ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 2, Issue 9, September 2013*

# AN OVERVIEW OF VARIOUS VISUAL CRYPTOGRAPHY SCHEMES

Suhas B. Bhagate [1], P.J.Kulkarni [2]

Department of Computer Science and Engineering, D.K.T.E.'s Textile and Engg Institute, Ichalkaranji, Maharashtra, India[1]

Deputy Director, Walchand College of Engineering, Sangli, Maharashtra, India[2]

**Abstract**: Information is increasingly important in our daily life. Information gets more value when shared with others. Due to advances in technologies related to networking and communication, it is possible to share the information like audio, video and image easily. It may give rise to security related issues. Attackers may try to access unauthorized data and misuse it. To solve this problem certain techniques are required. Techniques to provide security, while sharing information are termed as Secret sharing schemes. When it comes to visual information like image and video, it is termed as Visual secret sharing scheme. Visual cryptography (VC) is a technique used for protecting image-based secrets. The basic concept of visual cryptography scheme is, to split secret image into some shares, which separately reveals no knowledge about the secret information. Shares are then distributed to participants. By stacking these shares directly, secret information can be revealed and visually recognized. All shares are necessary to combine to reveal the secret image. Starting from the basic model, many visual cryptographic techniques have been evolved day by day.

**Keywords**: Information security, Secret sharing scheme, Visual Cryptography, Data hiding

## I. INTRODUCTION

Appropriate techniques are required to prevent illicit usage of information. Such techniques are called as Secret Sharing Schemes. G.R. Blakley and Adi Shamir independently invented secret sharing scheme in 1979[1, 2]. When it comes to visual information like image and video, it is termed as Visual secret sharing scheme. Visual cryptography (VC) is a technique used for protecting image-based secrets. Moni Naor and Adi Shamir proposed the basic model of visual cryptography [3]. The main concept of the original visual cryptography scheme is to encrypt a secret image into some shares. Secret information cannot be revealed with few shares. All shares are necessary to combine to reveal the secret image. There has been a steadily growing interest in visual cryptography. Visual cryptography is simple, secure and effective cryptographic scheme. Since the origin of this, various extensions have been developed to improve the things. These extensions to basic visual cryptography are outlined in this paper in Section II, which includes Basic visual cryptography model, (2, 2) Visual Cryptography Scheme, (k, n) visual cryptography scheme, Visual cryptography scheme for General Access Structure, Recursive Threshold Visual cryptography scheme, Halftone visual cryptography scheme, Visual Cryptography scheme for Grey images, Visual Cryptography scheme for color images, Multiple Secret Sharing Scheme, Extended Visual Cryptography scheme, Progressive Visual Cryptography scheme, Region Incrementing Visual Cryptography scheme and Segment based Visual Cryptography Scheme. Section III contains conclusion and future work.

## II. VARIOUS VISUAL CRYPTOGRAPHY SCHEMES

### A. *(2, 2) Visual Cryptography Scheme*

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

There are many techniques for encoding the pixels of original image. In a technique, in which each pixel in original image is represented by two sub-pixels in each share, while reading the pixels in original image, if a white pixel is encountered, one of the first two rows in Figure 1 is selected with probability 0.5, and the shares are assigned 2 pixel blocks as shown in the third and fourth columns in figure 1. Similarly, if a black pixel is encountered, one of the last two rows is selected with probability 0.5, from which a sub-pixel block is assigned to each share. When two shares are superimposed, if two white pixels overlap, the resultant pixel will be white and if a black pixel in one share overlaps

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 2, Issue 9, September 2013*

with either a white or black pixel in another share, the resultant pixel will be black.

This implies that the superimposition of the shares represents the Boolean OR function. The last column in Figure 1 shows the resulting sub-pixel when the sub-pixels of both the shares in the third and fourth columns are superimposed [3].

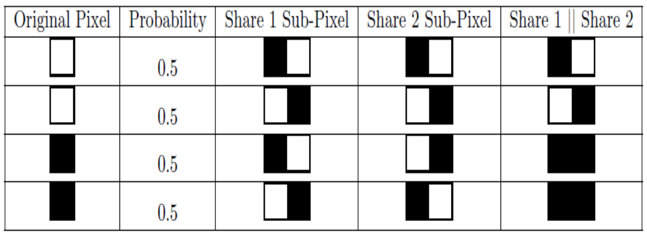


Figure 1: 2 out of 2 using 2 subpixels per original pixel

### B. (k, n) Visual Cryptography Scheme

In (2, 2) visual cryptography, both the shares are required to reveal secret information. If one share gets lost due to some technical problem, secret information cannot be revealed. So there is a restriction of keeping all the shares secure to reveal information and user can not afford to lose a single share. 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 can be generated from original image and distributed. Original image is recognizable only if k or more shares stacked together, where value of k is between 2 to n. If fewer than k shares stacked together, original image cannot be recognized. It gives flexibility to user. If user loses some of the shares still secret information can be revealed, if minimum k number of shares is obtained.

### C. Visual Cryptography Scheme for General Access Structure

In (k, n) visual cryptography scheme, all n shares have equal importance. Any k out of n shares can reveal the secret information. It may compromise the security of system. To overcome this problem, G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson extended (k, n) visual cryptography model to general access structure [4]. In general access structure scheme, given set of n shares 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 reveal secret information, but less than k shares from qualified subset of shares can not reveal any secret information. Even k or more shares from forbidden set can't reveal secret information. So, Visual cryptography for general access structure improves the security of system

### D. Recursive Threshold Visual Cryptography Scheme

In (k, n) visual secret sharing scheme, a secret of 'b' bits is distributed among 'n' shares of size at least 'b' bits each. Since only k out of n shares is needed to reveal secret, every bit of any share conveys at most 1/k bits of secret. It results in inefficiency in terms of number of bits of secret conveyed per bit of shares. To overcome this limitation Abhishek Parakh and Subhash Kak proposed "Recursive threshold visual cryptography" [5].

The basic idea behind Recursive threshold visual cryptography is recursive hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step, and thereby increasing the information, every bit of share conveys to (n-1)/n bit of secret which is nearly100%.

### E. Halftone Visual Cryptography Scheme

Halftone visual cryptography uses halftoning technique to create shares. Halftone is the reprographic technique. It simulates continuous tone imagery through the use of dots, which may vary either in size, in shape or in spacing. 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, in each of the 'n' shares. By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained. It maintains good contrast and security and increases quality of the shares.

### F. Visual Cryptography Scheme for Grey images

All previous visual cryptography schemes were only limited to binary images. These techniques were capable of doing operations on only black and white pixels. It is not sufficient for real life applications. 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

Visual cryptography schemes were applied to only black and white images till year 1997. 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 divided into c color regions. In each sub pixel, there is exactly one color region colored, and all the other color regions are black.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 2, Issue 9, September 2013*

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. It works similar to basic visual cryptography model. Limitations of this approach are large pixel expansion and quality of decoded image is degraded.
- 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. This approach reduces the pixel expansion but quality of image gets degraded due to halftoning process.
- In third approach, binary representation of color of a pixel is used and secret image is encrypted at bit-level. This results in better quality of image.

### *H. Multiple Secret Sharing Scheme*

All the previous researches in visual cryptography were focused on securing only one image at a time. Wu and Chen [10] were first researchers, who developed a visual cryptography scheme to share two secret images in two shares. In this scheme, two secret binary images can be hidden into two random shares, namely A and B, such that the first secret can be seen by stacking the two shares, denoted by $A \otimes B$, and the second secret can be obtained by rotating A by 90 degree anti-clockwise. J Shyu et al [11] proposed a scheme for multiple secrets sharing in visual cryptography, where more than two secret images can be secured at a time in two shares.

### *I. Extended Visual Cryptography Scheme*

In traditional visual cryptography scheme, shares are created as random patterns of pixel. These shares look like a noise. Noise-like shares arouse the attention of hackers, as hacker may suspect that some data is encrypted in these noise-like images. So it becomes prone to security related issues. It also becomes difficult to manage noise-like shares, as all shares look alike. 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.*

### *J. Progressive Visual Cryptography Scheme*

In (k, n) visual secret sharing scheme, it is not possible to recover the secret image though one less than k shares are available. This problem is solved in progressive visual cryptography scheme developed by D. Jin, W. Q. Yan, and M. S. Kankanhalli [13].

In progressive visual cryptography scheme, it is not necessary to have at least k shares out of n, as in (k, n) secret sharing scheme. If more than one share obtained, it starts recovering the secret image gradually. The quality of recovered image improves, as the number of shares received increases.

### *K. Region Incrementing Visual Cryptography Scheme*

In traditional visual cryptography scheme, one whole image is considered as a single secret and same encoding rule is applied for all pixels of one image. So it reveals either entire image or nothing. It may be the situation that different regions in one image can have different secrecy levels, so we can't apply same encoding rule to all pixels. 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.

### *L. Segment based Visual Cryptography Scheme*

Traditional visual cryptography schemes were based on pixels in the input image. The limitation of pixel based visual cryptography scheme is loss in contrast of the reconstructed image, which is directly proportional to pixel expansion. 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 and it may be easier for a non-expert human user of an encryption system to understand the working.

## III. CONCLUSION

Providing security to the digital information shared in day to day life is an important issue in real life. Since the origin of Visual cryptography, various extensions have been developed to improve the things, ranging from (2, 2), (k, n) to progressive visual cryptography models, black and white to color images and random dot like shares to meaningful shares. Many researches carried out on these extensions, still there is much scope to do research in progressive visual cryptography, Region Incrementing Visual Cryptography, Segment based Visual Cryptography Scheme and overcome the common limitations of these techniques like large pixel expansion and lower contrast.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 2, Issue 9, September 2013*

## REFERENCES

[1] Shamir, A. 1979. How to Share a Secret. Communications of the ACM. 22: 612-613.
[2] Blakely, G. R. 1979. Safeguarding Cryptographic Keys. Proceedings of the National Computer Conference, American Federation of Information Processing Societies Proceedings. 48: 313-317.
[3] Moni Naor and Adi Shamir, “Visual cryptography”. In Proceedings of Advances in Cryptology, EUROCRYPT 94, Lecture Notes in Computer Science, 1995, (950):pp. 1-12.
[4] G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson, “Visual cryptography for general access structures”, Proc.ICAL96,Springer, Berlin,1996,pp.416-428.
[5] Abhishek Parakh and Subhash 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,Sept 2003, vol. 1, pp. 521–52
[7] Chang-Chou Lin, Wen-Hsiang Tsai, “Visual cryptography for gray-level images by dithering techniques”, Pattern Recognition Letters, v.24 n.1-3.
[8] E. Verheuland H. V. Tilborg, ”Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes.”Designs, Codes and Cryptography, 11(2), pp.179–196, 1997.
[9] F. Liu, C.K. Wu, X.J. Lin, “Colour Visual Cryptography Schemes”, IET Information Security, vol. 2,No. 4, pp 151-165, 2008.
[10] 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.
[11] S. J. Shyu, S. Y. Huanga,Y. K. Lee, R. Z. Wang, andK. Chen, “Sharing multiple secrets in visual cryptography”, Pattern Recognition, Vol. 40, Issue 12, pp. 3633 - 3651, 2007.
[12] Nakajima, M. and Yamaguchi, Y., “Extended visual cryptography for natural images” Journal of WSCG. v10 i2. 303-310.
[13] . Jin, W. Q. Yan, and M. S. Kankanhalli, “Progressive color visual cryptography,” J. Electron. Imag., vol. 14, no. 3, pp. 1–13, 2005.
[14] Wang, R.Z.[Ran-Zan], “Region Incrementing Visual Cryptography”, SPLetters(16), No. 8, August 2009, pp. 659-662.
[15] Bernd Borchert, “Segment-based Visual Cryptography”, WSI 2007ISSN 0946-3852