Efficient Data Security System Using Room Reservation Approach on Digital Images for Secret Sharing using Color Visual Cryptography

Aparna T. Deshmukh[1], Jyoti Raghatwan[2]

[1]M.E. Semester-III student, Dept of CSE, RMD Sinhgad School of Engineering, Pune, India

[2]Assistant Professor, Department of CSE, RMD Sinhgad School of Engineering, Pune , India

Abstract: *Reversible data hiding is the technique in which the cover image can reversibly be retrieved after the extraction of hidden data in it. This technique provides secrecy for data, and for its cover image. All the previous methods of reversible data hiding were vacating room for data hiding after encryption process, which leads to introduction of some error rates at the time of data extraction and image restoration. Here we have described a novel method of reversible data hiding in which, Reserving room before encryption (RRBE) in images using visual cryptography, so that image extraction will be error free. Also here we are proposing an LSB replacement method for the data hiding, which will result in more space for embedding secret data.*

Keywords: Reversible data hiding, RRBE, LSB replacement, visual cryptography

1. Introduction

Data security means safeguarding data from unauthorised users or hackers and providing high security to prevent misuse of data. The area of data security gained more significance due to the enormous increase in data transfer rate over the internet. In order to enhance the security during communication through the internet, many techniques such as cryptography, steganography have been developed.

Data hiding is a form of steganography, in which data is embedded in digital media. In most cases of data hiding, distortion can occur in the original cover media because of data hiding and cannot be restored to the original cover. In various applications, such as medical diagnosis and law enforcement, it is necessary to recover the marked media back to the original cover media after the embedded data are retrieved for some legal considerations.

A. Reversible Data Hiding

Reversible data hiding is defined as a technique in which the data is hidden in the host image that can be original cover image. A reversible data hiding is a technique, in which we can restore the original cover image without loss after extracting the hidden data. The sender side of such systems involves a cover image, additional data to be embedded, the encryption key and the data hiding key. The original image is encrypted, then the data needs to be hidden and after that image will be transmitted. The receiver thus needs to decrypt the image and data extraction .Reversibility means not only the embedded secret data but also the encrypted cover image must be extracted with preserved secrecy at the receiver side.

B. Two Basic Approaches to Hide Data in the Cover Image

Some of the previous methods in the area of RDH are based on the concept of hiding data in the encrypted image. Here the content owner first encrypts the original image using a standard encryption algorithm with an encryption key. After the encrypted version of the image is generated the space for storing the data is reserved from the image in a lossless manner [1]. The data hider can hide some secret data in the vacated space with the data hiding key. Then a receiver or any authenticated user can extract the embedded data from encrypted image with the data hiding key and also the original image can be recovered without loss of quality by using the encryption key [1].
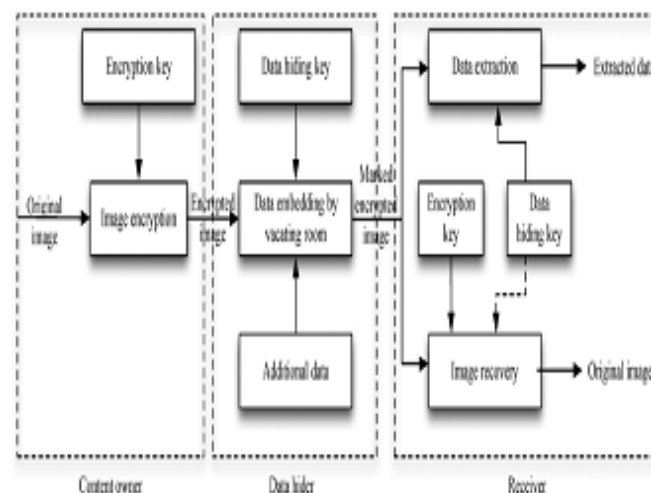
Figure 1: Vacating Space after Encryption for RDH

The above approach requires the lossless vacating of space from the encrypted image which is difficult and sometimes inefficient. Thus Kede ma. Weiming Zhang, Xianfeng Zhao, Nenghai Yu, Fenghua Li, in [1] proposed the approach of reserving room for embedding the secret data before image encryption. Here reverse order is followed. The approach is explained in fig 2. By using this method the data hider gets extra space vacated out before encryption thus making data hiding process effortless.
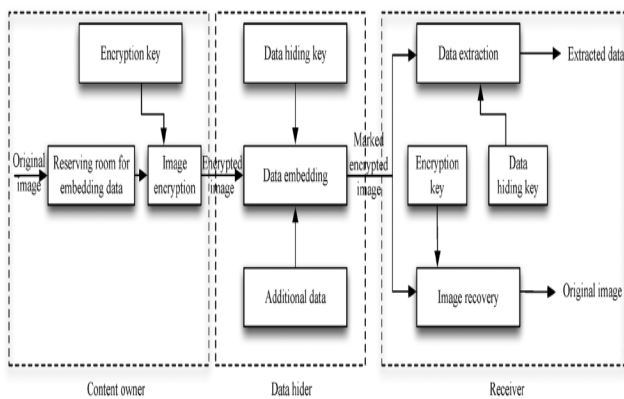
Figure 1: Vacating Space before Encryption for RDH

C. Performance of the RDH techniques

There are various methods used for reversible data hiding in image. All these methods considered provides one or the other advantage. There are different parameters on the basis of which the performance of these techniques can be measured. The following parameters must be considered:

A. *Quantity of Data:* It refers to the maximum amount of secret data that can be embedded in the cover image.
B. *Complexity of technique:* Simplicity and complexity of these techniques is also important measure as it may affect the usability of the techniques.
C. *Quality of cover image:* The distortion of the image after data extraction will not be accepted in RDH. Hence quality of image is an important measure.

The RDH can become a secret communication channel since there is no visual discrimination between the embedded image and original image. The paper is organised in the following sections: section II discusses the related work, section III describes the basic techniques of RDH, section IV describes the proposed scheme, section V discusses overall conclusion.

2. Related Work

Lots of research has been done in the area of reversible data hiding. Many efficient methods have been introduced for reversle data hiding and color image visual cryptography. Some work in area of reversible data hiding is as follows:

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

In [5] Wen-Chung Kuo, Po-Yu Lai, Lih-Chyau Wuu introduced a new methodology of adaptive reversible data hiding based on histogram. With the aim to enhance the data hiding capacity and embedding point adaptively a new proposed scheme was based on histogram and slope method. This method gives high embedding capacity and maintains the high quality of stegno-image.

In [1] Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu and Fenghua Li introduced a new method for reversible

data hiding for embedding data in an image by reserving room before encryption. As losslessly vacating room from the encrypted images is difficult and sometimes inefficient.

In the area of reversible data hiding José .R; Abraham .G, in [7] have proposed a novel scheme to reversibly hide data into encrypted greyscale image in a separate manner. Content owner firstly encrypts the image by permutation of pixels using encryption key. The data hider then hides the data into the image already in the encrypted version 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 extended color visual cryptography technique. Visual cryptography was proposed by Naor [8]. In a k-out-of-n scheme of VC, a secret binary image isencoded into n shares of random binary pattern. The n shares are Xored with n transparent factors, respectively, and distributed amongst n p end users. k or more users can visually reveal the secret image by superimposing any k transparencies together.

In [9] InKoo Kang, Gonzalo R. Arce , Heung-Kyu Lee introduced a color visual cryptography encryption method that produces meaningful color shares by visual information pixel synchronization and error diffusion halftoning.

In [10] Wei Qiao, Hongdong Yin, Huaqing Liang proposed a new secret visual cryptography scheme for color images based on halftone. First of all a colored image is decomposed into three monochromatic images in tone cyan, magenta and yellow. Then these three images are transmitted into binary images by halftone technique. Finally, the traditional binary to hide to get the sharing images.

3. RDH Techniques

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

A. LSB Modification Technique
B. Difference Expansion Based Technique
C. Histogram Shifting Based Technique

A. LSB Modification Technique
One of the widely used methods is the LSB (Least Significant Bit) modification. In this method, the LSBs of each signal sample is replaced by a data bit. During extraction process, these bits are read in the same order, and secret data is reconstructed finally.

B. Difference Expansion Based Technique
Difference expansion based techniques used in [13] was proposed by Tian]. In [12] Jui Tian introduced a difference expansion technique which finds extra storage space by exploring the redundancy in the content of image. The secret data embedding capacity limit and the visual quality of embedded images of the DE method also with a low computational complexity.

Paper ID: SUB14240

249

C. Histogram Shifting Based Technique

The histogram shift based reversible data hiding scheme [13,14,15,16] embed data by shifting the histogram into a particular direction. And there are two points which are important are to be considered in these schemes, which are the peak points and zero points. The peak point is for the grayscale value, corresponding to the maximum number of pixels in the histogram of the input image. The zero point is usually the point that the number in histogram is zero. And minimum number of pixels is selected as the zero point to increase the embedded capacity.

In the histogram-shifting 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 step of histogram shift algorithm is as follows:

1. Generate the histogram of image
2. Then find the peak points and zero points.
3. Assume the peak point as 'a' and the zero point as 'b'. Shift the points between ranges reducing by 1.
4. If the embedded bit is 1, the peak point is reserved; otherwise, we have to change the peak point value by reducing 1.

In order to achieve real reversibility requirements, the location of pixels in the minimum point must be recorded an embedded. Then record the peak point, the zero points and some other auxiliary information.

4. Proposed Methodology

The proposed method is combining two different approaches together that are reversible data hiding and color visual cryptography which gives an efficient technique to overcome the limitations of existing schemes in the area of reversible data hiding. The proposed scheme gives the novel approach for data hiding and image 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 embedding data prior to the image encryption [1], thus vacated room can be used to hide the secret message. Here we are reversing the order of encryption and data hiding so that we overcome the difficulty of reserving room for data in the encrypted version of image. The use of color visual cryptography algorithm. The proposed scheme makes use of enhanced visual cryptography algorithm for deviding the image in two shares data is protected using standard encryption algorithm, image encryption can be done by standard encryption algorithm such as AES or by visual cryptography where shares of original image are secured using public key encryption. The proposed scheme makes the use of enhanced algorithm. The method aims at achieving complete reversibility with minimum computation.

Following figure gives the framework for proposed scheme. The steps are; vacating room for data embedding, Data Embedding in the already reserved room, Image Encryption and Original image recovery and data extraction.
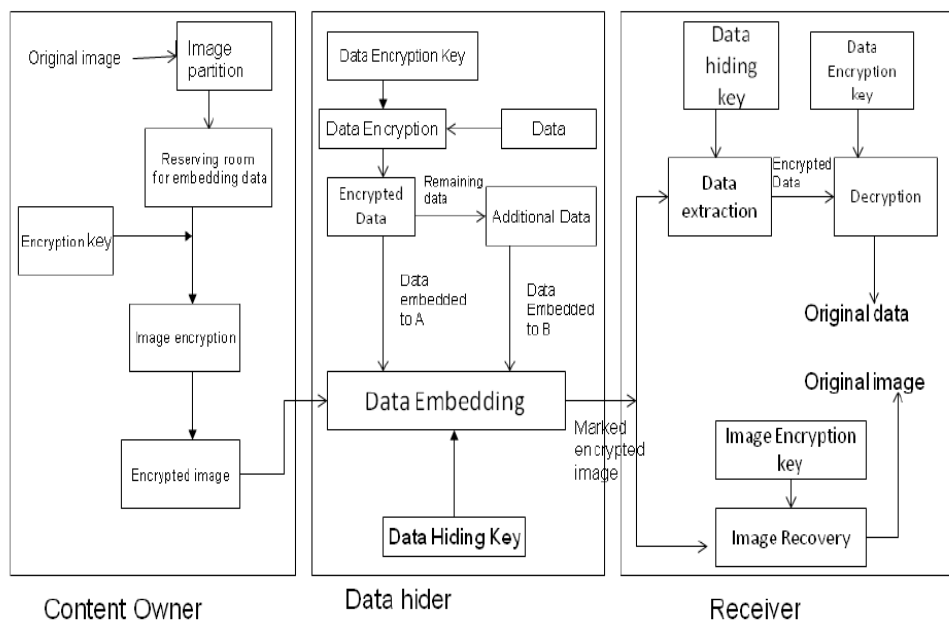

Figure 3: Framework for Proposed Scheme

5. Conclusions

The Reversible data hiding in encrypted image is drawing lots of attention because the security maintaining requirements are growing rapidly. 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 image encryption. Thus the data hider is benefited from the extra space emptied out in previous stage before encryption to make data hiding process relatively easy and efficient. In the proposed approach we take advantage of visual cryptography approach for image encryption. Thus the image is secured during transmission and secret data is also transmitted securely. Confidentiality of image and data is maintained.

References

[1] Kede Ma. Weiming Zhang, Xianfeng Zhao, Nenghai Yu,Fenghua Li, "Reversible Data Hiding in Encryted Images by Reserving Room Before Encrytion", 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", Internatoional Conference on Microelectronics, Communication and Renewabble Energy, ICMiCR-2013

[3] W. Hong T. Chen and H. Wu, "An improived 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, 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] 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.

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

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

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

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

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

[13] 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

[14] 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

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

[16] 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

Paper ID: SUB14240

251