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. 2, Issue 1, January 2014

Reversible Data Hiding using Visual Cryptography: A Review

Shruti M. Rakhunde[1]

Assistant Professor, Dept of MCA, Shri Ramdeobaba College of Engg. and Mgmt., Nagpur, India[1]

ABSTRACT: Data security and data integrity are the two challenging areas for research. There are so many research is progressing on the field like internet security, steganography, cryptography. Data hiding are a group of techniques used to put a secure data in a host media with small deterioration in host and the means to extract the secure data afterwards. Reversible data hiding is a technique to embed additional message into some distortion-unacceptable cover media, such as military or medical images, with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. The reversibility means not only embedding data but also original image can be precisely recovered in the extracting stage. Most hiding techniques perform data embedding by altering the contents of a host media. These types of data hiding techniques are thus irreversible. However in a number of domains such as military, legal and medical imaging although some embedding distortion is admissible, permanent loss of signal fidelity is undesirable. This highlights the need for Reversible (Lossless) data embedding techniques. This paper gives a review on various reversible data hiding techniques and also proposes a novel approach for reversible data hiding using visual cryptography. This involves no use of keys thus keeping the computation cost for encryption/decryption low. This scheme applies a method of vacating the room for data prior to the image encryption 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.

Keywords: Reversible Data Hiding, RDH, SDS

I. INTRODUCTION

For 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 stegno- image. Data hiding conceals the existence of secret information 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. 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*

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. 2, Issue 1, January 2014

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 and, 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.

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. 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].

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] has 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.

D. *Measuring 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 are 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.

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. 2, Issue 1, January 2014

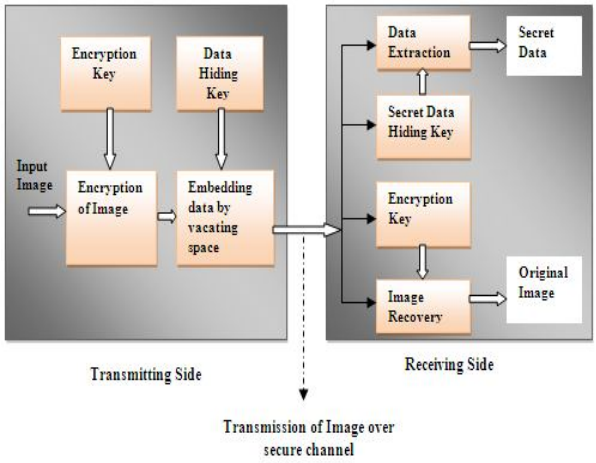

Fig. 1: Vacating Space after Encryption for RDH

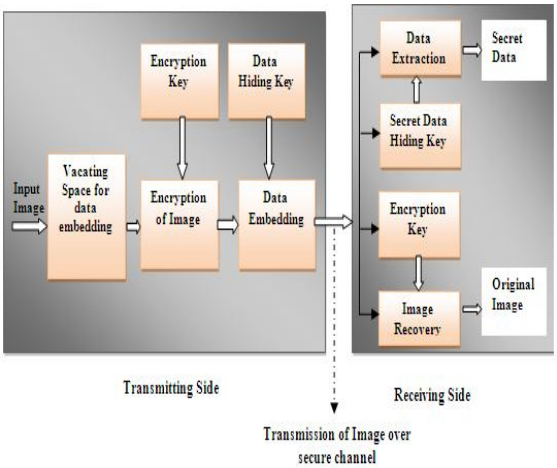

Fig. 2: Vacating Space before Encryption for RDH

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

The organization of the paper is as follows: section II discusses the related work, section III describes the basic techniques of RDH, section IV gives overview of Visual cryptography approach, section V describes the proposed scheme, finally section VI discusses overall conclusion.

II. 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 [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 [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-Chyau Wuu 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 a new scheme was proposed based on histogram and slope method. This method keeps the embedding capacity high and also maintains the high quality of stegno-image.

In [6] Kuo-Ming, Wen-Kai Su, Ting-Wen Chen, Li-Ming Chen has proposeda method that combines reversible data hiding, halftoning and vector quantization (VQ) technique to embed a grayscale image in other image. In embedding,

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. 2, Issue 1, January 2014

first use halftoning to compress the image from grayscale to halftone. Next, compute the difference between original image and one which inversed by LIH. Employing the VQ compress the difference and embed it with secret data. 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 [8] 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.

Proposed scheme is combining two different approaches together that are reversible data hiding and color visual cryptography. Visual cryptography was introduced by Naor [9]. 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 [11] 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 [12] Wei Qiao, Hongdong Yin, Huaqing Liang has proposed a new secret visual cryptography scheme for color images based on halftone. Firstly a chromatic image is decomposed into three monochromatic images in tone cyan, magenta and yellow. Secondly, these three images are transformed into binary images by halftone technique. Finally, the traditional binary secret sharing scheme is used to get the sharing images.

Yi-Hui Chen, Ci-Wei lan and Chiaio-Chih Huang in [13] 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.

III. 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

A. 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

B. Difference Expansion Based Technique

Difference expansion based techniques used 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.

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. 2, Issue 1, January 2014

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

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:

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

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

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

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

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

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

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

And the original pixels can be restored by:

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

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.

C. Histogram Shifting Based Technique

The histogram shifting [16, 17, 18] 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 is 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.

D. Prediction Error Based Technique

Reversible data hiding [19, 20] 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 $p'(x, y) = p(x - 1, y)$.

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. 2, Issue 1, January 2014

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

E. Vector Quantization based Technique

This scheme is based on compression of image [21]. 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 rate 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

IV. VISUAL CRYPTOGRAPHY

Visual Cryptography is an emerging cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by human visual system, without the aid of computers. It uses a simple algorithm unlike the complex. It needs neither cryptography knowledge nor complex computation. Visual cryptography technique (for black and white images) is introduced by Naor and Shamir in 1994 during EUROCRYPT'94. For security concerns, it also ensures that hackers cannot perceive any clues about a secret image from individual cover images. Any visual secret information (pictures, text, etc) is considered as image and encryption is performed using simple algorithm to generate n copies of shares depending on type of access structure schemes. The simplest access structure is the 2 out of 2 scheme where the secret image is encrypted into 2 shares and both needed for a successful decryption. These shares are random dots without revealing the secret information. Basic visual cryptography is expansion of pixels.

Visual cryptography is a method of sharing a secret image among a group of participants, where certain group of participants is called as qualified group who may combine their shares of the image to obtain the original, and certain other group is defined as forbidden group who cannot obtain any information on the secret image, even if they combine knowledge about their parts. The scheme gives an easy and fast decryption process that is done by stacking the shares onto transparencies to reveal the shared image for visual inspection.

.

V. PROPOSED SCHEME

The proposed method combines the benefits of two different approaches together that are reversible data hiding and visual cryptography to give a novel reversible data hiding scheme. This gives an efficient solution to overcome the limitations of existing schemes in the area of reversible data hiding. Following figure gives the framework of proposed scheme.

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. 2, Issue 1, January 2014

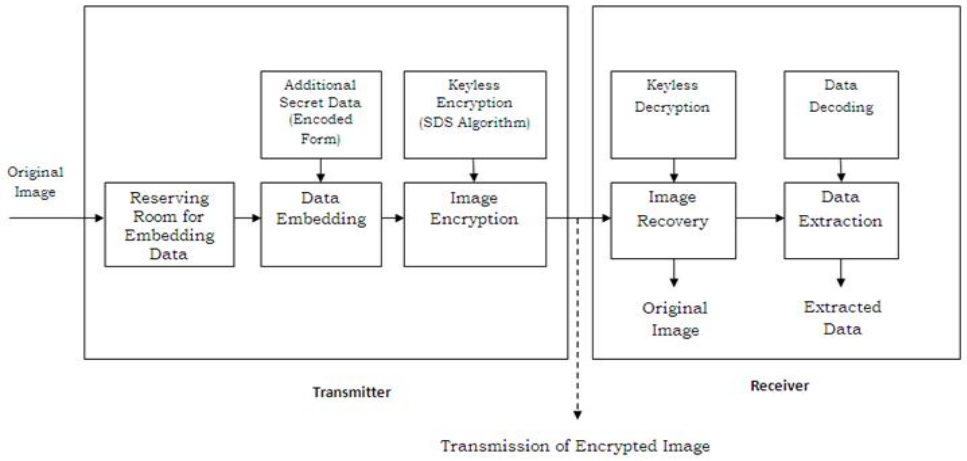

Fig.3: Framework of Proposed Scheme

The proposed scheme suggests the novel approach for data hiding and image encryption. In the proposed scheme we used the concept of vacating the room for embedding data in the image before encryption. Since losslessly vacating the room from the encrypted image is relatively difficult and sometimes inefficient thus proposed scheme apply a method of vacating the room for data prior to the image encryption, thus vacated 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. For image encryption instead of using any standard cipher, a method of visual cryptography is used. In visual cryptography approach the image is divided into random shares and for retrieving the image all the shares will be required. This encryption scheme does not involve the use of keys for encryption, has low storage and bandwidth requirements, while also keeping the computation cost during encryption/decryption low. The scheme makes the use of color visual cryptography algorithm for encrypting the image after hiding the data. The proposed scheme makes the use of enhanced Seiving-Division-Shuffling [10] algorithm. The method aims at achieving complete reversibility with minimum computation by employing keyless approach of visual cryptography.

VI. CONCLUSION

Reversible data hiding in encrypted image is drawing lots of attention because of security maintaining requirements. Thus proposed scheme provides a completely new framework for reversible data hiding. Here in this approach we have used a new technique for reserving room before encryption of image. Thus the data hider can benefit from the space emptied out in previous stage before encryption to make data hiding process effortless. In the proposed approach we take advantage of visual cryptography for encrypting the image. Thus the image is protected in transmission and secret data is also transmitted securely. As this approach does not involve any use of keys is a keyless approach for image encryption, thus key management is not an issue but promises complete lossless image recovery and data extraction. The scheme is also robust to withstand brute force attack.

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 Jun Tian, “Reversible Data Embedding Using a difference Expansion”, IEEE Transaction on circuits and systems for video technology,

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. 2, Issue 1, January 2014

Vol.13, No. 8, Aug 2003

5 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/

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

15 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

16 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

17 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

18 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

19 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

20 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

21 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)