Mathematical Biosciences and Engineering

http://www.aimspress.com/journal/mbe

MBE, 19(12): 12160–12179.
DOI: 10.3934/mbe.2022566
Received: 09 May 2022
Revised: 02 July 2022
Accepted: 24 July 2022
Published: 19 August 2022

Research article

Adaptive visual cryptography scheme design based on QR codes

Li-na Zhang[1,2,*], **Chen-yu Cui**[1], **Xiao-yu Zhang**[1] **and Wei Wu**[1]

[1] College of Computer Science and Technology, Xi'an University of Science and Technology, Xi'an 710054, China

[2] School of Computer Science, Shaanxi Normal University, Xi'an 710119, China

* **Correspondence:** Email: zhangln@xust.edu.cn; Tel: +8617795724270.

Abstract: QR code based visual encryption schemes are still relatively rare, and the existing schemes are mainly implemented by averaging grayscale maps. They become distorted when recovering complex secret images. In this paper, we propose a visual cryptography scheme based on QR codes. We use two adaptive schemes to improve the distortion problem in secret image recovery. The algorithm for generating the QR code shared matrix is improved, and the secret image can be restored quickly. This scheme could ensure the uniform distribution of secret vectors. Meanwhile individual shared QR codes would never reveal any secret information. The proposed algorithm reduces the space consumed by the secret vector and the probability of falling prey to illegal attacks. Compared with other schemes, the secret image recovered via the proposed method is clearer and the scheme is suitable for scenarios in which the secret images are more complex, as it yields better security and practicality.

Keywords: QR code; grayscale mapping; visual cryptography scheme; XOR operation

1. Introduction

With the development of the Internet, one-dimensional barcodes have become rapidly popularized in daily life, which has caused the speed of information collection and data processing to increase rapidly. However, it can only hold a limited amount of information and does not have enough capacity to provide more descriptions of the attributes of the items. Therefore, the quick response code (QR code) [1] was proposed; it can effectively solve the shortcomings of 1D codes, such as carrying too little information and being unable to correct errors. However, the QR code data conversion encoding process is intrinsically public, which leads to its low practicality in areas with high security requirements. How to use QR codes to hide secret information has become a very important topic.

Since visual cryptography [2] was formally proposed at the European Cryptography Annual Conference in 1994, it has been widely studied and applied by a large number of scholars. Based on secret

sharing and digital image technology, the application of secret sharing technology to visual cryptography has become a new research hotspot.Visual cryptography is an encryption scheme for sharing secret images, and it has the advantages of simplicity, security and stealth over traditional cryptography. The encryption process is to share the image code and print the shared share on transparencies or store it in the form of a digital matrix, whereas the decryption process is to superimpose the shared transparencies or perform a heterogeneous operation on the digital matrix that is then observed it by human visual systems. Visual cryptography is a lightweight recovery technology constructed based on human visual characteristics, and it requires only simple superposition or an anomaly operation to achieve the recovery of secret images without any other cryptography techniques.

Most schemes in the early days of visual cryptography development used binary images as carrier images to design sharing schemes. In the literature [3], a fully recoverable visual secret sharing scheme is proposed. This scheme satisfies the condition that pixels do not expand. It achieves lossless reconstruction of secret images via linear addition operations. The study in [4] resulted in an image secret sharing scheme with a threshold of (t, k, n), and the method entails the use of the secret image to influence the selection of the sharing matrix. Unlike other schemes, t participants can only decrypt low-quality secret image information, while k participants can recover accurate information. A two-level threshold-based visual cryptography scheme has also been proposed in the literature [5]. The first-level threshold is used to distinguish low-frequency and high-frequency regions, and different sharing methods have been adopted for different frequency regions. Low-frequency regions are shared with solid color pixel blocks, and high-frequency regions are shared using the second-level threshold to modulate the mapping relationship between the gray values of the secret image and the sharing matrix. The scheme is based on two-level threshold processing, which enhances the details of secret image recovery. Researchers [6] have also proposed an optimization scheme based on error diffusion, which reduces the random patterns of the shared image and only encodes the black pixels of the secret image to minimize the pixel expansion. A physically based visual secret sharing scheme has been proposed in the literature [7]. This scheme only needs two parts of sharing, requires no arbitrary pixel expansion and the recovered pixels have well-defined colors and good resolution. In the literature [8], for the first time, Tuyls et al. introduced the concept of XOR visual cryptography (i.e., an XOR-based visual cryptography scheme (XVCS)). This scheme gives a new direction for the development of visual cryptography. The visual cryptography sharing scheme in which the secret information can be fully recovered is introduced in the paper, and the pixel expansion of this scheme is 1. The main advantage of the XVCS is that the XOR operation is extremely easy in secret recovery. XVCSs have received much attention from many experts and scholars.

1.1. Related work

With the maturity of QR code application technology, more scholars increasingly combine QR code and visual cryptography technology. Nowadays, the secret sharing scheme based on QR codes has become a hotspot of visual cryptography research. In [9], the QR code is used as a carrier image for the secret image. Part of the pixels can be adjusted to make the shared image present the image information of the QR code. Secret sharing units were designed in [10], mainly by using machine vision recognition features. The size of the secret unit is composed of 2×2 modules, and the secret information of the carrier module can be determined by calculating the ratio of black and white pixels. However, the applicability of the shared QR code generated via this scheme is limited, and the pixel expansion is too

large, which reduces the recognition accuracy of the QR code. To solve the above problems, a secret sharing based algorithm is proposed in the literature [11]; it combines the error correction mechanism of QR codes reasonably with the secret sharing scheme. It improved upon the recognition efficiency of QR codes, but the payload of the secret information is limited. The study in [12] yielded an XVCS wherein the pixels are divided in the first step. Then the mapping relationship between the gray values and the division levels is established. A matrix set corresponding to a series of templates is generated according to the generation algorithm for the sharing matrix. Finally, the corresponding sharing matrix is selected by the gray value of the secret image to fill and update the individual shared QR codes. And it is ensured that each shared image itself cannot extract any information. Only by performing XOR operations on all shared images can the secret image be directly obtained. The scheme is very convenient in terms of recovering the secret information without computer calculation. And it satisfies the conditions of non-expanding pixels; however, the secret image will be distorted with this scheme. When the secret image is too bright or too dark, the mapping scheme for the average gray value cannot restore the secret image. Through continuous development, the QR code can also be graded [13–17] to make the secret payload larger.

1.2. Our contribution

This paper introduces an adaptive visual cryptography scheme based on QR codes, and our contributions are as follows:

- Our scheme considers the self-features of the secret image when establishing the mapping between the gray level and the series of templates. In this work, two methods of adaptive secret image enhancement and adaptive secret image grayscale mapping were used to design the scheme. The scheme is suitable for more complex scenes, such as scenes in which the secret image can be quickly recovered when the secret image is too dark or too bright.
- This paper introduces a new vector construction method to make "1" evenly distributed. The scheme guarantees the randomness of the vector values, that is, the probability of taking any value is the same. It solves the space consumption and security problems of vectors.
- We demonstrate the safety and effectiveness of the proposed scheme. We also verify the strong performance of the scheme in real experiments compared to other schemes in the literature.

1.3. Organization

The rest of the paper is organized as follows. In Section 2, we present the main contents of the scheme. Section 3 mainly proves the effectiveness of the scheme in terms of its comparability and security; In Section 4, we gives the experimental results. In Section 5, we give the performance analysis for our scheme. Section 6 gives the summary.

2. Our construction

The visual cryptography sharing scheme, which is a lightweight secret recovery scheme designed according to the visual properties of the human body. The scheme is mainly for secret sharing and secret recovery, making it slightly different from traditional cryptography schemes. It is not equivalent

to traditional encryption algorithms or decryption algorithms. In this section, we present the main contents of the scheme, which consists of four main algorithms. It includes an algorithm for mapping grayscale values to templates, an algorithm for generating a set of shared matrices, a secret sharing algorithm and a secret recovery algorithm.

2.1. Algorithm for mapping grayscale values to templates

We can divide the gray values by intervals to produce different mappings, which allows us to simplify the secret image to get its characteristic image. In the establishment of the mapping relationship between the image gray level and the series template, the self-characteristics of the secret image should be considered. The closer the mapping relationship to the image, the higher the similarity between the obtained features and the original image. In this paper, two methods will be demonstrated for the construction. The first method is to enhance the input secret image and then divide the gray level into five gray-level intervals. The second method is the adaptive gray-scale partition of the secret image, which makes the number of pixels in the partition as equal as possible according to the characteristics of the image itself. Then divide the five gray-level intervals according to the principle of equal probability as much as possible.

2.1.1. Scheme I: Adaptive secret image mapping

In the visual cryptography scheme, if the secret image is too dark or too bright, it is not accurate enough in the interval division of gray mapping; this leads to distortion of the recovered secret image. We can perform adaptive partitioning of the secret image so as to establish an effective mapping relationship and prevent distortion when recovering the secret image.

Based on the above analysis, our partitioning process for the adaptive secret image was developed as is shown in Figure 1.

The specific steps of the adaptive secret image mapping process are as follows: (The scheme grayscale mapping designed in this work has five levels.)

Step 1: Input the secret image, generate the histogram of the secret image, $H(X_k)$ as the number of pixels under the gray level X_k for the total pixel value $Count$ for the secret image.

Step 2: Generate a cumulative histogram for the secret image based on the histogram $W(X_k)$ as the cumulative probability of the gray level X_k such that $W(X_k) = \frac{\sum_{k=\min}^{\max} H(X_k)}{Count}$ and $X_{\min}$ and $X_{\max}$ is the gray minimum and gray maximum of the secret image, respectively.

Step 3: Order $m = 1$.

Step 4: Find X_k satisfying $Min\left|\frac{Count}{5} \times m - W(X_k)\right|$ and store them in the array $b[m] = X_k$.

Step 5: Order $m = m + 1$ and continue the execution of Step 4; when, $m > 5$ execute Step 6.

Step 6: Output the array b with the interval divided into $(\min, b[1]), (b[1], b[2]), \cdots, (b[4], \max)$

Example 1 is given below to further illustrate Scheme I.

Example 1: The shared secret image is an image with overall darker grayscale values, as shown in Figure 2.

The overall grayscale of the secret image is low, so we need to use the adaptive secret image mapping algorithm, as shown in Figure 2. First calculate the histogram, and then generate the cumulative

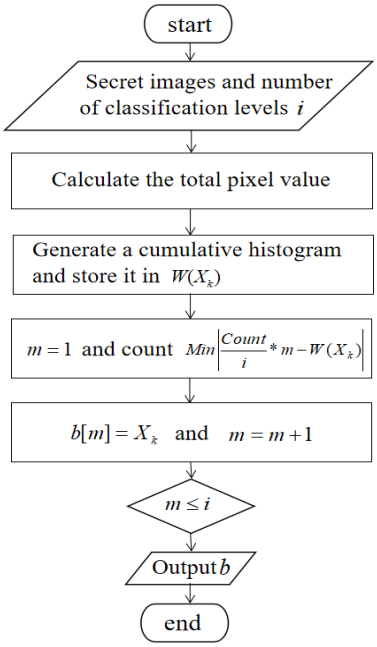
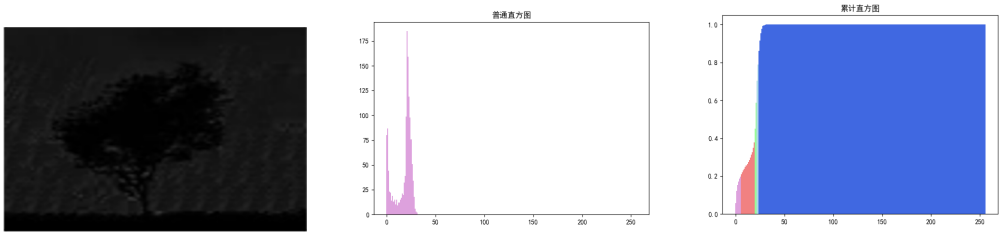


Figure 1. Flowchart of adaptive partitioning process for secret images.



(a) (b) (c)

Figure 2. Test diagrams and results for Example 1: (a) secret image; (b) histogram; (c) cumulative histogram.

histogram; finally, use it to get the endpoints of the interval division to get the grayscale mapping table of the secret image, as shown in Table 1.

2.1.2. Scheme II: Adaptive secret image enhancement

Image enhancement is a hot research topic in image processing, which is mainly purposed to improve the visual effects of images. Such effects include increasing the contrast, improving the brightness, enhancing the clarity, enriching the details, etc. In the visual cryptography scheme, if the secret image is too dark or too bright, it is not accurate enough in the interval division of the gray-scale mapping, which leads to distortion of the recovered secret image. So, we need to process the secret image at first, and the commonly used image enhancement method is the histogram equalization algorithm. However, the traditional histogram equalization method will introduce visual degradation while enhancing the image, such as over-enhancement and halos in some regions.

Through [18], we know that the following three characteristics should be maintained in the image

Table 1. Mapping table for Example 1.

Grayscale level	Grayscale value interval
5	[0,4]
4	(4,19]
3	(19,21]
2	(21,23]
1	(23,255]

enhancement process to make the image truly processed: (i) the average value of the enhanced image should be consistent with that before enhancement as much as possible; (ii) after enhancement, the contrast of the image needs to be enhanced, that is, the grayscale standard deviation of the output image needs to be as large as possible; (iii) in the process of image enhancement, it is necessary to ensure that details are not lost, that is, details with low probability density need special treatment to prevent them from being merged.

In summary, our enhancement process for the secret image is shown in Figure 3.

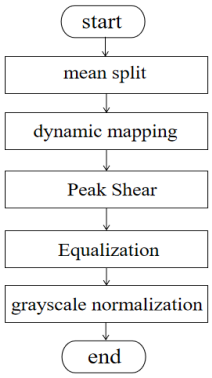


Figure 3. Flow-chart for secret image enhancement.

The specific steps of adaptive covert image enhancement are as follows:

Step 1: Input the secret image and calculate the grayscale mean X_{Aver} of the image; use the result to divide the secret image into two sub-images, where the grayscale range of the image is partitioned as in the following equation:

$$X = \begin{cases} X_L = \{X(i,j) | X(i,j) < X_{Aver}\} \\ X_R = \{X(i,j) | X(i,j) > X_{Aver}\} \end{cases} \tag{2.1}$$

Step 2: Adaptively expand the sub-region to find an optimal segmentation point, X_{Best}, so that the pixel density of the two sub-regions after the dynamic mapping process is as uniform as possible. X_{Best} satisfies Eq (2.2):

$$\frac{Count_L}{X_{Best} - 0} = \frac{Count_R}{255 - X_{Best}} \Leftrightarrow X_{Best} = \frac{255 \times Count_L}{Count_L + Count_R} \tag{2.2}$$

where $Count_L$, $Count_R$ is the number of pixels in the left and right sub-regions.

Then the two new sub-regions are those described in Eq (2.3):

$$X = \begin{cases} \tilde{X}_L = [0, X_{Best}) \\ \tilde{X}_R = [X_{Best}, 255] \end{cases} \tag{2.3}$$

The grayscale values of all of the pixels in the secret image are also changed, and the mapping relationship is described by Eq (2.4):

$$\tilde{X}(i,j) = \begin{cases} \dfrac{X(i,j) - X_{Min}}{X_{Aver} - X_{Min}} \times X_{Best}, X(i,j) \in \tilde{X}_L \\ X_{Best} + \dfrac{X(i,j) - X_{Aver}}{X_{Max} - X_{Aver}} \times (255 - X_{Best}), X(i,j) \in \tilde{X}_R \end{cases} \tag{2.4}$$

where $\tilde{X}(i, j)$ is the grayscale value of the image in the position (i, j) and the minimum and maximum grayscale values of the secret image are respectively X_{Min} and X_{Max} . The grayscale range of the new secret image at this point is $[0, 255]$.

Step 3: Find the best cut point at P_L and P_R to the new left and right sub-regions, respectively. The clipped sub-region does not have the phenomenon of large pixel density in the sub-region. The best cut point (P_L, P_R) satisfies Eq (2.5):

$$P_L = \frac{Count_L}{X_{Best} - 0} and P_R = \frac{Count_R}{255 - X_{Best}} \tag{2.5}$$

Then the new two sub-region shear conditions are as presented in Eq (2.6):

$$\tilde{H}_L(X_k) = \begin{cases} H(X_k), H(X_k) \le P_L \\ P_L, H(X_k) > P_L \end{cases} \tag{2.6}$$

$$\tilde{H}_R(X_k) = \begin{cases} H(X_k), H(X_k) \le P_R \\ P_R, H(X_k) > P_R \end{cases}$$

where X_k is the gray level, the left sub-region satisfies $0 \le X_k < X_{Best}$, the right sub-region satisfies $X_{Best} \le X_k \le 255$, $H(X_k)$ is the number of pixels under the gray level $H(X_k)$ and $\tilde{H}_L(X_k)$ and $\tilde{H}_R(X_k)$ respectively denote the numbers of pixels under the gray level X_k for the left and right sub-regions after clipping.

Step 4: Perform histogram equalization on the new left and right sub-regions respectively to get the new left and right sub-regions X'_L and X'_R. The histogram after secret image enhancement at this point is $X' = X'_L \cup X'_R$.

Step 5: Normalize X'; the normalization of the whole histogram is achieved by calculating the translation factor. At this point, the normalized histogram $\hat{X}$ satisfies Eq (2.7):

$$\hat{X}(i,j) = \frac{X_{Aver}}{X'_{Aver}} \times X(i,j) \tag{2.7}$$

where $\hat{X}(i, j)$ denotes the gray values at the locations (i, j) of the original secret image; X'_{Aver} denotes the mean gray values of the histogram after the equalization process.

Step 6: Average the grayscale range to obtain the mapping relationship between grayscale levels and grayscale intervals as shown in Table 2.

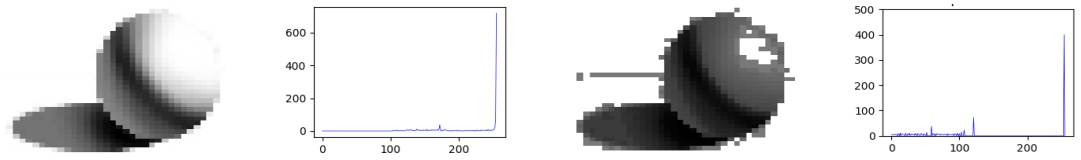
Table 2. Mapping table for Scheme II.

Grayscale level	Grayscale value interval
5	[0,51]
4	(51,102]
3	(102,153]
2	(153,204]
1	(204,255]

In summary, we can know that Step 1 improves the stability of the image grayscale mean. Too much partitioning will prevent contrast enhancement, and no partition will affect the grayscale mean value. So we need to determine the number of partitions according to the mean; Step 2 can achieve a better image enhancement effect. Due to the large pixel density of some intervals, the image enhancement effect cannot be guaranteed if the traditional histogram equalization method is directly used. We need to reallocate the interval positions and adjust the grayscale mapping range of the sub-regions; Step 3 makes the grayscale mean more stable after image enhancement. It prevents the pixel points from being too concentrated in a small interval, which leads to over-enhancement. When a small probability of gray levels are merged, more details are lost and the histograms of the left and right sub-regions need to be cut. Step 4 is the image enhancement, and the ideal state is that the pixels are evenly distributed on each gray level. Step 5 makes the processed grayscale mean stable. The histogram is shifted to make the gray level stable.

Example 2 is given below to further illustrate Scheme II.

Example 2: The shared secret image is an image with overall brighter grayscale values as shown in Figure 4.



(a) (b) (c) (d)

Figure 4. Test diagrams and results for Example 2: (a) original secret image; (b) original histogram; (c) secret image after processing; (d) histogram after processing.

The overall grayscale value of the secret image is high, so the direct equalization interval for mapping will be severely distorted. We need to enhance the secret image by using the algorithm of Scheme I. As shown in Figure 4, we can find that the peak of the enhanced secret image is reduced and more equalized, making the contour and contrast of the image more obvious. Next, using the enhanced image for mapping, we can get the mapping table as shown in Table 3.

2.2. Algorithm for generating the set of shared matrices

From the information storage structure of the QR code, it is clear that the binary information storage structure $a \times a (a \geq 3)$ is used to replace one pixel of information in the QR code. The intermediate pixels in the information storage structure are controlled without changing the QR code coding and

Table 3. Mapping table for Example 2.

Grayscale level	Grayscale value interval
5	[0,51]
4	(51,102]
3	(102,153]
2	(153,204]
1	(204,255]

decoding rules. The new QR code obtained via the visual sharing scheme can still be extracted and read by the decoding tool of the QR code, and this structure is called a modular recognition unit.

In this work, a modular cell 3×3 was used; the central area aligned with the carrier QR code. The remaining eight pixels store secret information sequentially in the order of top to bottom and left to right. That is, the surrounding eight pixels are a set of row vectors in the sharing matrix M. From this, we can see that the size of the sharing matrix is $n \times 8$, where n is the number of shared QR codes.

The sharing matrix designed in the scheme plays the role of a key in the visual cryptography sharing scheme, and the corresponding sharing matrix will be selected to fill the shared copies according to the size of the pixel values.

The sharing matrix generation algorithm is as follows: (The scheme grayscale mapping designed in this paper have five levels.)

Step 1: Order $i = 1$; at this point, $j = 0$.

Step 2: Set j as an 8-bit binary number equal to s.

Step 3: Generate $n - 1$ random 8-element vectors, $r_i (i = 1, 2, \ldots n - 1)$, and satisfy $H(r_i) = 4$.

Step 4: Calculate $r_n = r_1 \oplus r_2 \oplus \cdots \oplus r_{n-1} \oplus s$; if $H(r_n) = 4$, then let $M = [r_1, r_2, \cdots, r_{n-1}, r_n]^T$, where $g = i$ and $M \in M_g$.

Step 5: Repeat Steps 3 and 4 until all cases of $n - 1$ random 8-element vectors $r_i (i = 1, 2, \ldots n - 1)$ are traversed.

Step 6: Perform a random permutation about the columns of s, repeat Steps 3 and 5 until all permutations are traversed.

Step 7: Make $i = i + 1$ and $j = 3 \times 4^{i-2} + j$; if $i \leq 5$ jump to Step 2; otherwise execute Step 8.

Step 8: Output $M_g (g = 1, 2, \ldots, 5)$.

We use the secret vector to calculate and generate the corresponding sharing matrix. The secret vector then makes different gray values correspond to different sharing matrices so that the contrast is enhanced and the recovered secret image is clearer.

Among the eight pixels added again, at that time, we cannot tell whether it is black or white when $H(r_i) = 4$, which confirms that a single shared copy of the QR code is unable to get any information of the secret image and ensures the security of the secret image. This is the reason why we choose 4 as the distance to be satisfied.

2.3. Secret sharing algorithm

For secret sharing, each pixel point in the secret image needs to be scanned. The corresponding sharing matrix is selected to fill the shared QR codes according to the size of the pixel value. The sharing matrix mainly depends on the grayscale mapping relationship established in Section 2.1. When

recovering the image, the binary vector of the corresponding position of the shared QR code is the row vector of the matrix. Two schemes are introduced in this paper, and the secret sharing algorithms for each of the two schemes are described next.

2.3.1. Steps of secret sharing for Scheme I

Step 1: Input n carrier QR codes $C_1, C_2, \cdots, C_n$ of size $q \times q$ and a secret image S of size $3q \times 3q$.

Step 2: Expand $C_1, C_2, \cdots, C_n$ by three times to get n shared QR codes $A_1, A_2, \cdots, A_n$, satisfying Eq (2.8):

$$\begin{bmatrix} A_t(3i-2,3j-2) & A_t(3i-2,3j-1) & A_t(3i-2,3j) \\ A_t(3i-1,3j-2) & A_t(3i-1,3j-1) & A_t(3i-1,3j) \\ A_t(3i,3j-2) & A_t(3i,3j-1) & A_t(3i,3j) \end{bmatrix} = \begin{bmatrix} C_t(i,j) & C_t(i,j) & C_t(i,j) \\ C_t(i,j) & C_t(i,j) & C_t(i,j) \\ C_t(i,j) & C_t(i,j) & C_t(i,j) \end{bmatrix} \tag{2.8}$$

where (i, j) is the ith row and jth column of the carrier QR code that satisfies $1 \le i \le q, 1 \le j \le q$; t is the number of the shared QR codes that satisfies $1 \le t \le n$.

Step 3: Partition both the secret image and the shared QR code into 3×3 pixel blocks. After processing, they all have $q \times q$ blocks. Each pixel block of the secret image corresponds to n shared QR codes.

Step 4: Order $i = 1, j = 1$.

Step 5: Calculate the grayscale mean value of the pixel blocks in the secret image according to Eq (2.9):

$$G_{average} = \frac{\sum_{m=3i-2}^{3i} \sum_{n=3j-2}^{3j} S(m,n)}{9} \tag{2.9}$$

Step 6: Determine the set of M_g according to $G_{average}$, g is the rank in the mapping table; different secret images have different gray mapping relationships, and the corresponding ranks will change.

Step 7: Randomly select a matrix M in the set of M_g and assign n vectors in the matrix to n shared QR codes such that

$$\begin{bmatrix} A_t(3i-2,3j-2) & A_t(3i-2,3j-1) & A_t(3i-2,3j) \\ A_t(3i-1,3j-2) & A_t(3i-1,3j-1) & A_t(3i-1,3j) \\ A_t(3i,3j-2) & A_t(3i,3j-1) & A_t(3i,3j) \end{bmatrix} = \begin{bmatrix} M(t,1) & M(t,2) & M(t,3) \\ M(t,4) & C_t(i,j) & M(t,5) \\ M(t,6) & M(t,7) & M(t,8) \end{bmatrix} \tag{2.10}$$

where t is the number of shared QR codes that satisfy $1 \le t \le n$.

Step 8: Order $j = j + 1$; if $j \le q$, then jump to Step 5; otherwise, execute Step 9.

Step 9: Order $i = i + 1$; if $i \le q$, then jump to Step 5; otherwise, execute Step 10.

Step 10: Output the updated n new shared QR codes of size $3q \times 3q$.

2.3.2. Steps of secret sharing for Scheme II

Steps 1–5: Follow the same steps of Scheme I. The grayscale mapping relationship of the two schemes is different, so the differences from Scheme I start at Step 6.

Step 6: Determine the set of sharing matrices M_g corresponding to the pixel blocks based on $G_{average}$, $g = 6 - \left\lceil \frac{G_{average}}{51} \right\rceil$. If $C_1(i, j) \oplus C_2(i, j) \oplus \cdots \oplus C_n(i, j) = 1$, order $g = g - 1$.

Steps 7–10: Follow the same steps of Scheme I. Finally, output the updated n new shared QR codes of size $3q \times 3q$.

According to the secret sharing algorithm, n shared QR codes with the same specification as the carrier QR code is generated. This is achieved by keeping the center area consistent with the carrier QR code and storing the secret level information in the order of the remaining eight pixels from top to bottom and left to right. This does not change the coding and decoding rules of the original QR code, as the public information on the original carrier QR code can be read out from the shared QR code by using standard QR code decoding tools.

2.4. Secret recovery algorithm

For secret recovery, the secret image can be recovered directly by using the visual characteristics of the human eye to perform the XOR operations for n shared QR codes. Since the Hamming distance of each shared QR codes is 4, the condition that a single set of shared QR codes cannot recover the secret image is satisfied. The direct decryption method for XOR operations is a lightweight decryption method that does not require computer involvement in computing, which greatly reduces the workload. And in the decryption process, the recovered image size is $q \times q$, so only $3q \times 3q$ times the position dissimilarity is needed to recover the secret image.

3. Proof of theorems

Theorem 1. Information about the secret image cannot be inferred from less than n shared QR codes.
Proof: The shared QR code is used for secret construction and secret recovery, so the security of shared QR codes determines the security of the whole system.

In the construction of the sharing matrix, at first, $n - 1$ vectors are created, i.e., $r_i (i = 1, 2, \ldots n - 1)$, and they have eight elements that are randomly generated and satisfy $H(r_i) = 4$. Then, we should compute r_n by $r_n = r_1 \oplus r_2 \oplus \cdots \oplus r_{n-1} \oplus s$ such that it satisfies $H(r_n) = 4$. At this point, a sharing matrix about s is generated $M = [r_1, r_2, \cdots, r_{n-1}, r_n]^T$. Therefore, a single shared QR code is unable to get any information about the secret image.

In recovery, the p shared QR codes performing XOR operations are equivalent to the p row vectors to obtain vector ξ. Then the remaining $n - p$ rows of vectors are subjected to the same operation to obtain vector ζ. The probability that vectors ξ and ζ belong to the set M_g of sharing matrices is the same, that is,

$$P(\xi \in M_g) = P(\zeta \in M_g) \tag{3.1}$$

In the schemes of this paper, the construction of the shared QR code is only related to the surrounding eight neighboring pixels. The pixels depend on the vector of the sharing matrix, so the security of the schemes introduced in this paper depend on the interrelationship between n vectors in the sharing matrix.

Therefore, the gray value range of the image cannot be judged; so, when there are less than n shared QR codes, the information of the secret image cannot be inferred.

Theorem 2. All vectors s find the vector $r_n = r_1 \oplus r_2 \oplus \cdots \oplus r_{n-1} \oplus s$ and satisfy $H(r_n) = 4$, and there exists a corresponding set M_g of sharing matrices for each gray level.

Proof: In the scheme, $n(n \geq 2)$ is the number of shared QR codes, and we can prove the truth of the theorem by using the converse method. We assume that an arbitrary r_n vector satisfies $H(r_n) \neq 4$, i.e., $r_n = r_1 \oplus r_2 \oplus \cdots \oplus r_{n-1} \oplus s$.

$$\begin{aligned} & H(r_n) \neq 4 \\ & \Leftrightarrow H(r_1 \oplus r_2 \oplus \cdots \oplus r_{n-1} \oplus s) \neq 4 \\ & \Leftrightarrow H(r_1) + H(r_2) + \cdots + H(r_{n-1}) + H(s) - 2k \neq 4 \\ & \Leftrightarrow H(r_1) + H(r_2) + \cdots + H(r_{n-1}) + even - even \neq 4 \\ & \Leftrightarrow H(r_1) + H(r_2) + \cdots + H(r_{n-1}) + even \neq 4 \\ & \Leftrightarrow 4 \times (n-1) + even \neq 4 \\ & \Leftrightarrow even \neq even \end{aligned} \tag{3.2}$$

By analysis, we find that the scheme is even number. When there are an odd number of 1's for the position component, the result of the XOR operation is "1", and when there are an even number of 1's, the result of the XOR operation is "0". That is, the number of 1's is the total number of 1's in all vectors minus $2k$, where k is the number of times to eliminate "1".

This is contradictory to natural common sense, so the hypothesis is not valid.

Theorem 3. When the image is recovered, the n shared QR codes are subjected to an XOR operation and the gray level of the secret image at that location is directly obtained.

Proof: For the secret sharing algorithm described in Section 2.3, we can determine the corresponding set of sharing matrices based on the gray mean values. In the case of the secret recovery described in Section 2.4, n shared QR codes are subjected to an XOR operation and the locus of the QR code affects the grayscale value of the heterogeneous operation result. If $C_1(i, j) \oplus C_2(i, j) \oplus \cdots \oplus C_n(i, j)$ is white, the value of g is not changed. If it is black, we make $g = g - 1$.The Hamming weight after the XOR operation is still the value obtained by the surrounding eight pixel points.

According to Section 2.2, this paper is divided into five levels. If $i = 1$, then $j = 0$ and, at this point, $s = 00000000$. We know that $r_n = r_1 \oplus r_2 \oplus \cdots \oplus r_{n-1} \oplus s$; therefore, $s = r_1 \oplus r_2 \oplus \cdots \oplus r_{n-1} \oplus r_n$. We can get $H(s) = 0$ from $s = 00000000$. If $i = 2$, then $j = 3$ and, at this point, $s = 00000011$. We can get $H(s) = 2$ if $i = 3$; then, $j = 15$ and, at this point, $s = 00001111$. We can get $H(s) = 4$ if $i = 4$; then, $j = 63$ and, at this point, $s = 00111111$. We can get $H(s) = 6$ if $i = 5$; then, $j = 255$ and, at this point, $s = 11111111$. We can get $H(s) = 8$.

That is,

$$H(s) = \begin{cases} 0 & if\, i = 1\ and\ j = 0 \quad and\, s = 00000000 \\ 2 & if\, i = 2\ and\ j = 3 \quad and\, s = 00000011 \\ 4 & if\, i = 3\ and\ j = 15 \quad and\, s = 00001111 \\ 6 & if\, i = 4\ and\ j = 63 \quad and\, s = 00111111 \\ 8 & if\, i = 5\ and\ j = 255\ and\, s = 11111111 \end{cases} \tag{3.3}$$

The five classes proposed in this paper exhibit a trend of grayscale transformation, which mainly originates from the Hamming distance after XOR operation. The gray transformation trend of each of the five grades proposed in this paper is mainly the change in Hamming distance; this allowed us to perform a comparison of different gray levels.

4. Experiment

This section will be divided into four parts to illustrate the effectiveness of the schemes. It contains the experimental results, presents an analytical comparison with other related schemes and provides verification of the homogeneity and robustness of the proposed schemes.

In this section, the grayscale mapping relationship already established in Examples 1 and 2 of Section 2.1 is used as an example to verify the effectiveness of the proposed schemes. Figure 5 shows the relevant test QR codes and secret images used for the experiments.

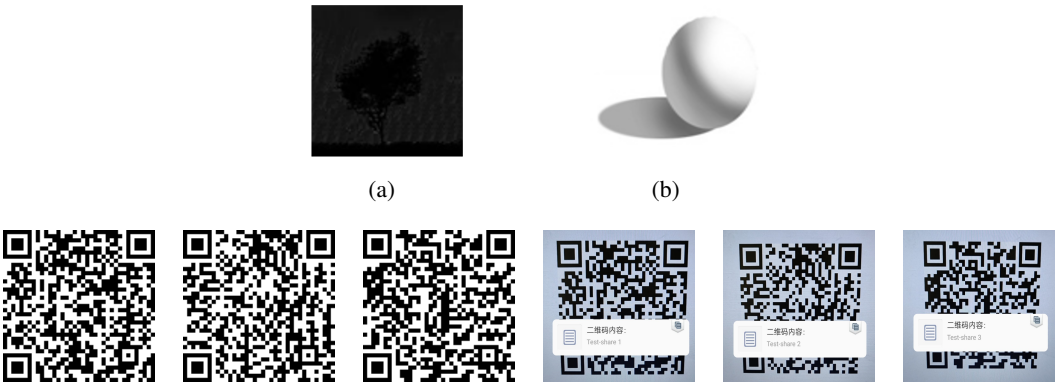


Figure 5. Experiment-related test plots: (a,b) secret images for Experiments 1 and 2; (c–e) carrier QR code image; (f–h) QR code decoding information.

From the secret sharing algorithm described in Section 2.3, we can use the carrier QR code image of size $q \times q$ shown in Figure 5 to generate a new shared QR code of size $3q \times 3q$, as shown in Figure 6, to verify the readability of the shared QR code.

The secret image recovered uses n shared QR codes to perform XOR operations. This involves performing XOR operations with the shared QR codes given as (a)–(c) in Figure 6 to recover m as shown in Figure 6. Similarly, we performed XOR operations with the shared QR codes given as (g)–(i) in Figure 6 to recover n in Figure 6.

The experimental results in Figure 6 show that Scheme I allows the shared QR codes to be read accurately. The secret image can be obtained when all of the shared QR codes undergo XOR operations and less than n shared QR codes cannot obtain any secret information.

The experimental results in Figure 7 show that Scheme II also allows the shared QR codes to be read accurately.

5. Performance analysis

5.1. Result comparison

In most visual cryptography schemes, the grayscale images are often converted to binary images through the use of halftone techniques, and then the traditional VCS techniques are used for secret sharing. Figure 8 presents a comparison with the traditional scheme [12]. When the grayscale distribution of the secret image is uniform, the recovered effect is very similar. However, when the grayscale

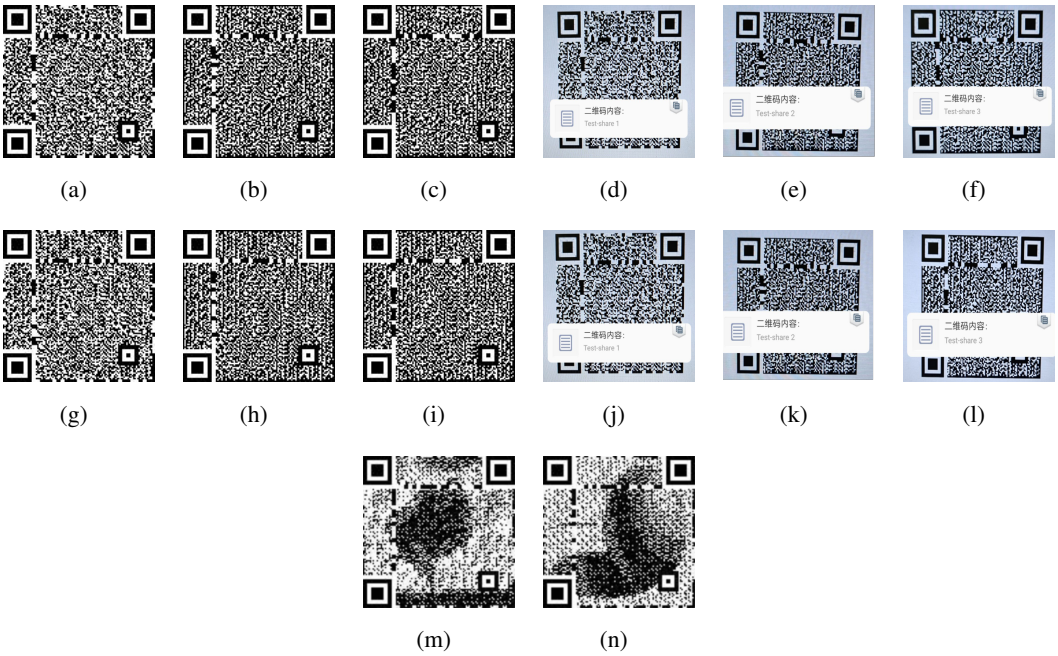


Figure 6. Resulting plots for Scheme I: (a–c) shared QR codes for Experiment 1; (d–f) shared QR code decoding information for Experiment 1; (g–i) shared QR codes for Experiment 2; (j–l) shared QR code decoding information for Experiment 2; (m,n) secret recovery for Experiments 1 and 2.

values of the secret image are concentrated in too dark or too bright areas, the recovered image from the conventional scheme will be distorted; thus, ours is better.

Both Schemes I and II strengthen the outline of the secret image. Scheme I mainly performs a series of enhancement operations on the secret image to increase the contrast. Scheme II mainly divides the interval according to the number of pixels, and the obtained grayscale map will be more in line with the characteristics of the secret image itself.

A qualitative analysis of the image recovery effect is summarized in Table 4; it can be seen that the image recovered by the conventional scheme will be distorted, and that the secret images recovered by using the proposed schemes have a better recovery effect. In Figure 8, a and d are the recovery effects of the traditional scheme for Experiments 1 and 2, b and e are the recovery effects of the proposed Scheme I for Experiments 1 and 2 and c and f are the recovery effects of the proposed Scheme II for Experiments 1 and 2.

Table 4. Similarity comparison.

	Experiment 1			Experiment 2		
	Traditional Scheme	Scheme I	Scheme II	Traditional Scheme	Scheme I	Scheme II
AHA	0.48	0.62	0.77	0.67	0.77	0.74
DHA	0.47	0.55	0.59	0.51	0.56	0.53
PHA	0.51	0.61	0.72	0.68	0.74	0.75

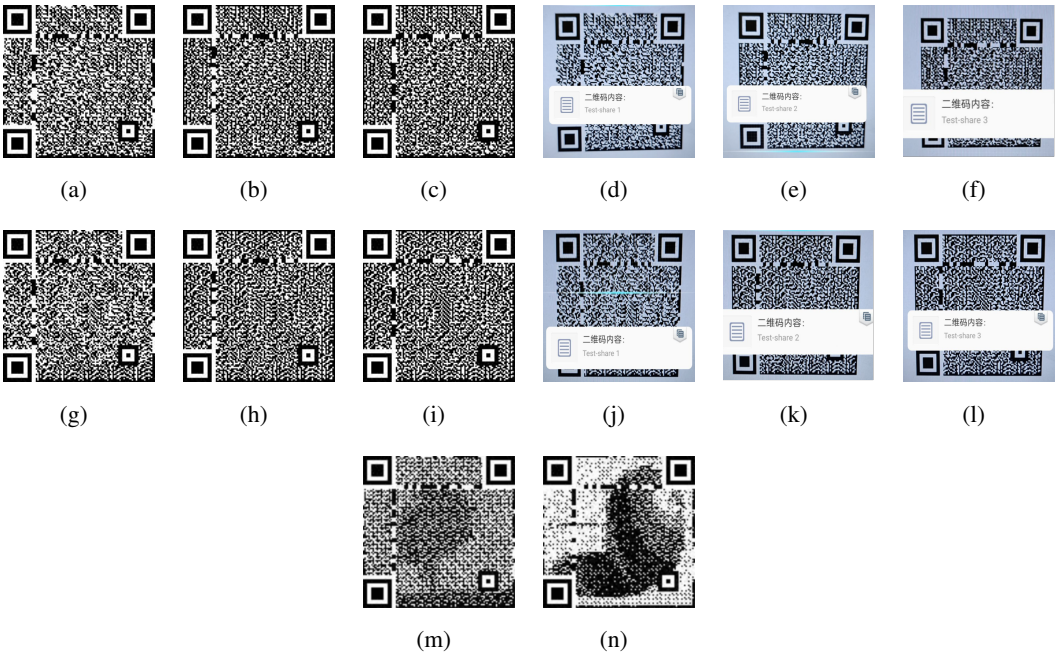


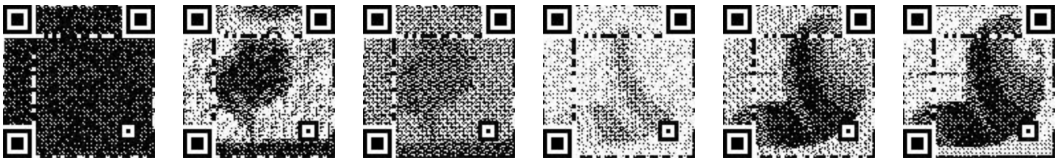
Figure 7. Resulting plots for Scheme II: (a–c) shared QR codes for Experiment 1; (d–f) shared QR code decoding information for Experiment 1; (g–i) shared QR codes for Experiment 2; (j–l) shared QR code decoding information for Experiment 2; (m,n) secret recovery for Experiments 1 and 2.

AHA is the average hash algorithm similarity. First find the gray average of the image. The pixel is binarized according to the average value. If it is larger than the average value, it is set to 1, and if it is smaller than the average value, it is set to 0. Every 8 bits is a hexadecimal value, which is converted to a string, and the corresponding hash value is generated; DHA is the difference hash algorithm similarity. First, the difference of gray image is calculated. The positive number is set as 1, and the negative number is set as 0. Every 8 bits is a hexadecimal value, which is converted to a string, and the corresponding hash value is generated; PHA is the perceptual hash algorithm similarity. Firstly, the gray image is subjected to discrete cosine transform (DCT), and the low frequency component is taken to calculate its average value.The pixel is binarized according to the average value. If it is larger than the average value, it is set to 1, and if it is smaller than the average value, it is set to 0. Every 8 bits is a hexadecimal value, which is converted to a string, and the corresponding hash value is generated.

In this paper, we present the above algorithm to compare the original image to the recovered image and hash value, where the same is represented as 1, a difference is represented as 0 and the number of same values relative to the total is the similarity. Through Table 4, we can find that the Schemes I and II proposed in this paper are better than the traditional algorithm in terms of this similarity algorithm, and that they have better practicality.

5.2. Security analysis

From the process of sharing matrix set generation, we can see that the vector s is a binary encoding of j. However, in the traditional scheme, the valid bits of the vector s are only the last four bits. The



(a) (b) (c) (d) (e) (f)

Figure 8. Comparison of experimental effects of programs: (a–c) traditional scheme and Schemes I and II results for Experiment 1; (d–f) traditional scheme and Schemes I and II results for Experiment 2.

distribution of "1" in vector r_n is not uniform, which not only means space consumption, but it also makes r_n vulnerable to illegal attacks.

The new construction method proposed in this paper makes the "1" as uniformly distributed as possible. Since the vector s will directly affect the value of r_n in the sharing matrix, the uniformity of the vector in each scheme depends on the distribution of the vector s. Figure 9 shows the frequency distribution of the vector s.

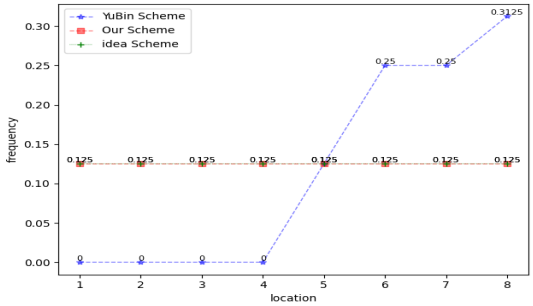


Figure 9. Frequency distribution of the vector s.

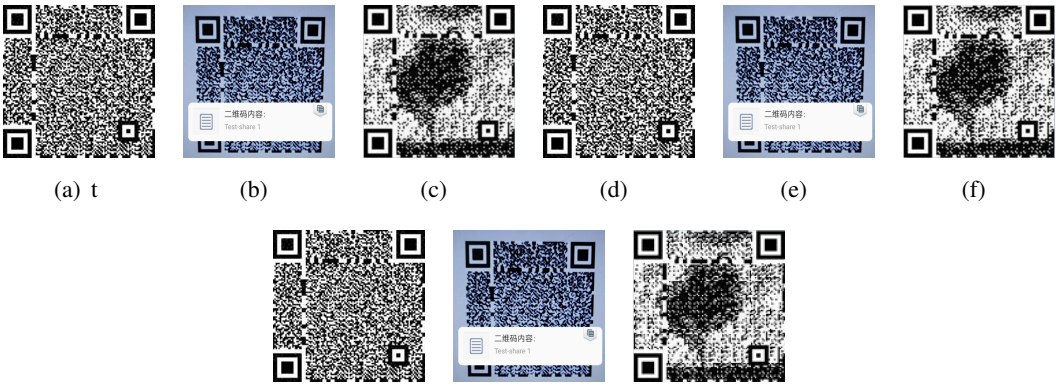
The blue and red lines respectively represent the traditional scheme probability and ours and "+" represents the distribution probability of the vector s in the ideal state of the vector. From the figure, we can know that the vector s from each of our schemes is fully consistent with the distribution in the ideal state. Our schemes make the vectors s and r_n more secure.

5.3. Robustness verification

In practical applications, shared QR codes are subject to various kinds of interference during transmission and storage. In this study, we verified the robustness of three common interference methods. Two schemes have been proposed in this paper; they process secret images differently, but the algorithms for embedding QR codes are the same. Therefore, the following three verification methods were verified only for Scheme I.

1) Regarding image storage, it is usually used to reduce the storage space of the shared QR codes. To test that the scheme is still effective after image compression, we constructed Figure 10 to show the test results for 10, 30 and 50% with lossy compression of the images.

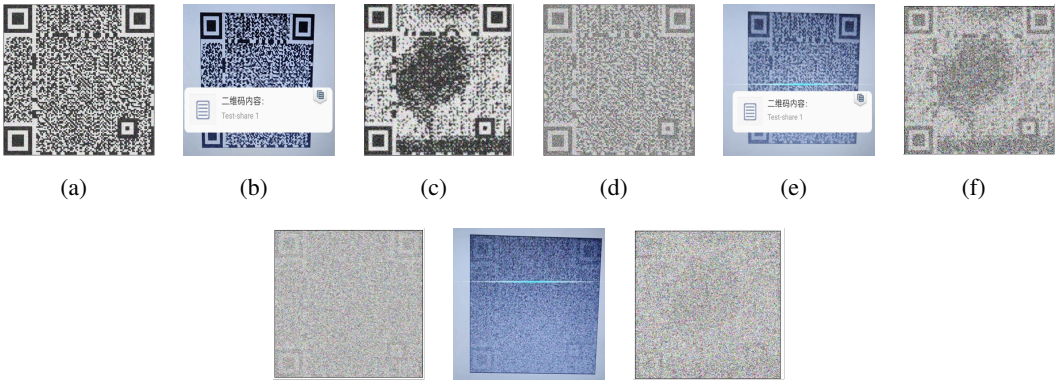
The results show that the QR codes with impaired quality are still readable, and that the secret image can still be recovered after performing XOR operations.



(a) t (b) (c) (d) (e) (f)

(g) (h) (i)

Figure 10. Compression test results: (a–c) shared QR code, decoding information and secret recovery at a 10% compression ratio, respectively; (d–f) respective results at a 30% compression ratio; (g–i) respective results at a 50% compression ratio.



(a) (b) (c) (d) (e) (f)

(g) (h) (i)

Figure 11. Results of Gaussion noise addition tests: (a–c) shared QR code, decoding information and secret recovery at $\mu = 0$ and $\delta^2 = 0.1$; (d–f) respective results at $\mu = 0$ and $\delta^2 = 1$; (g–i) respective results at a $\mu = 0$ and $\delta^2 = 10$; (j–l) respective results at a $\mu = 0$ and $\delta^2 = 10$.

2) During the transmission of the image, the shared QR code may face interference from noise or unintentionally lose some pixel information. To test the resistance of our scheme to noise interference, we used the Python platform to add Gaussian noise to the shared QR codes. As can be seen in Figure 11, the results show that, when the Gaussian noise intensity is within a certain range, the shared QR code can be read and the secret image can be recovered. However, when the variance of the Gaussian noise is large, neither the shared QR code nor the secret image can be recovered.

Adding channel transmission attacks, such as multiplicative noise and salt-and-pepper noise, can also lead to recovery of the secret image, as shown in Figure 12.

3) When the mobile device scans the shared QR code during the image scanning process, its angle may change arbitrarily. In this study, we applied 45° rotation tests to the shared image using Adobe Photoshop. Figure 13 shows that the rotated shared QR code can still be read, and that the secret image information can be recovered.

(a) (b) (c) (d) (e) (f)

Figure 12. Results of noise addition tests: (a–c) shared QR code, decoding information and secret recovery under the condition of added multiplicative noise; (d–f) under the condition of added salt-and-pepper noise.

(a) (b) (c)

Figure 13. Rotation test results: (a–c) shared QR code, decoding information and secret recovery at 45° rotation.

6. Conclusions

This paper introduced an adaptive visual cryptography method based on QR codes. We consider the secret image's own characteristics and use two schemes to adjust the secret image adaptively. The recovered image is distorted even when the grayscale value of the secret image is too dark or too bright. This method is suitable for the scenarios in which there is a more complicated secret image; additionally, it offers good security and practicality. The secret image can be recovered quickly. In addition, the generation algorithm for the shared matrix is improved. The experimental results show that the proposed scheme has high feasibility and robustness. The proposed schemes can be applied to the sharing scheme for visual cryptography, not just the QR code. In the future, our research will focus on the use of QR codes to enable multiple sharing of text secrets and image secrets at the same time. How to improve the schemes proposed in this paper to make the recovered secret image clearer is also one of the research directions.

Acknowledgments

The authors thank the anonymous reviewers for their valuable comments. This work was supported by the National Natural Science Foundation of China (No. 62102309); Shaanxi Provincial Department of Science and Technology Youth Project (No. 2021JQ-575 and No. 2021JQ-57); Shaanxi Provincial Department of Education Project (No. 19JK0526) and Yulin Science and Technology Bureau Project (No. 2016-24-4 and No. 2019-173).

Conflict of interest

The authors declare that they have no conflicts of interest.

References

1. Jtc1/Sc, Information technology—Automatic identification and data capture techniques—QR Code 2005 bar code symbology specification, 2006.
2. F. Pichler, *Advances in Cryptology—EUROCRYPT' 85: Proceedings of a Workshop on the Theory and Application of Cryptographic Techniques Linz, Austria, April 1985*, Lecture Notes in Computer Science, 1986. https://doi.org/10.1007/3-540-39805-8
3. X. Liu, S. Wang, J. Sang, W. Zhang, A novel lossless recovery algorithm for basic matrix-based VSS, *Multimedia Tools Appl.*, **77** (2018), 16461–16476. https://doi.org/10.1007/s11042-017-5215-7
4. P. Li, P. Ma, X. Su, F. Liu, Multi-threshold image secret sharing scheme, *Acta Electronica Sin.*, **40** (2012), 518–524. https://doi.org/10.3969/j.issn.0372-2112.2012.03.018
5. R. Sun, Z. Fu, X. Li, B. Yu, A pixel non extended visual cryptography scheme based on two-level threshold, *J. Cryptogr.*, **4** (2021). https://doi.org/10.13868/j.cnki.jcr.000459
6. M. E. Hodeish, V. T. Humbe, An optimized halftone visual cryptography scheme using error diffusion, Multimedia tools and applications, **77** (2018), 24937–24953. https://doi.org/10.1007/s11042-018-5724-z
7. M. E. V. Melgar, M. C. Q. Farias, A (2,2) XOR-Based visual cryptography scheme without pixel expansion, *J. Visual Commun. Image Represent.*, **63** (2019), 102592. https://doi.org/10.1016/j.jvcir.2019.102592
8. P. Tuyls, H. D. L. Hollmann, J. H. Van Lint, L. Tolhuizen, XOR-based visual cryptography schemes, *Des. Codes Cryptogr.*, **37** (2005), 169–186. https://doi.org/10.1007/s10623-004-3816-4
9. J. Weir, W. Q. Yan, Authenticating visual cryptography shares using 2D barcodes, in *International Conference on Digital-forensics & Watermarking*, **7128** (2011), 196–210. https://doi.org/10.1007/978-3-642-32205-1_17
10. Y. Liu, Z. Fu, Y. Wang, Two level information management scheme based on visual password and QR code, *Appl. Res. Comput.*, **33** (2016), 3460–3463.
11. Y. Chow, W. Susilo, G. Yang, J. G. Phillips, I. Pranata, A. M. Barmawi, Exploiting the error correction mechanism in QR codes for secret sharing, in *Information Security and Privacy*, Springer, Cham, (2016), 409–425. https://doi.org/10.1007/978-3-319-40253-6_25
12. B. Yu, S. Liu, Z. Fu, Design of gray visual cryptography based on fast response code, *J. Comput. Aided Des. Graphics*, **32** (2020), 635–642.
13. H. Fu, S. Zhou, L. Liu, N. J. Mitra, Animated construction of line drawings, *ACM Trans. Graphics*, **30** (2011), 1–10. https://doi.org/10.1145/2024156.2024167
14. Y. Cheng, Z. Fu, B. Yu, G. Shen, A new two-level QR code with visual cryptography scheme, *Multimedia Tools Appl.*, **77** (2018), 20629–20649. https://doi.org/10.1007/s11042-017-5465-4
15. Z. Fu, Y. Cheng, S. Liu, B. Yu, A new two-level information protection scheme based on visual cryptography and QR code with multiple decryptions, *Measurement*, **141** (2019), 267–276. https://doi.org/10.1016/j.measurement.2019.03.080
16. B. Yu, Z. Fu, S. Liu, A novel three-layer QR code based on secret sharing scheme and liner code, *Secur. Commun. Netw.*, **5** (2019), 1–13. https://doi.org/10.1155/2019/7937816

17. S. Liu, Z. Fu, B. Yu, Rich QR codes with three-layer information using Hamming code, *IEEE Access*, **7** (2019), 78640–78651. https://doi.org/10.1109/access.2019.2922259

18. G. Zou, T. Li, G. Li, X. Peng, G. Fu, A visual detection method of tile surface defects based on spatial-frequency domain image enhancement and region growing, in *2019 Chinese Automation Congress (CAC)*, 2019. https://doi.org/10.1109/cac48633.2019.8997215

AIMS Press