IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 39-44
www.iosrjournals.org

A Novel and Secure Approach for Reversible Data Hiding using Visual Cryptography

Prof. Monali C. Nikose[1], Prof. Mrunali L. Vaidya[2], Prof. Priyanka A. Jalan[3], Prof. Roshan V. Chaudhari[4]

[1]*Dept. of CE, Bapurao Deshmukh College of Engg. , Sevagram, Wardha(MS)*
[2]*Dept. of CE, Bapurao Deshmukh College of Engg. , Sevagram, Wardha(MS)*
[3]*Dept. of CE, Bapurao Deshmukh College of Engg. , Sevagram, Wardha(MS)*
[4]*Dept. of CE, Bapurao Deshmukh College of Engg. , Sevagram, Wardha(MS)*

Abstract: *Steganography is one form of data hiding, in which data is embedded in digital media. But in almost all forms of such data hiding, distortion can occur in the original cover media and cannot be restored to the original cover. Reversible data hiding is different from such form of data hiding, here additional message is embedded in cover media (distortion-unacceptable cover media), such as military or medical images, in reversible manner, so that the original cover content can be perfectly restored after extraction of the hidden message. 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 lossless recovered after data embedded is extracted while protecting the image content's as confidential. This paper provides the brief about various techniques of RDH.*

Keywords: *Reversible data Hiding, RDH, SDS*

I. INTRODUCTION

Reversible Data hiding can be also called as Reversible steganography; it is the method of hiding data inside a cover file so that both the cover file and data could be recovered lossless at the receiver side. The transmitting side of such systems involves a cover image, encryption key, additional data and data hiding key. In the original image before hiding data image will be encrypted, data will then be hidden into it and then image will be transmitted to another side. The receiving side thus needs to decrypt the image and extract the data from it. Information and data security have always been a vibrant area of research. In the area of data security various traditional approaches like Steganography, Cryptography, Encryption 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. Cryptography protects the content of messages while data hiding conceals the existence of secret information. As retrieving data from encrypted image can be difficult more and more attention is paid to reversible data hiding in images before encryption.

Reversible data hiding (RDH) 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 lossless after the data have been extracted. The transmitting side of such systems involves a cover image, additional data, data hiding key and encryption key. The original image will be encrypted first, data will be hidden into it and then image will be transmitted to other end, this is general type of RDH. The receiver thus needs to decrypt the image and extract the data from it. The reversibility means that not only the embedded secret data but also the encrypted cover image must be extracted lossless at the receiver side. Let take an example, suppose a medical image database is stored in a data center and server in the data center, and embed any 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.

The RDH can become a promising secret communication channel since there is no visual discrimination observed 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 Methods for hiding data in the cover image, finally section VI discusses overall conclusion.

II. RELATED WORK

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 [6] 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 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 [8] 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 gray scale image in other image. In embedding, first use halftoning to compress the image from gray scale 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. 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 [10] 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.

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 [12] has proposed another promising approach for color visual cryptography which involve 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.

III. BASIC RDH METHODS

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

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

A. LSB Modification

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

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

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

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:

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

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

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

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. 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

Reversible data hiding 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: horizontal predictor, vertical predictor, etc.

IV. VISUAL CRYPTOGRAPHY

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. The technique was proposed by Naor and Shamir in 1994. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images and layers are required to reveal the information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet. Information is increasingly important in our daily life. Information gets more value when shared with others. Due to advances in technologies related to networking and communication, it is possible to share the information like audio, video and image easily. It may give rise to security related issues. Attackers may try to access unauthorized data and misuse it. To solve this problem certain techniques are required. Techniques to provide security, while sharing information are termed as Secret sharing schemes. When it comes to visual information like image and video, it is termed as Visual secret sharing scheme. Visual cryptography (VC) is a technique used for protecting image-based secrets. The basic concept of visual cryptography scheme is, to split secret image into some shares, which separately reveals no knowledge about the secret information. Shares are then distributed to participants. By stacking these shares directly, secret information can be revealed and visually recognized. All shares are

necessary to combine to reveal the secret image. Starting from the basic model, many visual cryptographic techniques have been evolved day by day.

V. METHODS 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. Following is the method which encrypts the image first then hides the data, as shown in the fig 1 below, the content owner first encrypts the original image using a standard cipher with an encryption keyt. 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].

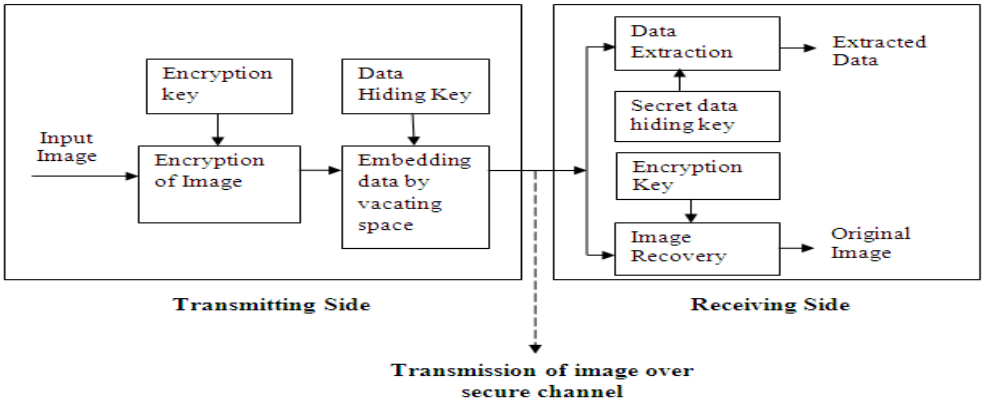

Fig. 1: Method 1: Vacating Space after Encryption for RDH

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. 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. This approach is used in [5] with the following in fig 2. Thus using this method the data hider gets extra space vacated out before encryption thus making data hiding process effortless. This approach is very useful and promising.

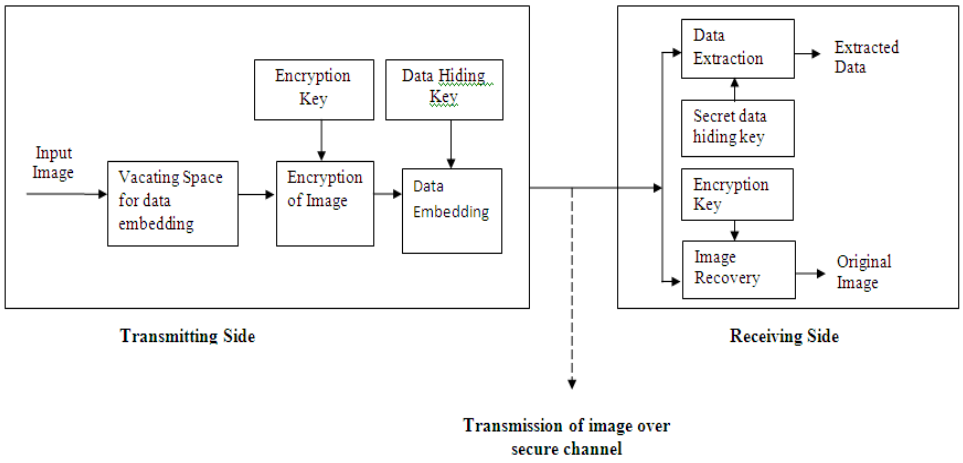

Fig. 2: Vacating Space before Encryption for RDH [5]

A. ***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.
- *Security of Cover Image:* The cover image which consists of data should be kept secure in transmission.

B. ***Visual Cryptography***

In RDH mostly traditional way of encryption is used to secure the cover image but RDH can also be combined with various visual cryptography algorithms to give more secure way of data transmission [5]. Like in [5] the SDS algorithm of Visual Cryptography is used to add more secure approach to RDH. This visual cryptography algorithm involves the three main steps Sieving, Division and Shuffling. **Sieving** as the name suggests involves filtering the combined RGB components into individual R, G and B components. Having filtered the original image into the R, G and B components the next step involves **dividing** the R, G and B components into parts or shares. The next step is shuffling the elements in the individual shares. The sequence in which the elements within the shares are shuffled depends on the value of one of the shares generated from the same primary color. After performing the above operation the generated shares are combined to form final z random shares. 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. After regenerating the image from random shuffled shares then the data can be retrieved.

The technique used to encrypt the image by generating random shares involve minimal computing for regenerating the original secret image without any loss of image quality. This framework provides two level securities first for embedded data and another for secret image. Both the secret data and original cover image will be retrieved lossless.

SDS algorithm involves following basic steps:

Sieving:

- Sieving as the name suggests involves filtering the combined RGB components into individual R, G and B components.
- 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 z parts/ shares each.

R _ (R_A, R_B, R_C,----------, R_Z)
G _ (G_A, G_B, G_C,----------, G_Z)
B _ (B_A, B_B, B_C,----------, B_Z)

- While dividing it is ensured that each element in R_{A-Z}, G_{A-Z} and B_{A-Z} 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_Z) should regenerate R and similarly for G/B components.

Shuffling:

- Thus 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-Z}, G_{A-Z} and B_{A-Z}, we perform the shuffle operation.
- This involves shuffling the elements in the individual shares. The sequence in which the elements within the shares are shuffled depends on the value of one of the other shares generated from the same primary

color. In other words R_B decides how R_A is shuffled, RC decides how R_B is shuffled, ---------- R_Z decides R_{Z-1} is shuffled and R_A decides how Rz is shuffled.

- The shuffling operation uses the comparison operator on the LSB of the determining element to decide the shuffle sequence.

Combine:

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

  RS_A _ ($R_{A\text{- shuffle}}$, $G_{A\text{- shuffle}}$ and $B_{A\text{- shuffle}}$)
  RS_B _ ($R_{B\text{- shuffle}}$, $G_{B\text{- shuffle}}$ and $B_{B\text{- shuffle}}$)
  - - - -
  RS_Z _ ($R_{Z,\text{- shuffle}}$ $G_{Z\text{- shuffle}}$ and $B_{Z\text{- shuffle}}$)

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. For image decryption all the shares are required.
As shown in the figure proposed scheme combines RDH approach with SDS thus data which is hidden in the image will be extracted only after the original image is recovered.

VI. CONCLUSION

Reversible data hiding in encrypted images is a new topic drawing attention because of the privacy-preserving requirements from cloud data management. RDH can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy. Furthermore, RDH method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images. Also in this we survey different techniques for data hiding along with SDS algorithms.

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, Vol.13, No. 8, Aug 2003.

[5]. Shruti M. Rakhunde, Archana A. Nikose, "New Approach for Reversible Data Hiding Using Visual Cryptography", IEEE International Conference on Computational Intelligence and Communication Networks 2014, Print ISBN: 978-1-4799-6928-9, Pages 846 – 855

[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]. Shruti M. Rakhunde, Archana A. Nikose, "Reversible Data Hiding using Color Visual Cryptography", International Journal of Advance Foundation and Research in Computer (IJAFRC), Volume 1, Issue 2, Feb 2014. ISSN 2348 – 485

[8]. 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).

[9]. 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.

[10]. 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.

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

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

[13]. Shruti M. Rakhunde, Archana A. Nikose, "A Novel and Improved Technique for Reversible Data Hiding using Visual Cryptography", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 6, June 2014, ISSN (Online) : 2278-1021, ISSN (Print) : 2319-5940