A NOVEL APPROACH TO VISUAL CRYPTOGRAPHY USING RANDOM NUMBER GENERATOR

Ankita Saxena$_1$, Vinay Rishiwal$_2$, Amit Doegar$_3$

$_1$ Researchscholar, ^{3}Asst.Professor, NITTTR, Chandigarh (India)

^{2}Asst.Professor, MJPRU, Bareilly (India)

ABSTRACT

Visual Cryptography is one of the efficient methods for secure image transmission, which adopts the technique to hide information in images in such a way that it can be decrypted by human visual system. The beauty of this technique is that decryption does not require any complex computations. Many variants of secret image sharing schemes are available in the literature. But yet there are certain issues which are being least focused upon. In VSS, a secret image is broken into number of random shares which separately reveals no information about the secret image except the size of the secret image. The secret image can be reconstructed by stacking the shares. The basic requirement is how to reconstruct the (k,n) threshold for share generation and how to superimpose them to get the original image data. In this paper, A new approach has been proposed which applies the concept of halftoning and a new k-n secret sharing scheme where shares are generated using a random number generator.

Keywords: Visual Secret Sharing, Halftoning ,Pixel Expansion, Image Transmission, Security Random Number Generator

I. INTRODUCTION

Various sensitive data such as credit card information, personal health information, military maps and personally identifiable information are transmitted over the Internet. Multimedia information is also transferred over the Internet conveniently, with the advancement of technology. Therefore, the protection of the digital data has become an area of critical research. To solve the problem of data theft, various techniques have been developed under a stream of science termed as Cryptography. Data remains more intact in the form of image and hence an information security technique called visual cryptography scheme was invented by Naor et al in 1994 [1].

Human visual system can decode secret (handwritten notes, printed text and pictures etc.) directly without performing any computations. and their vision acts as an OR system i.e if 2 transparent objects are stacked together, final stack=transparent but if any one of them is nontransparent final will also be nontransparent .Which means—0 OR 0=0 ,1 OR 0=1 ,0 OR 1=1,1 OR 1=1 where 0=transparent and 1= nontransparent. Simplest visual cryptography scheme is given by following structure. A secret image will be made up of a gathering of black and white pixels, where each pixel is served independently [1]. To encrypt the image, we split the image into n modified versions such that each pixel in a share subdivides in *m* black and white sub-pixels [1].For deciphering the image, we pick a subgroup S of those n shares. If S is a “qualified” subset, then stacking all these shares will allow recovery of the image. In this paper the idea is to divide a digital color image into n number of shares where a minimum k shares are sufficient to reconstruct that image. If in image certain position of a pixel is 1,then in (n-k)+1 no of shares will also have 1 and the remaining shares will have that position as 0.So a random number generator is used to identify those shares.

There are various other schemes working on the same pattern for carrying out Visual Cryptography on gray and colored single or multiple images..Paper [16] gives the standard definition of a (k; n) threshold secret sharing scheme and its properties.& continue by exploring polynomial evaluations as the mathematical background for Shamir's scheme. In [17] exploits the human visual system to decrypt secret images without computation, but also have the backward compatibility with the previous results in black-and-white visual cryptography, such as the t out of n threshold scheme, and can be applied to gray-level and color images easily .In [18] two k-out-of-n secret sharing schemes are incorporated i.e

Shamir’s secret sharing scheme and matrix projection secret sharing scheme. which allows a colored secret image to be divided as n image shares that are sufficient to reconstruct the secret image in the lossless manner and fewer image shares cannot get enough information to reveal the secret image. In [19]scheme for multiple secret image is proposed which uses a stacking relationship graph of secret pixels and generates the share blocks indicating the encryption functions, which makes the number of secret images not restricted and extends it to be general. In [20] procedure is given to transform a color secret image into three C, M, and Y halftone images. Then, every pixel of the halftone images is expanded into a 2×2 block to which a color is assigned according to the model Every block of the sharing images therefore includes two transparent (white) pixels and two color pixels so that the entropy reaches its maximum to conceal the content of the \secret image. Furthermore ,they have designed a half black-and-white mask to shade unexpected colors on the stacked sharing images so that only the expected colors show up.

II. HEADINGS

1. Introduction
2.Related work.
3.Proposed algorithm
3.1 Encryption algorithm.
3.2 Reconstruction-Decryption Algorithm
4.Performance of proposed scheme.
5.Results
6.Conclusion

III. INDENTATIONS AND EQUATIONS

IV. FIGURES AND TABLES

Figure 1. Structure of a 32-bit pixel

Figure 2.Human Visual System as OR function

Figure 3.Source Image

Figure 4. Encrypted Shares

Figure 5. Final Image Reconstructed .

Table 1. Comparison of proposed scheme with two traditional approaches

V. CONCLUSION (11 , TIMES NEW ROMAN, BOLD)

Here a new idea is proposed which utilizes the concept of half toning and stacking of the shares which are bitwise –ored together to generate the newly reconstructed image which appears close in proximity to original image. If number of shares to be taken for the reconstruction are less than k than it results to generate a distorted image.

This scheme can be further improved by keeping the problem of contrast loss and pixel expansion into consideration. Camouflaging with maximum density process can be used to improve the problem of pixel expansion and contrast loss.Also this scheme can be further extended to be used for multiple images and also some scret keys can be taken to encode the original image to some encoded form and than apply the encryption algorithm.

REFERENCES

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

[2]. H. C. Hsu, T.-S. Chen, Y.-H. Lin, "The Ring Shadow Image Technology Of Visual Cryptography By Applying Diverse Rotating Angles To Hide The Secret Sharing", *In Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control*, Taipei, Taiwan, March 2004, pp. 996–1001.

[3]. Liguo Fang, BinYu, "Research On Pixel Expansion Of (2, n) Visual Threshold Scheme", *1st International Symposium on Pervasive Computing and Applications*, IEEE, 2006, pp. 856-860.

[4]. 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, pp. 300-304.

[5]. Feng Liu,Chuankun Wu Embedded Extended Visual Cryptographic Schemes, Vol.6,No.2 IEEE Transaction on Information Forensics ans Security, June 2011.

[6]. 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.

[7]. Jung-San Lee, T. Hoang Ngan Le, "Hybrid (2, N) Visual Secret Sharing Scheme For Color Images", 978-1- 4244-4568-4/09, *IEEE*, 2009.

[8]. W. Hawkes, A. Yasinsac, C. Cline, An Application of Visual Cryptography to Financial Documents, technical report TR001001, Florida State University (2000).

[9]. Z. Zhou, G. R. Arce, and G. Di Crescenzo, Halftone visual cryptography, Vol.58,No.7 IEEE Transaction on Image Processessing ,Aug. 2006.

[10]. Young-Chang Hou,"Visual Cryptography for Color images",www.elsevier.com/locate/patcog Aug 2002. Amos Beimel,"Secret schemes for secret sharing and key distribution",Research thesis,Israel Institute of Rudolph Ahlswede & Imre Crizar,"Common Randomness in information theory & Cryptography: Secret Sharing", IEEE Transaction on Information theory,VOL 39,JULY 1993.

[11]. Madhuri ghuge ,Prof Kanchan Duke,"A comprehensive study on various visual cryptography schemes with an application" IJETAE,Vol 4,Issue 2, Feb 2014.

[12]. Yuliang Zheng ,Thomas Hardjonos,Jennifer seberry,"Reusing shares in Secret sharing

Schemes”,Computer

[13]. Journal,University of Wollong,1994.

[14]. Nazanin Askari,Cecilia Moloney,”A novel Visual Secret Sharing Scheme without Image Size Expansion”,Electrical and computer engineering,Memorial University of New Foundland,St Johns,Canada.

[15]. Dan Bogdanov,” Foundation and properties of shamir’s secret sharing scheme”,Research Seminar in Cryptography,University of Tartes,may 2007.

[16]. Li Bai, Saroj Biswas, Albert Ortiz, Don Dalesandro,”An Image Secret Sharing Method”,Institute of information technology, IEEE Explore.

[17]. Talal Mousa Alkharobi, Alleem Khalid 2009 Alvi, ”New Algorithm for halftone Image Visual Cryptography”,King Fahd University of pete and min Dahran.

[18]. Ch Ratna Babu, M Sridhar,B Raveendra Babu,”Improved PRVC Algorithm for Halftone Images” National conference on emerging trends in IT-2013,www.elsevier.com

[19]. Aarti,Pusphpendra k Rajput,”Multiple Secret sharing scheme with gray level Mixing using Evcs”,IJCA-Issue and Challenges in Networking Intelligence and Computing Technology 2012.

[20]. Chang-Chou Lin,Wen-Hsiang Tsai,”Visual Cryptography on gray level images by Dithering techniques”,www.elsevier,com/locate/patrec.

[21]. N. Askari, H.M. Heys, and C.M. Moloney, "An Extended Visual Cryptography Scheme Without Pixel Expansion for Halftone Images", Proceedings of IEEE Canadian Conference on Electrical and Computer Engineering (CCECE 2013), Regina,Canada,May2013.

[22]. Shyamlendu kandar ,” k-n secret sharing scheme forVSSS using random number generator.”,IJEST-Issues and Challenges Of Upcoming Security Threats And Information Technology.2013