ISSN 2320 – 2602
International Journal of Advances in Computer Science and Technology (IJACST), Vol. 3 No.2, Pages : 29 – 33 (2014)
Special Issue of ICCSIE 2014 - Held during February 16, 2014,Bangalore, India

An Overview of Visual Cryptography Schemes for Encryption of Images

Moumita Pramanik[1], **Kalpana Sharma**[2]
[1]Sikkim Manipal Institute of Technology, Majitar, India, Email: moumita.pramanik@gmail.com
[2] Sikkim Manipal Institute of Technology, Majitar, India, Email: kalpanaiitkgp@yahoo.com

Abstract *:* Information Security has become an inseparable issue in the rapid growth of computer and communication technology. Data is vulnerable to various attacks. Although, cryptography schemes are used to protect data, still it suffers various issues viz., computational complexity, processing delay and more storage medium. Visual Cryptography (VC) is an emerging cryptographic scheme, which splits an image into different shares in its encryption process and the image can be decoded by stacking the shares with each other. Decryption process is not required any cryptography knowledge as it requires the human visual system to retrieve the original image. Various visual cryptography schemes have been proposed so far. This paper reviews few VC schemes with its different characteristics.

Key words : Visual Cryptography, VC, Shares.

INTRODUCTION

Now-a-days, the biggest threat in information communication is the possibility of data being hacked. Visual Cryptography(VC)[1] is a scheme for protecting image based information such as handwritten notes, printed text, picture etc. It was first introduced by Naor and Shamir in 1994 [1]. In the encryption process of VC, it splits the original image into different shares. The decryption process of VC is computation free. It recovers the original image by superimposing the different shares which can directly recognized by human visual system [3]. The rest of the paper is as follows. Section II describes the basic VC Scheme, then its general access structure in section III. Section IV focuses on enhance perceive visual quality of VC followed by section V and VI, which emphasizes on various gray scale VC scheme and color VC scheme respectively. The paper is concluded in section VII.

BASIC VISUAL CRYPTOGRAPHY SCHEME

A new type of cryptography scheme named Visual Cryptography, which encrypt the written material such as printed text, hand written notes, pictures etc in a secure way and decode the same directly by the human visual system [1]. In (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. Anyone, having only one share can not get any information about the secret image. In the process of decryption, stacking of both the shares with each other can provide the information about the secret image. Encryption of a (2, 2) VC Scheme is shown in Figure.1.

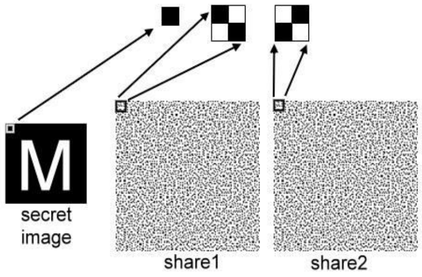


Fig 1. A (2,2) Visual Cryptography Scheme [13]

Working Principle

A pixel P is split into two sub-pixels in each of the two shares. If the pixel P is white, randomly choose one of the first two rows of the Figure 2. If the pixel P is black randomly chooses one of the last two rows as shown in Figure 2. Then pixel P is encrypted as two sub pixels in each two shares, as determined by the chosen rows in Figure 2.

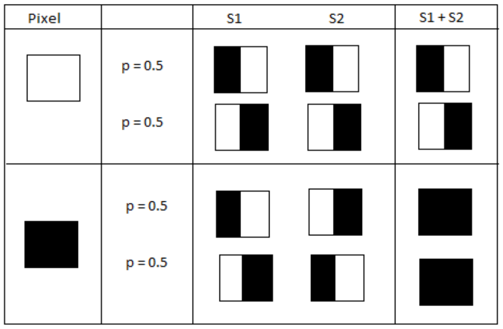


Fig 2. VC scheme for encoding a binary pixel into two shares [14]

The technique used for encoding one pixel, applied to every pixel P in secret images in order to construct the two shares [14]. The important parameters of this scheme are Pixel expansion (m), contrast (α) and size of recover image (r). The 'm' is the number of sub-pixel in a share. It is better to be as small as possible. The contrast, which is a relative difference of Hamming weight of combined shares that come from a black and white pixel [3]. This relative difference needs to be as large as possible [3]. The (k,n) VC scheme generates 'n' numbers of shares for a secret image. Minimum k' numbers of shares are required to recover the secret image. Any 'k-1' numbers of shares are not given any information about the secret image.

VISUAL CRYPTOGRAPHY WITH GENERAL ACCESS STRUCTURE

G. Ateniese et al [2] extend the Naor and Shamir's VC model to general access structures. An access structure is an order of all qualified and forbidden subsets of participants. It proposed two techniques to implement VC schemes through general access structures. It analyzes the structure of VC schemes and establishes bound on the size of the shares circulated to the participants. In the first technique, lower bounds on the size of the shares distributed to the participants. It provides a novel technique to realize k out of n threshold VC scheme. Another technique considered graph based access structures[2] that offer both lower and upper bounds on the size of the shares. In graph based access structures qualified set of participants hold at least an edge of a given graph whose vertices represent the participants of the scheme. For example, considered that there are four participants such as P = {1,2,3,4} and qualified sets are all subsets of P containing the one of the three sets {1,2}, {2,3} or {3,4}. Hence, the probability of qualified sets is:

Γ_{Qual} = {{1,2}, {2,3}, {3,4}, {1,2,3}, {1,2,4}, {1,3,4}, {2,3,4}, {1,2,3,4}}

And rest of the subsets of P is forbidden.

Working Principle

General access structure of the proposed model shows that P = {1, ….. n} a set of participants and 2^P the set of all subsets of P. $\Gamma_{Qual} \subseteq 2^P$ and $\Gamma_{Forb} \subseteq 2^P$, where $\Gamma_{Qual} \cap \Gamma_{Forb} = \varnothing$ and qualified sets are member of Γ_{Qual} and forbidden sets are member of Γ_{Forb}. The pair of $(\Gamma_{Qual}, \Gamma_{Forb})$ is known as access structure of VC Scheme. It defines all the minimal qualified sets as Γ_0 , where

$$\Gamma_0 = \{ A \in \Gamma_{Qual :} A' \notin \Gamma_{Qual} \text{ for all } A' \subset A\}.$$

A member p ∈ P is an essential participant if there exists a set $X \subseteq P$ such that $X \cup \{P\} \in \Gamma_{Qual}$ but $X \notin \Gamma_{Qual}$. If a member P is not essential then provide a share completely white or even nothing in that share.

ENHANCED PERCEIVED VISUAL QUALITY OF VISUAL CRYPTOGRAPHY SCHEME

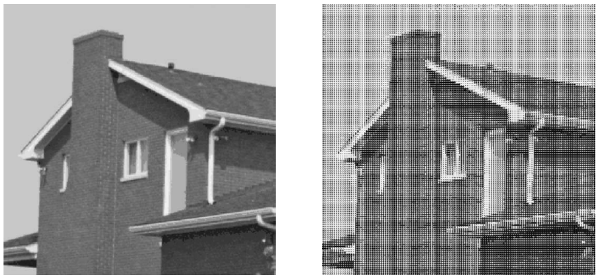
The primary aim of VC is that human visual system can directly decoded the secret image. But at the time of superimpose, visual quality of recovered image is reduced. Hence, it is required to improve perceived visual quality of the recovered image, which can be done by performing image filtering prior to encryption [4]. Yang and Chen [3] observed that the contrast of a recovered image is reduced and it is likely to prioritize certain most important pixels during the encryption. In this scheme, edge detection is performed on the secret image to identify important pixels. These edge detections give the most meaningful information about the image. After identification, the significant pixels and less significant pixels are gives different pixel expansions during encryption. Hence, the size of the resulting shares is smaller than that of the traditional size expanded VC Schemes.

Instead of performing edge detection[4], authors propose a method to enhance the perceive edges by passing the secret image through a sharpening filter[4]. This has the effect of increasing the local contrast at discontinuities in the gray level image that make easier to recognize edges in the image. As a result it appear sharper to the human visual system. This scheme applies a Laplacian filter[4] to the image for sharpening. After sharpening, the dithered image can be encrypted using (2, 2)-VC scheme into two different shares.

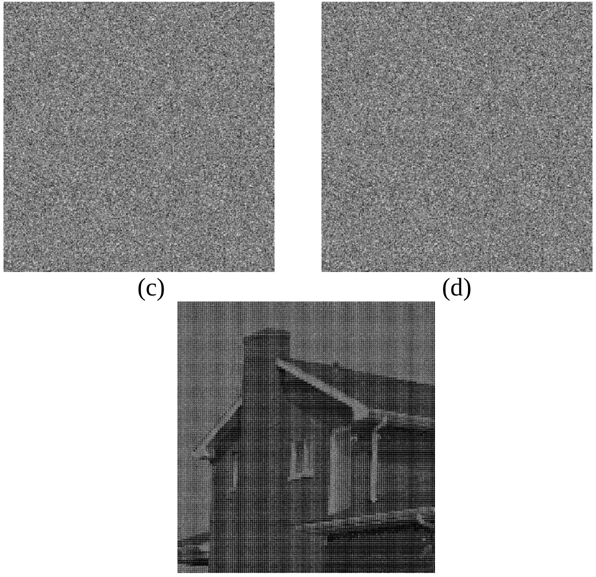
In addition to sharpening filter of an image, which raises the local contrast at discontinuities, the global contrast of the secret image can also be improved using histogram equalization [4]. Usually, a grayscale image has 256 potential intensity values. An image histogram represents the intensity allocation of the pixels in an image over these values. Histogram equalization is a technique that is used to spread the image intensity to cover (0 – 255) range of values. For images that do not cover the full range of values, histogram equalization effectively increases the global contrast of an image. The entire process can be summaries as first perform histogram equalization, pass the resulting image through a sharpening filter, then dither the image produced from the previous step and finally apply a (2,2) VC Scheme to enhance the perceived visual quality of the recovered image.

VISUAL CRYPTOGRAPHY FOR GRAY SCALE IMAGE

Verheul and Van Tilborg [5] was proposed the visual cryptography scheme for gray scale images. In this approach shares are generated from the gray levels existing in original images instead of using the values of black and white pixels. But this method has the disadvantage of size increase at the time of decryption. Another new method for gray level images was proposed that uses digital image half-toning [6] to convert a gray level image into an approximate binary image. Then the VC scheme is used for binary images. The advantage of this scheme is that the recovered image is less enlarges as compared to the basic VC scheme[1]. Ordered dithering is a technique used in it which performs fast and parallel transformation of gray level image into an equal sized binary image. The space filling curve ordered dithering (SFCOD) algorithm[6] also used to keep the image quality. The figure 3 shows a gray level image and the dithered image and generated shares and decoded image.



(a) (b)

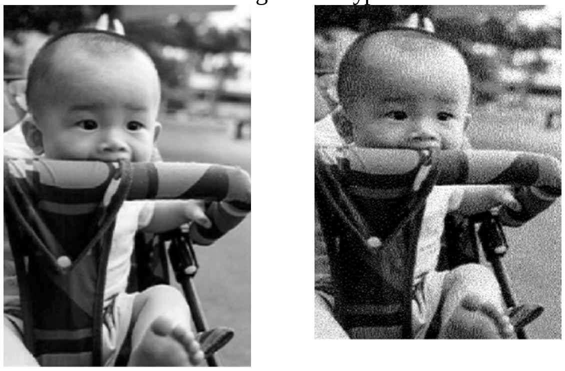

(c) (d)

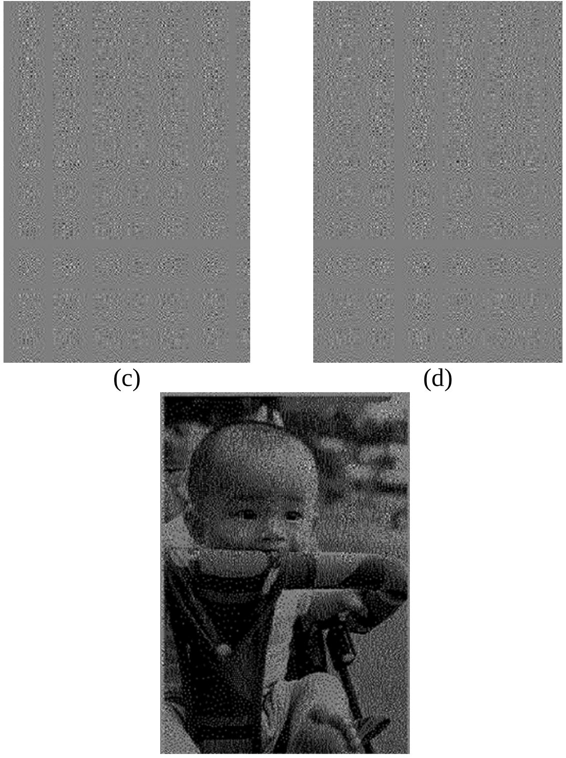
(e)

Fig 3. VC Scheme using Dithering:(a) Original Image (b) Dithered Image, (c) Share 1 (d) share 2 and (e) Decoded image [6]

In [7] author describe that different media use different ways to represent the gray or color level of image according to their characteristics. The computer screen applies the electric current to manage the lightness of the pixels. The range of the lightness generates different color levels. The general printer, such as dot-matrix, laser, and jet printers can control gray level image by a single pixel to be printed i.e. black pixel, not to be printed white pixel. The technique applied to represent the gray level of images is to use the density of printed dots. The quantity of printed dots in the light part of an image is sparse and dark part is dense. The method that uses the density of the net dots to simulate the gray level is also known as Halftone. Before generate shares, a gray level image is transformed into halftone image. Every pixel of the halftone image has only two possible color levels i.e. black / white. The algorithm used in it as follows:

i) Read the image for encryption.
ii) Transform the gray-level of image into a black-and-white halftone image.
iii) For each black or white pixel in the halftone image, decompose it into a 2×2 block of sub-pixel.
iv) Apply basic VC scheme to create shares.
v) Repeat Step (ii) to (iv) until all pixels in the halftone image is encrypted.


(a) (b)


(c) (d)

(e)

Fig 4. Encryption and decryption of gray level VC (a) Original Image (b) Halftone image (c) Share 1 (d) share 2 (e) recovered image [7].

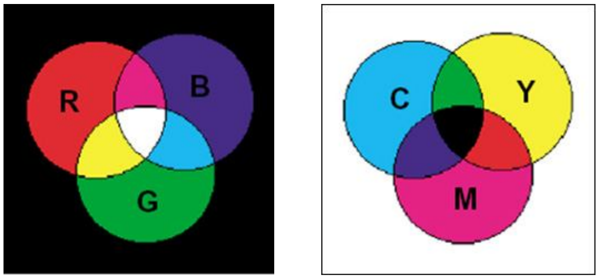
The result of two stacked pixels shows black if it combines black and black pixel, shows half black & half white if it combines white and black pixel, and white and white is white. Therefore, when stacking two shares, the corresponding blocks of black pixels full black, and those corresponding to white pixels are half-black-and-half-white i.e. 50% gray pixel in the recovered secret image. Figure 4 shows the gray level VC scheme using Halftone process.

VISUAL CRYPTOGRAPHY FOR COLOR IMAGES

Until the year 1997 VC schemes were limited to black and white images only. First colored VC scheme was proposed by Verheul and Van Tilborg [5]. Colored secret images can be represented with the concept of arcs to build a colored visual cryptography scheme. In c-colorful VC scheme, one pixel is changed into m sub pixels, and each sub pixel is separated into c color regions. There is exactly one color region in each sub pixel, and rest all of the color regions are black. The color of each pixel depends on the interrelations between the stacked sub pixels. For a colored VC scheme with c colors, the pixel expansion m is c × 3 [8]. Yang and Laih [9] enhanced the pixel expansion to c × 2 of Verheul and Van Tilborg. Both of these schemes generated shares were meaningless.

Chang and Tsai [10] generate meaningful share to transmit secret image using color visual cryptography scheme. In this scheme two different color images are used as a cover images which have the same size as the secret color image. Then according to a predefined color index table, the secret color image is hidden into two cover images. It requires extra space to accumulate the color index table.

Young-Chang Hou [7] proposed an additive and subtractive model which is commonly used to describe the structure of colors. In the additive model, three primary color red, green and blue (RGB) are used and desired colors being get by mixing these RGB components. To calculating the intensity of red/green/blue components, it adjusts the amount of red/green/blue in the compound light. More combination of these three color represent light color, as result white color is given by mixing all red, green and blue components. The computer monitor is an example of the additive model. In the subtractive Model, color is represented by applying the combinations of colored-lights reflected from the surface of an object. This model use Cyan (C), Magenta (M) and Yellow (Y) color components and produce a wide range of colors. More component gives less intensity of the light, and thus the darker is the light. The color printer is an application of the subtractive model.



(a) (b)

Fig 5. Color component (a) for additive model (b) for subtractive model [7]

It proposed VC methods to decompose the color secret image into three separate images that are respectively colored cyan (C), magenta (M) and yellow (Y). Then the halftone technique is applied to translate the three color images into halftone images. Finally, by combining the three halftone images, a color halftone image can be generated. The color halftone image generation process is shown in Fig. 6.

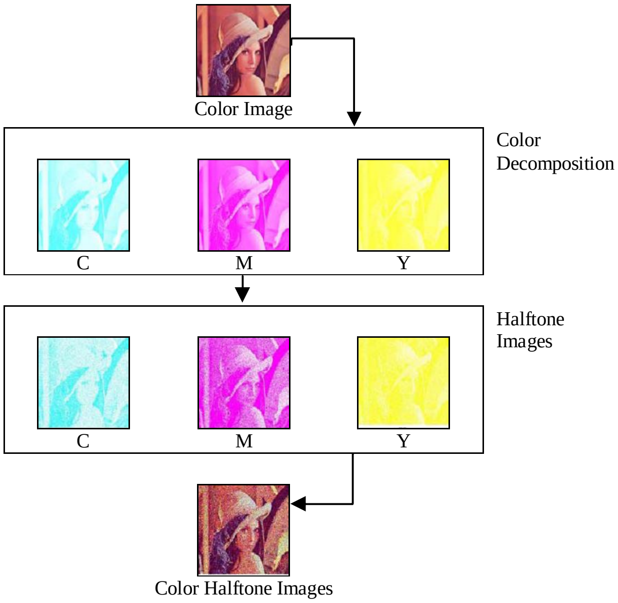


Fig 6. Color Decomposition for color halftone image [11]

This color halftone image obtains eight dissimilar colors such as cyan, magenta, yellow, black, red, green, blue and white. For each pixel of the color halftone image, first, 2×2 blocks are built according to Share 1, and the four pixels C, M, Y and W are randomly permuted. Then, the number of blocks is calculated for Share 2 according to the color ratio of the four pixel pixels with the coding table.

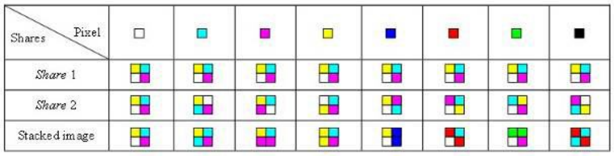

Pixel
Shares
Share 1
Share 2
Stacked image

Fig 7. Coding table [11]

If one pixel is green, then the pixel's color ratio would be 100%, 0% and 100% for C, M and Y, respectively [11]. Thus, block in Share 1 is the permutation of cyan, magenta, yellow and white pixel. Then, using the above order and coding table share 2 is produced where the permutation of the pixels is yellow, magenta, cyan and white. After all the pixels are decomposed two shares are produced. Each block of the two shares composed with C, M, Y and W colors. The secret image can be retrieved visually when the two shares are superimposed.

Hsien-Chu Wu et al [11] extend a single pixel into a 2×4 block. The size of the share remains the same in contrast of the 2×2 pixel expansion case. This approach saved the considerable storage space and also the shares are not look like random noise. In [12] author proposed an encryption method for color Visual Cryptography scheme with Error diffusion and VIP Synchronization for visual quality improvement.

CONCLUSION

There are a variety of innovative ideas and extensions of VC proposed since its introduction. The VC technique is being used by a number of countries for secretly transfer of hand written documents, financial documents, text images, internet voting etc. The basic VC scheme and the visual cryptography scheme for gray level and color image encrypt the secret image securely where the decoding is computation free as only super-imposing the shares reveals the secret image. The existing visual cryptography schemes still lead to pixel expansion and insufficient visual quality. Though the various VC scheme are proposed by different researcher at different time to overcome this problem, it raises other problem like increase of storage space, computation complexity etc. Hence, further work to enhance the visual cryptography mechanism for more security of the information can be carried out. Integrating VC scheme with digital watermarking, steganography could be enhance the security level of the information.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology-EUROCRYPT'94, pp. 1-12,1995.

[2] Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson. Visual cryptography for general access structures. Inf. Computer., 129(2):86-106, 1996.

[3] C.-N. Yang and T.-S. Chen. Visual secret sharing scheme: Improving the contrast of a recovered image via different pixel expansions. In A. C. Campilho and M. S. Kamel, editors, ICIAR (1), volume 4141 of Lecture Notes in Computer Science, pages 468-479. Springer, 2006.

[4] Yang-Wai Chow, Willy Susilo and Duncan S. Wong "Enhancing the Perceived Visual Quality of a Size Invariant Visual Cryptography Scheme" ARC Future Fellowship FT0991397.

[5] Verheul, E.R., van Tilborg, H.C.A., 1997 "Construction and Properties of k out of n visual secret sharing schemes" Designs Codes Cryptography. (11), 179–196.

[6] Chang-Chou Lin, Wen-Hsiang Tsai, "Visual cryptography for gray-level images by dithering techniques", Pattern Recognition Letters 24 (2003) 349–358.

[7] Young-Chang Hou "Visual cryptography for color images" Pattern Recognition 36 (2003) pp-1619 – 1629, 2003

[8] Thottempudi Kiran and K. Rajani Devi, "A review on visual cryptography schemes", Journal of Global Research in Computer Science, Volume 3, No. 6, June 2012 pp: 96-100.

[9] C.Yang and C. Laih, "New Colored Visual Secret Sharing Schemes". Designs, Codes and cryptography, 20, pp. 325–335, 2000.

[10] C.Chang, C. Tsai, and T. Chen."A New Scheme For Sharing Secret Color Images In Computer Network", Proceedings of International Conference on Parallel and Distributed Systems, pp. 21–27,July 2000.

[11] Hsien-Chu Wu, Hao-Cheng Wang, and Rui-Wen Yu, "Color Visual Cryptography Scheme Using Meaningful Shares" Eighth International Conference on Intelligent Systems Design and Applications, pp-173-178

[12] Pankaja Patil,Bharati Pannyagol, "Visual cryptography for color images using error diffusion and pixel synchronization", International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 1 Issue 2 July 2012 ISSN: 2278-621X, pp: 1 – 10

[13] Jagdeep Verma, Dr.Vineeta Khemchandani "A Visual Cryptographic Technique to Secure Image Shares" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 1, pp.1121-1125, Jan-Feb 2012.

[14] Archana B. Dhole, Prof. Nitin J. Janwe, "An Implementation of Algorithms in Visual Cryptography in Images", International Journal of Scientific and Research Publications, Volume 3, Issue 3, March 2013 ISSN 2250-3153 pp:1-5.