Journal of Information Systems Engineering and Management
2025, 10(22s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Lossless Recovery Scheme for Grayscale Visual Cryptography Based on Random Grids

Yanyan Han[1], Xiaoyu Huang[1*], Lin Zhou[2]
1.Department of Cryptographic Science and Technology, Beijing Electronic Science and Technology Institute, Beijing 100070, China
2. Department of Postgraduate, Beijing Electronic Science and Technology Institute, Beijing 100070, China
Corresponding Author's Email: 15838317130@163.com

ARTICLE INFO

Received: 24 Dec 2024

Revised: 06 Feb 2025

Accepted: 20 Feb 2025

ABSTRACT

With the advancement of digitalization, the demand for grayscale image encryption has been increasing. Previous visual cryptography schemes for grayscale images have encountered issues such as information loss during recovery, poor recovery quality, and significant pixel expansion. This study introduces novel grayscale visual cryptography schemes based on grayscale threshold segmentation, including the (n,n) and (k,n) schemes, utilizing random grids. These schemes enable lossless recovery of the secret image when all shares are involved in the decryption process. Furthermore, by incorporating the particle swarm optimization algorithm, a scheme for generating share images containing grayscale information was proposed. This method relies on the grayscale-overlay principle, allowing secret image recovery through the overlay of shares without requiring computational devices, demonstrating the applicability of the extended scheme. Theoretical analysis demonstrates the security of the proposed schemes, and experimental results further verify their effectiveness.

Keywords: Random grids; Visual cryptography; Grayscale image; Lossless recovery

1. INTRODUCTION

A visual cryptography scheme is an encryption scheme that applies the concept of secret sharing to directly perform encryption and decryption operations on the pixels of digital images [1,2]. Unlike traditional cryptographic schemes, visual cryptography is characterized by its suitability for scenarios involving low computational complexity recovery, multi-channel covert communication, access control, and tolerance to loss. In the context of digital big data, it has attracted widespread attention from scholars and has found various forms of application.

Visual cryptography schemes based on base matrices require the involvement of encryption matrices in the computation, which leads to issues such as pixel expansion and contrast distortion. Kafri [3] proposed a visual cryptography scheme based on random grids, which eliminates the need for encryption matrices during the encryption process. This approach has led to a branch of research in visual cryptography. Traditionally, visual cryptography schemes have focused on binary images. However, with the development of information technology, the demand for the encryption of grayscale and colour images, which carry more information, has been increasing. Grayscale images consist of pixels with varying levels of brightness, where the range of grayscale values typically spans from 0 to 255 (with black being 0 and white being 255). Because the essence of colour images is to divide grayscale images into three channels—R, G, and B—and process each channel separately, research on colour and grayscale images primarily focuses on grayscale images.

Hiroki [4] proposed a colour and grayscale image encryption scheme based on an enhancement model, which restores the secret image using the additive operator add. The resulting scheme has a relatively small pixel expansion, but it uses an expansion matrix and cannot achieve high-quality image recovery. Blundo [5] proposed a grayscale image encryption scheme based on concatenated matrices, which can achieve high-quality recovery of the secret image, but it suffers from significant pixel expansion. Similarly, Lin [6] proposed a grayscale image encryption scheme based on halftone technology, which avoids the traditional pixel expansion problem, but the error diffusion technique still leads to cumulative errors and cannot achieve lossless recovery. Hou [7] proposed a colour visual cryptography

encryption scheme with no pixel expansion, but the contrast of the recovered image suffers from distortion. Sun Rui [8] proposed a two-level threshold-based visual cryptography scheme, which achieves no pixel expansion but is not suitable for grayscale images and does not implement lossless recovery.

However, He [9] proposed a lossless recovery multi-level visual cryptography scheme, but their approach involves first converting grayscale images into binary 8-bit numbers and introducing error correction coding mechanisms. This method does not directly handle pixels, resulting in high computational complexity. In another study, Liu Jian [10] proposed a grayscale visual cryptography scheme based on grayscale addition, which achieves lossless recovery, but each level requires the generation of a corresponding encryption matrix and does not completely resolve the pixel expansion issue. Liu Xin [11] proposed a (k, n) threshold visual secret sharing algorithm based on random grids, which, when all shadow images are involved in the recovery, can achieve lossless recovery. While this algorithm does not have pixel expansion and implements lossless recovery, it has not been extended to grayscale images.

This study applies the concept of grayscale threshold segmentation and proposes a random grid-based grayscale visual cryptography scheme for (n, n) and (k, n) thresholds. The rest of this paper is organized as follows. Section 2 shows the related word. Section 3 gives the proposed scheme and some related algorithms. Section 4 gives the simulation testing and performance analysis. The conclusion and future work are given in Section 5.

2. METHODOLOGY

2.1 Grayscale Image

In computer science, a grayscale digital image refers to an image where each pixel has only one sampled color, displayed from the darkest black to the brightest white. Grayscale images are typically stored with a fixed nonlinear scale for each sampled pixel, comprising bits, and currently come in various types, such as 8-bit and 16-bit. For example, an 8-bit grayscale image represents the grayscale value of each pixel stored in 8 bits, which can cover 2^8 different levels of grayscale. This level of precision helps avoid visible banding distortion, and it is easy to program and compute, making it widely used in current applications. The grayscale images addressed in this paper are those with 8-bit sampled pixels.

2.2 $(2, 2)$ Random Grid Visual Cryptography Scheme

The random grid-based visual cryptography scheme was first proposed by Kafri [3]. In this scheme, a share image SC_1 is randomly generated with the same dimensions as the original secret image S, and then SC_2 is generated based on equation (1).

$$SC_2(i,j) = \begin{cases} SC_1(i,j) & if \ \ S(i,j) = 0 \\ \overline{SC_1(i,j)} & if \ \ S(i,j) = 1 \end{cases} \tag{1}$$

In the recovery phase, the scheme performs overlay calculations based on equation (2). For black pixels (value 1) in the secret image, the result of the overlay on the share images is also 1. For white pixels (value 0) in the secret image, the recovery result has a 50% chance of being 0 and a 50% chance of being 1. This way, the pixel contrast is restored, effectively recovering the secret image.

Since SC_1 is randomly generated, SC_2 also inherits its randomness, making both shadow images noise images. This randomness enhances the security of the recovery process, as a single share image cannot easily reveal the secret image, thereby improving the privacy protection of the scheme.

The key design of this approach is to leverage randomness to ensure the unpredictability of the recovery process while still allowing for reasonable contrast restoration of the secret image, despite some uncertainty in the recovered pixels.

$$S'(i,j) = SC_1(i,j) \otimes SC_2(i,j) =$$
$$\begin{cases} SC_1(i,j) \otimes SC_1(i,j) & if S(i,j) = 0 \\ SC_1(i,j) \otimes \overline{SC_1(i,j)} = 1 & if S(i,j) = 1 \end{cases} \tag{2}$$

This scheme extends from (2,2) to (n, n), meaning that the share images are encoded into n Random Grids . In the recovery process, only when all n shares participate in the recovery can the human visual system recognize the secret image.

2.3 Grayscale superposition

Grayscale superposition [10] refers to the phenomenon where pixels with different grayscale values combine to produce a darker grayscale pixel, which aligns with the visual characteristics of the human eye. The calculation of grayscale superposition is as equation (3):

$$add(g_1, g_2) = L - int\frac{(L - g_1) \cdot (L - g_2)}{L} \tag{3}$$

In this case, int() represents the floor function, which rounds down to the nearest integer. Similarly, given the grayscale level L, and the result of the grayscale superposition add (g_1, g_2), we can reverse-engineer the original grayscale values g_1 and g_2.

The principle of grayscale superposition is similar to the superposition of black-and-white binary pixels. This superposition rule is based on the human eye's imaging principle and does not require complex computational operations. The reversal process involves solving for g_1 and g_2. given the result of the superposition, typically relying on constraints or approximations since the operation is not perfectly invertible in every case, but it follows the general idea of combining two values to yield a new one that approximates the visual effect seen by the human eye.

The key idea is that the combination of two grayscale values results in a darker pixel, in line with the human eye's response to light, which perceives a more intense combination as producing a darker shade.

2.4 Threshold method

Grayscale levels refer to the brightness of a pixel. In most current grayscale images, the grayscale values range from 0 to 255, resulting in 256 grayscale levels. However, in real-life situations, the human visual system is not capable of distinguishing all 256 grayscale levels accurately. Typically, an image with 16 grayscale levels can already convey a significant amount of information. Therefore, in practical applications, grayscale images can be preprocessed according to the actual requirements.

One common method of preprocessing is the thresholding technique based on image segmentation. This method divides the grayscale values into different levels or categories, reducing the number of grayscale steps. The resulting subsets or sub-images, with pixels of consistent grayscale values within each subset, can then undergo encryption and decryption. This approach helps to compress the data size and simplify the analysis and processing steps, as fewer distinct grayscale levels are used, reducing computational complexity and storage requirements while still maintaining useful visual information.

3. SCHEME DESIGN

In this chapter, a (n, n) grayscale visual cryptography scheme based on random grids is designed using the concept of grayscale threshold segmentation. Furthermore, by incorporating the lossless visual cryptography algorithm based on random grids proposed by Liu Xin [11], a (k, n) grayscale-overlay visual cryptography scheme is designed.

3.1 (n, n) GVCS

The (n, n) GVCS algorithm based on random grids primarily consists of three parts, as shown in the flowchart of Figure1:

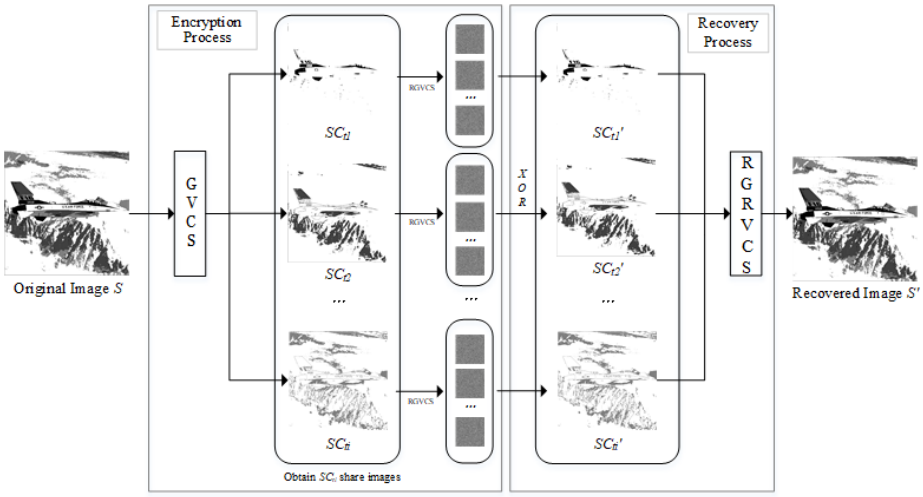

Figure.1 Flowchart of the encryption and decryption process for the (n,n) grayscale visual cryptography algorithm

First, the original image S is input, and through grayscale threshold segmentation (GSTS), it is converted into several segmented grayscale images S_{t1} to S_{ti}Algorithm 1) Then, for each segmented grayscale image, the random grid visual cryptography scheme (RGVCS) algorithm(Algorithm 2) is applied to encrypt and generate multiple share images S_{ti_1} to S_{ti_n}.

During the recovery phase, the share images are processed in reverse order using the XOR operation to obtain the encrypted image set S_{t1} to S_{ti}.

Finally, through the recovery grayscale visual secret sharing (RGRVCS) algorithm (Algorithm 3), the encrypted image set is restored to the final image S', which is then output as the recovered image S'.

Algorithm 1 GSTS

Input: Original image S

Output: Segmented images $S_{t1} \cdots S_{ti}$

Define grayscale levels and calculate the interval t
Based on t, generate the number of grayscale levels numLevels and the grayscale levels vector grayLevels
Initialize the image collection dividedImages$\{i\}$
for i = 1 **to** numLevels **do**
  if i = numLevels **then**
    Calculate the lower bound of the grayscale value for the interval
  else
    Calculate the upper bound of the grayscale value for the interval
  end if
end for
Return the segmented image set
Output the segmented images $S_{t1} \cdots S_{ti}$, totaling 256/ t images

For each segmented image S_{ti}, binary processing is first performed, followed by the execution of the (n, n) RGVCS operation. The $(2, 2)$ algorithm has already been introduced in Section 2.2. To extend this to the (n, n) algorithm, as shown in Algorithm 2, an additional loop is required. Share images are generated by determining the parity of the index values. This method ensures that every step of the generated share images retains the complementarity and symmetry of the original image information.

Algorithm 2 (n, n) RGVCS

Input: Original image S_{ti}

Output: Segmented images $S_{t_{i1}} \cdots S_{t_{in}}$

Execute the $(2, 2)$ RGVCS algorithm to generate S_{ti_1} and S_{ti_2}
for j = 3 **to** $2n - 2$ **do**
  if RGVCS algorithm to generate **then**
    Obtain the share image with the previous even index as previousImage
      Generate a random matrix C and a zero matrix I
      for each pixel of previousImage **do**
        if the pixel is white **then**
          Assign the corresponding pixel value from C to I
        else
          Assign the negated corresponding pixel value from C to I
        end if
      end for
      Assign I to the current index of shareImages
  else if the generated image index is even **then**
    Assign the previous index's matrix C to the current index of shareImages
  end if
end for
Renumber and store the share images corresponding to odd indices and the final share image at the even index
Return and output the encrypted images $S_{ti_1} \cdots S_{ti_n}$

In the image recovery phase, the secret image can be restored through overlay or, alternatively, by performing simple calculations. This section focuses on the results of Algorithm1 and introduces the recovery algorithm for grayscale images.

Algorithm 3 RGRVCS

Input: Set of segmented images

Output: Recovered image S'

Initialize the image combinedImage as a zero matrix of size $m \times n$
for i = 1 **to** n d**o**
  for j = 1 **to** n d**o**
    Initialize a vector pixelValues of length t
    for k = 1 **to** t **do**
      Store the grayscale value of image kat position (i, j) into pixelValues[k]
    end for
    if pixelValues is empty **then**
      Set combinedImage(i, j) to 255
    else
      Set combinedImage(i, j) to the minimum value in pixelValues
    end if
  end for
end for
Return and output the decrypted image S'

We now prove that the algorithm possesses lossless properties during the recovery process using simple calculations. Let the original grayscale image be represented by the matrix I, where the element $I(i,j)$ denotes the pixel value at position (i,j). Let the segmented images be $S_{t1}, S_{t2}, \dots, S_{ti}$.

During both the segmentation and recovery phases, no actual changes in the pixel positions or grayscale values of the image occur; only the grayscale values are used as the sole reference standard. The segmented images contain pixels of the same grayscale level except for the white pixels. Therefore, if the grayscale levels can cover all the grayscale values of the original image, the lossless recovery condition is satisfied; that is, $I(i,j) = D(S_{t1}, S_{t2}, \dots, S_{ti})$.

In the random grid encryption process, let $b_1, b_2, \dots, b_n$ represent the pixel values at corresponding positions (i,j) in $S_{ti_1}(i,j), S_{ti_2}(i,j), \dots, S_{ti_n}(i,j)$, respectively. According to the generation process, $S_{t_i}(i,j) = b_1 \oplus b_2 \oplus \dots \oplus b_n$. Therefore, when the XOR method is used for recovery, the algorithm's encryption and decryption process for grayscale images can achieve lossless recovery.

Of note, when the number of grayscale levels is large and the value of n is also large ($n \geq 8$), each grayscale level image requires the generation of n share images for the encryption and decryption process. Although the algorithm does not involve complex calculations, it still leads to significant storage consumption. Therefore, in this context, the principle of grayscale overlay is applied to propose a scheme that can be recovered through overlay, aiming to reduce image storage consumption.

From the grayscale-overlay principle in Section 2.3, we know that when a specific grayscale value is given, the grayscale values g_1, g_2 involved in the overlay can also be derived. Expanding this idea to include more share images involved in the overlay process allows for the calculation of grayscale values $g_1, g_2, \dots, g_n$. These grayscale values are then randomly assigned to the pixels of the original image that contain grayscale information. For pixels without grayscale information, grayscale values within the random number assignment range are distributed. The range of random numbers can cover all the grayscale values present in the original image, ensuring that, after the overlay, the pixels with grayscale information can be recovered, and the original image information can be perceived by the human visual system.

During the algorithm design, we noticed that if the difference between grayscale values is too large or if excessive continuous extreme values are present (such as 0 or 255), secret information is at risk of being revealed through visual observation. Therefore, to ensure that the grayscale values generated are random while avoiding extreme values, we employ a Particle Swarm Optimization (PSO) algorithm to calculate the different grayscale values. This algorithm provides global and individual optimality, avoiding local optima. The PSO algorithm is encapsulated as a grayscale value generation function, which is used in the generation of share images. The specific description of the Grayscale Random Grid Visual Cryptography Scheme (GRGVCS) algorithm is shown in Algorithm 4.

Algorithm 4 (n,n) GRGVCS

Input: i segmented images

Output: n share images

Initialize variables, input images, and set the grayscale levels and the number of share images
Convert the pixels with grayscale information from the i input segmented images to black, and generate the corresponding binary image S_b
Apply the (n,n) RGVCS algorithm to the S_b image to generate binary images $S_{b1}, S_{b2}, \dots, S_{bn}$
Generate a random permutation of grayscale share images:
  for each of the i segmented images **do**
    Select a grayscale value add_g
    Call the grayscale value generation function to generate n grayscale values—gn_values
    Randomly assign the grayscale values to the corresponding positions in $S_{b1}, S_{b2}, \dots, S_{bn}$
    For pixels without grayscale information, randomly assign grayscale values
end for
Output the n share images

3.2 (k, n) GVCS

To enhance the practicality of the algorithm, a (k, n) threshold scheme is proposed based on the (n, n) lossless visual cryptography sharing scheme using random grids [12]. Unlike the (n, n) algorithm, the (k, n) algorithm introduces random bit values to generate the shared images. Specifcally, the frst k bits are generated initially, followed by assigning values to the remaining $(n - k)$ bits, which are then randomly distributed to produce n shared images. The workfow of the (k, n) RGVCS algorithm is illustrated in Figure 2.

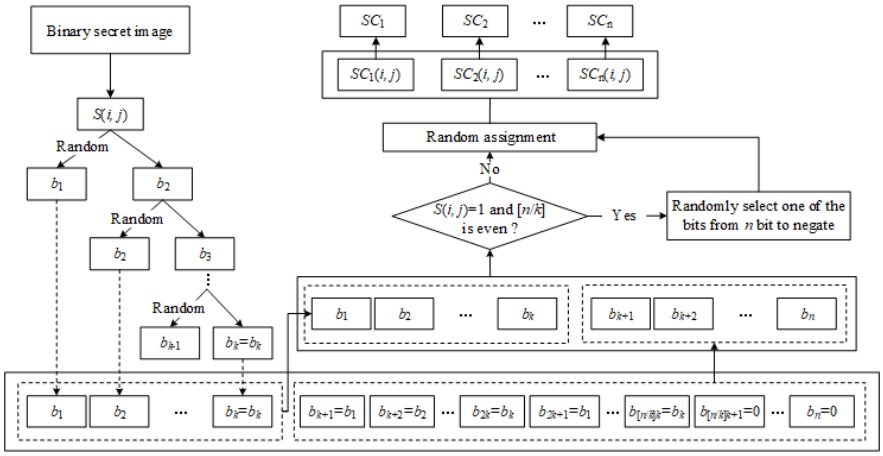

Figure.2 Flowchart of a (k, n)Threshold Lossless Visual Cryptography Scheme Utilizing Random Grids

The workflow of the (k, n) GRGVCS closely resembles that of the (n, n) scheme. It incorporates Algorithm 4 for image encryption and recovery, with the detailed process depicted in Figure 3.

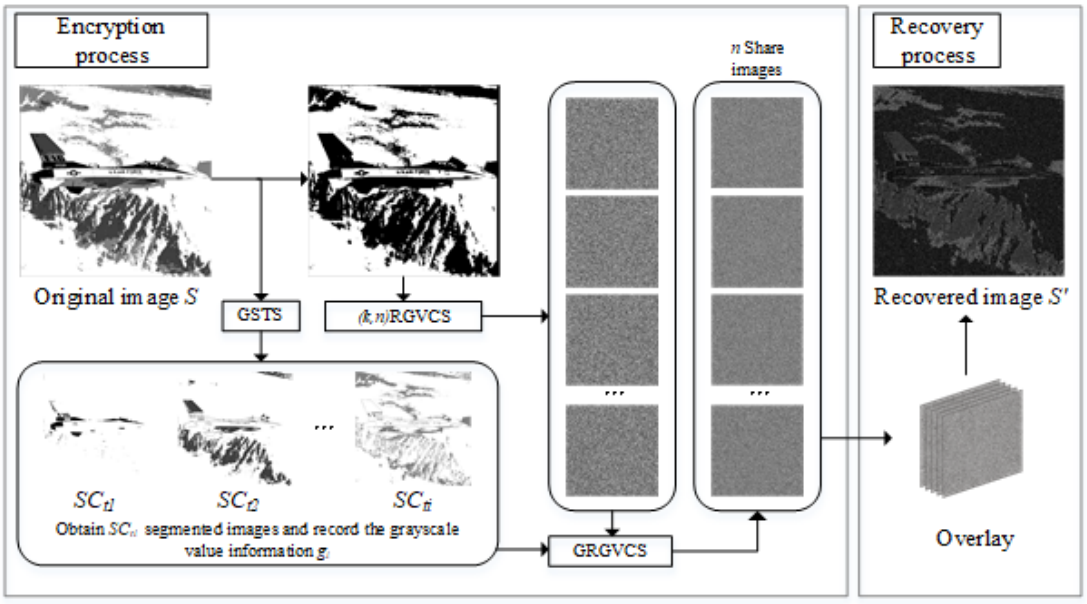

Figure.3 Flowchart of the encryption and decryption process for the (k, n) grayscale superposition algorithm

The process describes the steps involved in encrypting the original image S and recovering the image S'. First, an original grayscale image S is input, and the GSTS scheme is used to segment it into i grayscale images while recording its grayscale information.The binary image S_b undergoes the (k, n) RGVCS and GRGVCS algorithms sequentially to generate n share images containing grayscale information. During the recovery process,the image S' is obtained through overlay. The specifc description is shown in Algorithm 5.The process fow of the algorithm is depicted in Figure 4:

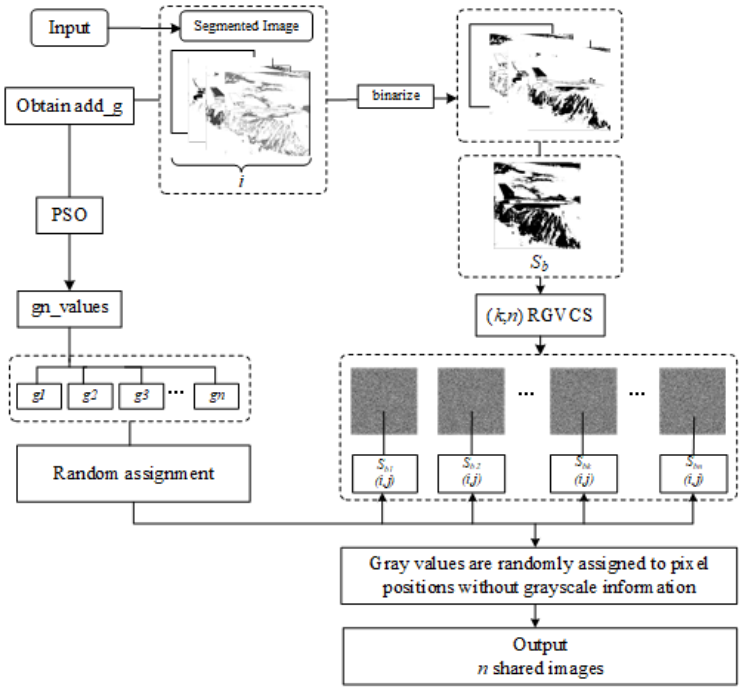

Figure.4 Flowchart of the(k, n) GRGVCS algorithm

Algorithm 5 (k, n) GRGVCS Algorithm

Input: i segmented images

Output: n share images

Initialize variables, input images, and set the grayscale levels and the (k, n) threshold value
Convert the pixels with grayscale information from the i segmented images into binary image S_b
Execute the (k, n) RGVCS algorithm on S_b:
    Obtain the first k bits
    Calculate the value of$N_k = \left[\frac{n}{k}\right]$, then assign$b_{k+1} = b_1$, $b_{k+2} = b_2, \ldots, b_{2k} = b_k, b_{2k+1} = b_1, \ldots, b_{N_k \times k} = b_k$, and finally set the pixels to zero $b_{N_k \times k+1} = b_{N_k \times k+2} = \cdots = b_n = 0$
if $S(i, j)$=1 and N_k is even **then**
    Randomly flip one bit in the generated n bits, such as 0→1 or 1→0
end if
Randomly distribute the bits $b_1, b_2, \ldots, b_n$ to the corresponding positions in the share images $S_{b1}(i, j), S_{b2}(i, j), \ldots, S_{bn}(i, j)$
Generate a randomly arranged grayscale share image:
for each of the i segmented images **do**
    Select a grayscale value add_g
    Call the grayscale value generation function to generate n grayscale values, gn_values
    Randomly distribute the grayscale values to the corresponding positions in $S_{b1}, S_{b2}, \ldots, S_{bn}$
    For pixels without grayscale information, randomly assign grayscale values
end for
Output the n share images

This algorithm outputs n grayscale shared images containing grayscale information, which can similarly achieve the restoration of the original image's pixels with grayscale information through overlay, as in the (n, n) algorithm. After introducing the threshold mechanism, the generated images cannot recover information when fewer than k share images are available. However, when the number of share images is greater than or equal to k and less than or equal to n, recovery can be achieved through overlay.

If decryption is performed under conditions with computational devices, the operator can choose not to execute step d and instead apply the (k, n) RGVCS algorithm to the i segmented images, recovering the secret via XOR operations. The specific process is the same as that described in Section 3.1. In this case, we can achieve lossless recovery of the grayscale threshold-segmented image. Therefore, If the grayscale level setting is the same as that of the original image, lossless recovery of the original image can be accomplished

3.3 Overall Security Analysis of the Scheme

This section provides a comprehensive security analysis of the scheme. Based on the Chosen-Ciphertext Attack model in cryptography, we apply a model more suitable for visual cryptography, namely the Chosen-Share Attack (CSA) model. The CSA model assumes that an attacker can selectively obtain l share images (where $l < k$) and attempt to infer information about the secret image.

By analysing the uniform distribution and statistical independence of pixels in the share images, we prove that the attacker cannot obtain any meaningful information about the secret image when possessing fewer than k shares. Specifcally, the entropy of each pixel in the share images reaches its maximum value, $H(SC_i(i,j)) = 1$, and the joint entropy of l share images is $H(C_{i1}, C_{i2}, \ldots, C_{il}) = l$. Since the conditional entropy of the secret image satisfies $H(S \mid C_{i1}, C_{i2}, \ldots, C_{il}) = H(S)$, the attacker's success probability is equivalent to random guessing, $P_{success} = \frac{1}{2^m}$, where m is the number of pixels in the secret image. This result demonstrates that the (k, n) GVCS scheme exhibits high security under the CSA model, effectively protecting the confidentiality of the secret image.

For a single share image, the process of generating non-grayscale share images is entirely random. In the (k, n) scheme, when no bit flipping is performed, the extra $n - k$ bits are randomly generated, which ensures the security of the algorithm. When bit flipping is required, the flipped pixels are also randomly selected, and all n bits are randomly distributed, ensuring the randomness of the pixels.

For the overlay of grayscale share images, we randomly generate the grayscale values using the PSO algorithm. During the generation process, boundaries can be set according to actual needs, and the resulting grayscale values are randomly assigned to the n share images. This ensures that the grayscale values within the original image's pixel areas that contain grayscale information are randomly distributed. For pixels in the original image that do not contain grayscale information, random grayscale values are also generated to fill those positions. This process promotes the randomness in the generation of the share images and supports the security of the algorithm.

An analysis of the threshold property that must be satisfied by visual cryptography schemes is conducted. Specifically, when the number of share images is less than k, no secret information can be obtained; whereas when the number of share images reaches or exceeds k, partial recovery of the original secret image information becomes possible. Without pixel flipping, the original recognizability and threshold properties hold. Furthermore, the flipping performed for lossless recovery does not affect the threshold property of the original algorithm. Therefore, the proposed scheme satisfies the threshold property.

4. SIMULATION TESTING AND PERFORMANCE ANALYSIS

4.1 Simulation of an (n, n) Grayscale Image Encryption Scheme Based on Random Grids

For the (n, n) GVCS proposed, to achieve better contrast in the experimental results under the human visual system, we performed a preprocessing step on the image. A 512 × 512 pixel four-level grayscale image was selected as the original secret image, as shown in Figure 5.

Figure.5 Original secret image

In this simulation with n = 2, the image is frst subjected to grayscale threshold segmentation, with an interval of

64, resulting in four segmented images. These segmented images are then binarized and processed using the (2, 2) GVCS algorithm for encryption and decryption operations, generating the corresponding share images. By overlaying the images in Figure 6(a)–(h), the recovered image can be obtained, as shown in Figure 6(i).To enhance the image recovery quality, we use XOR operations for the restoration of the image, followed by the application of Algorithm 3 to recover the grayscale information.The fnal recovered image is shown in Figure 6(j).

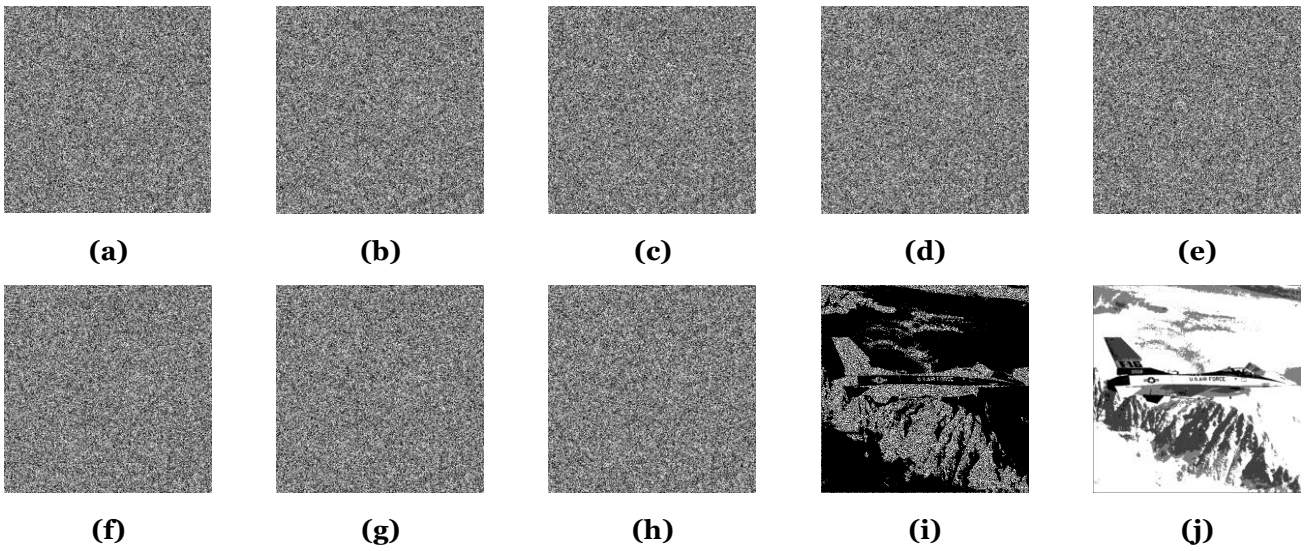

Figure.6 Simulation results of (2,2) GVCS: (**a**)–(**h**) Sharing images. (**i**) Overlay recovered image *S*‘. (**j**) XOR recovered image *S*“.

The shared images generated by the (2, 2) GVCS are binary images. The probability density of black and white pixels in each column of the shared images is computed. As shown in Figure 7, the black curve represents the distribution of black pixels, while the gray curve represents the distribution of white pixels. Both pixel types exhibit random distribution characteristics, and the pixel distributions of each shared image do not display high similarity to one another.

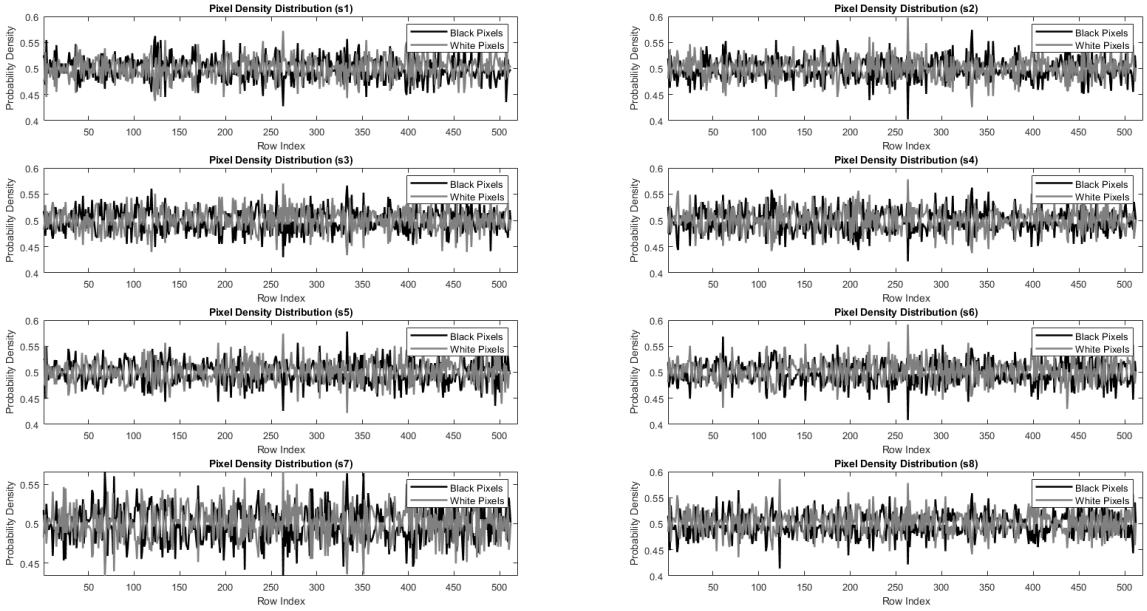

Figure.7 Probability Density Distribution of Black and White Pixels in the Shared Images.

4.2 Simulation of a (k, n) Grayscale Image Encryption Scheme Based on Random Grids

As described in this section, we carried out a simulation based on the flow of Algorithm 5, using the image in Figure 3 as the original secret image. The simulation experiment selected (4,8) as the threshold for the share images, and the eight share images containing grayscale information are shown in Figure 8(a)–(h). Images in Figure 8(i)–(k) represent the recovered images obtained by overlaying three, four, and eight share images, respectively. Figure 8(l) shows the recovered image after computation.

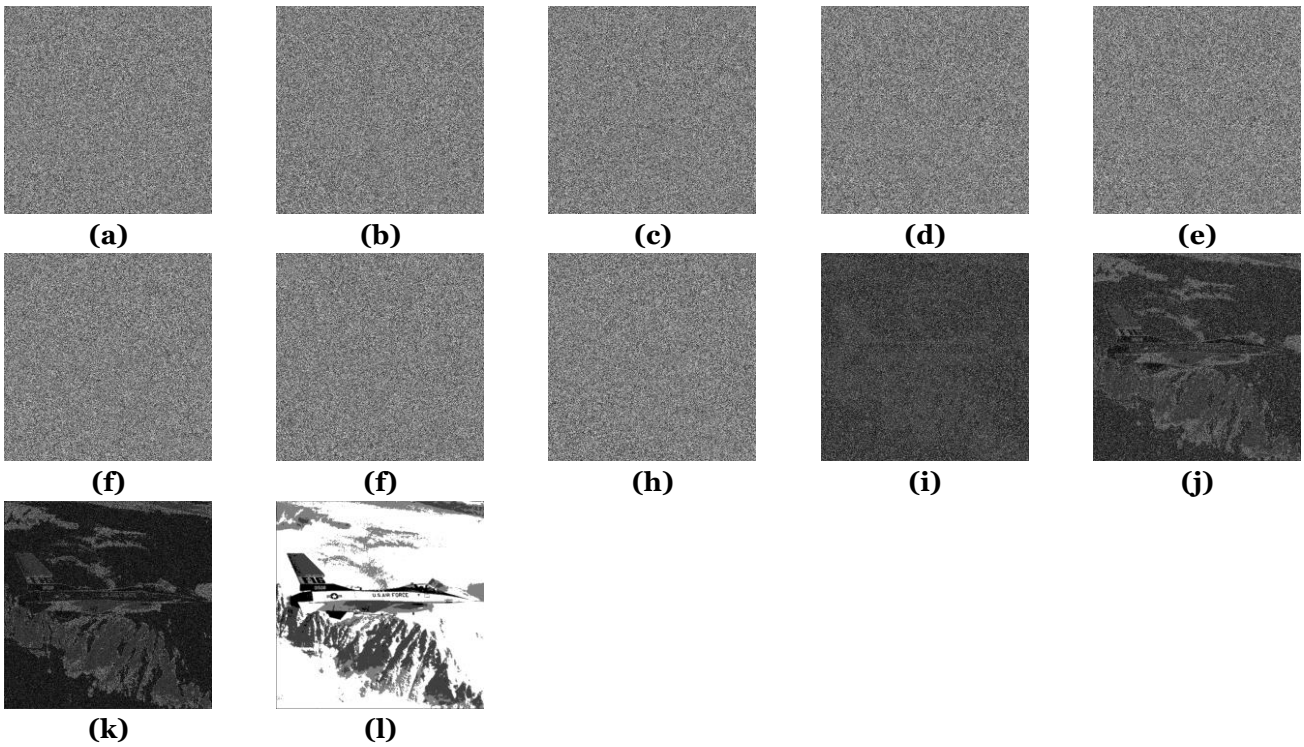

Figure.8 Simulation results of (k, n) GRGVCS: (**a**)–(**h**) Sharing images. (**i**) Overlay with three images S'. (**j**) Overlay with four images S''. (**k**) Overlay with eight images S'''. (**l**) Reconstructed image R.

Since the output shared images in the experiment are all grayscale images, grayscale histograms of the eight shared images are plotted for quantitative analysis. All shared images exhibit characteristics of noise images, with the grayscale values of different shared images showing differentiated distributions, meeting the requirements of the visual cryptography scheme.

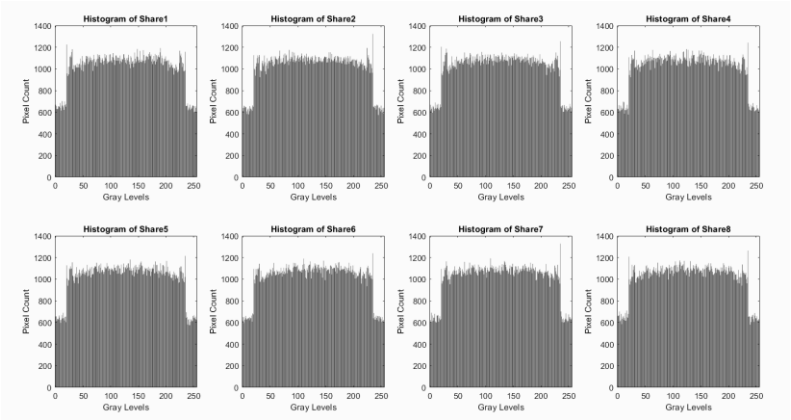

Figure.9 Display the grayscale histogram of the image.

4.3 Analysis and Comparison

For the grayscale image encryption simulation based on random grids, we used the peak signal-to-noise ratio (PSNR) and structural similarity index measure (SSIM) to verify the quality of image recovery.

a)PSNR

The PSNR is an objective criterion used to evaluate the quality of image recovery. After the image undergoes encryption and decryption operations, noise distortion is introduced. The PSNR is used to measure this distortion, where a higher PSNR value indicates better image recovery quality. Its definition is as equation (4):

$$\text{PSNR} = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{\text{MSE}}\right) \tag{4}$$

Where MAX_I^2 is the maximum possible pixel value of the image and the mean squared error (MSE) is defined as equation (5)

$$\text{MSE} = \frac{1}{MN}\sum_{\text{i=1}}^{\text{M}}\sum_{\text{j=1}}^{\text{N}}[X(i,j) - Y(i,j)]^2 \tag{5}$$

MSE measures the average squared difference between the original and reconstructed images; M and N are the dimensions of the image, representing the number of rows (height) and columns (width), respectively; $X(i,j)$ is the pixel value of the original image at coordinates (i,j); $Y(i,j)$ is the pixel value of the reconstructed image at coordinates (i,j); the summation $\sum_{i=1}^{M}\sum_{j=1}^{N}$ calculates the total squared difference for all pixels in the image; and the term $\frac{1}{MN}$ normalizes the result by the total number of pixels, giving the average squared error.

b)SSIM

The SSIM is used to measure the similarity between two images. It integrates structural information of the images and aligns with the human visual system's image evaluation model. The closer the SSIM value is to 1, the better the image recovery quality. Its definition is as equation (6):

$$\text{SSIM} = \frac{(2\mu_I\mu_D + C_1)(2\sigma_{ID} + C_2)}{(\mu_I^2 + \mu_D^2 + C_1)(\sigma_I^2 + \sigma_D^2 + C_2)} \tag{6}$$

where μ_I and μ_D represent the mean values of the input image I and the decrypted image D, respectively; σ_I^2 and σ_D^2 represent the variances of I and D, respectively; σ_{ID} represents the covariance between I and D; C_1 and C_2 are regularization constants; and $C_1 = (K_1L)^2$ and $C_2 = (K_2L)^2$ are constants added to avoid division by zero. Here, L is the dynamic range of pixel values (typically 255 for 8-bit images), and K_1 and K_2 are small constants, typically chosen as $K_1 = 0.01$ and $K_2 = 0.03$.

c) Image contrast

$$\alpha = \frac{P_0 - P_1}{1 + P_1} \tag{7}$$

where α represents the image contrast, P_0 denotes the probability of correct decoding for white pixels, and P_1 represents the probability of incorrect decoding for black pixels.

When the image is recovered by overlaying, pixels without grayscale value information tend to become darker, resulting in lower PSNR and SSIM values. Therefore, contrast is introduced as another quantifiable metric. A quantified image contrast of nearly 0 indicates that the recovered image cannot reveal the information of the secret image.

Now, based on the above metrics, we analyze the simulation results from Sections 4.1 and 4.2, as shown in Table 1.

Table 1 Analysis of image recovery quality

Schemes	(n,n)GVCS		(k,n)GRGVCS			
	Image(i)	Image(j)	Image(i)	Image(j)	Image(k)	Image(l)

PSNR	46.5053	Inf	0.7236	3.1424	3.8640	Inf
SSIM	0.9228	1	0.001	0.0025	0.0035	1
α	\	1	≈0	0.46	0.47	1
Size	512^2px	512^2px	512^2px	512^2px	512^2px	512^2px

For the (n, n) GVCS simulation results, regardless of whether a computational process is involved, the size of the recovered image is the same as that of the original image. This indicates that the share images generated by the scheme do not exhibit pixel expansion. Without any computation, it can be observed that the recovered image obtained through overlaying can be recognized by the human visual system. After simple computation, the recovered image has a PSNR value of Inf and an SSIM value of 1, indicating no distortion occurred during the image recovery process, and the scheme can achieve lossless recovery of the secret image relative to the original image.

Similarly, we analyze the quality of the four recovered images obtained using the (k, n) GVCS scheme. The results also show that the share images generated by the scheme do not exhibit pixel expansion. For the images recovered by overlaying, the image (i)'s contrast is less than 0, indicating that when the number of images involved in the recovery is smaller than the required k-threshold, the recovered image cannot reveal the information of the secret image, thus satisfying the security requirements for visual cryptographic shared images. The contrast of images (j) and (k) is 0.46 and 0.47, respectively, indicating that the recovered images can reveal the information of the secret image. Visual observation also shows that when the number of overlayed images reaches the threshold, the content of the original image can be identified.

When computational devices are available, as with the (2,2) scheme, using the method of performing GSTS first, followed by encryption and decryption recovery with the (k, n) scheme, we can achieve lossless recovery of the image. The PSNR of image (l) is Inf, and the SSIM value is 1, both of which meet the requirements of the lossless definition.

Table 2 Comparison of grayscale visual cryptography schemes

Scheme	Sharing	No Pixel Expansion	Lossless recovery	Satisfies the (k, n)	Computational complexity
Our Scheme	Grayscale	Yes	No	Yes	$O(1)$
	Binary	Yes	Yes	Yes	$O(n)$
Reference [2]	Binary	No	No	No	$O(1)$
Reference [10]	Grayscale	No	Yes	No	$O(n)$
Reference [12]	Binary	No	No	No	$O(1)$
Reference [14]	Grayscale	Yes	No	Yes	$O(1)$
Reference [16]	Binary	Yes	No	No	$O(n)$

Table2 shows that the scheme proposed in this paper demonstrates significant advantages over other existing schemes in several aspects. It supports (k, n) image sharing, with share images showing no pixel expansion, a capability that is not available in some schemes, especially those handling grayscale images, which are more limited in this regard. In terms of lossless recovery, the proposed scheme ensures lossless recovery for black-and-white shares and achieves high recovery quality for grayscale shares, preserving the integrity of the image information. In contrast, the schemes in references fall short in this respect.

Additionally, this paper introduces a (k, n) GVCS algorithm where the share images are grayscale, providing the overall scheme with better adaptability and flexibility—features not found in other methods. This scheme, like other visual cryptography schemes for grayscale images, also exhibits no pixel expansion, satisfies the (k, n) threshold, and features low computational complexity.

In conclusion, the proposed scheme outperforms existing solutions in key metrics such as no pixel expansion, threshold selection, lossless recovery, and computational complexity, demonstrating its exceptional performance and broad application potential.

5. CONCLUSION

This study explores grayscale visual cryptography schemes and proposes a GVCS with lossless recovery capabilities. Compared to previous schemes, the proposed approach eliminates the need for generating encryption matrices and avoids pixel expansion in the shared images. During the image encryption and decryption phases, the scheme employs XOR operations for construction and recovery, which simplifies the computational process. Moreover, when all shared shares participate in the recovery, the scheme achieves lossless image reconstruction. Additionally, to address real-world scenarios without computational devices, a grayscale visual cryptography scheme based on the grayscale overlay principle is proposed. This scheme utilizes the PSO algorithm to generate random grayscale values, directly producing shared images with grayscale information that can be restored through overlay operations. The study provides a detailed description of the algorithms for generating and recovering shared images and theoretically analyzes the security of the proposed scheme. Simulation experiments validate the feasibility of the scheme, demonstrating its enhanced applicability, improved security, and suitability for distributed systems or cloud computing environments.

The scheme is suitable for secure data storage and transmission in cloud computing, privacy protection in medical or financial image processing, and secure image sharing in military communications. However, limitations include computational complexity for lossless recovery, incomplete systematization of grayscale threshold segmentation, and suboptimal random grayscale value distribution. Future research should focus on optimizing grayscale image processing, systematizing threshold rules, improving grayscale value distribution, and extending the scheme to colour images. Large-scale real-world testing will further enhance the algorithm's practicality and performance, broadening its impact in visual cryptography and related fields.

Acknowledgements

The authors acknowledge the National Natural Science Foundation of China (Grant: 62072014)

References

[1] Shamir. A. How to share a secret. Commun. ACM 1979, 24, 612–613.
[2] Naor. M.; Shamir. A. Visual cryptography. In EUROCRYPT 1994; Lecture Notes in Computer Science; Springer Press: Berlin, Heidelberg, 1995; Vol. 950, pp. 1–12.
[3] Kafri. O, Keren. E. Encryption of pictures and shapes by random grids. Opt. Lett. 1987, 12(6), 377–379.
[4] Hiroki. K., Yamamoto, H. Proposal of a Lattice-based Visual Secret Sharing Scheme for Color and Gray-scale Images. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 1998, 81(6), 1262–1269.
[5] Blundo. C, De Santis. A., Naor. M. Visual cryptography for grey level images. Inf. Process. Lett. 2000, 75(6), 255–259.
[6] Lin. C, Tsai. H. Visual cryptography for gray-level images by dithering techniques. Pattern Recognit. Lett. 2003, 24, 349–358.
[7] Hou. Y, Tu. C. F. Visual cryptography techniques for color images without pixel expansion. J. Inf. Technol. Soc. 2004, 1, 95–110.
[8] Sun. R., Fu. Z., Li. X., et al. A novel size-invariant visual cryptography scheme based on two-level threshold. J. Cryptologic Res. 2021, 8(4), 572–581.
[9] He. W, Liu. C, Han. Y, et al. Multi-level visual cryptography scheme with lossless recovery. Appl. Res. Comput. 2017, 34(5), 1540–1543.
[10] Liu. J, Zhang. Y, Liu. Y, et al. Analysis and design of visual secret sharing scheme for gray image. Chin. J. Netw. Inf. Secur. 2020, 6(4), 140–147.
[11] Liu .X , Wang .S, Yan .X .H, et al. Random grid-based threshold visual secret sharing with improved visual quality and lossless recovery ability. Multimedia Tools and Applications, 2018, 77(16):20673-20696..
[12] Kennedy. J, Eberhart. R. Particle swarm optimization. In Proceedings of ICNN'95 - International Conference on Neural Networks; IEEE: Perth, WA, Australia, 1995; Vol. 4, pp. 1942–1948.
[13] Alex. N. S, Anbarasi. L. J. Enhanced image secret sharing via error diffusion in halftone visual cryptography. In Proceedings of the 3rd International Conference on Electronics and Computer Technology; IEEE: Kanyakumari, India, 2011; pp. 393–397.
[14] Kumar. S, Sharma. R. K. Threshold Visual Secret Sharing based on Boolean Operations. Security & Commun. Networks 2014, 7(3), 653–664.

[15] Chen. Y, ST. J. J. XOR-Based (n, n) Visual Cryptography Schemes for Grayscale or Color Images with Meaningful Shares. Appl. Sci. 2022, 12(19), 10096.
[16] Huang. B, ST. J. Flexible meaningful visual multi-secret sharing scheme by random grids. Multimed. Tools Appl. 2020, 79, 7705–7729.
[17] Ibrahim, D.R., Teh, J.S. & Abdullah, R. An overview of visual cryptography techniques. Multimed Tools Appl 2021,80, 31927–31952.
[18] Bachiphale, P.M., Zulpe, N.S. A comprehensive review of visual cryptography for enhancing high-security applications. Multimed Tools Appl,2024.
[19] Wu.X.T , Yang.CN. Probabilistic color visual cryptography schemes for black and white secret images, Journal of Visual Communication and Image Representation, 2020,70,102793.
[20]Wang. L, Yan. B, Yang. H.-M.and Pan. J.-S. Flip Extended Visual Cryptography for Gray-Scale and Color Cover Images. Symmetry 2020, 13, 65.