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. 3, Issue 6, June 2015

Reversible Data Hiding in Encrypted Images Using Room Reservation Approach and Visual Cryptography for Color Images

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

M.E. Student, Dept. of CSE, RMD Sinhgad School of Engineering, Pune, India[1]

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

ABSTRACT: Information embedding systems in digital images, have various important multimedia and high precision applications. Such systems embed one signal into another.In recent years, more attentiveness is paid towards Reversible Data Hiding (RDH) in encrypted images.The reason behind is, it maintains the property that the original cover can be losslessly recovered after the embedded secret data is extracted while preserving the image content's secrecy. All the previous methods of reversible data hiding were vacating room for data hiding after encrypting the image , which results in the introduction of some error rates at the time of data extraction and image recovery.This paper presents a new technique for Reversible Data Hiding which can recover the original image after hidden data have been extracted successfully. Here a method for hiding data in an encrypted image is used with the concept of reserving room before encryption and also makes use of a new method for encrypting the image using color visual cryptography. This method aims to extract the correct data and the original cover in order to preserve the security for data and the cover media.

KEYWORDS: Reversible data hiding(RDH), RRBE, LSB replacement, visual cryptography.

I. INTRODUCTION

Communication is one of the most important needs of people to carry out their day –to-day work. People are using different devices such as the mobile phones, laptops etc. These devices makes use of network to ease the communication. Security can be ensured with the use of techniques like setting passwords, biometric authentication etc. but the major challenge at network level security that the world is facing is data security. Data security means protecting data from unauthorised access and providing high security to prevent misuse of data. The area of data security gained more significance in recent years due to the enormous increase in data transfer rate over the communication network. In order to increase the security during communication through the internet,many techniques for data hiding have emerged.

Data hiding is one form of steganography, in which data is embedded in digital cover media. In many 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, as the medical diagnosis and law enforcement, it is necessary to recover the encrypted media back to the original cover media after the embedded data are retrieved for some legal considerations.

Data hiding is a process used to hide data into the cover media. In most of the cases of data hiding process, the cover media becomes distorted due to data hiding in it and cannot be reversed to the original cover media. Hence, cover media has permanent distortion even after the extraction of hidden data from it. In the applications, such as medical diagnosis and law enforcement techniques it is desirable that the original cover can be recovered with no loss. Techniques that satisfy this requirement are referred to as reversible, lossless or distortion free. Thus, reversible data hiding technique not only provides security for embedded data but also preserve secrecy for the encrypted cover media and maintains integrity.

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. 3, Issue 6, June 2015

Various techniques are used for reversibly hiding data in the cover media or image. These techniques provide one or other benefit on use. The importatnt feature of RDH technique is the reversibility.Image is retrieved in a lossless manner and then the secret data which was embedded is extracted.

Reversible data hiding (RDH) is a technique which can transfer the secret message or data from the content owner to the authorized recepient with the use of carrier media.This enables privacy preservation in transferring the data via the communication network. In recent years, this technique is used in information security and forensics,also the highly confidential data. Therefore, confidentiality and authentication plays significant role in transmitting the confidential data over the networks. The hiding technique first encrypts the original image using various encryption algorithms and by using cryptographic techniques after that the secret data is embedded in the cover image. At last the authorized user receives the image and by applying the same techniques used reversibly in order to extract the cover image and secret message.

II. RELATED WORK

Various techniques has been proposed and research is done in the area of reversible data hiding. Also many advanced methods have been introduced for reversible data hiding and visual cryptography. Some research work in the area of reversible data hiding is illustrated below:

In [11] Jun Tian has introduced a difference expansion technique which finds extra storage space by exploring the redundancy in the image content. Here the secret data embedding capacity limit and the visual quality of embedded images of the DE method are with a low computational complexity.

In [4] Wen-Chung Kuo, Po-Yu Lai, Lih-Chyau Wuu introduced a new methodology of adaptive reversible data hiding based on histogram shift. The aim was to enhance the data hiding capacity and embedding point adaptively a new proposed scheme was based on histogram and slope method. This method provides high embedding capacity and also maintains the high and better quality of stego-image.

In [1] Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu and Fenghua Li introduced a new method for reversibledata hiding for embedding data in an image by reserving room before encryption. Vacating room in lossless manner from the encrypted images is difficult and sometimes inefficient.

In the area of reversible data hiding Jose .R; Abraham .G, in [6] 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 the key for encryption . After which the data hider hidesthe data into the image already in the encrypted version by histogram modification based hiding by using data hiding key.

The method of Visual cryptography was proposed by Naor [7]. In a k- outof- n scheme of VC, a secret binary image is encoded into n shares of random binary pattern. These n shares are Xored with n transparent factors, and then distributed amongst n p end users. k or more users can visually reveal the secret image by superimposing any k transparencies together.

In [8] In Koo Kang, Gonzalo R. Arce , Heung-Kyu Lee introduced the new color visual cryptography encryption method that produces meaningful color shares by visual information pixel synchronization and error diffusion halftoning.

In [9] 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. These images are transmitted into binary by the halftone technique. And finally, the traditional binary to hide to get the sharing images.

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. 3, Issue 6, June 2015

III. PROPOSED SYSTEM

The two basic approaches that can be used in RDH are as follows:

- Vacating room for data hiding after image encryption.
- Vacating room in the image for data hiding before image encryption.

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

Based on this concept here reverse order of encryption and data hiding is used so that we can overcome the difficulty of reserving room for secret data in the encrypted image.With the use of color visual cryptography algorithm image is encrypted. The proposed method use the color visual cryptography algorithm for deviding the image in two shares, data is secured using standard encryption algorithm, image encryption can be done by standardencryption algorithm such as AES.The proposed smethodology uses the enhanced algorithm. This method aims at achieving complete reversibility with minimum computation.

The proposed method is the combination of two different approaches together that are : reversible data hiding and color visual cryptography which gives an new improved technique to overcome the limitations of the existing techniques in the area of reversible data hiding(RDH). The proposed methodology gives the new approach for data hiding and image encryption process. Losslessly reserving the room from the encrypted image is difficult and sometimes inefficient so proposed method apply a technique of reserving the room for embedding data prior to the image encryption [1], thus the reserved room can be used to hide the secret message.

This method makes use of color visual cryptography for image,AES algorithm for data encryption and also for encrypting the image.The main steps involved in this methodology are:

- Partitioning the image.
- Embedding A and B together by reserving room for data.
- Data encryption and image encryption.
- Data extraction and decryption and image recovery.

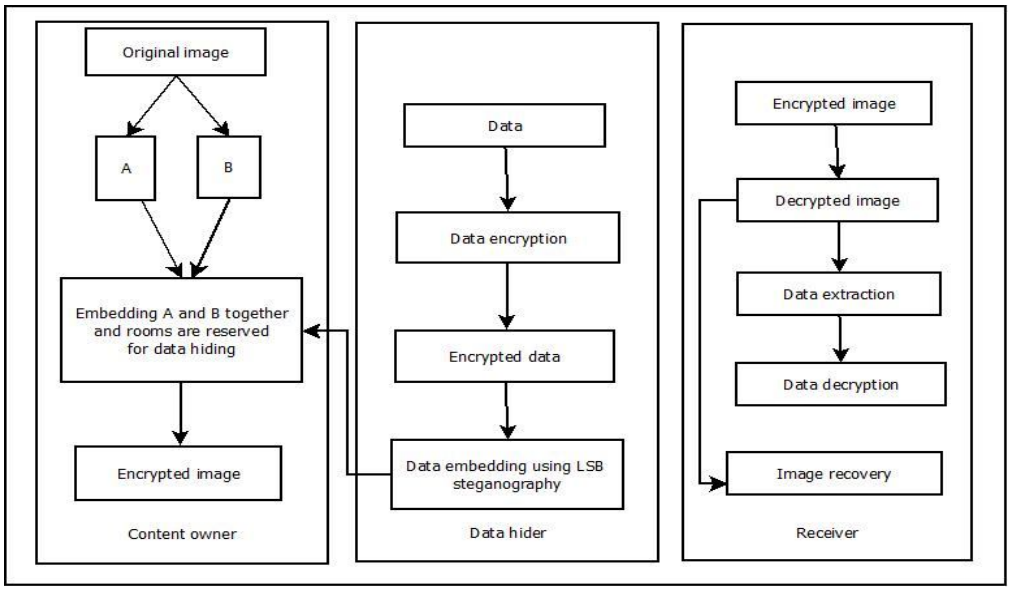


Figure 1. Framework for Proposed Scheme

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. 3, Issue 6, June 2015

The first step can be divided as: Image Partitioning and Self Reversible Embedding which is then followed by image encryption.Image partitioning step divides the original cover media or image into two shares using the color visual cryptography algorithm then, the two shares generated are embedded together and rooms are reserved for the purpose of data hiding and finally encrypt the new rearranged image to generate itsencrypted version.

The content owner encrypts the original image and hands over it to the data hider where he can embed some confidential data data the encrypted image by reserving room. Then the receiver, who may be the content owner or some other third party can extract the embedded secret data and recover the original image from the encrypted image with the help of encryption key.

IV. ALGORITHMS

The main algorithms used in the proposed work are illustrated in this section:

A. Visual Cryptography for color images

This algorithm devides the original image into two shares by converting it from *ARGB* to *CMYK* form as follows:

Input: ARGB image.

Process:

1. First the color pixel values are fetched from the image as *ARGB*(*alpha; red; green; blue*).
2. Then these *ARGB* values are seperated.
3. Convert the *ARGB* values to *CMY K*(*cyan; magenta; yellow; black*) values usingrelevant mathematics.
4. After this the *CMY K* values of pixels are devidedinto two splits as split A with values *CM* and splitB with values *Y K*.
5. Thus we get the two shares of image with share A as*CM* and share B with *Y K* color.

Output: Share A(*CM*) and share B(*YK*).

Relevant mathematics associated (*ARGB* to *CMYK* conversion formulae):

- The *R; G;B* values are divided by 255 in order to change the range from 0 to 255 to 0 to 1:
  R'= R/255
  G'= G/255
  B'= B/255
- The black key (*K*) color is calculated from the red(*R'*), green (*G'*) and blue (*B'*) colors:
  K=1-max (R',G',B')
- The cyan color (*C*) is calculated from the red (*R'*)and black (*K*) colors:
  C=(1-R'-K)/(1-K)
- The magenta color (*M*) is calculated from the green (*G'*)and black (*K*) colors:
  M=(1-G'-K)/(1-K)
- The yellow color (*Y*) is calculated from the blue(*B'*)and black (*K*) colors:
  Y=(1-B'-K)/(1-K)

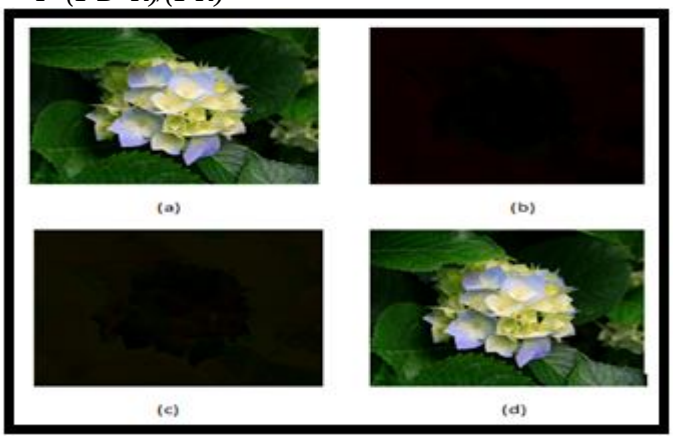


Figure 2. Visual cryptography output (a)Original image,(b)Share1(CM),(c)Share 2(YK),(d)Losslessly recovered image.

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. 3, Issue 6, June 2015

After getting the two shares, these shares are embedded together in an image and rooms are reserved for the secret data which is to be embedded.

B. AES algorithm for data and image encryption

For encrypting the secret data to be embedded the data is encrypted using the AES(Advanced Encryption Standard algorithm and also the image containing the secret data:

This algorithm is flexible as it supports any combination of data and also the key of size 128,192, and 256 bits. In AES a 128 bit length data which is divided into four blocks. These blocks can operate on array of bytes and organized as a 4 *4 matrix which is called as the state array.During encryption, the data is passed in iterative rounds.

In the round function this algorithm is comprised of four different byte transformations:

- Substitution using a substitution table.
- Shifting rows of the State array.
- Mixing of data within each column of the State array.
- Adding a Round Key to the State.

In case of data encryption we use the plaintext which is the secret message along with the username who is embedding that data and the time at that instance.

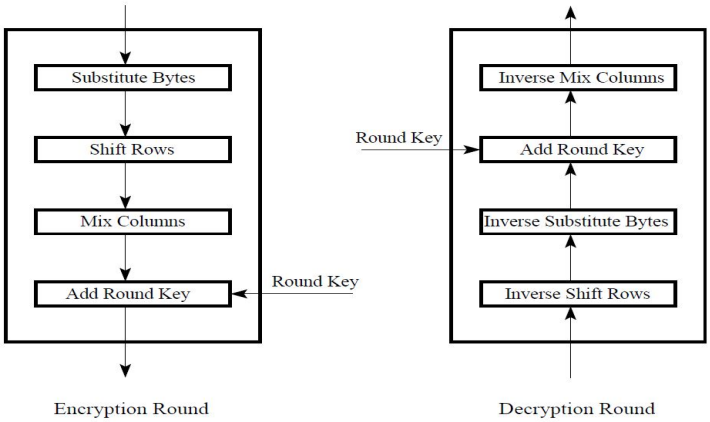


Figure 3. AES encryption algorithm.

C. LSB (Least Significant Bit) based steganography

It is the simplest and most common type of steganography,and is used to reversibly embed data in the image for secret message passing. Similar to all methods of steganography, LSB method also embeds the data into the cover media or image so that it cannot be detected by an observer. This method replaces some information in a given pixel with the information from the data in the image.

Least Significant Bit Steganography is an efficient technique to encode data digitally in the cover media or coverimage,in our proposed system we are making use of this method to embed data in the image.

- One's bit in a byte is used to encode the hidden data or information.
- If we want to encode the letter *A* (ASCII 65 or binary 01000001) in the following 8 bytes of a carrier file.
  01011101 11010000 00011100 10101100
  11100111 10000111 01101011 11100011
  becomes
  01011100 11010001 00011100 10101100
  11100110 10000110 01101010 11100011

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

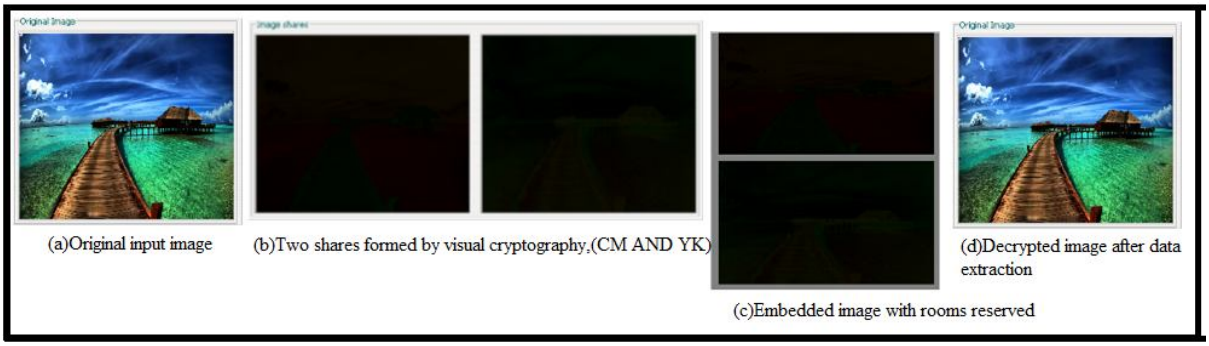
(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

V. RESULTS

The proposed methodology of Reversible Data Hiding is a combination of well known efficient techniques and new technique to extract the hidden data and restore the original cover media.

The system provides a secure way to transfer data without degrading the quality of cover image,color visual cryptography technique has also contributed to it, as the cover is losslessly recovered.This enables to achieve real reversibility which is desirable in medical or military applications.Figure 2 depicts the original image which is splited in two encrypted shares of *CM* and *Y K* colors and on recovery gives the image same as the original one without any distortion even after embedding data in the self reversible embedded image ,thus image quality is maintained which is a major issue even after data extraction.As the data is also encrypted before embedding data security is maintained and further image with hidden data is encrypted providing a more secure way for secret message passing.Thus proposed method gives better results, further the results can be explored by camparing the quality of images by calculating their PSNR values.The results of the proposed method are shown below:



Fifure 4.Results obtained from the proposed system.

VI. CONCLUSION AND FUTURE WORK

The Reversible data hiding(RDH) in encrypted image has gained significance,as the security maintaining requirements are increasing at alarming rate. Thus proposed methodology provides a new framework for reversible data hiding. Here in this approach we have used a new technique for reserving room.

Thus the data hider get the advantage from the extra spacereserved for secret data in previous step before encryption to make data hiding process easy and efficient. In the proposed approach advantage of visual cryptography approach for image encryptionis taken. Thus the image is secured during transmission over the communication network and secret data is also transmitted securely. Confidentiality of image and data is maintained with integrity.Further we can reduce the computation time by resizing the given color image.

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. 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,c IEEE 2010 (2002) The IEEE website.[Online]. Available: http://www.ieee.org/
5. 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).

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. 3, Issue 6, June 2015

6. 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 c IEEE 2013.
7. Moni Naor, Adi Shamir," Visual Cryptography",in Proc. EUROCRYPT' 94, Berlin, Germany, 1995, vol. 950, pp. 1-12,Springer-Verlag,LNCS.
8. InKoo Kang, Gonzalo R. Arce , Heung-Kyu Lee, " Color Extende visual cryptography using error diffusion", ICASSP 2009 c IEEE 2009.
9. 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.
10. Yi-Hui Chen, Ci-Wei lan and Chiao Chih Huang, " A verifiable Visual Cryptography Scheme", Fifth International Conference and Evolutionary Computing IEEE 2011.
11. Jun Tian, "Reversible Data Embedding Using a difference Expansion",IEEE Transaction on circuits and systems for video technology, Vol.13,No. 8, Aug 2003.
12. 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.