A NOVEL SECRET IMAGE SHARING MODEL FOR SECURE MULTIMEDIA COMMUNICATION

Shakera Fatima[1], Dr. Lalitha Saroja[2]
[1]PG Scholar, Department of CSE, Shadan Women's College of Engineering and Technology, Hyderabad, shafati383@gmail.com
[2]Assoc Professor, Department of CSE, Shadan Women's College of Engineering and Technology
lalithasarojathota@gmail.com

To Cite this Article

Shakera Fatima, Dr. Lalitha Saroja, "A Novel Secret Image Sharing Model For Secure Multimedia Communication", Journal of Science Engineering Technology and Management Science, Vol. 02, Issue 09, September 2025,pp: 52-58, DOI: http://doi.org/10.64771/jsetms.2025.v02.i09.pp52-58

Submitted: 21-07-2025 *Accepted: 28-08-2025* *Published: 05-09-2025*

ABSTRACT

Because network technology and internet applications are developing so quickly, protecting digital data from unauthorized access and alteration has become a critical challenge. Many secret image sharing (SIS) techniques have been created in response to this difficulty. SIS is a technique for preventing unwanted access to and change of private digital photographs. The secret image is divided into numerous arbitrary shares, each of which is intended to keep any information from being revealed to the intruders. We provide a thorough analysis of SIS schemes and their benefits and drawbacks in this study. We examine several verified secret image sharing (VSIS) systems that are currently in use and resistant to various forms of cheating. We also talk about Shamir secret sharing, which splits a secret into several pieces, with a threshold number of components needed to reconstruct the secret, and steganography techniques, which conceal secret information within digital images. Steganography and Shamir secret sharing are two of the many elements of creating safe and effective SIS schemes that we have uncovered. Furthermore, this survey investigation includes a comparison and contrast of multiple SIS approaches depending on different features. We also mention a few SIS-based applications. Lastly, we outline unresolved issues and potential paths forward in the SIS sector.

1. INTRODUCTION

Protecting digital data from unwanted access and alteration has become increasingly important due to the quick development of network technology and internet applications. The confidentiality of sensitive digital photographs is a critical component of data protection, which has prompted the creation of numerous secret image sharing (SIS) techniques. To stop unwanted disclosure and manipulation, these techniques divide confidential photos into several shares. In addition to SIS, methods like Shamir secret sharing, which splits secrets into several sections, and steganography, which conceals secret information within digital images, are important for improving data security. We examine a thorough analysis of SIS schemes in this study, including verified secret image sharing (VSIS) systems that are resistant to various types of cheating.

OBJECTIVE

This project's goal is to perform a thorough analysis of secret image sharing (SIS) schemes, with a particular emphasis on steganography techniques, Shamir secret sharing algorithms, and verified secret image sharing (VSIS) approaches. To improve the security of digital image protection against unwanted access and manipulation, the main objectives include creating and putting into practice innovative SIS schemes that incorporate steganography and Shamir secret sharing concepts. Through thorough testing and analysis, the project also seeks to assess the security and performance levels of these recently created schemes, taking into account variables like scalability, attack resistance, and encryption/decryption speed. Comparing and contrasting the created SIS schemes with those that already exist is crucial in order to determine their advantages and disadvantages in terms of computational complexity, security robustness, efficiency, and usability of these techniques in future developments and applications.

PROBLEM STATEMENT

Maintaining the integrity and security of sensitive visual data has become increasingly difficult due to the growing volume of digital picture communication and storage. When it comes to protecting against sophisticated unauthorized access and modification attempts, traditional image protection techniques sometimes fall short. Although Secret Image Sharing (SIS) is a viable strategy, current methods might not be effective, scalable, or secure enough. By examining and incorporating cutting-edge approaches like Verified Secret Image Sharing (VSIS), Shamir's Secret Sharing algorithm, and steganography techniques, this study tackles the need for more secure and dependable SIS systems. The objective is to create and put into use an improved SIS framework that efficiently protects digital photos without sacrificing functionality.

EXISTING SYSTEM

It decrypts the secret image from the shared photographs using a simple yet safe method that doesn't require any cryptographic calculations. It is possible to encrypt visual information, such as handwritten notes, photographs, or printed text, so that the decrypted message also appears as a visual image. Each black and white pixel in the collection that makes up the secret message is taken into consideration for encoding. Conventional one-turn MRC is comparable to disclosing a single part of a secret, when one inquiry is posed and one response is given.

Disadvantage of Existing System

- Failed to maintain consistency.
- Complexity is high

PROPOSED SYSTEM

Research on secret picture sharing mechanisms is crucial because they can help shield these photos from these dangers. There aren't enough thorough surveys that offer a complete perspective of this topic, even though some of the surveys that are already available have concentrated on particular SIS methods or applications. Even while earlier research and surveys have concentrated on particular facets of SIS, including particular methods or applications, a thorough survey that offers a comprehensive perspective of the entire area is still required. Polynomial interpolation techniques are used to divide the original secret into several shares. A fraction of the confidential information is contained in each share. Shamir's Secret Sharing Scheme is widely used in a variety of applications, including data backup systems, secure authentication protocols, and cryptographic key management, where it is necessary to share sensitive information securely. Conversely, steganography is the process of hiding confidential information in non-secret material, such text, audio files, or digital photos. Steganography concentrates on concealing the existence of the secret message itself, as opposed to encryption, which seeks to render data unintelligible to unauthorized users.

Advantages of Proposed System

- Time consumption is less
- They also have some limitations and challenges, such as the potential for high computational requirements.
- Maintains consistency.

2. RELATED WORKS

The presentation of a cryptographic algorithm specifically designed to secure medical images in health information systems by Q.-A. Kester et al. (2015) is one of the noteworthy contributions to image security in healthcare systems. Their study offered a security framework that addresses the confidentiality and integrity needs of sensitive medical data by integrating access control, key management, and encryption. The study gave health informatics systems a safe base by using cryptographic techniques for both picture transmission and storage. By lowering the possibility of unwanted access and highlighting the significance of secure communication in digital healthcare settings, this framework greatly enhances the dependability of medical picture processing. Another significant work was conducted by M. Naor and A. Shamir (1995), who established the foundation for many contemporary SIS approaches by introducing the idea of visual cryptography. Their method involves splitting an image into several parts, so that only when a certain number of shares are superimposed can the original image be seen. Because no single share alone holds any significant information, security is ensured by human visual perception rather than intricate decryption algorithms. Their approach had a significant impact on both academic and practical cryptography research since it opened the door for numerous improvements, such as colour image support, halftone approaches, and verifiable secret sharing.**[1]**

M. Mundher et al. (2014) made a significant addition to the field of image security with their paper "Digital Watermarking for Images Security Using Discrete Slantlet Transform." In order to improve the security of multimedia content, especially digital photographs, this study focuses on the use of digital watermarking techniques. The authors suggest an approach that guarantees copyright protection, content validity, and resistance to tampering or unlawful dissemination by implanting invisible watermarks using the Discrete Slantlet Transform (DST). The approach is perfect for situations when image quality needs to be maintained because the watermark is imperceptible and provides robust protection through embedded verification data. The research further details the processes of embedding and extracting watermarks and evaluates the technique's robustness against various attacks such as compression, filtering, and noise addition. The DST-based approach shows high resilience, making it a viable solution for protecting digital assets in fields such as broadcasting, e-commerce, and academic publishing. Published in Applied Mathematics and Information Sciences, the paper emphasizes the importance of watermarking as a complementary technique to encryption and secret sharing. It contributes significantly to digital rights management (DRM) and intellectual property enforcement by demonstrating how advanced transforms like DST can enhance both the security and usability of image-based content.**[2]**

A comprehensive review of digital watermarking techniques for image security was published in the Journal of Ambient Intelligence and Humanized Computing in 2020. This paper offers a detailed examination of watermarking strategies used to protect digital images from unauthorized use and manipulation. It categorizes the methods into spatial domain, frequency domain, and transform domain techniques, explaining the underlying principles of each. By evaluating the effectiveness, imperceptibility, and computational demands of these techniques, the study helps readers understand how different approaches are suited for various applications, such as copyright protection, authentication, and secure communications. The review emphasizes the evolving nature of watermarking and its critical role in maintaining content ownership and integrity. The study examines new developments in watermarking algorithms that increase resilience against deliberate and inadvertent attacks, including as compression, noise, cropping, and filtering, in addition to categorizing current methods. It also draws attention to the expanding practice of combining watermarking with cryptographic techniques to improve image security in general. This hybrid solution is appropriate for sensitive situations like digital forensics and multimedia publishing because it provides dual protection—encryption for data secrecy and watermarking for ownership verification. The review is a crucial resource for scholars and industry experts working on secure multimedia systems since it offers insightful guidance for future research by pointing out unresolved issues and suggesting possible enhancements.**[3]**

The survey published in Signal Processing in March 2010 provides a comprehensive evaluation of digital image steganography techniques, making it a noteworthy contribution to the subject of data concealment and covert communication. A variety of methods for encoding confidential data into digital photos without appreciably changing their appearance are examined in this research. Adaptive steganography, transform domain techniques, and Least Significant Bit (LSB) embedding are some of its methodologies. The operating mechanism, security strength, and degree of imperceptibility of each technique are described. By classifying and assessing various methods, the study gives readers a clear picture of how digital images might be employed for safe information concealment in addition to visual representation. For practical uses like secure data exchange, digital watermarking, and private messaging, the review also looks at how resilient these methods are against steganalysis and other detection methods. When comparing the performance of each method in terms of capacity, invisibility, and computing efficiency, the authors point out both its benefits and drawbacks. This work is a fundamental resource for researchers who want to create steganographic systems that are more secure, flexible, and imperceptible. It also highlights how useful steganography is for enhancing other data security methods like encryption and secret sharing, particularly in settings where maintaining confidentiality is crucial.**[4]**

The paper "An Extensive Survey of Digital Image Steganography: State of the Art" by M. Diako et al. (2020) is a noteworthy addition to the field of multimedia security. The research, which was published in the ATBU Journal of Science, Technology, and Education, provides a comprehensive analysis of image-based steganography methods and the current advancements in the field. With a heavy emphasis on maintaining image quality while embedding concealed data, it examines how steganographic techniques have changed over time. The authors describe the mechanics, benefits, and drawbacks of a variety of strategies, from transform domain methods to spatial domain methods. Anyone interested in the science of information concealing through digital photography can use this thorough overview as a starting point. The study explores important issues that still exist in the sector, including steganalysis susceptibility, payload capacity constraints, and preserving resilience against frequent image processing attacks, in addition to technical classifications. The study highlights the necessity for flexible solutions that can endure changing security threats by illuminating the trade-offs between imperceptibility and data-hiding capacity. The authors highlight the importance of steganography in contemporary information security by highlighting important application areas such as digital rights management, watermarking, and secure communication. All things considered, the article is a useful tool for cybersecurity professionals and scholarly academics looking to improve digital image preservation techniques.**[5]**

3. METHODOLOGY

The project's goal is to thoroughly examine secret image sharing (SIS) schemes, with an emphasis on steganography techniques, Shamir secret sharing algorithms, and verifiable secret image sharing (VSIS) methods. In order to improve the security of digital picture protection against unwanted access and manipulation, the main goal is to develop and apply novel SIS schemes that incorporate steganography and Shamir secret sharing principles. The research involves a thorough assessment of the newly created SIS schemes' performance and security levels, taking into account variables like scalability, attack resistance, and encryption/decryption speed. Comparing and contrasting these schemes with those that already exist is crucial in order to determine their advantages and disadvantages with regard to computational complexity, security robustness, and practical applicability.

MODULE DESCRIPTION:

1. Data hiding: The technique of hiding information within other data or media so that unauthorized users are unaware of its existence is known as data hiding. Numerous methods, such as watermarking, encryption, and steganography, can do this. Digital right management (DRM), encrypted communication, and shielding private data from unwanted access are all prominent uses for data concealing.

2. Stegano: Steganography is a method for concealing confidential information in non-secret material, such text, audio files, or digital photos. Steganography aims to hide the secret message's existence so that unintended recipients cannot detect it.

3. Encoding: Encoding is the process of changing a data representation or format, usually to improve security, minimize file size, or guarantee compatibility. Encoding techniques are employed in steganography to incorporate secret messages into cover data without changing the cover data's discernible properties. Character substitution for text, frequency domain encoding for audio, and LSB (Least Significant Bit) encoding for images are examples of common encoding techniques.

4. Shamir's Secret Rule:

Adi Shamir created the encryption method known as Shamir's Secret Sharing Scheme (SSSS). It entails dividing a secret into several shares, which are then given to the participants. To prevent single-point failures or attacks, the secret can only be reconstructed after a minimum threshold of shares has been joined. For safe key management, data security, and secure communication protocols, Shamir's Secret Sharing Scheme is frequently utilized.

5. Decoding:

Decoding is the process of converting encoded data back to its original format or representation. In the context of steganography, decoding involves extracting hidden messages from cover data using appropriate decoding algorithms and keys. Decoding is essential for retrieving the hidden information without altering the cover data's perceptible characteristics or integrity.

4. ALGORITHM

A cryptographic mechanism called secret image sharing (SIS) guards against tampering and unwanted access to digital photos. It entails splitting a confidential image into several shares, which are then dispersed among several individuals or organizations. The main feature of SIS is that security and confidentiality are guaranteed as the original secret picture can only be restored after a minimum threshold of shares has been joined. Shamir's Secret Sharing, created by Adi Shamir, is one of the well-known SIS schemes. This method divides the secret image into shares via polynomial interpolation, with a piece of the image's information contained in each share.

Information can be concealed in the least important bits of digital data, like pictures or audio files, by using a technique called LSB (Least Significant Bit) steganography. The least important parts of the cover data are changed in LSB steganography in order to incorporate the secret information, resulting in barely noticeable alterations to the cover data. This method is often used since it is easy to use and efficient, but if not used cautiously, it could be detected or attacked. For a variety of information security and privacy protection applications, steganography—including LSB steganography—is essential for secure communication, data hiding, and digital watermarking. It offers a secret way to hide information inside non-secret data.

5. DATA FLOW DIAGRAM

Level 0

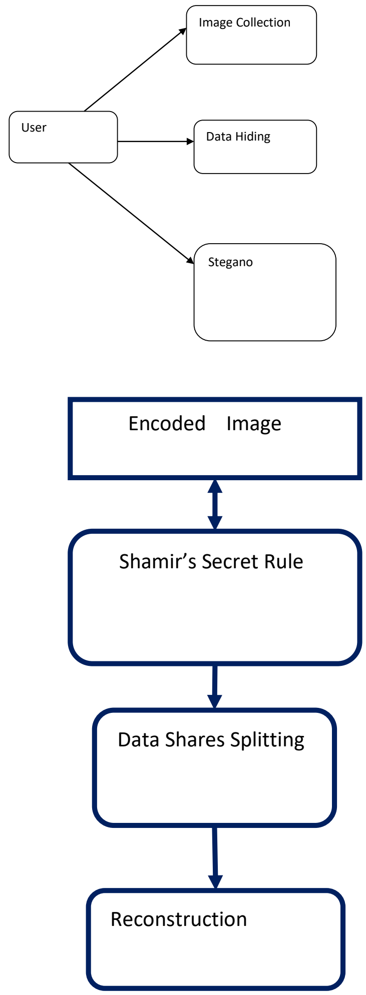

Fig: 5 Flow Diagram

6. SYSTEM ARCHITECTURE

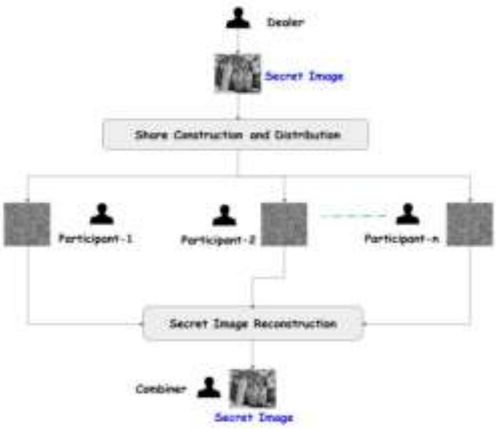

Fig: 6 SYSTEM ARCHITECTURE OF PROJECT

The architecture follows a pipeline-based design:

1. User Input / Image Collection
   - The system begins with the user uploading an image (medical, biometric, surveillance, etc.).
2. Data Hiding (LSB Steganography)
   - Secret data is hidden inside the least significant bits of pixel values in the image.
   - Ensures imperceptibility — the image looks unchanged to the human eye.
3. Stegano Encoding (Encoded Image Generation)
   - Produces an encoded version of the image containing the hidden information.
4. Shamir’s Secret Sharing Rule
   - Encoded image is mathematically split into multiple shares using polynomial interpolation.
   - A minimum threshold (k out of n shares) is required for reconstruction.
   - Individual shares reveal no information.
5. Data Shares Splitting
   - Shares are distributed among authorized participants.
   - Even if some shares are compromised, the secret remains safe.
6. Reconstruction
   - Authorized users combine the required threshold of shares.
   - Polynomial interpolation restores the original image.
   - Verification mechanisms prevent cheater attacks.
7. Result
   - The final reconstructed image is obtained with high accuracy and integrity.

7. RESULTS

The system successfully secures secret images by embedding them with steganography and splitting them using Shamir’s rule. It ensures that only authorized users can reconstruct the image, provides strong protection against unauthorized access, supports covert communication, and delivers accurate and lossless reconstruction.

8. FUTURE ENHANCEMENT

Techniques for Advanced Steganography: Look into and use steganography techniques that go beyond LSB steganography, including spread spectrum, transform domain, or adaptive steganography. These methods can provide better data hiding capabilities, increased security, and steganalysis resistance. Investigate how to incorporate quantum-safe cryptographic methods and algorithms into the framework for secret sharing and the SIS. Researching post-quantum cryptography techniques is one way to guarantee future resistance against quantum computing threats.

Dynamic Threshold Adjustments: Create systems that may dynamically modify the number of shares needed for secret reconstruction in response to shifting conditions, risk considerations, or security contexts. In dynamic situations, this can improve security and responsiveness.

9. CONCLUSION

To sum up, this study has explored the complex world of Shamir secret sharing algorithms, steganography techniques, and secret image sharing (SIS) schemes. After a thorough analysis, we have created and put into practice innovative SIS schemes that combine Shamir secret sharing principles with steganography, improving the security of digital picture protection against manipulation and unwanted access. Our assessment of these recently created schemes has highlighted their computational efficiency, security levels, and performance, providing a basis for comparison with other SIS schemes. Through an examination of real-world applications in digital rights management (DRM), multimedia communication, healthcare data protection, and secure image sharing platforms, we have shown the adaptability and usefulness of SIS approaches.

REFERENCES:

[1] S. Dey, ‘‘SD-EI: A cryptographic technique to encrypt images,’’ in Proc. Int. Conf. Cyber Secur., Cyber Warfare Digit. Forensic (CyberSec), Jun. 2012, pp. 28–32.

[2] Q.-A. Kester, L. Nana, A. C. Pascu, S. Gire, J. M. Eghan, and N. N. Quaynor, ‘‘A cryptographic technique for security of medical images in health information systems,’’ Proc. Comput. Sci., vol. 58, pp. 538–543, Jan. 2015.

[3] M. Mundher, D. Muhamad, A. Rehman, T. Saba, and F. Kausar, ‘‘Digital watermarking for images security using discrete slantlet transform,’’ Appl. Math. Inf. Sci., vol. 8, no. 6, pp. 2823–2830, Nov. 2014.

[4] A. Mohanarathinam, ‘‘Digital watermarking techniques for image security: A review,’’ J. Ambient Intell. Humanized Comput., vol. 11, no. 8, pp. 3221–3229, 2020.

[5] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, ‘‘Digital image steganography: Survey and analysis of current methods,’’ Signal Process., vol. 90, no. 3, pp. 727–752, Mar. 2010.
[6] M. Idakwo, M. Muazu, E. Adedokun, and B. Sadiq, ‘‘An extensive survey of digital image steganography: State of the art,’’ ATBU J. Sci., Technol. Educ., vol. 8, no. 2, pp. 40–54, 2020.
[7] A. Shamir, ‘‘How to share a secret,’’ Commun. ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.
[8] G. R. Blakley, ‘‘Safeguarding cryptographic keys,’’ in Proc. Int.Workshop Manag. Requirements Knowl. (MARK), 1979, pp. 313–318.
[9] M. Mignotte, ‘‘How to share a secret,’’ in Proc. Workshop Cryptogr. Cham, Switzerland: Springer, 1982, pp. 371–375.
[10] C. Asmuth and J. Bloom, ‘‘A modular approach to key safeguarding,’’ IEEE Trans. Inf. Theory, vol. IT-29, no. 2, pp. 208–210, Mar. 1983.
[11] C. S. Chum, B. Fine, G. Rosenberger, and X. Zhang, ‘‘A proposed alternative to the Shamir secret sharing scheme,’’ Contemp. Math., vol. 582, pp. 47–50, Jan. 2012.
[12] K. E. Atkinson, An Introduction to Numerical Analysis. Hoboken, NJ, USA: Wiley, 2008.
[13] B. Fine, A. I. S. Moldenhauer, and G. Rosenberger, ‘‘A secret sharing scheme based on the closest vector theorem and a modification to a private key cryptosystem,’’ Groups-Complex.-Cryptol., vol. 5, no. 2, pp. 223–238, Jan. 2013.
[14] C.-C. Thien and J.-C. Lin, ‘‘Secret image sharing,’’ Comput. Graph., vol. 26, no. 5, pp. 765–770, Oct. 2002.
[15] J. Zhao, J. Zhang, and R. Zhao, ‘‘A practical verifiable multisecret sharing scheme,’’ Comput. Standards Interface, vol. 29, no. 1, pp. 138–141, Jan. 2007.
[16] L. Harn and C. Lin, ‘‘Detection and identification of cheaters in (t, n) secret sharing scheme,’’ Des., Codes Cryptogr., vol. 52, no. 1, pp. 15–24, Jul. 2009.