

A Comprehensive View on Encryption Techniques of Visual Cryptography

Raj Yadav

Assistant Professor

Department of CSE , University of Technology, Jaipur

Email: yadavrajc@gmail.com

Dr. Anoop Sharma

Professor

Department of CSE , University of Technology, Jaipur

Email: sharmaanoop001@gmail.com

R.L. Yadav

Department of CSE, Jaipur National University, Jaipur

Email: ram.bitspilani@gmail.com

Abstract — Visual Cryptography plays an important role in area of information security. It is a technique of cryptography to secure the visual information by encrypting them in to cipher text. At user's end human visual system is used for decryption. For this there is no need of any computer aid. Performance of Visual Cryptography scheme depends on the several measures these are generated share is meaningful or meaningless, computational complexity, accuracy, security pixel expansion, number of secret images. This paper explores a study and performance analysis of the various schemes of visual cryptography on the basis of number of secret images, image format, type of shares generated and pixel expansion.

Keywords- Security, Computational complexity, Pixel Expansion, Contrast, Accuracy, Visual Cryptography Scheme (VCS)

INTRODUCTION

In 1994 Naor & Shamir introduced Visual Cryptography [1]. Visual Cryptography is an encryption technique to encrypt the information (e.g. printed text, hand written text, images) in a manner that at the user's end decryption can be done by human visual system. There is no need of any computer aid.

Visual Cryptography scheme remove the complexity of computation in the process of decryption and secrete image can be recover by stacking the shares. Visual cryptography mainly helpful for it's less complexity of computation.














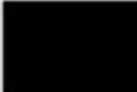
In this paper we express the view of different Visual Cryptography schemes. In the consideration of limited bandwidth & storage there are two major points (i) pixel expansion (ii) no of shares generation. Pixel expansion of smaller results in share with smaller size. Multiple secret image encoding in to same share image take 's less overhead while sharing multiple secrete.

This paper includes four sections; first section gives the comprehensive view of black & white Visual Cryptography schemes, second section includes color Visual Cryptography scheme, section third includes performance of Visual Cryptography, last section includes Conclusion.

SECTION 1: BLACK & WHITE VISUAL CRYPTOGRAPHY SCHEMES

Sharing Single Secret: encoding scheme proposed by Naor and Shamir's [1] to generate the share from a binary image in to two shares Share1 and Share2. The above two rows of Table 1 is chosen to generate Share1 and Share2 If pixel is white one. For black pixel below two rows of Table1 is chosen to generate Share1and Share2. Every pixel p of share encoded in to two black and two white pixels each of share alone gives noise clear out the pixel p whether it is white or black. Secret image is shown only when both of the images became shares are superimposed.

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

Pixel	Probability	Share ₁	Share ₂	Share ₁ ⊗ Share ₂
	50%			
	50%			
	50%			
	50%			

Hidden a binary image in to two meaning full shares Chin-Chen Chang et al [5] proposed spatial-domain image hiding schemes. Embedded these two secret shares in to two gray level cover images. Embedding images can be superimposed to decrypt the hidden information. Performance balancing between contrast and pixel expansion Liguang Fang [6] proposed a $(2, n)$ scheme. 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 is only that one set of confidential messages can be embedded, so several shares have to be generated to share large amounts of confidential messages.

Sharing Multiple Secrets: The visual cryptography schemes to share two secret images in two shares presented by Wu and Chen [2] were first researchers. According to them two binary secret images hidden into two random Shares, namely s_1 and s_2 , such that by stacking the two shares the first secret can be visible, denoted by $s_1 \otimes s_2$ and by first rotating s_1 Θ anti-clock wise 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° . Hsuet al. [3] Proposed a scheme to overcome the angle restriction of Wu and Chen's scheme [2], in this scheme two secret images hidden in two rectangular share images with arbitrary rotating angles. The idea of Wu and Chen [2] also refined by Wu and Chang [4] encoding shares to be circles so that there striations to the rotating angles ($\Theta=90^\circ, 180^\circ$ or 270°) can be removed.

Multiple secrets sharing in visual cryptography is advised by S J Shyu et al [7] he was the first researchers in this field. According to this scheme it encodes secrets of a set of $n \geq 2$ in to two circle shares. By stacking the first share and the rotated second shares with n different rotation angles n secrets can be obtained one by one. Fang [8] proposed reversible visual cryptography scheme to encrypt unlimited shapes of image and to discard the limitation of transparencies to be circular. According to this scheme two secret images which are encrypted into two shares; by just stacking two shares one secret image can appears and with stack two shares after reversing one of them the other secret image can appears. A visual secret sharing scheme was developed by Jen-Bang Feng et al [9] for hiding multiple secret images into two shares. This 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 additional randomness for generating the shares Mustafa Ulutas et al [10] advised secret sharing theme supported the rotation of shares. During this theme shares square measure rectangular in form and square measure created in an exceedingly totally random manner. Stacking the 2 shares reconstructs the primary secret. Rotating the primary share by 90° counterclockwise and stacking it with the second share reconstructs the second secret. Tzung-Her bird genus et al [11] offered the multiple image encoding schemes by rotating random grids, with none picture element enlargement and codebook plan. A non-expansion reversible visual secret sharing technique that doesn't ought to outline the operation table offered by Fang [13]. To cipher four secrets into 2 shares and convalescent the reconstructed pictures while not distortions Zhengxin Fu et al [14] supposed a rotation visual cryptography theme. Rotation visual cryptography theme construction was supported correlative matrices set and random permutation, which may be accustomed cipher four secret pictures into 2 shares. Eating apple Weir et al [15] prompt sharing multiple secrets mistreatment visual cryptography. A key is generated for all the secrets; correspondingly, secrets square measure shared mistreatment the key and multiple shares square measure obtained.

Above schemes are only applicable for black and white image, but visual cryptography schemes should also support color secrete images. For this demand researches have been made to share the color images.

SECTION 2: COLOR VISUAL CRYPTOGRAPHY SCHEMES

Sharing Single Secret: Verheul and Van Tilborg [17] developed the first color visual cryptography. The concept of arcs can be shared with Colored secret images to construct a colored visual cryptography scheme. According to c-colorful scheme, one pixel is converted into m sub pixels, and each sub pixel is divided into c color regions. In each sub pixel contains exactly one color region colored, and all remaining color regions are black. The pixel's color depends on the interrelations between the stacked sub pixels. The pixel expansion m is $c \times 3$ for a colored visual cryptography scheme with c colors. Yang and Lai [18] revised the pixel expansion to $c \times 2$. But both schemes produce the meaningless shares.

For generating a meaningful secretes of color image and sharing a secret color image a scheme "anticipated color visual cryptography" was developed by Chang and Tsai [19]. Two significant color images are selected as cover images for a secret color image, size are the same as the secret color image. On the basis of predefined Color Index Table, the secret color image will be hidden into two

camouflage images. This scheme has one disadvantage that is for accumulate the Color Index Table it required extra space. In this scheme also number of sub pixels is in proportional to the number of colors in the secret image as in Verheul and Van Tilborg [17] Yang and Lai [18] schemes. More colors in the secret image produce the larger size of shares. To reduce this limitation a scheme of a secret color image sharing based on modified visual cryptography was proposed by Chin- Chen Chang et al [20]. According to this scheme to hide a gray image in different shares it contains a more efficient way. This scheme contains shares of the fixed size; it does not vary when the number of colors appearing in the secret image differs. Any predefined Color Index Table does not require in this Scheme. It is not suitable for true- color secret image due to the pixel expansion is fixed in [20] this scheme. Lukac and Plataniotis [21] introduced bit-level based scheme to share true-color image by operating directly on S-bit planes of a secret image. For hiding secret color image in to multiple color image, for this it is expected that the created camouflage images is filled with less noise. To overcome this problem and get a desirable output R.Youmaran et al [22] proposed an advanced visual cryptography scheme for hiding a secret image in to multiple colored cover image. This gives improved signal to noise ratio of camouflage images by producing similar quality to the originals. S.J.Shyu [23] advised a more efficient colored Visual secret sharing scheme with pixel expansion of $\lceil \log_2 c * m \rceil$ for reducing pixel expansion in color visual cryptography scheme where m is the pixel expansion of the exploited binary scheme. By considering color image transmission over information measure constraint channels a price effective visual cryptography theme was fictitious by Mohsen Heidarinejad et al [24]. the answer offers excellent reconstruction whereas manufacturing shares with size smaller than that of the input image exploitation most distance severable. This theme provides picture element growth but one. to boost the speed of secret writing Haibo Zhang et al [25] bestowed a multi-pixel secret writing which may write variable variety of pixels for every run. F. Liu et al [26] developed a color visual cryptography theme below the visual cryptography model of Naor and Shamir with no picture element growth. During this theme the rise within the variety of colors of recovered secret image doesn't increase picture element growth. Wei dynasty Qiao et al [27] advised visual cryptography theme for color pictures supported halftone technique. A secret image sharing theme for true-color secret pictures was devised by Du-Shiau Tsai et al [28]. Within the projected theme through combination of neural networks and variant visual secret sharing, the standard of the reconstructed secret image and camouflage pictures are visually identical because the corresponding original pictures. For secret writing multiple color pictures exploitation visual cryptography very little researches have been carried out that are mentioned here.

Sharing Multiple Secrets: A multi-secrets Visual Cryptography which is extended from traditional visual secret sharing produced by Tzung-Her Chen et al [12]. To generate share images macro block by macro block, the codebook of traditional visual secret sharing implemented in such a way that multiple secret images are merged into only two share images and decrypt all the secrets images one by one by superimposing two of share images in a way of shifting. This scheme helps for multiple gray, color, and binary secret images with pixel expansion of 4.

A simple construction for extended visual cryptography schemes using matrix extension algorithm produced by Daoshun Wang et al [29]. It is simple construction method for single or multiple and grayscale, color, binary secret images using matrix extension utilizing meaningful shares. With the help of extension matrix algorithm, Modification can easily implemented any existing visual cryptography scheme with random-looking shares.

SECTION 3: PERFORMANCE ANALYSIS OF VISUAL CRYPTOGRAPHY SCHEMES

Various parameters area unit suggested by researchers to gauge the performance of Visual Cryptography theme. Naor and Shamir [1] instructed 2 main parameters: constituent enlargement m and distinction. Constituent enlargement m refers to the amount of sub constituents within the generated shares that represents a pixel of the initial input image. It represents the loss in resolution from the initial image to the shared one. Distinction is that the relative distinction in weight between combined shares that return from a white constituent and a black constituent within the original image.

Jung-San Lee et al [30] suggested security, element enlargement, accuracy and procedure quality as a performance measures. Security is glad if every share reveals no info of the initial image and also the original image can't be reconstructed if there square measure fewer than k shares collected. Accuracy is taken into account to be the standard of the reconstructed secret image and evaluated by peak signal-to-noise (PSNR) live. Procedure quality considerations the full variety of operators needed each to get the set of n shares and to reconstitute the initial secret image C. Chang et al [19] prompt that visual cryptography theme ought to support wide image format like color and grey scale. Author additionally argued that random trying shares seem to be suspicious and so area unit at risk of attacks by attackers within the middle, to fill during this security gap, meaning shares ought to be made. Jen-Bang Feng et al [9] prompt that VCS ought to support multiple secret to figure with efficiency. If

theme support only 1 secret to share at a time to share multiple secret pictures varied shares has got to be generated, transmitted and maintained.

Abbreviations in Visual Cryptography Schemes:

m shows pixel extension of corresponding Visual Cryptography plans, c number of colors in visual cryptography schemes, n is the amount of shares. As demonstrated in the Table 2 just few visual are cryptography plans attain least pixel expansion. Assuming that $m > 1$ huge storage room needed to store and transmit the stakes. Plans with $m=1$ [11, 13, 16, 25] are great hopeful for secure transmission over constrained band width communication systems. Genuine allotments [5, 19, 20, 28] might be useful to avoid attacks by programmer. Plan supporting color pictures [5, 19, 20, 22, 28] are advantageous in the earth. Less overhead for capacity and transmission is obliged to share multiple insider facts while utilizing the plan [7, 9, 12].

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	Author	year	Secret image	Expansion of pixel	format	Type of share
1	Naor & Shamir	1995	1	4	binary	random
2	Wu and Chen	1998	2	4	binary	random
3	Hsu et al	2004	2	4	binary	random
4	Wu and Chang	2005	2	4	binary	random
5	Chin-Chen Chang et all	2005	1	4	binary	meaningful
6	Ligou Fang et al	2006	1	2	binary	random
7	S.J. Shyu et al	2007	$n(n \geq 2)$	2n	binary	random
8	W.P.Fang	2007	2	9	binary	random
9	Jen-Bang Feng et al	2008	$n(n \geq 2)$	3n	binary	random
10	Mustafa Ulutas	2008	2	4	binary	random
11	Tzung-Her Chen et al	2008	2	1	binary	random
12	Tzung-Her Chen et al	2008	$n(n \geq 2)$	4	Binary, gray, color	random
13	Wen-Pinn Fang	2009	2	1	binary	meaningful
14	Zhengxin Fu	2009	4	9	binary	random
15	Jonathan Weir et al	2009	n	4	binary	random
16	Xiao-qing tan	2009	1	1	binary	random
17	Verheul Tilborg	1997	1	$C*3$	color	random

18	Yang & liah	2000	1	C*2	color	random
19	Chang and Tsai	2000	1	529	color	random
20	Chin chen chang et al	2002	1	9	gray	meaningful
21	Lukac and Plataniotios	2005	1	2	color	random
22	R.Youmaran et al	2006	1	9	Color	meaningful
23	S.J.Shyu	2006	1	[log c*m]	Color	Random
24	Mohsen Heidarinejad et al	2008	1	Sep-16	Color	Random
25	Haibo Zang et al	2008	1	1	Gray	random
26	F.liu et al	2008	1	1	color	random
27	Wei Qiao et al	2009	1	M	color	random
28	Du-Shiau Tsai et al	2009	1	9	color	meaningful

SECTION 4: CONCLUSION

This Paper includes considerations of different Visual Cryptography Scheme. Overall Performance assessed on four areas: type of share generated, image format, pixel expansion, and number of secret images while opting visual cryptography for a specific application Table II is useful. Assuming that if less bandwidth is available for base data transmission to share the secrets plans then [24, 11, 13, 16, 25] are better decision. For sharing various color images schemes [12, 27] might be utilized. For evading consideration of programmer's (hackers) while transmitting the secret information [5, 19, 20, 22, 28] are suitable determinations.

REFERENCES

- [1]. Moni Naor and Adi Shamir, "Visual Cryptography", advances incryptology–Eurocrypt, pp1-12,1995.
- [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 Conferenceon Networking, Sensing & Control, Taipei, Taiwan, pp.996–1001, March2004.

- [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-YuLin, “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]. Liguang Fang, Bin Yu, “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 Proceedings 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-ChuWu, 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, Rifat 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, Wei Qi Yan, “Sharing Multiple Secrets Using Visual Cryptography”, 978-1-4244-3828-0/09, IEEE, pp509-512, 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 ColorImages”, Pattern Recognition 39(5) ,pp. 866–880, 2006.
- [24]. Mohsen Heidarinejad, Amirhossein Alamdar Yazdi and Konstantinos N, Plataniotis “Algebraic Visual Cryptography Scheme For ColorImages”, ICASSP, pp. 1761-1764, 2008.
- [25]. Haibo Zhang,Xiaofei Wang,WanhuaCao,YoupengHuang, “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, “Akind Of Visual Cryptography Scheme For Color Images Based On Halft one 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-TeHuang, “ANovel Secret Image Sharing Scheme For True-Color Images With Size Constraint”, Information Sciences 179 3247–3254 Elsevier, 2009.
- [29]. Daoshun Wang, Feng Yi, 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.