Survey of Visual Cryptography Schemes

P.S.Revenkar, Anisa Anjum, W .Z.Gandhare
Government College of Engineering, Aurangabad, M.S., India
prevankar@gmail.com, anisa.anjum@gmail.com,wzgandhare@yahoo.com

Abstract

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 the visual cryptography schemes on the basis of pixel expansion, number of secret images, image format and type of shares generated.

Keywords: *visual cryptography scheme (VCS), pixel expansion, contrast, security, accuracy, computational complexity.*

1. Introduction

With the rapid advancement of network technology, multimedia information is transmitted over the Internet conveniently. Various confidential data such as military maps and commercial identifications are transmitted over the Internet. While using 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.

Visual cryptography is introduced by first in 1994 Noar and Shamir [1]. Visual cryptography is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes and pictures) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement.

This paper provides overview of various visual cryptography schemes. Taking limited bandwidth and storage into consideration two criteria pixel expansion and number of shares encoded is of significance. Smaller pixel expansion results in smaller size of the share. Encoding multiple secret images into the same share images requires less overhead while sharing multiple secrets. Meaningful shares avoid attention of hacker considering the security issues over the communication channels. To meet the demand of today's multimedia information gray and color image format should be encoded by the schemes. Other performance measures such as contrast, accuracy, security and computational complexity that affect the efficiency of visual cryptography are also discussed in this paper.

This paper is organized as follow: Section 2 provides overview of black and white visual cryptography schemes, color visual cryptography scheme are elaborated in section 3, performance of visual cryptography schemes are analyzed in section 4 and last section concludes the paper.

2. Black and White Visual Cryptography Schemes

2.1 Sharing Single Secret

Naor and Shamir's[1] proposed encoding scheme to share a binary image into two shares $Share_1$ and $Share_2$. If pixel is white one of the above two rows of Table 1 is chosen to generate $Share_1$ and $Share_2$. Similarly If pixel is black one of the below two rows of Table 1 is chosen to generate $Share_1$ and $Share_2$. Here each share pixel p is encoded into two white and two black pixels each share alone gives no clue about the pixel p whether it is white or black. Secret image is shown only when both shares are superimposed.

Table1. Naor and Shamir's scheme for encoding a binary pixel into two shares

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

To hide a binary image into two meaningful shares Chin-Chen Chang et al [5] suggested spatial-domain image hiding schemes. These two secret shares are embedded into two gray-level cover images. To decode the hidden messages, embedding images can be superimposed. Balancing the performance between pixel expansion and contrast Liguo Fang [6] recommend a (2, n) scheme based on combination. Threshold visual secret sharing schemes mixed XOR and OR operation with reversing and based on binary linear error-correcting code was suggested by Xiao-qing and Tan [16].

The disadvantage of the above schemes is that only one set of confidential messages can be embedded, so to share large amounts of confidential messages several shares have to be generated.

2.2 Sharing Multiple Secrets

Wu and Chen [2] were first researchers to present the visual cryptography schemes to share two secret images in two shares. They hidden 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⊗ B, and the second secret can be obtained by first rotating A Θ anti-clockwise. They designed the rotation angle Θ to be 90◦. However, it is easy to obtain that Θ can be 180◦ or 270◦. To overcome the angle restriction of Wu and Chen's scheme [2], Hsu et al. [3] proposed a scheme to hide two secret images in two rectangular share images with arbitrary rotating angles. Wu and Chang [4] also refined the idea of Wu and Chen [2] by encoding shares to be circles so that the restrictions to the rotating angles (Θ = 90◦, 180◦ or 270◦) can be removed.

S J Shyu et al [7] were first researchers to advise the multiple secrets sharing in visual cryptography. This scheme encodes a set of $n \geq 2$ secrets into two circle shares. The n secrets can be obtained one by one by stacking the first share and the rotated second shares with n different rotation angles. To encode unlimited shapes of image and to remove the limitation of transparencies to be circular, Fang[8] offered reversible visual cryptography scheme. In this scheme two secret images which are encoded into two shares; one secret image appears with just stacking two shares and the other secret image appears with stack two shares after reversing one of them. Jen-Bang Feng et al [9] developed a visual secret sharing scheme for hiding multiple secret images into two shares. The proposed scheme analyzes the secret pixels and the corresponding share blocks to construct a stacking relationship graph, in which the vertices denote the share blocks and the edges denote two blocks stacked together at the desired decryption angle. According to this graph and the pre-defined visual pattern set, two shares are generated.

To provide more randomness for generating the shares Mustafa Ulutas et al[10] advised secret sharing scheme based on the rotation of shares. In this scheme shares are rectangular in shape and are created in a fully random manner. Stacking the two shares reconstructs the first secret. Rotating the first share by 90° counterclockwise and stacking it with the second share reconstructs the second secret. Tzung-Her Chen et al [11] offered the multiple image encryption schemes by rotating random grids, without any pixel expansion and codebook redesign. A non-expansion reversible visual secret sharing method that does not need to define the lookup table offered by Fang [13]. To encode four secrets into two shares and recovering the reconstructed images without distortions Zhengxin Fu et al [14] intended a rotation visual cryptography scheme. Rotation visual cryptography scheme construction was based on correlative matrices set and random permutation, which can be used to encode four secret images into two shares. Jonathan Weir et al [15] suggested sharing multiple secrets using visual cryptography. A master key is generated for all the secrets; correspondingly, secrets are shared using the master key and multiple shares are obtained.

All the above schemes can be used only to share the black and white secret images, but it is demand of time that schemes should also support color images. To meet this demand researches have been made to share the color images.

3. Color Visual Cryptography Schemes

3.1 Sharing Single Secret

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 [17]. Colored secret images can be shared with the concept of arcs to construct a colored visual cryptography scheme. In c-colorful visual cryptography scheme one pixel is transformed into m subpixels, and each subpixel is divided into c 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. For a colored visual cryptography scheme with c colors, the pixel expansion m is c× 3. Yang and Laih [18] improved the pixel expansion to c × 2 of Verheul and Van Tilborg [17]. 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 [19] anticipated color visual cryptography scheme. For a secret color image two significant color images are selected as cover images which are the same size as the secret color image. Then according to a predefined Color Index Table, the secret color image will be hidden into two camouflage images. One disadvantage of this scheme is that extra space is required to accumulate the Color Index Table. In this scheme also number of subpixels is in proportional to the number of colors in the secret image as in Verheul and Van Tilborg [17] Yang and Laih [18] schemes. When more colors are there in the secret image the larger the size of shares will become. To overcome this limitation Chin-Chen Chang et al [20] developed a secret color image sharing scheme based on modified visual cryptography. This scheme provides a more efficient way to hide a gray image 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 [20] this scheme is not suitable for true-color secret image. To share true-color image Lukac and Plataniotis [21] introduced bit-level based scheme by operating directly on S-bit planes of a secret image.

To hide a color secret image into multiple colored images it is desired that the generated camouflage images contain less noise. For this purpose R.Youmaran et al [22] invented an improved visual cryptography scheme for hiding a colored image into multiple colored cover images. This scheme provides improvement in the signal to noise ratio of the camouflage images by producing images with similar quality to the originals. For reducing pixel expansion in color visual cryptography scheme S.J.Shyu [23] advised a more efficient colored visual secret sharing scheme with pixel expansion of $\lceil \log_2 c*m \rceil$ where m is the pixel expansion of the exploited binary scheme. By considering color image transmission over bandwidth constraint channels a cost effective visual cryptography scheme was invented by Mohsen Heidarinejad et al[24]. The solution offers perfect reconstruction while producing shares with size smaller than that of the input image using maximum distance separable. This scheme provides pixel expansion less than one. To improve the speed of encoding Haibo Zhang et al [25] presented a multi-pixel encoding which can encode variable number of pixels for each run. F. Liu et al [26] developed a colour visual cryptography scheme under the visual cryptography model of Naor and Shamir with no pixel expansion. In this scheme the increase in the number of colors of recovered secret image does not increase pixel expansion. Wei Qiao et al [27] suggested visual cryptography scheme for color images based on halftone technique. A secret image sharing scheme for true-color secret images devised by Du-Shiau Tsai et al [28]. In the proposed scheme through combination of neural networks and variant visual secret sharing, the quality of the reconstructed secret image and camouflage images are visually the same as the corresponding original images.

For encoding multiple color images using visual cryptography little researches have been carried out that are discussed here.

3.2 Sharing Multiple Secrets

Tzung-Her Chen et al [12] anticipated a multi-secrets visual cryptography which is extended from traditional visual secret sharing. The codebook of traditional visual secret sharing implemented 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.

Daoshun Wang et al [29] provided general construction for extended visual cryptography schemes using matrix extension algorithm. A general construction method for single or multiple and binary, grayscale, color secret images using matrix extension utilizing meaningful shares was suggested. Using matrix extension algorithm, any existing visual cryptography scheme with random-looking shares can be easily modified to utilize meaningful shares.

4. Performance analysis of visual cryptography schemes

Various parameters are recommended by researchers to evaluate the performance of visual cryptography scheme. Naor and Shamir [1] suggested two main parameters: 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 represents the loss in resolution from the original picture to the shared one. Contrast α is the relative difference in weight between combined shares that come from a white pixel and a black pixel in the original image.

Jung-San Lee et al [30] advised security, pixel expansion, accuracy and computational complexity as a performance measures. Security is satisfied if each share reveals no information of the original image and the original image cannot be reconstructed if there are fewer than k shares collected. 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 C.

Chang et al [19] suggested that visual cryptography scheme should support wide image format like color and gray scale. Author also argued that random looking shares appear to be suspicious and thus are vulnerable to attacks by attackers in the middle, to fill in this security gap, meaningful shares should be produced. Jen-Bang Feng et al[9] suggested that VCS should support multiple secret to work efficiently. If scheme support only one secret to share at a time to share multiple secret images numerous share have to be generated, transmitted and maintained.

Table 2. Comparison of visual cryptography schemes on the basis of number of secret images, pixel expansion, image format, type of share generated

Sr. No.	Authors	Year	Number of Secret Images	Pixel Expansion	Image Format	Type of Share generated
1.	Naor and Shamir [1]	1995	1	4	Binary	Random
2.	Wu and Chen [2]	1998	2	4	Binary	Random
3.	Hsu et al [3]	2004	2	4	Binary	Random
4.	Wu and Chang [4]	2005	2	4	Binary	Random
5.	Chin-Chen Chang et al [5]	2005	1	4	Binary	Meaningful
6.	Liguo Fang et al [6]	2006	1	2	Binary	Random
7.	S. J. Shyu et al [7]	2007	n(n>=2)	2n	Binary	Random
8.	W. P. Fang [8]	2007	2	9	Binary	Random
9.	Jen-Bang Fenget al [9]	2008	***n*(n>=2)**	3n	Binary	Random
10.	Mustafa Ulutas [10]	2008	2	4	Binary	Random
11.	Tzung-Her Chen et al in [11]	2008	2	1	Binary	Random
12.	Tzung-Her Chen et al [12]	2008	n(n>=2)	4	Binary, gray, color	Random
13.	Wen-Pinn Fang [13]	2009	2	1	Binary	Random
14.	Zhengxin Fu[14]	2009	4	9	Binary	Random
15.	Jonathan Weir et al [15]	2009	n	4	Binary	Random
16.	Xiao-qing Tan [16]	2009	1	1	Binary	Random
17.	Verheul Tilborg [17]	1997	1	c*3	Color	Random
18.	Yang & Liah [18]	2000	1	c*2	Color	Random
19.	Chang and Tsai [19]	2000	1	529	Color	Meaningful
20.	Chin Chen Chang et al [20]	2002	1	9	Gray	Meaningful
21.	Lukac and Plataniotis [21]	2005	1	2	Color	Random
22.	R.Youmaran et al [22]	2006	1	9	Color	Meaningful
23.	S.J.Shyu [23]	2006	1	$\lceil \log_2 c*m \rceil$	Color	Random
24.	Mohsen Heidarinejad et al [24]	2008	1	9/16	Color	Random
25.	Haibo Zhang et al [25]	2008	1	1	Gray	Random
26.	F. Liu et al [26]	2008	1	1	Color	Random
27.	Wei Qiao et al [27]	2009	1	m	Color	Random
28.	Du-Shiau Tsai et al	2009	1	9	Color	Meaningful

	[28]					

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

As shown in the Table 2 only few visual cryptography schemes achieve minimum pixel expansion. If m>1 large storage space required to store and transmit the shares. Schemes with m=1 [11, 13, 16 and 25] are good candidate for secure transmission over limited bandwidth communication networks. Meaningful shares [5, 19, 20 and 28] can be helpful to avoid attacks by hacker. Scheme supporting color images [5, 19, 20, 22 and28] are useful in the multimedia environment. Less overhead for storage and transmission is required to share multiple secrets while using the scheme [7, 9 and 12].

5. Conclusion

In this paper various visual cryptography schemes are studied and their performance is evaluated on four criteria: number of secret images, pixel expansion, image format and type of share generated. While selecting visual cryptography for a particular application Table II is helpful. If minimum bandwidth is available to share the secrets then schemes [24, 11, 13, 16 and 25] are better choice. For sharing multiple color images schemes [12 and 27] can be employed. For avoiding attention of hackers while transmitting the confidential messages [5, 19, 20, 22 and 28] are suitable selections.

6. References

[1] Moni Naor and Adi Shamir, “Visual Cryptography”, advances in cryptology– Eurocrypt, pp 1-12,1995.

[2] 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.

[3] H.-C. Hsu, 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, pp. 996–1001, March 2004.

[4] H.-C. Wu, C.-C. Chang, “Sharing Visual Multi-Secrets Using Circle Shares”, Comput. Stand. Interfaces 134 (28) ,pp. 123–135, (2005).

[5] 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.

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

[7] S. J. Shyu, S. Y. Huanga,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.

[8] Wen-Pinn Fang, “Visual Cryptography In Reversible Style”, IEEE Proceeding on the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP2007), Kaohsiung, Taiwan, R.O.C, 2007.

[9] Jen-Bang Feng, Hsien-Chu Wu, Chwei-Shyong Tsai, Ya-Fen Chang, Yen-Ping Chu, “Visual Secret Sharing For Multiple Secrets”, Pattern Recognition 41 ,pp. 3572 – 3581, 2008.

[10] Mustafa Ulutas, Rıfat Yazıcı, Vasif V. Nabiyev, Güzin Ulutas, (2,2)- “Secret Sharing Scheme With Improved Share Randomness”, 978-1-4244-2881-6/08, IEEE, 2008.

[11] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, “Multiple-Image Encryption By Rotating Random Grids”, Eighth International Conference on Intelligent Systems Design and Applications, pp. 252-256 , 2008.

[12] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, “Multi-Secrets Visual Secret Sharing”, Proceedings of APCC2008, IEICE, 2008.

[13] Wen-Pinn Fang, "Non-Expansion Visual Secret Sharing In Reversible Style", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.2, February 2009.

[14] Zhengxin Fu, Bin Yu, "Research On Rotation Visual Cryptography Scheme", International Symposium on Information Engineering and Electronic Commerce, pp 533-536, 2009.

[15] Jonathan Weir, WeiQi Yan, "Sharing Multiple Secrets Using Visual Cryptography", 978-1-4244-3828-0/09, IEEE, pp 509-512, 2009.

[16] Xiao-qing Tan, "Two Kinds Of Ideal Contrast Visual Cryptography Schemes", International Conference on Signal Processing Systems, pp. 450-453, 2009.

[17] E. Verheul and 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.

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

[19] C. Chang, 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.

[20] Chin-Chen Chang , Tai-Xing Yu , "Sharing A Secret Gray Image In Multiple Images", Proceedings of the First International Symposium on Cyber Worlds (CW.02), 2002.

[21] R. Lukac, K.N. Plataniotis, "Bit-Level Based Secret Sharing For Image Encryption", Pattern Recognition 38 (5), pp. 767–772, 2005.

[22] R.Youmaran, A. Adler, A. Miri , "An Improved Visual Cryptography Scheme For Secret Hiding", 23rd Biennial Symposium on Communications, pp. 340-343, 2006.

[23] S.J. Shyu, "Efficient Visual Secret Sharing Scheme For Color Images", Pattern Recognition 39 (5) ,pp. 866–880, 2006.

[24] Mohsen Heidarinejad, Amirhossein Alamdar Yazdi and Konstantinos N, Plataniotis "Algebraic Visual Cryptography Scheme For Color Images", ICASSP, pp. 1761-1764, 2008.

[25] Haibo Zhang, Xiaofei Wang, Wanhua Cao, Youpeng Huang , "Visual Cryptography For General Access Structure By Multi-Pixel Encoding With Variable Block Size", International Symposium on Knowledge Acquisition and Modeling, pp. 340-344, 2008.

[26] F. Liu1, C.K. Wu X.J. Lin , "Colour Visual Cryptography Schemes", IET Information Security, vol. 2, No. 4, pp 151-165, 2008.

[27] Wei Qiao, Hongdong Yin, Huaqing Liang , "A Kind Of Visual Cryptography Scheme For Color Images Based On Halftone Technique", International Conference on Measuring Technology and Mechatronics Automation 978-0-7695-3583-8/09, pp. 393-395, 2009.

[28] Du-Shiau Tsai , Gwoboa Horng , Tzung-Her Chen , Yao-Te Huang , "A Novel Secret Image Sharing Scheme For True-Color Images With Size Constraint", Information Sciences 179 3247–3254 Elsevier, 2009.

[29] Daoshun Wang, FengYi, XiaoboLi, "On General Construction For Extended Visual Cryptography Schemes", Pattern Recognition 42 (2009),pp 3071 – 3082, 2009

[30] Jung-San Lee, T. Hoang Ngan Le, "Hybrid (2, N) Visual Secret Sharing Scheme For Color Images", 978-1-4244-4568-4/09, IEEE, 2009.