ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 8, Issue, 06, pp.32445-32449, June, 2016

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

A REVIEW PAPER ON VARIOUS VISUAL CRYPTOGRAPHY SCHEMES

[1]Mr. K. Das and [*,2]Prof. S. K. Bandyopadhyay

[1]Department of Information Technology, St. Thomas College of Engineering and Technology Kolkata, India
[2]Department of Computer Science and Engineering, University of Calcutta, India

ARTICLE INFO

Article History:
Received 23rd March, 2016
Received in revised form
10th April, 2016
Accepted 26th May, 2016
Published online 15th June, 2016

Key words:

Visual Cryptography, Cipher Image, Secret Sharing, Shares, Natural Images, Security, Data Hiding, Quality, Computational Complexity, Multiple Images, Pixel.

ABSTRACT

Visual cryptography is special type of technique for encipher the confidential visual information (e.g. printed text, handwritten notes, and picture) in such a way, that decipher can be performed by an authorized user with the help of human visual system (HVS) without any complex process. It also provides high security, so that hackers cannot observe any clues about a secret image from individual cover images. 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, gray 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 the visual cryptography schemes and also a comparative analysis on various visual cryptography schemes.

Citation: Mr. K. Das and Prof. S. K. Bandyopadhyay, 2016. "A review paper on various visual cryptography schemes", *International Journal of Current Research*, 8, (06), 32445-32449.

INTRODUCTION

In recent days, security is a big threat in the transmission medium due to the development of the Internet and multimedia contents such as audio, image, video etc. For transmitting secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want. To deal with the security problems of secret images, various image secret sharing schemes have been developed which gave rise to new technologies in the area of Image Cryptography which would require less computation and less storage. Naorand Shamir (1995) proposed the concept of Visual cryptography (VC) which allows the encryption of secret information in the image form. Visual cryptography is a technique that encrypts a secret image into n shares with each participant holding one or more shares. By using the concept of visual cryptography, a secret image was broken up into some shares and then distributed to the n participants. By stacking their n shares, the secret information can be revealed and visually recognized by human visual system.The first form of visual cryptography is also known as secret sharing.

Corresponding author: Prof. S. K. Bandyopadhyay
Department of Computer Science and Engineering, University of Calcutta, India.

The simplest form of visual cryptography separates a secret image into two parts so that either part by itself conveys no information. When these two parts are combined together by means of superimposition, the original secret can be revealed. These parts are called as shares. There are several advantages of visual cryptography. Basically it is simple to use and no mathematical computations are required to reveal the secret. Secondly, the individuals who do not have knowledge of cryptography are indirectly getting involved in decryption.

Most of these studies, however, concentrate on binary images; few of them proposed methods for processing gray-level and color images. Most of the techniques which are employed on color images such as do not give the original image back. This paper provides overview of various visual cryptography schemes.

I.A Broad Review on Visual Cryptography Schemes

Many authors has published different Visual Cryptography Schemes for different applications. Each scheme has its own advantages and disadvantages. Few such schemes are mentioned below.

Black and White Visual Cryptography Scheme

a) Single Secret Sharing Scheme

The concept of visual cryptography was first proposed by Naor and Shamir (1995) in 1994. Naor and Shamir proposed a k out of n scheme where for a given message, n transparencies will be generated and it is impossible to get any information about the secret images from individual shares. The original message is visible if any k (or more) of them are stacked together, but totally invisible if fewer than k transparencies are stacked together (or analyzed by any other method).The original encryption problem can be considered as a 2 out of 2 secret sharing problem. In (2, 2) Visual Cryptography Scheme each pixel P is split into two pixels in each of the two shares (each such pixel in the shares is called sub pixel) by following any one row of the corresponding pixie in Figure 1. If P is white, then a row is chosen randomly from one of the first two rows in the Figure 1. If P is black, then a row is chosen randomly from one of the last two rows in the Figure 1.

Pixel	Probability	$Share_1$	$Share_2$	$Share_1 \otimes Share_2$
□	50%	■□	■□	■■
	50%	□■	□■	□■
■	50%	■□	□■	■■
	50%	■□	■□	■■

Figure 1. Naor and Shamir's scheme for encoding a binary pixel into two shares

Now when two shares are superimposed the black pixels in the secret image we will get two black pixels whereas the white pixels will result in one white and one black pixel as shown in the last column of Figure1. Thus we can say that in this particular case the reconstructed pixel has grey level of 1 if P is black and a grey level of 1/2 if P is white.

The advantage of the above scheme is that the decoding can be performed without any cryptographic computations in a simple way. But it lacks in balancing the contrast of the decoded image with respect to the original one, so the recovered image can't be reused.

Fig 2a. Original Image

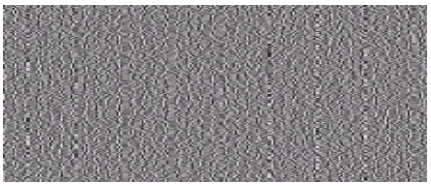

Fig 2b. Share1

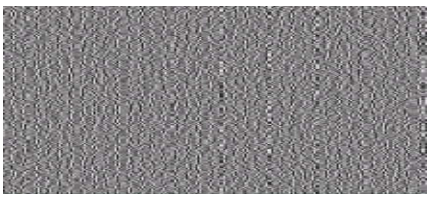

Fig 2c. Share 2

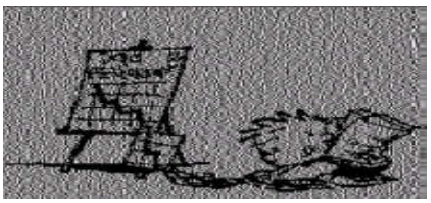

Fig 2d. Output of the Superimposed Shares

Figure 2. Example of (2, 2) Visual Cryptography Scheme (Moni Naor and Adi Shamir, 1995)

Balancing the performance between pixel expansion and contrast Liguo Fang (2006) recommended a (2, n) scheme based on combination

Both the schemes satisfy the security requirement for protecting secret content, but they suffer from transmission risk problem because holding noise like shares will cause hacker's suspicion and share may be intercepted.To conceal a binary image into two meaningful shares Chin-Chen Chang *et al*.(2005) suggested a spatial-domain image hiding scheme. Here the generated shares are embedded into two gray level cover images. To decode the hidden messages, the extracted shares from the secret-share-carrier images (namely the embedding images) need to be superimposed. The advantage of the scheme is simple computation and good security, and thus it is very suitable for applications involving low power verification systems.

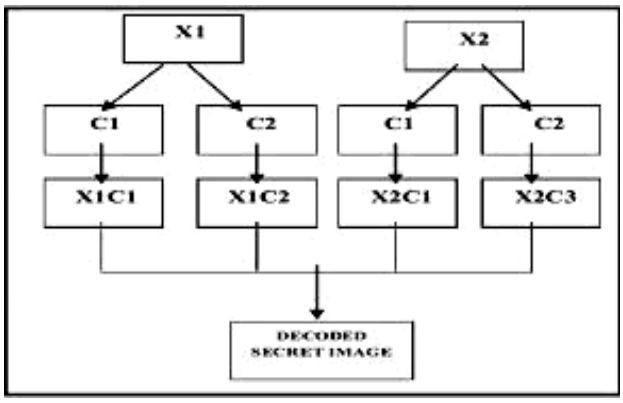

Figure 3. Block diagram of the scheme suggested by Chin-Chen Chang (2005)

X1, X2: Share Images, C1, C2: Cover Images

Xiao-Qing and Tan (2009) has suggested threshold visual secret sharing schemes mixed XOR and OR operation with reversing and based on binary linear error-correcting code. They show that 2 out of 2 schemes mixed on XOR and OR operation with reversing where the reconstruction of both black and white pixels is perfect.

All these are suitable for binary images only. For other cases large numbers of shares have to be produced.

b) Multiple Secrets Sharing Scheme

All the previous researches in visual cryptography, only one image can be secured at a time. Wu and Chen (1998) were first researchers to present the visual cryptography schemes to share two secret images in two shares. In this scheme, two secret binary images can be hidden into two random shares. They are denoted as A and B. By stacking the two shares can be seen in the first secret denoted by A B. For rotating A by Θ anti-clockwise the second secret can be obtained. They designed the rotation angle Θ to be 90 . However, it is easy to obtain that Θ can be 180 or 270 .

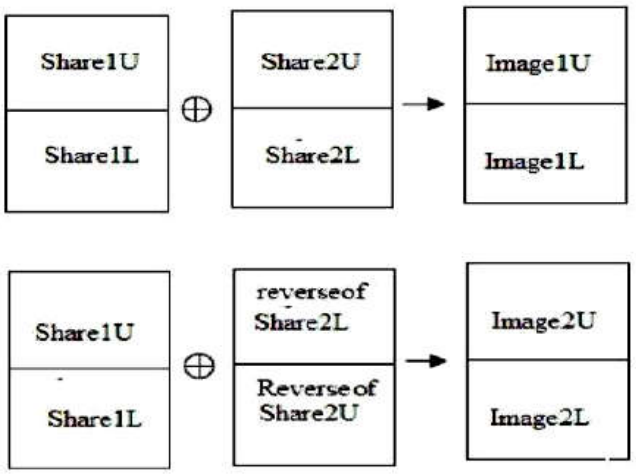

Figure 4. Block diagram of the scheme suggested by Wu and Chen (1998)

To overcome the angle restriction of Wu and Chen's scheme (1998), Hsu *et al*. (2004) proposed a scheme to hide two secret images in two rectangular share images with arbitrary rotating angles. Wu and Chang (2005) also refined the idea of Wu and Chen (1998) by encoding shares to be circles so that the restrictions to the rotating angles (Θ = 90 , 180 or 270) can be removed.

B. Gray Image Sharing Schemes

When more colors are there in the secret image the larger the size of shares will become. To beat this limitation developed a secret color image sharing theme supported modified visual cryptography. Chen Chang *et al*. (2002) suggested a scheme which provides a more efficient way to hide a gray image (256 colors) in different shares. In this scheme size of the shares is fixed; it does not vary when the number of colors appearing in the secret image differs. Scheme does not require any predefined Color Index Table. Though pixel expansion is a fixed in this scheme is not suitable for true color secret image. Tzung-Her Chen *et al*. (2008) offered the multiple image encryption schemes by rotating random grids, without any pixel expansion and codebook redesign. The new scheme encrypts two secret images into two random grids without any pixel expansion and, later, decrypts the original secrets by directly stacking two random grids in an additional way of rotating one random grid at 90°, 180° or 270° degrees. It not only reduces the pixel expansion but also raises the capacity of secret communication.

To improve the speed of encoding Haibo Zhang *et al*. (2008) presented a multi-pixel encoding which can encode variable number of pixels for each run. The length of encoding at one run is equal to the number of the consecutive same pixels met during scanning the secret image. The proposed scheme can work well for general access structure and chromatic images without pixel expansion.

C. Color Image Sharing Schemes

a) Single Secret Sharing

Until the year 1997 visual cryptography schemes were applied to only black and white images. First colored visual cryptography scheme was developed by Verheul and Van Tilborg (1997). Colored secret images can be shared with the concept of arcs to construct a colored visual cryptography scheme. In the c-colorful visual cryptography scheme one pixel is transformed into the m sub pixels, and each sub pixel is divided into the c color regions. In each and every sub pixel, there is exactly one color region is colored, and all the other color regions are black. The color of one pixel depends on the inter relationships between the stack sub pixels. In this colored visual cryptography scheme with c colors, the pixel expansion m is c*3.

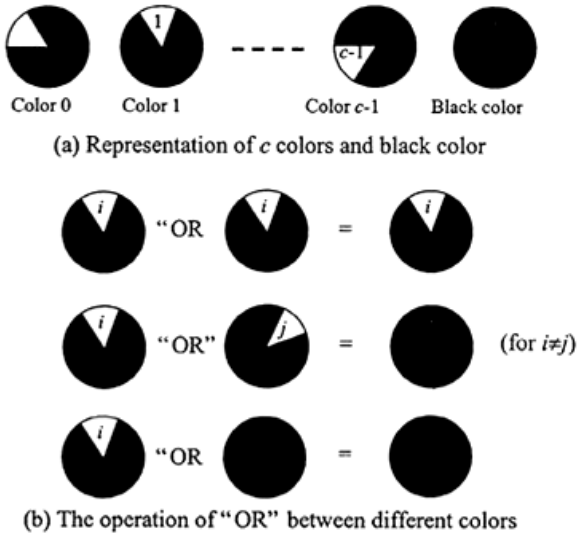

Figure 5. Infrastructure of colored subpixels and its OR operations in Verheul-Van Tilborg Scheme

Table 1. Comparison of visual cryptography schemes on the basis of number of secret images, pixel expansion, image format, type of share generated

Authors Year	Pixel Expansion(m)	Number of Secret Images	Image Format	Type of Share generated
Naor and Shamir, 1995	4	1	Binary	Random
Liguo Fang, 2006	2	1	Binary	Random
Chin-Chen Chang, 2005	4	1	Binary	Meaningful
Xiao-Qing, 2009	1	1	Binary	Random
Wu and Chen, 1998	4	2	Binary	Random
Hsu *et al*. 2004	4	2	Binary	Random
Wu and Chang, 2005	4	2	Binary	Random
Chin Chen Chang *et al*. 2002	9	1	Gray	Meaningful
Tzung-Her Chen *et al*. 2008	1	2	Gray	Random
Haibo Zhang *et al*. 2008	1	1	Gray	Random
Verheuland, 1997	C*3	1	color	Random
Yang and Liah, 2000	C*2	1	Color	Random
Chang and Tsai, 2000	529	1	Color	Meaningful
Tzung-Her Chen *et al*. 2008	4	n(n>=2)	Color	Random

Yang and Laih (2000) proposed a scheme which improves the pixel expansion to c*2. The scheme was implemented on basis of a black & white VSS scheme and got much better block length than the Verheul-Van Tilborg scheme (Verheul and Tilborg, 1997). But in both of these schemes share generated were meaningless.

For sharing a secret color image and also to generate the meaningful share to transmit secret color image Chang and Tsai (2000) anticipated color visual cryptography scheme. For a secret color image two effective color images are chosen as cover images which are the exactly same size of the secret color image. Then according to a predefined Color Index Table, the secret color image will be concealed into two disguise images. In this scheme also number of sub pixels is in proportional to the number of colors in the secret image as in the previous schemes. The only disadvantage of this scheme is that extra space is required to accumulate the Color Index Table.

b) Multiple Secrets Sharing Scheme

Tzung-Her Chen *et al*. (2008) anticipated a multi-secrets visual cryptography which is extended from traditional visual secret sharing. The codebook of traditional (2,2) VSS is used to generate share images macro block by macro block in such a way that multiple secret images are turned into only two share images and decode all the secrets one by one by stacking two of share images in a way of shifting. This scheme can be used for multiple binary, gray and color secret images with pixel expansion of 4.

III. Performance Analysis

Performance of the visual cryptography scheme is evaluated on the basis of some parameters which are recommended by the researchers are as follows. Naor and Shamir (1995) has suggested two main parameters they are pixel expansion m and contrast α. Pixel expansion m refers to the number of subpixels in the generated shares that represents a pixel of the original input image. It shows the loss in resolution from the original picture to the shared one. Contrast α is the difference in weight between combined shares that come from a white pixel and a black pixel in the original image. Accuracy is considered to be the quality of the reconstructed secret image and evaluated by peak signal-to-noise ratio (PSNR) measure. Computational complexity concerns the total number of operators required both to generate the set of n shares and to restructure the original secret image.

***Abbreviations in Visual Cryptography Schemes*:** m indicates pixel expansion of corresponding visual cryptography schemes, C number of colors in visual cryptography schemes, n is the number of shares.

IV. Directions for future research

Currently, many new schemes are proposed in the field of Color Visual Cryptography. We have seen that all the schemes discussed above, use Naor and Shamir's (1995) basic model of visual cryptography as the basis. But at the same time, the shares produced by all the methods above are either meaningless or are dependent upon some factors like the number of colors in the secret image. All those schemes generating meaningful shares may suffer from transmission risk problem because holding noise like shares will cause hacker's suspicion and share may be intercepted. To fill in this security gap, meaningful shares should be produced.As shown in the Table1 only few visual are a cryptography schemes achieve minimum pixel expansion.

From this analysis, a number of shortcomings and limitations were highlighted of these techniques. If for all the cases (binary, gray and color images) we perform encryption and hiding at the same time, organically combining steganography and cryptography, then this security hazard can be avoided. For more security purpose symmetric key algorithm can be applied in VCS. The transmission risk problem can also be solved very easily using Natural image based visual secret sharing scheme.

V. Conclusion

In this paper, we briefly review the research of visual cryptography schemes as special cases of secret sharing methods among participants. Their performance is evaluated on four criteria: number of secret images, pixel expansion, image format and type of share generated. The schemes (Moni Naor

and Adi Shamir, 1995; Liguo Fang and BinYu, 2006; Chin-Chen Chang *et al*., 2005; Xiao-Qing, 2009; Wu and Chen, 1998; Hsu *et al*., 2004; Wu and Chang, 2005) describe binary image sharing, (Chin-Chen Chang and Tai-Xing Yu, 2002; Chen *et al*., 2008; Zhang *et al*., 2008) describe gray image sharing and (VerheulandTilborg, 1997; Yang and Laih, 2000; Chang *et al*., 2000; Tzung-Her Chen *et al*., 2008) describe color image sharing schemes. The summary of all those VCS are represented in Table1. The comparative study of different visual cryptography techniques will help us to find better method to provide security.

Acknowledgment

F. A. Author thanks to the anonymous referees for their valuable suggestions and comments.

REFERENCES

ChangC., 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.

ChenT. H., K. H. Tsao and K. C. Wei, "Multiple-Image Encryption by Rotating Random Grids," 2008 Eighth International Conference on Intelligent Systems Design and Applications, Kaohsiung, 2008, pp. 252-256.

Chin-Chen Chang and Tai-Xing Yu, "Sharing a secret gray image in multiple images," Cyber Worlds, 2002. Proceedings. First International Symposium on, 2002, pp. 230-237.

Chin-Chen Chang, Jun-Chou Chuang, Pei-Yu Lin, "Sharing A Secret Two-Tone Image In Two Gray-Level Images", Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05), 2005, pp. 300-304.

HsuH. C., T.-S. Chen, Y.-H. Lin, "The Ring Shadow Image Technology Of Visual Cryptography By Applying Diverse Rotating Angles To Hide The Secret Sharing", In Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control, Taipei, Taiwan, March 2004, pp. 996–1001.

Liguo Fang, BinYu, "Research On Pixel Expansion Of (2, n) Visual Threshold Scheme", 1st International Symposium on Pervasive Computing and Applications, IEEE, 2006, pp. 856-860.

Moni Naor and Adi Shamir, "Visual Cryptography", *advances in cryptology– Eurocrypt*, 1995, pp 1-12.

Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multi-Secrets Visual Secret Sharing", Proceedings of APCC2008, IEICE, 2008.

VerheulandE., 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.

Wu C.C., 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

Wu H.C., C.-C.Chang, 2005. "Sharing Visual Multi-Secrets Using Circle Shares", *Comput. Stand. Interfaces,* 134 (28), pp.123–135.

Xiao-Qing, T., "Two Kinds of Ideal Contrast Visual Cryptography Schemes," 2009. International Conference on Signal Processing Systems, Singapore, 2009, pp. 450-453.

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

ZhangH., X. Wang, W. Cao and Y. Huang, "Visual Cryptography for General Access Structure by Multi-pixel Encoding with Variable Block Size," Knowledge Acquisition and Modeling, 2008. KAM '08. International Symposium on, Wuhan, 2008, pp. 340-344.

****