On (k, n) Threshold Secret Image Sharing based on Pixel Coordinates for Simple Images

Srijan Sharma
Indian Institute of Information Technology Vadodara, India
srijan_s@diu.iiitvadodara.ac.in

Trijay Patel
Indian Institute of Information Technology Vadodara, India
trijay_p@diu.iiitvadodara.ac.in

Yuvraj Chauhan
Indian Institute of Information Technology Vadodara, India
yuvraj_gc@diu.iiitvadodara.ac.in

Tanay Patel
Indian Institute of Information Technology Vadodara, India
tanay_p@diu.iiitvadodara.ac.in

Gaurav Pareek
Indian Institute of Information Technology Vadodara, India
gaurav@diu.iiitvadodara.ac.in

Purushothama B R
National Institute of Technology Karnataka, Surathkal, India
puru@nitk.edu.in

***Abstract*—Pixel coordinate-based (k, n) threshold secret image sharing (SIS) approaches have garnered attention in the past few years as they are more efficient in terms of the size of the image shares or shadow images required to share an image secretly over an insecure communication channel in a fault-tolerant manner. In this paper, we point out that these approaches do not feature the desirable performance for images with very high frequencies of a single or very few number of pixels. We refer to such images as simple images. To address this issue, we present a new threshold image secret sharing scheme (SS scheme) using pixel coordinates, which despite featuring constant shadow image size, requires nearly a constant number of such shadow images. This is true for standard as well as simple images. The sender and the receiver do not require any secret keys or permutations to be pre-shared between them. We carry out experimental evaluation for the proposed scheme over grayscale images to analyze its comparative efficiency with respect to the existing similar approaches.**

***Index Terms*—Information security, Secret image sharing, Visual cryptography, Image encryption**

I. Introduction and Motivation

Secret sharing plays a critical role in securing sensitive information, especially in distributed environments where no single party should have complete access to the data. By dividing a secret into multiple parts and requiring a minimum threshold to reconstruct it, secret sharing ensures both confidentiality and fault tolerance. Shamir's (k, n) polynomial-based SS scheme [8] is a foundational method for secure data sharing, which allows a secret to be split into some n parts such that any non-sequential k parts can reconstruct the original, while fewer provide no information. Building on this concept, Thien and Lin [9] extended secret sharing to digital images. They treat the intensity value of each pixel as a secret to share. As a result, there are n shares corresponding to each pixel in the original image. If the i^{th} share of each pixel value is arranged in a 2-D grid, we get the i^{th} image share or the so-called i^{th} shadow image [4]. Upon combining at least k shadow images out of the n image shares, the original image is reconstructed. The schematic description of the process of (k, n) threshold SIS is shown in Figure 1.

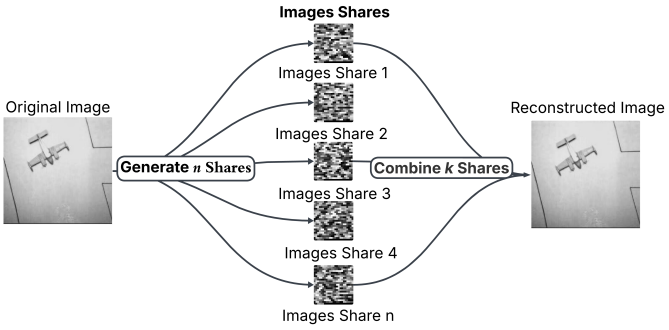


Fig. 1: (k, n) threshold SIS

Ever since the work by Thien and Lin [9], threshold image sharing has seen many developments [7], one of which is the work by Patil and Purushothama [4]. They design their scheme for grayscale images, where instead of securing the gray values of each pixel, they secure the position or coordinate of all the pixels having a certain gray value. Since there are potentially multiple pixels (and multiple coordinates) having the same gray value, the goal of SIS is achieved by using threshold-based MSS. [2]. The scheme in [4] uses threshold-based MSS scheme to secretly share two vectors of secrets—-a collection of the x and y values of each pixel coordinate – corresponding to each gray value. Since the number of gray values for any given pixel in a grayscale image can only be 256 (i.e. 0-255), the size of each shadow image required to secretly share the image is also 256 pixels. While keeping the size of a share to be constant, independent of the original image to be shared, the number of shares in their scheme is *at least the max of the pixel value frequencies* in the image. We point out

that this could be a problem with simple images where there are often high frequencies of a single or very few number of colors (gray-values). Moreover, from the viewpoint of a threshold-based SS scheme, the number of shares n and the threshold k should be determined by nothing except the choice of the owner. On a contrary, n and k are determined by the frequencies of various gray-values in it. We aim to overcome this shortcoming by designing a new SIS scheme for simple images. In the proposed scheme, the numbers n and k are "almost" constant with respect to the frequencies of the pixel-values in a given simple image. We first define the lower bound on the number of shadow images any pixel coordinate based SIS scheme can have. Secondly, we reduce the numbers n and k very close to their lower bounds thereby making the resulting pixel coordinate based SIS scheme more efficient in practical application scenarios.

A. Our contributions

In this paper, we point out an important research gap in the design of the recently proposed pixel coordinate-based approach and various different schemes for (k, n) threshold-based SIS [4]. We stress that while each shadow image remains constant in terms of its dimension, using the pixel coordinate-based approach leads to both k and n to depend on the frequency histogram of the original image, which is to be concealed. In particular, the minimum number of shares n is a function lower bounded by the maximum of the frequencies of the grayscale values, i.e., [0, 255], of all the pixels in the image. We address this gap by designing a new pixel coordinate-based SIS scheme featuring the count of shares very close to the total number of pixels in the original image independent of its frequency histogram. The proposed scheme satisfies all other performance requirements of pixel coordinate-based SIS schemes. That is, it has constant size of each shadow image. Also, despite featuring the constant number of shadow images, it does not need any pre-shared secrets between any of the communicating parties.

B. Paper organization

The rest of the paper is structured as follows. Section II examines a few current, relevant works in the field of exchanging secret images. In Section III, we present the specific proposed scheme. Section IV outlines our experiments and their outcomes. SectionV brings the paper to a close.

II. Related Works

The idea of *secret sharing (SS)*, particularly the (k, n) threshold scheme, was introduced by Shamir [8]. The data is partitioned into n individual components, termed as *shares* or *shadows*, by either the data owner or a designated third party known as the *dealer*. Each of these *shares* is subsequently distributed to n trusted participants, with every participant receiving precisely one share. In *threshold secret sharing (TSS)* schemes, even if some participants become corrupt, their collusion cannot reconstruct the original data unless at least k out of the n participants collaborate.

Thien and Lin [9] employed the secret sharing to images and designed the first threshold SIS. They developed a SS scheme specifically designed for digital images, aiming at reducing storage and transmission demands. Instead of processing every pixel, their method randomly selects a subset of pixels and applies a threshold SS technique to only those pixel values. Ever since the work by Thien and Lin, several works were carried out in SIS, especially in threshold-based schemes. Wang et al. [10] discussed a scalable SIS scheme where the quality of the reconstructed image improves as more shares become available. Yang et al. [11] aimed to reduce the size of shadow images without breaching security using predictive coding and compression techniques. Prasetyo et al. [5] and Deshmukh et al. [1] introduced schemes that use the Chinese Remainder Theorem (CRT) to improve computational efficiency.

Recently, the idea of SIS based on pixel coordinates [4], [6] rather than the pixel values has emerged as an interesting new research area. The basis scheme for this paper comes from [4], in which Patil and Purushothama hide the pixel coordinates of the image and store the polynomials in shadow images of size 23×23. Any given grayscale image of size $m \times n$ will have pixel values or grayscale values in the range $[0, 255]$, and hence we are required to create sets of polynomials to store x and y coordinates for each pixel value $v \in [0, 255]$.

III. Proposed SIS scheme

In the following section, we first discuss the mathematical preliminaries, including the SS, followed by a review and critical analysis of the scheme by Patil and Purushothama [4]. Thereafter, we present the concrete proposed SIS scheme.

A. Preliminaries

1) Secret sharing [8]: A secret is divided into n parts referred to as `shares`, such that any k of the n parts can reconstruct the secret, but $k-1$ parts reveal no information; additionally, at least k `shares` are required. The technique is derived from the concept of polynomial interpolation, where in a *secret* is concealed by incorporating it with a randomly generated polynomial of $k-1$ degree, where in each coefficient is chosen randomly, and the constant term amounts as our secret. So the polynomial $\mathbf{q}(x)$ is defined as

$$\mathbf{q}(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} \tag{1}$$

where a_0 is the secret, and $a_1, a_2, \ldots, a_{k-1}$ are randomly chosen coefficients. Now, the polynomial $P(x)$ is evaluated at x, $\forall x \in [1, k] \cap \mathbb{Z}^+$, and each $\mathbf{q}(1)$, $\mathbf{q}(2) \ldots \mathbf{q}(k)$ is a `share`.

Now, the reconstruction of polynomial will be done using Lagrange's Interpolation as

$$\mathbf{q}(x) = \sum_{i=0}^{k} L_i(x) \tag{2}$$

where the Lagrange basis polynomial $L_i(x)$ is defined as:

$$L_i(x) = \prod_{\substack{j=0 \\ j \neq l}}^{k} \frac{l}{l-j}, \quad \text{where } l \in [1,k] \cap \mathbb{Z}^+, \\ j \in [0,k] \cap \mathbb{Z}^+, \quad j \neq l. \tag{3}$$

2) Review of Patil and Purushothama's scheme [4]: Patil et al.[4] (2021) discussed a novel approach leveraging Shamir's (k, n) threshold scheme [8] to secure image data by concealing pixel coordinate information rather than the full pixel intensity values. For each pixel value $p \in [0, 255]$, the coordinates where it appears in the image are grouped into two sets:

$$S_{p_x} = \{x_i \mid \text{pixel at } (x_i, y_i) = p\} \tag{4}$$

$$S_{p_y} = \{y_i \mid \text{pixel at } (x_i, y_i) = p\} \tag{5}$$

The constant term a_0 of a polynomial of degree $k-1$ contains each coordinate in these sets, which are secrets:

$$\mathbf{q}(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} \tag{6}$$

where a_0 is a coordinate value from S_{p_x} or S_{p_y}, and $a_1, \ldots, a_{k-1}$ are random coefficients.

For each p, two such polynomials are constructed (one for x-coordinates and one for y-coordinates), resulting in a total of $2 \times 256 = 512$ polynomials. These polynomials are evaluated at multiple points $x = 1, 2, \ldots, t$, where $t \geq k$, to generate shares. These shares are stored in shadow images of size 23×23, each corresponding to one evaluation index across all 512 polynomials.

The number of required shadow images, denoted N, is directly dependent on the pixel value with the highest frequency in the image:

$$N \geq \max_{p \in [0,255]} |S_{p_x}| \tag{7}$$

While this approach effectively hides the coordinate data, the main drawback is that both computation and storage costs grow with the peak of the histogram of pixel frequencies.

B. The concrete proposed scheme

We present the basic idea behind the proposed scheme along with various algorithms involved in the scheme.

1) The basic idea: In pixel coordinate-based SIS schemes, the number of points required for reconstruction are determined by the degree of polynomial. To ensure security, the scheme mandates that the polynomial's degree $t-1$ satisfies the following condition:

$$t > \max(n_p), \quad \forall p \in \mathbb{Z} \cap [0, 255] \tag{8}$$

where n_p denotes the number of pixels having a particular gray value p.

The scheme constructs polynomials corresponding to S_{p_x} and S_{p_y}, where each polynomial must have a total degree of $t-1$. Since each n_p contributes to this degree, additional randomness of degree $(t-1) - n_p$ is incorporated to maintain security.[4]

The quantity of shares in our modified scheme is directly influenced by the peak value ($\max(n_p)$) in the pixel histogram. A higher peak value will require a higher polynomial degree for reconstruction, increasing number of shares. This will increase the storage and computation overhead.

We need to equalize the pixel histogram, which would reduce the peak frequency value. This lowers the required polynomial degree, which reduces the number of shares. This is achieved by augmenting the image with random noise, which redistributes pixel frequencies.

The following procedure was adopted for carrying out the objective evaluation of our modified scheme:

- Load the `input_image` and preprocessed into a matrix.
- A `noise_image` was created of the same dimension as the original image, with each pixel value p of the image is chosen at random from a uniform distribution.

$$p \sim \mathcal{U}(0, 255)$$

- Using modular arithmetic, augment the two images to create an `augmented_image`

$$\text{augmented\_image}[i][j] = (\text{noise\_image}[i][j] + \\ \text{input\_image}[i][j]) \mod 256, \forall i, j \in [0, m-1]$$

- After augmenting `input_image` with `noise_image`, the `augmented_image` was passed through the `share_generation` phase of the protocol, and the `noise_image` was stored in a public repository.

Algorithm 1 Extraction of Pixel Locations

Require: Image I
Ensure: $\mathcal{S}_{p_x}$, and $\mathcal{S}_{p_y}$ are the coordinate set of the abscissa and ordinate for the pixel value p, where $p \in [0, 255]$

```
for p ← 0 to 255 do
    S_{p_x} = S_{p_y} = ∅                ▷ Initialization
end for
for i ← 0 to m − 1 do
    for j ← 0 to m − 1 do
        Let p = I_{i,j}
        S_{p_x} = S_{p_x} ∪ {i}
        S_{p_y} = S_{p_y} ∪ {j}
    end for
end for
```

2) Construction of Shares Phase: Any given simple image I of dimension $m \times n$ will have the corresponding grayscale values or pixel values in the range $[0, 255]$. Each grayscale value $p \in [0, 255]$ can be associated with several coordinate positions or locations in the image I. We extract the location of each of the pixel values by applying the algorithm 1. Each of the grayscale values or pixel values $p \in [0, 255]$ will have sets S_{p_x} and S_{p_y}, where S_{0_x} is the set of x coordinates for pixel value $p = 0$ and S_{0_y} is the set of y coordinates for pixel value $p = 0$. These sets are then used as an

Algorithm 2 Encoding Positions using Lagrange's Polynomial

Require: k, $\mathcal{S}_{p_x}$, $\mathcal{S}_{p_y}$, for each $p \in [0, 255]$

Ensure: $q_p^{(x)}(z)$ and $q_p^{(y)}(z)$, Lagrange's polynomial for sharing abscissa and ordinate of pixel value p for each $p \in [0, 255]$ (refer [4])

// Construction of $q_p^{(x)}(z)$ and $q_p^{(y)}(z)$ using Eqs. (1) and (2) for each pixel value $p \in [0, 255]$ (refer [4])
for $i \leftarrow 0$ to 255 **do**
  Compute $n_i = |\mathcal{S}_{i_x}| = |\mathcal{S}_{i_y}|$
  Generate a purely randomized polynomial $r_i(z)$ of degree $(k-1) - n_i$
  Initialize $temp_i^{(1)} = 1$
  for $j \leftarrow 1$ to n_i **do**
    $temp_i^{(1)} = temp_i^{(1)} \times (z - j)$
  end for
  $temp_i^{(1)} = temp_i^{(1)} \times r_i(z)$
  Initialize $temp_{i_x}^{(2)} = temp_{i_y}^{(2)} = 0$
  for $j \leftarrow 1$ to n_i **do**
    Initialize $temp_j = 1$
    for $k\prime \leftarrow 1$ to n_i **do**
      if $j \neq k\prime$ **then**
        $temp_j = temp_j \times \frac{z - k\prime}{j - k\prime}$
      end if
    end for
    $temp_{i_x}^{(2)} = temp_{i_x}^{(2)} + (\mathcal{S}_{p_x}(j) \times temp_j)$
    $temp_{i_y}^{(2)} = temp_{i_y}^{(2)} + (\mathcal{S}_{p_y}(j) \times temp_j)$
  end for
  $q_i^{(x)}(z) = temp_i^{(1)} + temp_{i_x}^{(2)}$
  $q_i^{(y)}(z) = temp_i^{(1)} + temp_{i_y}^{(2)}$
end for

Algorithm 3 Construction of Shares

Require: $q_i^{(x)}(z), q_i^{(y)}(z)$ for each $p \in [0, 255]$

Ensure: constructed shares $I^{(1)}, I^{(2)}, \ldots, I^{(n)}$ each of size 23×23 (refer [4])

Let max_x represent the maximum value from $\{n_0, n_1, \ldots, n_{255}\}$
for $i = max_x + 1$ to $max_x + n$ **do**
  $row \leftarrow 0$
  $col \leftarrow 0$
  for $j = 0$ to 255 **do**
    $q_{x_j} \leftarrow q_j^{(x)}(i)$
    $q_{y_j} \leftarrow q_j^{(y)}(i)$ ▷ Arrangement of q_{x_j} and q_{y_j} values to progressively form the 23×23 shadow image share
    $I^{(i-max_x)}(row, col) \leftarrow q_{x_j}$
    if $col + 1 > 22$ **then**
      $row \leftarrow row + 1$
      $col \leftarrow 0$
    else
      $col \leftarrow col + 1$
    end if
    $I^{(i-max_x)}(row, col) \leftarrow q_{y_j}$
    if $col + 1 > 22$ **then**
      $row \leftarrow row + 1$
      $col \leftarrow 0$
    else
      $col \leftarrow col + 1$
    end if
  end for
  $I^{(i-max_x)}(22, 22) \leftarrow i$
end for

input for encoding positions using Lagrange Polynomial (refer algorithm 2), which will give us $q_i^{(x)}(z)$ and $q_i^{(y)}(z)$. $q_i^{(x)}(z)$ represents the set of encoded polynomials for x component with an intensity $p \in [0, 255]$.

After we get the polynomials $q_i^{(x)}(z)$ and $q_i^{(y)}(z)$ for the sets S_{p_x} and S_{p_y} we are ready to generate the shares of our image. We will use the share generation algorithm mentioned in [4] (refer algorithm 3).

Now after generating shares, they can be distributed or stored among n servers as secrets and the histogram i.e. pixel values and frequency can be stored in a public database.

3) Image Retrieval Phase: Applying Algorithm 4 will give us the reconstructed polynomials as well as give us the coordinates of the pixels. The reconstructed polynomials are formed in a manner that for each polynomial, evaluating them on $1, 2, 3 \ldots n$ will result in the sets S_{p_x} and S_{p_y}.

Applying Algorithm 5 will result in the `augmented_image` i.e. the image after mixing the noise. From this image, the original image can extracted by:

$$\text{input\_image}[i][j] = (\text{augmented\_image}[i][j] - \text{noise\_image}[i][j]) \mod 256, \forall i, j \in [0, m-1]$$

IV. Experiments and results

We implement the proposed scheme in MATLAB and check the applicability with multiple images of two different patterns:

1) Images of same size, but different pixel distribution.
2) Images of varying size ranging from 16×16 to 1024×1024 , but with similar pixel distribution.

Due to space constraints, experimental results are shown only for two images – Baboon and Airplane. Note that Baboon is a standard image whereas Airplane is a simple image. The metric for performance comparison is the reduction in in the min. number of shares required to secretly share the image, which we define as follows:

$$\% \text{ Decrement } = \frac{\text{shares}_{\text{before}} - \text{shares}_{\text{after}}}{\text{shares}_{\text{before}}} \times 100$$

Here, $\text{shares}_{\text{before}}$ and $\text{shares}_{\text{after}}$ denote the number of shares constructed by the scheme in [4] and in the proposed scheme, respectively.

For airplane image, the size is 256×256 pixels. The scheme in [4] generates 6495 shares, due to its high concentration in a *grayish* color, which is again evident from

Algorithm 4 Polynomial Reconstruction

Require: Shares $I^{(1)}, I^{(2)}, \ldots, I^{(k)}$
Ensure: $\phi_p^{(x)}(z)$ and $\phi_p^{(y)}(z)$ where $p \in [0, 255]$

for $row \leftarrow 0$ to 22 **do**
  for $col \leftarrow 0$ to 22 **do**
    if $row\%2 == 0$ **then**
      $index \leftarrow \left|\frac{row \times 23}{2}\right| + \left|\frac{col}{2}\right|$
      if $col\%2 == 0$ **then**
        $co\_ord \leftarrow x$
      else
        $co\_ord \leftarrow y$
      end if
    else
      $index \leftarrow \left|\frac{row \times 23}{2}\right| + \left|\frac{col+1}{2}\right|$
      if $col\%2 == 0$ **then**
        $co\_ord \leftarrow y$
      else
        $co\_ord \leftarrow x$
      end if
    end if
    $q_{index}^{(co\_ord)}(z) \leftarrow 0$
    for $i \leftarrow 1$ to t **do**
      $temp \leftarrow 1$
      for $j \leftarrow 1$ to t **do**
        if $i \neq j$ **then**
          $temp \leftarrow temp \cdot \frac{z - I^{(j)}(22,22)}{I^{(i)}(22,22) - I^{(j)}(22,22)}$
        end if
      end for
      $temp \leftarrow temp \cdot I^{(i)}(row, col)$
      $q_{index}^{(co\_ord)}(z) \leftarrow q_{index}^{(co\_ord)}(z) + temp$
    end for
    if $row == 22$ and $col == 6$ **then**
      Exit
    end if
  end for
end for

Algorithm 5 Reconstruction of Secret Image

Require: $q_p^{(x)}(z)$ and $q_p^{(y)}(z)$ for each $p \in [0, 255]$
Ensure: Reconstructed image RI

for $i \leftarrow 0$ to 255 **do**
  for $j \leftarrow 1$ to n_i **do**
    $x\_cord \leftarrow q_i^{(x)}(j)$
    $y\_cord \leftarrow q_i^{(y)}(j)$
    $RI_{x\_cord, y\_cord} \leftarrow i$
  end for
end for

Figure 2, where, we can observe that there is a sudden peak in the original Histogram. To reduce this peak, we perform our Histogram Equalization technique to make the peaks uniform, after which the peak is reduced from 6495 to 288.

For Baboon, the image size is 512 × 512. The Histogram of Baboon image is more *normal* when compared to airplane image as observed in Figure 3, but still has a peak of 2952, which is reduced to 1112 after applying our histogram equalization technique.

Using the proposed scheme, it can be seen in Fig.4 that we almost equalized the pixel frequency and bringing the number of the shares almost equal to the ideal scenario. This would be true for any image used in our scheme. Also the security of the underlying cryptographic scheme is not affected as the noise image is completely random. This will lead to a reduced storage overhead and also a reduced computation overhead during the decryption process.

V. Conclusions

We discuss an approach to make the pixel coordinate-based SIS efficient even for simple images, where a very large number of pixels take a single or very few number of gray values. Our modified (k, n) threshold SIS scheme that requires a near-constant number of shares. Since each constructed share is of the same dimensions, i.e.23×23, the discussed modifications to the scheme are efficient. The proposed scheme has been tested against some existing approaches for its practical applicability for various simple and standard images. The accompanying experimental results have further confirmed our claims that the suggested scheme works more efficiently than the other existing ones in terms of the quantity while maintaining constant size shares simultaneously.

References

[1] M. Deshmukh, N. Nain, and M. Ahmed, "A novel approach for sharing multiple color images by employing chinese remainder theorem," *Journal of Visual Communication and Image Representation*, vol. 49, pp. 291–302, Nov. 2017.

[2] 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 (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.

[3] A. Nag, S. Biswas, D. Sarkar, and P. P. Sarkar, "A new (k, n) verifiable secret image sharing scheme (vsiss)," *Egyptian Informatics Journal*, vol. 15, no. 3, pp. 201–209, 2014.

[4] 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.

[5] H. Prasetyo and J.-M. Guo, "A note on multiple secret sharing using chinese remainder theorem and exclusive-or," *IEEE Access*, vol. 7, pp. 37 473–37 497, 2019.

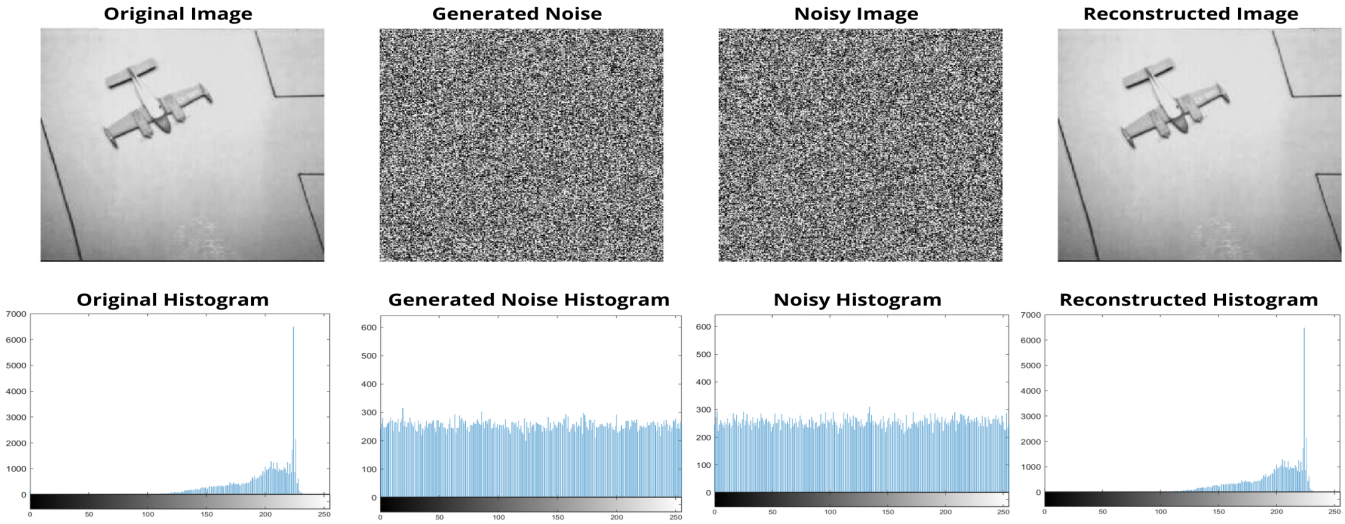


Fig. 2: Airplane image variations: Original, Noise, Augmented, and Reconstructed

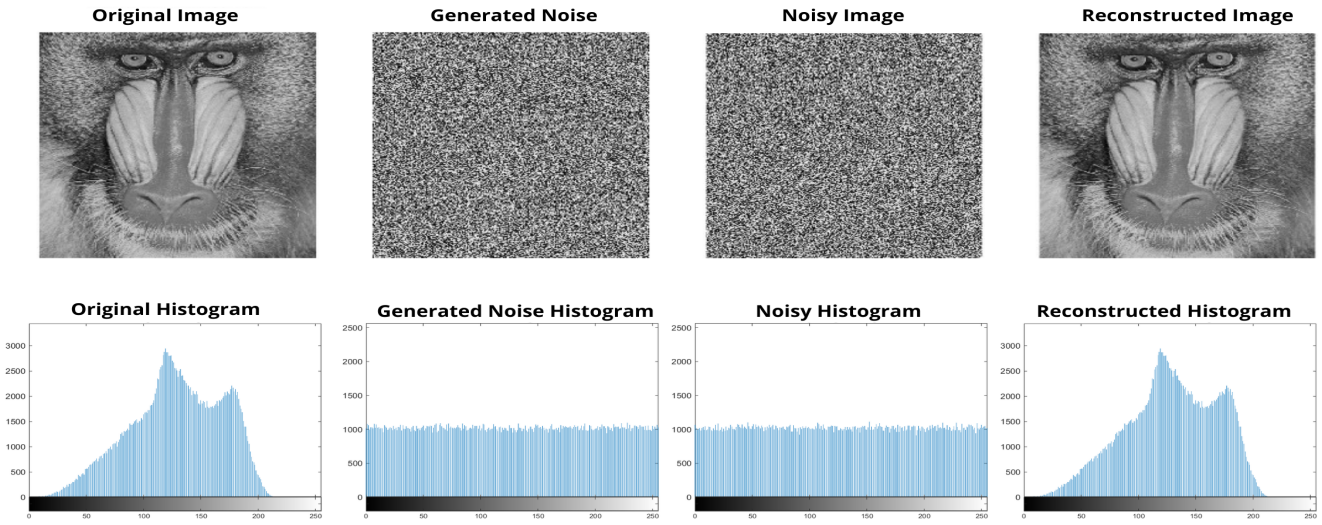
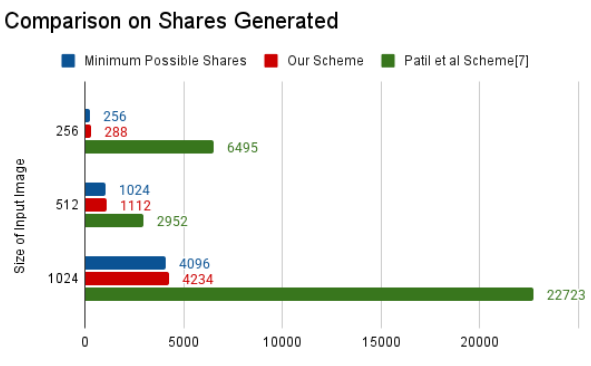
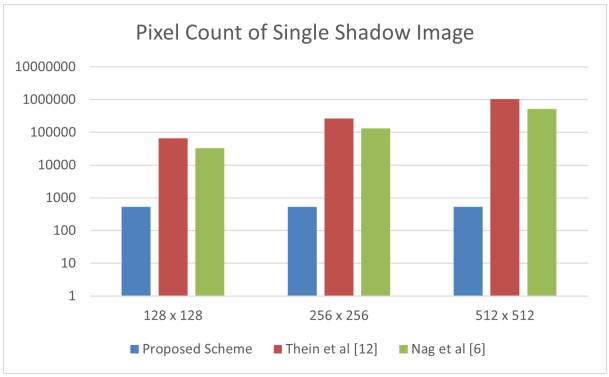


Fig. 3: Baboon image variations: original, noisy, augmented, and reconstructed



(a) Number of shares with [4] and the proposed scheme



(b) Size of the shares in [3], [9] and the proposed scheme

Fig. 4: Comparison on the basis of the number of image shares and size of each image share

[6] P. Reshma Sagar, J. Pruthvi Sri Chakra, and B. R. Purushothama, "Pixel position based efficient image secret sharing scheme," in *Recent Findings in Intelligent Computing Techniques*, P. K. Sa, S. Bakshi, I. K. Hatzilygeroudis, and M. N. Sahoo, Eds., Singapore: Springer Singapore, 2018, pp. 527–533, ISBN: 978-981-10-8633-5.

[7] S. Saha, A. K. Chattopadhyay, A. K. Barman, A. Nag, and S. Nandi, "Secret image sharing schemes: A comprehensive survey," *IEEE Access*, vol. 11, pp. 98 333–98 361, 2023. DOI: 10.1109/ACCESS.2023.3304055.

[8] 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.

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

[10] R.-Z. Wang and S.-J. Shyu, "Scalable secret image sharing," *Signal Processing: Image Communication*, vol. 22, no. 4, pp. 363–373, Apr. 2007.

[11] C.-N. Yang, P. Li, C.-C. Wu, and S.-R. Cai, "Reducing shadow size in essential secret image sharing by conjunctive hierarchical approach," *Signal Processing: Image Communication*, vol. 31, pp. 1–9, Feb. 2015.