International Journal of Engineering Technology and Applied Science

(ISSN: 2395 3853), Vol. 5 Issue 8 August 2019

"SURVEY OF VARIOUS VISUAL CRYPTOGRAPHY METHODS TO IMPROVE SECURITY IN IMAGE TRANSACTION

Ranjana Rathore[1]
ranjanajadon@yahoo.co.in
M. Tech Scholar, RKDF University
Department of Computer Science & Engg

Mr. Gagan Sharma[2]
M. Tech Guide, RKDF University
Department of Computer Science & Engg

Abstract- ***Picture cryptography assumes a significant job in information security. Visual cryptography is a technique which is utilized to encode data in any organization like content, picture, drove show to such an extent that unscrambling is finished by human eye. It doesn't require any key for unscrambling so security during picture change is constantly alluring yet testing errand. Fast development in the methods for doing as such is additionally expanding. Web has turned out to be most generally utilized media for correspondence and subsequently message, voice, video, Images and a lot more are transmitted through Internet. These might incorporate Military Secrets, Commercial Secrets and Information of people and accordingly it must be transmitted by more secure methods with improved security. During the time spent Visual Cryptography a mystery picture is scrambled into offers which will not reveal data about the first mystery picture. Different specialists are chipping away at progress of security includes in picture exchange. In this audit paper we are displaying examination of different visual cryptography strategies for and security upgrade procedures during picture exchanges.***

Keywords- Image Security, Security, Visual Cryptography, Visual Secret Share

1. INTRODUCTION

Because of fast improvement in web innovation, various kinds of data can be moved over web. Thus there is security issues related with transmitting high worth resources like business information, client individual data, banking or exchange information, and information identified with military. Security of such information move must be thought about in light of the fact that programmer can utilize different techniques and take such high worth resources which results in high fiscal, social, individual misfortune. Visual mystery sharing (VSS) conspire is an effective secure technique for concealing a mystery picture by isolating it into offer pictures and any one can interpret it effectively by the human visual framework. The fundamental idea of the first visual mystery sharing (VSS) plot is to encode a mystery picture into n inane offer pictures. It can't release any data of the mutual mystery by any blend of the n offer pictures with the exception of all of pictures [4, 5].

When it isn't changed into Cipher content, human nor can machine appropriately process it until it is decoded. This empowers the transmission of classified data over unreliable channels without unapproved divulgence. At the point when information is put away on a PC it is secured by legitimate and physical access controls. At the point when this equivalent delicate data is sent over a system, the data is in significantly more helpless state. Naor and Shamir presented the new idea of Visual Cryptography in 1994[11], requiring no calculation aside from human Visual System to decode. They proposed an essential (2, 2) Visual Cryptography plot where a mystery picture is isolated into 2 shares, uncovering the mystery picture through Share Stacking. Picture that can be considered for Visual Cryptography can be Binary Image, Grayscale Image and Color Image. The plan given by Nair and Shamir for sharing a mystery double picture was by utilizing their very own coding table. In this plan the double picture is isolated into two offers, for the white pixel in the mystery picture, one of the upper two lines of table I is picked to make share1 and share2. On the off chance that the pixel of the mystery picture is dark, one of the lower two columns of table I is utilized to make share1 and 2. This plan comprises of pixel development where each pixel from the mystery picture is extended to 4 pixels, so when the offers are produced and superimposed together the reproduced picture will be multiple times the first mystery picture size on account of this pixel extension. Additionally the goals of the recreated picture will be not exactly the first mystery picture as each white pixel is

deteriorated into two white and two dark pixels. Just a single mystery could be concealed utilizing this system [6, 7, 8].

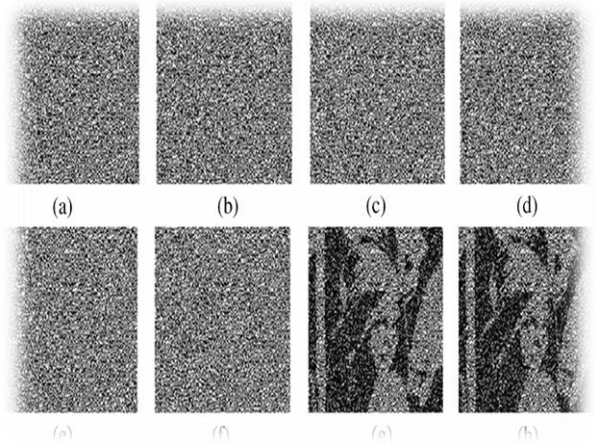

Figure 1: Visual Cryptography

2. RELATED WORK

Arya k.rakhee baiju et al [1] worked on A Novel Visual Cryptographic Scheme for Improved Binary Image Quality. According to Arya Visual Cryptography is an encryption method which shares secret information into n shares and decrypted into original image without any cryptographic technique. Existing visual cryptography does not provide good visual quality reconstructed image. Hence author proposed novel visual cryptography method with additional post processing technique which preserves good quality recovered image. Experimental results on this technique clearly shown that recovered image has competitive visual quality compared with input binary image.

Naor & Shamir [4] proposed visual cryptography scheme in 1994. This is the basic scheme of visual cryptography in which the secret image is divided into two shares. The shares generated are meaningless. When the two shares are stacked together, it produces the original secret image. This scheme is only for black & white images. Ateniese, Blundo & Stinson [2,3] proposed extended visual cryptography in 1996. This scheme contains meaningful shares. The (2,2) EVC theme projected during this needed enlargement of one picture element within the original image to four sub pixels which may then be chosen to supply the specified pictures for every share. Up to 1997, Visual cryptography schemes were applied to only black & white images.

Verheul & Tilborg [3, 4], proposed first colored visual cryptography scheme. But this scheme produces meaningless share. Wu and Chen [4] in 1998, were the first researchers to present the visual cryptography schemes to share two secret images in two shares Hsu et al [5] proposed another scheme in 2004. The scheme hides two secret images in two share images with arbitrary rotating angles. Verheul and Van Tilborg [6] proposed a scheme for colored secret images can be shared; the concept of arcs was used to construct a colored visual cryptography scheme S J Shyu et al [7] were first researchers to advise the multiple secrets sharing in visual cryptography. This scheme encodes a set of $n \geq 2$ secrets into two circle shares. The n secrets can be obtained one by one by stacking the first share and the rotated second shares with n different rotation angles. To encode unlimited shapes of image and to remove the limitation of transparencies to be circular.

3. VISUAL CRYPTOGRAPHY METHODS

1. Visual Cryptographic Schemes for Black and White Images / Binary Images-

a) Binary Images: Wu and Chen [4, 9] in 1998, were the first researchers to present the visual cryptography schemes to share two secret images in two shares. In this scheme two secret binary images were considered which were hidden into two random shares, namely share A and share B. In retrieving phase the first secret image can be revealed by stacking the two shares, denoted by $A \otimes B$, and the second secret can be revealed by first rotating share A by angle Θ anticlockwise. The rotation angle Θ was designed to be 90°.

b) Previous efforts in visual cryptography were restricted to binary images which is insufficient in real time applications. It is proposed visual cryptography for gray level images by dithering techniques. Instead of using gray sub pixels directly to constructed shares, a dithering technique is used to convert gray level images into approximate binary images. Then existing visual cryptography schemes for binary images are applied to accomplish the work of creating shares. The effect of this scheme is still satisfactory in the aspects of increase in relative size and decoded image quality, even when the number of gray levels in the original image still reaches 256 [16,18].

2. Visual Cryptography Schemes for color images -

a) For Single Secret Sharing- Till 1997 visual cryptography schemes were applied to only black and white images. Verheul and Van Tilborg [3] developed Colored visual cryptography scheme. Colored images with r colors, the pixel expansion m is r×3. These

schemes share generated were meaningless. This is very popular in use, Colored secret images can be shared using this method; the concept of arcs was used to construct a colored visual cryptography scheme [11, 13]. As color images are extremely famous, in c-colorful visual cryptography scheme one pixel is transformed into m sub pixels, and each sub pixel is divided into c color regions. In each sub pixel, there is exactly one color region colored, and all the other color regions are black. Cryptography scheme color of one pixel depends on the interrelations between the stacked sub pixels.

b) The first approach to realize color VCS is to print the colors in the secret image on the shares directly similar to basic model. It uses larger pixel expansion which reduces the quality of the decoded color image [10].

c) The second approach converts a color image into black and white images on the three color channels (red, green, blue or equivalently cyan, magenta, yellow), respectively, and then apply the black and white VCS to each of the color channels. This results in decrease of pixel expansion but reduces the quality of the image due to halftone process.

3. **Visual cryptography for general access structures:** In (k,n) Basic model any "k" shares will decode representation is extended to general access structures by G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson [6], where an access structure is a specification of all qualified and forbidden subsets of "n" shares. Any subset of "k" or more qualified shares can decrypt the secret image but no information can be obtained by stacking lesser number of qualified shares or by stacking disqualified shares. The secret image which reduces security level. To defeat this concern the fundamental.

4. **Halftone Visual Cryptography:** The meaningful shares generated in extended visual cryptography proposed by Mizuho nakajima and yasushi yamaguchi [7] was of poor quality which again increases the suspicion of data encryption. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo proposed halftone visual cryptography which increases the quality of the consequential shares.

3.1 Challenges in Visual Cryptography Methods-

As protecting template in the database securely is one of the Challenges in any biometric system. Here visual cryptography technique is applied to iris authentication system. In this system there are two modules: Enrollment module and Authentication module. For accessing any secure resource by authenticated users this system can be used.

3.1.1 Enrollment The administrator will collect the eye image of the eligible users those are having access to secure resource. The enrolled eye image is required to be processed so characteristic iris features can be extracted for this purpose algorithms are developed from.

Three steps that are: segmentation, normalization, and feature extraction are performed as conferred below:

- **Segmentation**- is performed to extract the iris from the eye image. By employing circular Hough transform boundary of iris is searched. By fitting two lines using the linear Hough Transform eyelids are detected and eyelash is separated by threshold technique.
- **Normalization** of iris region is carried out using Daugman's rubber sheet model. This model remaps each pixel within the iris region to a pair of polar coordinates. The center of the pupil is considered as the reference point and the radial vectors circle through the iris region.
- **Feature extraction** is done by convolving the normalized iris pattern into one dimensional Log- Gabor wavelets. The resulting phase information for both the real and the imaginary response is quantized, generating a bitwise template which is of 20*480 sizes. In the existing system generated template is stored in the database.

3.1.2 **Authentication** For authentication user will provide share in the form of ID card. System finds the corresponding share from database. By stacking two shares first I1iris template image is created. And from this image iris feature template is generated. The new eye image supplied by user will be processed with three steps: segmentation, normalization and feature extraction which generates iris feature template. Then these two feature templates are matched using hamming distance.

4. COMPARATIVE ANALYSES OF VARIOUS VISUAL CRYPTOGRAPHY METHODS

Table 1 shows Comparative analyses of various Visual Cryptography methods. This analysis shows comparisons of various images such as binary, grey scale and colored images.

Author	Year	No. of Secret Images	Type of Image	Types of Shares Generated	Description	Reference No.
Naor & Shamir	1994	1	Binary	Meaningless	Use coding table to generate the shares.	[1]
Ateniese, Blundo & Stinson	1996	1	Binary	Meaningful	Extended visual cryptography scheme	[2]
E.R. Verheul and van Tilborg	1997	1	Colored	Meaningless	Colored secret images can be shared; the concept of arcs was used to construct a colored visual cryptography scheme.	[3]
Wu and Chen	1998	2	Binary	Random	This visual cryptography scheme is to share two secret images in two shares, with rotation angle restriction	[4]
Hsu et al	2004	2	Binary	Meaningless	Arbitrary angle rotation to create the second secret.	[5]
Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei	2008	n>=2	Binary, Gray, Color	Meaningless	turn more secret images into the same share images	[6]
Daoshun Wang	2009	n>=1	binary, grayscale, color	Meaningful	Extended visual cryptography schemes using matrix extension algorithm	[7]
Siddharth Malik, Anjali Sardana, Jaya	2012	1	Colored	Random	The proposed technique is implemented with the SDS algorithm and involves three steps that are Seiving, Division and Shuffling	[8]
Hirdesh Kumar , Awadhesh Srivastava	2014	1	Colored	Meaningful	based on secret image sharing and key safeguarding technique, an effective and generalized scheme of color image hiding is proposed by means of numerical computations	[9]

Table 2: Comparative analyses of various Visual Cryptography methods

5. CONCLUSION AND FUTURE WORKS

Cryptography is outstanding and broadly utilized tech. That controls much data so as to figure or conceal their reality. This tech. Have numerous applications in software engineering and other related fields; they are utilized to secure email messages, Visa data, and corporate information and so on. This paper talks about the presentation of various kinds of Visual Cryptography plans. It thinks about the picture quality and security utilizing different visual cryptography plans. So as to conceal the mystery we go for development and expanding of the quantity of offers, yet this influences the goals .in this way an ideal number of offers are required to shroud the mystery simultaneously security is likewise a significant issue. Thus explore in VC is towards keeping up the complexity simultaneously keeping up the security. In future work we will show a

proficient security conspire for visual cryptography for dim scale pictures. This investigation causes us to comprehend different parts of visual cryptography.

References

1. Arya k.1,rakhee baiju2, sreenarayanan n. M.3 , lakshmi m.4, nimisha mohan 5, soumya m. K.6, aswathy a.s.7, reshmi k.c., a novel visual cryptographic scheme for improved binary Image Quality, International Conference On Information Communication And Embedded System(ICICES 2016), PP 252-257
2. Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li. Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption. IEEE Transaction on Information Forensics and Security: March 2013;Vol.8; No.3.
3. Jun Tian. Reversible Data Embedding Using a Difference Expansion.Transactions on circuits and systems for video technology: AUGUST 2003; VOL. 13, NO. 8.
4. Siddharth Malik, Anjali Sardana, Jaya. A Keyless Approach to Image Encryption. International conference on Communication systems and Network Technologies:2012; IEEE.
5. R. Vijayaraghavan, S. Sathya, N. R. Raajan. Security for an Image using Bit-slice Rotation Method–image Encryption. Indian Journal of Science and Technology:April 2014;Vol 7(4S); p 1–7.
6. C. Anuradha, S. Lavanya. Secure and Authenticated Reversible Data Hiding in Encrypted Image. International Journal of Advanced Research in Computer Science and Software Engineering: April 2013; volume 3, issue 4.
7. Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, Wei Su. Reversible Data Hiding. IEEE transactions on circuits and systems for video technology: March 2006; vol. 16, no. 3.
8. Asha S.N, Dr. Shreedhara. Performance Evaluation Of Extended Visual Cryptography Schemes With Embedded Extended Visual Cryptographic Scheme. International Journal of Scientific & Engineering Research: April-2012; Volume 3, Issue 4.
9. R. Lukac, K.N. Plataniotis. Bit-level based secret sharing for image encryption. The Journal of Pattern Recognition Society: 2005.
10. InKoo Kang, Gonzalo R. Arce, Heung-Kyu Lee. Color extended visual cryptography using error diffusion. IEEE:2009.
11. Yi, Feng; Wang, Daoshun; Luo, Ping, Huang, Liansheng, Dai, Yiqi.Multi Secret Image Color Visual Cryptography Schemes for General Access Structures. April 2006; Volume 16, Number 4; pp. 431-436.
12. J. Fridrich, M. Goljan, and D. Rui. Lossless Data Embedding - New Paradigm in Digital Watermarking. In Special Issue on Emerging Applications of Multimedia Data Hiding: February 2002; Vol. 2; pp. 185-196.
13. Chen Y, Tsai D-S, Horng G (2012) Comment on Bcheating prevention in visual cryptography. IEEE Trans Image Process 21:3319–3323
14. Corke P (2011) Image feature extraction robotics. Vision Control, Springer 73:335–379
15. Corke P (2011) Image feature extraction. Robotics, Vision Control, Springer 73:335–379
16. Desmedt Y, Van Le T (2000) Moire cryptography. In: the 7th ACM conference on Computer and Communications Security, 116–124
17. . Hersch RD, Chosson S (2004) Band moiré images. ACM Trans Graphics (TOG) 23(3):239–247
18. Hou Y, Chang C, Tu S (2001) Visual cryptography for color images based on halftone technology. In IEEE conference on Image, Acoustic, Speech and Signal Processing