International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Survey of Cheating Prevention Techniques in Visual Cryptography

Smita Patil[1], Jyoti Rao[2]

[1, 2] Dr. D. Y. Patil Institute of Engineering and Technology, Pimpri, Pune-18, India

Abstract: ***Visual cryptography (VC) is a technique of encoding a secret image into share images such that stacking a sufficient number of shares reveals the original secret image. Shares are generally presented in transparencies. So each participant holds a transparency. The original secret image is recovered after superimposing the transparencies one to other. Basically, the performance of visual cryptography scheme depends on different measures, like pixel expansion, security, contrast, computational complexity, accuracy, share generated, number of secret images and type of secret images encrypted by the scheme. Most of the prior research work on VC focuses on improving two parameters: pixel expansion and contrast. Visual cryptography (VC) has numerous applications, such as authentication and identification, steganography, and image encryption. Horng et al. showed that cheating is possible in VC, where some participants can betray the remaining participants by fake transparencies. So, designing cheating-prevention visual secret-sharing (CPVSS) schemes has been proposed by many researchers to overcome cheating problem from existing VC. Intent of this paper is on study and performance analysis of the cheating prevention visual cryptography schemes and cheating problem in VC and extended VC.***

Keywords: Cheat-preventing scheme, cheating, secret sharing, visual cryptography, Security

1. Introduction

Naor and Shamir, in 1994 developed one of the best-known techniques known as visual cryptography. Visual cryptography is a cryptographic technique which allows visual information in the form of pictures, text, etc. to be encrypted in such a way that decryption does not require any computational devices and is done by the human visual system. Their research demonstrated a visual secret sharing scheme, where a secret image was split up into 'n' shares so that only someone with all 'n' shares could decrypt the secret image, while any one with less than 'n' shares discovered no information about the original secret image. The shares were printed on a separate transparency, and decryption was performed by stacking operation of the shares. When all 'n' shares were overlaid, the original secret image would be seen. The fundamental properties of Visual Cryptography are Pixel expansion, Contrast and Security.

The main goal of visual secret sharing scheme is to protect important secret data, from being lost or destroyed without accidental exposure. The protection of participants is not the main concern but security of data is important factor. Since there is no restriction on the behavior of the participants, any participant, called a cheater, who can reveal a fake share on purpose. Of course, cheaters may collude in an attempt to increase their profits. In 2006, Horng et al. showed that cheating is possible in a k-out-of-n visual secret-sharing scheme [7]. So, designing cheating-prevention visual secret-sharing (CPVSS) schemes has been proposed by many researchers to overcome cheating problem from existing VC. A visual secret-sharing scheme is said to be a cheating-prevention scheme if the probability of successful cheating is negligible. Naturally, cheating can be prevented in visual secret sharing scheme if participants suspect that some shares or the reconstructed images are not genuine. Based on this intuition, there are two approaches in designing CPVSS schemes. One is based on share authentication where each participant is provided with an additional share to authenticate other shares. The other is based on blind authentication where some property of the image is used to authenticate the reconstructed secret image [6]. Thus, the goal of share authentication is to provide the participants the ability to verify the integrity of the shares before reconstructing secret images, and the goal of blind authentication is to make it harder for the cheaters to predict the structure of the shares of the other participants. Usually, in a share-authentication-based CPVSS scheme, each participant receives two shares, i.e., one secret share and one verification share. The secret share is used to reconstruct the secret image, and the verification share is used to verify the integrity of the secret shares held by other participants. Therefore, the advantages of the CPVSS based on share-authentication approach are twofold. One is that checking the authenticity of shares is optional. It can be done only when someone is suspected of cheating. The other is that the generation of verification shares is done after the generation of secret shares. Therefore, any visual secret-sharing schemes (for any access structures) can be turned into a cheating-prevention scheme. The quality of the reconstructed secret image is not affected or only slightly degraded. The disadvantages of this approach are also twofold. One is that additional shares for verification purposes are needed. The other is that these schemes lack formal proof of security. Collusive cheating is still possible in VC so that, such scheme is still insecure. As per the Security is concern it is important to study how cheating is possible in visual cryptography and also how to prevent cheating in Visual Cryptography schemes.

This paper is organized as follows: Section 2 provides overview of cheating in visual cryptography schemes, how to prevent cheating is elaborated in section 3, performance of cheating prevention schemes are analyzed in section 4 and last section concludes the paper.

2. Cheating in Visual Cryptography Schemes

Cheating in Visual Cryptography is well studied and understood in secret-sharing schemes [8], [9]. Since VC is a

variant of secret sharing, it is natural to also consider this issue. Most cheating attacks in VC are known plaintext attacks where the cheaters know the secret image and are able to infer the blocks of victim's transparency based on the base matrices. It is observed that cheating is possible in (k, n) VC when k is smaller than n. There are two types of cheaters in VC. One is a malicious participant (MP) who is also a legitimate participant, namely MP € P (Qualified participant) and the other is a malicious outsider (MO), where MP € P. A cheating process against a VCS consists of the following two phases:

1) Fake share construction phase: the cheater generates the fake shares.
2) Image reconstruction phase: the fake image appears on the stacking of genuine shares and fake shares.

In order to cheat successfully, honest participants who present their shares for recovering the secret image should not be able to distinguish fake shares from genuine shares. A reconstructed image is perfect black if and only if the sub pixels associated to a black pixel of the secret image are all black. Most of the Visual Cryptography schemes have the property of perfect blackness. Some of common ways how MO and MP cheat visual cryptography are:

1) Cheating a VC by an MP
2) Cheating a VC by an MO
3) Cheating an EVCS by an MP.

2.1 Cheating a VC by an MP

A qualified participant can also be a cheater, where the participant creates a fake share image by using his original share images. By doing so, he will try to cheat the other participants. By doing so, he will try to cheat the other genuine participants because the fake share generated will be indistinguishable from the original share images and also the decoded output image will be different from the original secret image.

2.2 Cheating a VC by an MO

A disqualified participant called as MO will create fake shares by using some random images as input and will try to decode the original image. The MO will try to create fake shares of different sizes because the size of the original share may vary.

2.3 Cheating an EVCS by an MP

The Qualified participant creates the fake share from the genuine share by interchanging the black pixels by the white pixels which leads to less contrast of the reconstructed image. The less contrast in reconstructed image will be hard to see the image. The fake image in the stacking of the fake shares has enough contrast against the background since the fake image is recovered in perfect blackness.

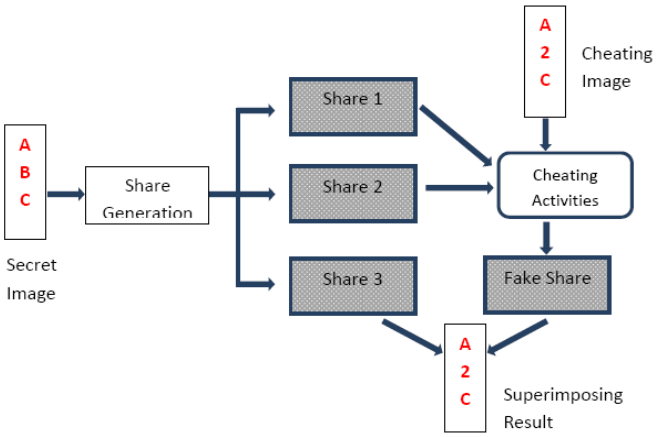

Figure 1: Cheating in Visual Cryptography

The above described way of cheating in Visual Cryptography is called individual cheating (IC), which is employed by a single participant. Since a certain participant presents a false or fake share images during the secret recovering phase, 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), practiced by several collusive participants. Victim's shares can be speculated with the shares they have in hand. Based on the speculation, 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 [11].

3. Cheating Prevention in Visual Cryptography Scheme

Jana, B et al [5] introduced Cheating prevention in Visual Cryptography using steganographic Visual scheme. The Visual Cryptography (VC) is a technique to encrypt a secret image into transparent shares such that stacking a sufficient number of shares reveals the secret image without any computation. 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. To achieve cheating prevention in VC we have proposed a steganographic scheme to embed a secret message 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 authentication of share images. In this method no verification share image is required to prevent cheating in VC.

Shuo-Fang Hsu et al [4] were first researchers to present Verifiable Visual Cryptography scheme. This scheme provides a verifiable visual cryptography (VC) technique for checking the validness to the shares available in a VC decoding instance. Compare to the reported cheating prevention VC schemes, the verifiable visual cryptography scheme maintains the original pixel expansion in VC scheme without cheating prevention ability. 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. Basically, the visual coherent among the revealed patterns of all pair of share images provides evidence to the genuine of the shares engaged in the decoding process. In this scheme the share verification process is done without resorting to any additional verification image. In addition to this, the proposed verification mechanism can easily be attached to any VC schemes in the literature to endow legitimate user with the ability to prevent cheating from malicious participants in secret sharing mechanism.

Jana B. et al [3] were first researchers to advise the Cheating prevention in Visual Cryptographic Schemes using message embedding. This scheme attempts to give a hardware based practical overview about cheating prevention of information hiding technique using Steganography and Visual Cryptographic Schemes (VCS). A combined technique has been proposed here, which allows visual information like printed text, handwritten notes, and images etc. to be distributed into 'n' secret shares as transparencies and embedding message into share became stego share for share authentication. In this scheme finally each of these stego shares embeds into a cover image using hardware module. At the time of recovering secret image the receiver first decode each stego shares from the cover work and then extract secret message from share to prevent cheating. The original secret image can be retrieve by overlapping the share images. The proposed encoding and decoding scheme for share generation is implemented in software module and embedding of message into share images and stego share into cover image are implemented in hardware-based system for 2-D images.

Many studies focused on the cheating problems in VCS, and consequently many cheating immune visual cryptography schemes (CIVCS) have been proposed. The classified techniques proposed in these CIVCSs 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 examining the above techniques, it 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 networks are available. The second technique requires the extra verification shares, which inevitably increases the burden of the participants. The third and forth 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 CIVCS can only be based on a VCS with specific access structure, for example, the (2, n) threshold access structure [10].

Bin YU. et al [11] were researchers to advise the Co Cheating prevention in Visual Cryptographic Schemes using trusty third party as the verifier and extra verification shares. Based on a trusty third party, a co-cheating prevention visual cryptography scheme (CCPVCS) is proposed and evaluated with extra verification shares. Also checking efficiency is improved by verifying the truth of several shares simultaneously, with designed special verification shares. Since the scheme idea is different from previous ones, the pixel expansion is small and the recovered secret image is good for viewing. By introducing a trusty third party as the verifier, the CCPVCS could prevent co-cheating through verifying the truth of several shares simultaneously.

The verifier owns a peculiar verification share and n optional verification shares. Through a peculiar verification share and n optional verification shares, the truth of several shares can be detected simultaneously. Not only co-cheating has been prevented effectively, but also the checking efficiency is better than the previous schemes. However, the number of verification shares which kept by the third party is large, which needs to be reduced significantly [11].

4. Performance analysis of cheating prevention schemes

In Visual Cryptography basically a blackness property is used to avoid cheating and also as performance measure of the VC scheme. The Generic Transformation method for Cheating Prevention is useful and has strong characteristics. By the attacks and improvement in different VC scheme, it is observed that an efficient and robust cheat-preventing method should have the following properties. 1) It does not rely on the help of an on-line TA. Since VC emphasizes on easy decryption with human visual system only, we should not have a TA to verify validity of share images. 2) The increase to pixel expansion should be as small as possible. 3) Each participant verifies the shares of other participants. This is somewhat necessary because each participant is a potential cheater. 4) The verification image of each participant involved in communication should be confidential and different. It spreads over the whole region of the share image. Since it is observed that this is necessary for avoiding the described attacks. 5) The contrast of the secret image in the stacking of shares is not reduced significantly in order to keep the quality of VC. 6) A cheat-preventing method should be applicable to any VCS [2].

The best performance measure of cheating in VC is Perfect Blackness Property. The participants in qualified set Q generates real secret image in perfect blackness so that it is not possible to cheat them. The cheating in a VC by an MO is done without any genuine share at hand. Basically it uses (2, 2) VCS to construct the fake shares. The problem identified in this type of cheating is right share size. The solution for this is to try all possible share sizes and the standard sizes are A3, A4 etc. Still it suffers from alignment problem during reconstruction phase and also uses solid frame. The performance of cheating prevention in EVCS by an MP depends on contrast. In VC it only requires contrast be non-zero. In EVCS it has too small contrast so that it is easily cheat by anyone just by adding a small no of Black

sub pixels.

5. Conclusion

In this paper various cheating prevention schemes are studied and their performance is evaluated on the basis of contrast. While selecting cheating prevention method in visual cryptography or in EVCS 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 incurs 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. There are many topics that deserve further investigations, e.g., to give formal definition of the security of CPVSS schemes and to design secure yet practical CPVSS schemes based on share authentication. It processes faster due to less traversal steps and minimizes the effect of Cheating. Participants colluding problem is solved in Co cheating prevention scheme with trusty third party.

References

[1] M. Naor and Shamir, “Visual cryptography," in Proc. Advances in Cryptology, 1994, vol. 950, LNCS, pp. 1-12

[2] Chih-Ming Hu and Wen-Guey Tzeng, ”Cheating Prevention in Visual Cryptography”, IEEE Transactions on Image Processing, Vol. 16, No. 1, January 2007

[3] Jana, B. ; Mondal, S.K. ; Jana, S. ; Giri, D., "Cheating prevention in Visual Cryptographic Schemes using message embedding: A hardware based practical approach” International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014, 319 – 324

[4] 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

[5] 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.

[6] 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

[7] 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

[8] T. Rabin, “Robust sharing of secrets when the dealer is honest or cheating,” J. ACM, vol. 41, no. 6, pp. 1089–1109, Nov. 1994.

[9] M. Tompa and H. Woll, “How to share a secret with cheaters,” J. Cryptol., vol. 1, no. 2, pp. 133–138, Aug. 1989.

[10] Liu, F., Wu, C., Lin, X. Cheating immune visual cryptography scheme, IET Information Security 5 (1), 2011, pp. 51-59.

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