Digital Image Secure Share Creation Techniques Analysis: A Survey

C. Devi Parameswari, K. Shankar

Abstract*: Security is a significant concern in data innovation that managing the web world today. In sharing based technique shares are created, encoded and stored into digital form. This paper discussed the various papers in secret share creation for image security like visual secret share creation, Chinese remainder theorem, Shamir secret sharing and so on. In this design, a secret image is programmed into n shadows of the random model. It is possible to interpret the secret image externally by overlay a certified subset of shadows. These shares are uncovering the secret image to assume to be imprinted on transparencies and in the wake of stacking them to one another. Here more than fifteen papers are analyzed; those papers are gathered from IEEE, Springer, Elsevier and some other Journals. In addition, security measures are analyzed for all image secret sharing procedure.

***Keywords* : Image security, Share Creation, Visual and cryptography..**

I. INTRODUCTION

Decryption process can be achieved by stack the shares over one another & see the secret image, which shows up the stacked shares through human visual framework [1]. Share the production of parallel image from the secret image is trailed by the watermarking strategy that gives the additional protection in excess of the essential visual cryptography method[2]. Thus, the security of advanced data against unapproved access has turned into a [3] prime goal. So as to handle this issue, different various technologies developed in the ongoing occasions, for example, steganography, encryption, multi-secret image sharing scheme [4-6] (figure 1). The symmetric key image necessitates the private key to share by each link of convey gatherings, & moreover, the key to be shared in a tied down medium [7]. In any case, first share created by this research is also not absolutely random image [8]. The technique varies from the customary secret sharing, which does not require troublesome cryptographic systems [9] and calculation. Rather, it very well may be make out directly by the individual delineation framework. Secret sharing plan can be utilized for circumstances where consent to get to the basic data relies upon a few people, not on a person. In this way, without all members, basic or secret data can't be recovered from individual share for image security [10].

A. Influences of Share Generation for Security

- Each secret pixel of the first binary image is changed over into four sub-pixels of two share images & recouped by basic stacking process. This is capable of utilizing logical OR operation among the shares.
- In Visual cryptography, the image is separated into n shares and that is circulated into n number of participants.
- The decoder can quick recuperate the secret by utilizing human eyes without the assistance of calculating devices. Secret sharing scheme can utilize XOR based visual cryptography plan to encode two secret images into two shares.
- Decrypting secret image by covering or stacking the secret image.
- The exposure of the binary secret shares is overwhelmed by concealing them undetectably into some host images.

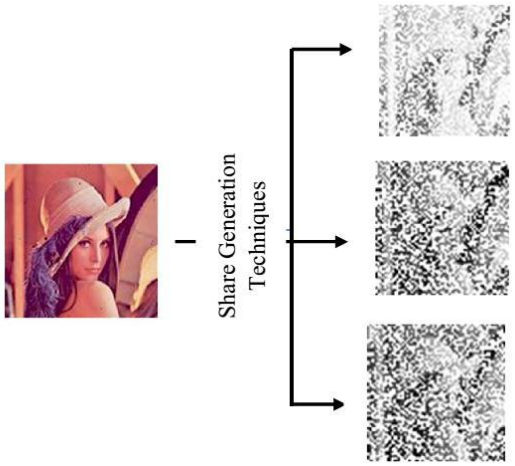


Fig. 1. Share Generation Model

II. REVIEW OF LITERATURE

Author: Yan, X et al.2019 [11]
Technique: Image secret sharing
Description: The secret image can be decoded by gathering adequate shares. Recently, several Image Secret Sharing (ISS) schemes were presented, among which polynomial-based ISS plot. Four security Levels were delegated well as the security of run of ISS plans was analyzed.
Pros & Cons: The benefits of a number of pixel extension and

Revised Manuscript Received on December 16, 2019.
***** Correspondence Author
C.Devi Parameswari*, Department of Computer Applications, Kalasalingam Academy of Research and Education, Krishnankoil, India. Email: deviparameswari6@gmail.com
K.Shankar, Department of Computer Applications,, Alagappa University, Karaikudi, India.
Email: shankarcrypto@gmail.com

codebook plan and cons of the article is, not viewed as general access structure for producing shares.

Author: Hu, W.,et al.2018 [12]
Technique: Image secret sharing with ODRM-CA
*Description:*1 D Reversible Memory Cellular Automata creates shadow images with ISS plot with no outsider encryption technique. To expand the principles of cellular sum& neighbor sweep to actualize the encryption procedure for the secret image.
Pros & Cons: High computational performance & parallel registering of cell automata to decrease the power utilization in this technique. The fundamental disadvantage is a multidimensional procedure, unfit to consider, so its impact the security procedure.

Author: Shankar, K et al.2018 [13]
Technique: Secret Image Sharing (SIS)
Description: Wavelet-based secret image sharing method was projected with encrypted shadow images utilizing ideal HE procedure. The encrypted shadow preserve be recuperated only by picking subset of 'n' shadows which formulates apparent& stack over one another.
Pros & Cons: Number of wavelets based on the shares are produced, so the calculation time of share generation is low and the disservice is its colossal procedure, the reason is optimization are considered, however, the security is high.

Author: Guo, Y et al. 2016 [14]
Technique: Quantum secret sharing (QSS)
Description :A quantum route selection dependent on the encoded quantum graph state, subsequently empowering the reasonable QSS conspires in little scale complex quantum arrange. The Chinese Remainder Theorem (CRT) fortifies the security of recuperating procedure by underlying secret between legitimate members.
Pros & Cons: Pros of QSS-CRT is to give genuinely verify data exchange. The protection is fortified by CRT in the secret division & recuperation stages that prompt the believability of the lawful members.

Author: Chahar, H, et al.2017 [15]
Technique: Shamir's secret sharing scheme
Description: The primary protocol utilizes the idea of Elliptic-bend based Paillier cryptosystem, those aides in accomplishing the integrity of communication. Nevertheless, the intrigue of two locales could influence the protection of individuals. To tackle this issue, the author consolidate Shamir's secret sharing plan in the second protocol.
Pros & Cons: It is lone wants "k" shares for decode the distortion less mystery image; it necessitates increasingly confounded calculation and furthermore averting the impact. The PSNR and computational expense is high real-time applications

Author: Wang, B.-J, et al. 2018 [16]
Technique: Random grid-based visual secret sharing
Description: VC and random grid have been created as of late. As both VC and RG have been considered as a protected route for communicating with high security. Two RG-based VSS schemes with misrepresentation counteractive action for the instances of (2, n) and (k,n).
Pros & Cons: It does not keep up any extra share, the pixel development is maintained a strategic distance from the contrast with the custom VSS plot and the computation cost in the encoding stage is exceptionally low.

Author: Wu, M, et al.2017 [17]
Technique: secret sharing Scheme
Description: To secure the protection data of images on distributed storage space, intend an incorporated plan including indiscernible watermarking, cover and mystery sharing methods. The histogram modification based plan could accomplish reversible information stowing away to guarantee the reliability and discretion of image information.
Pros & Cons: The invisible watermarking in the picture, afterward change the watermarked image into the conceal image and secure the picture protection on distributed storage when the non-verified client can't recover the satisfactory key.

Author: Sharma, H et al.2011 [18]
Technique: Cover Image Share Embedded security algorithm (CISEA)
Description: A CISEA was to create significant offers from the mystery image. This idea for the age of tribute images of a spread image over which offers secret image was to be implanted.
Pros & Cons: Simplicity of use of this plan is one of its real merits and the Security standard is expanded contrasting with that given by regular visual cryptography conspire and furthermore it gives one more layer of security.

Author: Karthik, R et al.2018 [19]
Technique: Multi Secret Image Sharing Scheme (MSIS)
Description: MSIS is an effective & vigorous strategy for transmitting at least one secret image safely. One could recoup fractional secret data from n-1 or less shared image, which postures chance for the private data encoded.
Pros & Cons: Sharing limit is expanded by multiple times because of that simpler to exchange the shares whereas exchanging enormous datasets of images. Since the examination images need to be not sent straightforwardly, the secret images offer stays safe to the hackers.

Author: Shankar, K. et al.2016 [20]
Technique: RGB-Based Secure Share Creation
Description: The multiple shares were utilized to exchange the secret image by utilizing encryption & unscrambling procedure by methods for the ECC system. The public key is arbitrarily created in encryption procedure & unscrambling process, the private key (H) is produced by using the enhancement system and for assessing the presence of optimization by utilizing PSNR.
Pros & Cons: the confidentiality of the image is maintained over the long haul & the recovered image furthermore ten MSE is minimal high for security investigation.

Author: Gharahi, M, et al.2018 [21]

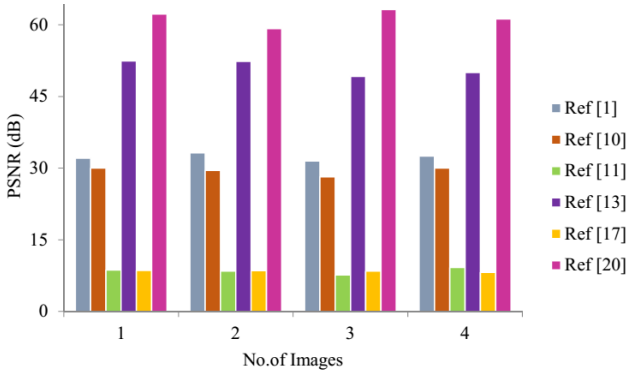
Technique: Optimal Linear Secret Sharing
Description: Optimal information ratio (OIR) of an entrance formation is the infimum of data proportions of all secret sharing plans acknowledging it. At the point when the infimum was assumed to control on the whole direct secret sharing plans, it is known as OLIR. Improved upper limits are accomplished by developing a straight secret sharing plan, utilizing an appropriate decomposition system for each entrance structure.
Pros & Cons: A probability distribution on the secrets and that this distribution is known. It's diminished decreases the calculation overhead.

III. ANALYSIS

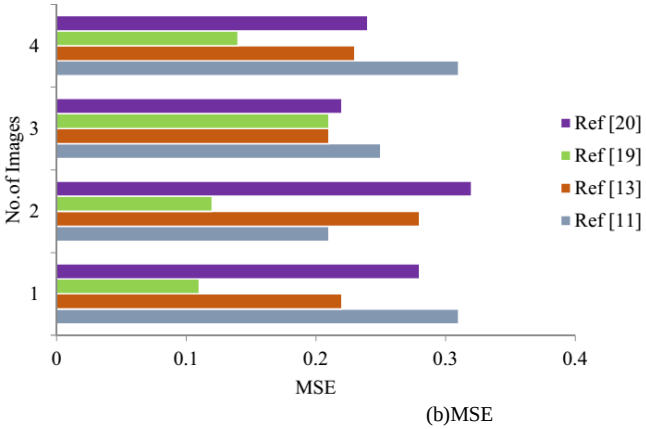
This section discussed some results in securing sharing techniques in terms of Reference Numbers. Here considerable parameters PSNR, CC, Means Square Error (MSE) and Structural Similarity Index (SSIM).

Ref Number	Performance Measures
[1]	PSNR, CC
[2]	Authentication Capability (%) and Image Quality
[10]	PSNR
[11]	PSNR, MSE, and SSIM
[13]	PSNR Entropy, MSE, MAE and CC
[17]	PSNR, SSIM
[19]	SSIM, PSNR, and RMSE
[20]	PSNR, CC, and MSE

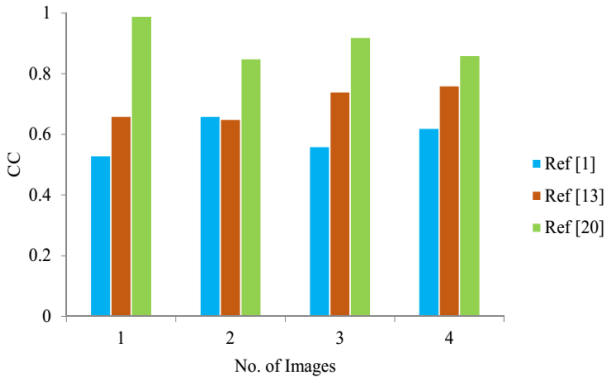
Table 1 explains the measures which are analyzed for the existing research papers that is referred as [1], [2], [10], [11], [13], [17], [19] and [20]. For [1], PSNR and CC are examined; the paper [2] explains the Authentication Capability (%) and Image Quality, [3] investigated PSNR, likewise, other measures are described in the table.



a) PSNR



(b)MSE



(c) CC

Fig. 2. Comparative Analysis

Figure 2 explains the comparative analysis of three performance measures such as PSNR, MSE, and CC. For PSNR analysis, four images are considered and compared among six different research techniques. The highest PSNR value is attained in ref [20] for all the images. For MSE analysis, Lena image achieves 0.28 error rate, likewise, other images are analyzed and compared among ref [20], ref [19], ref [13] and ref [11]. In addition to this, the measure CC is analyzed among four images and compared with ref [1], ref [13], and ref [20].

IV. CONCLUSION

This Chapter expresses to the overview of different secure offer creation for image security and literary works. The significant image transfer will happen over the unbound internet organize. Thus Security is the significant worry for any framework to keep up the honesty, confidentiality and image genuineness. Every method is novel in its own specific manner and this makes it reasonable for some applications. Specific image encryption procedure gives great image quality at the recipient side while different gives debased images, likewise certain picture encryption method by the created offers. From this survey analysis, the optimal ECC method produce the better security level and maximum performance metrics like PSNR, CC, MSE, MAE and a few parameters. From the investigation, all offer creation methods get greatest verifying progressively applications.

REFERENCES

1. Wang, P., He, X., Zhang, Y., Wen, W. and Li, M., 2019. A robust and secure image sharing scheme with personal identity information embedded. Computers & Security. .
2. Dayanand, I.E. and Kumar, R.S., 2014. Analysis of secret image sharing using a shared image. International Journal of Computer Applications, 108(7).
3. Alsmadi, D. and Prybutok, V., 2018. Sharing and storage behavior via cloud computing: Security and privacy in research and practice. Computers in Human Behavior, 85, pp.218-226.
4. Sharma, H., Kumar, N. and Jha, G.K., 2011, September. Enhancement of security in Visual Cryptography system using Cover Image share embedded security algorithm (CISEA). In 2011 2nd International Conference on Computer and Communication Technology (ICCCT-2011) (pp. 462-467). IEEE.
5. Huang, C.P. and Li, C.C., 2006, October. A secret image sharing method using integer multiwavelet transform. In 2006 International Conference on Image Processing (pp. 1969-1972). IEEE.
6. Weir, J. and Yan, W., 2010. A comprehensive study of visual cryptography. In Transactions on data hiding and multimedia security V (pp. 70-105). Springer, Berlin, Heidelberg.
7. Pratt, W.K. ed., 1979. Image transmission techniques (No. 12). New York: Academic Press.
8. Elhoseny, M., Shankar, K., Lakshmanaprabu, S.K., Maseleno, A. and Arunkumar, N., 2018. Hybrid optimization with cryptography encryption for medical image security in Internet of Things. Neural Computing and Applications, pp.1-15.
9. Bai, L., 2006, September. A reliable (k, n) image secret sharing scheme. In 2006 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (pp. 31-36). IEEE.
10. Chen, Y.F., Chan, Y.K., Huang, C.C., Tsai, M.H. and Chu, Y.P., 2007. A multiple-level visual secret-sharing scheme without image size expansion. Information Sciences, 177(21), pp.4696-4710.
11. Yan, X., Liu, L., Lu, Y. and Gong, Q., 2019. Security analysis and classification of image secret sharing. Journal of Information Security and Applications, 47, pp.208-216.
12. Hu, W., Yao, Y., Zhou, D., Zheng, Q. and Choo, K.K.R., 2018. A Novel Image Secret Sharing Scheme without Third-Party Scrambling Method. Mobile Networks and Applications, pp.1-19.
13. Shankar, K., Elhoseny, M., Kumar, R.S., Lakshmanaprabu, S.K. and Yuan, X., 2018. Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique. Journal of Ambient Intelligence and Humanized Computing, pp.1-13.
14. Guo, Y., Luo, P. and Wang, Y., 2016. Graph state-based quantum secret sharing with the chinese remainder theorem. International Journal of Theoretical Physics, 55(11), pp.4936-4950.
15. Chahar, H., Keshavamurthy, B.N. and Modi, C., 2017. Privacy-preserving distributed mining of association rules using Elliptic-curve cryptosystem and Shamir's secret sharing scheme. Sādhanā, 42(12), pp.1997-2007.
16. Wang, B.J., Chen, T.S., Jeng, F.G. and Chen, T.H., 2018. On the security of threshold random grid-based visual secret sharing. Multimedia Tools and Applications, pp.1-24.
17. Wu, M.Y., Yu, M.C., Leu, J.S. and Chen, S.K., 2017. Enhancing security and privacy of images on cloud by histogram shifting and secret sharing. Multimedia Tools and Applications, pp.1-21.
18. Sharma, H., Kumar, N. and Jha, G.K., 2011, September. Enhancement of security in Visual Cryptography system using Cover Image share embedded security algorithm (CISEA). In 2011 2nd International Conference on Computer and Communication Technology (ICCCT-2011) (pp. 462-467). IEEE.
19. Reddy, K., 2017. High Capacity, Secure (n, n/8) Multi Secret Image Sharing Scheme with Security Key. arXiv preprint arXiv:1710.09550.
20. Shankar, K. and Eswaran, P., 2016. RGB-based secure share creation in visual cryptography using optimal elliptic curve cryptography technique. Journal of Circuits, Systems and Computers, 25(11), p.1650138.
21. Gharahi, M. and Khazaei, S., 2019. Optimal linear secret sharing schemes for graph access structures on six participants. Theoretical Computer Science, 771, pp.1-8.

AUTHORS PROFILE

C.Devi Parameswari received her B.Sc and M.Sc (Computer Science) from Madurai Kamaraj University in 2013 and 2018 respectively. Now, she is a Research Scholar in the Department of Computer Applications, Kalasalingam Academy of Research and Education, Krishnankoil, Tamilnadu, India. Her current research areas include cryptography, secret image sharing scheme, Image security.

Dr. K. Shankar. received the M.C.A., M.Phil., and Ph.D. degrees in computer science from Alagappa University, Karaikudi, India. He is currently Post Doc Fellow in the Alagappa University, Karaikudi, India. He has several years of experience in research, academia, and teaching. Collectively, Dr. K. Shankar authored/co-authored over 38 ISI Journal articles (with total Impact Factor 99.636) and 107 Scopus Indexed Articles. Dr. K. Shankar guest-edited several special issues at many journals published by Inderscience and MDPI. He has been a part of various seminars, paper presentations, research paper reviews, and conferences as a convener and a session chair, a guest editor in journals. He has authored or co-authored many research papers in reputed journals and conferences. He serves as the reviewer in some SCI indexed Journals like IEEE, Elsevier, Springer and the IEEE conferences. He displayed vast success in continuously acquiring new knowledge and applying innovative pedagogies and has always aimed to be an effective educator and have a global outlook. His current research interests include Secret Image Sharing Scheme, Digital Image Security, Cryptography, Internet of Things, Healthcare applications and Optimization algorithms.