International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-6, Issue-8)

Research Article | **August 2017**

Security Concern and Countermeasures for Cheating in Visual Cryptography

Ekta
Department of Computer Science and Engineering, Bhagat Phool Singh Mahila Vishwavidyalaya,
Khanpur Kalan, Sonipat, India

Abstract—

As IT sector is ruling the world now,confidentiality and security of information has become the most important inseparable aspect in information communication system. Keeping in view the same, a new approach called Visual Cryptography (VC) has been suggested by many researchers but there are some limitations with this scheme and cheating is one of the main problem among them. This paper intends to show the basis of cheating in VC in terms of cheating process, its detection methods and its prevention methods suggested by various researchers along with their merits and demerits. Finally, a good Cheating Immune Visual Cryptography Scheme (CIVCS) has been discussed which states the properties to be adopted by every Visual Cryptography scheme to make it immune to cheating attacks.

Keywords—Visual Cryptography, cheating, Cheating Immune Visual Cryptography, Cheating Prevention visual cryptographic schemes.

I. INTRODUCTION

This is the era of information technology and there is astonishing advancement in the computer technology, even then it is not always feasible to have a computer for secret decryption. In some circumstances, human visual system i.e. eyes are the most convenient and easy tool to check some secret information. Therefore, in 1995, Naor and Shamir invented a new cryptographic scheme called the Visual Cryptography (VC), in which the secret is encrypted in such a way that its decryption can be possible by human visual system directly [2].

VC is a technique of encoding a secret image into a number of shares (usually presented in transparencies) in such a way that stacking sufficient number of shares will reveal the secret image. The decryption process in VC is simply stacking the shares and viewing the secret image which appears on the stacked shares simply by human visual system without any complex computational algorithm. Most of the prior research work in VC has focused on improvement of two parameters such as contrast of image and pixel expansion. But, in 2006, Horng et al. [7] showed that cheating is also possible in VC (K, n) scheme where n is larger than K. The fraudulent participants called cheaterscollude or co-operate with each other for some unauthentic work to make some honest participants fool called victimto do what is called CA (cheating activity). The cheater makes unforeseeable damage to the victim by merging the fake shares with the victim's genuine shares and victim accepts a fake secret image instead of actual image[1][4][17].

Cheating process can be done in two ways i.e. individual cheating (IC) and co-cheating (CC). IC is done by single fraudulent cheater by presenting a fake share during stacking phase and inaccurate revamp of secret image. On the other hand, CC, which is a vital issue of cheating detectable VC schemes, causes the generation of fake secret image because of several collusive participants by colluding activity i.e. the cheaters support themselves by merging their fake shares with the victim's genuine shares.

VC scheme is said to be cheating prevention scheme if the probability of successful cheating is negligible. Since 2006, a variety of Cheating Preventing Visual Secret Sharing (CPVSS) schemes have been proposed by many researchers [2]. CPVSS is mainly designed based on two approaches: one is based upon share authentication and another is based upon blind authentication [1][6]. In share authentication, each participant has an extra share used to authenticate other shares with the goal of helping the participants with the potential of verifying the shares' integrity or correctness and this approach should be applied only in the case when some participant is suspected to the cheating act. In blind authentication approach, some inbuilt property of image is used to authenticate the secret image with the goal of making it complex for the colluding cheaters to guess the structure or anatomy of other honest participants[1][4].

II. CHEATING IN VC

This section defines some widely accepted definitions of cheating in VC and overview of cheating process to show that how a malicious participant and malicious outsider does the cheating in reconstruction phase of secret image by using their fake shares.

A. Abbreviations

VC— Visual Cryptography
VCS— Visual Cryptography Scheme

CA— Cheating Activity
CIVCS— Cheating Immune Visual Cryptography Scheme
SCM— Successful Cheating Method
MP— Malicious Participant
MO— Malicious Outsider
EVC— Extended Visual Cryptography
CPVCS— Cheating Preventing VCS
BPCS— Bit Plane Complexity Steganography
VSS— Visual Secret Sharing
DD2— Detectable Distortion

B. Definitions

Here, some widely accepted definitions [2][3] about cheating in VC scheme are given:

a) 'A' is a cheater, if during the stacking phase of reconstructing the secret image, he gives a fake share and merging of that fake share with genuine share produces an image different from the original secret image. A participant is called a Victim if he has to trust that the reconstructed image is the original image and cannot be certain about whether it is fake or genuine one.
b) A participant is called a cheater, if during image reconstruction phase; he presents a fake transparent share which is not the real one he received from dealer.
c) A successful cheating method (SCM) is cheating method that succeeds with probability of 1.
d) In VC, if any loyal participant called the victim accepts a reconstructed image different from the actual secret image as authentic then the cheating method is said to be successful.
e) A cheating immune visual cryptographic scheme (CIVCS) is a VC scheme in which the probability of cheating is negligible.

C. Overview of Cheating Process

Broadly, two types of cheaters are possible in VC. One is MP (malicious participant) and another is MO (malicious outsider). MP is a person who belongs to the qualified subset of the participants and the MO is a person who does not belong to the qualified subset of participants [5][16]. A cheating process mainly consists of following phases as shown in fig. 1.

a) In the first phase, the cheaters generate fake shares.
b) Second phase consists of secret image reconstruction phase. Stacking of fake shares with the genuine shares reveals the fake secret image and the honest participants will not be able to differentiate fake shares from genuine ones. Even they will not able to show whether the reconstructed image is original secret image or not [5].

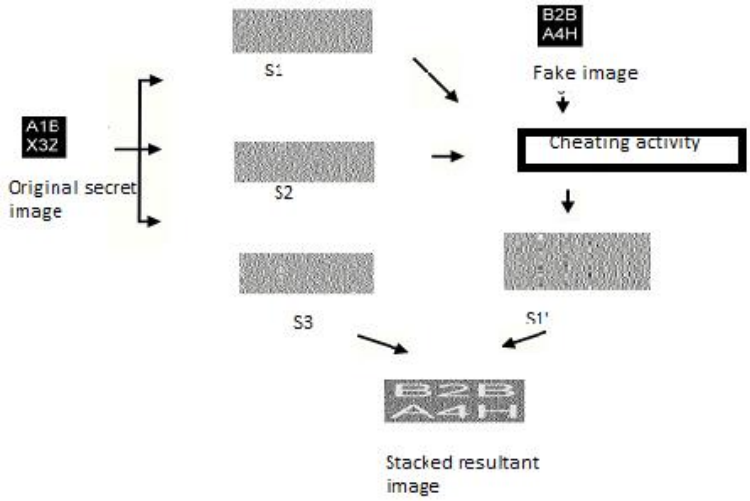

Fig. 1: Basis of cheating [3]

D. Common Ways of Cheating in VC

The most common way of cheating in VC are mainly:

a) Cheating in VC by an MP
b) Cheating in VC by an MO
c) Cheating in extended VC (EVC) by an MP

a) Cheating by MP

MP belongs to the qualified participants and act as a cheater by using his original share to generate fake shares and cheat the genuine participants because the generated fake share are indifferent from the original shares and the final stacked resultant image will be different from the original image[5].

b) Cheating by MO
MO is a cheater who does not belong to the qualified participants and makes some fake shares on the basis of some random images to decrypt the original secret image. MO always tries to make the fake shares of various sizes because the size of the original image may vary[5].

c) Cheating EVCS by an MP:
By interchanging the black pixels by white pixels, the cheater generates the fake shares and causes the less contrast of reconstructed stacked image. The resultant fake image has enough contrast against the background because the fake image is reconstructed in perfect blackness [5].

III. CHEATING DETECTION METHODS

There are various possible ways to detect whether there are some cheating activities in VC scheme or not:

a) Check whether the shares excluding the participants genuine shares gives a relevant image because the fake image reconstruction can also be possible with the stacking of colluding cheaters' shares only [3][5].
b) If a participant takes more than one share in stacking phase, it means he is a cheater because only the cheater can take more than one share at a time.
c) Check if any prohibited set of participants are taking part in the stacking phase. If so, means there are some cheaters in the VC scheme [2][3].

IV. CHEATING PREVENTION

In many researches, focus has been made on cheating preventing visual cryptographic schemes (CPVCS) which consists of approaches such as [5][2]:

a) Use blind authentication means to use some inbuilt characteristics such as to embed some authentication detail in the image itself to know whether it is fake image or original but it will cause the image contrast reduction and pixel expansion [5].
b) Generate extra verification shares to authenticate the reconstructed image but it results into increase in extra overhead to the participants.
c) To authenticate the stacked shares, make use of some online trusted authority but it results into compromising the core property of the VC i.e. its simplicity.
d) To make it harder for the cheater to predict the structure of the victims' genuine share,generate more than one share but it will cause the contrast reduction of the secret image.

Many researchers have done a lot of work on cheating prevention in VC scheme using various types of visual secret sharing scheme and proposed a variety of cheating preventing schemes. The following Table 1 shows the comparative study of various cheating prevention schemes along with their merits and demerits.

Table 1: Comparison of Various Visual Cryptography Schemes [4]

Author Name & Year	**Visual Secret Sharing Type**	**Cheating Prevention Scheme**	**Merits**	**Demerits**
Shayali et al. 2016 [15]	(2,2) VSS	Two factor prevention scheme.	Proves whether cheating occurred in VSS or not, low computational cost.	Cannot find the exact location of the cheater.
Angel Rose et al. 2015 [14]	(2,n) VSS	BPCS	Low cost.Integrity can determine whether cheater exists or not.	Extra overhead of verification. Sharescannot find the exact location and identification of cheater.
Jana B. Etal. 2015 [13]	(n,n)VSS	Steganographic scheme.	No extra verificationshare isrequired.	Applicable only to(n,n)VSS
Tsai,Horng et al. 2013 [11]	WVSS	A newcheatingprevention(2,n) -VSS	Does notrely on addedtransparencies.Low pixelexpansion.	Applied only for (2,n) scheme.Verifiable message isrequired for eachparticipant.
Tsai,Horng et al. 2012 [12]	(2,n)- VSSfor sharetransparency&(2,2)-VSSFor verificationtransparency	A newABCPScheme.	Pixel expansion issmaller thanHT,DD1,DD2HCT2	Verification is partiallyknown.
Thasai et al. 2011[9]	(k,n)-VSS	Verificationparameter basedCPVCS.	More secure. Prevention based on aposition. Check both fakesecrete share& fakeverification share. No extra share needed. Reduce	Based on pixel positioncoordinate. Pixel expansion (m+2n). Reduces contrast.

			the load ofshare management.	
De Priso et al. 2010 [10]	(n,n)-VSS	DD2	Transparencynot required.	Insecure.
Hu et al. 2007 [8]	(k,n)-VSS	HTCP	Quite efficient.	Pixel expansion islarge. The contrast is slightly reduced. It generates two sharesfor eachparticipant.
Horng et.al 2006[7]	(n,n)-VSS	HCT1	Simple	Each participantBurdened with anextra verificationshare.Extra verificationtransparency is required.

V. CHARATCTERISTICS OF CHEATING IMMUNE VCS (CIVCS)

The results of different cheating preventing schemes show that VCS is not secure against cheating. So, a new scheme is needed to build a cheating immune system which should follow the following properties [3]:

a) A cheating immune VCS should not increase the pixel expansion and should not decrease the original image contrast.
b) It should not depend upon some online trusted authority because it compromises with the simplicity of the VC scheme.
c) It should be applicable for any VCS for general access structure and should not be structure specific.
d) The information needed to authenticate the reconstructed secret image should be in fewer amounts as much possible because it causes pixel expansion.
e) This scheme will be ideal if it is able to detect the existence of cheating and the real cheaters.

VI. CONCLUSION

In the present era, the use of open network to share informationhas increased exponentially and therefore the risk of an invader accessing secret information has been an ever prevailing concern for the information security experts. VC is an interesting and user friendly technique for the purpose of information communication but cheating is also possible in it because of some untrustworthy participants called cheaters. Therefore, the applications which are based upon VC are vulnerable to lose their privacy. In this paper, the basis of VC cheating method along with their detection methods and the various types of cheating prevention schemes along with their merits and demerits have been discussed which show that a progressive continual research work is needed for a cheating preventable VC scheme to get the desired level of security and quality.

REFERENCES

[1] Yu- Chi, GwoboaHorng and Du- Shiau Tsai, "Comment on Cheating Prevention In Visual cryptography" in IEEE Transaction on Image processing , Vol. 21, No. 7, July 2012.
[2] GwoboaHorng, Tzungher Chen and DU- Shian Tsai, "Cheating In Visual Cryptography" in SPRINGER, vol. 38, pp. 219-236, 2006.
[3] F. Liu and W.Q. Yan, "Various Problems in Visual Cryptography" in SPRINGER, DOI- 10.1007/978-3-319-09644-5_2 , 2014.
[4] Biltta P George and Deepika M P, "Cheating Prevention Schemes for Visual cryptography" in International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 4, Issue 07, July 2015.
[5] MorapudiNaresh Kumar, Datrika, Rao D. Sravanthi, "A Novel Approach For Cheating Prevention Through Visual Cryptographic Analysis" In International Journal of Computer Science & Engineering (IJCSES), Vol. 2, No. 4, November 2011.
[6] A. Shamir And M. Naor, "Visual Cryptography: Improving The ContrastVia The Cover Base," In Processing Security Protocols, 1 Vol. 1189, pp. 197–202, 1996.
[7] G. Horng, T. H. Chen, and D. S. Tsai, "Cheating In Visual Cryptography," in Des Codes Cryptography, Vol. 38, no. 2, pp. 219–236, Feb. 2006.
[8] C. M. Hu and W. G. Tzeng, "Cheating prevention in visualcryptography,"IEEE Transaction on Image Processing, Vol. 16, no. 1, pp.36–45, Jan.2007.
[9] C.S Tasai,H.C.Wang,H.CWu,C.H.M Wang, "A Cheating –Preventing Visual Cryptography Scheme By Referring TheSpecial Position", International Journal ofInnovativeComputing,Information And Control volume 7, No. 7(A), July 2011.
[10] R.DePrisco, A.DeSantis, "Cheating Immune Threshold VisualSecret Sharing", in Computational Journal 53, pp. 1485–1496, 2010.
[11] Y.C. Chen, D. S. Tsai, G. Horng, "Visual Secret Sharing WithCheating Prevention Revisited", In Digital Signal Processing 23, pp. 1496-1504, 2013.

[12] Du-Shiau Tsai,Tzung-Her Chen,GwoboaHorng, "ACheatingPrevention Scheme For Binary Visual Cryptography WithHomogeneous Secret Images", In Pattern Recognition 40, pp. 356 - 2366,www.elsevier.com/locate/pr, 2007.

[13] Jana, B. Mallick, M. Chowdhuri, P. Mondal,S.K.,"CheatingPrevention In Visual Cryptography Using SteganographicScheme", In International Conference On Issues And Challenges InIntelligent Computing Techniques (ICICT), pp.706 –7122, 2014.

[14] Angel Rose, Sabu M. Thampi, "A Secure Verifiable Scheme for Secret Image Sharing" in ELSEVIER, Second International Symposium on Computer Vision and the Internet,Procedia Computer Science 58, pp. 140 – 150, 2015.

[15] Shayali Gupta, Prof.JyotiRao, "Two Factor Cheating Prevention In Visual Cryptography Using Codebook" In International Journal Of Computer Science And Information Technologies (IJCSIT), Vol. 7 (3) ,pp. 1630-1634, 2016.

[16] M. Naor and B. Pinkas, "Visual authentication and identification," in Proc. Advances inCryptology, 1997, Vol. 1294, LNCS, pp. 322–336.

[17] Liu F, Wu CK, "Embedded Meaningful Share Visual Cryptography Schemes"in IEEE Transaction Information Forensics Security 6(2), pp. 307–322, 2011.

