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
www.iosrjournals.org

RKO Technique for Color Visual Cryptography

Ms. Moushmee Kuri[1], Dr. Tanuja Sarode[2]
[1](Computer Department, W.I.E.E.C.T/ Mumbai University, India)
[2](Computer Department, T.S.E.C/ Mumbai University, India)

Abstract : *To maintain the secrecy and confidentiality of images two different approaches are being followed, Image Encryption and Visual Cryptography. The former being encrypting the images through encryption algorithms using keys, and the later approach involves dividing the image into random shares without the use of keys. Unfortunately heavy computation cost and key management limit the employment of the first approach and the poor quality of the recovered image from the random shares limit the applications of the second approach. In this paper we propose a novel approach with the use of random share and key share. The approach employs generating two shares of the original image. One random share and the other key share. The original secret image can be recovered from the two shares simply by Xoring the two shares without any loss of image quality.*
Keywords: *Visual Cryptography , Overlapping , Shares, Image Encryption, Keyless Encryption, Color images*

I. INTRODUCTION

The advent of internet introduced to its users a whole new dimension as to how images can be shared from one part of the world to the other in near real time. However along with these opportunities came the challenges, such as, how to maintain the confidentiality of the image being transmitted. And also the required amount of computation to encrypt the images and the overhead required to maintain the keys and perform the computation is a matter of concern. This 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. Since it can be employed by anyone without any cryptographic knowledge and does not require any computations while decrypting, many researches' have been focused on it. 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[4].

Most of the techniques which are employed on color images such as does 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 called RKO technique for visual cryptography of color images based on past studies in black-and-white visual cryptography. In this method encryption is done by creating two shares of the original image called key share and random share. While decryption is done just by XORing the two shares. This method can also be used on gray scale images, too. The retrieved image is same as original and no loss of picture quality occurs. The proposed technique requires no pixel expansion, number of secret images is two and creates random shares.

II. REVIEW OF LITERATURE

The Various methods have been employed for maintaining secrecy and confidentiality of images.

2.1 Image Encryption (using Keys)

This approach is basically similar to the conventional encryption methods which involve using an algorithm (and a key) to encrypt an image. Some of the proposed techniques for encrypting images use "Digital Signatures" , "Chaos Theory" , "Vector Quantization" etc. to name a few. There are some inherent limitations with these techniques; they involve use of secret keys and thus have all the limitations as regards key management. In addition, in some cases the available keys for encryption are limited (restricted key space). Also high computation involved in encryption as also weak security functions are also an issue. However the greatest strength of most of these schemes is that the original image is recovered in totality[5].

1.2 Visual Cryptography (Image Splitting)

The idea of Image splitting more often referred to as Visual Cryptography Schemes (VCS) involves splitting a secret image into n random shares such that these shares individually reveal no information about the secret image (but for its size) but a qualified subset of the shares(as specified by the encrypter) when stacked up reveal the secret image. The random image shares (qualified set) are merely printed on transparencies and

stacked up revealing the original image). The major issues which restrict its employment is the poor quality of the recovered image limited color representation[5].

1.3 Hybrid Approach

In this approach using some kind of an encryption key the image is split into random shares. This scheme proposed the concept of sieves for encrypting images. Sieve is typically a binary key. The original image is placed over the sieve. Pixels from the original image situated above a hole of the sieve go through and form one share of the image. The pixels that stay on the sieve on a black pixel will form the other share[3].

Many research papers have been published using this approach, starting from a binary image [7, 9] moving to grayscale image [11] and finally employing it to color images[12, 13]. Though with each subsequent research paper the quality of the recovered image improved, however, but for [14] no other scheme was able to completely recover the original image from the shares. When evaluating the performances of these suggested solutions they are often evaluated on performance measures such as contrast, accuracy, security, computational complexity etc. Thus an ideal solution would regenerate the original image from the shares in terms of colors and contrast, it would also have to be secure and computationally inexpensive. Table I gives a comparison of six such techniques.

TABLE I. COMPARISON OF VISUAL CRYPTOGRAPHY SCHEMES [5]

Authors Year	Pixel Expansion	Number of Secret Images	Image Format	Type of Share generated
Naor and Shamir [1]-1995	1	4	Binary	Random
Wu and Chang [9] 2005	2	4	Binary	Random
Chin-Chenet.al [10] 2005	1	4	Binary	Meaningful
Tzung-Her Chen et al [11] 2008	n(n>=2)	4	Binary, gray, Color	Random
F. Liu et al [3] 2008	1	1	Color	Random
Du-Shiau Tsai et al [12] 2009	1	9	Color	Meaningful

III. PROPOSED METHOD

3.1 Method Definition

Our proposed method is a hybrid approach of Visual Cryptography where we take the color image and split the image into two shares. The first share is the random share and the second share is the key share. These two shares have no resemblance to the original image. When the two shares are combined using XOR it reveals the original image. 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 images without any loss of image quality.

3.2 RKO Algorithm

The proposed method involves there steps:

Step 1 : **R**andom Share generation

Step 2 : **K**ey Share generation

Step 3 : **O**verlapping the two shares

In additive model or RGB model [5] every color image is composed of pixels where each pixel is a series of bits composed of RGB values. 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 RKO technique proposed by us creates the two shares using step 1 and step 2 of the algorithm.

In step 1 : Random Share generation, a random share is generated by taking any random value for R,G and B for each pixel. The size of the share is same as the original image. Every time we create a random share it gives a different value for each pixel. So no two random shares of the same image are same.

In step 2 : Key share generation, a key share is generated by xoring every pixel of random share with every pixel of the original image. The size of this share is also same as the original image. No two key shares of the same image are same since no two random shares are same.

In step 3 : Overlapping of the shares is done by xoring the random share with the key share pixel by pixel. This results in the generation of the original image.

Algorithm RKO ( )
{
For every pixel i=0 to n
{
$RS_i = R_{(0-255)} + G_{(0-255)} + B_{(0-255)}$

$KS_i = RS_i \oplus OI_i$

}
$OI = RS \oplus KS$
} /* OI = Original Image */

3.3 Implementation Details

RKO technique was implemented using JAVA on Windows XP where two functions RGBencrypter and RGBdecrypter were used. RGBencrypter encrypts the image by creating the two shares : random and key share. RGBdecrypter decrypts the image by XORing both the shares pixel by pixel. This functions can work for both color images as well as gray scale images.

In our proposed technique both during encryption and decryption the computation cost is low since the majority of the operations use logical XOR operators. In our proposed scheme there are no keys involved and hence there is no key management. All that is required is to transmit key share on a secret channel while random share can be transmitted on an unsecure channel.

IV. EXPERIMENTAL RESULTS

4.1 Color Image

The RKO technique was implemented on color image showed in Fig.1. The two shares of the image are share1 and share2 shown in Fig 2 and Fig 3 respectively. The resultant image after overlapping both the shares is shown in Fig 4.

Fig 1. Color Image

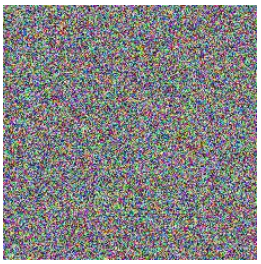

Fig 2 . Share 1

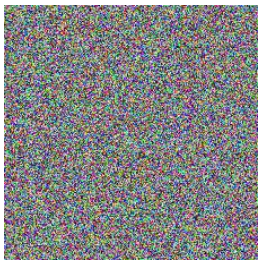

Fig 3. Share 2

Fig 4. Resultant image

1.4 Gray Scale Image

The RKO technique was also implemented on gray scale image shown in Fig 5. The two shares of the image are share1 and share2 shown in Fig 6 and Fig 7 respectively. The resultant image after overlapping both the shares is shown in Fig 8.

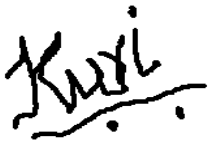

Fig 5. Gray scale Image

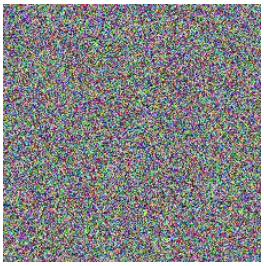

Fig 6 . Share 1

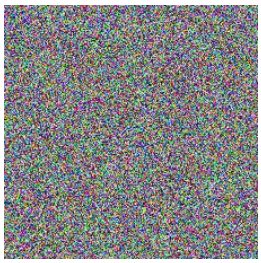

Fig 7. Share 2

Fig 8. Resultant image

In [12] the quality of the recovered image is almost similar to the original secret image, however the fact remains that the recovered image is not same as the original secret image. In our proposed scheme the recovered image is an exact replica of the original image as no data is lost during the RKO operations. The results were validated using Normalized Correlation (NC). NC is used to measure the correlation between the original secret image and the recovered images from the random shares.

$$NC = \sum_{i=1}^{w} \sum_{j=1}^{h} \frac{\overline{(Sij \oplus Rij)}}{w \times h}$$

S represents the secret image and R the recovered image. w, h represents the width/height of the photographs and $\oplus$ represents the exclusive OR operator. We repeated the test over multiple images, the NC for all the recovered images was 1.000. The generated shares are highly secure as the spatial correlation between the pixels is eliminated by employing the randomization function thrice for each pixel value per share. A comparison of our scheme with similar other schemes is listed in Table II.

TABLE II COMPARISON OF TECHNIQUES

SCHEMES				
FEATURES	**RKO TECHNIQUE**	**Tsai, Chen et.al. [12]**	**Lukac, and Plataniotis [13]**	**Chang and Yu's scheme [14]**
Noise Correlation	Always 1.000	Always< 1.000	1.000	Always< 1.000
Image delivery Transparency	No	Yes	No	Yes
Additional Data Structure	No	Yes AX, BX	No	Yes S-E table (Local)
Key Management	No	Yes S, BX have to be kept secret	No	No
Pixel Expansion (256 color, (n, n) scheme)	No expansion	1 : 9 expansion	1: $2^{(n-1)}$	1 : 529

V. Conclusion

In this paper a new enhanced hybrid Visual Cryptography technique is presented. It is a hybrid of the traditional VCS and the conventional image encryption schemes. A secret image is split into two images, one random image and one key image and with minimum computation the original secret image can be retrieved back.

The proposed algorithm has the following merits (a) The original secret image can be retrieved in totality (b) There is no pixel expansion and hence storage requirement per random share is same as original image (c) Key management is not an issue since there are no secret keys involved as encryption is carried out based on RGB value of the pixels (d) the scheme is robust to withstand brute force attacks. (e) the quality of the image recovered is same as the original image. (f) The same technique can be used on gray scale images also without any change in the algorithm.

The scheme is suitable for authentication based application [2] where authentication can be done by overlapping the shares over one another to reveal the secret image. If the secret image matches the original image then only access can be granted[2].

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in Proc. *EUROCRYPT' 94, Berlin, Germany, 1995, vol. 950, pp. 1–12, Springer-Verlag, LNCS*

[2] Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana, " Novel Authentication System Using Visual Cryptography", *in 2011 World Congress on Information and Communication Technologies.*

[3] F. Liu1, C.K. Wu X.J. Lin , "Colour Visual Cryptography Schemes", *IET Information Security, vol. 2, No. 4, pp 151-165, 2008.*

[4] Y. C. Hou, "Visual cryptography for color images," *Pattern Recognition, vol. 36, pp. 1619-1629, 2003.*

[5] Siddharth Malik, Anjali Sardana, Jaya "A Keyless Approach to Image Encryption", *2012 International Conference on Communication Systems and Network Technologies*

[6] L. W. Hawkes, A. Yasinsac and C. Cline, "An Application of Visual Cryptography to Financial Documents," *Technical report TR001001,Florida State University, 2000.*

[7] George Abboud, Jeffrey Marean, Roman V. Yampolskiy, "Steganography and Visual Cryptography in Computer Forensics", *in 2010 Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering*

[8] A. Shamir, "How to share a secret," *Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.*

[9] H.-C. Wu, C.-C. Chang, "Sharing Visual Multi-Secrets Using Circle Shares", *Comput. Stand. Interfaces 134 (28) ,pp. 123–135, (2005).*

[10] Chin-Chen Chang, Jun-Chou Chuang, Pei-Yu Lin , "Sharing A Secret Two-Tone Image In Two Gray-Level Images", *Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05), 2005.*

[11] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multiple-Image Encryption By Rotating Random Grids", *Eighth International Conference on Intelligent Systems Design and Applications, pp. 252-256 , 2008.*

[12] Du-Shiau Tsai , Gwoboa Horng , Tzung-Her Chen , Yao-Te Huang , "A Novel Secret Image Sharing Scheme For True-Color Images With Size Constraint", *Information Sciences 179 3247–3254 Elsevier, 2009.*

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

[14] C.C. Chang, T.-X. Yu, Sharing a secret gray image in multiple images, in: Proceedings of First International Symposium on Cyber orlds, 2002, pp.230–240.