A Novel Scheme for Mutual Authentication and Cheating Prevention in Visual Cryptography using Image Processing

B.Padhmavathi¹, P.Nirmal Kumar², M.A.Dorai Rangaswamy³
¹Department of Computer Science & Engineering, Easwari Engineering College, Chennai – 600 089, Tamil Nadu, India
²padmas9169@yahoo.co.in
³drdorairs@yahoo.co.in

Abstract— Visual cryptography (VC) is a method of encrypting a secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are usually presented in transparencies. Each participant holds a transparency. In this paper, we studied the cheating problem in VC by malicious adversaries. We considered the attacks of malicious adversaries who may deviate from the scheme and create fake shares, whose stacking reveals a different Secret image. This paper proposes a solution to this Cheating problem by an Invisible and Blind Watermarking scheme. This scheme not only provides Authentication for the VC shares but also makes these secret shares invisible by embedding them into not so significant Host images. Thus secret shares are not available for any alterations by the adversaries who try to create fake shares. In the proposed invisible and blind watermarking scheme, every pixel of the binary VC share is invisibly embedded into the individual blocks of the host image sized 2x2. In this proposed scheme, the process of watermark extraction necessitates only the watermarked image and it doesn’t require the original host image or any of its characteristics, making the proposed scheme blind. The efficiency of the proposed Cheating prevention scheme by Invisible Blind watermarking scheme has been demonstrated via the experimental results. A Perfect restoration technique is added to the Visual Cryptography Scheme to improve the quality of the restored secret image as well as memory space utilization. Hence the proposed Cheating prevention scheme along with Perfect restoration techniques provides a Novel Visual Cryptography scheme.

Keywords - Visual Cryptography, Cheating Prevention, Invisible Watermarking, Blind Scheme, Secret shares, Host Images.

I. INTRODUCTION

Visual Cryptography (VC) is a method of encrypting a Secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are binary images usually presented in transparencies. Each participant holds a transparency (share). Unlike conventional cryptographic methods, VC needs no complicated computation for recovering the secret. The act of decryption is to simply stack shares and view the Secret image that appears on the stacked shares.

In these cases, all participants who hold shares are assumed to be honest i.e., they will not present false or fake shares during the phase of recovering the secret image. Thus, the image after stacking them is considered as the real Secret image. Nevertheless, cryptography is supposed to guarantee security even under the attack of malicious adversaries who may deviate from this scheme in any way. We have seen that it is possible to cheat [1], [2], [3] in VC, though it seems hard to imagine. For cheating, a malicious participant presents some fake shares such that the stacking of fake and genuine shares together reveals a different secret image making the genuine participants to believe it to be the original. It is observed that the participant shares are vulnerable for Cheating attacks. In this paper, we consider this problem and provide security to the participant shares by hiding them in some insignificant images. For example, Lena, Peppers etc.

Watermarking is the technique of embedding a secret image into a cover image without affecting its perceptual quality so that secret image can be revealed by some process. One significant advantage of watermarking is the inseparability of the watermark(secret image) from the cover image. Some of the vital characteristics of the watermark are: hard to perceive, resists ordinary distortions, endures malevolent attacks, carries numerous bits of information, capable of coexisting with other watermarks, and demands little computation to insert and extract Watermarks. Generally, robust watermarking is used to resist un-malicious or malicious attacks like scaling, cropping, lossy compression, and so forth. Watermarking techniques can be categorized into different types based on a number of ways. Watermarking can be divided into Non-blind, Semi-Blind and Blind schemes [4], [5] based on the requirements for watermark extraction or detection. Non-blind watermarking schemes necessitate the original image and secret keys for watermark detection. The Semi-Blind schemes require the secret key(s) and the watermark bit sequence for extraction, whereas, the Blind schemes need only the secret key(s) for extraction. Another categorization of watermarks based on the embedded data (watermark) is: visible and invisible. With visible watermarking of images, a secondary image (the watermark) is embedded in a
primary image in such that it is perceptible to a human observer, whereas the embedded data is not detectable in case of Invisible watermarking; nevertheless, it can be extracted by a computer program.

Here our proposed scheme will add the merits of both visual cryptography as well as Invisible and Blind watermarking techniques, where we will generate the secret shares using basic visual cryptography model and then we will watermark these shares into some host image using invisible and blind watermarking. Thus the secret shares are protected from cheating attacks. The decryption will be same as in the visual cryptographic model i.e. by stacking of the shares after the secret shares have been extracted by a simple watermark extraction technique. The proposed watermarking scheme doesn’t necessitate the original image or any of its characteristics for the extraction of watermark, and hence the proposed scheme is blind. The experimental results have been demonstrated for efficiency of the proposed Invisible and Blind Watermarking scheme for Binary images in [6],[7].

The rest of this paper is organized as follows. The models for Visual Cryptography scheme (VCS), Cheating behaviors in VC and Digital watermarking for the protection of digital images are discussed along with brief review of their previous works in Section 2. We then describe the proposed Innovative Invisible and Blind Watermarking scheme for Cheating prevention in Section 3. The experimental results are provided in Section 4 and conclusions are summed up in Section 5.

II. REVIEW OF RELATED TOPICS

A. (2,2) Visual Cryptography Scheme

Visual Cryptography (VC) was first introduced by Moni Noar and Shamir at Eurocrypt’94 [8]. It involved breaking up the image into n shares so that only someone with all n shares could decrypt the image by overlaying each of the shares over each other. To encode a secret employing a (2, 2) VC Scheme, the original image is divided into two shares such that each pixel in the original image is replaced with a non-overlapping block of two or four sub-pixels as shown in Fig.1.

![Fig 1. A (2,2) Visual Cryptography scheme](image)

Fig 1. A (2,2) Visual Cryptography scheme

Anyone who holds only one share will not be able to reveal any information about the secret. To decode the image, each of these shares is Xeroxed onto a transparency. Stacking both these transparencies will permit visual recovery of the secret.

There are several schemes of encoding the pixels of the secret image. In our scheme, each pixel in the secret image is broken into four sub pixels. A white pixel is shared into two identical blocks of four sub-pixels. A black pixel is shared into two complementary blocks of four sub-pixels. Fig. 2 illustrates this scheme of encoding one pixel into four pixels in a (2, 2) VC scheme. All the pixels in the original image are encrypted similarly using this scheme. These shares can be either Vertical or Horizontal or Diagonal Share as shown in the figure.

![Vertical Shares, Horizontal Shares, Diagonal Shares](image)

Fig 2. Pixel encoding in (2,2) Visual Cryptography scheme

B. Cheating Behaviour in Visual Cryptography

A cheating process against a VCS [9] consists of the following two phases:

1) Fake Share Construction Phase, where the cheater participant generates the fake shares.

2) Image Reconstruction Phase, where the Fake image appears after stacking the genuine shares with fake shares.

In the case of cheating, honest participants who present their shares for recovering the secret image are not able to distinguish fake shares from genuine shares. A reconstructed image is a perfect image indistinguishable from the original. The key point of cheating is how to predict and rearrange the positions of black and white sub pixels in the victim’s and cheater’s share. Fig. 3 shows the whole cheating process and Table 1 shows how the cheaters create fake shares to change the decoded image.

![Fig 3. Cheating Process in VCS](image)

**TABLE I**

<table>
<thead>
<tr>
<th>FAKE SHARE PIXEL CREATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>------------------------</td>
</tr>
<tr>
<td>white</td>
</tr>
<tr>
<td>white</td>
</tr>
<tr>
<td>black</td>
</tr>
<tr>
<td>black</td>
</tr>
</tbody>
</table>
C. Digital Watermarking

Our work has been motivated by a copious number of earlier works available in the literature that utilize digital image watermarking for protecting copyrights of digital images. Debasish Jena Sanjay Kumar has proposed Data hiding in halftone images using conjugate ordered dithering (DHCOD) algorithm is given, which is a modified version of existing Data hiding in halftone image by conjugate error diffusion (DHCED) algorithm. Lu et al. [10] have presented a digital watermarking technique that is intended to solve some vital issues of the digital world, such as copyright protection, copy protection, and image authentication. Wei-Che Chen [11] have presented a digital image copyright protection scheme on the basis of visual cryptography (VC) and singular value decomposition (SVD) techniques. Initially, the scheme applies SVD to a host image to construct a master share. This scheme embeds the secret image without affecting any modification of the host image. All the above mentioned schemes provide copyright protection to the VC Secret image but where as VC secret shares are still vulnerable to the Cheating attacks. In this research, we propose an innovative Invisible and Blind watermarking scheme [6], applied to VC shares to secure them against Cheating attacks by the adversaries.

III. PROPOSED MUTUAL AUTHENTICATION AND CHEATING PREVENTION SCHEME USING INVISIBLE BLIND WATERMARKING

This section presents the proposed Invisible and blind watermarking Algorithm for the protection of Secret shares in VC. The proposed scheme utilizes the binary VC secret share image as watermark data. With the aid of the embedding strength and signum function, the scheme discussed, embeds this binary watermark image pixel into every 2x2 non-overlapping block of some insignificant host images. This process protects the VC secret shares from any adversary manipulations, which may result in fake shares. Also, during extraction, the embedded binary watermark is extracted from the watermarked host image using watermark image size and the embedding strength. As this digital watermarking scheme doesn’t require the original image or any of its characteristics for watermark extraction, it is said to be blind. The VC Secret shares are completely hidden from malicious users. Hence it is proved that above stated Cheating behaviour in VC is prevented by this novel watermarking algorithm. In our paper, we have chosen the user’s signature images for VC encryption phase and this provides mutual authentication during any transaction at the VC Decryption phase. The following subsections describe the steps involved in the watermark embedding and extraction processes and also various phases of the entire scheme.

A. Watermark Embedding

This sub-section presents the process of binary VC secret share image embedment into the host image. The size of the host image chosen is dyadic (2nx2n) and the watermark used is a binary image. Firstly, non-overlapping blocks sized 2x2 are extracted from the host image and every pixel of the watermark VC share image is embedded into a single block of the host image. The watermark embedding process involves: mean calculation, embedding strength (β) and signum function. Each non-overlapping block is converted into a vector, and the mean value of the vector is computed and divided with the embedding strength (β) Since, the watermark is a binary image; the process of watermark embedding involves two cases: embedding pixel value ‘1’ and embedding pixel value ‘0’. Two different inserting mathematical operations are carried out for embedding pixel value ‘0’ and ‘1’.

B. Watermark Extraction

This sub-section details the steps involved in the extraction of the binary watermark image from the watermarked image. As the proposed scheme is blind, watermark extraction necessitates the watermarked image, size of watermark image and the embedding strength, whereas it doesn’t require the host image or any of its characteristics. Initially, non-overlapping blocks sized 2x2 are extracted from the watermarked image and the number of blocks extracted varies based on the size of the watermark image. The blocks that are extracted are stored in a vector. Subsequently, all the extracted blocks are converted into a vector and the mean value of the vector is computed. Afterwards, the mean values of all the blocks are divided by the embedding strength (β). The resultant value is made use of in the extraction of watermark. Finally, a matrix of the size of the watermark image is created and the extracted pixel values are placed in it so as to obtain the watermark image.

C. Phases of the Proposed Scheme

In the proposed scheme we shall generate the VC-shares using basic visual cryptography model and then embed them into a cover image using an Invisible Blind Watermarking technique, so that the secret shares will be more secure and meaningful. And the shares are protected from the malicious adversaries who may alter the bit sequences to create the Fake shares. During the Decryption phase, the secret shares are extracted from their cover images without needing any of the cover image characteristics to provide mutual authentication.

Proposed scheme consists of three phases which are described in the following subsections.

Phase I – Visual Cryptographic Encryption: In this very first phase we will do visual cryptography encryption. It consists of generation of shares using any basic visual cryptography model. Visual cryptographic solutions operate on binary inputs. In our proposed scheme, a (2,2)VC share creation is performed. During encoding due to Pixel expansion the size of the shares will be large. Since each pixel in the original image is replaced by four sub-pixels in each share, the width of the decoded image is more than twice that of the original image. But after applying the Perfect Restoration techniques [12], the original size of the secret image can be restored. So the result of this phase will be 2 unintelligible shares of black and white pixels. In real time applications share 1 will available with Client and share 2 will be saved in the Server database for future authentication purposes. Fig. 4
shows the result of Share 1 creation with perfect restoration technique applied.

Fig 4. Share 1 creation using (2,2) VC Encryption

Phase II - Hiding the Shares using invisible blind watermarking: This is the second phase of our approach which will embed shares of the client and server, generated from the first phase into some host images. For watermarking we will use Invisible and Blind Watermarking scheme discussed under section 3. Use of watermarking will give an added advantage of double security over other visual cryptographic schemes. The watermarked host images are robust against various attacks like Blurring, Cropping, Sharpening, JPEG Lossy compression. This forbids any malicious participant to access the secret shares and modify them into Fake shares thus preventing Cheating problem in VC. The result of this phase would be innocent looking watermarked host images that do not seem to contain any secret in them because of the invisible watermarking methodology applied. The watermarked host image 1 and 2 will be available with the client and server databases.

Phase III - Visual Cryptographic Decryption and Authentication: This is the last phase of proposed scheme. In this phase we extract the binary watermarked shares from the host images of the client and server. The proposed watermarking scheme doesn’t necessitate the original image or any of its characteristics for the extraction of watermark, and hence the proposed scheme is blind. Then we apply the visual cryptographic decryption. As we know that visual Cryptographic decryption does not need any type of decryption algorithm or computation. It uses human visual system for decryption which is the core advantage for which visual cryptography was developed. Now we can decrypt the original secret image by overlapping or stacking the shares. When the two shares are stacked together, the black pixels in the original image remain black and the white pixels become grey. Although some contrast loss occurs, the decoded image can be clearly identified. Now again the perfect restoration technique is used to remove the greying effect to give more contrast. Hence the result of this phase will be an image consisting original secret image. Fig 5 is the structure of proposed scheme.

IV. SIMULATION RESULTS

For simulation we have used MATLAB 7.0 tool and tested with images of different sizes. The proposed scheme achieves effective embedment of the binary share images into the host images. Also, the proposed scheme depicts efficient extraction of the embedded watermarks from the watermarked images. The watermarked images possess good Peak Signal to Noise Ratio (PSNR) and good visual quality. Fig. 6 depicts the results obtained on experimentation of the entire proposed Visual Cryptography scheme.

The results include original secret image, encoded secret shares, host image, watermarked images and the decoded secret image. Thus the encoded secret shares have been authenticated to prevent Cheating attacks.
Fig. 6. Experimentation Results

V. CONCLUSION

Visual cryptography is the current area of research where lot of scope exists. Currently this particular cryptographic technique is being used by several countries for secretly transfer of hand written documents, financial documents, text images, internet voting etc. There are various innovative ideas and extensions exist for the basic visual cryptographic model introduced till now. One such enhancement we are trying to do in terms of preventing cheating attacks. In the existing VC schemes no security is provided to the secret shares and adversaries can alter its bit sequences to create fake shares. And in our proposed scheme, the vulnerability of these binary secret shares is overcome by hiding them invisibly into some host images. During the decryption phase, the secret shares are extracted from their cover images without needing any of the cover image characteristics because the watermark extraction technique is blind. The overlapping of these shares reveal the original secret. The decoded secret signature image quality is improved by using perfect restoration technique. Yet many possible enhancements and extensions can be made to improve further.

REFERENCES