

A Brief Introduction of Visual Cryptography

Sandhya N.

Department of Computer
Engineering

Padmashree Dr. D. Y. Patil College of Engineering
Pimpri Pune India

Prof. Jyoti Rao

Department of Computer
Engineering

Padmashree Dr. D. Y. Patil College of Engineering
Pimpri Pune India

Abstract: Visual cryptography is a cryptographic method for securing images. In visual cryptography images are divided into n -number of shares which provide security for the images and stacking or overlapping of these shares reveal the original secret image. Initially, it was developed for binary images. Different schemes are used to generate shares for secret images. Later in visual cryptography many advance methods are came into exist, those are extended visual cryptography, Visual cryptography for color images i.e. grey and RGB/CMY images. These methods are meant only for revealing the whole secret image. For revealing images part-wise which means region by region image, Region Incrementing Visual cryptography method is developed.

Keywords: Visual cryptography; Pixel Expansion; Contrast; Secret image; Secret Sharing.

I. INTRODUCTION

A Secure and an efficient communication of confidential and sensitive information is the initial concern in communication and network storage system. It is also important for any data not to be tamper. Now a day's much multimedia information is transmitted in large amount over internet. Especially while using images, secrecy is a major challenge. Because of this advancement in the network application securing image became a wide area to give attention.

Visual cryptography is a cryptographic technique which is used for securing images or text. It is introduced in 1994 by Moni Naor and Adi Shamir[1]. Visual cryptography hides secrets within the images i.e. image is divided into multiple shares and afterwards decode without any computation. This decoding is done by superimposing the shares which will reveal the secret image or text by the human visual system. Initially the model which was developed consists of a page of ciphertext and a page of transparency(secret key)[1]. The cleartext(original text) is obtained by superimposing the transparency with the key over the ciphertext. Later on this model is extended by k out of n secret sharing scheme where secret sharing is a technique in which secret i.e shares are distributed among the participant. Thus the secret is able to reveal only when a adequate number of shares are stacked together. In (k,n)

secret sharing scheme[1] secret image is revealed only when k or more than k shares are stacked. But shares less than k will not reveal any information. Later visual cryptography is advanced for color images[5]. Many techniques

are developed based on the color decomposition technique for color images and RGB/CMY images.

Image or a text used in secret sharing is a combination of black and white pixels. These white and black pixels appear in n modified version called shares. Each shares consists of a collection

of black and white subpixels. Consider visual cryptographic scheme:

White pixel always results one black and white subpixel after superimposing whereas black pixel results two black subpixels. When shares are stacked together, if the number of subpixel is more than constant threshold then that pixel is considered as "on" if it is less than constant threshold it is considered as "off".















Pixel	White 	Black 
Prob.	50% 50%	50% 50%
Share 1	 	 
Share 2	 	 
Stack share 1 & 2	 	 

Figure 1: Construction of $(2,2)$ VC scheme.

This reconstruction leads to contrast loss and also pixel expansion will also take place where contrast " α " is the difference between number of on and off threshold of transparent pixels. Disadvantage of this scheme is only single set of secret message can be embedded but a large amount of secret messages or images requires generation of more number of shares.

Multiple sharing technique is introduced by Wu and Chen [2] to overcome this problem. They hide two secret binary images into two random shares, namely A and B, such that the first secret can be seen by stacking the two shares, denoted by $A \oplus B$, and the second secret can be obtained by first rotating $A \oplus B$ anti-clockwise. Many researchers have been made in multiple secret sharing but all of them based on black and white images. But as per the time there is a demand that scheme should also support color images. VCS is used in applications such as E-Voting system, financial documents and copyright protections. In this paper, second section describes the basic model, third section describes the schemes of visual cryptography and at least fourth section describes the conclusion.

II. BASIC MODEL

The basic model of visual cryptography proposed by Naor and Shamir [1] accepts binary image 'X' as secret image, which is divided into 'n' number of shares. Each pixel of image 'X' is represented by 'm' sub pixels in each of the 'n' shared images. The resulting structure of each shared image is described by Boolean matrix 'B' Where $S=[B_{ij}]$ an $[n \times m]$ matrix $B_{ij}=1$ if the jth sub pixel in the ith share is black $B_{ij}=0$ if the jth sub pixel in the ith share is white. When the shares are stacked together secret image can be seen but the size is increased by 'm' times. The grey level of each pixel in the reconstructed image is proportional to the hamming weight $H(V)$ of the OR-ed Vector 'V', where vector 'V' is the stacked sub pixels for each original pixel. A solution of the 'n' out of 'n' visual secret sharing consists of two collections of $n \times m$ Boolean Matrices C_0 and C_1 . To share a white pixel, randomly choose one of the matrices from C_0 , and to share a black pixel, randomly choose one of the matrices from C_1 . The following conditions are considered for the construction of the matrices:

1. For any 'B' in C_0 , the OR-ed 'V' of 'n' rows satisfies $H(V) \leq n - \alpha m$.
2. For any 'B' in C_1 , the OR-ed 'V' of any 'n' rows satisfies $H(V) \geq n$.

By stacking fewer than 'n' shares, even an infinitely powerful cryptanalyst cannot gain any advantage in deciding whether the shared pixel was white or black. Let us describe the construction of matrix for (n, n) visual cryptography for $n=3$.

C_0 = all the matrices are generated by permuting the columns complement of [YX]

C_1 = all the matrices are generated by permuting the columns of [YX]

Where, X is the matrix of order $n \times (n-2)$ which contains only ones I is the identity matrix of order $n \times n$

$$\text{For } n=3 \text{ } X = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ and } y = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\text{Hence } C_1 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix} \text{ and } C_0 = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

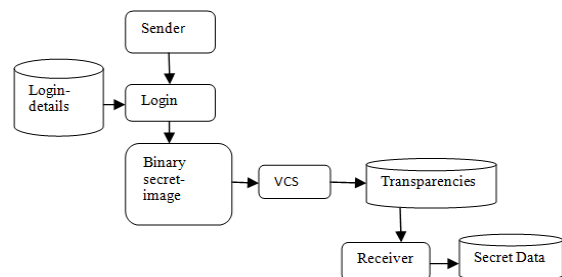
The basic model was then extended to (k, n) threshold cryptography where any 'k' or more shares will reveal the secret image. The construction of 'k' out of 'n' visual secret sharing is similar to the basic model with one difference. That is in basic model the threshold value is n whereas here it is k which is the subset of n.

III. EMERGING VISUAL CRYPTOGRAPHY

A. Binary Image

In visual cryptography many new methods are recently implemented. First of all, It is introduced in 1994 by Moni Naor and Adi Shamir [1]. Visual cryptography hides secrets within the images i.e. image is transformed into multiple shares and decoding takes place without any computation. Decoding is usually done by stacking the shares which will reveal the secret image or text by the human visual system. Initially the model which was introduced by Naor and Shamir consists of a page of ciphertext and a page of shares or transparency. The cleartext i.e. original text is obtained by overlapping or stacking the transparency with the key over the ciphertext. Later this model is extended by k out of n secret sharing scheme where secret sharing is a technique in which secret i.e. shares are distributed among the participant. Thus the secret is able to reveal only when an adequate number of shares are stacked together. In (k,n) secret sharing scheme secret image is revealed only when k or more than k shares are stacked. But shares less than k will not reveal any information.

Basic architecture of visual cryptography is shown below:



Later visual cryptography is advanced for color images. Many techniques are developed based on the color decomposition technique for color images and RGB/CMY images. Many researchers have been made in multiple secret sharing but all of them based on black and white images. But as per the time there is a demand that scheme should also support color images

B. Colored VC Using Arcs

In 1997 first colored visual cryptographic technique was introduced by Verheul and Van Tilborg [2]. Colored secret images can be shared with the concept of arcs to construct a colored visual cryptography scheme. In this visual cryptography scheme one pixel is transformed into n subpixels, and each subpixel is divided into c number of color regions. In each subpixel, there is exactly

one color region colored, and all the other color regions are black. The color of one pixel depends on the interrelations between the stacked subpixels. Afterwards many researches have been made on color cryptographic scheme.

C. Extended VC.

In the year 2002 Nakajima [3] introduced new technique in visual cryptography called as extended visual cryptography scheme for natural images which is to improve the visual quality of images. The basic idea of this scheme is shown in the figure that is, three images are taken as input and generates two images from three input images. The third resulted picture is reconstructed by printing the two output images onto transparencies or shares and overlapping them together.

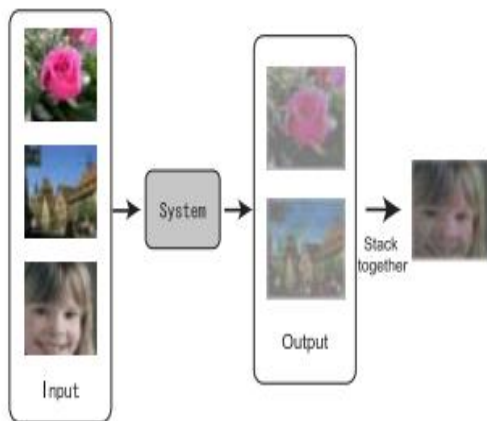


Figure 2: Basic idea of Extended visual cryptography.

D. Halftoning Visual Cryptography

Hou [5] has proposed the binary visual cryptography scheme which is used to apply for gray level images, that a gray level image is converted into halftone images in the year 2004. The method which uses the thickness of the net dots to simulate the gray level is called "Halftone" and before processing only transforms the secret image with gray level into a binary image. Thus in this scheme, first the gray level image is transformed into a halftone image and then construct two transparencies or shares of visual cryptography. Apparently, undeniably cannot identify any data about the secret image from the transparencies individually, but the result clearly shows a picture when the shares are overlapped together.

Original

Halftoned

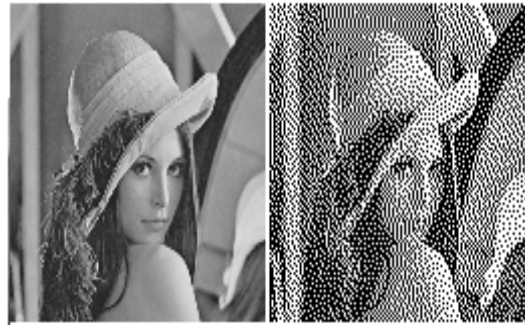


Figure 3: Halftone VC

Hou [5] considered decomposition of the colour image into three that is yellow, magenta and cyan halftone images and then it is improvised into three coloured 2-out-of-2 VC schemes which uses the below subtractive model shown in the figure.

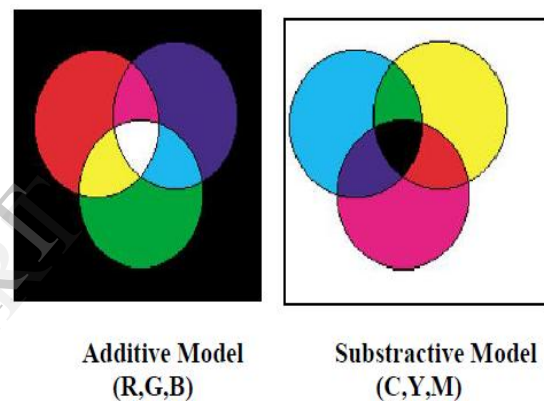


Figure 4: Additive and subtractive model

E. Region Incrementing Visual Cryptography

The above mentioned schemes for visual cryptography are used for processing the content of the image as a single secret. This type of sharing scheme discloses either the whole secret image or nothing, and hence this concept limits the secrets in an image. Ran-Zan Wang proposed [6] Region Incrementing Visual cryptography (RIVCS) for sharing visual secrets in multiple secrecy level in a single image. The 'n' level RIVC scheme consider an secret image S associated with multiple regions having different secret levels, and encoded to shares with the following features:

- Single share cannot reveal any of the secrets in the secret image S,
- Any $x(2 < x < n+1)$ shares are consider to reveal $(x-1)$ levels of secrets
- the secrets which are not-yet revealed are unknown to users.
- When all of the $(n+1)$ shares are available, all the secrets in secret image S can be disclosed.

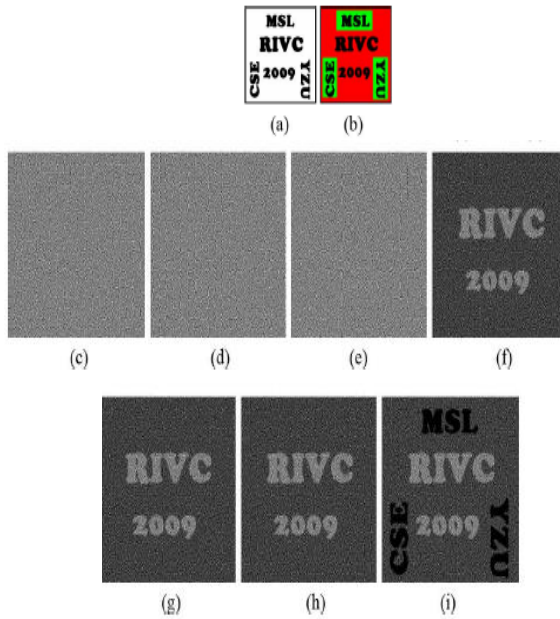


Figure 5: (a) Secret image, (b) secrecy-level decomposition, (c)–(e) three encoded shares,(f)–(h) superimposing any two of the three shares, and (i) superimposing all three shares.

IV. CONCLUSION

In this paper, We briefly review some of the schemes of visual cryptography. Among all the various advantages of visual cryptographic schemes (VCS), we accentuate the property that VCS's decoding is completely depends on human visual system which give opportunity to lot of application in different sectors of our society. To hide secrecy in VC, usually we go for expansion which leads to increase the number of shares, but this causes failure in image's resolution. So, an optimum number of shares must be generate, considering security issue. Hence in VC, research in mainly towards contrast and security.

REFERENCES

- [1] Moni Naor and Adi Shamir, "Visual Cryptography", advances in cryptology–Eurocrypt, pp 1-12,1995.
- [2] R. Verheul and H. C. A. Van Tilborg, Constructions and properties of k out of n visual secret sharing schemes, *Designs, Codes and Cryptography*, Vol. 11, No. 2 (1997) pp. 179–196.
- [3] C.C. Wu, L.H. Chen, "A Study On Visual Cryptography", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.
- [4] Nakajima, M. and Yamaguchi, Y., Extended visual cryptography for natural images. *Journal of WSCG*. v10 i2. 303-310.
- [5] Y.-C. Hou, "Visual cryptography for color images," *Pattern Recognit.*, vol. 36, no. 7, pp. 1619–1629, 2003.
- [6] R.-Z. Wang, "Region incrementing visual cryptography," *IEEE Signal Process. Lett.*, vol. 16, no. 8, pp. 659–662, Aug. 2009.
- [7] S. J. Shyu, S.-Y. Huang, Y.-K. Lee, R.-Z. Wang, and K. Chen, "Sharing multiple secrets in visual cryptography," *Pattern Recognit.* vol. 40, no. 12, pp. 3633–3651, Dec. 2007.
- [8] T. Hofmeister, M. Krause, and H. U. Simon, "Contrast optimal k out of n secret sharing schemes in visual cryptography," *Theor. Comput. Sci.*,vol. 240, no. 2, pp. 471–485, Jun. 2000.