Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Contrast Enhancement in Color Extended Visual Cryptography

**Alkha Mohan*, Jayakrishnan A**
Department of Computer Science College of Engineering,
Karunagappally, Kerala, India

***Abstract— Visual cryptography is a secret sharing technique mainly used for image sharing. In the case of extended visual cryptography we use meaningful shares to hide image. Contrast loss in decrypted image is a major problem. Here we use Additional basis matrix and perfect white pixel reconstruction to improve the contrast in color extended visual cryptography.***

***Keywords— Visual Cryptography (VC), Halftoning, Error diffusion, Secret sharing, Pixel expansion***

## I. INTRODUCTION

Cryptography means hiding information or secret writing. It becomes a sufficient tool to maintain information secret in widespread internet. For this information are changes to secret format called encrypted data. Only the legitimate user can retrieve the data from encrypted data. This method is called decryption. In modern cryptography there are 2 types of encryption algorithms; symmetric key and public key encryption. But key management is the main issue of these novel methods. Secret sharing improves the reliability and robustness of key management system. Here key is divided into number of pieces and distribute through users. Pre-determined set users can recover the key jointly.

Based on the idea of secret sharing, Naor and Shamir introduce visual cryptography. It called visual cryptography because here the decrypting module is human visual system (HVS). The idea of the visual cryptography model is to split a secret image into two random shares (printed on transparencies) which separately reveals no information about the secret image other than the size of the secret image. The secret image can be reconstructed by stacking the two shares. The underlying operation of this scheme is logical operation OR. An example of traditional (2, 2) visual cryptography is shown in Fig. 1. In Fig. 1 shares (a) and (b) are kept with each user, when they are stacking together will give the secret image. Each of them cannot get any information individually. In general (k, n) - VC means that the secret image is divided into n shares and distribute to n users. Out of n, k shares will reveal the hidden image [1],[2].

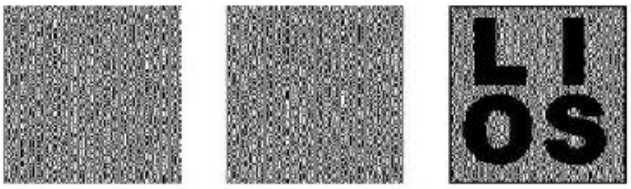



Fig. 1 Traditional (2, 2)-VCS

Extended visual cryptography scheme (EVCS) is similar to basic visual cryptography. The name extended means that here the shares are meaningful images. An example of (2, 2)-EVCS is shown in Fig. 2. Here the shares are meaningful images. EVCS is treated as a technique for steganography. It has fewer chances to detect the secret information. If the shares are colored meaningful images, it is called Color Extended visual cryptography. Here we introduce contrast enhancement in color EVCS [2],[3].

Fig. 2 Traditional (2, 2)-EVCS

The rest of the paper is organized as follows: section II give some preliminary survey on traditional VCS, EVCS and Color EVCS. In section III, we discuss the contrast enhancement in color EVCS. Lastly in section IV we conclude the paper.

## II. RELATED WORKS

In this section we discuss some definitions of VCS, EVCS, Color EVCS and its preliminary works.

### *A. Traditional VCS*

In (k, n) - VCS encrypt a secret message into n shares to be distributed to n participants. Suppose the participants ν= {0, 1, 2,..., n-1}. Here k participants out of n participants can recover the secret message. They are called the qualified subsets of ν and rest of them are called forbidden subsets. A black and white (k, n) - VC scheme consist of two n X m matrices S0 and S1. m is called the pixel expansion, i.e. a single pixel in secret image is represented by m number of pixels in share image. Fig. 3 shows the S0 and S1 with pixel expansion 4. If pixel is white one of the above two rows of Fig.3 is chosen to generate Share1 and Share2. Similarly if pixel is black one of the below two rows of Fig.3 is chosen to generate Share1 and Share2. Here each share pixel p is encoded into two white and two black pixels each share alone gives no clue about the pixel p whether it is white or black. Secret image is shown only when both shares are superimposed. The main drawback of this method is that it only works for black and white images. Later this scheme is advanced to gray scale share images. For apply basic VC method in gray scale image we have to convert it into binary format. This method is called dithering or half toning. Different dithering methods are available. Fig.4 shows an example of gray scale visual cryptography[2].

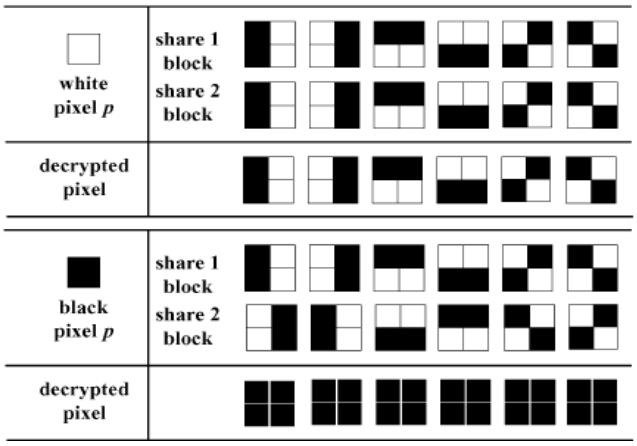



Fig. 3 Traditional (2, 2) VC share matrices

Visual cryptography for color images was developed by Young-Chang Hou. For a secret color image two significant color images are selected as cover images which are the same size as the secret color image. Then according to a predefined Color Index Table, the secret color image will be hidden into two camouflage images. One disadvantage of this scheme is that extra space is required to accumulate the Color Index Table. When more colors are there in the secret image the larger the size of shares will become. To overcome this limitation Chin-Chen Chang et al developed a secret color image sharing scheme based on modified visual cryptography. This scheme provides a more efficient way to hide a gray image in different shares. Scheme does not require any predefined Color Index Table[5 ].

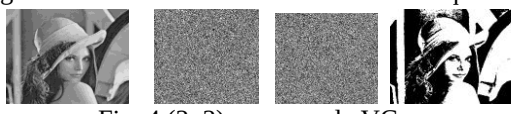


Fig. 4 (2, 2) - gray scale VC

Fig. 5 (2, 2) - color VC

Because the subtractive model is more suitable for printing colors on transparencies, we will use the CMY model to represent colors in visual cryptography. One of the algorithms uses black, cyan, magenta and yellow combination to represent a pixel in shared image. It only gives small amount of whiteness preservation in decrypted image. In order to overcome this disadvantage another one uses cyan, magenta, yellow and transparency combination. But this method can't improve the contrast. Therefore here we use the concept of basic visual cryptography developed by Naor and Shamir. For this we first convert the color image into CMY format and apply any of the dithering technique in each color channel. Now the image is binarised and applies basic share matrices for black and white pixel. Fig. 5 shows an example of color visual cryptography [3].

### *B. Extended VCS*

Naor and Shamir have mentioned an extension of the model which conceals the very existence of the secret message. That is, each sheet carries some meaningful images rather than random dots. They referred to the (2, 2) example with the number of sub pixels m = 4. Ateniese has formalized this framework as the Extended Visual Cryptography and developed a scheme for general access structures. They also discuss the trade-off between the contrast of the each images on the sheets and that of the resulting image when stacked together in (k, k) cases. For EVCs, initially researchers use natural images (Gray scale images).They use the same share matrices of binary images for share generation. Therefore we need to convert the grayscale image into binary. This technique is called half toning. There are a variety of half toning techniques. They are averaging, pattern dithering, error diffusion etc. Error diffusion is the efficient method for half

toning. Fig. 6 shows the block diagram for error diffusion. The recursive structure of the block diagram indicates that the quantization error e(m, n) depends upon not only the current input and output but also the entire past history. The error filter is designed in such a way that the low frequency difference between the input and output image is minimized. The error that is diffused away by the error filter is high frequency or blue noise. The algorithm for extended color visual cryptography is described [3], [4], [5].

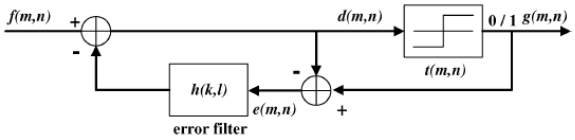


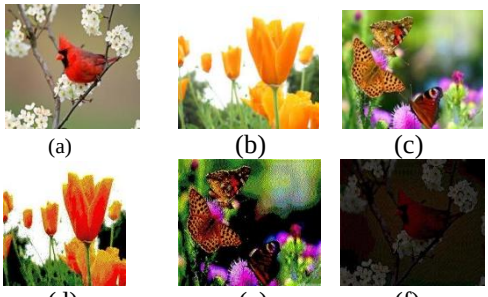

Fig. 6 Error diffusion

Step I: Take a secret image as input.
Step II: Apply error diffusion in secret image and develop n shares using traditional VCS
Step III: Take n other meaningful images.
Step IV: Embed individual secret image share into the Meaningful image.
Step V: Distribute the meaningful images among n participants.
Step VI: Take minimum of k shares out of n.
Step VII: XOR them to get the original secret image

### *C. Color EVCS*

InKoo Kang and Gonzalo R. Arce developed a new technique in color extended visual cryptography using error diffusion and Visual Information Pixel (VIP) synchronization. As we said Error diffusion is a simple but efficient algorithm for image halftone generation. Synchronization of the VIPs across the color channels improves visual contrast of shares. In color VC schemes, the colors of encrypted pixels and the contrast can be degraded due to random matrix permutation. Random matrix permutations are key security features in VC schemes. In grayscale VC schemes, it does not affect the visual quality; however, in color schemes, independent execution of random matrix permutation for each color channel can cause color distortion by placing VIPs at random positions in sub pixels which finally degrades the visual quality. VIP synchronization prevents the color and contrast of original images from degradation even with matrix permutation [4].

The first step of this method is to convert input image into CMY color format. Develop share matrices with VIP synchronization. VIP positions are synchronized across channels regardless of pixel colors and this result in high visual quality of the encrypted shares. Next step is to distribute the matrices in each color channel. Halftone each channel in CMY using error diffusion technique. Apply the newly developed matrices to create share. The visual quality of shares via error diffusion can be improved through edge enhancement methods. Fig. 7 shows an example of color EVCS. Here (a) is the original image, (b) and (c) are the covers used to embed secret image (a). (d) and (e) are the shares. (f) is the decrypted image.



(a) (b) (c)

(d) (e) (f)

Fig. 7 Color EVCs

## III. CONTRAST ENHANCEMENT

In order to improve the contrast of decrypted image in color EVCS we use 2 another techniques. They are Additional Basis Matrix (ABM) and Perfect Reconstruction of White Pixel (PRWP). These techniques are used in contrast enhancement in basic VCS in a new thesis paper. Here we uses the same technique in color EVCS. As we seen in share matrices of basic VCS black pixel is perfectly reconstructed, but the problem is for white pixels. For perfect reconstruction of white pixel we use these techniques in our color EVCS.

Additional Basis Matrix technique use additional combination of basis matrices in the case of white pixel. By increasing the number of pixel patterns for white pixels, the contrast of the reconstructed image can be improved without adding any computational complexity. We apply error diffusion and VIP synchronization in these newly developed ABM and use for share generation. Fig 8.shows the ABM matrix for (2, 2) - VCS with pixel expansion 4 [6].

The existing pixel patterns for the visual cryptography scheme are based on the perfect reconstruction of black pixels (PRBP). Here, a visual cryptography scheme which is focused on the perfect reconstruction of white pixels (PRWP) and hence can provide better clarity [6]. Fig 9 shows the different outputs (a), (b) and (c) of color extended visual cryptography using basic method, ABM and PRWP respectively.

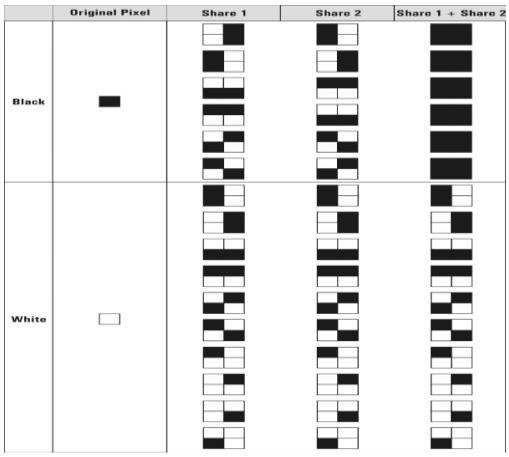



Fig. 8 (2,2)- VCS with ABM

(a) (b) (c)

Fig. 9 Output of (2, 2) - EVCS using different methods

## IV. CONCLUSIONS

The concept of VIP synchronization and error diffusion used to attain a color visual cryptography encryption method that produces meaningful color shares. Error diffusion suppresses the noise content in encryption. It is obvious that there is a tradeoff between contrast of encryption shares and the decryption share. However, we can recognize the colorful secret messages having even low contrast. In order to improve contrast we used ABM and PRWP in the basic visual cryptography share matrices developed by Naor and Shamir. It improves the SNR value. We hope we can develop a method with perfect reconstruction.

## ACKNOWLEDGMENT

During the paper preparation, many reviewers provided many valuable constructive comments. We gratefully acknowledge all the reviewers.

## REFERENCES

[1] Moni Naor and Adi Shamir, "Visual Cryptography", *advances in cryptology Eurocrypt*, pp 1-12,1995.

[2] Chin-Chen Chang, Jun-Chou Chuang, Pei-Yu Lin, "Sharing A Secret Two-Tone Image In Two Gray-Level Images", *Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05)*, 2005.

[3] C. Yang and C. Laih, "New Colored Visual Secret Sharing Schemes". *Designs, Codes and cryptography*, 20, pp. 325335, 2000.

[4] InKoo Kang, Member, IEEE, Gonzalo R. Arce, Fellow, IEEE, and Heung- Kyu Lee, Member, IEEE, "Color Extended Visual Cryptography Using Error Diffusion", *IEEE TRANSACTIONS ON IMAGE PROCESSING*, VOL. 20, NO. 1, JANUARY 2011

[5] Y. C. Hou, "Visual cryptography for color images", *Pattern Recognit.*, vol. 36, pp. 16191629, 2003.

[6] Thomas Monoth and Babu Anto P, *Contrast-Enhanced Visual Cryptography Schemes Based on Additional Pixel Patterns*, Proc. of the IEEE International Conference on Cyber Worlds (CW 2010), NTU, Singapore, pp. 171-178, 2010. (IEEE Computer Society