Multidisciplinary Review Journal

Journal of Critical Reviews

ISSN- 2394-5125 Vol 7 , Issue 9, 2020

VISUAL SECRET SHARING: A REVIEW

L Jani Anbarasi[1] , J.Prassanna[2], Abdul Quadir Md[3], Christy Jackson J[4],R.Manikandan[5], Robbi Rahim[6], G.Suseendran[7]

[1,2,3,4]SCOPE, Vellore Institute of Technology, Chennai, India
[5]School of Computing , SASTRA Deemed University, Thanjavur, India
[6]Department of Management, Sekolah Tinggi Ilmu Manajemen Sukma, Medan, Indonesia
[7]Department of Information Technology, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, India ,
Email id : suseendar_1234@yahoo.co.in

Received: 25.03.2020 ***Revised: 26.04.2020*** ***Accepted: 27.05.2020***

Abstract
Secured transmission is an important concern in today's Internet world in the field of information technology. Recent technological developments in the computer networks have made digital data transmission a popular task and digital images are no exception. Visual Secret Sharing is a process of encrypting an image secret in "n" cipher images termed as shares, that can be transmitted or distributed over an unreliable channel of communication. Secret sharing has been used in various applications to perform a secure communication. This paper details a review of the secret sharing schemes presented by different researchers, its applications and the performance evaluation metrics.

Keywords: Visual Secret Sharing, Image Processing, Shamir secret sharing, PSNR, Correlation Coefficient

DOI: http://dx.doi.org/10.31838/jcr.07.09.221

INTRODUCTION:

Communication of the data is an essential activity that is accomplished through cryptography where sensitive information is encrypted such that only the intended recipients can decrypt the key. Cryptography is a research art in which information is distributed where the specific recipients can intercept it. The Caesar cipher used by Julius Caesar is the oldest cryptographic style. In ancient times, military and government institutions used cryptographic techniques extensively. Security has become the requisite requirement to protect the public data available in the internet. When unknown individuals try to secure data among a group of people, secure distributed computing come into place. This methodology operates in the mutual agreement of the inputs given by groups, where group communication is conducted. Computation is carried out between the interconnected parties. In order to achieve that, the data is encrypted so that it can only be obtained or decrypted by the intended parties. The visual secret sharing encrypts the data into ciphers termed as shares and is made accessible to multiple parties involved in the process. Only when a sufficient number of ciphers termed as shares is pooled by the parties, and then they can restore the secret in a confidential manner.

Secret sharing is used in many applications including the opening of a bank vault, launching a nuclear attack, electronic fund transfer, telediagnosis, and so on. Secret sharing addresses the exceptional security awareness growth of individuals, groups, agencies. Threshold visual secret sharing is a cryptography scheme that encrypts a secret image into n' cipher images called shares or transmitted via unknown communications networks. In order to recover the secret, 't' or more participants must combine their shares, while the secret cannot be retrieved by fewer participants than 't.' Participant as a whole group is useful but individual participant is treated as useless and therefore cannot play any part in the secret reconstruction process.

Secret sharing plays an important role in ensuring the security of the secrets from alteration, data loss and disclosure to wrong individuals. Secret third parties known as the dealer are approached to carefully distribute the secret between 'n' participants in such a way that every single cipher or share has a small portion of the information into it. Secret sharing can generally be classified as a static, threshold and dynamic threshold. 't' or 't+1' threshold can be combined to re-construct a single secret in threshold-based schemes, whereas the secret is not modified in the static schemes after sharing.The shares should be redistributed proactively to participants with the same or different secrets at regular intervals. The presumption that participants would be truthful during the entire process will not result in the secret sharing of most applications in real time.

Shamir Secret Sharing for Single Secret

The Secret Sharing schemes which are used in various fields was introduced by Shamir et al (1999) [1]. The two main phases of secret sharing are encryption and reconstruction. During the sharing process secret information called as shares that are created and distributed to the participants by the dealer. Suitable participants are combining their shares to restore confidentiality in the reconstruction process by a trusted group named dealer.

In order to fragment a secret 'X' into 'n' parts, so that 'X' can be easily reconstructed from any 'm' parts, are defined by Shamir (1979) is refereed as (m, n), where a full knowledge of (m – 1) parts does not reveal any information on 'X'. The Shamir schemeused a secret 'X' and a prime number 'x' to generate a polynomial of (m-1) degree as given in the Equation (1).The $D_1, D_2 \dots D_{m-1}$ are the random coefficients that can range from 1 to t-1. The shares are generated for every participantas $Y_i$are given using equation 2.

$$F(Q) = X + D_1Q^1 + D_2Q^2 + \cdots . D_{m-1}Q^{m-1} \;\; mod\ t \qquad (1)$$

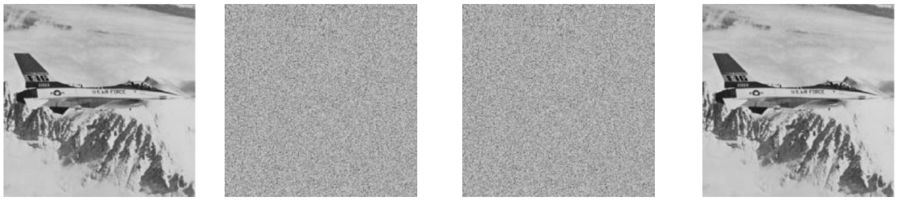
$$Y_1 = F(K_1)Y_2 = F(K_2) \dots \dots . Y_n = F(K_n) \qquad (2)$$

Lagrange's interpolation is used to reconstruct the secret and is given in equation 3 and 4.

$$L = \sum_{j=0}^{m} Y_j l_j\, (Q) \qquad (3)$$

$$I_j(Q) = \prod_{\substack{0 \le t \le m \\ t \ne j}} \frac{Q - Q_t}{Q_j - Q_t} \qquad (4)$$

The secret and the shares created for two participants are shown in the figure 1.

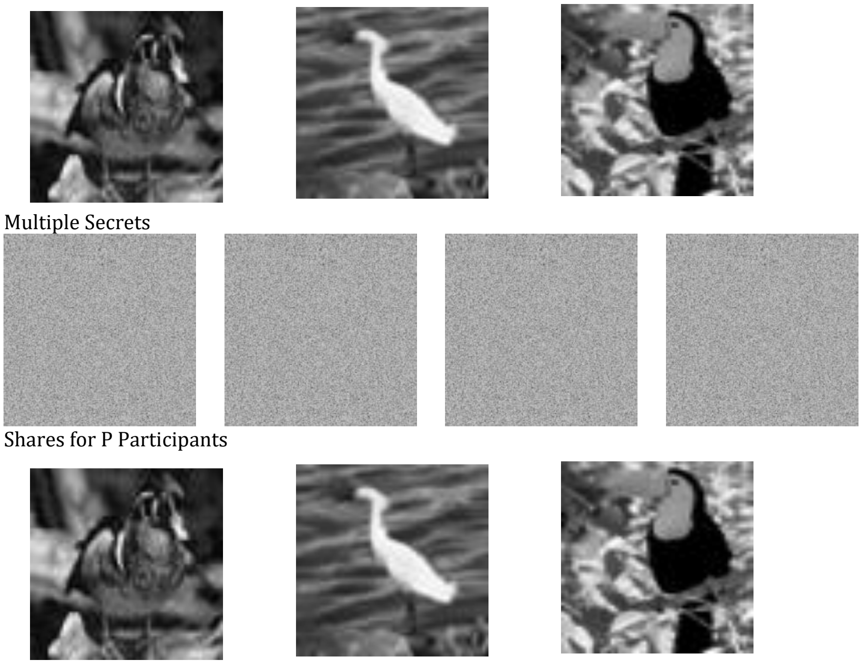


Secret Share 1 Share 2 Reconstructed Secret

Fig 1: Secret Sharing using Shamir Model

Smaller shares were created by Thien& Lin [2] and later Lin & Tsai [3] enhanced the secret sharing by including steganography, and verification process. Steganography resulted in the meaningful shares. Chang et al [4,5] generated shares using Chinese remainder theorem along with stego shares. Ulutas et al (2011b) [6] have proposed a secret sharing framework (t,n) that shares medical images along with the Electronic Patient Record and is reconstructed without loss between 'n' clinicians. Eslami&Ahmadabadhi (2011) [7] suggested a secret sharing system using a chaining technique. Kishor et al [8] used the Shamir's secret sharing method to authenticate the server using hashing and this scheme also used threshold cryptography to authenticate and reconstruct the passwords.

Similarly secret sharing can also be performed for multiple secrets where the threshold has to be chosen either less than the number of secrets or greater than the secrets.Anbarasi et al [10,12] performed multiple secret sharing using DNA based cryptography along with EPR contents. Also Shamir secret sharing was also performed using 3D models and retrieved the watermark efficiently from color images [11,13]. Selective qubits positioning can be performed using quantum secret sharing and secret reconstruction process [9]. Adel et al [14] performed multi secret sharing using Berkley's method which is based on hyper planesinterception and reconstructed the secrets using linear complementary (LCD) codes.Selda et al [15] proposed a multi secret sharing scheme over finite fields where determining the access structure plays a major role in obtaining a perfect and ideal scheme. Na Wang et al [16] proposed a verifiable secret sharing scheme along with information privacy protection using a simple structure. The participants can verify their correctness based on the information publicly given by the dealer. This prevents the fake users in restoring the original secret.Mayank et al [17] proposed a single secret sharing scheme using neutral cryptography scheme. Neutral cryptography is a new algorithm based on the number theory which has advantageous over memory and computation time. This scheme allows the secret information to flow in the public domain.Azza1 et al [18] proposed a multi secret sharing based on elementarycellular automata along with steganography. Since steganography is used the generated shares are meaningful shares. Kumar et al [19] proposed an end to end verifiable platform to check whether the system has correctly counted the recorded ballots or not. New identity based blind short signature scheme is used for the process and the privacy is achieved using Elliptic curve cryptography. Figure 2 shows the shares created using a multiple secrets.



Multiple Secrets

Shares for P Participants

Reconstructed Multiple Secrets

Fig 2: Multiple sharesconstructedusing multiple secretimages

Performance Evaluation

Various performance analyses performed to show the secureness of the secret sharing are computed among the shares and the secret reconstruction is detailed as follows.

a)Correlation Coefficient

In order to avoid statistical attack, it is very important to reduce the association between two adjacent pixels. In the original image and sharing image, the correlation coefficient of adjacent horizontal and diagonal pixels is examined. The correlation plot reveals that the secret pixel values are focused to display strong correlation and the share pixels are evenly distributed, indicating less correlation and is given in table 1.

$$cov(m,n) = \frac{1}{X}\sum_{j=1}^{X}(m_j - E(m))\,(n_j - E(n)) \quad (5)$$

Table 1: Correlation coefficient achieved

Ref	Correlation coefficient of the Shares	Correlation coefficient of the Reconstructed Secret
[17]	0	0.99
[18]	-0.015	1
[10]	0	**1**
[12]	0	**1**

b) Peak to Signal Noise Ratio (PSNR)

Mean Square Error is an estimator measure that indicates how the estimator varies from what is predicted. In relation to the variance and degree of distortion from original secrets MSE accesses the quality of the reproduced image.The highest possible signal and the corrupting values due to noise, which influences the fidelity of its representation between the reconstructed and the original data is determined using the PSNR. PSNR values are is high if the similarity is more and is shown in table 2.

$$MSE = \frac{1}{YXZ}\sum_{i=1}^{Y}\sum_{j=1}^{Z}(m_{ij} - n_{ij}) \quad (6)$$

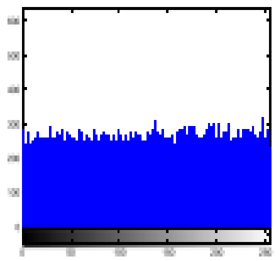
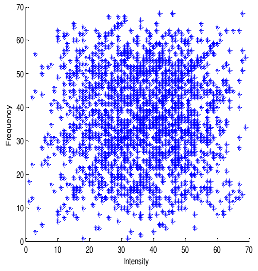
$$\text{PSNR} = 10\times 10\log\left[\frac{255^2}{\text{MSE}}\right]\text{dB} \quad (7)$$

Table 2: Peak Signal to Noise Ratio achieved

Ref	PSNR between the Secret and Shares		PSNR between the Reconstructed Secret and the original secret
	PSNR	RMSE	PSNR
[17]	27	10	
[18]			54.0674
[10]	7.5		49
[12]	12		51

d)Histogram Distribution Analysis

Histogram represents the frequency of the gray value of an image. If the distributed values are identical, then the encrypted shares are stronger against statistical and differential attacks. The histogram distribution of the secret and the generated shares are shown in figure 3.

Ref	Histogram of shared image
[18]	
[10	

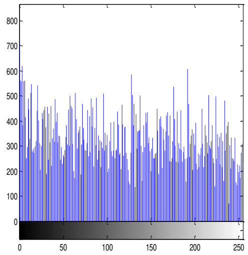
[12]	

Fig 3:Histogram distribution of the generated shares

e) Influence of similarity of some secret images are computed using UACI The UACI measure the mean intensity differences between two images' pixels, where UACI's expected value is almost equal to 33 percent for two random images and is given in table 3.

$$UACI = \frac{1}{MXN}\left(\sum_j \sum_j \frac{S(i,j)-O(i,j)}{255}\right) * 100 \quad (8)$$

Table 3: Similarity index using UACI and NPCR

Ref	NPCR	UACI
[18]	0.9933	0.3293

f)Bit Error Rate identifies the modification that has been occurred with respect to every bits and its almost 0.76 in achieved [18].

Table 4 shows the various comparison that exists among the research works.

	[16]	[17]	[18]	[10]	[12]	[13]	[19]
Resist Cheating by the Dealer	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Resist Cheating by the Participants	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Can be accessed in public Domain	Yes	Yes	Yes	Yes	Yes	No	Yes
Reuse of the Shares	Yes	Yes		No	No	No	
Single Secret	No	Yes				Yes	
Multiple Secret			Yes	Yes	Yes		
Meaningful Shares			Yes	No	No	No	No

CONCLUSION:

This paper highlighted the different facets of secret sharing metrics that are carried out to protect the multimedia material. Several secret sharing algorithms are investigated and a comprehensive literature review is presented in this paper.This paper details a review of the secret sharing schemes presented by different researchers, its applications and the performance evaluation metrics. The future work can be concentrated in the following areas: Unfair participants can mislead honest participants by pooling forged shares resulting in illegal secret reconstruction. In order to prevent forged shares from pooling, verification must be carried out. Cryptanalysis can be automated to detect fake shares, using self-adaptive search optimization techniques.

REFERENCES

1. Shamir, A 1979, 'How to share a secret', Communications of the ACM, vol.22, pp.612-613.
2. Thien, CC & Lin, JC 2002, 'Secret image sharing', Computers & Graphics, vol.26, pp.765–770.
3. Lin, CC & Tsai, WH 2004, 'Secret image sharing with steganography and authentication', The Journal of Systems and Software, vol.73, pp. 405–414.
4. Chang, CC, Lin, CC, Lin, CH & Chen, YH 2008, 'A novel secret image sharing scheme in color images using small shadow images', Information Sciences, vol.178, pp.2433-2447.
5. Chang, CC, Chen, YH & Wang, HC 2011, 'Meaningful secret sharing technique with authentication and remedy abilities', Information Science, vol.181, pp. 3073–3084.
6. Ulutas, G, Ulutas, M &Nabiyev, V 2011, 'Distortion free geometry based secret image sharing', Procedia Computer Science, vol.3, pp. 721–726.
7. Eslami, Z &Ahmadabadi, JZ 2011, 'Secret image sharing with authentication-chaining and dynamic embedding', The Journal of Systems and Software, vol.84, pp. 803–809.
8. Gupta, KishorDatta, et al. "Shamir's Secret Sharing for Authentication without Reconstructing Password." 2020 10th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2020.
9. Musanna, F., & Kumar, S. (2020). Quantum secret sharing using GHZ state qubit positioning and selective qubits strategy for secret reconstruction. arXiv preprint arXiv:2002.09182.
10. Anbarasi, L. Jani, GS Anandha Mala, and ModigariNarendra. "DNA based multi-secret image sharing." Procedia Computer Science 46 (2015): 1794-1801.
11. Anbarasi, L. Jani, and Anandha Mala. "Verifiable Multi Secret Sharing Scheme for 3D Models." International Arab Journal of Information Technology (IAJIT) 12 (2015).
12. Anbarasi, L. Jani, and Anandha Mala. "EPR Hidden Medical Image Secret Sharing using DNA Cryptography." International Journal of Engineering and Technology 6 (2014): 1346-1356.
13. Narendra, Modigari, et al. "An efficient retrieval of watermarked multiple color images using secret sharing." 2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN). IEEE, 2017.
14. Alahmadi, Adel, et al. "A Multisecret-Sharing Scheme Based on LCD Codes." Mathematics 8.2 (2020): 272.
15. Çalkavur, Selda, and Patrick Solé. "Some multisecret-sharing schemes over finite fields." Mathematics 8.5 (2020): 654.
16. Wang, Na, et al. "Information Privacy Protection Based on Verifiable (t, n)-Threshold Multi-Secret Sharing Scheme." IEEE Access 8 (2020): 20799-20804.
17. Gupta, Mayank, Manu Gupta, and MarotiDeshmukh. "Single secret image sharing scheme using neural cryptography." Multimedia Tools and Applications (2020): 1-22.

18. Azza, A. A., and ShiguoLian. "Multi-secret image sharing based on elementary cellular automata with steganography." MULTIMEDIA TOOLS AND APPLICATIONS (2020).
19. Kumar, Mahender, Satish Chand, and C. P. Katti. "A Secure End-to-End Verifiable Internet-Voting System Using Identity-Based Blind Signature." IEEE Systems Journal (2020).