ANALYSIS OF THE VARIOUS TYPES OF SECURITY ATTACKS ON VISUAL CRYPTOGRAPHY

Ankit Saxena[#1] , Abhishek Kumar Mishra[#2]

[#] IFTM University, Moradabad, Uttar Pradesh, INDIA

[1]ankit.saxena5@yahoo.com

[2]abhimishra2@gmail.com

Abstract

Security has become an inseparable issue in information technology is ruling the world. Now days the most popular issue is to provide the security of the private (confidential) data from the unauthorised access . Today every person is want to hide the information from the another person. But, Another person is interested to access the unauthorized data (information) of another person.

The visual cryptography is used to hide the secret information from the unauthorized person. Visual cryptography scheme is firstly introduced by Naor and Shamir[1] in 1994 using the black and white images. In the visual cryptography schemes the dealer encoded the secret image in the 'n' numbers of shares. And the 'k' out of 'n' numbers of shares are used to reconstruct of secret image. In the visual cryptography the secret information (printed text, hidden note, image, pictures etc) in the form of image can be revealed without any complex cryptography mathematical computation. In the visual cryptography the decryption process is done human vision system without the aid of computer. The visual cryptography can be used for copyright for images, unauthorized access of information or data, visual authentication etc.

But , In the visual cryptography the cheaters can cheat the data and access the information. In this paper we provide the analysis of the security attacks on visual cryptography that how the unauthorized person try to access the data (information) of another, which type of methodology they used, and who are they person.

Keywords

Security attack in visual cryptography, security issues in visual cryptography, unauthorized access to information (data), in visual cryptography, cheating visual cryptography, hacking visual cryptography.

I. INTRODUCTION

In 1994 in the open literature for black and white images, The concept of the (k, n) visual cryptography technique was firstly introduced by Naor and Shamir[1]. Visual Cryptography is a new technique which provides the information security by using the simple algorithm unlike the complex , computationally intensive algorithm (such as DES, IDEA,, RSA). used in other techniques like in traditional cryptography.

Visual Cryptography is a new technique which provides the information security by using the simple algorithm unlike the complex , computationally intensive algorithm (such as DES, IDEA,, RSA) as used in other techniques like in traditional cryptography. visual cryptography can be applied for copyright for images, access control to user images, visual authentication and identification of any kind of image like (normal or digital).

Visual cryptography techniques allows the visual information to be encrypted in such a way that their decryption process can be performed by human visual system without the aid of any complex computer programming algorithm.

In the (k, n) visual cryptography schemes the secret information is encrypted by dividing the secret image into the 'n' numbers of shares and in the decryption process the only 'k' numbers of shares out of 'n' numbers of shares are used to reconstruct the secret image. in which the 'n-k' numbers of shares are useless.

In the visual cryptography the chance of the attack is increase when the value of k<n so the attacker can easily access the secret data. As only 'k' numbers of shares are needed to reconstruct the image.

And 'n-k' shares are useless. But, the 'n-k' numbers of shares also have the part of secret information and if 'n-k' numbers of shares are used then the hacker/ cheater can access the secret information. The cheater also used the concept of the fake share construction to access the secret image (information/ data).

II. BASIC MODEL OF VISUAL CRYPTOGRAPHY

A dealer encodes the secret into 'n' share and gives each participant equal number of share(one participant has only one share), where each share is a transparency. The secret is visible if any 'k' of participant’s stack where transparencies together but none can see shared secret individually.

The receiver aligns the share and the secret information is revealed by human visual without the help of any computer system Visual Cryptography techniques allow the visual information to be encrypt in such a way that the decryption can be performed by human visual system, without the aid of computer system.

1) Division Of The Pixel

In the visual cryptography techniques the encryption process of secret (source) image is done by dividing the secret image into 'n' numbers of shares. In this one pixel is divided into two sub pixel and the sub pixel is divided into two color region black and white which is given below in Fig 1

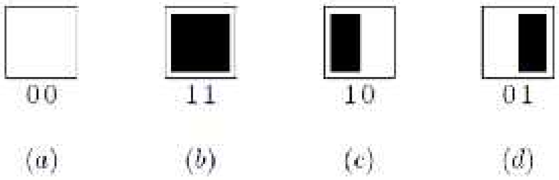

Fig 1:Division of sub pixel into black and white color

(a) White pixel (b) Black pixel

(c) LB pixel (d) RB pixel

The decryption process is done by the human visual system for which decryption is done by overlapping the 'k' share into a stack on the overhead projector.

2) Superposition Of Pixel

If we stack two LB pixels (or two RB pixels) we get nothing new, whereas, if we stack an LB pixel and an RB pixel, we get a black pixel. This can be shown as in Figure 2 We can see that by the representation used for pixels, the superposition of two pixels can be thought of as if a binary "OR" operation.

In this one pixel is divided into two sub pixel and the sub pixel is divided into two color region black and white.

The division of pixels is as follow

White -00

Black – 11

LBlack -10

RBlack -01

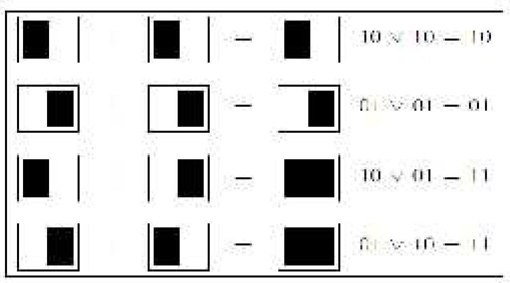

Fig 2: The overlapping mechanism

The mechanism behind the overlapping is that if we match same we get same and if we match different pixel we get black pixel as output which is shown in fig 2.The identification of the stack it just like as a Boolean -OR operation denoted by 'V'. which is as follows

A	B	O/P
0	0	0
0	1	1
1	0	1
1	1	1

III. (K, N) VISUAL CRYPTOGRAPHY OF SECRET IMAGE

In the encryption process the secret image is encrypted (divided) into 'n' numbers of shares. As shown in the Fig 4, Fig 5, Fig 6 the secret image Fig is divided into 3 shares which are share1, share 2 and share 3 .The share is work as cipher image.

The decryption is done by human visual system for which decryption is done by overlapping the any two shares and result via overhead project. As shown in the Fig 7

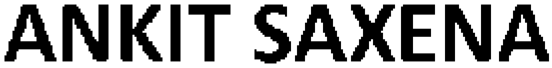

Fig 3 Secret image

Fig 4 share 1

Fig 5 Share 2

Fig 6 Share 3

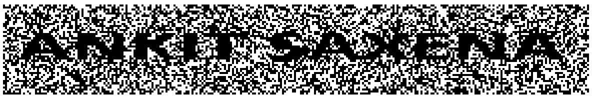

Fig 7 Reconstruct image

In the above example the secret image Fig 3 is divided into 3 shares (share 1,2 ,3) and we use any two share to reconstruct the share out of three. So the third share is useless.

IV. ATTACKS AND SECURITY

Horng et al proposed that the any unauthorized person (cheater/ hacker) can access the information of any other person in visual cryptography. When the number of selected shares for reconstruction of image is smaller than the total numbers of shares means that the[2,4,5]

$$k<n$$

where

k = numbers of selected shares for reconstruction of secret image

n = Total number of the share of secret image at the time of encryption.

V. TYPES OF CHEATERS

In the visual cryptography the secret image (information in the form of image) is divided into the n shares and the shares are divided equally to the 'k' participant which are authorized to access the image. When the 'k' numbers of participant overlap there shares the can easily access the secret image.

In the visual cryptography there are two types of participant

1. The Authorized participant which are known as Qualified participant
2. The Unauthorized participant which are known as outsiders.

These two types of participant may work as the cheater in the visual cryptography for access the unauthorized data (information). and as a cheater they are known as

1. Malicious participant (MP) who are Qualified participant
2. Malicious outsider(MO) who are outsiders

VI. OVERALL CHEATING PROCESS

A cheating process against a VCS consists of the following two phases:[2,3,4,5]

1. Fake share construction phase: In this the the cheater generates the fake shares.

2. Image reconstruction phase: In this the fake image appears on the stacking of genuine shares and fake shares.

The overall cheating process is depend upon to predict the alignment of the pixels position. In order to cheat successfully the prediction must be accurate so that the genuine (honest) participants (Those participant who are also authorized and have the shares out of 'n' numbers of shares and not interested in cheating) 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 the sub pixels associated to a black pixel of the secret image are all black. Most proposed VC schemes have the property of perfect blackness. An example of the cheating process is shown in fig.8

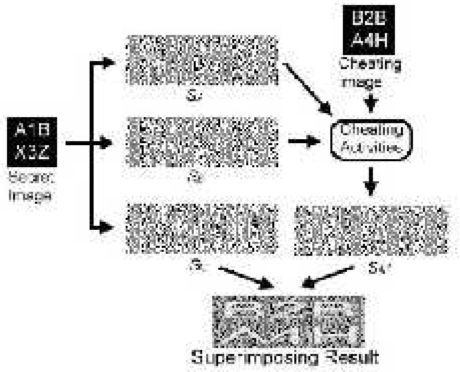

Fig 8 The Cheating Process

VII. METHOD USED FOR CHEATING BY MALICIOUS PARTICIPANT (MP) AND MALICIOUS OUTSIDERS (MO)

1) Cheating a VC by an Malicious Participant (MP)

A qualified participant [2] (who is the authorized participant and have the one share out of the 'n' numbers of shares of secret image) can also be a cheater, For the cheating the Malicious participant with the help of his original share create a fake share. With the help of this he/she will try to cheat the other genuine (honest) participants(Those participant who are also authorized and have the shares out of 'n' numbers of shares and not interested in cheating) because the generated fake share will not be able to distinguishable it from the original shares. The resultant of the overlapping the with the fake share the decrypted reconstructed image will be different from the original secret image. So, the original image will not be reconstructed with the help of fake share and another image is created with the alignment with fake share. The process of cheating is shown in the Fig.9

In this the secret image is divided into two shares s1 and s2 and a fake share is created by Malicious Participant fs when the reconstruct of image is with fake share then we will not get the secret image but we get any other image as fs + s1 and fs + s2 and when we reconstruct the image with s1 an d s2 we will get secret image s1 +s2.

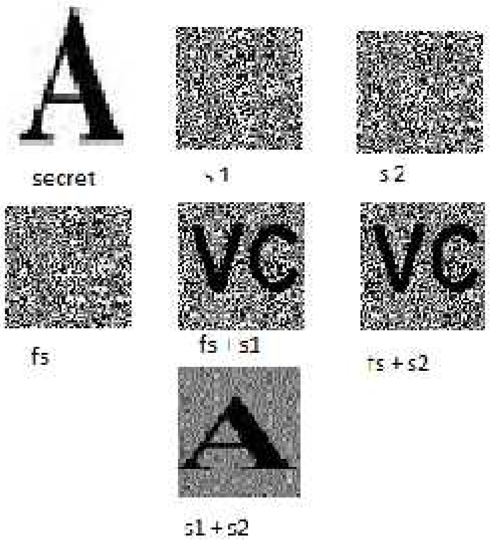

Fig. 9- Cheating a VC by an MP

2) Cheating a VC by an Malicious Outsiders (MO)

A person which is not authorized to access the image is known as disqualified participant or he / she can also be known as Malicious Outsiders (MO). the MO can also cheat the visual cryptography for which he/ she will create fake shares by using some random images shares as input and will try to decrypting the secret image. For decrypting the secret image the malicious Outsider create numbers of fake shares of different sizes to match the secret image because the the secret share maybe of any size. The process is shown below in Fig 10

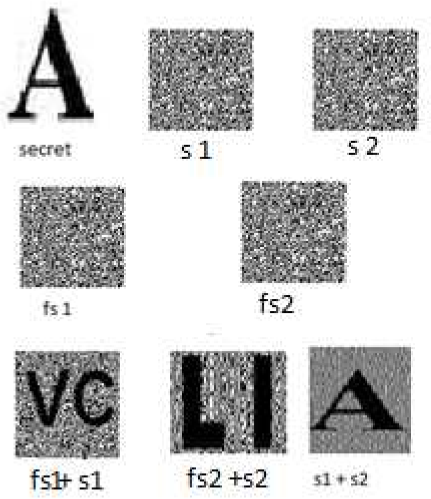

Fig. 10 Cheating a VC by an MO

As shown in the above Fig 10 the secret image is divided into shares s1 and s2 and the Malicious Outsiders create the fake shares fs1 and fs2 by overlapping the fs1 with s1 and fs2 with s2 we cannot get the secret but we get the different image.

3) Cheating an Extended Visual Cryptography Schemes (EVCS) by an Malicious Participant (MP)

The Malicious Participant(who have the original share and authorized to access the secret image and interested in cheating) have the one ('1') share out of 'k' numbers of shares so he/ she can easily access the information related to the share which he/ she have. So, he/ she can easily known the pixels place of their share. For the cheating of the Extended visual Cryptography Schemes he / she create the fake share from the original share by interchanging the position of the black pixel with the position of the white pixels. By the interchange of the pixels position to each other the reconstruct image have low contrast than the secret image, Resulting this it is difficult to recognize the image. The process is shown below in Fig 11

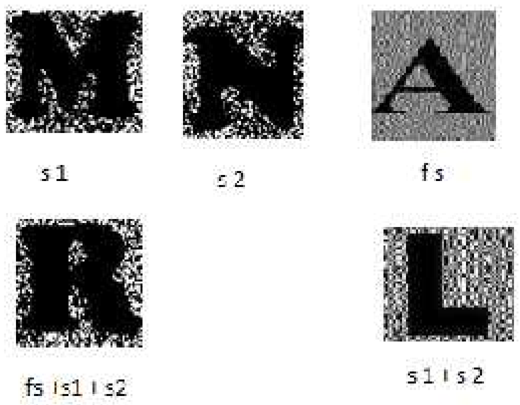

Fig. 11 Cheating an EVCS by an MP

VIII. CONCLUSION

In this paper we analysis the various of attacks on the visual cryptography. which are done by the Malicious Participant (MP) and Malicious Outsiders (MO). We also provide the methods that they use to cheat the visual cryptography. We also describe the concept of the fake shares that how they are build ? And how they are used to cheat the visual cryptography. With the help of the example figures we try to provide the process of each method.

References

❖ Naor and Shamir,"Visual cryptography", in Advance in Cryptology-Eurocrypt 94 [1]

❖ Qin, Wen-Fang Peng, Min Zhang, Yi-Ping Chu,"An (n,n) threshold Visual Cryptography Scheme for Cheating Prevention", IEEE 2010 [2]

❖ Zhi-hui Wang,Chin-Chen Chang, Huynh Ngoc Tu, Ming- Chu Li, "Sharing a Secret Image in Binary Image with Verification", Journal of Information Hiding and Multimedia Signal Processing, ISSN 2073-4212, Volume 2, Number 1, January 2011q[3]

❖ B.Padhmavathi, P. Nirmal Kumar, M.A Dorai Rangaswamy, "A Novel Scheme for Mutual Authentication and cheating Prevention In Visual Cryptography using Image Processing", ACEEE Int. J. On Signal & Image Processing, Vol. 01, No. 03. Dec 2010 [4]

❖ Chwei-Shyong Tsai, Hao-Cheng Wang, Hsien-Chu Wu and Chung-Ming Wang, "A Cheat-Preventing Visual Cryptography Scheme By Referring The Special Position", International Journal of Innovative Computing, Information and Control, Volume 7, Number7 (A), July 2011 [5]