An Efficient Interception Mechanism Against Cheating In Visual Cryptography With Non Pixel Expansion Of Images

Linju P.S, Sophiya Mathews

Abstract: Visual cryptography is a technique of cryptography in which secret images are divided into multiple shares and are distributed to different entities. Each secret can be reconstructed by superimposing these shares using different operations. Common traditional drawbacks of all existing methods are pixel expansion and noise at output. Another major issues that can occur in existing visual cryptography systems are Cheating between share holders and Share holders cheating owner. In order to overcome these limitations, sealing algorithm is used with two applications of VC such as MIVC and EVC. Here two secret images can be send at the same time by converting them to halftone representations which in turn are partitioned as three shares in total.

Index Terms: Cheating, Cover image, Halftone image, Pixel expansion, Sealing

1. Introduction

Visual cryptography is simply a secret sharing technique or cryptographic technique which allows the encryption of an image without requiring any complex computations or knowledge of cryptography. In this, secret images are divided into multiple share images and are distributed to different entities. The technique was initially proposed in 1994 by Naor and Shamir. Visual Cryptography uses two transparent images in which one image contains random pixels and the other image contains the secret information. It is hopeless to retrieve the secret information from one of the images and both transparent images or layers are needed to reveal the information. Because, here decryption is performed by overlaying the share images. When all shares are imbricate together, the original image would appear. Figure 1 shows the basic model of visual cryptography. Biometrics is an important security application of visual cryptography systems in which a person's authentication information is generated by digitizing measurements of a physiological or behavioral characteristic. Biometric informations such as facial, fingerprint, and signature images can be kept secret by dividing into share images, which can be distributed for safety to a number of entities. After the different entities releasing their shares, the secret can be recovered by overlaying these shares. This work proposed a novel method of visual cryptography for solving common drawbacks and traditional drawbacks of VC which includes loss of contrast, pixel expansion, cheating between share holders and cheating to the image content owner. Here, two secret images are divided into three shares and therefore three cover images are sealed into these shares for increased security. In addition, a pin or password can be entered before the share creation and this should be identified correctly at the time of imbrications of the shares. Then only the secret images will be revealed to the user.

- *Linju P.S is currently pursuing masters degree program in computer science and engineering, Kerala, E-mail: linjups@gmail.com*
- *Sophiya Mathews is currently working as assistant professor in computer science and engineering, Kerala,*

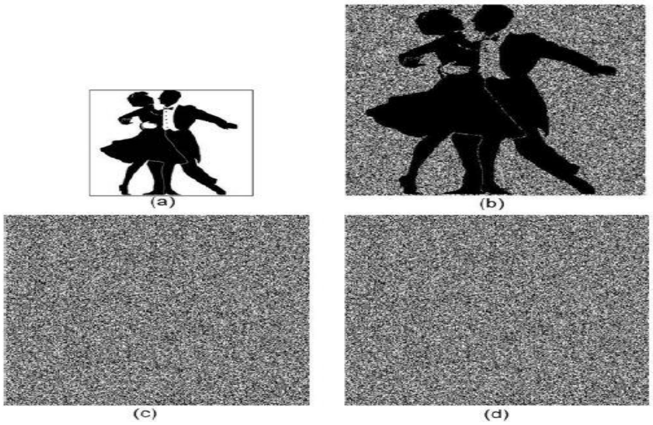

Figure 1: *Basic model of Visual Cryptography*

2. Scope and Objectives

The main objective of the research presented here is to derive and test secure visual cryptography scheme for application with halftone images, where the visual cryptography scheme do not require more pixels in the share images and recovered images than in the original secret images. Therefore preserve better image quality for the recovered images. The inference of non pixel expansion of recovered secret was proposed with the following objectives.

- ➢ To get better visual quality for secret images.
- ➢ To obtain same number of pixels in the recovered images as in the original secret images.
- ➢ A novel method with an efficient cheating prevention mechanism for secure transmission of secrets.

3. RELATED WORKS

A basic (2, 2) visual cryptography scheme produces two share images from an original image and must stack both the shares to reproduce original image. Generally, a (k, n) scheme produces n shares, but only k shares needs combining to regenerate the secret image. To preserve the aspect ratio for the recovered secret image for a 2 out of 2 scheme, each pixel present in the original image could be replaced in the share images by a 2 out of 2 block of sub pixels. The original secret image will be revealed after stacking the shares with white transparent and black opaque, Stacking can be viewed as mathematically XORing, where white is equivalent to 0 and black is equivalent to 1. The resulting share images and the recovered secret image hence contain four times as many pixels as in the original image. It may also be noted that the recovered image has a degradation in their quality in vision since a recovered white pixel is comprises of 2 white as well as 2 black subpixels, whereas a black pixel is represented by 4 black subpixels in the recovered image. To support grayscale images and color images, many studies have been done on applying visual cryptography [1][8], while some researchers have focused on image size expansion and contrast degradation. Nazanin askari et al. [4] introduced a visual secret sharing scheme which prevented size expansion by a novel method. They represent each pixel in the secret image as a black or white pixel in the share images and the secret image can be revealed by stacking the shares together. Yang et al. proposed a similar probabilistic method called ProbVSS for binary and grayscale images in 2004. Hsien-Chu Wu and Hao Cheng Wang proposed paper titled Color Visual Cryptography Scheme Using Meaningful Shares[8] in the year of 2008. This proposed scheme comprises of four main procedures. The first procedure is halftone transformation of color image, where the color image is converted into a color halftone image. The second procedure is focused on pixel extraction process where the pixels are extracted from the color halftone image. Then follows the encoding and decoding procedures, respectively. Two coding tables referred in the encoding procedure: secret coding table (SCT) and cover coding table (CCT). Pallavi V. Chavan and Dr. Mohammad Atique proposed paper titled Design of Hierarchical Visual Cryptography [5] in the year 2012. This paper describes the concept of hierarchical visual cryptography. The key idea behind hierarchical visual cryptography is to encrypt the secret information in number of levels. As the number of levels in hierarchical visual cryptography increases, the secrecy of data tends to increase. An intelligent authentication system is also proposed using hierarchical visual cryptography. The shares generated out of Hierarchical visual cryptography are found to be random giving no information. The expansion ratio is also reduced to 1:2 from 1:4. The paper on Novel Visual Cryptography Schemes Without Pixel Expansion for Halftone Images [1] was proposed by Nazanin Askari et.al in the year 2014. VC is a secret sharing scheme which uses the images which are distributed as shares and acts in such a way that when the shares are stacked, a secret image which is hidden is revealed. While VC was developed for application to binary images, it can also be applied to gray scale images through their halftone representations. This paper illustrates a new method for processing halftone images that increases the quality of recovered secret images in a Visual Cryptography scheme.

4. PROPOSED METHOD

In the proposed system, two secret color images are used which can be divided into three shares in total. Initially, these secret images should be changed into its halftoned representations. Then an improved preprocessing phase uses the simple block replacement method and the halftoned images are preprocessed using SBR technique. Hence these are converted into preprocessed images. Since the images are color images, both preprocessing as well as halftoning must be performed in 3 planes R, G and B. Once these processes are completed, 3 shares are generated. At this stage, the system request for 3 cover images. These requests are met by shareholders by providing the cover images and hence embedded cover image share is obtained. The shares obtained are superimposed by using a particular way to obtain the final secret image. This output overcome the common limitations like loss of image clarity as well as pixel expansion. Along with this, the system also provides a cheating prevention mechanism which can prevents both cheating between share participants and cheating to the image content owner. The proposed work has 4 modules:

1. Preprocessing Phase
2. MIVC Share Construction
3. Cheating Prevention Phase
4. Secret Recovery

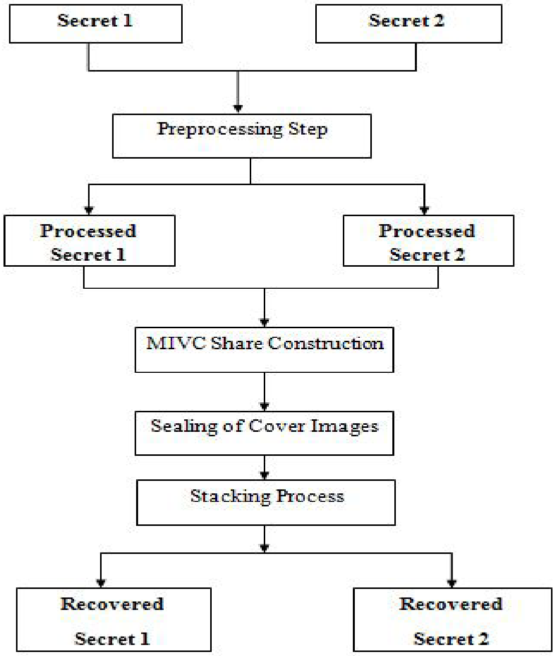

Figure 2: *Flow chart for proposed scheme*

4.1. Preprocessing Phase

Preprocessing is the initial module of this work. In this module, consider the application of visual cryptography to color images by first converting the images to binary images using a halftoning algorithm. After the creation of a halftone image, a simple method is applied to preprocessing the binary halftone image. This secure method that is easy to implement is based on a block wise approach and hence it is known as simple block rearrangement method. This can preserve the image size when applying visual cryptography in multiple image visual cryptography and extended visual cryptography. From the halftone secret image, the block replacement scheme considers a 2x2 block which is a group of four pixels. This is referred to as a secret block. Then generates the share images through block by block approach instead of pixel by pixel approach. Here, size of the reconstructed image is the same as the original secret image after superimposing the two shares together. Because, each secret blocks of four pixels encodes into two secret share images in which each containing four pixels. Before visual cryptography encoding, all the secret blocks in an image need to be processed. Each secret block is replaced by the corresponding predetermined blocks, which is a block with 4 white pixels (considered as a white block) or a block with 4 black pixels (considered as a black block). This replacement process of block in the Simple block rearrangement preprocessing scheme is based on the number of white and black pixels in each secret block. If the number of black pixels in the secret block is greater than or equal to 2, the secret block is converted to a black block. similarly if the number of pixels in black in a secret block is less than or equal to 1, those are converted to a white block. This step generates a new secret image which contains only white and black blocks. The output image which has been obtained from this step is referred to as processed secret image. The processed secret image now can be used as a secret image in VC schemes, such as traditional visual cryptography, multiple image visual cryptography, and extended visual cryptography. The Simple block rearrangement approach is clear and is very effective for unprocessed binary secret images, which has large numbers of all white and all black blocks. Therefore, the resultant processed recovered image is visually closer in quality to the original secret image. Among the three shares, Combining share 1 and share 2 generate secret 1 image. Then secret image 2 is revealed by rotating blocks of pixels in share1 and combining the same with share 3.

4.2. MIVC Share Construction

Here, two secret images are masked simultaneously by using a rotation technique where binary images are divided into two random independent shares, in accordance with the encoding process. The first secret image becomes visible by superimposing the first and second shares and the second secret image is revealed by rotating the blocks of 4 sub pixels of the first share, individually, counterclockwise by , where is 90^0; 180^0; or 270^0; and stacking this block-rotated version with the second share. When the images are provided to the system after verifying that the same are error free, the images are merged based on white and black pixel combination to reconstruct the final images. This visual cryptography system does not need any complex decryption algorithm as we can very easily attain the secret images by combining the shares.

4.3. Cheating Prevention Phase

An efficient interception mechanism against cheating in visual secret sharing scheme is the sealing of cover images on shares of secret images. When the shares are created, the owner(dealer) asks a cover image from each shareholder and are embedded in the shares at the time of creation. So each share holder does not have any information of the cover image which they have shared with the owner. So even if a share holder succeeded in creating the shares of other share holder, he will not be able to stack or superimpose the two shares since he does not have any information of the cover image (which has been embedded in the share) used by the other share holder at the time of share creation. That is, it depends on share authentication without the added transparencies. This scheme is developed with the properties of share authentication for white pixels and blind authentication for black pixels. The proposed scheme does not depend on the verification transparencies. The main idea of this scheme is that a variable message decided by a participant P_i is inserted into the stacking result of $T_i + T_j$ ($i \neq j$); however, the verifiable message does not in influence the secret, and P_i can check whether T_j is fake or not from the stacking result of $T_i + T_j$. In addition to this, here the owner will create a pin at the time of creating shares. And this pin is needed to superimpose the shares. So the shareholders cannot superimpose the shares without the owners consent. Only and only if the pin is entered, the share holders can superimpose the images. Hence the share holders cannot cheat owners. Below shows the flowchart of the method.

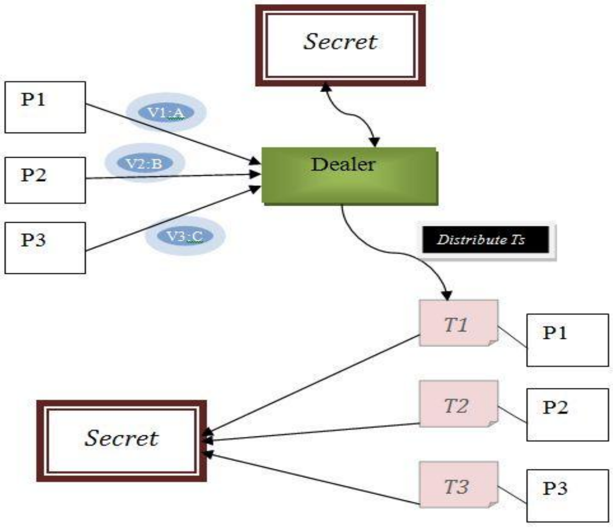

Figure 3: *Flow chart for cheating prevention scheme*

4.4. Secret Recovery Phase

when the images are provided to the system after verifying that the same are error free, the images are merged based on white and black pixel combination to reconstruct the final images. This visual cryptography system does not need any complex decryption algorithm as we can very easily attain the secret images by combining the shares.

5. RESULTS AND DISCUSSIONS

When compared to past visual cryptography methods, the proposed work provides better results with increase in the quality of recovered secret images. Various parameters like security, pixel expansion, accuracy and computational complexity are recommended by researchers as a performance measures to evaluate the performance of visual cryptography schemes. Here, the quality of the reconstructed secret image is considered based on its accuracy and are evaluated by peak signal-to-noise ratio (PSNR) measure. The output image is visually much closer to the original one and the PSNR gain of this method is larger. The performance of the system can be mainly analyzed using three parameters.

- Peak-Signal to Noise Ratio (PSNR)
- Mean Square Error (MSE)
- Number of pixels in output images with respect to the original secret images

Performances of the recovered secret images are analyzed with various inputs. Test is conducted using many secret images which are shown in figure 4.

Figure 4: *Test Images*

PSNR measure is an estimation of reconstructed image quality compared with original image. A higher PSNR value implies that the reconstructed secret image has higher quality. The PSNR values of the reconstructed secret images with respect to the original secret images are computed. These values indicates that the output secret images are similar to the original secret images. PSNR is defined by using the below equation.

PSNR = 10log (S^2/MSE) ------------- (1)

Where S = 255 for an 8-bit image. MSE is the Mean Square Error. MSE is computed by averaging the squared intensity of the original secret image and the recovered secret image pixels. The below table illustrates the PSNR value of recovered secret images of both proposed and old method. As shown in table 1, the PSNR value of proposed method has higher value when compared with the previous method. Hence the visual clarity of recovered secret image is much more in proposed method than previous method.

Secret Images	PSNR of Proposed Method	PSNR of Previous Method
Parrot	32.36	6.85
Horse	30.51	7.17
Lena	28.83	6.76
Baboon	22.74	6.77
Balls	30.60	4.78
Girl	26.69	4.18

Table 1: *PSNR Values of Proposed and Previous Methods*

Graphical representation of figure 5 shows different values of both method with the same images.

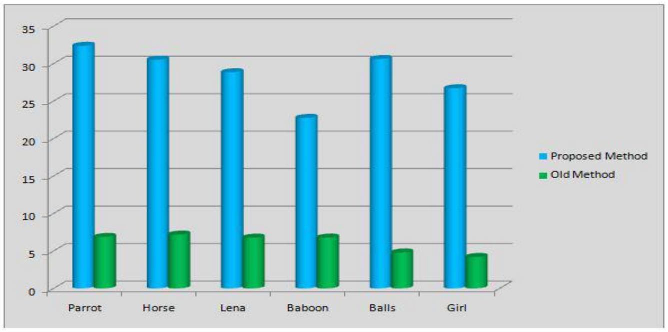

Figure 5: *Plot of Proposed Method PSNR Versus Previous Method PSNR*

Table 2 illustrates a simple comparison of visual cryptography schemes on the basis of number of secret images, pixel expansion, image format, type of share generated.

Sl. No	Authors	Year	No.ofSecrets	Format	Pixel Expansion	Share Format
1.	Moni Naor and Shamir	1995	1	Binary	4	Random
2.	Z. Zhou	2006	1	Binary	4	Meaningful Shares
3.	Hsien Chu Wu & Hao Cheng Wang	2008	1	Color	2	Meaningful Shares
4.	Pallavi V. Chavan & Dr. Mohammad Atique	2012	1	Binary	2	Random Shares
5.	Young-Chang Hou & Shih-Chieh Wei	2013	1	Color		Meaningful Shares

Table 2: *Comparison of previous visual cryptography schemes*

Different features in proposed method is shown in below:

Sl. No	Method	Year	No. of Secrets	Format	Pixel Expansion	Share Format
1.	Proposed Method	2015	2	Color	No	Meaningful Shares

Table 3: *Comparison of previous visual cryptography schemes*

From the above two tables, we can arrive at the conclusion that the features in proposed method is better than all other visual cryptography schemes. In addition to all above advantages of the proposed system, it acts as an efficient interception mechanism against cheating visual cryptography. Also the proposed system works better in both cheating methods (cheating to the owner, cheating between share holders) than any other methods by using a secret key and different cover images while creating share images. Hence this system is the best when compared to all other system currently available.

6. CONCLUSION

Due to the different security problems while sharing secret images visual cryptography has become an important area of research. Visual cryptography is a an efficient secret sharing scheme which partitions the secret into number of encrypted images or shares for increased security. Each secret can be reconstructed by superimposing these shares using different operations. This work proposed a novel visual cryptographic method which can use two secret colour images that can be divided into three shares in total. Combining share 1 and share 2 generate secret image 1. Secret image 2 is revealed by rotating blocks of pixels in share 1 and combining the same with share 3. In order to implement cheating prevention, the system request for 3 cover images. These requests are met by shareholders by providing the cover images and hence embedded cover image share is obtained. The shares obtained are superimposed to obtain the final secret image.

From the point of view of cheating in VC, this approach successfully solves the open questions. The experimental results also show that, this approach has better performances than previous researches. Because, output images overcome the common limitations like loss of image clarity as well as pixel expansion by maintaining the same aspect ratio as that of the original images.

ACKNOWLEDGMENT

I express my sincere thanks to all respected personalities who had guided, inspired and helped me in the successful completion of this paper. I express my thanks to The Lord Almighty for guiding me in this endeavor and making it a success. I am extremely grateful to all lectures, Department of Computer Science & Engineering, CKC, Ernakulam, for the inspiring and sincere guidance.

REFERENCES

[1] Nazanin Askari, Howard M. Heys, Member, IEEE, and Cecilia R. Moloney, Member, IEEE \Novel Visual Cryptography Schemes Without Pixel Expansion for Halftone Images" IEEE Trans. 2014

[2] Xiaotian Wu and Wei Sun, \Extended Capabilities for XOR-Based Visual Cryptography" in IEEE, 2014.

[3] Young-Chang Hou, Shih-Chieh Wei and Chia-Yin Lin\Random-Grid-Based Visual Cryptography Schemes" in the year 2013 in IEEE, 2013

[4] N. Askari, C. Moloney, and H. M. Heys, \A novel visual secret sharing scheme without image size expansion" in Proc. 25th IEEE Canadian Conf. Electr. Comput. Eng. (CCECE), Montreal, QC, Canada, May 2012, pp. 14.

[5] Pallavi V. Chavan and Dr. Mohammad Atique, \Design of Hierarchical Visual Cryptograpghy" in IEEE, 2012.

[6] Nitty Sarah Alex and L. Jani Anbarasi, \Enhanced Image Secret Sharing via Error Di_usion in Halftone Visual Cryptography" in IEEE 2011.

[7] A. Ross and A. A. Othman, \Visual cryptography for biometric privacy" IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 7081, Mar. 2011.

[8] Hsien-Chu Wu, Hao-Cheng \Color Visual Cryptography Scheme Using Meaningful Shares" IEEE, 2008.

[9] Z. Zhou, G. R. Arce, and G. D. Crescenzo, \Halftone visual cryptography" IEEE Trans. Image Process., vol. 15, no. 8, pp. 24412453, Aug. 2006.

[10] M. Naor and A. Shamir, \Visual cryptography" in EUROCRYPT94 (Lecture Notes in Computer Science), vol. 950. Berlin, Germany: Springer-Verlag, 1995, pp. 112.