International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-11, September 2019

A Quantitative and Qualitative Reasoning of Various Visual Cryptographic Schemes to Uphold Secrecy

R Logeshwari, L. Rama Parvathy

Abstract: ***The secret sharing scheme plays a vital role in cryptography which allows to transmit the secret digital information (image, video, audio, handwritten notes etc.) over a communication channel. The Encoding is done in special way using Visual cryptographic schemes and decoding is carried out by the human sensory system without complexity. The secrets are encrypted into shares in these schemes, stacking these shares with minimal loss will disclose the secrets. These shares are presented in n number of transparencies. This paper provides an overview of various VC schemes of single secret and multi secret of grayscale and color secret images. Also, comparative analysis study on these schemes are presented, based on pel expansion, contrast, accuracy, capacity, security, type of share, number of shares, image format.***

Index Terms: Contrast, Multi secret VCS, Pixel Expansion, Single Secret VCS, Shares, Security.

I. INTRODUCTION

In the present era, due to the enhancement of network technology, digital communication over the internet conveniently. This increases the concern over security in digital environment. There are so many cryptographic techniques developed to implement secured communication in global network. The Secret sharing theme is one amongst the cryptologic techniques that involves encrypting the key images into noisy image shares and transmitted. The transmitted image shares are retrieved using simple computation. Initially these VC schemes can be applied on single secret image to produce multiple shares. A (k, n) – VCS, where k ≤ n, divides the single key image into n-parts, one can reclaim the secret picture from k or further shares. But now the single secret sharing schemes extended to n images to n shares. To cipher n private images into n parts n (n, n) multi-secret VC scheme is developed. All n-parts are needed to retrieve n private images.

The secret image is broadly classified into 3 types. Binary, gray and color. Binary and gray are two dimensional images where color is a three-dimensional image. Each binary image pixel is depicted as 0's and 1's, either black or white. Each gray image pixel includes values ra nging from 0 to 255. Each value corresponds to one gray level. Each pixel of RGB image contains three values which lies in between 0 to 255 whereas 0≤r, g, b≤255. Therefore, RGB images takes more computation time when compared with binary and gray images. Secret sharing schemes has many applications spanning different fields. it's widely used in military maps, missile launch codes, while transferring data through unsecured channels and access control. The schemes provide improved authentication and higher confidentiality with no data loss. The VC systems have two significant parameters like ex panding and contrasting pixels. The minimal extension o f pixels and a high contrast make the systems of secret sh aring superior. The conditions of minimal pixel expansion and maximum contrast were discussed previously [28]-[31]. The prospects of sharing n secret images analyzed using Multi secret VCS techniques [46]- [51]. VCS is proposed with various unique features, such as fraud prevention, dealing with malignant issues, resolving the optimal contrast, a color image sharing [32]-[39]. The VC scheme involves sharing the secret information in a secure pattern were proposed by [40] – [45]. The primary function of the VC schemes is to use the partitioning method to encrypt the confidential information. The private message cannot be revealed by the help of some split data. The original image requires all split data's to be revealed. The VC scheme is to split an image into prearranged number of parts and then without any computation or algorithm, the secret data can be reclaimed by aligning and bundling together. The other sections of the paper are structured as follows, section 2 describes about variants of VC schemes. In Section 3, we have done a comparative analysis on single secret visual cryptographic schemes. In section 4, we done comparative analysis on multi secret visual cryptographic schemes, finally we concluded in section 5.

II. DESCRIPTIONS OF VARIOUS VISUAL CRYPTOGRAPHIC SCHEMES

In today's world, the multimedia and internet has made digital communication to play a vital role in all domains. In order to maintain the confidentiality of secret in the year 1979 Blakely [1] and Shamir [2] created a secret sharing system in which a binary image is divided into various shares and circulated to various respondents with strong confidentiality. The secret image is retrieved from k shares or more than k shares where k is a threshold in (k, n) threshold schemes [3,4]. To evaluate the proposed secret sharing schemes, the security, contrast, pixel expansion, incorrect color filling, computational complexity and capacity are to be satisfied.

Manuscript published on 30 September 2019.
***Correspondence Author(s)**
R Logeshwari, Research Scholar, Department of Computer Science & Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India.
Dr. L. Rama Parvathy, Department of Computer Science & Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India.

We describe some of the visual cryptographic algorithms which supports single and multi-secret sharing schemes. In 1987 Kafri[5] designed the concept of Random grids to overcome computational complexity but pixel expansion problem is not eliminated. The drawbacks mentioned above is resolved by (k, n) probabilistic visual schemes [6, 7, 8] but it suffered from reclaim mechanism. To resolve the reclaim precision, Cimato et al, [6] perceives the white component frequency to retain the distinction of the reconstructed image by activity exclusive OR and AND operation that permits recovering the lossless secret image. Y. C. Hou et al, suggested [9] a non-expanded shadow size system. The disjoint property and union property are fulfilled in this system. These characteristics ensure progressive recovery and also the secret image will be regained by all the respondents.

C. N. Yang et al, [10] designed generalized (k, n) Block based Progressive VC scheme for any k and n. this method defines the construction method according to application's need. This method also highlights some issues non-uniform stacked results, image reconstruction problem and the ratio of progress recovery differs. Wang et al, have planned[11] n-level Region Incrementing VC schemes (RIVCS), the secret image is split into completely different regions correlate n secret levels and conceal to n+1 share where each region maintains reticence property. C. N. Yang et al, [12] says that Wang's phenomenon has a drawback of incorrect color problem in reconstruction phase. Also, the Wang's methodology is only applicable for (2/n) case. So, Yang proposed generalized (k, n) RIVCS to overcome the incorrect color problem, it also fulfills the circumstances of security and contrast. Yang shows the customized version to trim the share size and improve the contrast where the problem is solved incorrectly.

C. C. Wu et al, recommended [13] to share two secret images A and B as two shares S_1 and S_2 using a Multi-secret VC schemes (MSVCS), secret A is recovered by stacking S_1 and S_2. Secret B is retrieved by rotating the S_1 in anti-clockwise and stacking, results the secret B. Hsu et al [14] proposed scheme of rectangular shares with arbitrary angles to overcome the rotation angle issues. To limit the angles of rotation H. C. Wu et al proposed [15] a system for encoding circle shares. Shankar et al, intended [25] a safe n shares with no pixel expansion and lossless recovery from n secret pictures. Karthick et al [26] generated n shares from n secrets using security key. Reconstruction of shares done by exclusive OR operation. Mohit et al, [27] produced n+1 shares of n secret images and implemented additive modulo operation to recover the secrets.

The following sections give the detailed comparative study on various single secret and multi secret visual cryptographic schemes.

III. SINGLE SECRET VCS FOR GREY SCALE IMAGES

The various Single Secret Visual Cryptographic Schemes worked only with black and white images from which meaningless shares are generated. The Pixel expansion and relative difference (contrast) are the two basic parameters in VCS. The pixel expansion decodes to number of subpixels in a share a single pixel of secret image. The contrast described in the decoded image as the relative difference in gray level between black and white pixels, which provides the measure of the comparison with which the image becomes noticeable. Maximizing the contrast and minimizing the pixel expansion is major concern whereas both cannot be optimized simultaneously. The maximum of the constructions of single secret visual cryptographic schemes are performed using two n-by-m matrices for white and black pixels called Basis Matrices. The contrast and security condition should meet by constructed basis matrices. The construction method combined with basis matrices to generate a share of original image whereas integer linear programming generates the shares with minimal pixel expansion. A Various Single Secret VC schemes are compared based on different parameters are listed in Table 1.

Table 1: Comparative study on Single Secret VCS

S.No	VC Schemes	Basis Matrices	Construction Method	Pixel Expansion Operation	Incorrect Color Problem	Property Satisfied	Progress Recovery
1.	(K,n) VCS	Boolean Matrices	Column Permutation	Concatenation	YES	Canonical Uniform	Threshold
2.	Modified (k,n) VCS	Primitive Matrices	Integer Linear Programming	Concatenation	YES	Canonical Uniform	Threshold
3.	Modified (k,n) tVCS	Primitive Matrices	Integer Linear Programming	Concatenation	YES	Canonical Uniform	Threshold
4.	(k,n) Probabilistic VCS	distribution Matrices	Based on Probability	OR operation	YES	Canonical Uniform	Threshold
5.	(k,n) Probabilistic VCS	Boolean Matrices	Based on non-expansible shadow size and parameter threshold probability	OR operation (No pixel Expansion)	YES	Canonical Uniform	Threshold
6.	(k,n) Block Based Progressive VCS	Image Blocks	Cons 1: nC_{k-1} Cons 2: nC_k choosen according to need.	Union Operation	YES	Canonical Uniform disjoint	Disjoint, threshold
7.	(2,n) Block Based Progressive VCS	Random grid	2 out of 2 random grids	Uses Random grid	YES	Canonical Uniform disjoint	Disjoint, threshold
8.	(k,n) Region Based BPVC	Boolean matrices	No construction method	Concatenation	Yes	Canonical Uniform	Threshold progressive decoding capability
9.	(2,n) Region Incrementing VCS	Boolean matrices	Construction method not clear	Union operation	YES	Canonical Uniform disjoint	Threshold, increment revealing
10.	(2,n) RIVC	Unit matrices	ILP with minimal pixel expansion	Union operation	YES	Canonical Uniform disjoint	Threshold, increment revealing
11.	(k,n) RIVC	Boolean matrices	Conventional VCS method	Union operation	NO	Canonical Uniform disjoint	Threshold progressive decoding capability

IV. MULTI SECRET VCS FOR GREYSCALE AND COLOR IMAGES

The Multi Secret VCS accepts both grey scale and color images as n inputs and generates the n shares. Most of the multi Secret VC Schemes works with no pixel expansion which has major concern in Single Secret VCS. Some implemented methods provide greater security to shares which never reveals the original image. The original images are recovered with less distortion using XOR operation compared to other operations like Stack, Additive Modulo. In literature [26] shared image capacity is taken into consideration, that is 8 shares are transferred as single share which increases the capacity. Whereas the single share holds 8 images as secret. Detailed comparative study on Multi Secret VCS is tabulated in Table 2.

V. CONCLUSION

This paper presented a survey on various studies conducted in the areas of secret image sharing schemes. Various characteristics of Single Secret VC and Multi-Secret VC systems are summarized in a comparative table.

Retrieval Number: J90710881019/19©BEIESP
DOI: 10.35940/ijitee.J9071.0981119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

We conclude that all techniques are good for data hiding and have their own advantages and disadvantages and gives a security so that no one can access the image in open network. Our future research will be aimed at creating video and audio shares using methods of biometric, picture scrambling, geometric patterning to improve safety.

Table 2: Comparative study on Multi Secret VCS

Parameters	[16]	[17]	[18]	[19]	[20]	[21]	[22]	[23]	[24]	[25]	[26]	[27]
Secret type	IMAGES											
Secret image	n				2	n		2	n			
Shared image	n		n + 1	n	2 * 4		2(2*n)	2	n		n / 8	n + 1
pel Expansion	no				yes			no				
Reconstruction type	lossless				recognizable			lossless				
Recovery strategy	Xor				Stack			Xor				Addit Mod
Sharing type	Rectangle				circle			Rectangle			square	Rect
Color depth	gray& color	grayscale			binary			gray	grayscale or color			
Sharing capacity	n / n		n/ n+1	n / n	2/2*4	n / 2*4		2 / 2	1 / n	n / n	8(n / n)	n/n+1
Shadow security	yes	No								yes		
Reveals Security	no	Limited								No		

REFERENCES

1. I. Ramya Princess Mary, P. Eswaran, K.Shankar, “Multi Secret Image SharingScheme based on DNA Cryptography with XOR”, International Journal of Pure and Applied Mathematics, Volume 118, No. 7, page(s) 393-398, February 2018.
2. Adi Shamir, “How to share a secret”, Communications of the ACM, vol. 22,no. 11, page(s): 612–613, 1979
3. Simmons and Gustavus J, “An introduction to shared secret and/or sharedcontrol schemes and their application”, Contemporary cryptology: The scienceof information integrity, page(s): 441–497, 1992.
4. G. Blakley, “Safeguarding crypographic keys”, presented at the Proceedingsof the AFIPS 1979 National Computer Conference, vol. 48, Arlington, VA,page(s): 313–317, June 1997.
5. Stinson and Douglas R, “An explication of secret sharing schemes”, Designs,Codes andCryptography, vol. 2, issue.4, page(s): 357–390, 1992.
6. Cimato, Stelvio, Roberto De Prisco, and Alfredo De Santis, “ProbabilisticVisual Cryptography Schemes”, The Computer Journal, vol. 49, No. 1,page(s): 97–107, 2006.
7. Ateniese, Giuseppe, et al. “Extended capabilities for visual cryptography”,Theoretical Computer Science, vol.250, issue.1, page(s): 143–161, 2001.
8. Chang, Chin-Chen, and Ren-Junn Hwang, “Sharing secret images usingshadow codebooks”, Information Sciences, vol. 111, issue.1, page(s): 335–345, 1998.
9. Y. C. Hou et al. “Block based Progressive visual secret sharing ,” Inf Sci., vol 223, June 2013, pp. 290-304.
10. Ching-Nung Yang et al. “k out of n Region- Based Progressive Visual Cryptography”, Transactions on circuits and systems for video technology, vol. 34, pp. 179-196, 2017.
11. R. Z. Wang, “Region Incrementing visual cryptography,” IEEE signal process. Let., vol16, no 8, pp. 659-662, Aug 2009
12. C. N. Yang, “k out of n Region Incrementing Scheme in Visual Cryptography”, IEEE Transactions on Circuits and Systems for Video Technology, vol.22, no.5, pp. 799-810, 2012
13. C.C. Wu, L.H. Chen, “A Study on Visual Cryptography”, Master Thesis, Institute of Computer andInformation Science, National Chiao Tung University, Taiwan, R.O.C., 1998.
14. H.-C. Hsu, T.-S. Chen, Y.-H. Lin, “The Ring Shadow Image Technology of Visual Cryptography byApplying Diverse Rotating Angles To Hide The Secret Sharing”, in Proceedings of the 2004 IEEEInternational Conference on Networking, Sensing & Control, Taipei, Taiwan, pp. 996–1001, March 2004.
15. H.-C. Wu, C.-C. Chang, “Sharing Visual Multi-Secrets Using Circle Shares”, Comput. Stand. Interfaces 134(28) ,pp. 123–135, (2005).
16. 16. Maroti Deshmukh ,N Nain and M Ahmed “An (n,n)-Multi Secret Image Sharing Scheme using Boolean XOR and Modular Arithmetic”, 2016 in IEEE 30th International Conference on Advanced Information Networking and Applications.
17. Yang, Ching-Nung, Cheng-Hua Chen, and Song-Ruei Cai. ” Enhanced Boolean-based multi secret image sharing scheme.” Journal of Systems and Software (2015)
18. Chen, Tzung-Her, and Chang-Sian Wu. ”Efficient multisecret image sharing based on Boolean operations.” Signal Processing 91.1 (2011): 90-97.
19. Chen, Chien-Chang, and Wei-Jie Wu. ”A secure Boolean based multi-secret image sharing scheme.” Journal of Systems and Software 92 (2014): 107-114.
20. Wu, H.C., Chang, C.C., 2005. Sharing visual multi-secrets using circle shares. Computer Standards and Interfaces 28, 123–135
21. Chen, J., Chen, Y.S., Hsu, H.C., Chen, H.W., 2005. New visual cryptography system based on circular shadow image and fixed angle segmentation. Journal of Electronic Imaging 14 (3), 033018-1–033018-5
22. Shyu, S.J., Huang, S.Y., Lee, Y.K., Wang, R.Z., Chen, K., 2007. Sharing multiple secrets in visual cryptography. Pattern Recognition 40, 3633–3651
23. Lin, S.J., Chen, S.K., Lin, J.C., 2010. Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion. Journal of Visual Communication and Image Representation 21, 900–916
24. Wang, D., Zhang, L., Ma, N., Li, X., 2007. Two secret sharing schemes based on Boolean operations. Pattern Recognition 40 (10), 2776–2785.
25. Dr.K.Shankar, Dr.G.Devika, 2017. Secure and Efficient Multi-Secret Image Sharing Scheme Based on Boolean Operations and Elliptic Curve Cryptography. IJPAM 293 – 300
26. Karthick R, TejasK,Ashok K, 2017. High Capacity , Secure(n,n/8) MSIS with security Key. I2C2
27. Mohit Rajput, Maroti Deshmukh, 2016. Secure (n, n+1) – MSIS using Additive Modulo, IMCIP – 2016, 677-683
28. C. Blundo, A. De Santis, and D. R. Stinson, “On the contrast in visual cryptography schemes,” *J. Cryptology*, vol. 12, pp. 261–289, 1999.
29. T. Hofmeister, M. Krause, and H. U. Simon, “Contrast-optimal k out of n secret sharing schemes in visual cryptography,” *Theoreti. Comput.Sci.*, vol. 240, pp. 471–485, 2000.
30. R. Ito, H. Kuwakado, and H. Tanaka, “Image size invariant visual cryptography,” *IEICE Trans. Fund. Electron. Commun. Comput. Sci.*, vol. E82-A, no. 10, pp. 2172–2177, 1999.
31. C. N. Yang and T. S. Chen, “Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion,” *Pattern Recogniti. Lett.*, vol. 26, pp. 193–206, 2005.
32. D. S. Tsai, T. H. Chen, and G. Horng, “A cheating prevention scheme for binary visual cryptography with homogeneous secret images,” *PatternRecognit.*, vol. 40, no. 8, pp. 2356–2366, Aug. 2007.
33. C. N. Yang, A. G. Peng, and T. S. Chen, “MTVSS: (M)isalignment (t)olerant (v)isual (s)ecret (s)haring on resolving alignment difficulty,” *Signal Process.*, vol. 89, no. 8, pp. 1602–1624, Aug. 2009.
34. F. Liu, C. K. Wu, and X. J. Lin, “The alignment problem of visual cryptography schemes,” *Designs Codes Cryptography*, vol. 50, no. 2, pp. 215–227, 2009.
35. S. Cimato, A. DeSantis, A. L. Ferrara, and B. Masucci, “Ideal contrast visual cryptography schemes with reversing,” *Inform. Process. Lett.*, vol. 93, no. 4, pp. 199–206, Feb. 2005.
36. C. N. Yanh, C. C. Wang, and T. S. Chen, “Visual cryptography schemes with reversing,” *Comput. J.*, vol. 51, no. 6, pp. 710–722, 2008.
37. E. R. Verheul and H. C. A. Van Tilborg, “Constructions and properties of k out of n visual secret sharing scheme,” *Designs Codes Cryptography*, vol. 11, no. 2, pp. 179–196, 1997.
38. S. J. Shyu, “Efficient visual secret sharing scheme for color images,” *Pattern Recognit.*, vol. 39, no. 5, pp. 866–880, May 2006.
39. C. N. Yang and T. S. Chen, “Colored visual cryptography scheme based on additive color mixing,” *Pattern Recognit.*, vol. 41, no. 10, pp. 3114– 3129, Oct. 2008
40. Shankar, K., & Eswaran, P. (2015). A secure visual secret share (VSS) creation scheme in visual cryptography using elliptic curve cryptography with optimization technique. Australian Journal of Basic & Applied Science, 9(36), 150-163.
41. AndinoMaseleno, Alicia Y.C. Tang, Moamin A. Mahmoud, Marini Othman, Shankar K, “Big Data and E - Learning in Education”, International Journal of Computer Science and Network Security, Vol.18 No.5, page(s): 171-174, May 2018.

42. M. Miftakul Amin, AndinoMaseleno, K.Shankar, Eswaran Perumal, R.M. Vidhyavathi, Lakshmanaprabu SK, "Active Database System Approach and Rule Based in the Development of Academic Information System", International Journal of Pure and Applied Mathematics Special Issue 1397International Journal of Engineering & Technology, Volume. 7, Issue-2.26, page(s): 95-101, June 2018.
43. Aarti Soni and Suyash Agrawal, "Key Generation Using Genetic Algorithm for Image Encryption", International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 2, issue. 6, page(s):376–383, 2013.
44. Yadav, Gyan Singh, and Aparajita Ojha, "A Novel Multi Secret Sharing Scheme Based on Bitplane Flips and Boolean Operations." ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol I. Springer International Publishing, 2014.
45. Muhammad Muslihudin, RismaWanti, Hardono, Nurfaizal, K.Shankar, Ilayaraja M, AndinoMaseleno, Fauzi, DwiRohmadiMustofa, Muhammad Masrur, Siti Mukodimah, "Prediction of Layer Chicken Disease using Fuzzy Analytical Hierarcy Process", International Journal of Engineering & Technology, Volume. 7, Issue-2.26, page(s): 90-94, June 2018.
46. H. C. Wu and C. C. Chang, "Sharing visual multi-secrets using circle shares," *Comput. Standards Interfaces*, vol. 28, no. 1, pp. 123–135, Jul. 2005.
47. S. J. Shyu, S. Y. Huang, Y. K. Lee, R. Z. Wang, and K. Chen, "Sharing multiple secrets in visual cryptography," *Pattern Recognit.*, vol. 40, no. 12, pp. 3633–3651, Dec. 2007.
48. J. B. Feng, H. C. Wu, C. S, Tsai, Y. F. Chang, and Y. P. Chu, "Visual secret sharing for multiple secrets," *Pattern Recognit.*, vol. 41, no. 12, pp. 3572–3581, Dec. 2008.
49. L. G. Fang, Y. M. Li, and B. Yu, "Multi-secret visual cryptography based on reversed images," in *Proc. Int. Conf. Inform. Comput.*, vol. 4. Jun. 2010, pp. 195–198.
50. K. H. Lee and P. L. Chiu, "A high contrast and capacity efficient visual cryptography scheme for the encryption of multiple secret images," *Opt.Commun.*, vol. 284, no. 12, pp. 2730–2741, Jun. 2011.
51. C. N. Yang and T. H. Chung, "A general multi-secret visual cryptography scheme," *Opt. Commun.*, vol. 283, no. 24, pp. 4949–4962, Dec. 2010.

AUTHORS PROFILE

R.Logeshwari, currently pursuing Ph.D. in Saveetha Institute of Medical and Technical Sciences, chennai. She received the Master's in Computer Science and Engineering from the St.Peter's Institute of Higher Education and Research (Formally known as St.Peter's University) and Bachelor's in Computer Science and Engineering from the Anna University Affiliated institute in 2011 and 2008 respectively. Since 2014, she is working as Assistant Professor in the Department of Computer Science and Engineering at SRM institute of Science and Technology, chennai. Her Research interest include Information Security, Image Processing, Video Processing. She is a member of IET since 2015.

Dr. L. Rama Parvathy, is a Professor in the Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai with 18 years of Academic Training and Teaching students including 8 years of Research. She graduated M.E. Computer Science and Engineering, from Anna University, Chennai and Ph.D. Information and Communication Engineering (I&C) from Anna University, Chennai in Computer Science and Engineering. Her research interests are Cloud Computing, Evolutionary Computing, Multi Objective Optimization and Image Processing. Her Research credential includes 12 international journal publications, two international conference publications and 10 National Conferences. She is a reviewer for reputed International Journals and Coordinator for National Conferences. She is a Subject Matter Expert (SME), Learning Assets Developer (LAD) and Trainer for Corporate companies such as HCL Technolgies, Cognizant Technology Systems.