International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 07, July-2015

Cheating Prevention Schemes for Visual Cryptography

Biltta P George
Computer Science and Engineering
Adi Shankara Institute of Engineering and Technology
Kalady, India

Deepika M P
Computer Science and Engineering
Adi Shankara Institute of Engineering and Technology
Kalady, India

***Abstract*—Visual cryptography is an encryption technique to encrypt a secret image into different shares such that stacking a sufficient number of shares reveals the secret image. Most of the previous research work on VC focuses on improving two parameters: pixel expansion and contrast. We considered the cheating problem in the visual cryptography scheme and investigate various cheating prevention schemes. During the reconstruction of the secret, one participant, called cheater, may release a false share. As a result a fake image will be revealed.**

Keywords—Visual cryptography; cheating;cheating prevention; fake share

I. INTRODUCTION

Visual cryptography is first introduced by Naor and Shamir in 1995[11].The main concern of all the encryption technique is to protect the important data from being tampered or modified. In 2006 Horng et al. proposed that cheating is possible in (k, n) VC when k is smaller than n. The dishonest participants (cheaters) collude and want to fool victims, which is called "cheating activity" (CA).CA cause unpredictable damage to the victims; therefore, the victims accept a fake secret image (cheating image) different from the actual secret image as authentic.

Cheating process can be divided into two: Individual cheating (IC) and co-cheating (CC).Individual cheating (IC) is employed by a single participant. During the secret recovering phase a certain participant presents a false or fake share images. Since the secret image cannot be reconstructed correctly. Moreover, the secret image can be revealed by deception if the cheater gets enough shares. Another way of cheating is called co-cheating (CC), accomplished by several collusive participants. Target's shares can be guessed with the shares they have in hand. Based on the assumption, the collusive cheaters create some fake shares; the stacking of fake and genuine shares together reveals a cheating image instead of the real secret image. A participant colluding is an important issue of cheater detectable visual cryptography schemes [7].

A visual secret-sharing scheme is said to be a cheating prevention scheme if the probability of successful cheating is negligble.There are two approaches in designing CPVCS schemes. One is based on share authentication where each member is provided with an additional share to validate other shares. The other is based on blind authentication where some property of the image is used to validate the reconstructed secret image. Thus, the objective of share authentication is to provide the members the ability to confirm the honesty of the shares before recreating secret images, and the objective of blind authentication is to make it tougher for the cheaters to guess the structure of the shares of the other members.

II. RELATED WORK

A secret sharing scheme allows a secret to be shared among a set of members, such that only authorized subsets of *M* can recover the secret, but any unauthorized subset cannot reveal the secret. In 1995, Naor and Shamir suggested a variant of secret sharing, called visual cryptography, [12] where the shares given to members are xeroxed onto transparencies. If A is an authorized subset of *M*, then the members in M can visually recover the secret image by stacking their transparencies together without performing any computation.

Horng et al. [1] showed that cheating is possible in (*k; n*)-VSS, traditional secret sharing. The cheating activity (CA) can cause unpredictable damage to sufferers, when sufferers accept a fake secret image different from the actual secret image as authentic. In their cheating method, the cheater needs to know the exact distribution of black and white sub pixels of the shares of honest participants. Based on this characteristic, they proposed a cheat-preventing method (HCT1) or an authentication based cheating prevention scheme to prevent the cheater from obtaining the distribution. However, the knowledge of the distribution is not a necessary condition for a successful cheat. They also proposed another cheat-preventing method (HCT2) or 2-out of (N+L) cheating prevention scheme, in which the assembling of the genuine share and verification share reveals the verification image in some small region. It is possible to attack the method.

Hu and Tzeng [2] presented three kinds of cheating activities: CA-1, CA-2, and CA-3. They also gave a generic transformation that can make all VSS schemes to achieve cheating prevention. HTCP scheme denotes Hu and Tzeng's transformation scheme, which is share authentication. The main idea of Hu-Tzeng's cheating prevention scheme uses a generic transformation to generate new transparencies with adding two subpixels to every block of every original

transparency. Then, this scheme generates a verification transparency for each participant such that the stacking result of the new transparency with the verification transparency will reveal a verification image. However, the extra verification share probably increases the risk and in addition, also produces share management issues for each participant.

Yu-Chi Chen, Gwoboa Horng, and Du-Shiau Tsai [3] cryptanalyze the Hu–Tzeng CPVSS scheme and show that it is not cheating immune. Cryptographic schemes are very useful for realizing information security. The goal of cryptanalysis is to find potential weaknesses in a cryptographic scheme.

De Prisco and De Santis [4] also measured the problem of cheating, and they showed that in (2, *n*)-VSS, cheating is successful by n_i-1 collusive cheaters, and in (*n, n*)-VSS, by 1 cheater. The collusive cheaters want to fool the victim for some reasons. De Prisco and De Santis proposed two cheating immune visual secret sharing schemes: the simple scheme and the better scheme. The better scheme is cheating prevention without a complementary image; therefore, for any black or white pixel, the cheaters cannot infer the actual value of victim's subpixels. But this method is Suffers from the deterministic white-to-black attack (DWtBA) and RCA (Region Cheating Attack).

Tsai, Wang and Wu propose a cheating scheme [5] for Hu and Tzeng's transformation scheme. This cheating scheme reveals that not only that the secret share can be faked but that the verification share can be faked also. This can cause to the cheater to cheating other members by using the fake secret share and the fake verification share. Because of this, a new transformation scheme is proposed. This proposed transformation can alter the existing VC-scheme into the cheat preventing VC-scheme by referring the special position. This scheme does not need an extra verification share which can reduce the load of share management.

In the existing VC schemes no security is provided to the secret shares and challengers can alter its bit sequences to create fake shares. And in the Invisible and Blind Watermarking scheme [6], the vulnerability of these binary secret shares is overcome by hiding them invisibly into some host images. The overlapping of these shares reveals the original secret. During the decryption phase, the secret shares are extracted from their cover images without needing any of the cover image characteristics because the watermark extraction technique is blind.

Bin YU. et al [7] were researchers to recommend the Co Cheating prevention in Visual Cryptographic Schemes using trusty third party. In this scheme trusted third party act as a verifier and checking the genuinity of the shares simultaneously. The verifier keeps a rare verification share and 'n' optional verification shares. Through a rare verification share and 'n' optional verification shares, the reality of several shares can be identified concurrently.

Shuo-Fang Hsu et al [8] were first researchers to present Verifiable Visual Cryptography scheme. The basic idea used in this scheme is to stamp a continuous pattern on the shares belonging to the same secret image. Also a part of the pattern can be revealed through aligning and stacking half of two share images together.

Jana, B et al [9] introduced Cheating prevention in Visual Cryptography using steganographic Visual scheme.
In order to prevent cheating in VC a steganographic scheme is used. In this scheme a secret message is embedded in each of the shares in random location during share generation phase called stego share. Before stacking operation the receiver can extract hidden message from stego share image for checking verification of share images. In this method no verification share image is required to prevent cheating in VC.

III. CHEATING PREVENTION SCHEMES

Most of the cheating prevention schemes are based on the traditional visual cryptography. Most usual disadvantages include the following: the scheme needs an online trusted authority, or it needs additional shares for the purpose of verification, or it has to sacrifice the properties by means of pixel expansion and contrast reduction of the original VCS or it can only be based on such VCS with specific access structures. Many studies focused on the cheating problems in VCS, and consequently many cheating prevention visual cryptography schemes (CPVCS) have been proposed. We classify the techniques in these CPVCSs as follows:

1. Make use of an online trusted authority who can verify the validity of the stacked shares.

2. Generate extra verification shares to verify the validity of the stacked shares.

3. Expand the pixel expansion of the scheme to embed extra authentication information

4. Generate more than *n* shares to reduce the possibility that the cheaters can correctly guess the distribution of the victims' shares.

5. Make use of the genetic algorithm to encrypt homogeneous secret images

By observing the above techniques, we found that the first technique is not practical in real applications, because the beauty of VCS is its simplicity, which is meant to be useful even when no computer network is available. The second technique requires the extra verification shares, which predictably increases the load of the participants. The third and fourth techniques increase the pixel expansion and reduce the contrast of the original VCS. The fifth technique requires strong computational overhead and degrades the quality of the recovered secret image, where the secret image can only be a password. It is also noted that most CPVCS can only be based on a VCS with specific access structure, for example, the *(2, n)* threshold access structure.

TABLE I. COMPARISON OF VARIOUS CHEATING PREVENTION SCHEMES

sl.no	Year& Author	Type of VSS	Cheating Activity	Cheating Prevention Scheme	Advantages	Disadvantages
1	2006, Horng et.al[1]	(n,n)-VSS	CA-1	HCT1	Simple	Each participant Burdened with an extra verification share. Extra verification transparency is required
2	2006, Horng et .al[1]	(n,n)-VSS	CA-2	HCT2	Simple	Extra one share is used White pixels of secret image is vulnerable.
3	2007,Hu and Tzeng[2]	(k,n)-VSS	CA	HTCP	Quite efficient	Pixel expansion is large The contrast is Slightly reduced It generates two shares for each participant.
4	2010, DePrisco &DeSantis [4]	(n,n)-VSS&(2,n)-VSS	CA-1,2, DD-CA	DD1	Low computational complexity	Verification transparency is required.
5	2010, De Priso & De Santis [4]	(n,n)-VSS	CA-1,2, DD-CA	DD2	Transparency not required	Insecure
6	2010, A Novel Scheme for Mutual Authentication and Cheating Prevention[6]	(n,n)-VSS	CA	Invisible and Blind Watermarking scheme	Image quality is improved by using perfect restoration technique Provides double security Robust against various attacks like Blurring, Cropping,, Sharpening, JPEG Lossy compression	Complex process
7	Bin YU. et al, CCPVC [7]	(k,n)-VCS	CA	CCPVC based on trusted third party	Checking efficiency is good Small pixel expansion	Extra verification share is used
8	2011 Thasai ,Wang,Wu[5]	(k,n)-VSS	CA	Verification parameter based CPVCS	More secure Prevention based on a position Check both fake secrete share& fake verification share No extra share needed Reduce the load of share management	Based on pixel position coordinate Pixel expansion (m+2n) Reduce contrast

9	2012, Tsai, Horng[11]	(2,n)- VSS for share transparency & (2,2)-VSS For verification transparency	HCT1, HT,DD2	A new ABCP Scheme	Pixel Expansion is small than HT,DD1,DD2 HCT2	Verification is partially known
10	2013,Tsai, Horng[10]	WVSS	Secure against Meaningful deterministic cheating	A new cheating prevention (2,n) -VSS	Does not rely on added transparencies Low pixel expansion	Applied only for (2,n) Scheme Verifiable message is required for each participant
11	2014,Jana B. et al[8]	(n,n)VSS	CA-1,CA-2	Steganographic scheme	No extra verification share is required	Applicable only to (n,n)-VSS

TABLE II. COMPARISON OF VARIOUS CHEATING PREVENTION SCHEMES

Scheme	Type of VSS	Pixel Expansion	Added Transparency	Computational Complexity	Type of C.P	Security
HCT1[1]	(n,n)- VSS	2n	required	O(n)	SA	insecure
HCT2[1]	(n,n)-VSS	2(n+l)	required	O(n)	BA	secure*
HT[2]	(k,n)-VSS,k<n	2(n+2)	required	O(n)	SA	insecure
DD1[3]	(n,n)-VSS	2(n+1)	required	O(n)	BA	secure*
DD2[3]	(n,n)-VSS	2^n+n+1	no	$O(2^n)$	BA	insecure
A new CPVSS [10]	(2,n)-VSS	2n+1	no	O(n)	SA	secure
Cheating Prevention using steganographic scheme[9]	(n,n) VSS	2n	no	O(n)	BA	secure

Table II shows the comparisons of various CPVSS schemes in the aspects of expansion of a pixel (Pixel Expansion), computational complexity, security against the meaningful deterministic cheating (Security), type of cheating prevention (Type of C.P., SA: share authentication, BA: blind authentication), and relying on added transparency or not (Added Transparency).* denotes the scheme must rely on complemental secret image to be secure. For the expansion of pixel, 2( ) denotes that the scheme relies on added transparencies.

IV. CONCLUSION

In this paper various cheating prevention schemes are studied. In today's information age, information sharing and transfer has increased exponentially. The threat of an intruder accessing secret information has been an ever existing concern

for the data communication experts. Cheating is possible in the Visual Cryptographic Schemes (VCS) by dishonest or malicious participant called a cheater, may provide a Fake Share (FS) to cheat the other participants. While selecting cheating prevention method in visual cryptography or in it must be space and time efficient. The cheat-preventing schemes are either not robust enough or still improvable. An efficient transformation of VCS for cheating prevention experiences minimum overhead on contrast and pixel expansion. It only added two sub pixels for each pixel in the image and the contrast is reduced only slightly. Cryptographic schemes are very useful for realizing information security. The goal of cryptanalysis is to find potential weaknesses in a cryptographic scheme.

REFERENCES

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

[2] C. M. Hu and W. G. Tzeng, "Cheating prevention in visual cryptography,"*IEEE Trans. Image Process.*, vol. 16, no. 1, pp. 36–45, Jan.2007.

[3] G. Horng, T. H. Chen, D.S. Tsai, Cheating in visual cryptography, Des Codes Cryp-togr.38 (2)(2006)219–236.

[4] R.De Prisco, A.De Santis, Cheating immune threshold visual secret sharing, Comput.J.53 (2010)1485–1496.

[5] C.S Tasai,H.C.Wang,H.C Wu,C.H.M Wang ,"A Cheating – Preventing Visual Cryptography Scheme By Referring The Special Position", International Journal Of Innovative Computing ,Information And Control volume 7 , N Umber 7(A),July 2011

[6] Aarti, Harsh K Verma, Pushpendra K Rajput ," Ideal Contrast Secret Sharing Scheme through Meaningful Shares with Enveloping Digital Watermarking using Bit Plane based(k,n)-VCS", International Journal of Computer Applications Volume 46,No.9,May2012

[7] Bin YU, Jin-Yuan LU, Li-Guo FANG," A Co-cheating Prevention Visual Cryptography Scheme", Third International Conference on Information and Computing, 2010 Conference on Information and Computing, 2010

[8] Shuo-Fang Hsu ; Yu- Jie Chang; Ran-Zan Wang; Yeuan- Kuen Lee; Shih-Yu Huang, "Verifiable Visual Cryptography" Sixth International Conference on Genetic and Evolutionary Computing (ICGEC), 2012,464 – 467

[9] Jana, B. Mallick, M. ; Chowdhuri, P.; Mondal, S.K., "Cheating prevention in Visual Cryptography using steganographic scheme", International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014, 706 – 712.

[10] Y.C. Chen, D. S. Tsai, G. Horng, visual secret sharing with cheating prevention revisited, digital signal processing 23 (2013)1496-1504

[11] Du- Shiau Tsai, Tzung-Her Chen,Gwoboa Horng,Acheating prevention scheme for binary visual cryptography with Homogeneous secret images,pattern recognition 40(2007) 2356 _ 2366 ,www.elsevier.com/locate/pr

[12] Y.C. Chen, D. S. Tsai, G. Horng, A new authentication based cheating prevention scheme in Naor–Shamir's visual cryptography, J. Vis. Commun. Image Repre-sent.23(8)(2012)1225–1233.

[13] M. Naor, A. Shamir, Visual cryptography, in: Proceedings of the Advances in Cryptology, ' 94, in: LNCS, vol.950, 1995, pp.1–12.