

An Enhance Color Visual Cryptography Scheme

Arpana jaiswal¹, Praveen Chouksey²

C.V.R.U., India

Email address: ¹jaiswal.arpana.arpana@gmail.com

Abstract— Visual Cryptography is one of the important encryption technique to hide the secret image into two or more images which are called shares. The shares are very safe because separately they reveal nothing about the secret image. The original secret image can be obtain by simply satcking all the shares together without any complex computation involved. Visual Cryptography has made the security of information easier and better than other cryptography techniques used in secret writing.

Keywords— Color visual cryptography; data hiding; encryption; decryption.

I. INTRODUCTION

Visual cryptography is a secure, easy, simple and effective cryptographic technique used for secret image sharing. Secret image sharing is the important subject in the field of communication techniques, information security and production. However we can provide security in many other ways like transmitting with password, image hiding, watermarking technique, authentication and identification. But the main drawback of these methods is that the secret images can be protected in single information carrier. To overcome this problem, Visual cryptography scheme for secret sharing was introduced by Naor and Shamir [3] In 1994, Moni Naor and Adi Shamir [3] combined the two mechanisms: secret sharing and traditional cryptography. They introduced a new concept named Visual Cryptography for the encryption and decryption of printed materials such as images or text.

In this scheme the secret image is split up into number of shares and transmit to the number of participants. In Visual cryptography, visual information (Image, text, etc) gets encrypted in such a way that the decryption can be performed by the simply human vision without any computer operation [1]. There are many visual cryptography scheme which are discussed in this paper in section II. In this paper i am putting light on “the color visual cryptography scheme”. For providing secrecy of an secret image.

II. VISUAL CRYPTOGRAPHY SCHEMES

A. (2, 2) Visual Cryptography Scheme

In (2, 2) Visual Cryptography Scheme, original secret image is splited into 2 shares. Each pixel in original image is represented by non-overlapping block of 2 or 4 sub-pixels in each share. Anyone, whose having only one share will not be able to find out secret image. To reveal the original secret image both of the shares are required to be superimposed [3].

B. (k, n) Visual Cryptography Scheme

In (2, 2) visual cryptography, both the shares are neccessary to reconsturct original secret image. To give some flexibility to user, basic model of visual cryptography proposed by Naor and Shamir can be generalized into a visual variant of k out of n visual cryptography scheme [3]. In (k,n) visual cryptography

scheme, n shares should be generated from original secret image and distributed. Original image is reconstructed iff k or more secret shares stacked together, where value of $k = 2$ to n . If less than k shares stacked together, original image should not be reconstructed.

















Original Pixel	Probability	Share 1 Sub-Pixel	Share 2 Sub-Pixel	Share 1 Share 2
	0.5			
	0.5			
	0.5			
	0.5			

Figure 1: 2 out of 2 using 2 subpixels per original pixel

C. VCS for General Access Structure

G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson extends (k,n) visual cryptography model to general access structure [4]. In GAS scheme, n shares generated by original secret image is divided into two subsets namely qualified and forbidden subset of shares as per the importance of shares. Any k shares from qualified subset of shares can reconstruct original secret image information, but less than k shares from qualified subset of shares can not reconstruct original secret image information. But k or more shares from forbidden set cannot reconstruct original secret image information. So, Visual cryptography for GAS improves the security of system

D. Recursive Threshold Visual Cryptography Scheme

Abhishek Parakh and Subhash Kak proposed “Recursive threshold visual cryptography” [5]. The purpose of Recursive threshold visual cryptography is recursive hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step.

E. Halftone Visual Cryptography Scheme

Halftone visual cryptography uses halftoning technique to generate shares. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo proposed halftone visual cryptography [6]. In halftone visual cryptography a secret binary pixel is encoded into an array of sub pixels, called as halftone cell. It provide

better contrast and security level and also increases quality of the shares.

F. Visual Cryptography Scheme for Grey Images

All previous visual cryptography schemes were only limited to binary images. Chang-Chou Lin, Wen- Hsiang Tsai proposed visual cryptography for gray level images [7]. In this scheme a dithering technique is used to convert gray level image into approximate binary image. Then existing visual cryptography schemes for binary images are applied to create the shares.

G. Visual Cryptography Scheme for Color images

Verheul and Van Tilborg proposed first color visual cryptography scheme [8]. In this visual cryptography scheme one pixel is distributed into m sub pixels, and each sub pixel is splitted into c color regions. In each sub pixel, there is exactly one color region colored, and all the other color regions are black. F. Liu, C. K. Wu, X. J. Lin proposed a new approach for colored visual cryptography scheme [9]. They proposed three different approaches for color image representation:

- In first approach, colors in the secret image can be printed on the shares directly.
- In second approach separate three color channels are used. Red, green, blue for additive model and cyan, magenta, yellow for subtractive model. Then normal visual cryptography scheme for black and white images is applied to each of the color channels.
- In third approach, binary representation of color of a pixel is used and secret image is encrypted at bit-level.

H. Extended Visual Cryptography Scheme

Nakajima, M. and Yamaguchi, Y., developed Extended visual cryptography scheme (EVS) [12]. An extended visual cryptography (EVC) provide techniques to create meaningful shares instead of random shares of traditional visual cryptography and help to avoid the possible problems, which may arise by noise-like shares in traditional visual cryptography.

I. Hou's Color Visual Secret Sharing Scheme

Hou [5] proposed three color VC methods where the same technique is used 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 used 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 figure 2.

J. Region Incrementing Visual Cryptography Scheme

Ran-Zan Wang developed a scheme "Region Incrementing Visual cryptography" for sharing visual secrets of multiple secrecy level in a single image [14]. In this scheme, different regions are made of a single image, based on secrecy level and different encoding rules are applied to these regions.

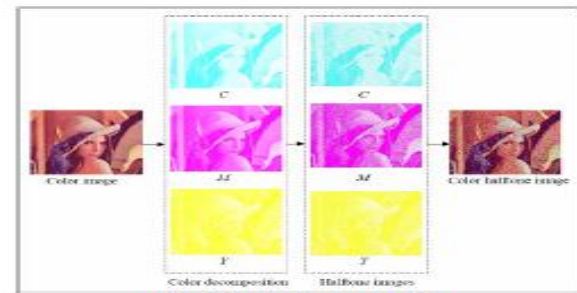


Fig. 2. Color decomposition

K. Segment based Visual Cryptography Scheme

Bernd Borchert proposed a new scheme which is not pixel-based but segment-based [15]. It is useful to encrypt messages consisting of symbols represented by a segment display. For example, the decimal digits 0, 1, ..., 9 can be represented by seven-segment display. The advantage of the segment-based encryption is that, it may be easier to adjust the secret images and the symbols are potentially easier to recognize for the human eye

III. METHODOLOGY

The methodology applied on this project can be described in 6 steps which is explain below:

Step 1. The source image is divided into primitive color (RGB) components.

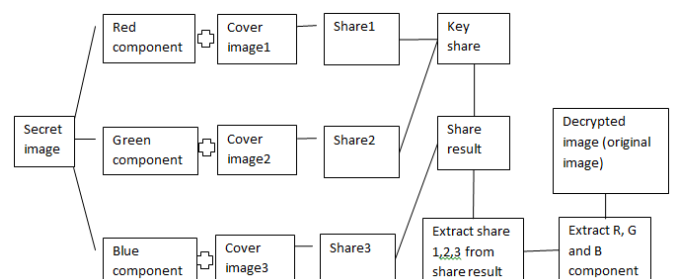
Step 2. Read three cover images cover1, cover2, cover3 this cover images is embedded to R, G, and B component consequently . Now we have 3 shares.

Step 3. Now starting 2 shares embedded with each other and form key share to provide extra security to the system

Step 4. Now embedded, key share with 3rd share.

Step 5. Now transmitting the result to the receiver with communication network.

Step 6. Receivers receive the message and extract the all three shares and extract the R, G, B component from the three shares respectively.



IV. CONCLUSION

Visual Cryptography is an exciting era of research where exists a lot of scope. Existing systems motivates us to improve the security of image for send over the network as well as secure sharing of key over the network. There is scope to automate the process of encryption for saving time and improve the quality of shares. Work can be done to improve quality of decrypted image at receiver side. Pixel expansion is

problem in various existing systems. Work can be done in n pixel expansion problem. Some technique can be made to improve the quality of resultant image and also to reduce the power consumption. In this we provided a detailed security visual cryptography algorithm for color image. The original secret image is color image and the adversary has acquired three of the R, G and B shares. Our results suggest that the security of the scheme depends critically on the color composition and distribution of the original secret image.

REFERENCES

- [1] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, issue 11, pp. 612-613, 1979.
- [2] G. R. Blakely, "Safeguarding cryptographic keys," *Proceedings of the National Computer Conference, American Federation of Information Processing Societies Proceedings*, vol. 48, pp. 313-317, 1979.
- [3] M. Naor and A. Shamir, "Visual cryptography," *In Proceedings of Advances in Cryptology, EUROCRYPT 94*, Lecture Notes in Computer Science, 950, pp. 1-12, 1995.
- [4] G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson, "Visual cryptography for general access structures," *Proceeding ICAL96*, Springer, Berlin, pp. 416-428, 1996.
- [5] A. Parakh and S. Kak "A recursive threshold visual cryptography scheme," CoRR abs/0902.2487, 2009.
- [6] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography," in *Proc. of IEEE International Conference on Image Processing*, Barcelona, Spain, vol. 1, pp. 521-52, 2003.
- [7] C. C. Lin and W. H. Tsai, "Visual cryptography for gray level images by dithering techniques," *Pattern Recognition Letters*, vol. 24, pp. 349-358, 2003.
- [8] E. Verheuland and H. V. Tilborg, "Constructions and properties of K out of N visual secret sharing schemes," *Designs, Codes and Cryptography*, vol. 11, issue 2, pp.179-196, 1997.
- [9] F. Liu, C. K. Wu, and X. J. Lin, "Colour visual cryptography schemes," *IET Information Security*, vol. 2, no. 4, pp. 151-165, 2008.
- [10] C. C. Wu and 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.
- [11] S. J. Shyu, S. Y. Huang, Y. K. Lee, R. Z. Wang, and K. Chen, "Sharing multiple secrets in visual cryptography," *Pattern Recognition*, vol. 40, issue 12, pp. 3633-3651, 2007.
- [12] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," *Journal of WSCG*, vol. 10, issue 2, pp. 303-310.
- [13] Y. C. Hou, "Visual cryptography for color images," *Pattern Recognition*, vol. 36, pp. 1619-1629, 2003.
- [14] R. Z. Wang, "Region incrementing visual cryptography," *SP Letters*, vol. 16, no. 8, pp. 659-662, 2009.
- [15] B. Borchert, "Segment-based visual cryptography," Universitat Tubingen, Germany, 2007.