Hindawi
Security and Communication Networks
Volume 2019, Article ID 7937816, 13 pages
https://doi.org/10.1155/2019/7937816

Research Article

A Novel Three-Layer QR Code Based on Secret Sharing Scheme and Liner Code

Bin Yu, Zhengxin Fu, and Sijia Liu

College of Computer, Information Engineering University, Zhengzhou 450004, China

Correspondence should be addressed to Zhengxin Fu; fzx2515@163.com

Received 30 July 2019; Accepted 6 September 2019; Published 11 November 2019

Academic Editor: Angel M. Del Rey

Quick Response (QR) code, a machine-readable symbol, is widely employed in all walks of life due to its large information capacity, strong error correction ability, and fast reading speed. However, anyone with a standard decoder could obtain stored information. In this paper, utilizing the characteristics of the Hamming code, wet paper code, and the recognition mechanism of the QR code, we introduce a high-capacity QR code with three-layer information to protect the sensitive information. In the proposed scheme, we utilize the XOR-based secret-sharing algorithm to embed the second-layer information on the column vector of the constructed random matrix block. Then, without affecting the embedding result of the second layer information, the matrix block elements are reused again, and the Hamming code is constructed with the column vector. Based on the error correction mechanism of the Hamming code, the third layer of information is embedded on the column vector and encoded by wet paper coding to realize the blind extraction. Finally, based on the recognition mechanism of the QR code, the random matrix block containing the secret information is fused with the carrier QR code, and the public information of the carrier QR code is used as the first-layer information. Compared with other schemes, the proposed scheme has the advantages of high information payload, low computational complexity, and strong robustness.

1. Introduction

Advancing and expanding in the field of machine vision, QR code [1] breaks the constraints of the traditional industry model and is widely used in the areas which require automated information management with its advantage of its online-to-offline information docking method. However, the QR code data easily can be decoded and retrieved via an automatic decoder system; the lack of security of the QR code with secret data creates problems for its real-world application. Considering the security problems, the researchers carried out a series of work.

In the initial stages of research, some scholars utilized traditional cryptography to protect the secret information in the QR code. Krishna and Dugar [2] proposed a product anticounterfeiting scheme using the packet encryption algorithm DES, which encoded the ciphertext together with the plaintext information into a two-level QR code. Wang et al. [3] proposed a nonlinear optical encryption scheme based on phase-truncated Fresnel transform, where secret QR code was encrypted into pseudorandom noise image under the control of two private keys, while the scheme needed special optical instruments during decryption, which was greatly reduced the practical application value.

Although the aforementioned schemes can effectively protect the security of secret data, the payload of the QR code is limited and the content of the QR code is meaningless, which cannot meet the certain scene needs. In many fields, the users only want to disclose a part of their own information, while they hope to protect the other part in the same QR code. For example, after receiving the express delivery, people often drop the express delivery slip, which causes the leakage of personal secret data. In order to protect the sensitivity while facilitating the delivery by courier, the recipient's personnel sensitive information such as the name, phone number, etc. should only be accessible to the courier instead of anyone. Therefore, the two-level QR code comes into being, in which the public information could be

obtained by any standard QR code decoding device, while the extraction of the private information required a legitimate key.

Using the pattern recognition technology, Teraura and Sakurai [4] designed a two-level QR code that replaced the module of the QR code by 3×3 or 5×5 submodule identification units to implement the embedding of private information. In order to improve the accuracy of the extraction, the Hamming code was used to correct errors. Tkachenko et al. [5] designed the two-level QR code based on machine vision and selected a unit that replaced the black module of the QR code from several pattern recognition units according to the secret scrambling sequence to achieve two-level storage of information. Based on the error correction mechanism of QR code, Chiang et al. [6] used wet paper code to embed secret information into the carrier image to achieve blind extraction of secret information. Lin and Chen [7] improved the algorithm to make the upper limit of the embedded bits reach the maximum data capacity of the QR code. Lin [8] proposed a (n, n) secret sharing scheme where n bit streams were obtained by the random number generation algorithm and hash function and embedded into the carrier image by wet paper code to form n two-level QR codes. Also some scholars shared the secret into several parts based on visual cryptography [9–11] and embedded the subsecrets into QR code to generate the two-level QR code, while there was distortion in the recovery results and the payload was really poor.

Despite the above schemes implementing the design of two-level QR code approximately, most existing solutions do not fully consider the information embedding efficiency, which leads to a low secret payload. Liu et al. [12] utilized the Hamming code to resume the carrier pixels, which promoted the efficiency of the pixels. However, it is limited by the error correction ability of the QR code that made some pixels not able to be used to construct the Hamming codes. What's more, in the extraction process, the location information which embeds the third level information is required, which brings security threats.

To overcome the drawback, this paper reuses Hamming code and wet paper code to design a three-layer QR code with high-efficiency embedding rate based on the recognition mechanism of the QR code. The pattern recognition technology of the QR code is employed to design information storage structure, which aims to full-use all the carrier pixels and improve the robustness of the scheme. In addition, the wet paper code is applied to achieve a blind extraction of the secrets to improve the security of the scheme. Finally, the experimental results and comparisons demonstrate the effectiveness and advantage of our work.

The contributions of this paper are as follows: (1) Three-layer information storage. Different from other two-level QR code, the proposed scheme can achieve three-layer storage of information, which makes the scheme have a higher secret payload and a wider application foreground. (2) High embedding efficiency. Based on the error correction principle of Hamming Code, the carrier pixels are reused to improve the efficiency of information embedding and the payload of secret bits. One pixel may transmit extra p bits at most. (3) Strong robustness. This paper embeds the secret information based on the QR code recognition mechanism without occupying the error correction codewords of the QR code, which explains that the strong robustness resists some common geometric attacks such as compression, rotation, and deformation. (4) Blind extraction of the embedded information. The proposed scheme can achieve a blind extraction by matrix multiplication based on the wet paper code.

The remainder of this paper is organized as follows. Section 2 introduces some preliminaries concerning our study. The proposed scheme is described in Section 3. The security of the proposed scheme is discussed in Section 4. Section 5 provides the experiments and analysis to illustrate the feasibility of this work and how this study improves on previous work. Finally, conclusions are given in Section 6.

2. Preliminaries

2.1. Method of [12]. Hamming code [13] is invented by Richard Wesley Hamming in 1950. Hamming code is a typical complete code and is a high-efficiency code that corrects a single error.

Taking (7, 4) Hamming code for example, we explain how to embed and extract 3 bits of messages into 7 pixels. Let H be the parity check matrix of the (7, 4) Hamming code whose columns are in the natural order of increasing binary numbers.

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}. \quad (1)$$

Given a 7-bit code word $x = [1\ 0\ 0\ 1\ 0\ 0\ 0]$ and a 3-bit secret message $m = [1\ 1\ 0]$, calculate

$$H \cdot x^T \oplus m = [1\ 0\ 1]^T \oplus [1\ 1\ 0]^T = [0\ 1\ 1]^T. \quad (2)$$

The result obtained according to equation (2) is a binary representation of three, that is, the third column of the check matrix H. The information is embedded by changing the third bit of x. When the secret information is extracted, only calculate

$$H \cdot x'^T = [1\ 1\ 0]^T = m^T. \quad (3)$$

Liu et al. [12] utilized the above to embed extra information bits based on the error correction capability of the QR code. The detailed algorithm is shown in Algorithm 1.

As despite in the Algorithm 1, only part pixels in the carrier QR code are reused to transmit extra pixels. What's more, in the decryption procedure, the matrix index *seed* is also required, which contains the information of the location of the third-layer information.

2.2. Wet Paper Code [14]. Wet paper code is realized by random binary linear code, which can be used to construct a steganographic mechanism with arbitrarily selected channels. The basic principle can be summarized as follows. Let carrier data X be a collection of n elements as

Input: Carrier QR code images $C_1, C_2, \ldots, C_2{}^p$ of size $m \times n$, the second layer information v, The third layer information s.
Output: *shares* $T_1, T_2, \ldots, T_2{}^p$ with size of $m \times n$, and matrix index *seed*.
Step 1: Let $T_k = C_k$ $(k = 1, 2, \ldots, 2^p)$ and denote i, j as the location coordinate of the unprocessed pixels in carrier QR codes.
Step 2: Calculate $V(i, j) = C_1(i, j) \oplus C_2(i, j) \oplus \cdots \oplus C_{2^p}(i, j)$.
Step 3: If $V(i, j) = v'$ (v' is an unprocessed element in v), *seed* $(i, j) = 0$ and no extra secret bits are transmitted. Else, treat a set of unprocessed bits in s as secret message and utilize the error correction principle of the Hamming code to decide the pixel of which QR code needs to be flipped. If it is within the error correction capability of the QR code, flip it and let *seed* $(i, j) = 1$. Else go to *Step 4*.
Step 4: Choose a pixel in the QR code which keep the error correction capability to be flipped, *seed* $(i, j) = 0$.
Step 5: Run *Step 2* to *Step 4* until all the elements in s is processed. If there is still element in v unprocessed, run *Step 2* and *Step 4*. Else, the algorithm ends

Algorithm 1: Sharing Algorithm in [12].

$X = \{x_i, i = 1, 2, \ldots, n\}$, $x_i \in J$, J is the value set of x_i. As for an 8-bit grayscale image, $J = \{0, 1, \ldots, 255\}$ and n is the number of pixels of the X. The sender uses a certain rule to select k changeable pixels (dry pixels) to carry secret information. In the process of embedding, x_j may be modified to y_j, and other n-k pixels (wet pixels) cannot be modified during the embedding process.

The least significant bit before and after the embedding process is represented by a vector form. Let $b = \{\mathrm{LSB}(x_i), i = 1, 2, \ldots, n\}$ and $b' = \{\mathrm{LSB}(y_i), i = 1, 2, \ldots, n\}$. It is assumed that the secret information to be embedded in the secret is a binary bit stream $m = \{m_1, m_2, \ldots, m_q\}$ of length q, and the sender uses the key to generate a pseudorandom binary matrix $D_{q\times n}$ and b' must satisfy

$$D_{q\times n} \times b'_{n\times 1} = m_{q\times 1}. \tag{4}$$

Let $v_{n\times 1}$ be a modified vector, then $v_{n\times 1} = b_{n\times 1} \oplus b'_{n\times 1}$ where $\oplus$ represents the modulo 2 arithmetic. Then, equation (4) can be converted to

$$D_{q\times n} \times v_{n\times 1} = m_{q\times 1} \oplus D_{q\times n} \times b_{n\times 1}. \tag{5}$$

For the sender, m, D, H, and b are all available, so they can calculate $m'_{q\times 1}$ by $m'_{q\times 1} = m_{q\times 1} \oplus D_{q\times n} \times b_{n\times 1}$. Since there are unchangeable elements in b, which means the modified vector is 0 at the corresponding position, the corresponding column vector in D has no effect on the result of equation (5). Delete the n-k column vectors in D to obtain the submatrices $H_{q\times k}$; then, Equation (5) can be transformed into

$$H_{q\times k} \times v_{k\times 1} = m'_{q\times 1}. \tag{6}$$

During the procedure of embedding, the sender solves the modified vector according to equation (6) and then modifies the carrier data. The recipient only needs to use equation (4) to extract secret information.

2.3. QR Code. The international standard for QR codes [1] defines a total of 40 symbol versions and 4 error correction levels, presented by *V*-*E*. *V* (1 to 40) is the version number, which determines the size of a QR code. *E* (*L*, *M*, *Q*, *H*) denotes four error correction levels, corresponding to four error correction capacities (7%, 15%, 25%, 30%), respectively. Figure 1 shows the structure of version 7.

When the QR code is decoded, the standard QR code decoder can recognize the QR code module based on the key pixels of the module [15], of which the method is called module recognition based on key pixels. As shown in Figure 2, it refers to determining the module recognition result according to the color of the middle region of each module. If the middle area of a module is dark, the module is a dark module. Conversely, it is a light module.

Based on the principle, this paper designs the 3×3 information storage structure of the module recognition unit (shown in Figure 3) to carry secret bits. And because of that, the functional region is used to locate and geometric correct the QR code, where no bits are embedded.

3. The Proposed Scheme

The motivation of our scheme is to design a high-capacity QR code with three-layer information to protect the sensitive information and overcome the drawbacks of [12], where the Hamming code is used to resume the carrier pixels (we adopt part of the methods in [12]) and the wet paper code is utilized to achieve the blind extraction of the third layer information. We choose the privacy QR code as the second-layer information whose version, error correction level, and module size are same as those of the carrier QR code. The overview and illustration of the proposed scheme are provided in Figure 4.

As despite in Figure 4, the scheme mainly includes two parts: secret embedding and secret recovery and extraction.

In the secret embedding phase, the secret distributor constructs a random matrix block with size of $2^p \times (m \times n)$, of which the second layer information is embedded on the column vector by using the XOR-based secret sharing algorithm. During the process of embedding the second-layer information, the pixels of a certain position on the random matrix block column vector are inverted. The positions of the flipped pixels are used as the index to embed the third-layer information utilizing the Hamming code and wet paper code without affecting the embedding result of the second layer information. Finally, combing the information storage structure of the module recognition unit, each row of the random matrix carrying the secret bits is fused with a single carrier QR code to generate a three-layer QR code.

In the secret recovery and extraction phase, the secret compositor obtains the second-layer information by

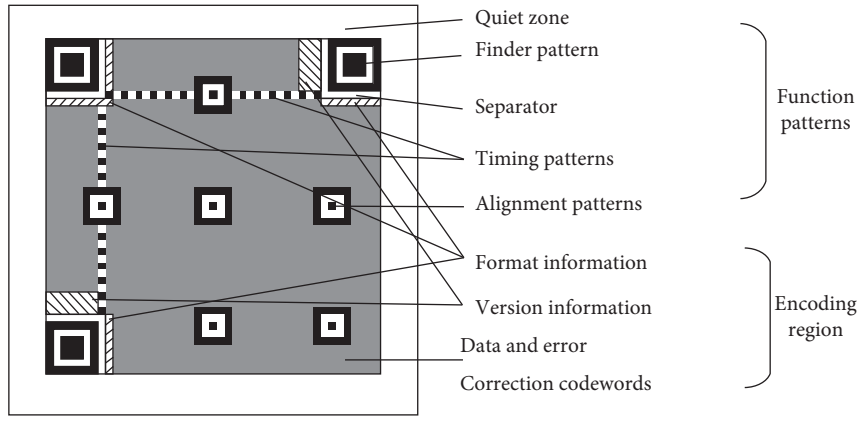


Figure 1: Symbol structure of version 7.

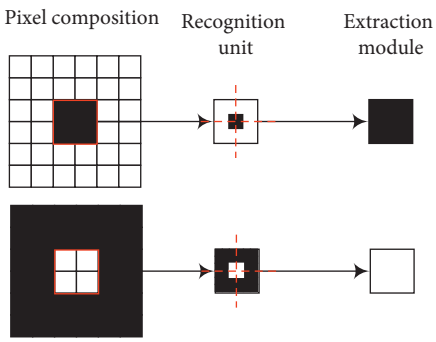
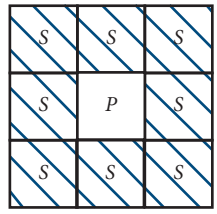


Figure 2: Module recognition based on key pixels.



S represents the secret information
P represents the public information

Figure 3: Information storage structure.

XOR-ing all the shares. Then, the third-layer information is extracted by matrix multiplication operation.

3.1. Secret Sharing and Embedding Procedure. It is assumed that the information stored in the carrier QR code image C_i ($i = 1, 2, \ldots, 2^p$) is different and can be decoded by a normal standard QR code decoder. The second-layer information is the privacy QR code S_v, and the third-layer information is s.

3.1.1. Preliminary Phase. The proposed scheme utilizes Hamming code and wet paper code to realize the embedding of the third-layer information. Therefore, the check matrix of the Hamming code needs to be shared between the secret distributor and the secret compositor. And because the scheme constructs a Hamming code of length $2^p - 1$ as a carrier of the third-layer information, it is necessary to agree on the parity check matrix $H_{p\times(2^p-1)}$ of the $(2^p - 1, 2^p - p - 1)$ Hamming code in advance.

In the wet paper encoding process, the "dry" and "wet" elements need to be marked, so it is necessary to set the matrix *dry_index* of size 1 row and $p \times m \times n$ columns, whose initial state is a zero matrix.

3.1.2. Sharing and Embedding Phase. The flow chart of the information sharing and embedding algorithm is shown in Figure 5. The detailed algorithm is provided as Algorithm 2.

3.2. Secret Recovery and Extraction Procedure. In this paper, the shares held by all participants are required to perform a superimposition XOR operation to decrypt the second layer information and then extract the third-layer information through matrix multiplication operations. Specific steps of the recovery of the second-layer information are provided in Algorithm 3, and the extraction of the third-layer information is shown in Algorithm 4.

4. Security Proof

Theorem 1. *The probability of success to infer the second-layer and the third-layer information based on an individual share will be bounded by* $1/2^{m\times n}$ *and* $1/C_{m\times n}^{l_2} \times ((2^p - 1)! \times 2^{n-2})^{l_2}$, *respectively.*

Proof. When the adversary has and only has an individual share S_t, it is possible to adopt the opponent a brute force strategy akin to a dictionary attack. According to the known share, it is possible to find that each module of the QR code is replaced by the submodule with size of $3m \times 3n$ and the surrounding eight bits are the same, so the attacker can extract $m \times n$ useful information from the available share.

Let $S_1 \oplus S_2 \oplus \cdots \oplus S_{i-1} \oplus S_{i+1} \oplus \cdots \oplus S_n = A$, since $S_1 \oplus S_2 \oplus \cdots \oplus S_n = S$. Thus, for each pixel in S_t, the $S_t(i, j) = S(i, j) \oplus A(i, j)$ exists, which means one secret pixel can be decoded correctly with a probability of 0.5 based on

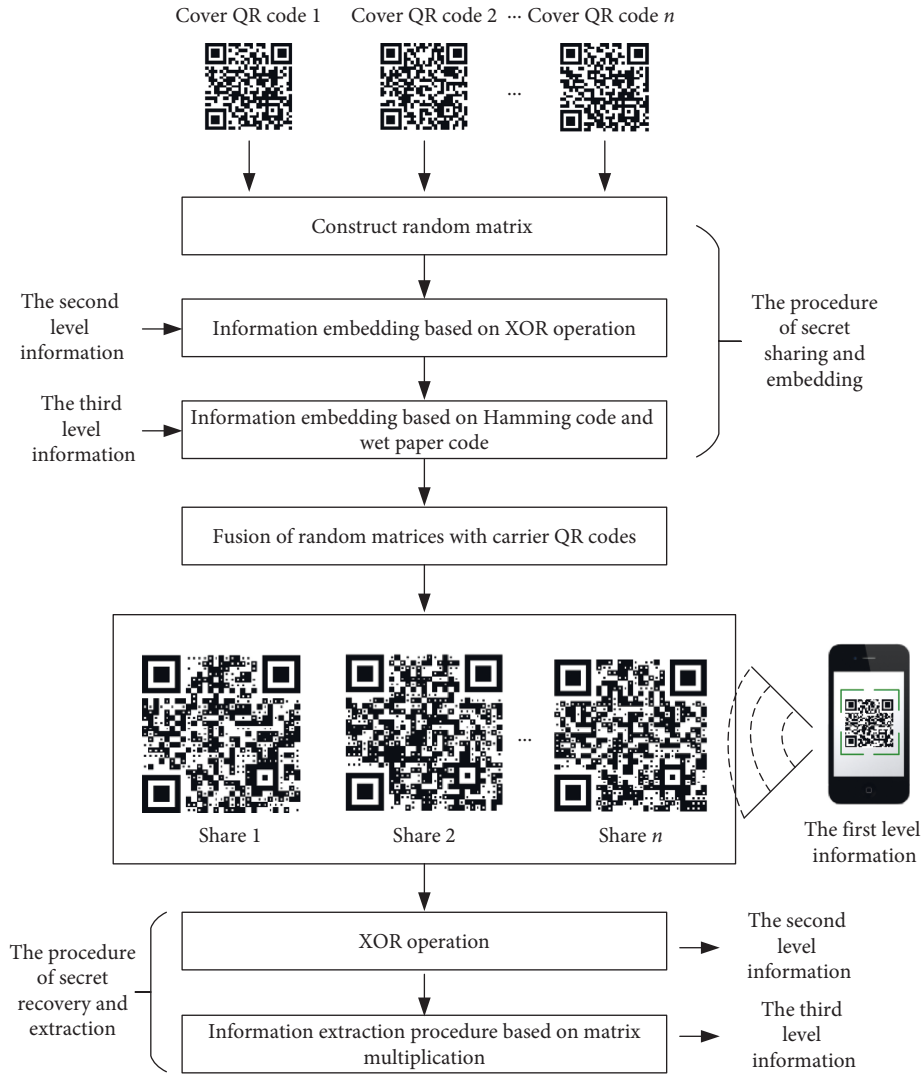


Figure 4: Illustration of the proposed scheme.

a corresponding pixel in the available share. Therefore, the probability of success to infer the second layer information will be bounded by $1/2^{m\times n}$.

In light of the fact that it is possible for the adversary to obtain the length of the third-layer information $l_2 = \text{length}(s)$ and the length of the Hamming code, which is $2^p - 1$, the adversary can infer the companion matrix and one corresponding Hamming code by $1/(2^p - 1)!$ and $1/2^{n-2}$, respectively. Meanwhile, it is difficult to obtain the embedding position, which leads to a $1/C_{m\times n}^{l_2}$ probability to accurately guess the positions. Thus, the probability of success for this attack of the third-layer information will be bounded by $1/C_{m\times n}^{l_2} \times ((2^p - 1)! \times 2^{n-2})^{l_2}$.

End.

Theorem 2. *The probability of success to infer the second-layer and the third-layer information based on $n-1$ shares will be bounded by $1/2^{m\times n}$ and $\{(1/[n \times C_{m\times n}^{l_2} \times (2^p - 1)!]) + (n-1)/[n \times C_{m\times n}^{l_2} \times (2^p - 1)! \times 2^{l_2}]\}$, respectively.*

Proof. It is conceivable that $n-1$ participants may collude and combine the information from their shares together in an attempt to find S, which is called collusion attack. Let $S_1 \oplus S_2 \oplus \cdots \oplus S_{n-1} = B$. Thus, $S_n(i, j) = S(i, j) \oplus B(i, j)$ exists, which is similar to the analysis in Theorem 1. As above, the probability to infer the second layer information will be bounded by $1/2^{m\times n}$.

Because the adversary has $n-1$ shares, there is at most one share that cannot participate in reconstructing the Hamming code. The probability that $n-1$ shares can construct the Hamming code accurately is $1/n$. In this case, the adversary can reconstruct the Hamming code with a probability of 1, so the third layer information can be obtained by $1/(n \times C_{m\times n}^{l_2} \times (2^p - 1)!)$. The probability that only a share does not participate in reconstructing the Hamming codes is $1 - 1/n$. In this case, the adversary can reconstruct the Hamming code with a probability of 0.5, so the third layer information can be obtained by $(n-1)/(n \times C_{m\times n}^{l_2} \times (2^p - 1)! \times 2^{l_2})$. Therefore, the total probability of decoding

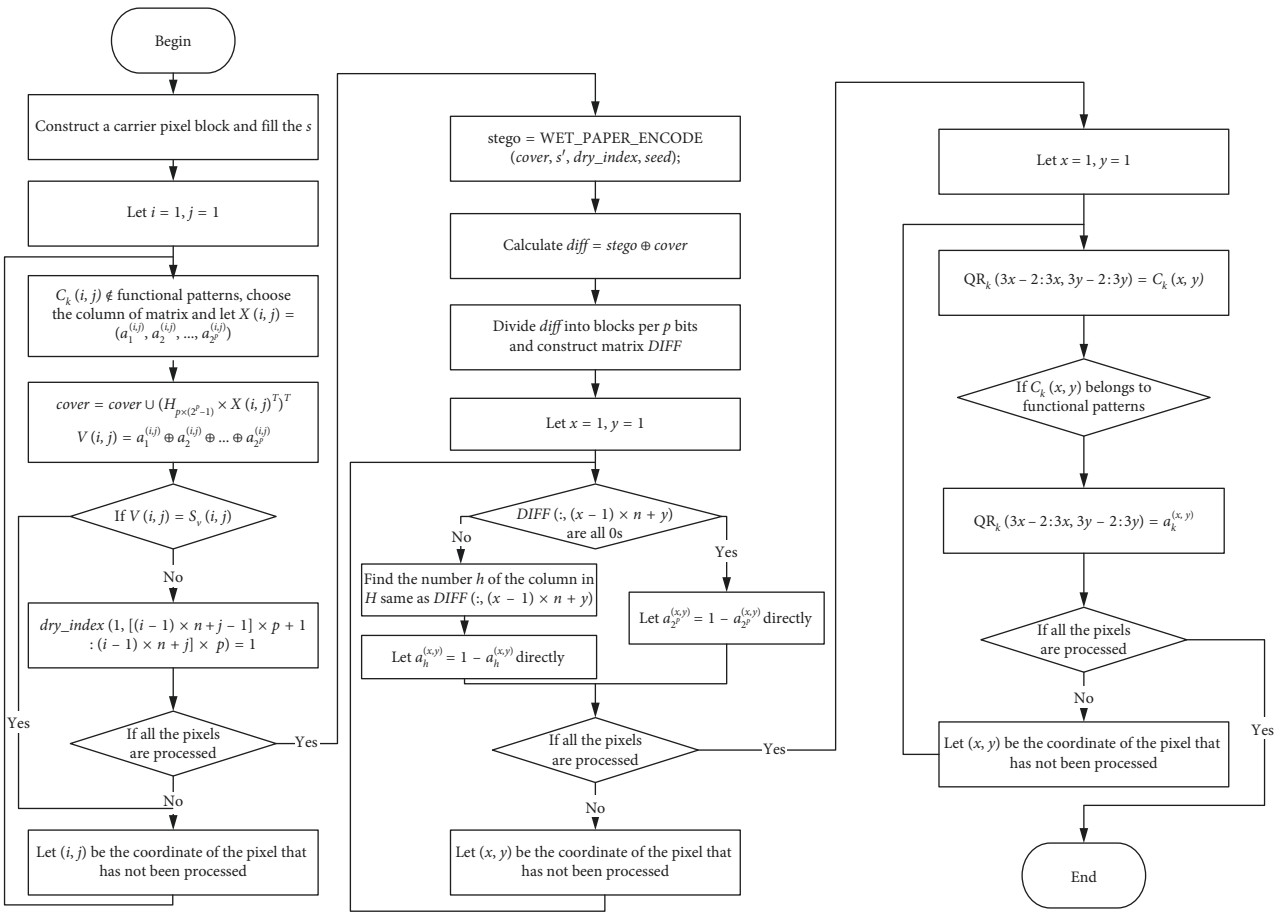


Figure 5: Scheme algorithm flow chart.

the third layer information is $(1/(n \times C_{m\times n}^{l_2} \times (2^p - 1)!)) + ((n-1)/(n \times C_{m\times n}^{l_2} \times (2^p - 1)! \times 2^{l_2}))$.

End.

5. Experiments and Comparisons

This section mainly includes two parts: Experimental Results and Comparison and Discussion.

5.1. Experiment Results. Taking the (8, 8) sharing scheme as an example, we choose the QR code of version 3 with error correction level M as the carrier image, a privacy QR code with the same specification as the second layer information, and 450-bit streams as the third layer information. The size of both carrier QR code and the privacy QR code is 37×37. Table 1 shows the dataset for the experiment.

The text images of the experiment are given in Figure 6, where Figures 6(a)–6(i) and 6(h) are the carrier QR codes and privacy QR code, respectively, which are generated by the standard QR code generator PsQREdit 2.4.3-Chinese, and the decoding result is consistent with the test case. Figures 7(a)–7(h) show the shares with sizes of 111×111. Each share can be decoded by the standard QR code decoder or the device with decoding function, of which the content is correspond to the carrier QR code.

5.2. Comparison and Discussion. Comparisons and discussions of this paper and other related schemes are provided in this section. Table 2 lists the overall comparisons of this paper and other related schemes.

5.2.1. Method and Recovery Computation. Based on the visual cryptography, of which the computational complexity of decryption is $O(N)$, authors of [17–19] designed a two-level QR code of which the public information can be read by any device with decoding function, and the secret information only can be extracted by the legal authorized personnel. The time complexity of [2], where an optical encryption was used, was decided by parameter λ. Based on information hiding technology, [5, 8, 16, 20] combined the characteristics of the QR code to embed sensitive information. Among them, the main operation of [8] was based on hash function, whose computational complexity is $O(N^2)$. The main operation of [5] focused on ECC decryption, while the operations in [16] were all addition and modulo operations, which led to a low computational complexity as $O(N)$. Reference [23] was a secret hiding scheme by improving exploiting modification direction to protect the private message in QR code with the computational complexity as $O(N)$. Based on the watermarking scheme, Ref. [21, 22] used digital watermarking technology

Input: Carrier QR code images $C_1, C_2, \ldots, C_{2^p}$ of size $m \times n$, Shared key *seed*, Privacy QR code S_v with size of $m \times n$ as the second layer information, The third layer information s.
Output: shares $QR_1, QR_2, \ldots, QR_{2^p}$ with size of $3m \times 3n$.
Step 1: Construct a random matrix block $\begin{bmatrix} a_1^{(1,1)} & a_1^{(1,2)} & \ldots & a_1^{(m,n)} \\ a_2^{(1,1)} & a_2^{(1,2)} & \ldots & a_2^{(m,n)} \\ \ldots & \ldots & \ldots & \ldots \\ a_{2^p}^{(1,1)} & a_{2^p}^{(1,2)} & \ldots & a_{2^p}^{(m,n)} \end{bmatrix}$, The third layer information stream s is zero-filled to obtain s', which satisfies $length(s') \bmod p = 0$.

Step 2: Let $i = 1$, $j = 1$, *cover* is an empty matrix. i and j represent the rows and columns of the carrier QR code, respectively.
Step 3: If $C_k(i, j)$ $(k = 1, 2, \ldots, 2^p)$ belongs to the functional patterns of QR code, go to Step 5. Else, select the corresponding column vector in the random matrix, and let $X(i, j) = (a_1^{(i,j)}, a_2^{(i,j)}, \ldots, a_{2^p-1}^{(i,j)})$, $cover = cover \cup (H_{p\times(2^p-1)} \times X(i, j)^T)^T$, where "∪" represents the merger of the matrix. Calculate the XOR result of each column element of the random matrix block by $V(i, j) = a_1^{(i,j)} \oplus a_2^{(i,j)} \oplus \cdots \oplus a_{2^p}^{(i,j)}$.
Step 4: If $V(i, j) = S_v(i, j)$, go to Step 5. Else, let $dry\_index(1, [(i-1) \times n + j - 1] \times p + 1 : [(i-1) \times n + j] \times p) = 1$.
Step 5: Let $j = j + 1$, if $j > n$, go to Step 6. Else, go to Step 3.
Step 6: Let $i = i + 1$, if $i > m$, go to Step 7. Else, go to Step 3.
Step 7: The carrier data $cover_{m\times n\times p}$, the secret information s', the matrix *dry_index* and the shared key *seed* are taking as the input of wet paper codes and the array $stego_{m\times n\times p}$ that carries the secret information is the output. Then, calculate $diff = stego \oplus cover$ and divide the *diff* into blocks by per p bits. Each block is treated as a column vector and all the vectors are arranged in order to form the matrix $DIFF_{p\times(m\times n)}$.
Step 8: Let $x = 1$, $y = 1$. x and y represent the rows and columns of the carrier QR code, respectively.
Step 9: If the column $(x-1) \times n + y$ of the *DIFF* is equal to $[0, 0, \ldots, 0]^T_{1\times p}$, let $a_{2^p}^{(x,y)} = 1 - a_{2^p}^{(x,y)}$. Else, find the number same column in the $H_{p\times(2^p-1)}$, of which the corresponding column number is recorded as h, and calculate $a_h^{(x,y)} = 1 - a_h^{(x,y)}$.
Step 10: If $C_k(x, y)$ $(k = 1, 2, \ldots, 2^p)$ belongs to the functional patterns of QR code, let $QR_k(3x-2 : 3x, 3y-2 : 3y) = C_k(x, y)$. Else, calculate $QR_k(3x-2 : 3x, 3y-2 : 3y) = a_k^{(x,y)}$ and $QR_k(3x-1, 3y-1) = C_k(x, y)$.
Step 11: Let $y = y + 1$, if $y > n$, go to Step 12. Else, go to Step 9.
Step 12: Let $x = x + 1$, if $x \le m$, go to Step 9. Else, output the QR code shares $QR_1, QR_2, \ldots, QR_{2^p}$.

Algorithm 2: Information sharing and embedding Algorithm.

Input: *Shares* $QR_1, QR_2, \ldots, QR_{2^p}$ with size of $3m \times 3n$.
Output: Privacy QR code S_v with size of $m \times n$.
Step 1: Construct a pixel matrix block $\begin{bmatrix} QR_1(1,1) & QR_1(1,2) & \ldots & QR_1(3m,3n) \\ QR_2(1,1) & QR_2(1,2) & \ldots & QR_2(3m,3n) \\ \ldots & \ldots & \ldots & \ldots \\ QR_{2^p}(1,1) & QR_{2^p}(1,2) & \ldots & QR_{2^p}(3m,3n) \end{bmatrix}$.
Step 2: Let $i = 1$, $j = 1$. i and j represent the rows and columns of the carrier QR code, respectively.
Step 3: If $QR_k(i, j)$ $(k = 1, 2, \ldots, 2^p)$ belongs to the functional patterns of QR code, go to Step 5. Else, go to Step 4.
Step 4: Calculate $S_v(1 + i/3, 1 + j/3) = QR_1(i, j) \oplus QR_2(i, j) \oplus \cdots \oplus QR_{2^p}(i, j)$.
Step 5: Let $j = j + 3$, if $j < 3n$, go to Step 3. Else, go to Step 6.
Step 6: Let $i = i + 3$, if $i < 3m$, go to Step 3. Else, go to Step 7.
Step 7: The algorithm ends.

Algorithm 3: Recovery algorithm of the second layer information.

to realize the embedding of secret information. However, the schemes utilized discrete cosine transform to perform operations in the frequency domain, its computational complexity is relatively high. In the proposed scheme, the second layer of information decryption is completed by a simple XOR operation, and the third layer of information is extracted by matrix multiplication. Apparently, our paper has low time complexity when compared with some other works.

5.2.2. Utilizing the Error Correction Capability. Based on the error correction mechanism of QR code, Ref. [8, 16, 19–22] employed part of error correction codewords to embed the secret bits with the condition of ensuring the readability of QR code. While, this paper and Ref. [17, 18] achieved the aim of embedding secret bits by replacing the module of the QR code with different recognition units.

5.2.3. Secret Payload. Assume that there are 2^p carrier QR codes with sizes of $m \times n$; the length of the second layer information is x bits, the length of the third layer information stream is y bits, and the total secret amount is *amount* that satisfies

Input: *Shares* QR_1, QR_2, ..., $QR_2{}^P$ with size of $3m \times 3n$, the length l of the secret information, the shared key *seed*.
Output: The third level information *s*.
Step 1: Construct a pixel matrix block $\begin{bmatrix} QR_1(1,1) & QR_1(1,2) & \ldots & QR_1(3m,3n) \\ QR_2(1,1) & QR_2(1,2) & \ldots & QR_2(3m,3n) \\ \ldots & \ldots & \ldots & \ldots \\ QR_{2^p}(1,1) & QR_{2^p}(1,2) & \ldots & QR_{2^p}(3m,3n) \end{bmatrix}$.
Step 2: Let $i = 1$, $j = 1$. i and j represent the rows and columns of the carrier QR code, respectively.
Step 3: Let $X(1 + i/3, 1 + j/3) = (QR_1(i,j), QR_2(i,j), \ldots, QR_{2^p-1}(i,j))$, $cover = cover \cup (H_{p\times(2^p-1)} \times X(i,j)^T)^T$, where "∪" represents the merger of the matrix.
Step 4: Let $j = j + 3$, if $j < 3n$, go to Step 3. Else, go to Step 5.
Step 5: Let $i = i + 3$, if $i < 3m$, go to Step 3. Else, go to Step 6.
Step 6: *cover* and *seed* are used as input of the wet paper code decoding algorithm to solve the embedded information.
Step 7: The first l bit is output as the third layer information, and the algorithm ends.

Algorithm 4: Extraction Algorithm of the third layer information.

Table 1: Experimental use.

Carrier QR code	C_1: cover response code 1 C_2: cover response code 2 C_3: cover response code 3 C_4: cover response code 4 C_5: cover response code 5 C_6: cover response code 6 C_7: cover response code 7 C_8: cover response code 8
The privacy QR code	S_v: private image
The third-layer information	"The world is not made of strings, but is made of things"

$$\text{amount} = x + y. \tag{7}$$

Based on the proposed scheme, some pixels may be changed, which is caused by the embedding of the second-layer information stream. The positions of these flipped pixels are used as position indexes to embed the third-layer information stream, and the 1-bit flipping pixels may transmit p bit information. Therefore, the amount of the third-layer information must satisfy Equation (8).

$$0 \le y \le px. \tag{8}$$

If, and only if, the XOR-ed results of each column of the carrier pixel block are equal to the second layer information stream, then $y = 0$ exists. In addition, when all the positions of flipped pixels satisfy the embedding condition of the third-layer information stream, $y = px$ exists. At this point, the *amount* of reaches the maximum value.

$$x \le \text{amount} \le (p + 1)x. \tag{9}$$

And because the private QR code with size of $m \times n$ is taken as the second layer of information, so equation (9) can turns into Equation (10).

$$m \times n \le \text{amount} \le (p + 1) \times m \times n. \tag{10}$$

Therefore, the payload of the single carrier QR code is

$$\frac{(m \times n)}{2^p} \le \text{payload} \le \frac{[(p + 1) \times m \times n]}{2^p}. \tag{11}$$

Compared with related works, the proposed scheme has a significant advantage of high secret payload rate. Let $p = 3$, and compare the secret payload of the proposed scheme with Ref. [8, 16–20].

References [8, 16, 19, 20] utilizes the error correction capability of the QR code to implement the embedding of secret information by modifying part of the pixels of the QR code, which limits the maximum payload of the secret information to the error correction capability. Based on the recognition mechanism of the QR code, this paper and Ref. [17, 18] replace all of the data codewords and error correction codewords by 3×3 submodules, so the amount of the secret bits are higher than that in Ref. [8, 16, 19, 20]. However, as the size of the shares generated in this paper and Ref. [17, 18] increases, the efficiency of information embedding is greatly reduced. Different from Ref. [17, 18], this paper employs the XOR operation and the error correction principle of the Hamming code to resume the pixels of the carrier QR codes. Therefore, the embedding efficiency is higher than that in Ref. [17, 18].

The results of the comparison are provided in Table 3 in detail. We assume $p = 3$, and there are half of the pixels that carry the extra secret bits.

The comparison of the secret payload rate which indicates the number of the secret bits carried by a signal pixel is shown as Figure 8.

5.2.4. Robustness. In practical applications, the three-layer QR code will be subject to various forms of interference from the outside world, inevitably. In this section, the feasibility and robustness of the scheme will be tested and analysed for four common interference forms. All the images contain 300×300 pixels.

In image storage, image compression technology is usually used to reduce the storage space of the shares at present. In order to test the feasibility of this scheme after image compression, JPEG2000 lossy compression with compression quality of 0, 45, 90, and 100 is done in this paper. The experimental results show that the compressed share still can be recognized and the secret information also can be decoded which illustrates the scheme is still feasible.

In the process of image transmission, (1) the share image may be modified or lost part of the pixel information. In order to test the feasibility under such circumstances, we

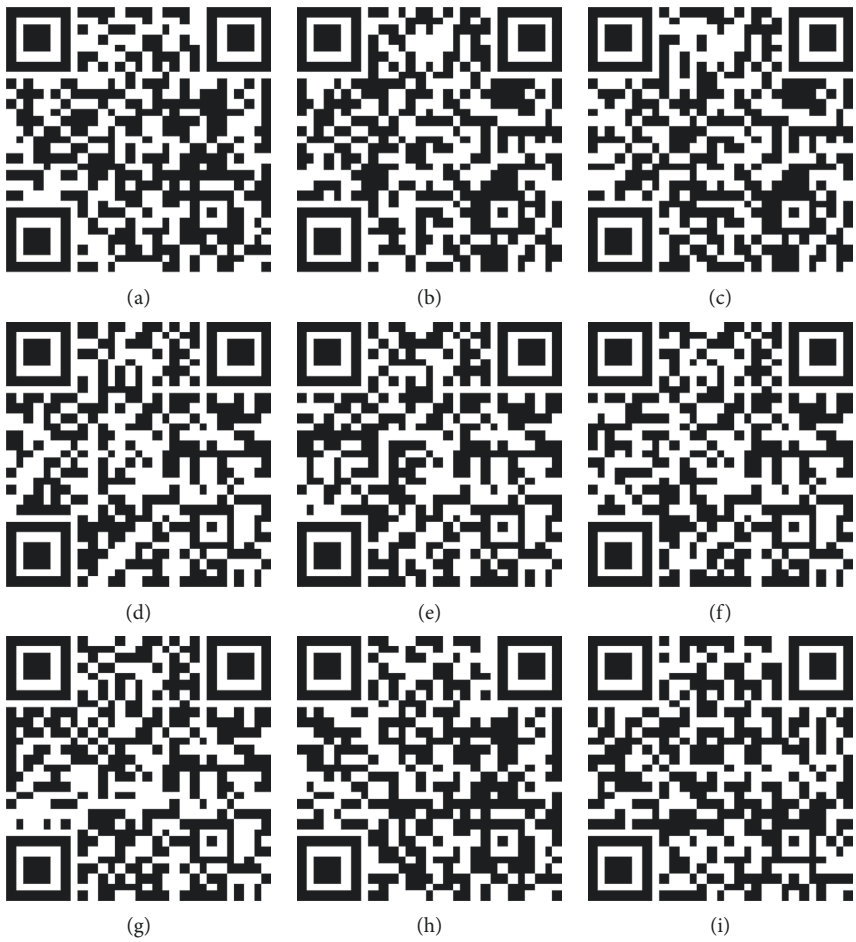


Figure 6: Carrier QR codes and privacy QR code.

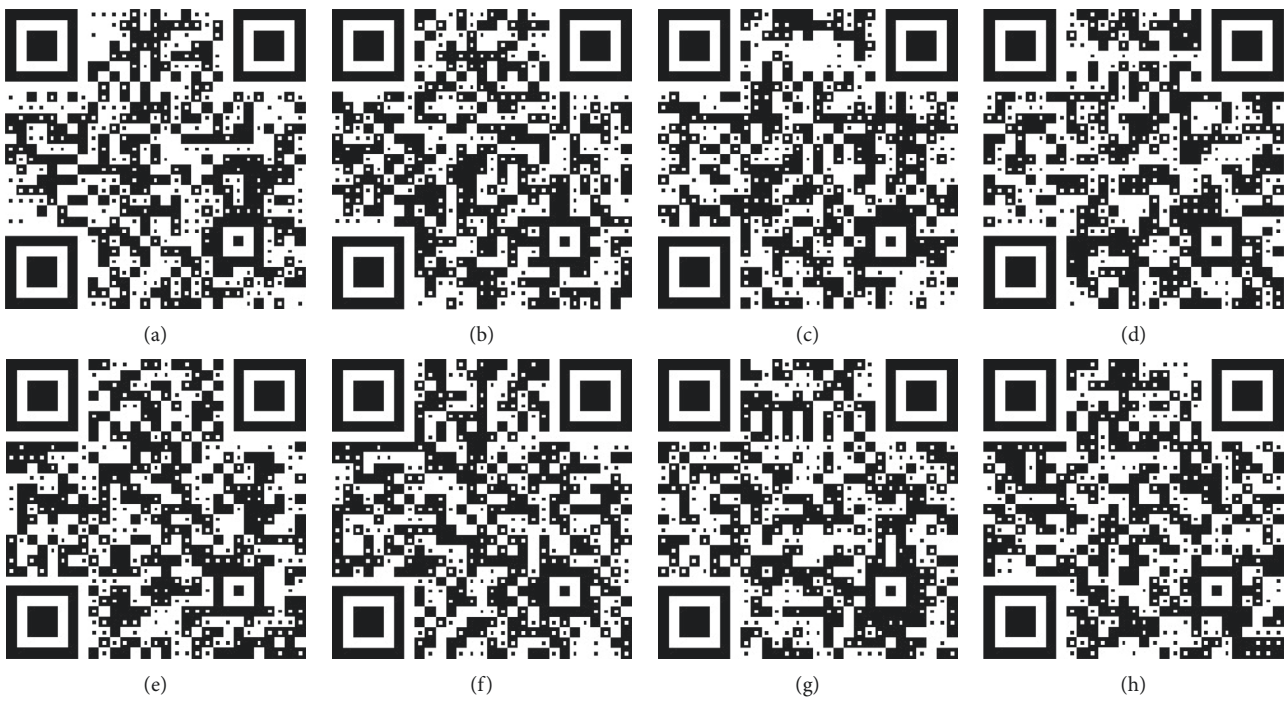


Figure 7: Carrier QR codes and privacy QR code.

Table 2: Overall comparison of related works.

Functionality	Method	Utilizing the error correction capability	Recovery computation	Secret payload	Robustness
[3]	Optical encryption	No	$O(N^{\lambda} \log N)(\lambda \geq 1)$	—	—
[5]	Secret hiding	No	$O(N \log N)$	—	Low
[8]	Secret sharing and hiding	Yes	$O(N^2)$	Low	Low
[16]	Secret sharing and hiding	Yes	$O(N)$	Low	Low
[17]	VCS	No	$O(N)$	Low	Low
[18]	VCS	No	$O(N)$	Low	Low
[19]	VCS	Yes	$O(N)$	Low	—
[20]	Secret hiding	Yes	$O(N)$	Low	—
[21, 22]	Watermarking	Yes	$O(N^4)$	—	—
This paper	Secret sharing and hiding	No	$O(N)$	High	High

Table 3: The number of secret bits in the proposed scheme and related works.

Paper	Version 2				Version 3				Version 4			
	L	M	Q	H	L	M	Q	H	L	M	Q	H
[8]	32	56	80	104	48	96	128	160	72	128	192	224
[16]	32	64	88	112	56	101	144	176	80	144	208	256
[17]	359	359	359	359	567	567	567	567	807	807	807	807
[18]	359	359	359	359	567	567	567	567	807	807	807	807
[19]	32	64	88	112	56	101	144	176	80	144	208	256
[20]	12	24	42	51	18	42	69	84	27	60	99	120
Ours	897	897	897	897	1417	1417	1417	1417	2017	2017	2017	2017

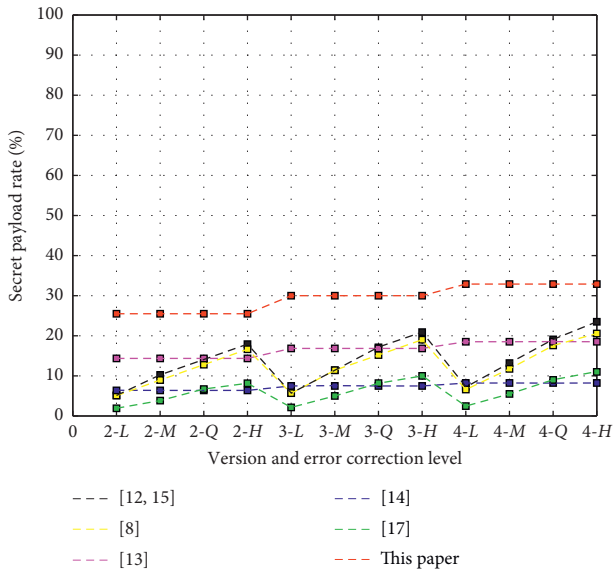


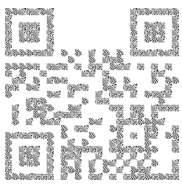
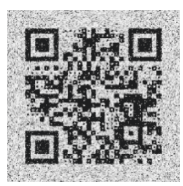
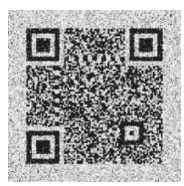
Figure 8: Comparison of secret payload rates.

crop some of the pixel information of the share image. After clipping, the damaged three-layer QR code can still be correctly recognized. In addition, by doing the same clipping operation for the three-layer QR code generated in Ref. [5, 8, 16], the strong robustness of the scheme is highlighted. Among them, the carrier QR code version adopted in Ref. [5, 8, 16] is 4, and the error correction level is H. The QR code version adopted in this paper is 3, and the error correction level is M. (2) Considering the condition of noise interference, we add the Gaussian noise with different δ^2 to the generated three-layer QR code, respectively. Experimental results show that when δ^2 reaches the value of 0.4, the QR code is unreadable, but the secret can be decoded. We assume the reason for this phenomenon is that the surrounding 8 bits of the 3×3 information storage structure of the module recognition unit, shown in Figure 3, stored the same subsecret bits, while only the middle bit is utilized to retain the information of the carrier QR code. The distribution characteristic makes the secret information difficult to damage and content in the carrier QR code difficult to recognize when the distortion happens to the three-layer QR code, because the surrounding 8 bits may change the recognition method of QR code from principle base on the key pixel to principle base on the density of the 3×3 information storage structure. To verify our guess, we take the result of Ref. [18] as contradistinction, where the surrounding 8 bits of the 3×3 information storage structure is different. As experimental result shows, when $\delta^2 = 0.4$, the content of the QR code cannot be recognized, and the secret cannot be decoded, which proves the correctness of our guess.

In the phase of image acquisition, there always exists distortion of the acquired image. In this paper, the share image is deformed in different directions and scanned by QR code decoder. Experiments show that the distorted shares can still be read accurately. Before secret reconstruction, the distorted share is geometrically corrected by normal correction algorithms [24]. The corrected image can accurately recover the embedded secret information.

In the process of image scanning, considering that the scanning angle is arbitrary when the mobile device scans the QR code, we use Photoshop to rotate the share image at different angles. Experiments show the three-layer QR code

Table 4: Results of the general image processing operations.

	Three-layer QR code			
Compression	$Q = 0$	$Q = 45$	$Q = 90$	$Q = 100$
Distorted QR code				
QR content	Readable	Readable	Readable	Readable
Secret	Decodable	Decodable	Decodable	Decodable
	Three-layer QR code			
Clipping	This paper	Reference [5]	Reference [8]	Reference [16]
Distorted QR code				
QR content	Readable	Unreadable	Unreadable	Unreadable
	Three-layer QR code			
Gaussian noise	This paper ($\mu = 0$, $\delta^2 = 0.1$)	This paper ($\mu = 0$, $\delta^2 = 0.2$)	This paper ($\mu = 0$, $\delta^2 = 0.4$)	Reference [18] ($\mu = 0$, $\delta^2 = 0.4$)
Distorted QR code				
QR content	Readable	Readable	Unreadable	Unreadable
Secret	Decodable	Decodable	Decodable	Undecodable
	Three-layer QR code			
Distortion				
Distorted QR code				
QR content	Readable	Readable	Readable	Readable
Secret	Decodable	Decodable	Decodable	Decodable
	Three-layer QR code			
Rotation	45°	90°	135°	270°
Distorted QR code				
QR content	Readable	Readable	Readable	Readable
Secret	Decodable	Decodable	Decodable	Decodable

can be recognized, and the embedded secret information can be extracted correctly after rotation.

The specific test results are shown in Table 4, in which the "Readable" means that the three-layer QR code are still readable and can be decoded after processing, and "Decodable" means that secret information can be normally decrypted and extracted.

Functional comparisons of the proposed scheme and other related works have been discussed above. And the major advantages of this paper are concluded as follows:

(i) The proposed scheme supports three-layer information storage, which exceeds the existing two-level QR code. The multiple layer information storage can solve the complex application requirements and has a wider foreground.

(ii) Based on the error correction principle of Hamming Code, the carrier pixels are reused to achieve a high embedding efficiency. As the experimental result shows, the secret payload rate is higher than that in Ref. [8, 16–20].

(iii) The three-layer QR code can against some common geometric attack. We analyse several situations the scheme usually encounters in real-word applications, and the results.

6. Conclusion

Different from traditional QR code researches, this paper reuses carrier pixels based on the error correction principle of Hamming code to improve the efficiency of the embedding. Wet paper code and recognition mechanism of QR code are employed to fuse the encrypted secrets with the carrier QR codes. Finally, a novel three-layer QR code is generated.

Compared with the other two-level QR code, the proposed scheme has the characteristics of high efficiency of information embedding, large secret payload rate, and strong robustness, which make the scheme have a wide range of application scenarios in real life. For example, in order to protect the patient's medical record information, the hospital can distinguish the doctor and other personnel with different rights, so that the patient's information cannot be maliciously disclosed. It can also be used to protect the privacy information in express logistics. What's more, according to the characteristics of the three-layer storage of information, the second tier information can be used to authenticate the identity; after the authentication is passed, the third-layer secret information is extracted to improve the performance of the scheme.

In addition, the scheme has strong portability. It can be extended to other two-dimensional codes with error correction functions, such as PDF417 and data matrix.

Data Availability

The data used to support the findings of this study are included within the article.

Disclosure

Bin Yu and Zhengxin Fu contributed equally to this work and should be considered co-first authors.

Conflicts of Interest

The author(s) declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The authors thank the support from National Natural Science Foundation of China under grant no. 61602513.

References

[1] ISO/IEC 18004:2006, *Information Technology—Automatic Identification and Data Capture Techniques—Barcode Symbology—QR Code*, ISO/IEC 18004:2006, Geneva, Switzerland, 2006.

[2] M. B. Krishna and A. Dugar, "Product authentication using QR codes: a mobile application to combat counterfeiting," *Wireless Personal Communications*, vol. 90, no. 1, pp. 381–398, 2016.

[3] J. Wang, L. Song, X. Liang, Y. Liu, and P. Liu, "Secure and noise-free nonlinear optical cryptosystem based on phase-truncated Fresnel diffraction and QR code," *Optical & Quantum Electronics*, vol. 48, no. 11, p. 523, 2016.

[4] N. Teraura and K. Sakurai, "Information hiding in subcells of a two-dimensional code," in *Proceedings of the 1st IEEE Global Conference on Consumer Electronics 2012*, pp. 652–656, Tokyo, Japan, October 2012.

[5] I. Tkachenko, W. Puech, C. Destruel, O. Strauss, J.-M. Gaudin, and C. Guichard, "Two-level QR code for private message sharing and document authentication," *IEEE Transactions on Information Forensics & Security*, vol. 11, no. 3, pp. 571–583, 2016.

[6] Y. J. Chiang, P. Y. Lin, R. Z. Wang, and Y.-H. Chen, "Blind QR code steganographic approach based upon error correction capability," *KSII Transactions on Internet & Information Systems*, vol. 7, no. 10, pp. 2527–2543, 2013.

[7] P.-Y. Lin and Y.-H. Chen, "High payload secret hiding technology for QR codes," *EURASIP Journal on Image & Video Processing*, vol. 2017, no. 1, p. 14, 2017.

[8] P.-Y. Lin, "Distributed secret sharing approach with cheater prevention based on QR code," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 1, pp. 384–392, 2016.

[9] H. Hu, G. Shen, Z. Fu, B. Yu, and J. Wang, "General construction for XOR-based visual cryptography and its extended capability," *Multimedia Tools and Applications*, vol. 75, no. 21, pp. 13883–13911, 2016.

[10] H. Hu, G. Shen, Y. Liu, Z. Fu, and B. Yu, "Improved schemes for visual secret sharing based on random grids," *Multimedia Tools & Applications*, vol. 78, no. 9, pp. 1–31, 2018.

[11] H. Hu, G. Shen, Z. Fu et al., "Improved contrast for threshold random-grid-based visual cryptography," *KSII Transactions on Internet & Information Systems*, vol. 12, no. 7, pp. 3401–3420, 2018.

[12] S. Liu, Z. Fu, and B. Yu, "Rich QR codes with three-layer information using hamming code," *IEEE Access*, vol. 7, pp. 78640–78651, 2019.

[13] J. Fridrich, *Steganography in Digital Media Principles, Algorithms, and Applications*, Cambridge University Press, Cambridge, UK, 2014.

[14] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, "Writing on wet paper," *IEEE Transactions on Signal Processing*, vol. 53, no. 10, pp. 3923–3935, 2005.

[15] H.-K. Chu, C.-S. Chang, R.-R. Lee, and N. J. Mitra, "Halftone QR codes," *ACM Transactions on Graphics*, vol. 32, no. 6, pp. 1–8, 2013.

[16] Y. Chow, W. Susilo, G. Yang, J. G. Phillips, I. Pranata, and A. Barmawi, "Exploiting the error correction mechanism in QR codes for secret sharing," in *Proceedings of the Australasian Conference on Information Security & Privacy*, pp. 409–425, Springer, Cham, 2016.

[17] L. Yingying, F. Zhengxin, and W. Yiwei, "Two-level information management scheme based on visual cryptography and QR code," *Application Research of Computers*, vol. 33, no. 11, pp. 3460–3463, 2016.

[18] Y. Cheng, Z. Fu, B. Yu, and G. Shen, "A new two-level QR code with visual cryptography scheme," *Multimedia Tools and Applications*, vol. 77, no. 16, pp. 20629–20649, 2018.

[19] W. Song, Y. Lu, X. Yan, Y. Wang, and C. Chang, "Visual secret sharing scheme for (*k*, *n*) threshold based on QR code with multiple decryptions," *Journal of Real-Time Image-Processing*, vol. 14, no. 1, pp. 25–40, 2018.

[20] P.-C. Huang, Y.-H. Li, C.-C. Chang, and Y. Liu, "Efficient scheme for secret hiding in QR code by improving exploiting modification direction," *KSII Transactions on Internet & Information Systems*, vol. 12, no. 5, pp. 2348–2365, 2018.

[21] S. Rungraungsilp, M. Ketcham, V. Kosolvijak, and S. Vongpradhip, "Data hiding method for QR code based on watermark by compare DCT with DFT domain," in *Proceedings of the International Conference of Computer and Communication Technologies*, pp. 144–148, Phuket, Thailand, May 2012.

[22] Q. Kang, K. Li, and J. Yang, "A digital watermarking approach based on DCT domain combining QR code and chaotic theory," in *Proceedings of the 2014 Eleventh International Conference on Wireless and Optical Communications Networks (WOCN)*, Vijayawada, India, September 2014.

[23] C. J. C. Chuang, Y. C. Hu, and H. J. Ko, "A novel secret sharing technique using QR code," *International Journal of Image-Processing*, vol. 4, no. 5, pp. 468–475, 2010.

[24] M. Kaur and A. S. Bhandari, "Deblurring, localization and geometry correction of 2D QR bar codes using Richardson Lucy method," *International Journal of Engineering Research & Applications*, vol. 4, no. 9, pp. 12–17, 2014.