A Survey on Cheating Prevention with Verifiable Scheme

Priya Venny
Research Scholar (Computer Engg.)
DYPIET (Pimpri)
Pune, India

Jyoti Rao
Assistant Prof. (Comp.Engg)
DYPIET(Pimpri)
Pune, India

ABSTRACT
Visual Cryptographic technique has become an important field of study in modern cryptography. Visual cryptography (VC) has quite a few applications and some of them are authentication and identification, steganography, and image encryption. As the era demands the need of security and Visual Secret Sharing to resist cheating scenario is a Visual Cryptographic technique. VSS is simple as it is easily detectable by human visual system. A secret image sharing scheme is used for identifying the existence of cheater. The use of verifiable scheme leads helps find the presence of a cheater. The problem of cheating prevention exists and researchers have proposed scheme like Cheating-prevention visual secret-sharing (CPVSS) schemes. This paper is based on the study of the cheating prevention happening in Visual Cryptography.

Keywords
Cheaters, Cheating Prevention, Cheating Activity, Visual Secret Sharing (VSS).

1. INTRODUCTION
Information Security is a main factor of concern in Information Technology and communication. The use of internet is increasing and security is becoming a reason of concern. In today's world our data is not safe and with the enhancement in technology, security measures have to be enhanced. By combining the of computer and communication technology more and more image information can be transmitted and exchanged quickly and easily on Internet.[3] Specially the in departments such as army, banking and airways the need for security level is high and many techniques such as steganography, cryptography are used. The use of Visual Cryptography technique has brought a huge enhancement in the security and helped in cheating prevention.

Cryptography is a technique and it Is the science and art of altering messages to make them secure and resistant to attacks and Visual Cryptographic (VC) technique is a technique of cryptography, images known as shares encrypts a secret image so that the secret image is recovered by stacking sufficient shares and these shares are given to different parties or participants. Pixel expansion security contrast is among few of the properties of VC. Various other methods like steganography, feature extraction helps in improving the security of the Visual Cryptography scheme.

It is important to know the basic information related to the terms like legitimate participants or users, cheaters, shares and Fake shares, etc. The legitimate participants or users are the people who are genuinely interested in the security of the secret image. Cheaters are the people who are malicious participants who have the intention of gaining the knowledge of the secret. In other words it can say that they are the people who even create shares which are not correct and are a part of cheating in cheating prevention. Images when broken up into multiple parts are known as Shares. Fake Shares are the shares produced by the Cheaters.

The efficient method for hiding secret image in a highly secure way is Visual secret sharing (VSS) and this is done by dividing a secret image it into images known as share images and encrypts them in order to secure. This is a system where anyone can decrypt it easily by the human visual system. The main concept behind the original visual secret sharing (VSS) scheme is the encryption of a secret image into n meaningless share images. Any information about the secret is not revealed of the shared secret by combining any the n share images if all the shares are not present. This scheme of (VSS) is a scheme that is used to spread the image securely in a non-computer environment [2].

The limitation of VSS scheme is it has a lot of transmission risk and attracts the attention of the malicious participants. Visual secret sharing scheme can easily be corrupted by dishonest participant or malicious participant. There is no security measure in this method and to secure the whole scheme verifiable scheme can be used. In this scheme there is use of Verification image. In Secret Image Sharing Scheme two types of attack might occur. Either sender or receivers can act as dishonest.

The secret Image is divided into shares and it is sent to the participants along with the verification Image. This helps detection of a cheater and also helps preserve the integrity of the secret image. If the detection is possible before the malicious participant hinders the secret the integrity is secured.

2. OVERVIEW OF VISUAL SECRET SHARING IN CHEATING PREVENTION
The encryption of visual information in the form of text, pictures in such a way that decryption can be done by the human visual system and it does not need any device for computation and this is known as Visual Cryptography. The Research is done and which says that the n shares produced of the secret image and it could be reconstructed by stacking with all n shares and if less than n shares are received then it was of no use to discover original image. The shares were produced on a separate transparency, and by stacking the shares decryption was performed. All 'n' shares when overlaid the original secret image would be gotten.[6]

VSS as it is known a secret image hiding scheme in a highly secure way. It can be said that the main property to differ VSS from secret sharing [1] is that the security in VSS is attained by losing the contrast and the resolution of the *SI*. Certainly, the original secret image created is inferior to the quality of the reconstructed secret but the secret is still seen by human's vision according to the human visual system. With the

advancement of this technique of VSS many more applications and linked technique have been proposed. Some of them are visual authentication, visual identification, and image encryption. Also it can be said that a variety of VSS schemes were proposed to be used in different scenarios or to gain different requirements [4].

The main essence of VCs is that the secret share is used to reconstruct the secret image, and for the integrity verification the verification share is used by the participants. Therefore, dual advantages of the share authentication approach are based on Cheating Prevention. By this the checking the authenticity of shares is our choice or optional and it is done only when someone is suspected of cheating. This involves other concept; the generation of verification shares is done after the creation of secret shares.

2.1 Activities of Cheating

There are two types of cheaters in VC. One of them is malicious participant or MP who is also legitimate participant, namely MP € P (Qualified participant) and the other is a malicious outsider (MO), where MP € P. A cheating process in VCS involves following the phases:

1. Construction of fake share: In this phase cheater produces fake shares;
2. Reconstruction of Image: In this phase, fake image appears by overlapping the genuine shares with fake shares.

Cheating can be successful if the honest participants that present their shares for reconstructing secret image are not able to recognize fake shares from the genuine shares. An image that is reconstructed is perfect black only if each sub pixels that are associated with black pixel of secret image are also black. Almost all the proposed VC schemes exhibits perfect blackness property.

There are three methods. The first cheating method is initiated by an MP, while the second cheating method is initiated by an MO. Both of them attempt to attack VC. The third cheating method is instigated by an MP and attempts to attack EVC.

In Cheating a VC by MP a cheater can also be among the qualified participant. In this the participant uses the original share in order to create a fake share. By doing so, he will try to cheat the other genuine participants because the fake share generated will be indistinguishable from the original shares and also the decoded output image will be different from the original secret image.

In Cheating a VC by an MO a participant called as MO is a disqualified participant. It will use some random images to create fake and will also try to decode the original image. The original share size may vary as MO will try to create fake shares of different sizes

In Cheating an EVCS by an MP **t**he Qualified participant creates the fake share from the legitimate share by interchanging the black pixels by the white pixels which leads to less contrast of the reconstructed image. The lesser is the contrast will be harder it to see the image in reconstructed image. The fake image in the stacking of the fake shares has enough contrast against the background as even in the presence of the perfect blackness the fake image can be

recovered. [6]

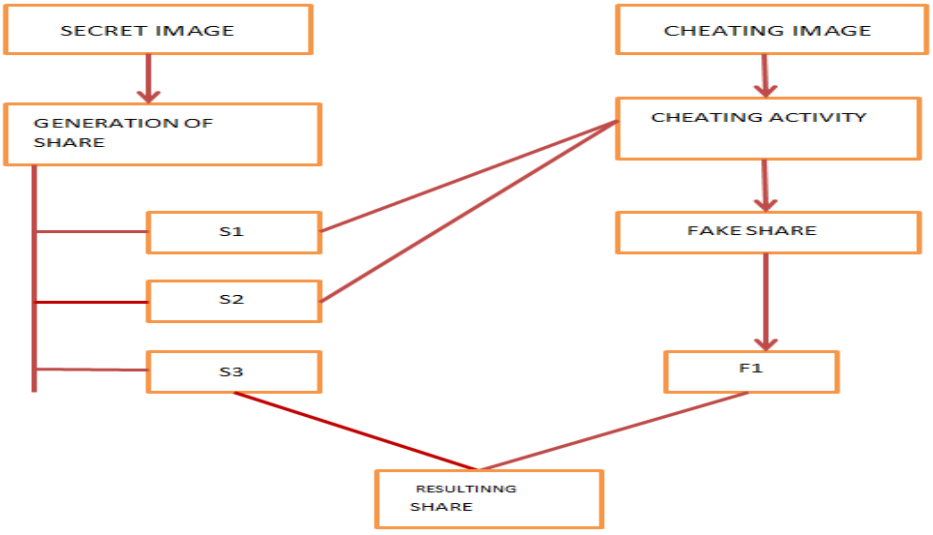

Fig 1: Cheating Activity

3. A REVIEW OF CHEATING PREVENTION METHODS

Moni Naor and Adi Shamir presented a Visual Secret Sharing technique which was termed as (k, n) secret sharing problem. They made assumptions that the image consists of B&W pixels where every pixel is controlled independently. The white pixel signifies the transparent color. The drawback is that the deciphering process results in loss of contrast [1].

Shares are encrypted and sent. A qualified group of participants can recover the secret message without using any cryptographic computation. But the original scheme can easily be corrupted by malicious participant. The proposal of an extension of VCS to verify cheaters based on digital

watermarking. Without any additional information and cryptographic computation, every participant can verify the validity of shares of other participants only by watermark extraction operation. Thus the security of VCS is enhanced. [3]

Cheating activity (CA) is a method in this the dishonest participants are referred to as cheaters have the motive of collude and want to fool the targets and can cause random damage to the victims. Therefore, the victims accept a fake secret image also known as a cheating image and are different from the actual secret image as. They presented two kinds of cheating prevention methods which are known as share authentication and blind authentication [4].

In Share authentication (SA) the use of verifiable messages the authentication of a share transparency from other participant is decided by the participant or the dealer. Usually fake transparencies are generated by the malicious participant and must pass the test of authentication. Therefore when the fake transparency passes the authentication the stacking result is accepted by the victim. In Blind authentication (BA) without depending on any verifiable message the malicious participants forecast the structure of the transparencies of all other participants is hard and such that the cheaters are not able to generate a fake transparency. [4]

Naor and Shamir[1] proposed a Visual cryptography (VC) technique, and it has many numbers of applications, containing identification and visual authentication, image encryption and steganography. A method was proposed that Cheating is possible in VC where some participants can deliberately mislead the remaining participants by producing fraudulent transparencies. So, from that time the design of cheating-prevention visual secret-sharing (CPVSS) schemes are being studied by many researchers. In this CPVSS scheme is used and has shown that it is not immune to cheating. For realizing information security Cryptographic schemes are very useful. The basic goal of cryptanalysis is to find potential weakness in cryptographic schemes. Therefore, cryptanalysis plays a very important role in practice. A cryptanalysis of a cheating-prevention scheme in VC and have shown that it is not cheating immune. There are many topics that need further analysis and investigations, e.g., to provide a formal definition of the security of CPVSS schemes and to design secure yet practical CPVSS schemes based on share authentication**.** [7]

In this method, the author dealt with cheating problem in VC and also in extended VC. They have explained that the attacks of malicious opponent who may move away from the scheme in any manner. The three of the cheating methods are shown and are also applied by attacking existent VC or extended VC schemes. In this one of the cheat-prevention schemes is improved. A method which is generic was proposed that has the property of cheating prevention and Converts a VCS to another VCS. The previously existing cheat-preventing schemes are well examined and it is seen that they are either not robust or still improvable. The cheat-preventing schemes are improved. By the attacks created by the author, an essential principle for a robust cheat-prevention VCS is pointed out here. Finally a transformation of VCS for cheating prevention is suggested. In this the transformation incurs minimum overhead on contrast and pixel expansion. Finally only two subpixels are added for each pixel in the image and the contrast is reduced slightly. [8]

Verifiable Secret Image Sharing has become an important field of study in modern cryptography. An analysis is done on a scheme to identify the existence of cheater in this new secret image sharing scheme as the need for security and verifiability is increasing to resist the cheating situation. In this a method of ensuring security is introduced. An n x n secret image and n x n verification image are used to create shares after that a cover image for transmission and before transmitting the shares are embedded into the cover image. Structural similarity and mean square error measure of regenerate verification image with original verification image verifies the coherence of the secret. Computational cost of this method is low which makes it suitable for covert message communication and sharing of scanned documents. [9]

In This method introduced the use of steganography in cheating prevention in Visual Cryptography scheme. In this scheme a stego share is created using cheating prevention scheme and steganography is also used to secure this secret image in the share construction phase. In order to prevent cheating in VC a steganography scheme is used. In this method verification image is not used. The hidden message is got by stacking the stego images and the secret image is verified. [10]

A new verifiable visual cryptography scheme (VCS) for colour image is presented by Han et.al. it fulfils the distribution and recovery of the secret image and verifiable image which relies on XOR algorithm. The distribution and regeneration of the secret image are done with the help of additive colour model and the halftone technology correspondingly. The presented scheme is easy and effective. The visual quality of recovered image is adequate with the VCS without incurring any pixel expansion and the regeneration of the verification image is clean without any distortion. To solve the problem of security, they have introduced a verification image which is used for distribution and reconstruction process. The recovered secret image is possesses characteristics such as the good contrast without pixel expansion, and the recovered verifiable image is clean and without distortion using XOR algorithm for stacking the shares and verification shares. The shares and the regained secret image are having the identical size as that of the original secret image without pixel expansion. Also, the recovery verifiable images have identical size as of the verifiable image without distortion. This scheme introduces trusted third party (TTP) which is used to validate the cheating activity of the participants. In these schemes, the pixels of the shares are randomly distributed. A Malicious set of users are not able to get any secret information related to the secret image and the participants cannot reconstruct the verifiable images without intervention of the trusted third party. Thus, this scheme improves the security of the colour VCS and can check the cheating of the participants. [11]

A new method was proposed for a chaotic visual cryptography algorithm In order to create a scheme in which two shares are produced, one share is based chaotic sequence and the other share is generated by an XOR between the chaotic share and the secret message. The used system of the chaotic system is highly sensitive to its parameter like the initial condition. By the use of brute force attack also, no one is easily able to guess these parameters, and also by using to a strong processor. The Using visual cryptography increases the security level of the system and also does not enforce a complex computational burden to the procedure. [12]

The Steganographic and Visual Cryptographic Schemes (VCS) are used for cheating prevention. The author presents a hardware based practical outline about information hiding in technique for cheating prevention using these schemes. Steganographic and Visual Cryptographic schemes altogether allows visual information such as printed text, images etc. to be divided into 'n' secret shares as transparencies and generating stago share for authentication which is obtained by embedding message. It is embedded into a cover image by using hardware module. Visual cryptography technique is used to generate the share in software platform. Then the message is embedded to each of these shares in the original hardware platform. Recovering process is done performed at the receiver by first decoding each stego shares from the cover work and then extracting secret message from share so that cheating can be prevented. The shares are overlapped to recover the original secret message. The division of the original secret image is done in such a way that after performing OR operation of qualified shares the secret image is retrieved. The author proposed the encoding and decoding scheme for share generation to be implemented in software module whereas, the hardware module is used to embed the message into share thus generating stego share which is embedded into cover image. The hardware device used is easy to carry anywhere as it has low-weight and convenient. Additionally, this handy hardware device could be used to support USB and which would help in sending or receiving and even decoding the secret information from MMS stego images. Such hardware module would consume less power than the existing computer based systems. An algorithm to generate share from Secret Image is taken. [13]

4. CONCLUSION

The above survey says that Cheating Prevention scheme helps preserve the integrity of the secret image by detecting the presence of the cheater hence performing a secure transmission. This is an important Scheme in Visual cryptography. The human visual System is able to recognise the secret image recovered. Therefore it can be said that the secret image recover has to be very accurate in order to avoid distortion. Some of the easy and simple way to prevent cheating prevention are described in this paper. The review can be useful for finding the cheaters location.

5. REFERENCES

[1] M. Naor And A. Shamir, "Visual Cryptography," In *Advances In Cryptology*, Vol. 950. New York, Ny, Usa: Springer-Verlag, 1995, Pp. 1–12.

[2] Kai-Hui Lee , Pei-Ling Chiu, "Digital Image Sharing by Diverse Image media",IEEE Transactions on Information Forensics and Security, vol 9, No. 1,pp.88-98,January 2014. Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.

[3] Tan, Xiaoqing, and Qiong Zhang. "A Kind of Verifiable Visual Cryptography Scheme." *Emerging Intelligent Data and Web Technologies (EIDWT), 2013 Fourth International Conference on*. IEEE, 2013.

[4] Chen, Yu-Chi, Du-Shiau Tsai, and Gwoboa Horng. "Visual secret sharing with cheating prevention revisited." *Digital Signal Processing* 23.5 (2013): 1496-1504.

[5] Horng, Gwoboa, Tzungher Chen, and Du-Shiau Tsai. "Cheating in visual cryptography." *Designs, Codes and Cryptography* 38.2 (2006): 219-236.

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

[7] Hu, Chih-Ming, and Wen-Guey Tzeng. "Cheating prevention in visual cryptography." *Image Processing, IEEE Transactions on* 16.1 (2007): 36-45.

[8] Chen, Yu-Chi, Gwoboa Horng, and Du-Shiau Tsai. "Comment on "cheating prevention in visual cryptography"." *Image Processing, IEEE Transactions on* 21.7 (2012): 3319-3323.

[9] Rose, A. Angel, and Sabu M. Thampi. "A Secure Verifiable Scheme for Secret Image Sharing." *Procedia Computer Science* 58 (2015): 140-150.

[10] Jana, Biswabandhu, et al. "Cheating prevention in Visual Cryptography using steganographic scheme." *Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on*. IEEE, 2014.

[11] Chen, Qin, et al. "An (n, n) threshold Visual Cryptography Scheme for Cheating prevention." *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on*. Vol. 8. IEEE, 2010.

[12] Mostaghim, Melika, and Reza Boostani. "CVC: Chaotic visual cryptography to enhance steganography." *Information Security and Cryptology (ISCISC), 2014 11th International ISC Conference on*. IEEE, 2014.

[13] Jana, Biswabandhu, et al. "Cheating prevention in Visual Cryptographic Schemes using message embedding: A hardware based practical approach."*Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on*. IEEE, 2014.