IJCAT International Journal of Computing and Technology, Volume 1, Issue 4, May 2014
ISSN : 2348 - 6090
www.IJCAT.org

Hierarchical Implementation of RKO Technique for Visual Cryptography

[1] Ms. Moushmee Kuri, [2] Dr. Tanuja Sarode

[1] Computer Department, WIEECT , Mumbai University
Worli, Mumbai-Maharashtra, India.

[2] Computer Department, TSEC, Mumbai University
Bandra, Mumbai-Maharashtra, India.

Abstract - This paper describes the concept of hierarchical visual cryptography using RKO technique. The key idea behind hierarchical RKO is to encrypt the secret information in number of levels. As the number of levels in hierarchical visual cryptography increases, the secrecy of data tends to increase. The shares generated out of Hierarchical visual cryptography are found to be random giving no information. The RKO technique generates two shares of the original image: one random share and the other key share. These shares are further divided into four more shares using the same RKO technique. From these four shares two final shares are generated. The original secret image can be recovered from the two shares simply by XORing the two shares without any loss of image quality. If any shares other than final shares are XORed it won't reveal the original image.

***Keywords*- Visual Cryptography, Hierarchical, RKO technique, Color image, Shares.**

1. Introduction

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. A hybrid approach of Visual Cryptography called RKO technique[16] takes the color image and splits 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.

Hierarchical visual cryptography[15] encrypts the secret in number of levels. Initially the secret is divided into exactly two share called share 1 and share 2. Each share is then encrypted independently resulting in four shares: share 11, share 12, share 21 and share 22. Later, among these four shares, any three shares are chosen to generate the key share. The superimposition of key share with the remaining share reveals the secret information. The superimposition is logically performed by the X-OR operation. As the level of encryption in hierarchical visual cryptography increases, secrecy tends to increase.

Figure 1 indicates the concept of hierarchical RKO technique.

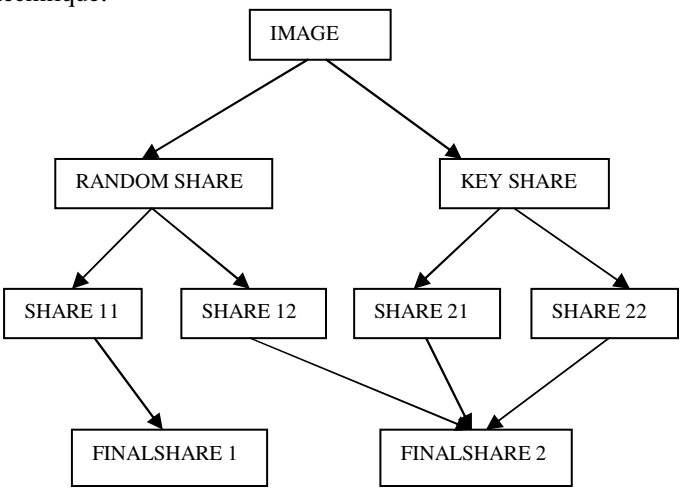

Fig. 1 Hierarchical RKO

.

2. RKO technique for Visual Cryptography

The RKO technique can be used which splits 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[16].

2.1 Algorithm[16]

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
{

$RS_i = R_{(0\text{-}255)} + G_{(0\text{-}255)} + B_{(0\text{-}255)}$

$KS_i = RS_i \oplus OI_i$

}

$OI = RS \oplus KS$

} /* OI = Original Image */

3. Hierarchical Implementation of RKO

Step 1 : Select an input image

Step 2 : Create two shares of the image called initial_share1 and initial_share2 using RKO

Step 3 : Initial_share1 is the random share and initial_share2 is the key share created by XORing original image with the random share.

Step 4 : From initial_share1 create share11 and share12 again using RKO technique.

Step 5 : Share11 is the random share and share12 is the XORing of initial_share1 and share11.

Step 6 : From initial_share2 create share21 and share22 again using RKO technique.

Step 7 : Share21 is the random share and share22 is the XORing of initial_share2 and share21.

Step 8 : Select Share11 as the finalshare1.

Step 9 : Create finalshare2 by XORing of share12 , share21 and share 22.

The finalshare2 is created using Truth Table 1.

To recover the original image we can overlap finalshare1 and finalshare2. The original image can also be recovered by overlapping initial_share1 and initial_share2. But overlapping of no intermediate shares: share11, share12, share21, share22 will reveal the image.

Table 1 :Truth table indicating pixel value in finalshare2

Share12	*Share21*	*Share22*	*FinalShare2*
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

4. Implementation

4.1 Details

The hierarchical implementation was implemented in JAVA. The encryptor function implements the RKO technique to create initial_share1 and initial_share2. It also creates share11 and share12 from initial_share1 using the same RKO technique and share21 and share22 from initial_share2. The decryptor function overlaps the selected share by XORing the two images pixel by pixel using the XOR truth table given in Table 2.

Table 2: Truth Table for XOR

A	***B***	O/P
0	0	0
0	1	1
1	0	1
1	1	0

4.2 Results

A image was taken and encrypted using RKO technique of visual cryptography to create initial shares : initial_share1 and initial_share2. Initial_share 1 is further broken down into share11 and share 12 using RKO technique. Same way Initial_share 2 is further broken down into share21 and share 22 using RKO technique.

Initial_share1 becomes the finalshare1. Share12, Share21 and Share22 are XORed to obtain Finalshare2. When Finalshare1 and Finalshare2 are overlapped (XORed) , we obtain the original image back without any loss of quality as shown in figure 2.

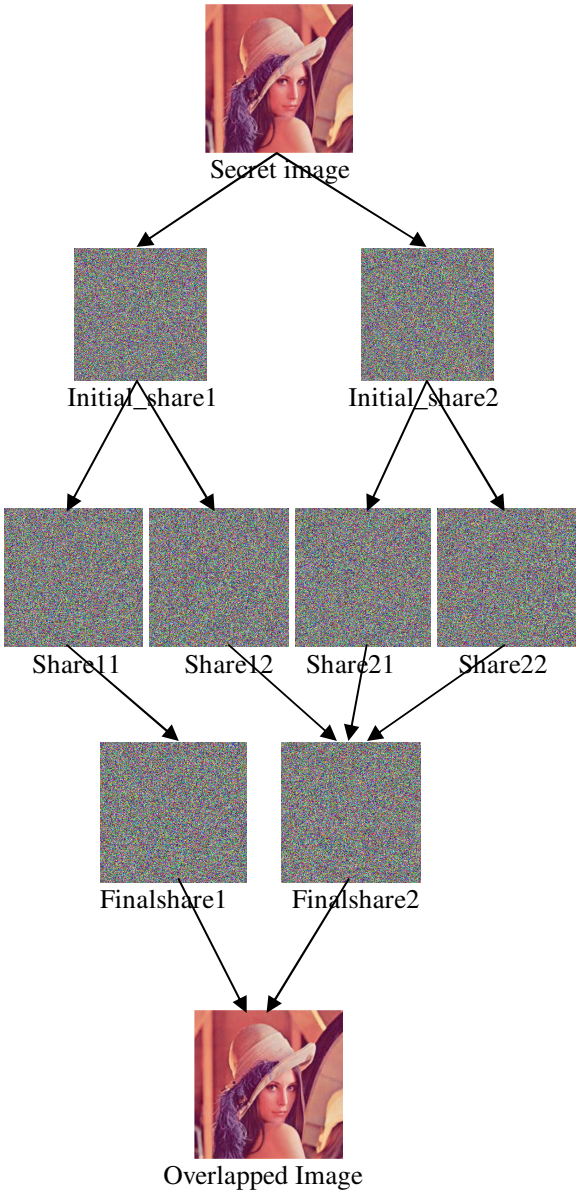

Fig. 2 Result for Hierarchical RKO .

In our proposed scheme the overlapped image is an exact replica of the original image as no data is lost during the RKO operations. Hence hierarchical RKO technique has perfect reconstruction property. This can be 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

⊕ represents the exclusive OR operator. We repeated the test over multiple images, the NC for all the recovered images was 1.000. A comparison of RKO scheme with similar other schemes is listed in Table 3.[5].

Table 3. Comparison of Visual Cryptography Techniques

SCHEMES				
FEATURES	***HIERAR-CHICAL RKO TECHNIQUE [16]***	***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

5. Conclusions

The proposed implementation 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[16].(e) Due to the hierarchical implementation, the randomness in the shares increases so its impossible to guess the original image by looking at any of the shares. (f) No intermediate shares can reveal the original image when combined.

Acknowledgments

Ms. Moushmee Kuri thanks the guide and TSEC for giving the support and opportunity to carry out the research work in the Visual Cryptography and come up with a new technique called RKO technique and take it to one more level by making it hierarchical.

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] Bhavani, A. B. "Cross-site Scripting Attacks on Android WebView." arXiv preprint arXiv:1304.7451 (2013).

[12] 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.

[13] 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.

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

[15] 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.

[16] Pallavi V. Chavan and Dr. Mohammad Atique "Design of Hierarchical Visual Cryptography" 2012 Nirma University International Conference on engineering, nuicone-2012, 06-08december, 2012, IEE 2013.

[17] Ms. Moushmee Kuri, Dr. Tanuja Sarode, "RKO Technique for Color Visual Cryptography", in : 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

Ms. Moushmee Kuri has received B.E.(Computer Engg) from Goa University in 1998, pursuing M. E. Compter Engg from Thadomal Shahani College of Engineering, Bandra, Mumbai, Working as Assistant Professor in Computer Dept. at Watumull Institute of Electronics Engg and Computer Technology., Worli Mumbai. She has more than 10 years of experience in teaching. Has published two papers in the field of Visual Cryptography. Her areas of interest are system Security, system programming and Image Processing.

Dr. Tanuja Sarode has Received Bsc.(Mathematics) from Mumbai University in 1996, Bsc.Tech.(Computer Technology) from Mumbai University in 1999, M.E. (Computer Engineering) from Mumbai University in 2004, Ph.D. from Mukesh Patel School of Technology , Management and Engineering, SVKM's NMIMS University, Vile-Parle (W), Mumbai, INDIA. She has more than 14 years of experience in teaching. Currently working as Associate Professor in Dept. of Computer Engineering at Thadomal Shahani Engineering College, Mumbai. She is life member of IETE, member of International Association of Engineers (IAENG) and International Association of Computer Science and Information Technology (IACSIT), Singapore. Her areas of interest are Image Processing, Signal Processing and Computer Graphics. She has 55 papers in National /International Conferences/journal to her credit.