A STUDY ON VARIOUS SECURITY METHODS IN VISUAL CRYPTOGRAPHY

[1]Ramya Arul Mary .G, [2]Sangeetha.N.
1 PG scholar M.E Computer Science and Engineering,
2 Assistant Professor M.E. Computer Science and Engineering
Alpha College Of Engineering, Chennai, India.
ramyaarulmary@gmail.com, sangeetha_na@yahoo.com

Abstract: **Visual Cryptography (VC) is an art of securing information that is kept as confidential proposed by Noar and Shamir. The creation of secret shares from the image or any information in the form of image which is called as the Visual Cryptographic shares (VC shares) is its basic concept. In today's scenario due to the rapid growth of internet and fast data transfer through internet securing the secret information is one of the challenging concepts. There is various security mechanisms developed to in order to bring protection in various fields of communication. Visual cryptography though a information securing concept has certain issues were security is violated. In this paper the study about various security issues in VC and the security mechanisms that is has been found in various researches are addressed in detail. The advantages and the disadvantages over the security mechanisms are analyzed in detail.**

Keywords: **Visual Cryptography, Visual Cryptographic Shares, security issues, security mechanisms.**

I. INTRODUCTION

The traditional secret sharing method is that in olden times the secret maps are torn into pieces and later bought together to obtain the secret back. In 1994, Noar and Shamir were the researchers who introduced the concept of Visual Cryptography (VC) based on the traditional secret sharing , were the information in the form image is been split up into shares by visual cryptographic techniques. The shares are been stacked together to produce the original information.

There are various security issues which makes the VC technique vulnerable to attackers. These issues may be due to internal or external attackers, the internal attackers may be the share holders who try to cheat internally and the external attackers would be the third person who requires the secret to be revealed.

A. Visual Cryptography

Visual Cryptography uses the transparency of images. One big advantage of the VC is that the decryption does not require any algorithm or mathematical computation. The information in the form of image that has to be secured is been spitted into shares by random pixel separation or the one time pad. The n shares can be generated and k shares are enough to obtain the information which we call as (k, n) share technique. The pixel in a black and white image has an equal number of black and white pixels. These pixels could be divided into any number of parts. The shares can be split vertically or in horizontal fashion.

The generated shares should be printed into the transparent sheets and to decrypt the original image the printed shares has to be stacked on top of the other, the original information is been obtained. Thus could protect the information from the attacker from knowing what is actually transformed. The following *fig1* shows how the visual cryptographic shares are created and how the shares are been stacked on after the other to produce the original image without a decryption algorithm or computation.

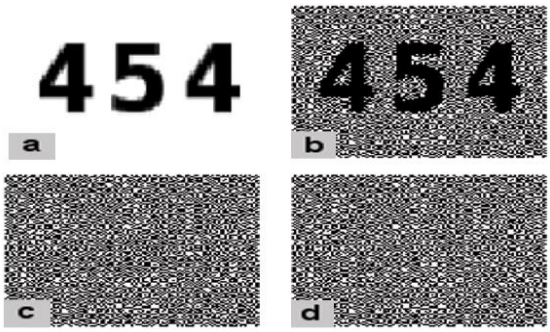

Fig1: Example of Visual Cryptography

B. Visual Steganography

The art of hiding text or image into the cover image or text is called as *Steganography*. The Steganography is performed by making use of algorithm and encryption techniques. Visual Steganography is similar to this but except the advantages in the decryption part as said earlier. After the encryption of image or text into the cover medium, the decryption part becomes as simple as that, the UV light ray is been made to project over the encrypted cover. The image absorbs the light rays and the hidden data is been projected making the decryption easy.

C. Visual Watermarking

Watermarking is a pattern or image that appears behind an image or text for confidentiality purpose. These kinds of marks could be transparent or visible through naked eyes. Visual Watermarking is that the watermarked image is been used to generate the shares and the decryption is same as the above.

II. TYPES OF VC SCHEMES

A. Visual cryptography for gray level images

The binary images were not used for real time applications. Chang-Choulin proposed VC for *gray level images* by ***dithering techniques***. Dithering method is used to convert the gray pixels into the binary form. Then the usual method is used to construct the shares. The effect of this scheme works well even if the image size is increased.

B. Visual cryptography for general access structures

In (k, n) model, k shares was found to be enough for reconstructing the original image from the shares; this leads the work of decryption easy for the attackers. To overcome this issue the general access structure is been proposed by G.Ateniese and C.Blundo. In this method there is an access structure specification made to the qualified shares. When the less qualified shares or disqualified shares are stacked the information cannot be retrieved.

C. Halftone visual cryptography

Zhi Zhou and Giovanni Di Cresenze proposed the halftone visual cryptography which enhances the quality of the shares. Here there is a secret binary pixel ‘p’ is been included into the each of the ‘n’ shares which is called as the halftone cells which increases the security.

D. Recursive threshold visual cryptography

Each generated shares consists of 1/k bits of shares. Abishak Parakh and Subhaskak proposed this method in such a way of eliminating the problem of hiding no of bits in per share. When there is much increased number of bits per share it would reduce the network traffic and reduces the load.

E. Visual cryptography for color images

The visual cryptography will reduce the quality of the image which also results the same in the color images. To overcome this, three approaches was proposed. The first is to print the color into the shares. Second is that to covert the color image to black and white by three color (RGB). Thus the third is to encrypt the secret into the binary image.

F. Regional increment visual cryptography

The regional increment techniques provide added security for the shares. K shares are enough for the secret to be revealed in visual cryptography. This method provides multiple level of secrecy in a single image. The shares are further divided into sub shares and thus enhancing the security of the cryptographic shares.

G. Extended visual cryptography for natural images

Since the creation of shares is made by random pixels the shares pattern does not capture any meaningful information which leads to the suspicion of encrypted data. Thus the extended VC provides the pattern for natural images were the shares are generated with some meaningful information.

III. SECURITY IN VISUAL CRYPTOGRAPHY

There are some techniques that is developed to address the security issues of the VC shares and the information.

A. Hu-Tzeng Cheating Prevention Scheme (CPVSS).

The shares are said to be secure only when the probability of success is negligible. There are two approaches in the CPVSS scheme.

1. *Blind Authentication*: In this the property of the image is used for authentication. The properties such as contrast, brightness etc, are taken as the authentication. The integrity of the shares is been included.
2. *Shares Authentication*: In this the participant who holds the share are given two shares, one is the secret share the other is the verification share. This verification share is also used for the integrity purpose.

When there is a scenario were three participants are found to hold the shares (Alice, Bob, Cathy). The secret shares are been distributed among these three. Now Alice and Bob tries to cheat Cathy by making modifications in their shares, thus Cathy while reconstructed will not obtain the original information. This kind of cheating is addressed in this method.

Advantages: The main advantage of this method is that the integrity of the shares is been maintained. The additional share produced for verification is used for avoiding this cheating to be done in shares.

Disadvantage: The problem in this CPVSS method is that the creation of the verification shares needs to an additional work for the people. There might be a overhead in the additional shares.

B. Generic transformation for cheating prevention

In this method before addressing the prevention technique three cheating has been addressed two for the visual cryptography scheme (VCS) and one for extended visual cryptography (EVC).

1. Cheating a VCS by an MP

Malicious participant (MP) is the one who tries to cheat by using the genuine shares to construct the fake shares. After the construction of the fake shares which is found to be of the same template as that of the original shares. When these fake shares are stacked together there is fake image that is produced of perfect blackness.

2. Cheating a VCS by an MO

Malicious outsiders (MO) are the cheater who is found out of the participant, he could cheat the shares by not even having the original shares in hand. He constructs an optimal no of fake shares which produces a fake image while stacking the shares. The only difficult work of the MO is that he has to tune the size of the fake shares according to the original shares. If he gets even one of the genuine shares it would become even more possible for the cheater to tune the size of the fake shares.

3. Cheating an EVCS by an MP

In VC the main consideration is the contrast to be non-zero. Thus in EVCS the fake shares are used to reduce the contrast of the shares since the fake shares on stacking together gives a perfect blackness.

To avoid all of the cheating that is mentioned an efficient and roust cheat prevention method called the generic transformation. The cheating prevention techniques follow some properties,

i. The method does not rely on the on-line Trusted Authority (TA). Since decryption is easy in VC TA should not be used.
ii. The pixel expansion should be avoided to a certain extent.
iii. Since there is lot of possibility for the participant to become a cheater, each of the participants should verify each other's shares.
iv. The verification of each of the shares given to the participant should be different.
v. The shares when stacked should maintain the same contrast.
vi. The prevention method should be applicable for any of the VCS.

Advantages: The main advantage fount in the generic method is that the shares are been given special verification and thus the internal and the external attackers are avoided.
The approach is applicable for any type of VCS that is been carried out.
There is no compromise made in terms of the contrast or brightness of the image in any way.

Disadvantages: Though the cheat is reduced by finding the entire internal participant and the outsider's changes are addressed, the prevention of the shares from being cheated and is been lost during the transmission of the shares from source to destination is not addressed.

C. Enhanced security system in visual cryptography

Due to the development of the communication and internet it is very important to bring the concept of security. All the above techniques and the methods deals with the prevention of the VC shares from being altered or by changes made by the share holding participant and by the outsiders.

This enhanced security system deals with the concept of securing the shares when it is been transmitted from two stakeholders, through internet or any other communication medium. When there is a strong growth of communication there are intruders who are also increasing, in the intend of obtaining the secret that has been transferred through the net.

This mechanism deals with the Least Significant Bit (LSB) substitution technique which is one of the methods that is used for securing the secret information. The main idea is to secure the shares by encrypting the secret into the image before the creation of shares.

The secret information or the image that has to be secured is first encrypted into any cover medium, an image or text using the LSB substitution technique. Thus the output of the encryption is the encrypted image that holds the secret information.

Steps for LSB encryption,

i. First the cover image is converted into binary matrix form by splitting the pixels.
ii. The text or the image that is considered secret is covert to binary matrix.
iii. The matrix size is compared and the least bit of the cover image matrix is been substituted by the binary bits if the secret information.
iv. Thus the encrypted image is obtained.

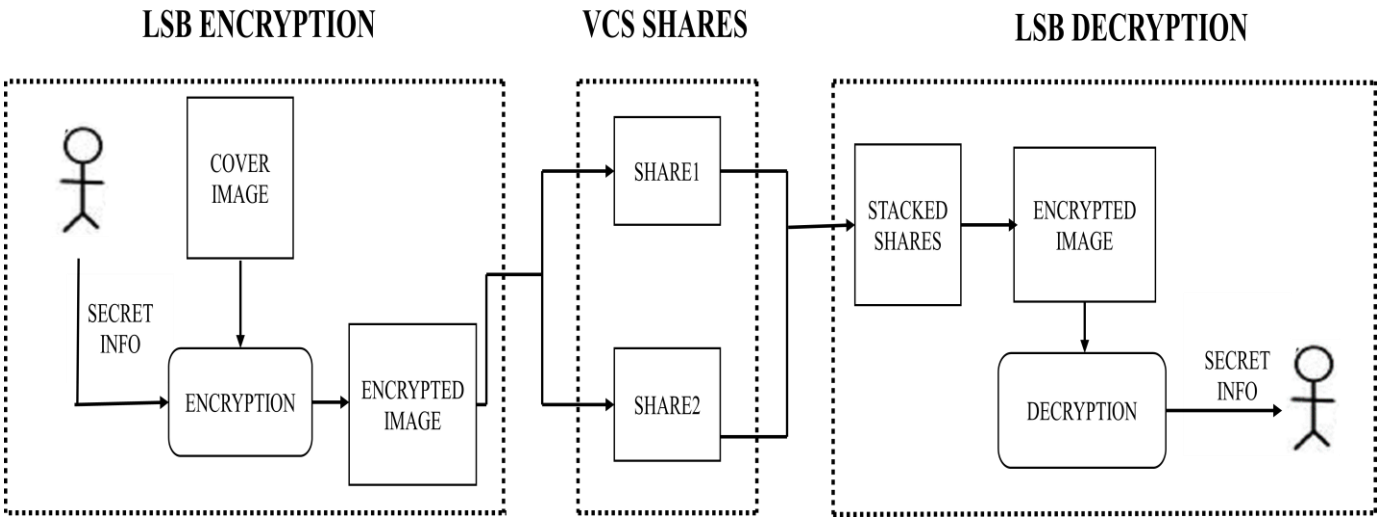

Fig2: LSB security system

After the encrypted image is obtained the shares are been created for the encrypted image by the VC technique. This enhances the security. This share of the encrypted image is transferred through the internet.

At the other end i.e. the destination receives the shares are stacked together by printing it into the transparent sheets. When the stacking process is completed the encrypted image is obtained back. Since the output of the stacking is encrypted form there is need for a decryption process to be carried out. The decryption part also involves LSB technique to be followed.

When there is an intruder who tends to obtain the information that is being passed to the other, he gets the shares. The intruder identifies that these are cryptographic shares by the nature of the share pattern or template. He then tries to stack the share that he obtained and gets the encrypted image and misunderstands that was the secret that has been shared. Thus this makes a strong point that the security is been enhanced.

Advantages: The big advantage of the enhanced security mechanism is that the shares are protected when it is been completely got into the hands of the attackers or the intruders.

It overcomes the disadvantages that were found in the cheating prevention technique, which is restricted only to the participants.

The encryption algorithm that is been used for the security gives an added prevention.

Disadvantages: The disadvantage here in this method is that the additional encryption and decryption becomes burden.

The VC decryption is made difficult by this method.

The shares may cause some difficulty in revealing the original image.

Stacking of the cryptographic shares may sometime not reveal the original image when the encryption process is not performed properly.

IV. CONCLUSION

Thus the study of various features and schemes of visual cryptography is discussed efficiently and the security issues were mentioned and addressed with the security mechanisms that overcome the issues of internal and external attacks of information. Since security is become a greatest task that has to be maintained in all the fields of communication , the various techniques which overcomes the disadvantages of visual cryptography is analyzed and the performance of all of those mechanism were discussed with its advantages and disadvantages.

REFERENCE

[1]. Yu-chi chen, "Comment on cheating prevention in visual cryptography", vol 21, July 2012.

[2]. C.Blundo, A.De Santis, "visual cryptography for gray level images", vol 75, Nov 2000.

[3]. R. lukac, K.N.Plataniotis, "Bit level based secret sharing for image encryption", vol 38, no5, May 2005.

[4]. A.Shamir, "How to share a secret", comm., ACM, vol 22, Nov 1979.

[5]. Chih – Ming Hu, Wen-Guey Tzeng, "Cheating prevention in visual cryptography", vol 16, Jan 2007.

[6]. G.Ateniese, C.Blundo, "Visual Cryptography for general access structures", vol 129, 1996.

[7]. Bin YU, Jin-Yuan YU, "A co-cheating prevention visual cryptography scheme",
International conference, 2010.

[8]. Ruchira Datta, "A novel approach towards LSB substituted data hiding in images", IJETAE, Vol 3, March 2013.

[9]. Chang.C.C, Tseng.H.W. "Data hiding in images by hybrid LSB substitution", international conference, 2009.

[10]. Neelima.Guntupalli, P.D.Ratna Raju, "An introduction to different types of visual cryptography schemes", vol 1, Sep 2011.

[11]. H.B. Kekre, Archana Athawale, "Increased capacity of information hiding in LSB's method for text and image", 2008.

[12]. Sabu M Thampi,"Information hiding techniques: A tutorial Review", LBSCE 2004.

[13]. Zhi-hui Wang, "Sharing a secret image in binary images with verification", ubiquitous international, vol 2, Jan 2011.

[14]. B.Surekha, Dr.G.N. Swamy, "A watermarking technique based on visual cryptography", Journal of information assurance and security, 2009.

[15]. Mihir Das, Jayanta Kumar Paul, "A simple Scheme for visual cryptography", issue of IJCCT, vol 1, Aug 2010.

[16]. Ming Sun Fu, "Joint Visual cryptography and watermarking", IEEE international conference of ICME, 2004.

[17]. Jaya, Siddhartha, "Novel authentication system using visual cryptography", world congress on international and communication, 2011.

[18]. E.F.Brickell, "The detection of cheaters in thresholds schemes", SIAM, 2003.