Available online www.jsaer.com

Journal of Scientific and Engineering Research, 2016, 3(2):235-242

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Modified LSBR and Pixel Sieve Technique to in Visual Cryptography for Multiple Colored Images

Kalyan Das[1], Aromita Sen[2], Samir Kumar Bandyopadhyay[3]

[1]Department of Information Technology, St. Thomas College of Engineering and Technology Kolkata, India.
[2]Department of Computer Science and Engg, St. Thomas College of Engineering and Technology Kolkata, India.
[3]Department of Computer Science and Engineering, University of Calcutta, India

Abstract Visual cryptography is a method for protecting image-based secrets that has a computation-free decoding process. In this paper we propose a new color visual cryptography scheme. Pixel Sieve method was proposed recently to encode an image into shares. Our proposed method suggested a way to encrypt multiple color images using symmetric key encryption procedure where we are using the idea of LSBR and pixel sieve method in a modified way. The proposed method is applied on several images and showed good result without any distortion. The algorithm proposed by this scheme reduces a considerable time for encryption and decryption in a much easier way and ensures the lossless transmissions of images.

Keywords Visual Cryptography, Encryption, Decryption, LSBR, Pixel Sieve

1. Introduction

In recent days, security is a big threat in the transmission medium due to the development of the Internet and multimedia contents such as audio, image, video etc. For transmitting secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want. To deal with the security problems of secret images, various image secret sharing schemes have been developed which gave rise to new technologies in the area of Image Cryptography which would require less computation and less storage. As kind of special secret sharing technology, Visual Cryptography (VC) was introduced by Naor and Shamir [1] in the Eurocrypt'94. This technique does not require any key management nor does it require any algorithm for decryption. Most of these studies, however, concentrate on binary images; few of them proposed methods for processing gray-level and color images. Most of the techniques which are employed on color images such as do not give the original image back. The quality of the generated images is not same as the original and there is lot of loss in the picture quality. This paper proposes a method which gives a way out for color image cryptography without any loss and pixel expansion. For this we have used proposed this new technique for encryption and share generation process.

2. Existing Work

Black and White Visual Cryptography Schemes

Sharing Single Secret:-

Naor and Shamir's [1] proposed encoding scheme to share a binary image into two shares Share1 and Share2. If pixel is white one of the above two rows of Figure 1 is chosen to generate Share1 and Share2. Similarly If pixel is black one of the below two rows of Figure 1 is chosen to generate Share1 and Share2. Here each share pixel p is encoded into two white and two black pixels each share alone gives no clue about the pixel p whether it is white or black. Secret image is shown only when both shares are superimposed. The disadvantage of the above schemes is that only one set of

confidential messages can be embedded, so to share large amounts of confidential messages several shares have to be generated.

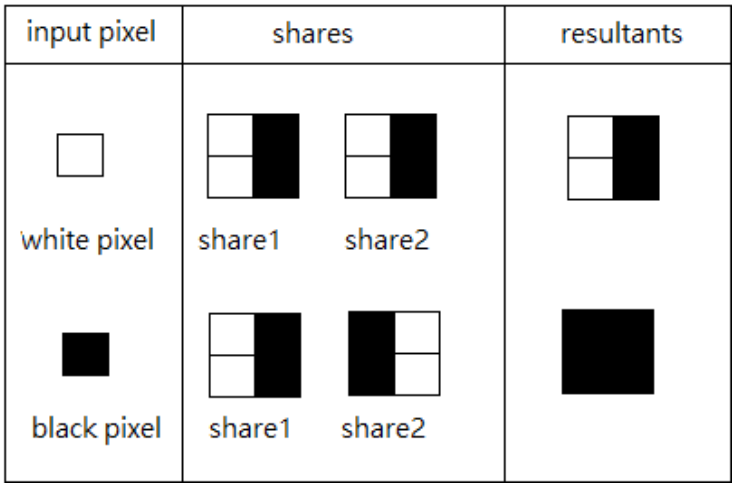


Figure1: Shares used by Naor and Shamir in (2, 2) VCS

Sharing Multiple Secrets:

Wu and Chen [2] were first researchers to present the visual cryptography schemes to share two secret images in two shares. They hidden two secret binary images into two random shares, namely A and B, such that the first secret can be seen by stacking the two shares, denoted by A⊗B, and the second secret can be obtained by first rotating A Θ anti-clockwise. They designed the rotation angle Θ to be 90◦. However, it is easy to obtain that Θ can be 180◦ or 270◦.

Color Visual Cryptography Schemes

Sharing Single Secret:

Until the year 1997 visual cryptography schemes were applied to only black and white images. First colored visual cryptography scheme was developed by Verheul and Van Tilborg [3]. But the shares generated were meaningless. For sharing a secret color image and also to generate the meaningful share to transmit secret color image Chang and Tsai [4] anticipated color visual cryptography scheme. For a secret color image two significant color images are selected as cover images which are the same size as the secret color image. Then according to a predefined Color Index Table, the secret color image will be hidden into two camouflage images. One disadvantage of this scheme is that extra space is required to accumulate the Color Index Table.

Sharing Multiple Secrets:

Tzung-Her Chen et al [5] anticipated a multi-secrets visual cryptography which is extended from traditional visual secret sharing. The codebook of traditional visual secret sharing implemented to generate share images macro block by macro block in such a way that multiple secret images are turned into only two share images and decode all the secrets one by one by stacking two of share images in a way of shifting. This scheme can be used for multiple binary, gray and color secret images with pixel expansion of 4.

Table1: Comparison of visual cryptography schemes on the basis of number of secret images, pixel expansion, image format, type of share generated

Pixel Expansion	Number of Secret Images	Image Format	Type of Share generated	Authors Year
1	4	Binary	Random	Naor and Shamir [1]-1995
2	4	Binary	Random	Wu and Chang [2] 2005
1	C*3	Color	Random	Verheul Tilborg [3] 1997
n(n>=2)	4	Binary, gray, Color	Random	Tzung-Her Chen et al [5] 2008
1	529	Color	Meaningful	Chang and Tsai [4] 2000
1	n(n>=1)	Color	Random	Proposed Algorithm

Abbreviations in Visual Cryptography Schemes: m indicates pixel expansion of corresponding visual cryptography schemes, c number of colors in visual cryptography schemes, n is the number of shares

3. Proposed Method

The simplest example of visual cryptography is a scheme in which we split the image into two different shares. The decryption of the image will be done by overlapping the shares. When we place both the shares one over another with proper alignment, we can interpret the original image. But there is no concept of any key so whoever gets the control over the shares, can retrieve the original information.

Pixel Sieve Method:

A.Incze [6] has proposed pixel sieve method for splitting the image into two different shares which uses a key to split the image. It is used to split a black and white image. The image is rebuilt from the shares not by applying a cryptographic process using a key. The key used in this method is a binary image which contains holes like a sieve.

The original image is placed over the key sieve. The pixels of the original image which are situated above the holes in the sieve go through and form one share. The remaining pixels form the other share of the image. The method is illustrated in the figure 2.

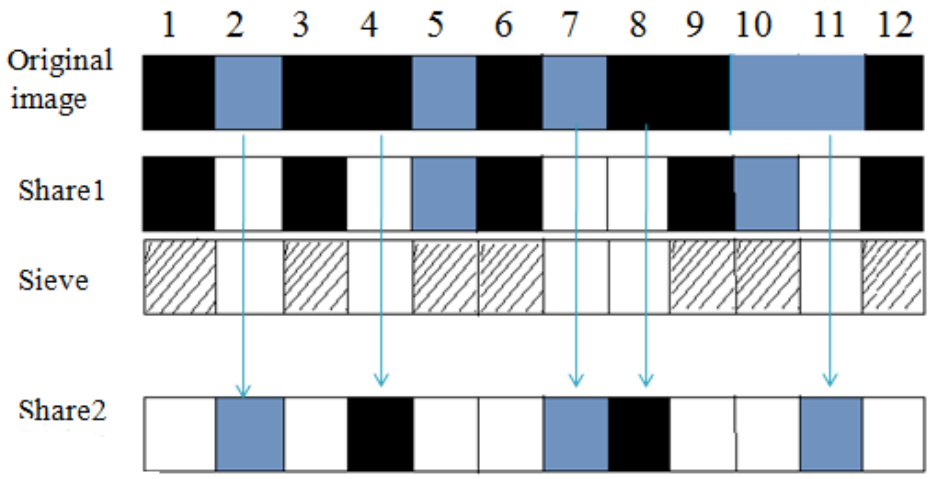


Figure 2

In this case the black and blue pixel represents the original image pixels and the white pixels are the redundant ones. To remove such redundancy and reduce the size of the shares some modifications are done which are shown below in figure 3.

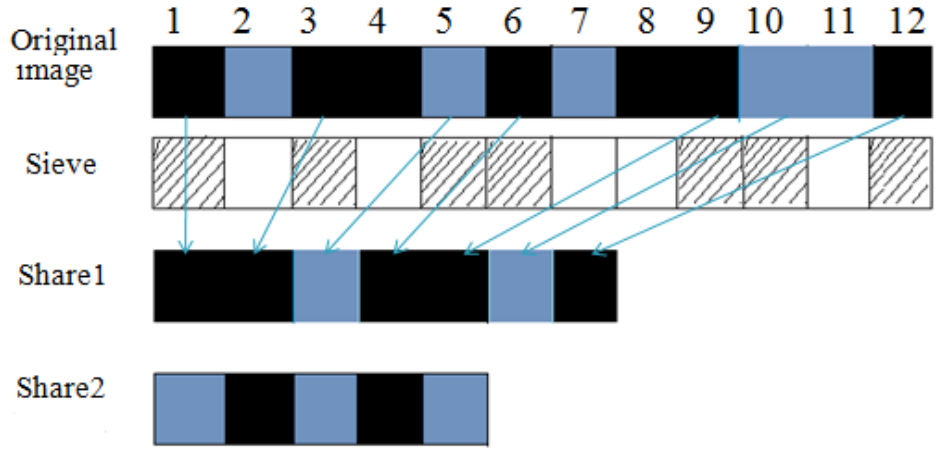


Figure 3

In this method shares have different size and total size of both the shares is equal to the size of original image and here only the original pixels are the part of the share images.

LSB Replacement algorithm:

In LSB steganography, the least significant bits of the cover media's digital data are used to conceal the message. The simplest of the LSB steganography techniques is LSB replacement. LSB replacement steganography flips the last bit of each of the data values to reflect the message that needs to be hidden. The difference between the cover (i.e. original) image and the stego image will be hardly noticeable to the human eye.

Consider an 8-bit grayscale bitmap image where each pixel is stored as a byte representing a grayscale value. Suppose the first eight pixels of the original image have the following grayscale values:

11010010		11010011
01001010	Binary Sequence	01001010
10010111	10000011	10010110
10001100	⟶	10001100
00010101		00010100
01010111		01010110
00100110		00100111
01000011		01000011

One of the reasons that intruders can be successful is that most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack One solution to this problem is to hide information in digital media and use of key for further security.

4. Methodology

In additive model or RGB model, every color image is composed of pixels where each pixel is a series of bits composed of RGB values with 24bit depth. Each value is in the range of 0-255 i.e. Red ranges from 0-255, Green ranges from 0-255 and Blue ranges from 0-255. When all these three values for RGB are combined we get a color which defines the pixel of the image. The proposed technique encrypts the color image using the following steps.

Step 1: Encryption using modified LSBR

Step 2: Share generation using Pixel Sieve method

Step 3: Retrieval of original image using symmetric key

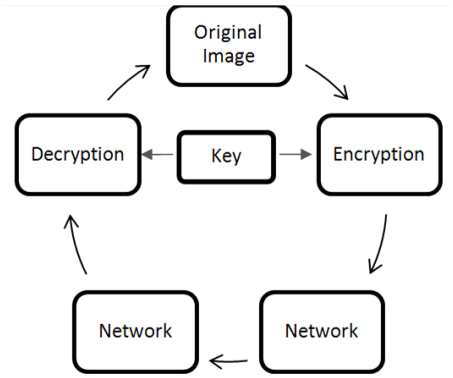


Figure 4: Flow chart representation of the proposed scheme

Brief description of each step:

Step 1: For multiple image encryption we are not taking any cover image separately, rather we are making a combination of input secret images for encryption. We are simply performing LSBR and cross merge technique. Here 4lsb of image1 are merged with 4 msb of image2 and vice-versa and thus resulting two random encrypted outputs.

For N number of secret images there can be ($^{N}P_{2}$-N) combinations used. So in that case we need some key to identify which encrypted form contains information of the images.

Taking 4bit LSB of img1 as MSB: K= img(x,y,z) bitwise AND (00001111)

K=K<<4

Taking 4bit MSB of img2 as LSB: L= img(x,y,z) bitwise AND (11110000)

L=L>>4

Combining for encrypted pixel: Encrypted(x,y,z)= K bitwise OR L

Step 2: Then the encrypted images are divided into multiple shares using pixel sieve method, for which we are using symmetric key algorithm. Generally the sieve used is nothing but a binary image [1, 0] of same size. But here we are using a color image as a key that's each pixel value itself will contain the information as of the sieve. For that we need some preprocessing so that the encrypted images can be distributed equally in a random manner within the shares. Then the shares are transmitted to the receiver along with the secret key.

```
if ( key(x,y,z) == hole)
        m1(x,y,z)=s1(x,y,z);        //s1 and s2 are the encrypted images
        m3(x,y,z)=s2(x,y,z);                //m1,m2,m3 & m4 are the shares
 else
        m2(x,y,z)=s1(x,y,z);
        m4(x,y,z)=s2(x,y,z);
 end
```

Step 3: The decryption process is just the reverse of the encryption procedure. When the shared images reach the destination, the receiver enters the key and the original image is decrypted without any distortion.

5. Implementation Details

In this paper, the number of pixel in the decoded image is same as in the original secret. After testing on many different images the results are as our expectation and the shares are clear without any visual abnormality. The above mentioned scheme is implemented into "MATLAB R2009a".This technique can work for both color images as well as gray scale images. All that is required is to transmit key on a secret channel while shares can be transmitted on an unsecure channel.

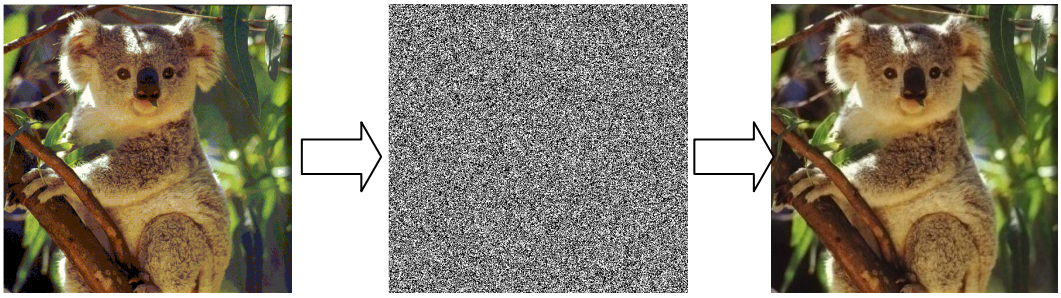
6. Experimental Results

In this process we have taken two natural images of .bmp format of size 512*512 for our experiment purpose. Then the original images were encrypted using technique described in step1.

*Figure 5: Original Color Images 512*512*

Figure 6: Encrypted Images

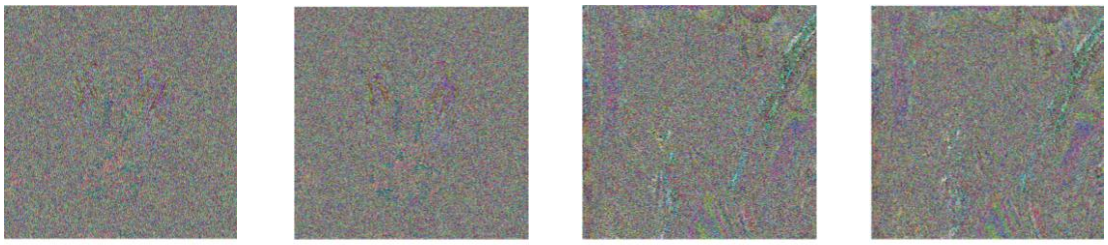
Now for applying pixel sieve method we have generated a random binary image of same size using random function and then modified a color image according to that, which will serve as the key for symmetric key encrypt- decrypt algorithm.



Cover Image Random Image Secret Key

Figure7: Key Generation

Now using the key the share generation is done over the encrypted images. In this algorithm, for share generation we need a binary image as a key of same size as of the original data image. And while encryption of more than 2 images we will need some more **keys** associated with each of the encrypted form, with **each of size 2N** where **total no of secret image <= 2^N**.



Share1 Share2 Share 3 Share 4

Figure 8: Share Generation Process

For the encryption purpose there is no need for pixel expansion, but considering the share generation part, pixel expansion=2 as we are dividing each image into two shares. But with some modification it can be reduced to 1. Now for **N no of secret images** to be transferred the **no. of shares** generated will be **2*N**.

Quality Measurement

For performance calculation we need to use SSIM or PSNR index. Here we have used the PSNR index for measuring the quality between two images. In PSNR quality measurement one of the images are compared provided the other image is regarded as of perfect quality. The formulae used are given below:

$$MSE = \frac{1}{NxM}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}[X(i,j) - Y(i,j)]^2 \qquad \text{PSNR} = 10\log_{10}\left(\frac{I_{\max}^2}{\text{MSE}}\right)$$

[X is the original image and Y is the output image; I is the dynamic range of pixel values normally 255; (M, N) are the dimensions of the image]

The quality measures are calculated between the original image and the encrypted/decrypted image. Table2 shows the quality measures of the images after encryption / decryption process.

Table2: Experimental results for encrypt-decrypt process

Image	PSNR index for img1	PSNR index for img2
Original Image	inf	inf
Encrypted Image	0	0
Decrypted Image	inf	inf

It is already confirmed that proposed method gives a lossless way of cryptography where symmetric key algorithm is used and generated shares are meaningless.

7. Conclusions & Future Work

As conclusion it can be said that; visual information where size and security is more concerned, the proposed visual cryptography scheme is undoubtedly fine and fantastic to use. In our proposed algorithm the original secret image can be retrieved in totality. There is no pixel expansion and hence storage requirement per encrypted image is same as original image without pixel expansion. The quality of the image recovered is same as the original image. The same technique can be used on binary or gray scale images also without any change in the algorithm. Visual Cryptography is an exciting era of research where exists a lot of scope. There exists various scope of enhancement in visual cryptography system. The future work is to improve the security of retrieval of the encoded message.

References

[1]. Naor and A. Shamir," Visual cryptography", Advances in Cryptology EUROCRYPT '94,M Lecture Notes in Computer Science, vol.950,no.7, pp.1–12, 1995

[2]. C.C. Wu, L.H. Chen, "A Study On Visual Cryptography", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[3]. E. Verheul and H. V. Tilborg, "Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes." Designs, Codes and Cryptography, 11(2) , pp.179–196, 1997

[4]. C. Chang, C. Tsai, and T. Chen, "A New Scheme For Sharing Secret Color Images In Computer Network", Proceedings of International Conference on Parallel and Distributed Systems, pp. 21–27, July 2000.

[5]. Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multi-Secrets Visual Secret Sharing", Proceedings of APCC2008, IEICE, 2008.

[6]. A.Incze, "Pixel Sieve method for secret sharing & visual cryptography". 9th RoEduNet IEEE International Conference 2010.

[7]. 'A Secure Keyless Colored Image Encryption', Amit B. Chougule, Nilam Nisar Shaikh, International Journal of Advanced Technology in Engineering and Science ,Volume No.02, Issue No. 12, December 2014 ISSN (online): 2348 – 7550

[8]. "RKO Technique for Color Visual Cryptography", Ms. Moushmee Kuri, Dr. Tanuja Sarode, IOSR Journal of Computer Engineering (IOSR-JCE)e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 89-93

[9]. "Survey of Visual Cryptography Schemes", P.S.Revenkar, Anisa Anjum, W .Z.Gandhare, International Journal of Security and Its Applications, Vol. 4, No. 2, April, 2010

[10]. "A Three Way Visual Cryptography& its Application in biometric Security : A Review", Mr. Praveen Chouksey, Mr.Reetesh.Rai, www.ijraset.com Volume 3 Issue V, May 2015, IC Value: 13.98 ISSN: 2321-9653

[11]. "Survey of Visual Cryptography Schemes", P.S.Revenkar, Anisa Anjum, W .Z.Gandhare, International Journal of Security and Its Applications, Vol. 4, No. 2, April, 2010

[12]. "A New Visual Cryptography Scheme for Color Images", B.SaiChandana , S.Anuradha, International Journal of Engineering Science and Technology Vol. 2(6), 2010, 1997-2000

[13]. "Visual Cryptography Scheme for Color Image Using Random Number with Enveloping by Digital Watermarking", Shyamalendu Kandar1, Arnab Maiti2, Bibhas Chandra Dhara3, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 1, May 2011, ISSN (Online): 1694-0814

[14]. "Secret Sharing Using Visual Cryptography", Renu Poriye, Dr S. S Tyagi, International Journal of Research Studies in Computer Science and Engineering (IJRSCSE) Volume 1, Issue 4, August 2014, PP 46-52 ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)

[15]. "New Visual Cryptography Algorithm For Colored Image", Sozan Abdulla, JOURNAL OF COMPUTING, VOLUME 2, ISSUE 4, APRIL 2010, ISSN 2151-9617

[16]. Champakamala .B.S, Padmini.K, Radhika .D. K, "Least Significant Bit algorithm for image steganography" International Journal of Advanced Computer Technology (IJACT), ISSN: 2319-7900

[17]. Vijay Kumar Sharma ,Vishal Shrivastava, "A Steganography Algorithm For Hiding Image in Image by Improved LSB substitution by Minimized Detection",Journal of Theoretical and Applied Information Technology, ISSN: 1992-8645