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

Survey of Various Techniques on Cheating Prevention in Visual Cryptography with Steganography Scheme

Sneha A.Deshmukh[1], P.B.Sambhare[2]

[1]Student, Computer Science & Engineering, P R Pote (Patil) college of Engineering & Management, Amravati, India

[2]Assistant Professor, Computer Science & Engineering, P R Pote (Patil) college of Engineering &Management, Amravati, India

Abstract: ***To maintaining the secrecy and confidentiality of images is a vibrant area of research, with two different approaches being followed, the first being encrypting the images through encryption algorithms using keys, the other approach involves hiding the data using data hiding algorithm to maintain the images secrecy. A content owner encrypts the original image using an encryption key, and a data-hider can embed additional data into the encrypted image using a data-hiding key though he does not know the original content. With an encrypted image containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key.***

Keywords: Cover image, data hiding, data extraction, Image encryption, Image decryption and Data recovery, DWT.

1. Introduction

Naor and Shamir [1], 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.

Steganography [8] is the process of hiding a secret message within a larger one in such a way that someone cannot know the presence or contents of the hidden message. One of the other main uses for Image Steganography is for the transportation of high-level or top-secret documents between international Governments.The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Technically in simple words “steganography means hiding one piece of data within another”.

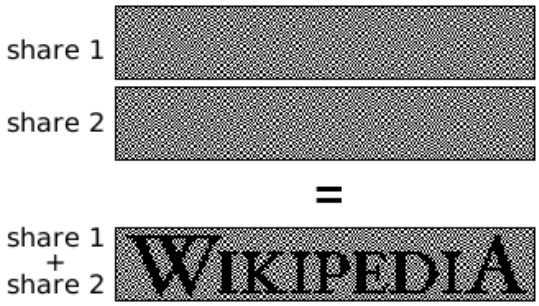

Figure: Visual Cryptography

The main goal of visual secret sharing [9] 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 . So, designing cheating-prevention visual secret- sharing (CPVSS) schemes has been proposed by many researchers to overcome cheating problem from existing VC.

Cryptography focuses on keeping the content of the message secret whereas data hiding concentrates on keeping the existence of the message secret . Data hiding[10] is the other technique for secured communication. Data hiding involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. Data hiding is the process of hiding a secret message within cover medium such as image, video, text, audio. Hidden image has many applications, especially in today’s modern, high-tech world. Privacy and secrecy is a concern for most people on the internet. Hidden image allows for two parties to communicate secretly and covertly.

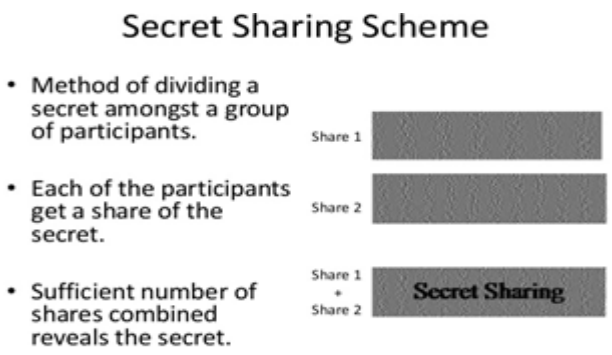

Figure: Secret sharing scheme

The strength of data hiding [9] gets amplified if it combines with cryptography. The terminologies used in data hiding are cover-image, hidden image, secret message, secret key and embedding algorithm. Cover-image is the carrier of the

message such as image, video or audio file. Cover- image carrying the embedded secret data is the hidden image. Secret message is the information that is to be hidden in a cover image. The secret key is used to embed the message depending on the hiding algorithm. The embedding algorithm is the way, which is used to embed the secret information in the cover image.

The security of the transformation of hidden data can be obtained by two ways: encryption and data hiding. A combination of the two techniques can be used to increase the data security. In encryption, the message is changed in such a way so that no data can be disclosed if it is received by an attacker. Whereas in Data hiding, the secret message is embedded into an image often called cover image, and then sent to the receiver who extracts the secret message from the cover message. When the secret message is embedded into cover image then it is called a hidden image . The visibility of this image should not be distinguishable from the cover image, so that it almost becomes impossible for the attacker to discover any embedded message.

Cheating in Visual Cryptography

Cheating in Visual Cryptography [3] is well studied and understood in secret-sharing schemes. 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 two phases as given:
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 [2] are:
1) Cheating a VC by an MP
2) Cheating a VC by an MO
3) Cheating an EVCS by an MP.

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) 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.

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.

2. Literature Review

In 2014, 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.

In 2012, 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.

In 2014, 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.

In 2010, Bin YU. et al [7] 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.

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 .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.

3. Overview of Proposed Method

Data hiding provides easy way of implementing the methods. The idea behind this design is to provide a good, efficient method for hiding the data from hackers and sent to the destination securely. This system would be mainly concerned with the algorithm ensuring the secure data transfer between the source and destination. For that we first used encryption and then data hiding and vice-versa. In data hiding we will use cover image for security purpose. The medium in which information is to be hidden, is called as cover image.

4. Conclusion

From the Literature Survey, it is conclude that the Steganography scheme is used for better transmission of data. In this paper various cheating prevention schemes are studied .There are various terms that can be used here is: secret share, half tone pixel swapping, steganographic scheme. A novel scheme for separable reversible data hiding in encrypted image is used, which consists of image encryption, data encryption, data embedding and data extraction / image recovery phase.

References

[1] Naor, M., and Shamir, A. (1995), Visual cryptography, in ‘‘Advances in CryptogolyEurocrypt ’94’’ (A. De Santis, Ed.), Lecture Notes in Computer Science, Vol. 950, pp. 112, Springer-Verlag, Berlin..
[2] SmitaPatil “Survey of Cheating Prevention Techniques in Visual Cryptography” Dr. D. Y. Patil Institute of Engineering and Technology, Pimpri, Pune-18, India 2012.
[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] Liu, F., Wu, C., Lin, X. Cheating immune visual cryptography scheme, IET Information Security 5 (1), 2011, pp. 51-59.

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

[8] Ravi Kumar. B #1, Murti. P.R.K.*2 ," Data Security and Authentication Using Steganography" 1,2 Department of Computer and Information Sciences, University of Hyderabad, (P.O) Central University, Gachibowli, Hyderabad 500046, India.

[9] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012

[10] W. Puech, M. Chaumont and O. Strauss "A Reversible Data Hiding Method for Encrypted Images" Author manuscript, published in "IS&T/SPIE Electronic Imaging 2008 - Security, Forensics, Steganography, and Watermarking of Multimedia Contents, San Jose, CA : United States".