AN OVERVIEW ON CHEATING PREVENTION TECHNIQUES USED IN VISUAL CRYPTOGRAPHY

Miss Ankita Bhimrao Patkure[1], Prof. Nikita J. Kulkarni[2]

PG Student, Computer Engineering Department, ZES' DCOER, Maharashtra, India, ankitapatkure@rediffmail.com

Assist. Prof., Computer Engineering Department, ZES' DCOER, Maharashtra, India, nikita.kulkarni@zealeducation.com

Abstract

Visual cryptography is the technique in which secret is encoding into number of share images, after stacking the sufficient number of share images it recovered the original secret image. Shares are generally in the form of transparencies. From these transparencies, each transparency can be hold by each participant. The original secret image is reconstructed by stacking the transparencies one other. Basically, the successful performance of Visual Cryptography scheme depends on the different measures like security, accuracy, pixel expansion, contrast, share generation, number of secret images etc. Most of the research work is done on the improvement of pixel expansion and contrast. Visual Cryptography has many applications like stegnography, halftoning, authentication, identification, image encryption etc. The dishonourable participants are called cheaters, which provide the fake secret image to fool the other participants. Sometimes fake participants are included which misbehave with the shares and reconstruct noise-like share image. In VSS, many prevention techniques are proposed by many researchers. Purpose of this paper is to study and performance analysis of different security techniques for Visual Cryptography Schemes

Index Terms: *Visual Cryptography, cheating, Security, cheating prevention schemes, Shares*

---------- *** ----------

1. INTRODUCTION

Secret sharing scheme allows secret information to be shared among set of participant P, in such a way that only authorized participant can recovered the original secret image. Naor and Shamir [1] develop[ed one technique known as Visual Cryptography. In Visual Cryptography, visual information is in the form of pictures, text etc. are encrypted in such a way that decryption does not required any computational devices to revered the secret image. Goal of Visual Secret sharing scheme is to protect important data from being lost or destroyed without incidental exposure. Here provide security to data is the main factor. Misbehave participants are called cheater, who can reveal fake shares. In 2006, Horng et. al. [2] proves that cheating is possible in K-out-of-n visual secret sharing scheme [2].

Cheating prevention in Visual Secret sharing method can be designed by many researchers to overcome cheating problem in Visual Cryptography. Mostly, cheating can be prevented in Visual Secret Sharing if a participant proves to that shares or reconstructed images are not authentic. Cheating prevention Visual Secret Sharing design two approaches, one based on share authentication and another is based on blind authentication. In share authentication, each participant can authenticate its share with other shares [3]. In blind authentication, some property of secret image is used to authenticate the reconstructed secret image [3]. In share

authentication, before reconstructing secret image it provide ability for participants to verify the integrity of shares and In blind authentication, it make harder for cheater to predict the original secret image.

In share authentication CPVSS scheme, each participant can hold two shares; one for secret shares and other for verification share. Verification share is used to identify the integrity of shares held by each participant. Advantage of this scheme is that cheating authentication of share is optional and generation of verification share is done after generation of secret shares. But only the quality of reconstructed image is slightly degrade. Disadvantage of CPVSS is that for verification purpose additional shares are needed and these scheme required formal proof of security.

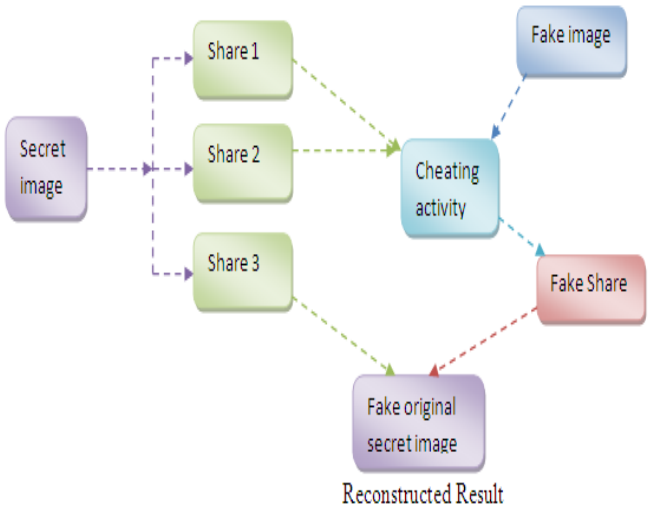

Fig1: Cheating in VC

Rest of the paper explains different methods used for cheating prevention in Visual Cryptography.

2. LITERATURE REVIEW

2.1 A New Authentication Based Cheating Prevention Scheme in Naor-Shamir's Visual Cryptography [4]

Naor and Shamir proposed a Visual Secret Sharing method. In which only authorized participants can recovered the secret image by stacking shares one to other. Here decryption is done by only human Visual System. Horng et al. [2] present the cheating activity found in K-out-of-n visual secret sharing. The cheating activity can cause unpredictable harm to victims, such victims accept fake secret image which is different from actual secret image. They propose two cheating prevention schemes, one is authentication based cheating prevention (ABCP) and another is (K, n+l) Visual secret sharing scheme.

In (ABCP) Authentication Based Cheating Prevention Scheme, it is divided into two part; one is share construction phase and other is share verification phase [4]. In this method secret image is taken as an input image and generate secret shares for each participant Pk called transparencies (Tk). Then dealer generates verification share Vk for each participant Pk Using (2,2) Visual Secret Share. But (Vk + Tm) contain nk "black points". In share verification phase, Pk uses Vk to stack with Tm and checks where as Black Points (BPs) are correct or not.

If Black pattern in (Vk + Tm) is not look like others then it considers transparency Tm is fake share. Here, Black pattern are only used to check whether share transparency is fake or not. This method is more efficient and effective to prevent cheating prevention.

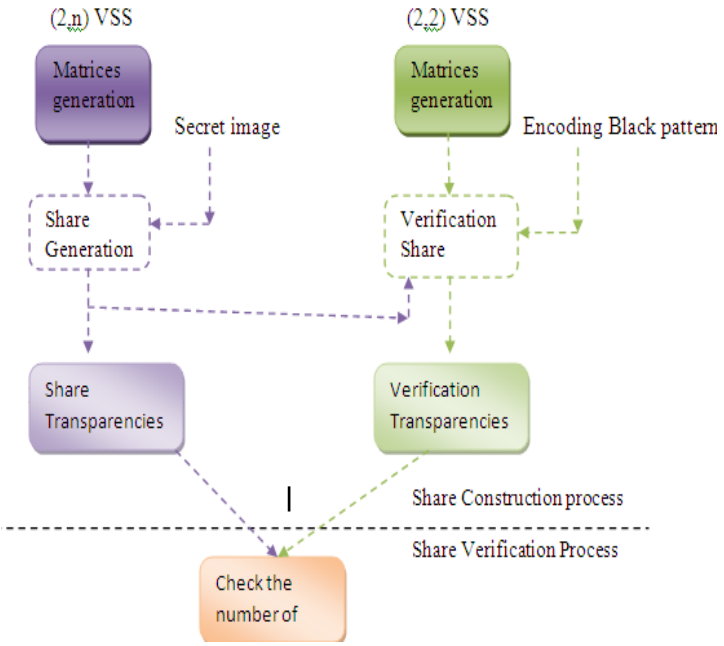

Fig2: Flow chart for ABCP

2.2 Random Grid Based Visual Secret Sharing for General Access Structure with Cheating Prevention Abilities [5]

A secret key provide to each participant is easily lost or decrypted by any other participants. In 2-out-of-2 Visual Secret Sharing, each pixel P is encrypted into sub-pixel patterns which are in six column format. If pixel P is white in six columns with equal probability which is randomly chosen and replace P. Each pattern consists of two white and two black pixels which not provide any information about secret image. In decryption process, corresponding patterns are stacked together.

In Visual Secret sharing, it considers all participants are to be honest. But sometimes, it is possible for some participant to provide fake share image to reconstruct fake secret image. To prevent cheating activity in Visual Secret Sharing, Horng et al. [2] proposed two method: 1) Authentication based Cheating prevention activity 2) (2, n+l) threshold Visual Secret Shares. This generates n+l shares but only n shares are given to n participants to decrease the probability of correctly guessing structure of shares. Here, General Access (GA) structure algorithm is used which is more flexible than existing Random Grid Based Visual Secret Sharing

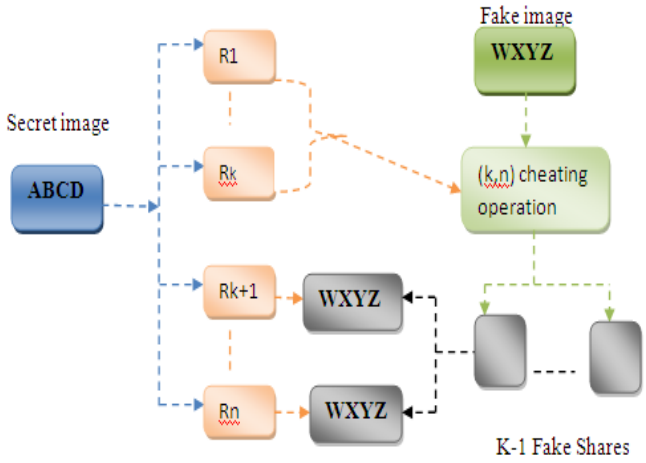

Fig3: An example for Collusion cheating process in (k,n) VSS

2.3 A novel participant authentication Share [6]

For participant authentication many techniques can be used like biometric based (sheng et al.2005) or password based authentication. Hwang and Lee [7] proposed a remote user PWA scheme which having some advantages: 1) allow user to choose free password 2) No password table in server database 3) no third party involved 4) impossible to hack the password. These all advantages fail to provide guarantee about user participants.

The idea of completely Automated Public Turning Test to Computers and Human Apart (CAPTCHA) (pope and Kaur, 2005) ask user to identify reconstructed image. CAPTCHA generate image of randomly chosen or distributed digits or characters with varying degree of noise like backgrounds, in such a way that most text recognition method cannot

recognize them. CAPTCHA is not limited to text, but also consist of registration, authentication and password updating phase. CAPTCHA is secure and effective method against different software recognition.

2.4 Halftone based Secret sharing Visual Cryptography for Color images using bit Analysis [8]

Visual Cryptography is a special type of encryption technique in which decryption is done by human visual system. In this, Variable length symmetric key based Visual Cryptography scheme for color image is introduced. In which secret key is used to encrypt the image and distribution of encrypted image is done by Random Number. In decryption phase, original image is decrypted by that secret key only. Here secret key provide security in Visual Cryptography. Digital color image is include four parts i.e. alpha, red, green, blue each of 8-bit means total 32-bit digital image. Alpha part provides information about degree of transparencies. If value of alpha is 0, then it is fully transparent.

11100111	11011001	11111101	00111110
Alpha	**Red**	**Green**	**Blue**

Fig4: Structure of 32-bit pixel

The secret key provides security to information so that attacker cannot hack the secret information without key. Original data is encrypted using key and produce cipher which are in the form of shares. Then it can be decrypted using secret key and reconstruct the original image. In symmetric encryption, same key is provided on both encryption and decryption side.

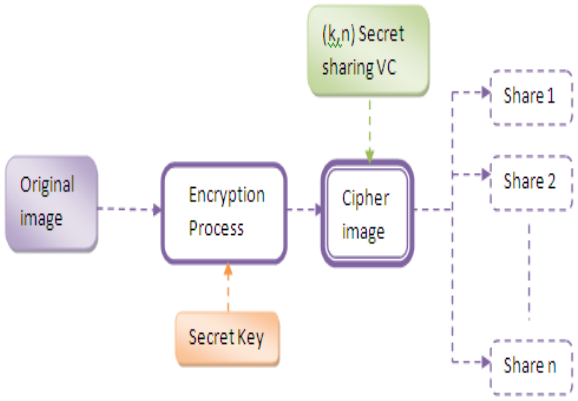

Fig 5: Encryption process for (k,n) VC

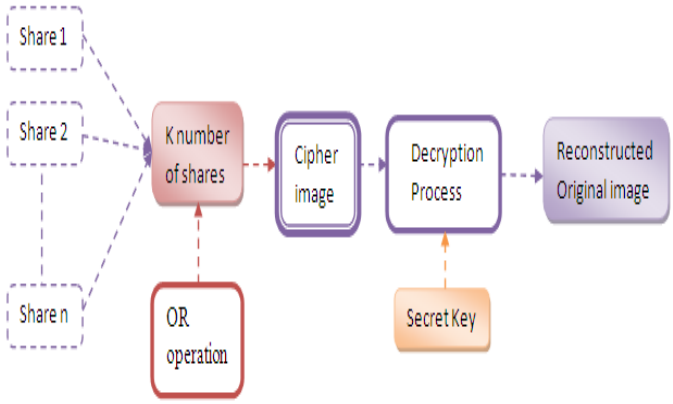

Fig 6: Decryption process for (k,n) VC

2.5 A novel Anti-Phishing Framework based on Visual Cryptography [9]

Phishing is a process like fishing in lake, but instead of capture fish phishers attack on your personal information. It is the process of fraud access to confidential or secure information about user like bank password or credit card number. In anti-phishing framework, first all users are registered with trusted server. At the time of registration unique is generated and that key is store in database of trusted server. When user is successfully registered with trusted server then he can login through username and password using client

application. For particular session, random image is chosen by server for purpose of verify server. Then client application applies Visual Cryptography over chosen image and generates two shares. After that one share is forwarded server for test. Server test and forward it along with its server name and password required to decrypt the share from trusted server. Trusted server decrypts the share using unique key which is already stored in database. Then decrypted image send to server for test if and only if server is registered with trusted server. After receiving decrypted share send it to client. Then client perform decryption to obtain original image.

3. CONCLUSION

In this paper, various cheating prevention techniques are summarized. Visual cryptography is very effective to protect multimedia data which is very large. The ability of cryptanalysis is to find weakness in cryptography scheme. There are various methods to find fake shares and fake participants. In CPVSS, authentication based and blind authentication is used. In which verification share is given to each participant for the security purpose. Also sometimes secret key is used which is provided on both encryption and decryption side to prove security to confidential data

REFERENCES

[1]. M. Naor and A. Shamir, "Visual cryptography," in Proc. Adv. Cryptolography EUROCRYPT'94, LNCS 950, 1995, pp. 1–12

[2]. G. Horng, T. H. Chen, and D. S. Tsai, "Cheating in visual cryptography, Des" Codes, Cryptography, vol. 38, no.2, pp. 219–236, Feb. 2006

[3]. Yu-Chi Chen, Student Member, IEEE, Gwoboa Horng, and Du-Shiau Tsai "Comment on Cheating Prevention in Visual Cryptography" IEEE Transactions on Image Processing, Vol. 21, No. 7, July 2012

[4]. Yu-Chi Chen, Du-Shiau Tsai, Gwoboa Horng, "A New Authentication Based Cheating Prevention Scheme in Naor-Shamir's Visual Cryptography", J. Vis. Commun. Image R. 23 (2012) 1225–1233

[5]. Xiaotian Wu, Wei Sun, "Random Grid Based Visual Secret Sharing for General Access Structure with Cheating Prevention Abilities" The Journal of Systems and Software 85 (2012) 1119– 1134

[6]. Tzung-Her Chen, Jyun-Ci Huang, "A novel participant authentication Share", The Journal of Systems and Software 83 (2010) 861–867

[7]. Tsai, C.S., Lee, C.C., Hwang, M.S., 2006. "Password authentication schemes", current status and key issues. International Journal of Network Security 3 (2), 101–115

[8]. Pavan Kumar Gupta, Naveen Hemrajani, "Halftone based Secret sharing Visual Cryptography for Color images images using bit Analysis", Pavan Kumar Gupta et al,Int.J.Comp.Tech.Appl,Vol 3 (1), 17-22.

[9]. Gaurav Palande, Shekhar Jadhav, Ashutosh Malwade, "A novel Anti-Phishing Framework based on Visual Cryptography", International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-3)

[10]. Smita Patil, Jyoti Rao, "Survey of Cheating Prevention Techniques in Visual Cryptography", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064

[11]. mizuho nakajima, yasushi yamaguchi, "extended visual cryptography for natural images"

[12]. D. C. Lou, H. H. Chen, H. C. Wu, and C. S. Tsai, "A novel authenticatable color visual secret sharing scheme using non-expanded meaningful shares," Displays, vol. 32, no. 3, pp. 118–134, 2011

[13]. Young-Chang Hou, Shih-Chieh Wei, And Chia-Yin Lin, "Random-Grid-Based Visual Cryptography Schemes",

IEEE Transactions On Circuits And Systems For Video Technology, Vol. 24, No. 5, May 2014

[14]. mizuho nakajima, yasushi yamaguchi, "extended visual cryptography for natural images"