A Secure Approach for Reversible Data Hiding using Visual Cryptography

Miss. Nuzhat Ansari
PG Scholar, Dept. of CSE
Rajiv Gandhi College Of Engg. Research & Tech.
Chandrapur. India
e-mail: ansari.rumi@yahoo.in

Abstract: Data is the essential part of communication between sender and receiver. So it needed to be secure and authenticated.Number ofapproaches like Cryptography, Steganography can be used to achieve security of data. Cryptography refers to the study of mathematical techniques and related aspects of Information Security like data confidentiality, integrity and authentication. RDH is gaining lot of importance. RDH is nothing but securely transmitting data inside a cover file, such that data and cover file can be properly recovered at the receiver.This paper gives a keyless reversible data hiding techniquebefore image encryptionto make data hiding process effortless. Also visual cryptographic approach is used for encryption which helps to protect the image during transmission.

Keywords: *SDS, Bit Slicing, Random Share Generation, Encryption, Decryption.*

*****

I. INTRODUCTION

Color image processing is an area that has been gaining in importance because of the significant increase in the use of digital images over the Internet.Today, there is almost no area of technical endeavor that is not impacted in some way by digital image processing. The applications of digital image processing are so wide. One of the simplest ways to develop a basic understanding of image processing applications is to categorizeimages according to their source e.g., visual, X-ray, Ultrasonic, law, forensic, militaryetc.

Image restoration is an area that also deals with improving the appearanceof an image. Image enhancement, which is subjective, image restorationis objective, in such a mannerthat restoration techniques tend to be based on mathematical or probabilistic models of image degradation. Enhancement is based on human subjective preferences regarding what constitutes a “good” enhancement result. As far as images are concerned, the cover mediacan get harmed in processing. Many different techniques have been proposed to recover the cover image without any loss. The reversible data hiding is not only embedding data but also recovering original image.In most of the techniques data embedding is performed by altering the contents of a host media. As a result the host image cannot be completely recovered after the bit extraction. Such data hiding techniques are thus irreversible. However in number of areas like military, law, forensics and medical imaging although some embedding distortion is not acceptable, permanent loss of signal contents is undesirable. This highlights the need for Reversible (Lossless) data hiding techniques.

1.1 Image Encryption using key:

This approach is similar to the traditional encryption methods which involve using an algorithm and a secret key to encrypt an image.Some common techniques for encrypting images include Digital Signatures, Chaos Theory, and Vector Quantization etc.

1.2 Image Encryption without using key:

Encryption technique without using secret key involves generation of random shares, this technique is visual cryptography. Visual cryptography is a process where a secret image is encrypted into shares which refuse to provide information about the original secret image. The strength of this method is that the decryption of the secret image is through human visual system without computation.

Thus the proposed approach gives a secure novel technique for reversible data hiding using visual cryptography. With the scheme involving use of secret keys have limitations regarding key management. In some cases the available secret keys for encryption are limited and have some restricted space, alsohigh computation involved in encryption. All these factors highlight the problem domain for using traditional encryption techniques in reversible data hiding. Opposite to this approach is visual cryptography that involves no use of keys for encryption. Thus the computations required are also less.

II. RELATED WORK

Lots of research has been done in the area of reversible data hiding. In last few years different methods havebeen proposed for reversible data hiding and color image visual cryptography. Some noticeable work in area ofreversible data hiding is as follows:

In [1] Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu and Fenghua Li has proposed a framework forreversible data hiding for embedding data in an image by reserving room before encryption,as vacating room from the encrypted images is difficult and inefficient.

In [4] JuiTian has introduced a difference expansion technique which finds extra storage space by exploring theredundancy in the image content. Secret data holding capacity limit and the visual quality of embedded imagesof the DE method are among the best methods, along with a low computational complexity.

In [5] the area of reversible data hiding José .R; Abraham .G, have proposed a novel scheme to hide data into encrypted grayscale image. This technique is seperable method. Content owner encrypts the image by permuting pixels using secret keyfor encryption. The data hider hides the data into the encrypted image by histogram modification based hiding by using data hiding key.

Jithi P V, Anitha T Nair in [6] has proposed the scheme based on Progressive Visual Cryptography. In proposed method, a digital watermarking technique is used to generate shares that provide some meaning. The secret image shares are watermarked with different cover images and are securely transmitted. At the receiver the cover images are extracted from the shares and stacked one by one which generates the secret image.

Yi-Jing Huang, Jun-Dong Chang in [6] have proposed a novel non-expanded visual cryptography scheme with authentication using block encoding. Thismethod includes the extra ability of hiding confidential data which combines the feature of authentication with the block encoding scheme to transmit the secret information.

In [8] RastislavLukac, Konstantinos N. Plataniotis gave a new secret sharing scheme capable ofprotecting image data coded with *n*bits per pixel. The proposed encryption solution generates *n*-bit shares by combining bit-level decomposition by stacking with a {*x*, *y*}threshold sharing strategy. Efficient reconstruction is achieved by performing decryption usingsimple logicaloperations in the decomposed bit-levels without the need for any postprocessing operations. This framework allows for costeffective cryptographic image processing of *n*-bit images over the Web.

III. PROPOSED WORK

Following figure gives the framework for proposed method. Proposed method works five main steps; vacating room for embedding data, Embedding data in reserved vacated room, keyless Image Encryption, image recovery and data extraction.

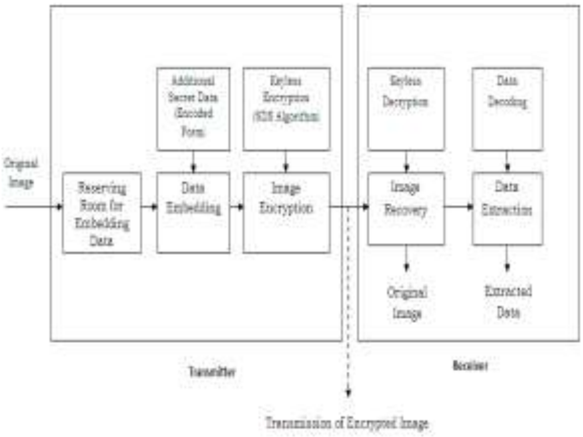


Figure 1: Framework for Proposed Scheme

The encryption technique using generation of random shares involves minimal computing for reconstructing the original secret image without any loss in image quality. This scheme provides two level securities;1.for embedded data, and 2.for secret image.

The proposed method combines the advantage of two different approaches together that are reversible data hiding and visual cryptography. In the area of reversible data hiding this provides effective solution to overcome the limitations of existing methods.As, in images we hide data only in the pixel value, but the proposed system will divide an image into individual RGB components and stores each bit in the corresponding components. Thus we are dividing the pixel value into three components, so the search space we get is three times more, which means we can add large amount of data in the image without affecting the quality of the image. The objective of proposed method is to provide complete reversibility with minimum computation by using visual cryptography.

Reserving room for embedding the data involves division of original image into individual RGB components and among the pixel pairs finding the minimum value pixels using DE technique, which can be further used for accommodating messages. Then next step is to embed the data into vacated area. Now after embedding the data this image will be encrypted using SDS algorithm. SDS algorithm involves the three main steps Sieving, Division and Shuffling. **Sieving** involves filtering of the combined RGB components into individual R, G and B components. Upon filteringout the original image into R, G, B components the next step involves **dividing** the R, G and B components into shares. S**huffling** the elements in the individual shares. The elements are shuffled randomly using bit slicing and shifting of bits. We get shuffled bits in each shares, here we are diving no. of random shares into four equal shares. The random shares so generated individually does not provide any information about the secret image, however to recover the contents of an image all the random shares would be required. After recollecting all the random shuffled data shares, original image reconstruction can be performed. The algorithm for the above described process is as under:

```
1. Sieving
Input _ Secret Image
Sieve(Secret Image)
Output_(individual R, G, B components)

2. Division
x= total number of pixels (0 to x-1)
Ri / Gi / Bi = individual values of the ith pixel in
the R, G, B components
z = total number of random shares
n =number of bits representing each primary color
maxval = 2n
Repeat step2 for R, G, B component
2(a) for i = 0 to (x-2)
{
for share k = A to (Z-1)
Rki = Random(0, maxval)
Aggr_Sumi = _ Rki
}
Rzi=(maxval + Ri – (Aggr_Sumi % maxval))
% maxval

3. Shuffle
Repeat for RA-Z, GA-Z and BA-Z (all generatedshares)
for k = A to Z
{
Rk-shuffle = Rk
PtrFirstVac = 1
PtrLastVac = x-1
For i = 1 to (x-1)
{
  If (R(k+1)*(i-1) is even)
{
R(k-shuffle) PtrFirstVac = Rki
PtrFirstVac ++,
i++
}
Else
{
R(A-shuffle) PtrFirstVac = RAi
i++, PtrLastVac --
}
}
}

4. CombineFor k = A to Z
RSk = (Rk-shuffle XOR Gk-shuffle XOR Bk-shuffle)
```

Thus, at the end of above process we get Random Shares (RSA,RSB…RSk)

Proposed method works in following steps:

Vacating room for embedding data: Intensity of each block in the image is calculated. Then calculating f-value of each block for finding first order smoothness of the blocks. Blocks having f-value less than average f-value are kept reserved for data embedding.

$$f=\sum_{i=2}^{x}\sum_{j=2_4}^{y-1} C_{i,j}\Big|- C_{i-1,j}+ \underline{C_{i+1,j}+C_{i,j-1}+C_{i,j+1}}\quad\Big|$$

Higher f-value represents block with more complexity.

Embedding data in reserved vacated room:

To reversibly embed the data in images we are employing Difference Expansion technique.The original image is grouped into pairs of adjacent pixels.By calculating the differences of this neighboring pixel values and selecting some difference values for the difference expansion (DE), the pixel having minimum value is used to embed data with difference value of those pixels.

Keyless Image Encryption:

To generate random shares and for image encryption SDS algorithm is used. Each pixel is shuffled and gives the encrypted imato generate random share. We modify the positions, values of pixels and it will result in a scrambled output.While transmitting an image it becomes more difficult for intruder to retrieve the contents because individual share convey no information. Thus, providing more security for data and cover file.

Image Recovery & Transmission:

In image retrieving phase the original image involves sieving the random shares and recollecting all the shuffled shares, further from these individual shuffled shares the original image can be generated and data is retrieved as well.

Data Extraction:

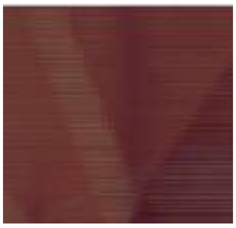
In data extraction phase the new calculated pixel value are considered and again difference is calculated using same Difference Expansion method in reverse order.The index position of those blocks and the positionof pixel pairs; where the data was embedded are required to losslessly extract original contents.

IV. EXPERIMENTAL RESULTS

The proposed reversible data hiding technique has been applied to many different types of images, including some common standard imagesand medical, texture, aerialand has always achieved satisfactory results, thus it is applicable to all types. The proposed reversible data hiding technique is able to embed about 5–80 kb into a 1024* 1024color image while guaranteeing the PSNR of the marked image versus the original image to be above 10dB. Furthermore, this algorithm is very simple, and the execution time is also less. Therefore, its overall performance is better than various existing reversible data hiding algorithms. It is expected that this reversible data hiding method will be employed for a wide range of applications in the areas such as secure medical image data systems, and image authentication in the medical field and law enforcement, and the other fields where the rendering of the original images is required or desired. Following figure shows experimentation results for proposed method.

(i)

(ii)


(iii)

(iv)

Figure 2: (i) Original Image, (ii) Image with hidden data, (iii) Encrypted image, (iv)Recovered image

All the existing methods gives a method for hiding a data into animage in a reversible manner that in the extraction phase the image will be restored lossless but while the image is holding a data the security of an image is also a major concern especially during transmission. And when the image and the data inside it have a relation in that case both the data and image should not be revealed to the unauthorized user. Thus image can be protected by applying different encryption techniques. In the proposed scheme after application of RDH for hiding data, the image is encrypted using visual cryptography which involves dividing the image into random shares. After data embedding we are modifying pixel values of used pixels. And in order to provide more security during image transmission we are using bit slicing and rotation before shuffling pixels.

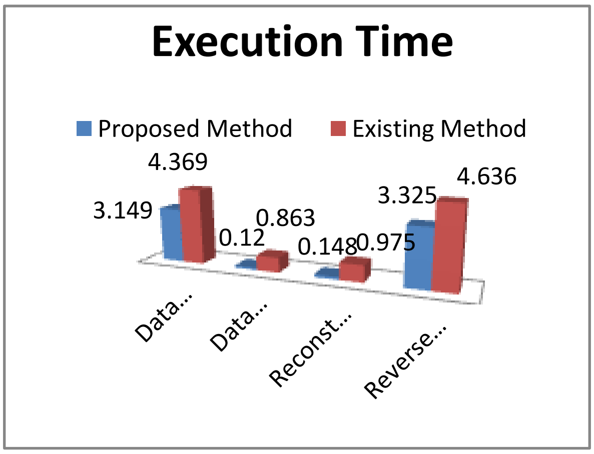


Figure3: Execution time comparison of Lena image

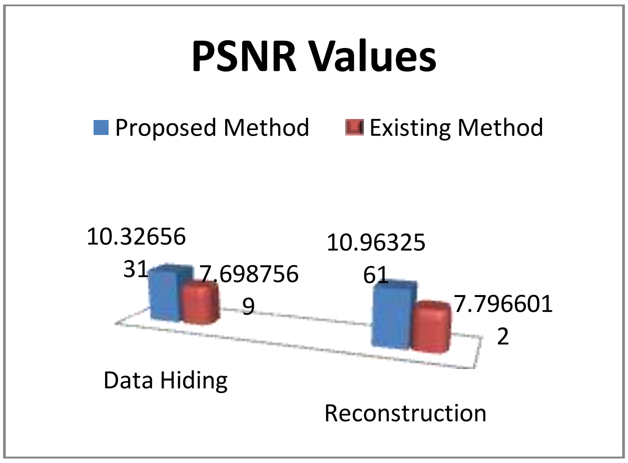


Figure 4: PSNR comparison of Lena image

Image		Proposed Method		Existing Method	
		Time(ms)	PSNR(db)	Time(m s)	PSNR(db)
Lena	Data Hiding	3.14	10.32	4.36	7.69
	Data Share	0.12		0.18	
	Reconstruction	0.14	10.96	0.19	7.79
	RDH	3.32		4.610	
Barbara	Data Hiding	3.21	12.92	3.623	7.39
	Data Share	2.02		2.32	
	Reconstruction	2.57	11.69	3.20	6.74
	RDH	3.07		4.53	
Baboon	Data Hiding	3.47	18.92	5.03	7.78
	Data Share	0.49		1.02	
	Reconstruction	0.36	19.19	0.90	7.76
	RDH	4.24		5.36	

Figure 5: Comparison table of some standard images with proposed method

The proposed scheme offers a high embedding capacity, security and good PSNR ratio as compared to other techniques.

V. CONCLUSION

Reversible data hiding in encrypted image is drawing lots of attention because of privacy preserving requirements. Thus proposed scheme provides a completely new framework for reversible data hiding. Here in this approach I have used a new technique for reserving room before encryption of image. Thus the data hider can benefit from the extra space emptied out in previous stage before encryption to make data hiding process effortless. In the proposed approach we take advantage of visual cryptography approach for encrypting the image. Thus the image is protected in transmission and secret data is also transmitted securely. The employed technique involves the three main steps that are sieving, division and shuffling the images. Thus random shares are so generated from shuffled shares of image are transmitted.In the proposed approach we take advantage of visual cryptography approach for encrypting the image.

Thus the image is protected in transmission and secret data is also transmitted securely.

REFERENCES

[1] Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li, " Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption" , IEEE Transaction on Information Forensics and Security, Vol.8, No.3, March 2013.

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

[3] Yu Jing, Song Wei,"Study on Reversible Data Hiding Scheme for Digital Images", 2010 2nd International Asia Conference on Informatics in Control, Automation and Robotics(CAR 2010) © IEEE.

[4] Jun Tian "Reversible Data Embedding Using a Difference Expansion" Transactions on circuits and systems for video technology, VOL. 13, NO. 8, AUGUST 2003

[5] 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

[6] Yi-Jing Huang, Jun-Dong Chang, "Non-expanded Visual Cryptography Scheme with Authentication", IEEE 2nd International Symposium on Next-Generation Electronics (ISNE), Feb 25-26, Taiwan.

[7] VikasTyagi "Data Hiding in Image using least significant bit with cryptography" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 4, April 2012.

[8] R. Lukac, K.N. Plataniotis "Bit-level based secret sharing for image encryption", The Journal of Pattern Recognition Society, 2005.

[9] R. Vijayaraghavan, S. Sathya and N. R. Raajan "Security for an Image using Bit-slice Rotation Method–image Encryption" , Indian Journal of Science and Technology, *Vol 7(4S), 1–7, April 2014.*

[10] MoniNaor and Adi Shamir, "Visual cryptography", inProceedings of Advances in Cryptology EUROCRYPT 94,LNCS Vol. 950, pages 1-12. Springer-Verlag, 1994

[11] Mehmet U. Celik, Gaurav Sharma, A. Murat Tekalp, Eli Saber,"Reversible Data Hiding", IEEE ICIP 2002.

[12] C. Anuradha, S. Lavanya, "Secure and Authenticated Reversible Data Hiding in Encrypted Image", International Journal of Advanced Research in Computer Science and Software Engineering, volume 3,issue 4, April 2013.

[13] Yi-Jing Huang, Jun-Dong Chang, "Non-expanded Visual Cryptography Scheme with Authentication", IEEE 2nd International Symposium on Next-Generation Electronics (ISNE), Feb 25-26, Taiwan.