Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 125 – 131

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

A Keyless Approach for RDH in Encrypted Images using Visual Cryptography

Miss. Nuzhat Ansari[a] ,Prof. Rahila Shaikh[b]*

[a]*PG Scholar,Rajiv Gandhi College of Engg. Research & Tech,.Babupeth,Chandrapur 442 403,India*
[b]*Asst. Professor,Rajiv Gandhi College of Engg. Research & Tech.,Babupeth,Chandrapur 442 403,India*

Abstract

This paper describes a keyless reversible data hiding technique using visual cryptography where data hiding is carried out before image encryptionto make lossless data retrieval process.Reversible Data Hiding technique is asecure way of transmitting data inside a cover media, so that data and cover file can be properly recovered at the receiver.Also visual cryptographic approach is used for encryption which helps to protect the image during transmission and a bit rotation technique is also employed in order to provide better encrypted image and make hacking more difficult. In proposed approach image is divided in three individual RGB components; such that the search space we get prior to data embedding is large. To overcome the limitations of key management a keyless approach is used; to provide more data security data shares are generated after encryption.

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords:SDS;Bit Shifting; Random Share Generation; Encryption; Decryption;Visual Cryptography

1. Introduction

Digital image processing refers to processing of digital images by means of a digital computer. Adigital image ismade up of a finite number of elements, each of which has some particular location and value. Theseelements areknown as *picture elements,image elements*, *pels*, and *pixels*.

* Corresponding author. Tel.: +0-942-014-1940;
E-mail address: ansari.rumi@yahoo.in

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.021

Pixel is the most widely used term to denote the elements of a digital image. Vision is the most advanced part of oursenses; it is not surprising that images play the single most important role in human perception. Unlike humans, who are limited to the visual band of electromagnetic spectrum, imaging machines covers almost entire EM spectrum, ranging from gamma rays to radio waves.Digital image processing encompasses a wide area of applications. The process of acquiring an image of the area containing the text, pre-processing that image, extracting the individual characters, describing the characters in a form suitable for computer processing, and recognizing those individual characters are in the scope; we call it as *digital image processing*.

Color image processing is an area that has been gaining lot of importance because of the significant increase in the use of digital images over the Internet. As far as images are concerned data hiding which cannot interpret between stego-image and cover image by human, the cover image can get harmed in processing. Various techniques have been proposed to get back cover image without any loss. The reversibility means not only embedding data but also original image can be precisely recovered in the extracting stage. Most of the data hiding techniques perform data embedding by altering the contents of a cover media. As a result the cover image cannot be completely recovered after the bit extraction. These type of data hiding techniques are called irreversible techniques. However, in a number of domains such as military, law and medical sciences although some embedding distortion is admissible, permanent loss of signal fidelity is not desirable. This gives rise to the need for Reversible (Lossless) data embedding techniques.

Image encryption can be carried out using:

- Image encryption using secret keys
- Keyless Image encryption

Using encryption keys is a traditional method of image encryption can be carried out using DES, AES algorithms, digital signatures, vector quantisation, chaos theory etc. In some cases secret key used for encryption is restricted and may have some limitations. It is inapt due bulk size of data. Also it requires heavy computational cost. In contrast to this technique image encryption without using key provides more security as there is no need to maintain secret key, involves low encryption/decryption cost.

Encryption technique without using secret key includes generation of random shares; this technique is known as visual cryptography. Visual cryptography is a process where the 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 using secret keys have limitations regarding key management. In some cases the available secret keys for encryption are limited and have some restricted space, also high computation involved in encryption. All these factors highlight the problem domain for using traditional encryption techniques in reversible data hiding. In converse to this approach is visual cryptography that involves no use of keys for encryption. Thus the computations required are also less.

The proposed scheme suggests the novel approach for data hiding and image encryption. Since losslessly vacating the room from the encrypted image is difficult and sometimes inefficient thus proposed scheme apply a method of vacating the room for data prior to the image encryption [1], 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 space for data from already encrypted image.The objective behind this is to implement secure keyless image encryption technique and to improve the quality of marked decrypted image.Bit plane slicing of digital image is used to provide more security. The main objective of BPS is used to divide the digital image into 8 bit planes such that the bit-plane is further rotated in order to provide better encrypted image and to make hacking more difficult. It focuses on two techniques such as bit plane slicing and image rotation for efficient image encryption.

2. Existing Work

Lots of research has been done in the area of reversible data hiding. In last few years different 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:

Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu and Fenghua Li[1] 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. Embedding data prior to image encryption also results in lossless retrieval of image.

Jun Tian 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 images of the DE method are among the best methods, along with a low computational complexity[2].From information hiding point of view, reversible data embedding technique hides some information in a digital image in such a way that third party could decode the hidden information and also restore the original image. The performance of RDH algorithm can be evaluated by following parameters:

1) *Payload capacity limit:* what maximum amount of information can be embedded?
2) *Visual quality:* the visual quality of the embedded image?
3) *Complexity:* what is the complexity of algorithm?

R. Vijayaraghavan, S. Sathya and N. R. Raajan proposed a bit slice rotation method of digital image for more security[4]. Bit Plane Slicing is used to divide the digital image into 8-bit planes. The bit plane is further rotated such that to provide better encrypted image and to make hacking more difficult. The classification of bit plane is used for analyzing the importance played by each bit of an image. It is used to estimate each pixel of an image. The proposed scheme involves rotation of bit planes providing highly secure image encryption. By this method scrambling of an image is based on efficient technique even it is intercepted, the information cannot be understood. It is mainly useful for image compression because it exhibits high coding efficiency.

Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su, gave a novel reversible data hiding algorithm, which can recover the original image without any distortion from the marked image after the hidden data have been extracted. This algorithm utilizes the zero or the minimum points of the histogram of an image and slightly modifies the pixel grayscale values to embed data into the image. This can hide more data than many of the existing RDH algorithms[6]. It is proved analytically and shown experimentally that the peak signal-to-noise ratio (PSNR) of the marked image generated by this method versus the original image is guaranteed to be more than 48 dB. This lower bound of PSNR is much higher than that of all reversible data hiding techniques reported in the literature. The computational complexity of the proposed technique is low and the execution time is less.#

Asha S.N, Dr.Shreedhara, *Visual* cryptography is a method where the secret image is divided into two or more shares which are known as shares and the secret image is revealed by overlaying the shares without any complex computation involved. This paper defines how to implement the embedded extended visual cryptography scheme by taking more than one input as well secret image. The image visual quality metrics like PSNR,MSE and MAXERROR are defined here.The generations of covering shares are carried out with the help of half toning technique using dithering matrix[7].

InKoo Kang, Gonzalo R. Arce, Heung-Kyu Lee [9], introduces a color visual cryptography encryption method that produces meaningful color shares via visual information pixel (VIP) synchronization and error diffusion halftoning. VIP synchronization retains the positions of pixels carrying visual information of original shares throughout the color channels and error diffusion generates shares pleasant to human eyes. Comparisons with previous approaches show the superior performance of the new method. It introduces a color VC encryption method which leads to meaningful shares and is free of the previously mentioned limitations. Error diffusion is a simple but efficient algorithm for image halftone generation. The quantization error at each pixel is filtered and fed back to future inputs.

3. 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.

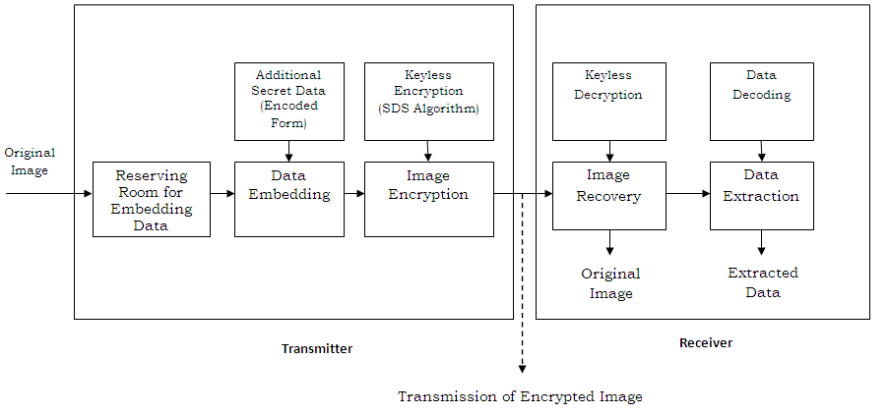

Fig. 1: Framework for Proposed Scheme

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. In proposed method we are dividing the pixel value into three components, so the search space we get for data embedding 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 works in three steps i.e. Sieving, Division and Shuffling. **Sieving** involves filtering of the combined RGB components into individual R, G and B components. Upon filtering out 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 are shuffled 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.

Proposed method works in following steps:

3.1 Vacating room for embedding data:In this phase we will reserve space for data embedding before Image encryption[1]. To do so first we will select an image and the entire space is used for data embedding; i.e. the size of a text file is equal to or less than the size of an image. Initially the image is divided into individual RGB components and then is grouped into no. of blocks. Intensity of each block in the image is calculated. Then calculating f-value of each block for finding first order smoothness of all the blocks. Blocks having f-value less than average f-value are kept reserved for data embedding.

$$f = \sum_{i=2}^{u} \sum_{j=2}^{v-1} \left| C_{i,j} - \frac{C_{i-1,j} + C_{i+1,j} + C_{i,j-1} + C_{i,j+1}}{4} \right| \quad (1)$$

Higher f-value represents block with more complexity.

3.2 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. Difference and average between pixel pair is calculated. By calculating the differences of this neighbouring 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. Data is embedded in its binary format; again providing more data security.

3.3 Keyless Image Encryption:

To generate random shares and for image encryption SDS algorithm is used. Each pixel is shuffled and gives the encrypted image generate random share. We modify the positions, values of pixels and it will result in a scrambled output. For this we divide the image into individual components. And equally dividing the no. of blocks into four data shares.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.

3.4 Image Reconstruction& Transmission:

In image reconstruction phase the original image involves sieving the random shares and recollecting all the shuffled shares, further from these individual shuffled shares we can get original image back with data hidden inside; without loss of picture quality. This image can be used for transmission; the bit-shuffling and difference expansion techniques used here provides higher data security.

3.5 Data Extraction: In data extraction phase the new calculated pixel value are considered and again average &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.

4.Experimental Results

The proposed reversible data hiding technique has been applied to many different types of images, including some

common standard images and medical, texture, aerial and 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 technique can 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.

Fig. 2: (a) Original Image, (b) Image with hidden data, (c) Encrypted image, (d) Recovered image

All the existing methods gives a method for hiding a data into an image 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.

Image	Size	Operation	Proposed Method		Existing Method	
			Time(ms)	PSNR(db)	Time(ms)	PSNR(db)
Lena	463kb	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	174kb	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	611kb	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	

Table 1. 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; higher the PSNR gives better quality of encrypted image. The proposed technique is experimented with the existing standard images; it is also applicable with any type of image. Here size of text used is less than or equal to the size of image. The performance of proposed method is faster than that of existing techniques.

Conclusion

Reversible data hiding in encrypted image is drawing lots of attention because of privacy preserving requirements. The proposed scheme gives a completely new framework for reversible data hiding technique. Here in this approach a new technique is used for reserving room before encryption of image. The data hider can take benefit from the extra space emptied out in previous stage before encryption to make data hiding process effortless. In the proposed technique we can take advantage of visual cryptography for encrypting the image. Hence, the image is protected during transmission and secret data is also transmitted securely. The employed technique comprises of three main steps that are sieving, division and shuffling the images. The random shares so generated from shuffled shares of image are transmitted.In the proposed approach we can 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: March 2013;Vol.8; No.3.

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

[3] Siddharth Malik, Anjali Sardana, Jaya. *A Keyless Approach to Image Encryption.* International conference on Communication systems and Network Technologies:2012; IEEE.

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

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

[6]Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, Wei Su. *Reversible Data Hiding.* IEEE transactions on circuits and systems for video technology: March 2006; vol. 16, no. 3.

[7] Asha S.N, Dr. Shreedhara. *Performance Evaluation Of Extended Visual Cryptography Schemes With Embedded Extended Visual Cryptographic Scheme*. International Journal of Scientific & Engineering Research: April-2012; Volume 3, Issue 4.

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

[9]InKoo Kang, Gonzalo R. Arce, Heung-Kyu Lee. *Color extended visual cryptography using error diffusion*. IEEE:2009.

[10]Yi, Feng; Wang, Daoshun; Luo, Ping, Huang, Liansheng, Dai, Yiqi.*Multi Secret Image Color Visual Cryptography Schemes for General Access Structures.* April 2006; Volume 16, Number 4; pp. 431-436.

[11] J. Fridrich, M. Goljan, and D. Rui. *Lossless Data Embedding - New Paradigm in Digital Watermarking.* In Special Issue on Emerging Applications of Multimedia Data Hiding: February 2002; Vol. 2; pp. 185-196.