Enhanced Secret Image Sharing with Polynomial Interpolation

Trijay Patel(202211066), Srijan Sharma(202211084), Tanay Patel(202211094), Yuvraj Chauhan (202211098)
Under the guidance of Dr. Gaurav Pareek
Indian Institute of Information Technology, Vadodara - International Campus Diu

***Abstract*—The report roots its search with the notion of Secret Sharing introduced by Shamir [1]. Traditional methods often require shadow images proportional to the original image size, resulting in increased storage and communication overhead. This report inspires from the work of a novel SIS scheme that generates constant-size shadow images (23 × 23 pixels), irrespective of the original image dimensions, [2] leveraging pixel coordinate-based sharing and multi-secret sharing (MSS)[3]. To address dependencies on pixel frequency distributions, our scheme incorporates a histogram equalization technique, which ensures uniform polynomial degrees. The proposed method achieves lossless recovery without requiring pre-shared keys, while optimizing storage, communication, and computational costs. Experimental results demonstrate the scheme's performance in reducing overhead while maintaining robust security properties.**

Keywords: Secret Image Sharing, Multi-Secret Sharing, Constant-Size Shadow Images, Lossless Recovery.

I. Introduction

Secret image sharing schemes (SIS) have become powerful tools for protecting image data. While traditional methods like Shamir's (k, n) threshold scheme [1] are widely used, they often struggle with inefficiencies in storage and computation, as the size of shadow images grows with the size of the original image. Patil and Purushothama addressed this issue by developing a method that generates fixed-size shadow images (23 × 23) regardless of the secret image's dimensions, using pixel coordinate-based sharing and multi-secret sharing (MSS) [2].

However, their approach relies on the threshold value t being tied to image properties like maximum pixel frequency, which can be a limitation. This report introduces a probabilistic equalization method that breaks this dependency, making shadow image generation and retrieval more efficient and flexible.

II. Related Works

- **Shamir's (k, n) Threshold Scheme [1]:** Shamir introduced the concept of (k, n) threshold schemes, where a secret is divided into n parts such that any k parts can reconstruct the secret, but $k-1$ parts reveal no information. This technique, based on polynomial interpolation over a finite field, is foundational in secure key management and secret sharing systems. However, direct application to image sharing results in shadow images whose size is proportional to the original image, limiting scalability for large datasets.
- **Franklin et al. (1992) [3]:** Introduced multi-secret sharing using polynomial-based schemes, enabling parallelization of secret sharing with minimal communication overhead. This concept is pivotal in constructing efficient SIS schemes, particularly when shadow size and reconstruction accuracy are critical metrics.
- **Thien et al. (2002) [4]:** Proposed the first SIS scheme leveraging Shamir's threshold secret sharing but optimized for images by reducing the shadow size relative to the secret image. This improvement, however, introduced trade-offs, such as reliance on pre-shared keys for image permutation, which limits practical deployment.
- **Patil and Purushothama (2021) [2]:** Addressing limitations of prior schemes, this work proposed a pixel-coordinate-based secret image sharing (SIS) scheme that generates constant-sized shadow images (e.g., 23×23) regardless of the secret image size. The scheme eliminates the need for pre-shared keys between the share generator and combiner, improving usability. However, the required threshold t depends on the maximum frequency of pixel values, which can increase computational complexity for images with high-frequency pixel clusters.

III. Proposed Scheme

The proposed Secret Image Sharing (SIS) scheme enhances prior approaches by ensuring constant shadow image size while addressing dependencies on image properties like maximum pixel frequency. The scheme operates in two primary phases: **Share Generation** and **Image Retrieval**.

A. Key Features of the Scheme

- **Constant Shadow Image Size:** Regardless of the original image size, the shadow images are fixed at 23 × 23 pixels, reducing storage and communication overhead.
- **Removing Dependence over Pixel Frequency:** By equalizing the histogram of the secret image before sharing, the scheme avoids the variability in polynomial degree caused by differences in pixel distributions.
- **Efficient Polynomial Representation:** Shares are constructed using polynomials where the pixel coordinates are encoded, ensuring that any t shares suffice for reconstruction while $t-1$ reveal nothing.
- **Lossless Recovery:** The reconstructed image is absolutely identical to the original.

- **Keyless Cryptography:** The scheme leverages the keyless cryptographic approach introduced by Shamir [1], eliminating the need for traditional key-sharing mechanisms and thereby simplifying the process.

B. Share Generation Phase

In this phase, the secret image is divided into n shadow images. Each pixel coordinate (x, y) corresponding to a grayscale value p is encoded using polynomial-based multi-secret sharing (MSS). These polynomials are evaluated at unique points to generate shadow images. For every pixel p:

- The coordinates are grouped into sets S_p^x and S_p^y.
- Each set is encoded using a $(t-1)$-degree polynomial.
- Shares are distributed across n nodes as constant-sized matrices.

The shadow images generated are independent of the size of the original image but retain all necessary information for recovery.

C. Image Retrieval Phase

The reconstruction process combines any t shadow images to recover the original secret image. Using Lagrange interpolation:

- Polynomials corresponding to pixel positions are reconstructed from shadow images.
- Evaluating these polynomials retrieves the original pixel coordinates (x, y) and grayscale values p.

This phase ensures exact recovery without requiring additional information or keys, demonstrating the scheme's robustness and practicality.

D. Optimization via Histogram Equalization

A key feature of this scheme is the use of probabilistic histogram equalization to redistribute pixel frequencies before generating the shares. This approach brings several practical advantages:

- The degree of polynomials is kept mostly uniform across all grayscale values.
- The parameters t and n are relatively fixed for an image size, independent of the pixel distribution in the image.
- Communication and computational costs are minimized, enhancing scalability.

This optimization ensures the proposed scheme maintains its efficiency across diverse image types while reducing the number of shadow images required for reconstruction.

E. Security Features

The security of the proposed scheme relies on the following principles:

- Individual shadow images reveal no information about the original image.
- The scheme adheres to the security properties of the underlying MSS framework.
- Items in public repository reveal no information about original image.

Overall, the proposed SIS scheme offers a practical and secure solution for applications requiring robust image sharing mechanisms, such as cloud based architectures.

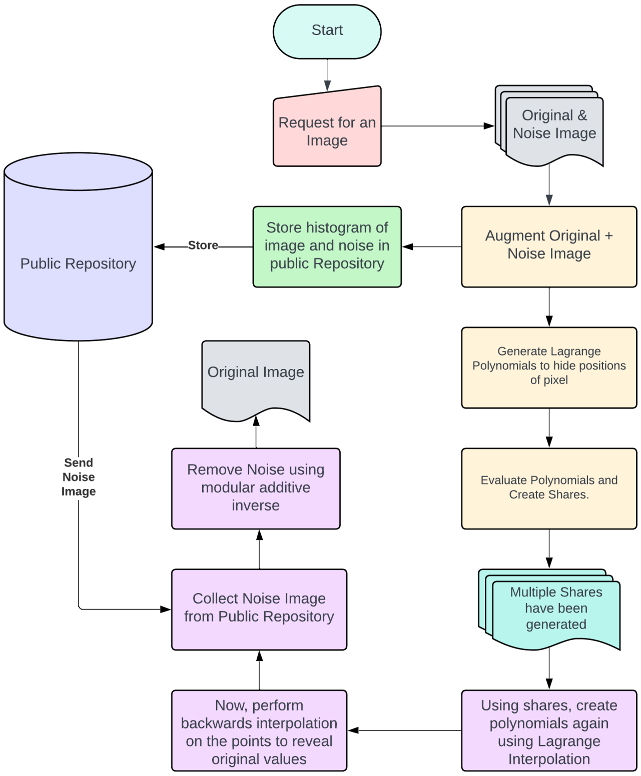
Start
Request for an Image
Original & Noise Image
Public Repository
Store
Store histogram of image and noise in public Repository
Augment Original + Noise Image
Original Image
Generate Lagrange Polynomials to hide positions of pixel
Send Noise Image
Remove Noise using modular additive inverse
Evaluate Polynomials and Create Shares.
Collect Noise Image from Public Repository
Multiple Shares have been generated
Now, perform backwards interpolation on the points to reveal original values
Using shares, create polynomials again using Lagrange Interpolation

Fig. 1. Proposed Scheme

IV. Results and Analysis

A. Comparison Metrics

The performance of the proposed scheme is evaluated against:

- **Shadow Image Size:** Remains constant at 23 × 23 pixels.
- **Reconstruction Accuracy:** Achieves lossless recovery.
- **Computational Overhead:** Reduced number of generated shares.

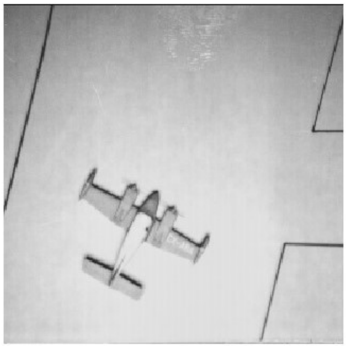

Fig. 2. Input Original Image for Secret Sharing Process

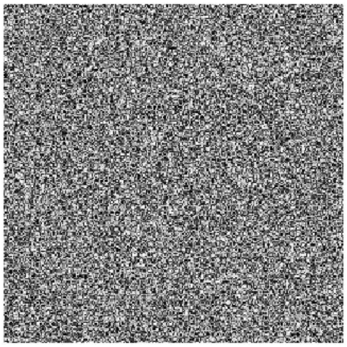

Fig. 3. Generated Noise

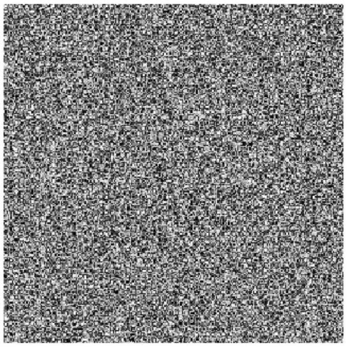

Fig. 4. Augmneted Image

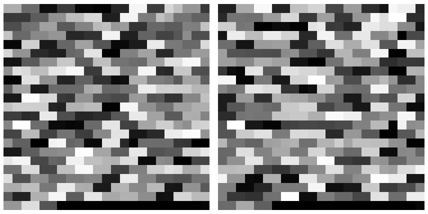

Fig. 5. Generated Shadow Shares from Lagrange's Polynomial Equation

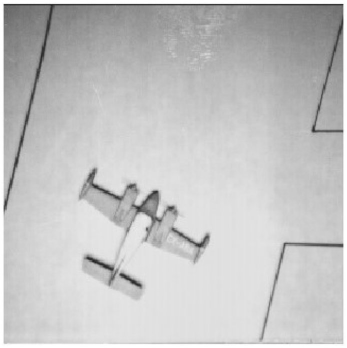

Fig. 6. Reconstructed Image after Applying Lagrange Interpolation

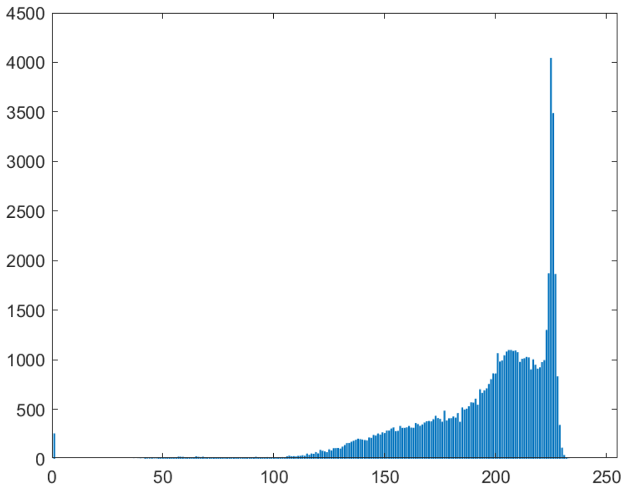

Fig. 7. Histogram of Original Airplane Image

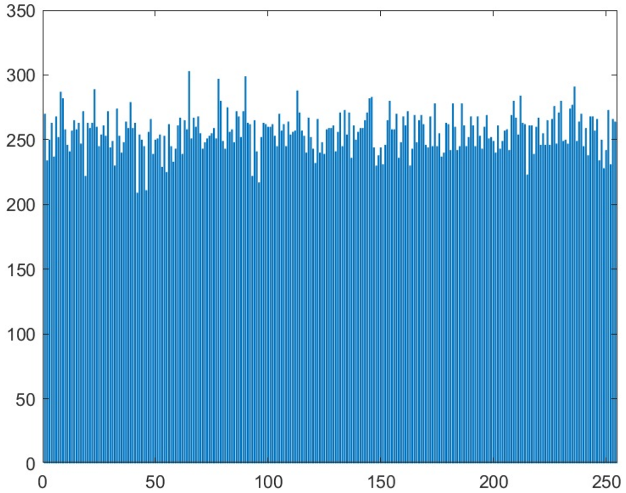

Fig. 8. Histogram of the generated Noise

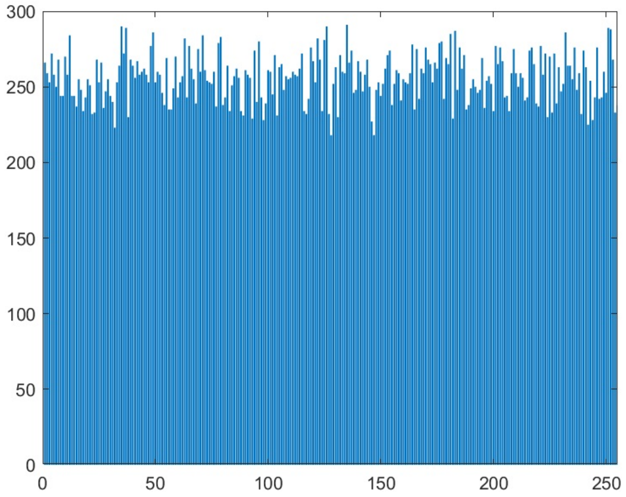

Fig. 9. Histogram of Augmented Airplane Image

B. Comparison against Normal SIS

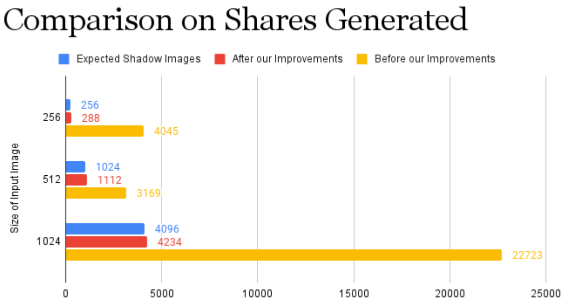

Fig. 10. Comparison against Normal SIS Scheme

Based on experiments conducted by us on different images available in public domain, a significant drop can be observed in the number of minimum t shares to be generated, also the t now becomes dependent over the pixel frequency distribution of the Augmented Image and not on the Original Image, while revealing no information about original image.
This makes our scheme much more practical when it comes to application perspective, while having similar computation overhead to original scheme, but less storage overhead.

C. Security Analysis

The scheme's security is rooted in the MSS framework, ensuring that any $t-1$ shadow images provide no information about the secret, making it resilient to attacks. The security can be formally established by reducing it to the security of Shamir's (t, n) sharing scheme [1]. Since Shamir's scheme is proven to be secure, our scheme inherits this security guarantee.

V. Conclusion and Future Work

The proposed SIS scheme offers significant improvements in efficiency and scalability while maintaining robust security. Future work includes implementing deterministic noise generation and further optimizing shadow image encoding.

References

[1] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979, ISSN: 0001-0782. DOI: 10.1145/359168.359176. [Online]. Available: https://doi.org/10.1145/359168.359176.

[2] S. M. Patil and B. Purushothama, "Pixel co-ordinate-based secret image sharing scheme with constant size shadow images," *Computers Electrical Engineering*, vol. 89, p. 106 937, 2021, ISSN: 0045-7906. DOI: https://doi.org/10.1016/j.compeleceng.2020.106937. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0045790620307850.

[3] M. Franklin and M. Yung, "Communication complexity of secure computation (extended abstract)," in *Proceedings of the Twenty-Fourth Annual ACM Symposium on Theory of Computing*, ser. STOC '92, Victoria, British Columbia, Canada: Association for Computing Machinery, 1992, pp. 699–710, ISBN: 0897915119. DOI: 10.1145/129712.129780. [Online]. Available: https://doi.org/10.1145/129712.129780.

[4] C.-C. Thien and J.-C. Lin, "Secret image sharing," *Computers Graphics*, vol. 26, no. 5, pp. 765–770, 2002, ISSN: 0097-8493. DOI: https://doi.org/10.1016/S0097-8493(02)00131-0. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0097849302001310.