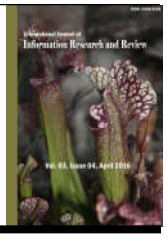
IJIRR

International Journal of Information Research and Review
Vol. 03, Issue, 04, pp. 2238-2241, April, 2016



Research Article

A NEW VISUAL CRYPTOGRAPHY SCHEME FOR COLOR IMAGE USING SLIDING PUZZLE TECHNIQUE

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

[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

ARTICLE INFO

Article History:

Received 22nd, January 2016
Received in revised form
19th, February 2016
Accepted 24th, March 2016
Published online 27, April 2016

Keywords:

Visual Cryptography,
Encryption,
Decryption, Color Image.

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. In visual cryptography the decipher can be performed by human visual system (HVS) without any complex process, providing high security. Our proposed method suggested a way to encrypt a color image using symmetric key encryption procedure. 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.

INTRODUCTION

In recent days, security is a big threat in the transmission medium due to the development of the Internet andmultimedia 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 (Moni Naor and Adi Shamir, 1995) 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.

****Corresponding author: Samir Kumar Bandyopadhyay,***
Department of Computer Science and Engineering, University of Calcutta, India.

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 sliding puzzle technique in which every block of image is used as a puzzle block and need to be arranged in an orderly manner.

Existing Work

Black and White Visual Cryptography Schemes

Sharing Single Secret

Naor and Shamir's (Moni Naor and Adi Shamir, 1995) 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 Table 1 is chosen to generate Share1 and Share2. Similarly If pixel is black one of the below two rows of Table 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.

Sharing Multiple Secrets

Wu and Chen (Wu and Chen, 1998) 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 (Verheul and Tilborg, 1997). 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 (Chang *et al*., 2000) 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*. (2008) 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.

Proposed Method

Our proposed method is a hybrid approach of Visual Cryptography where we take the color image and split the image into multiple rows and columns, resulting image tiles.

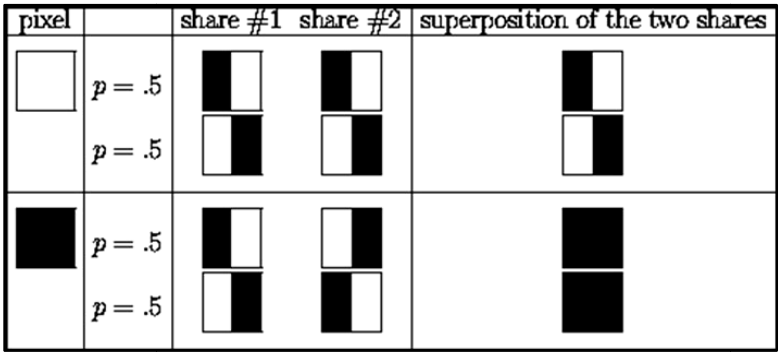


Figure 1. Naor and Shamir's scheme for encoding a binary pixel into two shares

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

Authors Year	Pixel Expansion	Number of Secret Images	Image Format	Type of Share generated
Naor and Shamir [10]-1995	1	4	Binary	Random
Wu and Chang [12] 2005	2	4	Binary	Random
VerheulTilborg [14]	1	C*3	Color	Random
Tzung-Her Chen et al [13] 2008	n(n>=2)	4	Binary, gray, Color	Random
Chang and Tsai [15]	1	529	Color	Meaningful
Proposed Algorithm	1	1	Color	Random

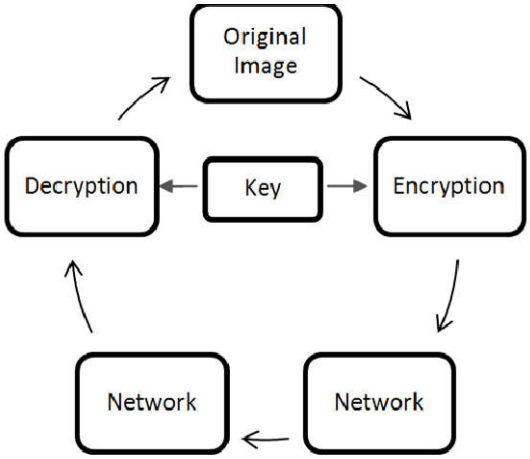


Figure 2.Flow chart representation of the proposed scheme

Figure 3. Experimental results of Encryption and Decryption process 128*128 color image

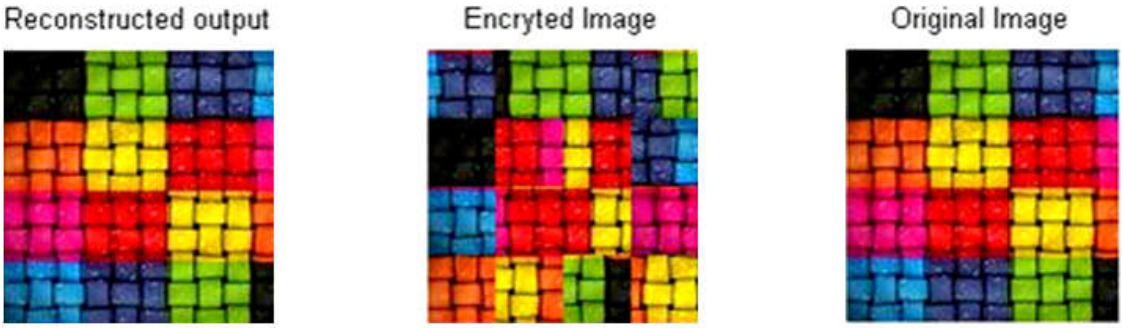


Figure4. Experimental results of Encryption and Decryption process 128*128 color image

Then these tiles are rearranged in a random order generating the encrypted form. For decryption we have (row*col)! combinations among which only one gives back the original image. For this we are using symmetric key. The quality of the image revealed is same as the original image. This algorithm has perfect reconstruction property and there is no loss of picture quality. This algorithm can also be used on gray scale and binary images without any loss of image quality.

MATERIALS AND METHODS

The proposed scheme can be design and implemented in following manner.

Step 1: Split into image tiles

Step 2: Re-arrange the tiles randomly

Step 3: Retrieval of original image using symmetric key

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 techniqueencrypts the color image using the following steps.

Step 1: In this step the color image is fed into cryptosystem and divided into multiple rows and columns creating image tiles of equal size so that we can replace any two of them for creating a new image.

Step 2: Then the image tiles are re-arranged in a new way by using sliding puzzle technique which is sent into receiver through a communication channel. This is done in such a way so that it is impossible to get any idea of the original image visually, which can be achieved by increasing the number of divisions.

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

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 encrypted form can be transmitted on an unsecure channel.

Experimental Results

In this process we have taken two natural images for our experiment purpose. We can consider any sized natural as well as secret image for visual cryptography.For encryption it takes 0.522679 seconds and at the receiver side it takes 0.031978 seconds for 128*128 sized secretimages. If the key length is increased the system will become more secure.As stated earlier, the efficiency of any cryptosystem depends on the quality of the reconstructed image. We used the Structural Similarity (SSIM) index (16) for measuring the quality between two

images. The SSIM index can be viewed as a quality measure of one of the images being compared provided the other image is regarded as of perfectquality. The quality measures are calculated between the original image and the encrypted/decrypted image. Table2 shows the quality measures of the images in figure 3 and in figure 4.

Table 2. SSIM Index

Image	SSIM index for fig. 3	SSIM index for fig. 4
Original Image	1	1
Encrypted Image	0.3	0.3
Decrypted Image	1	1

Conclusion and Future Work

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. Encryption is carried out based on RGB value of the pixels. 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. This scheme can be extended for multiple colored images and providing more security.

REFERENCES

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

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

"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

"New Visual Cryptography Algorithm ForColored Image", Sozan Abdulla, JOURNAL OF COMPUTING, VOLUME 2, ISSUE 4, APRIL 2010, ISSN 2151-9617

"RKO Technique for Color Visual Cryptography", Ms. MoushmeeKuri, Dr. TanujaSarode, 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

"Secret Sharing Using Visual Cryptography",RenuPoriye,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)

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

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

"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

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.

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

Moni Naor and Adi Shamir, "Visual Cryptography", advances in cryptology– Eurocrypt, pp 1-12,1995.

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

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

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

Wang, Z., Bovik, A. C., Sheikh, H. R. and Simoncelli, E. P. 2004. "Image quality assessment: From error visibility to structural similarity". IEEE Transactions on Image Processing, April. 13(4): 600-612.

****