IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Secure Image Encryption Using Share Authentication and Visual Cryptography

[1]VEMALI NAGAMANI,
Student in Dept. Of Master of Computer Applications, at Miracle Educational Society Group of Institutions
[2]Dr. S SRIDHAR, Miracle Educational Society Group of Institutions
[3]DATLA RAJITHA, Miracle Educational Society Group of Institutions
[1]manivemali2000@gmail.com

ABSTRACT:

Image Secret Sharing (ISS) is an efficient method of safeguarding sensitive image information by dividing it into multiple shares. This project presents a robust (k, n) threshold ISS model with both dealer participatory and non-participatory authentication. A combination of Visual Secret Sharing (VSS) and encryption by a polynomial yields lossless decryption with low computational overhead and no pixel expansion. The shares can be screened for authentication, which enhances security without transmission. The proposed method enables bounding and efficient verifiable decryption with a high fidelity image. This method is suited for identity management, cloud storage, and digital watermarking where privacy and integrity are essential.

Keywords: Cryptography, Image Decryption, Secret Sharing

INTRODUCTION

Protecting images and multimedia content has become critical in the digital era due to their use in identity verification, blockchain, watermarking, and cloud storage. Conventional cryptographic methods are efficient but can be exploited if the media is damaged or lost. Image Secret Sharing (ISS) is a robust technique of cryptography which has gained prominence as it splits an image into multiple dangerously close to impossible shares to reconstruct without a minimum threshold number of shares. This project investigates a hybrid implementation of polynomial cryptography and Visual Secret Sharing (VSS) in the (k,n) threshold ISS system to improve security. The originality of the system stems from its special two-tiered participative and non-participative dealer authentication system which enables distortion free and data leakage free flexible pathways during decryption. With the introduction of a screening filter and a YXOR based encryption method, the project achieves strong image protection at a low computational cost, which serves a growing market for image transmission and storage systems.

RELATED WORK

The area of image secret sharing ISS has grown rapidly, motivated by the desire to transmit and store multimedia data securely. One of the earliest

works, Shamir (1979), proposed polynomial based (k,n) threshold secret sharing in which a secret is distributed in such a way that it can only be reconstructed by a specified number of shares which ensures strong confidentiality to unauthorized users. A. A. El-Latif et al. (2020) build on this idea with a quantum walk based encryption for 5G-IoT environments in understanding the problem of secured data transmission in distributed networks. This provides an insight into the possibility of using classical cryptography and quantum computing for advanced secure multimedia systems. X. Zhang et al. (2018) developed a coverless image steganography technique based on Discrete Cosine Transform (DCT) and Latent Dirichlet Allocation (LDA). This technique was a step forward in image steganography as a modification of the original image was not necessary—this concept could aid in image security within ISS systems. M. Fukumitsu et al. (2017) studied the application of blockchain technology and secret sharing in a P2P storage system. Their research proved that blockchain's decentralized nature could strengthen the system's integrity and non-participatory authentication of the shared image data, thus reinforcing the reliability and traceability of the data. Y. Cheng et al. (2018) proposed a VSS for QR codes where the shares are also QR codes that are readable. This contribution was in line with the objective of non-suspicious image sharing as it provided improved usability and compactness. Y. Li and L. Guo (2018) proposed a sparse coding technique for image fingerprinting which was distortion-resistant and provided a recognition accuracy that was markedly high. This work illustrates the necessity of steganographic image preservation when it comes to the fidelity of decrypted outputs.

TABLE1. Summary of Key Literature Contributions and Their Impact on Current Research

Author(s)	Contribution	Impact on Research
Shamir (1979)	Introduced polynomial-based (k, n)-threshold secret sharing.	Laid the foundation for secure image division and reconstruction methods.
El-Latif et al. (2020)	Developed quantum walk-based encryption for 5G-IoT secure data transfer.	Inspired future-proof ISS systems integrating quantum security principles.
Zhang et al. (2018)	Proposed coverless steganography using DCT and LDA topic classification.	Strengthened ISS systems by minimizing image alteration and improving detection safety.
Fukumitsu et al. (2017)	Combined blockchain with secret sharing for P2P secure storage.	Supported decentralized and tamper-resistant share authentication schemes.
Cheng et al. (2018)	Created QR-based VSS where shares are valid QR codes.	Promoted usability and stealth in image sharing applications.

PROPOSED APPROACH

This project proposes a hybrid image secret sharing (ISS) framework that is tailored for efficient and

secure image transmission based on a (k, n)-threshold model. What sets this method apart is its capability to facilitate both dealer participatory and dealer non-participatory share verification, adding to its flexibility and dependability during the decryption phase. This method integrates Shamir's polynomial-based secret sharing and Visual Secret Sharing (VSS) to achieve high-quality image protection while maintaining low overhead. During the encryption phase, a secret image is concealed within an authentication image by means of a proprietary LSB embedding method based on XOR. The image is then transformed using randomized techniques to create multiple encrypted share images. These shares are distributed to the users separately. For confirming the authenticity of each share, a special screening method is used which greatly improves security by not requiring the original share to be sent. In the decryption phase, any k or more shares can be used to reconstruct the secret image, which is restored fully without expansion or data loss. This method is useful for identity authentication, secure cloud storage, and sharing medical images as it enables lossless recovery, is tamper-resistant, and is low on computational resources.

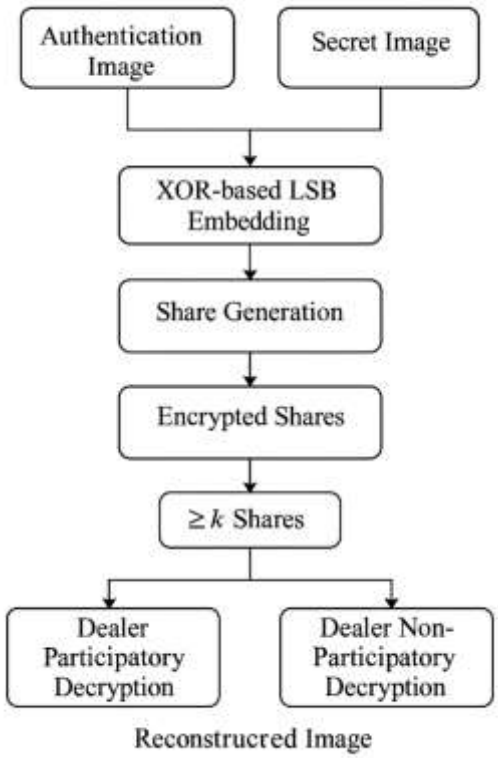


Figure 1: Proposed Secure Image Authentication System

METHODOLOGIES

Image Upload and Preprocessing

Users upload two images: the authentication image and the secret image. These images are resized and aligned for compatibility. Input parameters kkk and nnn are set to define the threshold model.

Image Encryption and Embedding

The secret image is hidden inside the authentication image using a customized **XOR-based Least Bit Substitution (LBS)** method. This process merges image pixel bits in such a way that the secret content is not visually detectable.

Share Generation

The resulting embedded image is divided into k×nk \times nk×n encrypted shares using randomized

transformations. The system applies increasing XOR randomization with pseudo-random values, ensuring that each share is unique and resistant to brute-force attacks.

Authentication and Decryption

For decryption, any kkk or more shares are collected. Using **Lagrange interpolation**, the secret image is reconstructed without relying on the original dealer. This is supported in both **dealer participatory and non-participatory modes**, improving flexibility.

Security Validation and Performance Measurement

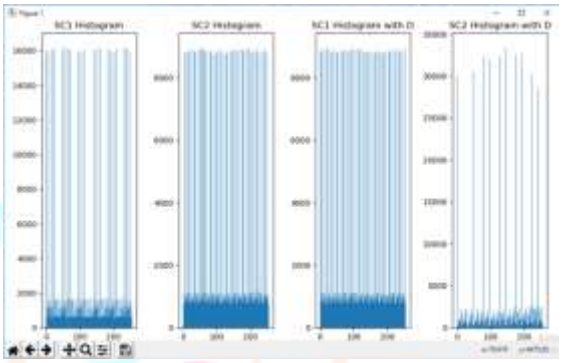
A histogram analysis of the encrypted shares is conducted to evaluate randomness. Execution time for both encryption and decryption is recorded and plotted for performance benchmarking.

RESULTS

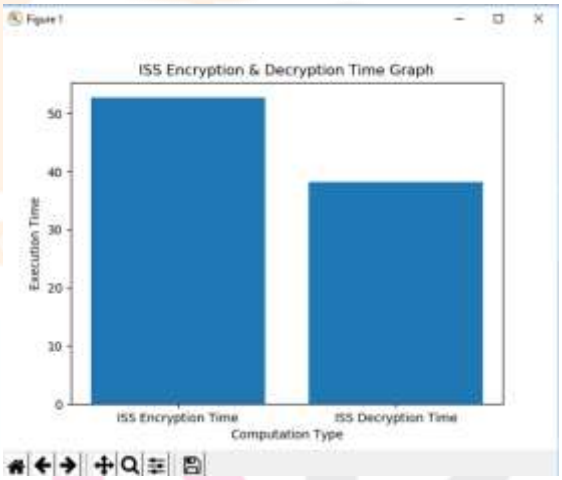
The implemented Image Secret Sharing (ISS) system successfully demonstrated its ability to securely encrypt and decrypt secret images using the proposed (k, n)-threshold method. During the encryption process, the secret image was embedded into an authentication image using a XOR-based LBS mechanism, followed by division into four encrypted shares (2x2 configuration). The resulting shares appeared visually distorted, confirming effective concealment.

Upon reconstruction, any two of the four shares (as per k=2k = 2k=2) were sufficient to retrieve the hidden image. The **decrypted image matched the original secret image** with no pixel expansion and no visible distortion, validating the **lossless recovery** capability.

Additionally, histogram analysis of the encrypted shares revealed dense, evenly distributed patterns an indicator of high entropy and strong resistance against statistical attacks. Time analysis graphs illustrated that encryption consumed slightly more time than decryption due to the complexity of XOR transformations and image division logic.



In Graph for each share from SC1, SC2 and D we can see histogram graph and all graph contains dense values so image is more secured



In above graph x-axis represents computation type like encryption and decryption and y-axis represents Execution time and ISS taking more time for encryption compare to decryption

DISCUSSION

The results from this project highlight the effectiveness of integrating polynomial-based secret sharing with visual cryptography in a dual-mode authentication framework. By enabling both dealer

participatory and non-participatory decryption, the system adds a **layer of flexibility** that is especially useful in distributed environments where the original dealer may not be available at all times. This feature expands the practical utility of the solution in cloud systems, peer-to-peer networks, and critical infrastructure.

One key achievement is the **lossless decryption** of the secret image without pixel expansion, which is often a limitation in traditional VSS schemes. The use of XOR-based Least Bit Substitution (LBS) ensures that the secret is securely embedded with minimal perceptible distortion. The randomized share generation, influenced by varying pseudo-random values, contributes to the **robustness against tampering and reverse engineering**.

Histogram analysis confirmed that encrypted shares maintain high entropy, reducing the likelihood of successful cryptanalysis. Furthermore, time performance evaluations show that the method maintains computational efficiency, with encryption and decryption times suitable for real-time or near real-time applications.

In summary, the proposed approach not only secures image content but also streamlines the authentication process while maintaining simplicity in implementation, thus addressing the limitations of existing ISS models.

CONCLUSION

The novel approach of combining VSS and polynomial techniques into a (k,n)-threshold scheme forms the basis of a secret-sharing process which provides both security and efficiency in image sharing. The system's flexible design with dealer participatory and non-participatory authentication removes the necessity of a central authority for decryption. The secret image is encrypted using XOR-based LBS methods which hide the image with no expansion or loss in quality. The experimental evaluation of all methods proves that the proposed system provides lossless decryption, high entropy in share images, and computational efficiency resulting in the ability for real-time transmitting images securely. Moreover, the ability to validate shares through screening strengthens the system's share security because the original share is never transfered. The system can be used in various systems such as identity verification systems, blockchain-based data storage, and in sharing in sharing medical images securely. All in all, the research offers a timely response to the challenge of ensuring secure multimedia communication.

REFERENCES

1. El-Latif, A.A.A., Abd-El-Atty, B., Mazurczyk, W., Fung, C. and Venegas-Andraca, S.E., 2020. *Secure data encryption based on quantum walks for 5G Internet of Things scenario*. IEEE Transactions on Network and Service Management, 17(1), pp.118–131.

2. Zhang, X., Peng, F. and Long, M., 2018. *Robust coverless image steganography based on DCT and LDA topic classification*. IEEE Transactions on Multimedia, 20(12), pp.3223–3238.

3. Fukumitsu, M., Hasegawa, S., Iwazaki, J., Sakai, M. and Takahashi, D., 2017. *A proposal of a secure P2P-type storage scheme by using the secret sharing and the blockchain*. In: IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), pp.803–810.

4. Cheng, Y., Fu, Z. and Yu, B., 2018. *Improved visual secret sharing scheme for QR code*

applications. IEEE Transactions on Information Forensics and Security, 13(9), pp.2393–2403.

5. Li, Y. and Guo, L., 2018. *Robust image fingerprinting via distortion-resistant sparse coding*. IEEE Signal Processing Letters, 25(1), pp.140–144.

6. Shamir, A., 1979. *How to share a secret*. Communications of the ACM, 22(11), pp.612–613.

7. Li, L., Hossain, M.S., El-Latif, A.A.A. and Alhamid, M.F., 2017. *Distortionless secret image sharing scheme for Internet of Things system*. Cluster Computing, 22(1), pp.2293–2307.

8. El-Latif, A.A.A., Abd-El-Atty, B., Hossain, M.S., Rahman, M.A., Alamri, A. and Gupta, B.B., 2018. *Efficient quantum information hiding for remote medical image sharing*. IEEE Access, 6, pp.21075–21083.

9. 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, 85, pp.107–121.

10. Chavan, P.V., Atique, M. and Malik, L., 2014. *Signature-based authentication using contrast enhanced hierarchical visual cryptography*. In: Proceedings of Electrical, Electronics and Computer Science.

11. Zou, S., Liang, Y., Lai, L. and Shamai, S., 2014. *An information theoretic approach to secret sharing*. arXiv preprint arXiv:1404.6474.

12. Komargodski, I., Naor, M. and Yogev, E., 2017. *Secret-sharing for NP*. Journal of Cryptology, 30(2), pp.444–469.

13. Wang, G., Liu, F. and Yan, W.Q., 2016. *Basic visual cryptography using braille*. International Journal of Digital Crime and Forensics, 8(3), pp.85–93.

14. Naor, M. and Shamir, A., 1995. *Visual cryptography*. In: EUROCRYPT. Lecture Notes in Computer Science. Springer, Perugia, Italy, pp.1–12.

15. Yang, C.N., Wu, C.C. and Lin, Y.C., 2019. *k out of n region-based progressive visual cryptography*. IEEE Transactions on Circuits and Systems for Video Technology, 29(1), pp.252–262.

16. Yan, X., Liu, L., Li, L. and Lu, Y., 2020. *Robust secret image sharing resistant to noise in shares*. ACM Transactions on Multimedia Computing, Communications, and Applications.

17. Asmuth, C. and Bloom, J., 1983. *A modular approach to key safeguarding*. IEEE Transactions on Information Theory, 29(2), pp.208–210.

18. Yan, X., Lu, Y., Liu, L. and Song, X., 2020. *Reversible image secret sharing*. IEEE Transactions on Information Forensics and Security, 15(5), pp.3848–3858.

19. Wang, Z., Arce, G.R. and Di Crescenzo, G., 2009. *Halftone visual cryptography via error diffusion*. IEEE Transactions on Information Forensics and Security, 4(3), pp.383–396.

20. Zhang, Y., Qin, C., Zhang, W., Liu, F. and Luo, X., 2018. *On the fault-tolerant performance for a class of robust image steganography*. Signal Processing, 146, pp.99–111.