TECHNIQUES OF VISUAL CRYPTOGRAPHY SCHEMES: A REVIEW

[1]Sangita Vishwakarma, [2]Mrs. Shahana Qureshi
[1]M. Tech Scholar, CSE, RITEE, Mandir Hasaud, Raipur (C. G.)
[2]Assistant Professor, Computer Science Dept., RITEE
Mandir Hasaud, Raipur (C. G.)

***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.*

I. INTRODUCTION

With the rapid advancement of network technology, multimedia information is transmitted over the Internet conveniently. Various confidential data such as similarity maps and commercial identifications are transmitted over the Internet. While using secret images and videos, 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 and videos, various schemes have been developed.

Visual cryptography is introduced by first in 1994 by Noar and Shamir [1]. Visual cryptography is a cryptographic technique which allows visual information (e.g. printed text, hand written 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 image can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement.

This paper provides a review of various visual cryptography schemes taking limited bandwidth and storage into consideration two criteria-pixel expansion and number of shares encoded 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 coded 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 follows: Section 2 provides overview of black and white visual cryptography schemes, color visual cryptography schemes are elaborated in section 3, section 4 describes the encryption of shares, visual cryptography in videos are elaborated in section 5 and performance of visual cryptography schemes are analyzed in section 6 and last section concludes the paper.

II. BLACK AND WHITE VISUAL CRYPTOGRAPHY SCHEMES

Sharing Single Secret:

Naor and Shamir's [1] proposed encoding scheme to share a binary image into two shares- Share1 and Share2. If pixel is white one of the above two rows of Table1 is chosen to generate Share1 and Share2. Similarly if pixel is black one of the below two rows of Table1 is chosen to generate Share1and Share2. Here each share pixel p is encoded into two white and two black pixels. Each of shares alone gives noise whether it is white or black. Secret image is shown only when both of the image shares are superimposed.

Pixel	Probability	Share$_1$	Share$_2$	Share$_1$ ⊗ Share$_2$
□	50%	■□	■□	■□
	50%	□■	□■	□■
■	50%	■□	□■	■■
	50%	■□	■□	■■

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

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 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 amount of confidential messages several shares have to be generated.

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 hide 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 Ө anti-clockwise. They designed the rotation angle Ө to be 90^{o}. However, it is easy to obtain that Ө can be 180^{o} or 270^{o}. To overcome the angle restriction of Wuand Chen's scheme [2], Hsuet al. [3] proposed a scheme to hide two secret images in two rectangular share images with arbitrary rotating angles. Wuand Chang [4] also refined the idea of Wuand Chen [2] by encoding shares to be circles so that the restrictions to the rotating angles (Ө=90^{o}, 180^{o} or 270^{o}) 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 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° counter clockwise 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 was 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.

III. COLOR VISUAL CRYPTOGRAPHY SCHEMES

Until the year 1997 visual cryptography schemes were applied to only black and white images. First color visual cryptography scheme was developed by Verheul and Van Tilborg [17]. Color secret images can be shared with the concept of arcs to construct a color visual cryptography scheme. In color visual cryptography scheme, one pixel is transformed into m sub pixels, and each sub pixel is divided into color regions. In each sub pixel, 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 sub pixels. For a color 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 sub pixels is in proportion 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 color 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 color 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 color visual secret sharing scheme with pixel expansion of |log2c*m| 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 color 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 was 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.

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, gray scale, color secret images using matrix extension utilizing meaningful shares with of suggested. Using matrix extension algorithm, any existing visual cryptography scheme with random-looking shares can be easily modified to utilize meaningful shares.

Ankush V Dahat and Pallvi V. Chavan [31] used CMY color space instead of RGB color space for implementing visual cryptography. In this scheme, the number of shares generated as per the user needs and the original image can be retrieved by stacking n-1 shares. This scheme was capable of maintaining secrecy as it used CMY color space.

To provide more security to the shares generated, Siddaram Shetty & Mintu P. Abraham [32] used RSA algorithm for encrypting the shares. Soumy S. Hegde and Bhskara Rao N [33] proposed Zigzag Scan approach prior to share generation to convert 2D image matrix into 1D vector in order to generate non-expanded shares. This approach also overcame the drawback of Hilbert Curve approach, i.e., there is no input image size restriction.

IV. ENCRYTION OF SHARES

The above visual cryptography schemes does not provide secrecy of the shares generated and due to this fake shares can be easily added or the generated shares can be modified in order to retrieve the secret image. K. Shankar and Dr. P. Eswaran [34] used Elliptical Curve Cyptography along with Differential Evolution Optimization technique that is applied in the private key generation phase. Elliptical Curve Cyptography uses plane curve as finite field, avoiding real numbers, thus provides minimal mathematical complexity and is more computationally efficient.

DiShiau Tsi, Tzung-Her Chen and Gwoboa Horng [35] incorporated Genetic Algorithm based Share Construction Method for preventing cheating where some participants can deceive the remaining participants by delivering forged transparencies. Through multiple secret images, each qualified subsets will only reveal the secret image and others are left unknown to potential cheaters. R. Anushiadevi, Padmapriya Praveen Kumar, John Bosco and Rengarajan [36] used two levels of encryption, one at plane level and other at pixel level.

Shankar K and Eswaran P [37] suggested encrypting the shares using AES algorithm. The combination of visual cryptography and encryption of images made the process complex but provides high security to the shares generated. This scheme used the four basic procedures of AES algorithm, i.e. SubBytes Transformation, Shiftrows Transformation, Mixcolumn and Addroundkey Transformation. Zhou, K. Panetta, S. Agaian and C. L. P Chen [38] introduced an encryption algorithm by combining parametric bit-plane decomposition along with bit-plane shuffling, pixel scrambling and data mapping. This algorithm utilized Fibonacci P-codes for bit-plane decomposition and 2D Fibonacci Transform for encryption.

A bit level permutation and high dimension chaotic map to encrypt a color image was proposed by Hongjun Lia and Xingyuan Wang [39].A. Any color image of size (MxN) is converted into grayscale image of size (Mx3N) and then transformed into a binary matrix. This matrix is permuted at bit level by scrambling mapping generated by Piecewise Linear Chaotic Map (PWLCM) and used Chen system to confuse and diffuse red, green and blue components simultaneously.

Obaida M. Al-Hazaimeh, Nouh Alhindawi, Sofyan M. A. Hayajneh and Ammar Almomani [40] used HANON chaotic map for encryption where the pixels shuffled randomly. The pixel values are modified using logic bitwise exclusive-OR operation between the original pixel value and the key that can be selected randomly from a dynamically updated key table whose values are generated either from the values that are not used in shuffling operation or from generating new chaotic values in the cases when table empty or fully used.

Encryption of large images causes considerable delay in successive transmission of encrypted images. In order to minimize this latency, a fast symmetric key encryption procedure, Matrix Array symmetric Key Encryption (MASK) based on matrix manipulation is proposed by Paul A.J, P. Mythili and K. Paulose Jacob [41]. This encryption scheme is a block cipher with a block size of 128 bits and key size of 128 bits and facilitates poly alphabetic substitution. The sub keys in the round operation are generated by key scheduling procedure.

V. VISUAL CRYPTOGRAPHY SCHEMES IN VIDEO

In the era of internet and with rapid advances in technology, an increasing number of images and videos with private and confidential information are generated, stored and transmitted every second. Not only the images but also the videos need to be encrypted from unauthorized access. Much of the efforts have been devoted to the implementation of visual cryptography in images. Many researchers are working to make transmission of videos more secure against attacks by visual cryptography.

Aman Chadha, Sushmit Malik, Ravdeep Kaur, Ankit Chadha and M. Mani Roja [42] proposed a video encryption using RSA algorithm and Pseudo Noise (PN) sequence. The audio and video components separately undergo two layers of encryption. Encryption of video component involves applying RSA algorithm followed by PN-based encryption. The audio component is encrypted by PN and Then by Discrete Cosine Transform (DCT).

Visual cryptography in videos has been implemented by Bhawna Shrivas and Shweta Yadav [43] using Halftoning technique. Halftoning is a process of transforming an image with greater amplitude resolution to one with lesser amplitude resolution. Floyd and Jarvis method has been used for halftoning.

VI. PERFORMANCE ANALYSIS OF VISUAL CRYPTOGRAPHY SCHEMES

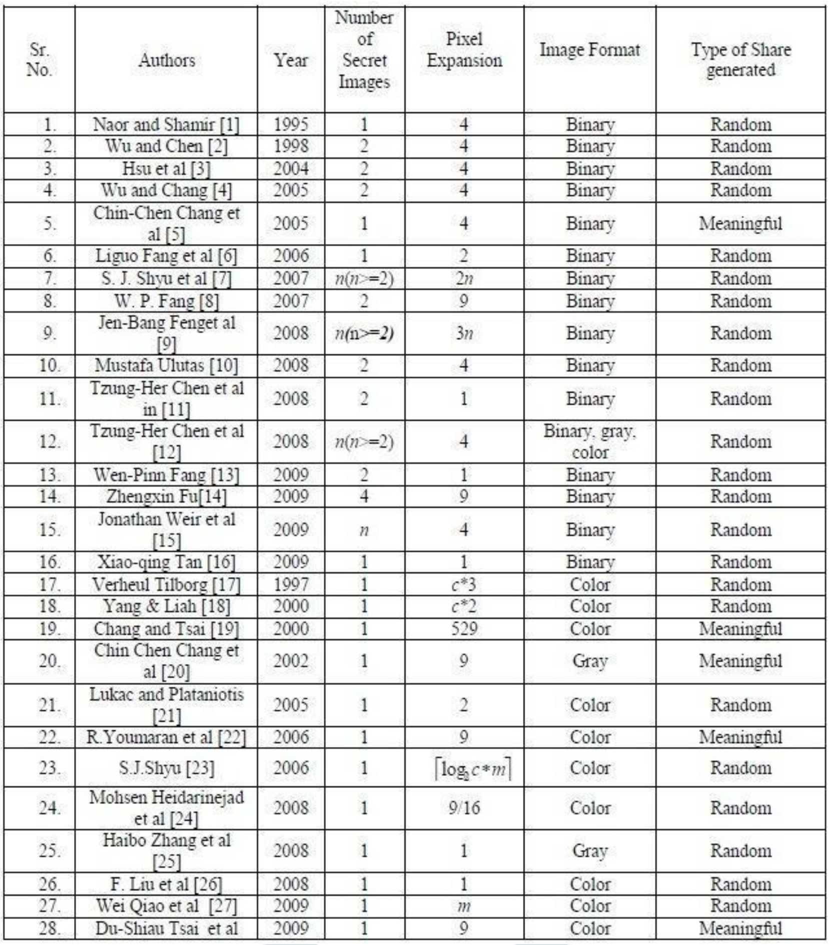
Various parameters are recommended by researchers to evaluate the performance of visual cryptography scheme. Naor and Shamir [1] suggested two main parameters: pixel expansion m and contrast. Pixel expansion m refers to the number of sub pixels in the generated shares that represents a pixel of the original input image. It represents the loss in resolution from the original picture to the shared one. Contrast 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 shares has to be generated, transmitted and maintained.

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. As shown in the Table 2 only few visual are a 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].



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

Table 2 Comparison of various cryptography schemes.

VII. 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. For encrypting the shares generated by the visual cryptography schemes [34, 35, 36, 37, 38, 39, 40, and 41] can be employed after the generations of shares.

REFERENCES

[1]. Moni Naor and Adi Shamir, "Visual Cryptography", advances in cryptology–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 Conference on 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]. Liguo 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 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-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, 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-HerChen, 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. Verheuland H. V. Tilburg, “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,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, “Color 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 TeHuang, “A Novel 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.

[31]. Ankush V Dahat and Pallavi V. Chavan, ‘”Secret Sharing Based Visual Cryptography Scheme Using CMY Color Space”, International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Procedia Computer Science 78 (2016) 563 – 570.

[32]. Siddaram Shetty & Mintu P. Abraham, “A Secure Visual Cryptography Scheme for Sharing Secret Image using RSA”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 4, April 2015, ISSN(Online): 2320-9801, ISSN (Print): 2320-9798.

[33]. Soumy S. Hegde and Bhskara Rao N, “Visual Cyptography Using Zigzag Scan Approach”, IJCSET, September 2011, Vol 1, Issue 8, 456-46, ISSN: 2231-0711.

[34]. K. Shankar and Dr. P. Eswaran, “ECC Based Image Encryption Scheme with aid of Optimization Technique using Differential Evolution Algorithm”, International Journal of Applied Engineering Research, ISSN 973-4562, Vol 10, No. 55 (2015).

[35]. DiShiau Tsi, Tzung-Her Chen and Gwoboa Horng, “A Cheating Prevention Scheme for Binary Visual Cryptography with Homogeneous Images ”, The Journal of Pattern Recognition Society, pattern Recognition 40 (2007) 2356-2366.

[36]. R. Anushiadevi, Padmapriya Praveen Kumar, John Bosco and Rengarajan, “Revolving of pixels and bits in Pixels-Plan (E) Tary Encryption ”, Reserch Journal of Information Technology, ISSN 1815-7432, DOI: 10.3923/rjit.2017.25.31.

[37]. Shankar K and Eswaran P, “Sharing a secret image with Encapsulated Shares in Visual Cryptography”, 4th International Conference on Eco-friendly Computing and Communication System, ICECCS, 2015, Procedia Computer Science 70 (2015) 462 – 468.

[38]. Zhou, K. Panetta, S. Agaian and C. L. P Chen, “Image Encryption Using P – Fibonacci Transform and Decomposition”, Optics Communication, 285: 594-608.

[39]. Hongjun Lia and Xingyuan Wang, “Color image encryption using spatial bit-level permutation and high-dimension chaotic system”, Optics Communications, 284 (2011) 3895–3903, August 2011.

[40]. Obaida M. Al-Hazaimeh, Nouh Alhindawi, Sofyan M. A. Hayajneh and Ammar Almomani, "HANON Chaotic Map-Based New Digital Image Encryption Algorithm", MAGNT Research Report (ISSN. 1444-8939) Vol.2 (4). PP: 261-266, August 2014.

[41]. Paul A.J, P. Mythili and K. Paulose Jacob, "Matrix based cryptographic procedure for efficient image encryption", Conference Paper · September 2011, DOI: 10.1109/RAICS.2011.6069296.

[42]. Aman Chadha, Sushmit Malik, Ravdeep Kaur, Ankit Chadha and M. Mani Roja, "Dual-Layer Video Encryption using RSA Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 1, April 2015.

[43]. Bhawna Shrivas and Shweta Yadav, "Visual Cryptography in the Video using Halftone Technique", International Journal of Computer Applications (0975 – 8887) Volume 117 – No.14, May 2015.