes. In this paper details of algorithms used in proposed scheme has been explained. In our next paper we are going to show actual implementation of the proposed algorithm. For proving the performance of the method the PSNR value of an original image and data hided image is considered and to prove the performance of reconstruction of image scheme the PSNR of original image and reconstructed image is considered.
The PSNR of the original image and data hided image should be maintained >40db and to prove that after the data is retrieved, the reconstructed image is same as original image, the PSNR should be infinity. This can be proved with proper implementation of the algorithm.

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] J.H. Hwang , J.W. Kim and J U Choi, "A Reversible Watermarking based on Histogram Shifting", IWDW 2006 LNCS 4283, PP.348-361, 2006

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

[5] Kuo Hui ll, Shuenn Shyang Wang, "Reversible Data Hiding based on CSD data Representation and an interleraving interger Transform", Thesis for master of science, Graduate Institute of Communication Engineering, Tatung University

[6] Wen Chung Kuo, Po Yu Lai, Lih Chyau Wuu, *"Adaptive Reversible Data Hiding Based on Histogram"*, 10th International Conference on Intelligent Systems Design and Application, © IEEE 2010 (2002) The IEEE website. [Online]. Available: http://www.ieee.org/

[7] 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)

[8] 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.

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

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

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

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

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

[14] 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

[15] Wen Chung Kuo, Po Yu Lai, Lih Chyau Wuu, *" Adaptive Reversible Data Hiding Based on Histogram"*, 10th International Conference on Intelligent Systems Design and Application, © IEEE 2010

[16] Zhenfei Zhaoa,b, Hao Luoc, Zhe-Ming Luc, Jeng-Shyang Pan, "*Reversible data hiding based on multilevel histogram medication and sequential recovery*", International Journal on Electronic and communication, Z. Zhao et al. / Int. J. Electron. Commun.(AEÜ) 65 (2011) 814–826

[17] C. Vinoth Kumar, V. Nataranjan and Deepika Bhogadi, "*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

[18] 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

[19] 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

[20] 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).

[21] 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