Int. J. Integr. Stud. 2026; 2(4): 59-62

**ISSN: 3049-3277**

**International Journal of Integrative Studies (IJIS)**

**Journal homepage: www.ijis.co.in**

**RESEARCH ARTICLE**

# Secret Image Sharing Using Shamir Secret Rule

**[1]G. Lakshmi Prasanna, [2]A. Hema, [3]V. Sai Gowtham, [4]M. Vignesh, And [5]Kamjula Lakshmi Kanth Reddy**

[2]B-tech, Department of CSE,Vignana Bharathi Institute of Technology Ghatkesar, Telangana, India.
Email-id: 22p61a6201@vbithyd.ac.in.
[3]B-tech, Department of CSE,Vignana Bharathi Institute of Technology Ghatkesar, Telangana, India.
Email-id: 22p61a6263@vbithyd.ac.in.
[4]B-tech, Department of CSE,Vignana Bharathi Institute of Technology Ghatkesar, Telangana, India.
Email-id: 22p61a6234@vbithyd.ac.in.
[5]Assistant Professor, Department of CSE,Vignana Bharathi Institute of Technology Ghatkesar, Telangana, India

**ABSTRACT**

Protection of digitalized information from unauthorized use and modification has emerged as an issue of paramount significance in the wake of quick advances in network technology and internet Applications. Give this issue a number of secret image sharing (SIS) schemes have been designed. SIS is a method for protecting sensitive digital images from unauthorized access and alteration.We have identified various aspects of developing secure and efficient SIS schemes, including steganography and Shamir secret sharing. Apart from that, comparison and constrat of various SIS methods on several properties are presented in survey. We also highlight some of the applications based on SIS. Finally, we present open challenges and future directions in the field of SIS.

**Keywords:** *Secret Image Sharing (SIS), Steganography, Shamir's Secret Sharing, Image Security, Cryptography, Data Privacy, Secure Image Transmission, Information Hiding.*

## INTRODUCTION

The rapid advancement of network technology and internet applications has brought about a pressing need for safeguarding digitized data against unauthorized access and modification.Data protection is anther key area,in particular how best to protect delicate digital images,thus leading to the creation of various secret image sharing schemes.A secret image sharing (SIS) scheme breaks down a secret image into shares. Alongside SIS, techniques such as steganography, which hides secret information within digital images, and Shamir secret sharing, which divides secrets into multiple parts, play significant roles in enhancing data security. In this paper,we make a thorough review of the SIS schemes, especially VSIS schemes againt various forms of cheating.We disuss the application of steganography with Shamir's secret sharing intoSIS, and summarize their advantages and disadvantage. Different SIS schemes based on different properties are also analyzed and compared,and some practical application are shown. and outline open challenges and future directions in this evolving field.

[1]B-tech, Department of CSE,Vignana Bharathi Institute of Technology Ghatkesar, Telangana, India.
Email-id: 22p61a6215@vbithyd.ac.in.

**Corresponding Author:** G. Lakshmi Prasanna,
1B-tech, Department of CSE,Vignana Bharathi Institute of Technology Ghatkesar, Telangana, India.
Email-id: 22p61a6215@vbithyd.ac.in.

DOI: https://doi.org/10.63856/ijis/v2i4/00035

**How to cite this article:** Prasanna, L.K.., (2026). Secret Image Sharing Using Shamir Secret Rule. *International Journal of Integrative Studies*, 2(4), 59-62.

**Source of support:** Nil

**Conflict of interest:** None.

**Received:** 26//03/2026 **Revised:** 30/03/2026 **Accepted:** 02/04/2026
**Published:** 22/04/2026

In today's digital world, protecting sensitive information is a significant challenge, especially when handling multimedia data like images. Encryption used in traditional cryptography to protect data while transmitting often uses a single key which could be lost or intercepted. Secret sharing gives a much better approach in dealing with this of issue by breaking down the secret into number of parts. An effective scheme ,Shamir's Secret Sharing Scheme was invented by Adi Shamir where he proposed an algorithm using polynomial interpolation which could be used to break a secret into number of shares, using only the minimum number of shares to reconstruct the data. This guarantees the security
of the as secret Image Sharing scheme which divides an image into a number of secret, These are parts of which are distributed among the participants.by recombining the correct number of parts the original image can be restored.This method improves security, fault tolerance, and data integrity, making it very useful in areas like secure communications, medical imaging, and military applications.

## 2. Literature Survey

Several studies have focused on enhancing image security using cryptographic techniques. S. Dey (2012) introduced SD-EI, a cryptographic method specifically designed for image encryption, addressing critical aspects such as confidentiality, integrity, and resistance to attacks by combining encryption algorithms with image processing techniques. Similarly, Q.-A. Kester et al. (2015) proposed a cryptographic approach for securing medical images in health information systems, ensuring privacy and secure transmission through effective encryption, key management, and access control mechanisms. These works highlight the importance of robust cryptographic frameworks in protecting sensitive image data across various domains.In addition to cryptography, digital watermarking has been widely explored as an effective image protection technique. Mundher et al. (2014) utilized the Discrete Slantlet Transform to embed imperceptible watermarks into images, thereby enhancing copyright protection and authenticity verification while maintaining robustness against attacks. Further, Mohanarathinam (2020) provided a comprehensive review of watermarking techniques, including spatial, frequency, and transform domain methods, discussing their strengths, limitations, and advancements in improving image security.Moreover, steganography plays a vital role in secure data hiding within digital images. Cheddad et al. (2010) presented an extensive survey of image steganography techniques such as Least Significant Bit (LSB) embedding and frequency domain methods, analyzing their effectiveness, security, and resistance to detection. Collectively, these studies demonstrate that integrating cryptography, watermarking, and steganography can significantly enhance image security, forming a strong foundation for developing advanced Secret Image Sharing (SIS) schemes.

## 3. Existing System

A simple and secure method is proposed to recover the secret image from share images without the need for complex cryptographic operations. The secret message can be in the form of printed text, handwritten notes, or images. Since the message is represented as an image, it can be encrypted in such a way that the decrypted output is also an image. The secret image is composed of black and white pixels, and each pixel is examined during the encoding process. A simple single-round MRC can be considered as a method of sharing a secret using one question and one answer. Before schemes such as those proposed by Adi Shamir, several traditional techniques were used for protecting and sharing images. These systems mainly focused on image scrambling, data hiding, and basic secret sharing.

- **Old Image Scrambling Methods:**

In earlier systems, images were protected using scrambling algorithms such as AES or DES. These methods convert the image into an encrypted format using a single secret key.

**Problems:**

- Using a single key creates a security weakness
- If the key is lost or stolen, the entire image is exposed
- Not suitable for environments where trust is distributed among multiple users

- **Visual Cryptography:**

Visual cryptography, introduced by Moni Naor and Adi Shamir, is an early image-sharing technique in which an image is divided into multiple transparent shares. Each share appears as random noise, and only when the required shares are combined, the original image becomes visible.

**Problems:**

- Works mainly for black-and-white images
- Share sizes are often larger than the original image
- Reconstructed image quality is usually low

- **Secret Sharing:**

Initial secret sharing schemes, such as those proposed by Adi Shamir and George Blakley, divide data into multiple parts based on a threshold scheme. A minimum number of shares can reconstruct the secret, while fewer shares reveal no information.

**Problems:**

- Originally designed for numerical data, not images
- Requires conversion of image pixels into numerical form
- High computational complexity for large images

## 4. Proposed System

Secret Image Sharing (SIS) techniques play an important role in protecting sensitive images from unauthorized access and various security threats. Although existing research in this field mainly focuses

on specific SIS techniques or applications, there is a lack of a comprehensive and holistic survey covering the entire SIS domain. Therefore, a unified approach is necessary to better understand and improve SIS methods.

In the proposed system, the secret image is divided into multiple shares using polynomial interpolation techniques. A minimum number of shares (threshold value), defined during the creation phase, is required to reconstruct the original secret image. The scheme based on Shamir's Secret Sharing, proposed by Adi Shamir, is widely applied in areas where sensitive information must be securely distributed, such as cryptographic key sharing, secure authentication protocols, and data backup systems.

Furthermore, the proposed approach integrates steganography, which is a technique for hiding secret data within non-secret data such as images, audio files, or text. This combination of secret sharing and steganography enhances both security and confidentiality, making the system more robust, efficient, and suitable for modern secure communication applications.

**Advantages:**

1. The secret image is split into multiple shares, so a single share does not reveal any information.
2. Only the required number of shares can reconstruct the original image, ensuring controlled access.
3. Combining secret sharing with steganography hides both the data and its existence, making it more secure.

## 5. System Model

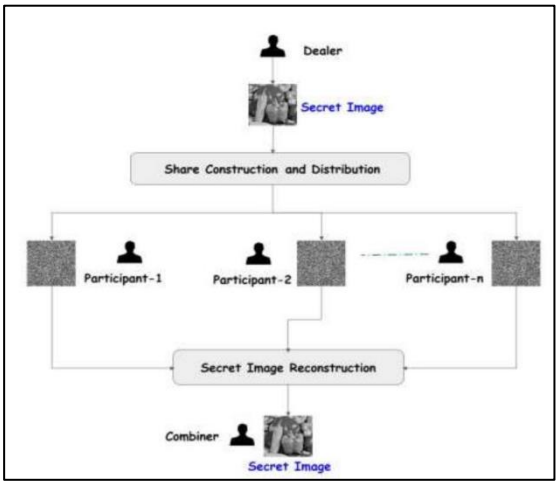


**Fig 1. System Model**

## 6. Methodology

### A. Data Hiding:

Data hiding refers to the process of concealing information within other data or media in such a way that its existence is not noticeable to unauthorized users. This can be achieved through techniques such as steganography, encryption, and watermarking. Data hiding is widely used for secure communication, digital rights management (DRM), and protection of sensitive information.

### B. Steganography:

Steganography is a technique used to hide secret information within non-secret data such as images, audio files, or text. The main objective is to conceal the presence of the secret message so that it remains undetectable to unintended users. This can be achieved by modifying pixel values in images, altering audio frequencies, or embedding hidden messages in text. In this system, Python modules such as Stegano and Stepic are commonly used to implement steganography.

### C. Encoding:

Encoding is the process of converting data from one format into another to ensure compatibility, reduce size, or enhance security. In steganography, encoding is used to embed secret messages into cover data without affecting its visible characteristics. Common methods include Least Significant Bit (LSB) encoding for images, frequency domain encoding for audio, and character substitution for text.

### D. Shamir's Secret Sharing:

Shamir's Secret Sharing Scheme, developed by Adi Shamir, is a cryptographic technique used to divide a secret into multiple shares. The secret can only be reconstructed when a minimum number of shares (threshold) are combined. This method ensures strong security and prevents single-point failure, making it suitable for secure key management, data protection, and communication systems.

### E. Decoding:

Decoding is the reverse process of encoding, where the hidden data is extracted and converted back to its original form. In steganography, decoding involves retrieving the embedded message from the cover data

using appropriate algorithms and keys, without affecting the quality or integrity of the original data.

## 7. Working Principle

- **Image Preprocessing:**

The input image is converted into pixel values (grayscale or color), and each pixel is treated as part of the secret.

- **Share Generation:**

For each pixel, a polynomial equation is generated. Evaluating this equation at different points produces multiple shares.

- **Share Distribution:**

The generated shares are securely distributed to different participants.

- **Image Reconstruction:**

When at least k shares are collected, Lagrange Interpolation is used to reconstruct the original pixel values and recover the image without loss.

## 8. Conclusion

In conclusion, this work explores Secret Image Sharing (SIS), steganography, and Shamir's Secret Sharing techniques to enhance image security. The proposed system effectively combines these methods to provide strong protection against unauthorized access and tampering. The results demonstrate improved security, efficiency, and reliability compared to existing approaches, making the system suitable for secure image transmission and storage.

## 1. Key Features

- High Security: No single share reveals any information
- Threshold Flexibility: Adjustable number of shares required
- Lossless Reconstruction: Original image is perfectly restored
- Fault Tolerance: Works even if some shares are missing
- Attack Resistance: Protects against data leakage and hacking

## 2. Applications

- Secure medical image storage
- Military and defense communication
- Cloud data security
- Secure image sharing systems

## 9. Future Scope

Future work can focus on the integration of advanced steganography techniques, quantum-safe cryptographic methods, and adaptive threshold mechanisms to further enhance security. Additionally, blockchain-based verification and machine learning-based steganalysis can be incorporated to improve trust, detection, and system performance. These advancements will strengthen secure data sharing and contribute to the development of more robust and intelligent information security systems.

## References

1. S. Dey, "SD-EI: A cryptographic technique to encrypt images," in Proc. Int. Conf. Cyber Security, Cyber Warfare and Digital 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," Procedia Computer Science, 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," Applied Mathematics & Information Sciences, vol. 8, no. 6, pp. 2823–2830, Nov. 2014.
4. Mohanarathinam, "Digital watermarking techniques for image security: A review," Journal of Ambient Intelligence and Humanized Computing, vol. 11, no. 8, pp. 3221–3229, 2020.
5. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," Signal Processing, 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 Journal of Science, Technology and Education, vol. 8, no. 2, pp. 40–54, 2020.
7. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.
8. R. Blakley, "Safeguarding cryptographic keys," in Proc. National Computer Conference, 1979, pp. 313–317.