"Survey of Visual Cryptography Schemes"

Shital B. Patel[1] & Pooja D. Pancholi[2]
[1,2]Assistant Professor, Department of Compute Science, Ganpat University.

Received: July 01, 2018 Accepted: August 24, 2018

ABSTRACT *In today's world handling and security of information from attacks becomes very important aspect for the individuals. Researchers are innovating new techniques to secure the information from unwanted intrusions. Various cryptography techniques are discovered and many are yet to be revealed. Visual cryptography scheme is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes, and picture) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. There are various measures on which performance of visual cryptography scheme depends, such as pixel expansion, contrast, security, accuracy, computational complexity, share generated is meaningful or meaningless, type of secret images(either binary or color) and number of secret images(either single or multiple) encrypted by the scheme. Intent of this paper is on study and performance analysis of various visual cryptography schemes on the basis of pixel expansion, number of secret images, image format and type of shares generated.*

Keywords: *"Visual cryptography, contrast, pixel expansion, Secret sharing, shares;"*

1. INTRODUCTION

Visual Cryptography (VC), first proposed in 1994 by Naor and Shamir [1], is a secret sharing scheme, based on black and white or binary images. Secret images are divided into share images which, on their own, reveal no information of the original secret. Shares may be distributed to various parties so that only by collaborating with an appropriate number of other parties, can the resulting combined shares reveal the secret image. Recovery of the secret can be done by superimposing the share images and, hence, the decoding process requires no special hardware or software and can be simply done by the human eye.

To illustrate the principles of Visual Security (VS), consider a simple 2-out-of-2 VC scheme shown in Fig. 1. Each pixel 'p' of the secret image is encrypted into a pair of sub pixels in each of the two shares. If 'p' is white, one of the two columns under the white pixels in Fig. 1 is selected. If 'p' is black, one of the two columns under the black pixels are selected. The first two pairs of sub pixels in the selected columns are assigned to share 1 and share 2 respectively. Since in each shares, p is encrypted into black and white or white and black pair of sub pixels, an individual share gives no clue about the secret image. Now consider the superposition of the two shares as shown in the last row of Fig. 1.

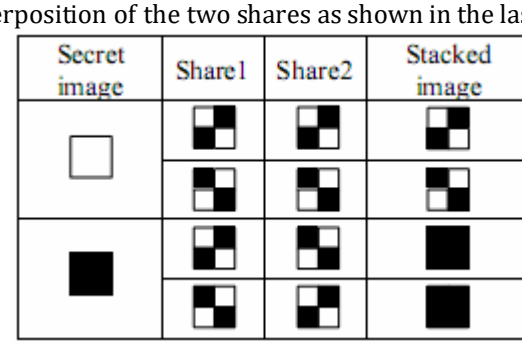

Fig.1 Sharing and Stacking scheme of Black and White Pixel.

If 'p' is white it always output one black and one white sub pixel during encryption. If 'p' is black, it outputs two black sub pixels. Fig. 2 shows an example of the application of the 2-out-of-2 VS scheme. Fig. 2(a) shows a secret binary image to be encoded. According to the encoding rule shown in Fig. 1, each pixel of image is split into two subpixels in each of the two shares, as shown in Fig. 2(b) and (c). Superimposing the two shares leads to the output secret image shown in Fig. 2(d). The decoded image is clearly identified, although some contrast loss occurs.

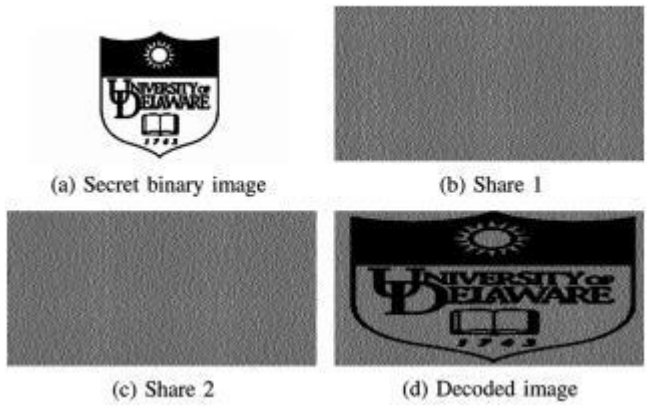

Fig. 2. Example of 2-out-of-2 scheme.

Based on the principle of, halftone visual cryptography has been proposed in void and cluster algorithm [3] to produce meaningful halftone image for the shares in the VC scheme. Halftone visual cryptography utilizes the void and cluster algorithm to encode a secret binary image into n halftone shares carrying significant visual information. Using the void and cluster algorithm to find positions for the secret pixels in the halftone cell, however, is computationally expensive. This paper is follow section II introduce various visual cryptography schemes such as (2,2) visual cryptography scheme,(k,n) visual cryptography scheme, visual cryptography scheme for general access structure, recursive threshold scheme, halftone visual cryptography scheme, visual cryptography for grey images, color images, extended visual cryptography scheme, segment base visual cryptography scheme ,section III contains comparative analysis of various visual cryptography scheme and section IV contains conclusion of paper.

2. 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 [1].

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 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 [1].

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 [1]. In (k, n) visual cryptography scheme, n shares can be generated from original image and distributed. Original image is recognizable only if k or m ore 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 [2]. 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 Gray 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 [6]. 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 [7]. 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.

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 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⊗ B, and the second secret can be obtained by rotating A by 90 degree anti-clockwise. J Shyu et al [9] 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) [8].

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 [10].

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 [11]. 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 [12].

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.

3. COMPARATIVE ANALYSIS OF VARIOUS VISUAL CRYPTOGRAPHY SCHEME

G. Ateniese, C. Blundo, A.DeSantis, and D. R. Stinson give a general access structure [4]. In which given set of n shares is divided into two subsets namely qualified and forbidden subset of shares as per the importance of shares. Any subset of 'k'or more qualified shares can decrypt the secret image but no information can be obtain by stacking lesser number of qualified shares or by stacking disqualified shares. Until year 1997 visual cryptography schemes were applicable to only black and white images.

Zhou, Arce, Gonzalo R, et al. [3] in "Halftone Visual Cryptography" presented halftone visual cryptography which increases the quality of the meaningful shares. In halftone visual cryptography a secret pixel 'P' is encoded into an array of Q1 X Q2 sub pixel, referred to as halftone cell, in each of the 'n' shares. By using halftone cells with an appropriate size, maintains contrast and security. Utilize Void and Cluster algorithm to encode a secret binary image into n halftone share.

Nakajima, M. and Yamaguchi, Y. [8],developed Extended visual cryptography scheme (EVS).

An EVC provide technique 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.

Chang-Chou Lin and Wen-Hsiang Tsai[6], "Visual Cryptography for gray-level images by dithering techniques" given new dithering techniques instead of using gray pixel directly to construct shares, A dithering technique is used to convert gray level images into approximate binary images. Then existing visual cryptography schemes for binary images are applied to accomplish the work of creating the shares.

Chavan and Mangrulkur [13] in "Encrypting Information Color Image using Color Visual Cryptograph " use algorithm that generate red, green , blue and alpha components for each pixel of an input image. That also removed basic limitation of VC regarding expansion of original image, The size of original and reconstructed images are same.

Sandeep Katta[14] in "Recursive Information Hiding in Visual Cryptography" presented to solve the problem by hiding of smaller secret in shares of larger secret with secret sizes doubling at every step. When recursive threshold visual cryptography is used in network application, network load is reducing. After simulation result the contrast will be loss. Applied algorithm use numbers of parameters and analysis reveal image.

V Hemanth, M Shareef and K S Ranjith in "Anti-Phishing uses Visual Cryptography" they introduced solution for anti-phishing with the help of visual cryptography. Using visual cryptography the security of the online banking system has been increased to some extent. By implementing the above technique the phishing attack can be eradicated. Identify how to phishing attacks occur, how to identify an E-mail is Fraud.

P.R.Sushma Priya and P.Vijaya Bharati[15] in "Transmission of cryptic Text using Rotational Visual Cryptography" proposed an empirical model of secure data transmission technique with a hybrid approach of cryptography , stenography and rotational analysis. Performance is efficient than the traditional approach.

Sesha Pallavi and Avadhani P [12] in "Segment based Visual Cryptography for key distribution" Visual Cryptography is presented by segment based instead of pixel based. The key (secret) which is in the form of digit that is to be distributed is converted in to segment display then encrypted. Segment displays are used more in electronic devices like digital clocks, electronic meters and other devices for displaying numerical information.

V.Chinnapudevi and Dr.Narsing Yadav[16] in " Analysis of Visual Cryptography Schemes Using Adaptive Space Filling Curve Ordered Dithering" implemented ASFCOD algorithm and applying that into halftone image. Using this algorithm it can reduce the size of the decrypted image. and quality of decrypted image can be increase . In this paper they are evaluated picture quality to tested some parameter like Mean Square error (MSE) , PSNR , Average Difference (AV) , Maximum Difference (MD) and Mean Absolute Error(MAE) . These are the different parameter calculated and apply in various algorithms and after that the evaluated picture quality.

Mohammad Soltani[17] in "A New Secure Image Encryption Algorithm using Logical and Visual Cryptography Algorithms and based on Symmetric Key Encryption" which has been demonstrated on framework in C Sharp using Dot Net framework, Object Oriented Programming , Random numbers and bitmap object. The result obtain by testing on that platform instances have performance of this algorithm.

Navjot Kaur and Dr. Rajiv Mahajan[18] in "A survey on Embedded Extended Visual Cryptography scheme" review various techniques for Extended Visual Cryptography (EVCS) and implementing two phases like a covering shares and Embedding VCS into covering shares. They measured share quality by two quantities PSNR and QUI. The proposed scheme has ability of providing better visual quality of shares which is competitive as compared with other embedded extended cryptography scheme.

Kaffri and keren [19] presented "A random grid based visual cryptography technique", In this method size of pixel is same as original image pixel size that means relieved secret image size and original image size is same so it reduces the problem of pixel expansion. In this method random grid R is defined as a two dimension. In this method random grid R is defined as a two dimensional array of pixels. Each pixel is either transparent (white) or opaque (black) by a coin-flip procedure. The numbers of transparent pixels and opaque pixels are probabilistically same and the average opacity of a random grid is 50%.

4. CONCLUSION

In this paper we review the existing techniques of visual cryptography. We were discussed a various visual cryptography techniques such as (2, 2) Visual Cryptography Scheme, Halftone visual cryptography scheme, Visual Cryptography scheme for Grey images, Multiple Secret Sharing Scheme, Extended Visual Cryptography scheme, Threshold Visual Cryptography Scheme , Visual secret sharing scheme ,Natural image based visual secret sharing scheme. For each technique we have provided a detailed explanation of the techniques which are used to provide security for the secret image. From this analysis, a number of shortcomings and limitations were highlighted of these techniques. Visual secret sharing scheme suffers from quality of image when share are marge.

REFERENCES

1. Naor, M., & Shamir, A. (1994, May). Visual cryptography. In Workshop on the Theory and Application of of Cryptographic Techniques (pp. 1-12). Springer, Berlin, Heidelberg.
2. Zhou, Z., Arce, G. R., & Di Crescenzo, G. (2006). Halftone visual cryptography. IEEE transactions on image processing, 15(8), 2441-2453.
3. Wang, Z., Arce, G. R., & Di Crescenzo, G. (2009). Halftone visual cryptography via error diffusion. IEEE transactions on information forensics and security, 4(3), 383-396.
4. Ateniese, G., Blundo, C., De Santis, A., & Stinson, D. R. (1996). Visual cryptography for general access structures. Information and Computation, 129(2), 86-106.
5. Parakh, A., & Kak, S. (2009). A recursive threshold visual cryptography scheme. arXiv preprint arXiv:0902.2487.
6. Lin, C. C., & Tsai, W. H. (2003). Visual cryptography for gray-level images by dithering techniques. Pattern Recognition Letters, 24(1-3), 349-358.

7. Verheul, E. R., & Van Tilborg, H. C. (1997). Constructions and properties of k out of n visual secret sharing schemes. Designs, Codes and Cryptography, 11(2), 179-196.
8. Nakajima, M., & Yamaguchi, Y. (2002). Extended visual cryptography for natural images.
9. Shyu, S. J., Huang, S. Y., Lee, Y. K., Wang, R. Z., & Chen, K. (2007). Sharing multiple secrets in visual cryptography. Pattern Recognition, 40(12), 3633-3651.
10. Hou, Y. C., & Quan, Z. Y. (2011). Progressive visual cryptography with unexpanded shares. IEEE transactions on circuits and systems for video technology, 21(11), 1760-1764.
11. Gupta, A., & Saxena, K. (2014, November). Region incrementing visual cryptography. In Medical Imaging, m-Health and Emerging Communication Systems (MedCom), 2014 International Conference on (pp. 247-250). IEEE.
12. Borchert, B. (2007). Segment-based visual cryptography.
13. Lin, C. C., & Tsai, W. H. (2003). Visual cryptography for gray-level images by dithering techniques. Pattern Recognition Letters, 24(1), 349-358.
14. Katta, S. (2010). Recursive information hiding in visual cryptography. preprint arXiv:1004.4914.
15. Priya, P. S., & Bharati, P. V. TRANSMISSION OF CRYPTIC TEXT USING ROTATIONAL VISUAL CRYPTOGRAPHY. network security, 6, 7.
16. Chinnapudevi, V., & Yadav, M. N. Analysis of Visual Cryptography Schemes Using Adaptive Space Filling Curve Ordered Dithering.
17. Soltani, M. (2013). A New Secure Image Encryption Algorithm using Logical and Visual Cryptography Algorithms and based on Symmetric Key Encryption.
18. Kaur, N., & Mahajan, R. A Survey on Embedded Extended Visual Cryptography Scheme.
19. Chen, T. H., & Tsao, K. H. (2011). User-friendly random-grid-based visual secret sharing. IEEE Transactions on Circuits and Systems for Video Technology, 21(11), 1693-1703.