PROMISE: A QR Code PROjection Matrix Based Framework for Information Hiding Using Image SEgmentation

Yixiang Fang[1*], Kai Tu[2], Kai Wu[1], Yi Peng[1], and Yunqing Shi[3]
[1] School of Mechanical and Electronic Engineering, Jingdezhen Ceramic University
Jingdezhen, 333000 China
[e-mail: fangyixiang@jci.edu.cn]
[2] Department of Computer Science and Engineering, The Pennsylvania State University
State College, PA, USA
[e-mail: kjt5562@psu.edu]
[3] Department of Electrical and Computer Engineering, New Jersey Institute of Technology
Newark, NJ, USA
[e-mail: yun-qing.shi@njit.edu]
[*]Corresponding author: Yixiang Fang

Received May 12, 2022; revised August 22, 2022; accepted February 12, 2023; published February 28, 2023

Abstract

As data sharing increases explosively, such information encoded in QR code is completely public as private messages are not securely protected. This paper proposes a new 'PROMISE' framework for hiding information based on the QR code projection matrix by using image segmentation without modifying the essential QR code characteristics. Projection matrix mapping, matrix scrambling, fusion image segmentation and steganography with SEL(secret embedding logic) are part of the PROMISE framework. The QR code could be mapped to determine the segmentation site of the fusion image as a binary information matrix. To further protect the site information, matrix scrambling could be adopted after the mapping phase. Image segmentation is then performed on the fusion image and the SEL module is applied to embed the secret message into the fusion image. Matrix transformation and SEL parameters should be uploaded to the server as the secret key for authorized users to decode the private message. And it was possible to further obtain the private message hidden by the framework we proposed. Experimental findings show that when compared to some traditional information hiding methods, better anti-detection performance, greater secret key space and lower complexity could be obtained in our work.

Keywords: information hiding, image segmentation, projection matrix, QR code, secret embedding logic

This work was supported by the National Natural Science Foundation of China under Grant 62062044, 62063010, 61762054 and science and technology project of Jingdezhen under Grant 2020ZDGG004. Many thanks to the anonymous reviewers for their insightful comments and valuable suggestions, which helped a lot to improve the paper quality. We express our thanks to Dr. Junxiang Wang who checked our manuscript.

http://doi.org/10.3837/tiis.2023.02.010 **ISSN : 1976-7277**

1.Introduction

The sharing of information is expanding with the increasing consumption rate of people in the world today. Because of the main features of QR code, including fast recognition and low cost, QR code is gradually becoming the link between offline and online content as the media for data sharing and collaboration. The traditional barcode only has a small storage capacity for information, so its development is limited. But two-dimensional codes in our time such as the DataMatrix[1], PDF417[2] code and QR code[3] are widely used in our daily life in the field of information storage[4], commodity identification, e-voting authentication[5], digital watermarking[6] and etc.. QR code, as the most common-use two-dimensional matrix code, was first designed in 1994 by the Japanese Denso Wave Corporation and has been adopted as a universal standard specification[7] published by ISO since 2000[8].

Manoj S. Rewatkar and Shital A. Raut[9] introduced some application methods which combine traditional information hiding techniques with QR codes, and made a comparison between these methods. Lin et al. first proposed in [10] that the secret information is hidden in the cover of QR code by using the feature of error correction of QR code. First using a shared key to encode the secret information, and then embedding it in the QR code. The ordinary browsers can only read the QR code content from the QR code, and only authorized users can encrypt the QR code and obtain secret message from it. However, once the encoded secret message is altered, the true secret message cannot be recovered. A method that can be used for authentication is presented in [11]. The QR code in this method is divided into two layers: public layer and private layer. The common layer is the same as the standard QR code storage layer which can be read by anyone. The private layer is created by replacing the black module with a specific texture mode. This texture mode is considered a black module for the standard QR code reader, and can only be read in a specific way. Therefore, not only the capacity of the QR code is increased, but also the sensitivity of the print-and-scan (P&S) process can be used for identity authentication. A two-layer two-dimensional code was also proposed in [12]. It can encode two independent information and read different information from the QR code by changing the scan angle. But its angle must be accurately calculated in advance to correctly scan the information. This method is relatively inapplicable in daily life. An improved application of visual secret-sharing scheme in QR code was proposed in [13], where extending the previous (n, n) sharing mechanism to (k, n) makes the QR code more secure when hiding information. You can also distribute information about secret messages into n shares. Each share is composed of a valid cover[14] of QR code that can be scanned and read by the QR code reader. And the secret message can be obtained by combining the information in all shares. A copy-proof authentication scheme was proposed by Changsheng Chen et al in[15], using the features of the QR code channel model to extract two sets of features. The extracted features are compared with the essential features of the QR code image in terms of frequency and spatial domains. And then a two-stage QR code authentication framework is formed by cascading. Based on the error correction function of the QR code, the secret message is hidden in the modified QR code module [16]. These modified modules act as keys that can only be used by authorized recipients. When the QR code is scanned by an ordinary code scanner, it can be scanned and read normally by using its error correction feature. And it is fantastic that later recovery of the wrong modules happens in the process of extracting secret information, which can effectively reduce the attention of the attacker.

The above studies focus primarily on modifying the image texture of the QR code and using the QR code error correction feature to embed the secret message. The visual image of the QR code will be changed by these methods. In this paper, the PROMISE framework proposed

avoids the above deficiencies. While the carrier is a QR code, the suspicion of the attacker is not easy to arouse, and the experimental results show that our work could achieve better anti-detection performance, greater secret key space and lower complexity when compared to some traditional methods of information hiding.

As follows, the paper is organized. In section 2, the QR code's secret information hiding scheme and the secret message extraction process are introduced in detail. In section 3, the experimental results verify the feasibility and effectiveness of the method proposed, and assess and analyze the system's performance. Finally, an overall summary of the full text is made up of the fourth section.

2. The Proposed Method

2.1 Hidden Process of Secret Message

In this paper, we propose a new 'PROMISE' framework to hide information based on the QR code projection matrix in the QR code fusion image, as shown in **Fig. 1**. First, the public message is encoded into a QR code. Since the information matrix mapped by the QR code consists essentially of (0, 1), it could be converted after logistic scrambling into a scrambled 'new' matrix. According to its features, the matrix is projected onto an image and then the image, which is a grayscale and pixel fusion of the original QR code image of general information and the bottom background image, is divided into segments.

The secret information logic is embedded in the center segment after segment separation. To embed the encoded secret message into other image blocks, the STC algorithm is used. Finally, an art-like image of the QR code is formed. Without changing the characteristics of the QR code itself, our method could make full use of the essential features of the QR code to hide information. The image is more aesthetic overall by a pixel fusion of QR code image and background image. In addition, the hiding capacity of information expands greatly in that there is a more complex texture in the image after pixel fusion. The implementation consists of five sections:

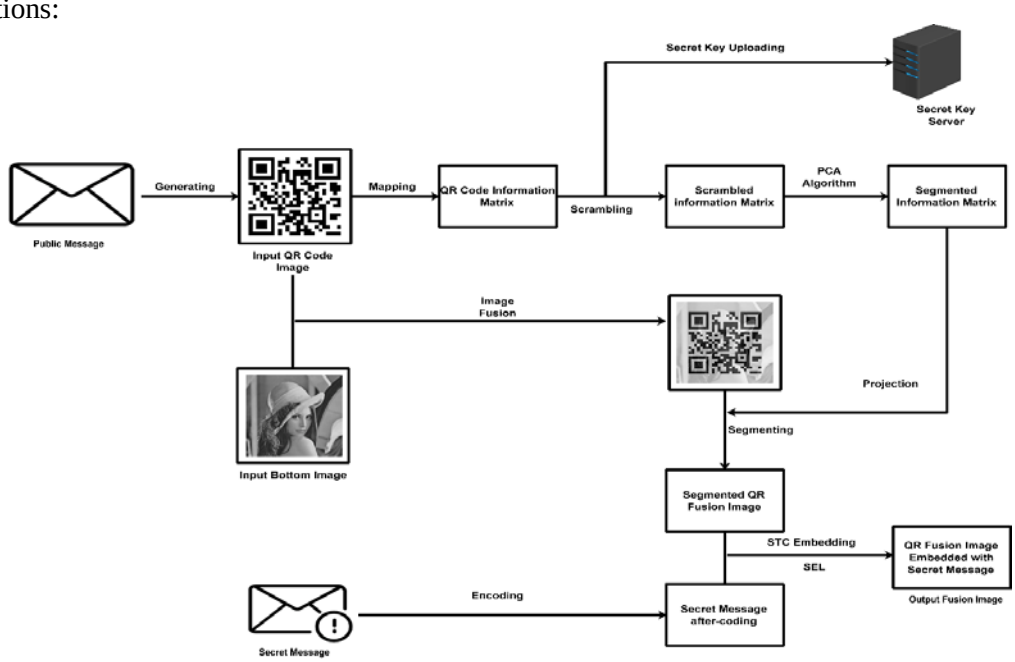

Fig. 1. Hidden process of secret message

2.1.1 QR Code Generation

The public message is encoded into a QR code image in this section. This information is publicly available, that is, anybody can access the original information from the QR code through such a common scanner. The QR code is presented in the form of a matrix, with the binary '1' representing black blocks and the binary '0' representing white blocks at the corresponding matrix element positions. The QR code could, in other words, be seen as an information matrix.

Fig. 2. QR code information matrix mapping

To generate a QR code image including ordinary information, use the QR code open source development library ZXing. Then convert it to a (0,1) matrix that could be regarded as an information matrix.

2.1.2 Matrix Scrambling

It is conducive to the implementation of the next segmentation to obtain some details from the matrix. In order to obtain a scrambled QR code information matrix, we use the Logistic scrambling algorithm to scramble the original QR code information matrix. The scrambling parameters are uploaded as the key to the server after they are encrypted during the matrix generation process.

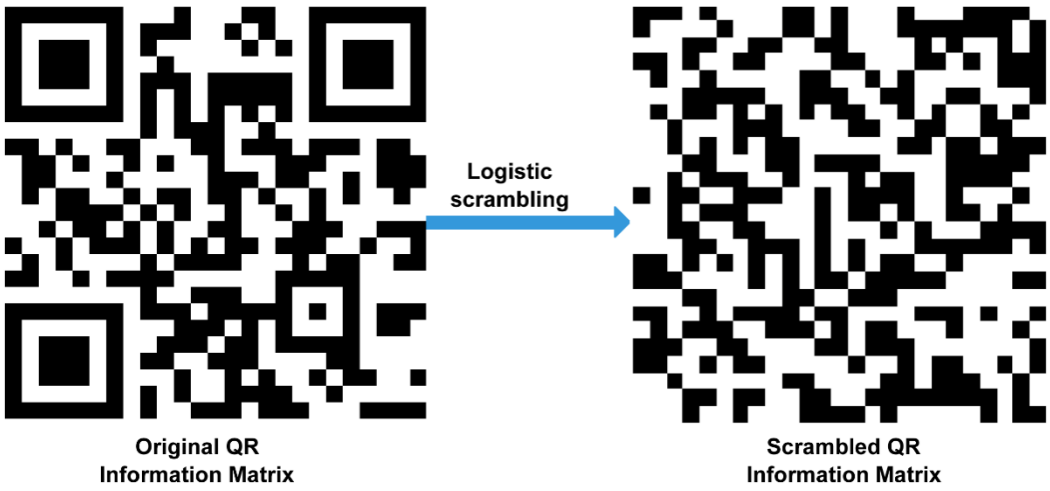

Fig. 3. Matrix scrambling

Hypothesizing the information matrix of two-dimensional code be Q and its size be $n \times n$ (n is the number of rows and columns of two-dimensional code information matrix), x, y represents the horizontal and vertical coordinates of the two-dimensional code information

matrix respectively. P_{xy} is the value of the information matrix at (x, y).

Logistic chaotic mapping iteration is:

$$X_{k+1} = \mu X_k \times (1 - X_k) \tag{1}$$

Within this equation: $X_k \in (0,1); n = 0,1,\cdots,n; \mu \in (0,4)$, μ is a system control parameter. When μ in the range of $[3.569, 4]$, the system begins to enter a chaotic state, then take a value from this range as the key for scrambling the QR code information matrix and upload it onto the key server.

Given initial value $X_0 = m_0, \mu = \mu_0$ and the number of iterations N, Pseudo-random sequences $A = \{m_0, m_1, \cdots, m_n - 1\}$ can be generated. Then make a 0,1-judgment based on $(y_n) = \begin{cases} 0, x_n < 0.5 \\ 1, x_n \geq 0.5 \end{cases}$. Get the binarized sequence B of A, $B = \{v_0, v_1, \cdots, v_n - 1\}$. Hypothesizing two-dimensional code information matrix coordinates $x = \frac{k}{n}, y = k \bmod n, F_{xy} = B_k$, The original two-dimensional code information matrix Q through the operation:

$$P_{x,y} = F_{x,y} \oplus Q_{x,y} \tag{2}$$

Then get the scrambled matrix P.

2.1.3 Image Fusion

QR Code is a typical binary image. The hidden data embedding ability would be limited if it were used directly as a carrier, and the detection resistance would be low. We enhance the texture of the QR code image before embedding the hidden message in order to increase the information embedding ability and boost the detection resistance of the QR code image.

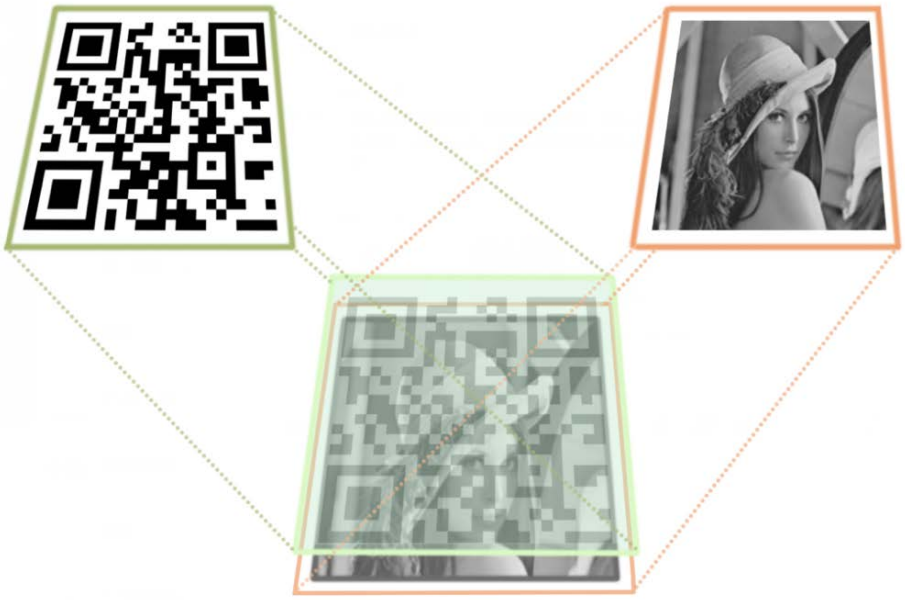

Fig. 4. Fusion Image Generation

In this module, a pixel fusion of background image with rich texture and the ordinary QR code image are generated originally[17， 18]. The QR code image after fusion can still be scanned

and identified correctly.

Assuming that the pixel value at the (I, j) position of the QR code image is $I(I, j)$ and the pixel value at the (I, j) position of the natural image is $j(I, j)$, then the pixel value $S(I, j)$ at the (I, j) position of the texture enhanced QR image is calculated as follows.

$$S(i, j) = \alpha \cdot (i, j) + \beta \cdot (i, j) \tag{3}$$

In equation (3), the parameter α value is 0.6, and the parameter β value is 0.4. After calculation, a fused grayscale image is obtained.

2.1.4 Image Segmentation

The information matrix is transformed to obtain the information matrix of the scrambled QR code. According to the characteristics of the scrambled QR code information matrix, the image could be partitioned by using the partitioning algorithms[19，20]. At present in this paper, PCA algorithm[21] is used to calculate the information matrix of the scrambled QR code. PCA is a principal component analysis which is often used to reduce data dimensions while still preserving important features of the original data set[22]. The implementation steps of PCA algorithm are as follows:

The QR code information matrix X after scrambling, size of $n \times n$ (n rows and columns of the matrix X) as an original data set.

Centralization of all original data sets (zero averaging):

$$x_j^{(i)} \leftarrow x_j^{(i)} - \frac{1}{m}\sum_{i=1}^{m} x_j^{(i)} \tag{4}$$

Calculate the covariance matrix of the original data:

$$C = \frac{1}{m} X X^T \tag{5}$$

Find the eigenvalue of the covariance matrix C and its corresponding eigenvector;

The eigenvectors are arranged into matrices according to the corresponding eigenvalues in descending order, and the first k rows are taken to form the matrix P .

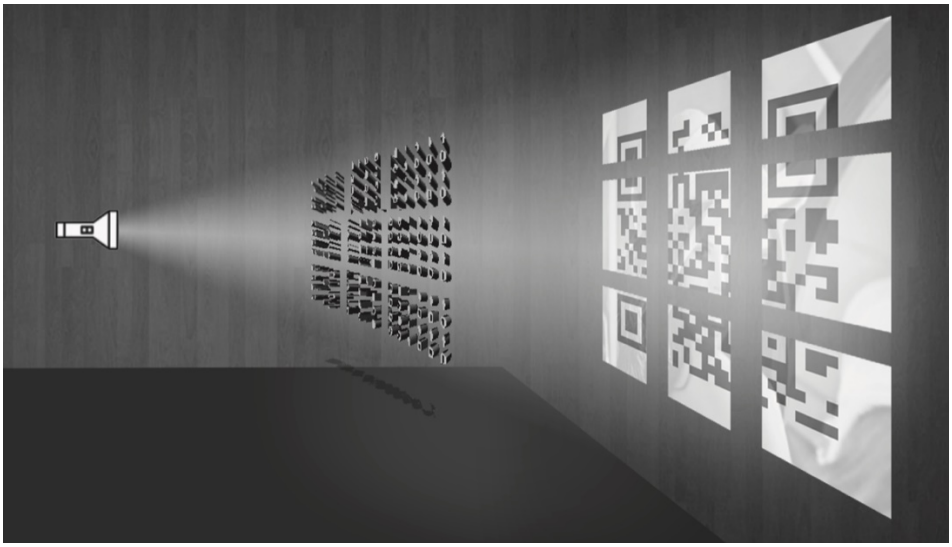

Fig. 5. Image Segmentation using PCA

We use the PCA algorithm in this paper to measure and select the two columns with the highest contribution value in the longitudinal direction of the matrix as the two cutting points. The theory of acquisition of the image's transverse cutting point is the same as that of the longitudinal cutting point. We just need to transpose and do another calculation of the scrambled QR code information matrix. The matrix can be divided into nine parts using four cutting sites as the dividing points of the cutting matrix. Then, after pixel fusion, we project this matrix's block position to the QR code image and guide the split QR code image into blocks. (The method used in this paper is merely a method of calculation and has no physical significance.) QR code images, color images, and fusion images may be the images described in this section. We use the gray image in this paper after the fusion of the pixels.

2.1.5 Secret Information Embedding

We first specify a set of SEL before embedding secret information into each small block of image, and embed the center block obtained by partitioning in SEL. After that, we perform BCH error correction coding on the secret information that needs to be hidden and then use STC[23] hiding algorithm to hide the secret information in every other image block according to SEL embedding logic.

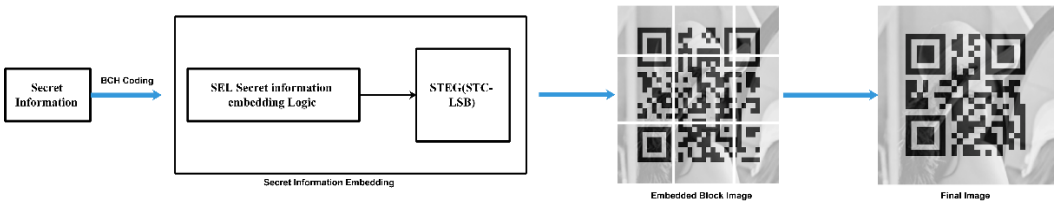

Fig. 6. Secret Information Embedding Process

STC algorithm is a steganographic model that minimizes embedded distortion. The principle is to find a path where the secret information is embedded with the least distortion through the Viterbi algorithm. Then the secret information is hidden in the carrier along this path to obtain the carrier containing the secret information. This algorithm does not directly embed secret information into the carrier, instead, it calculates the distortion of the original carrier after embedding the secret information to find an optimal hidden path before hiding the secret information. As a result, it can minimize the overall embedding distortion in the process of embedding secret information. In the method proposed in this paper, the STC algorithm is used to embed secret information in the lowest bit plane of a grayscale image. Its approach is as follows:

Introduce two binary vectors $X=(x_1,\cdots,x_n), Y=(y_1,\cdots,y_n)\in(0,1)^n$, X represents the carrier image, Y stands for a carrier image containing secret message.

Find a target vector Y such that $Hy^T=m$, and satisfy $D(x,y)$ minimum. Where m is the secret information to be hidden. $D(x,y)$ is the distortion caused by information hiding in the carrier, that is, the cost, defined as:

$$D(x,y)=\sum_{i=1}^{n}\rho_i\left|x_i-y_i\right| \tag{6}$$

In order to ensure use the number of changes in the sample value to reflect the embedding cost $D(x,y)$, the cost required to change x_i to embed a message ρ_i is always 1.

Find the sequence y that minimizes D through the Viterbi algorithm. Along the best path, the secret information is embedded in the lowest bit plane of the carrier image, that is, the secret message carrier image Y after the secret message m is embedded.

After the above steps, a fusion QR code image with secret message is finally formed. With a common scanner, this QR code image can be scanned to get public information, and the actual secret message is concealed in the image.

2.2 Extraction Process of Secret Message

In the extraction process, the user extracts the information by using the obtained secret key or uses a dedicated device to process the encrypted fusion QR code image to extract the encrypted information. The matrix transformation module and the image segmentation module in this process have the same processing methods as the secret information hiding process.

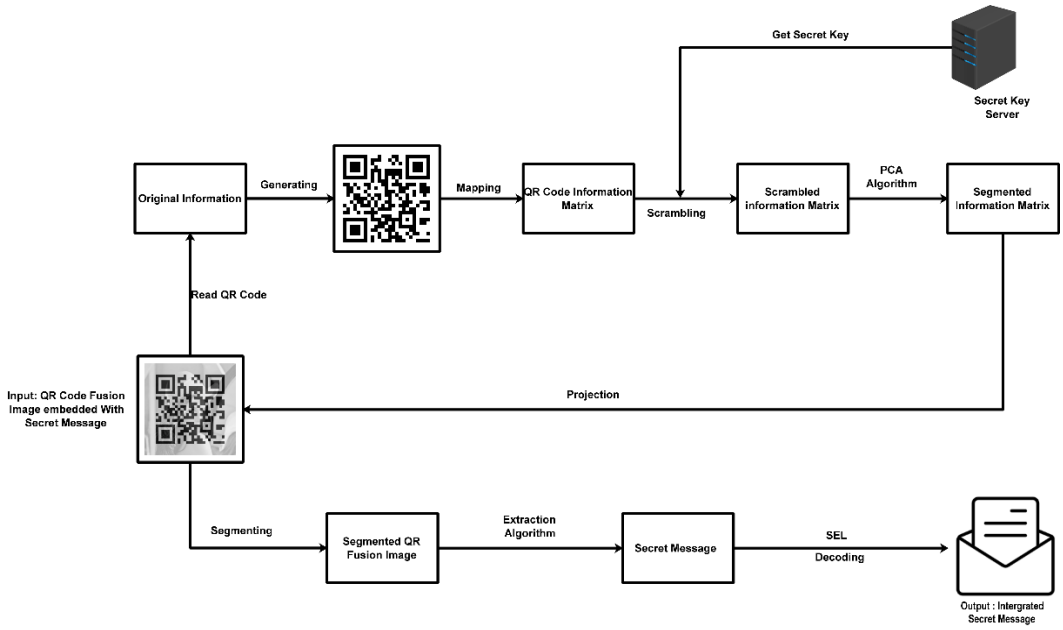

Fig. 7. Extraction Process of Secret Message

2.2.1 Extract QR Code from The Fusion Image

First, the user obtains a fusion QR code image containing secret information and scans it with a common scanner to get the content of the QR code. Then the user uses the original ZXing library to generate a QR code image which is the same as the originally standard QR code image.

2.2.2 Generate The Secret Key

After obtaining the original QR code image, convert it into a QR code information matrix, before authorizing the user to obtain the key through the server. That is, the logistic algorithm private key μ, X_0 in the matrix transformation process, the hidden parameter h of the STC algorithm and the length L of the secret information needed in the secret information extraction process matrix. In order to carry out the correct matrix transformation and secret information extraction.

2.2.3 Matrix Scrambling

The authorized user obtains the logistic algorithm private key μ, X_0 in the key, and performs the same scrambling on the two-dimensional code (0,1) information matrix as in the secret information hiding process to obtain a transformed two-dimensional code information matrix.

2.2.4 Image Segmentation

The authorized user uses the matrix block algorithm (PCA algorithm, etc.) to execute the transformed QR code information matrix. According to the position calculated by the PCA algorithm, the scrambled QR code information matrix can be divided into segments to obtain a block matrix. By doing so, the authorized user can calculate the block information of the matrix, thus he can get the blocked method of the image.

2.2.5 Secret Message Extraction

The authorized user processes the fusion QR code image containing secret information (Art-like QR code image embedded with secret message) after specifying the blocked method. First the central block should be read to get SEL parameter. Then the secret information in each image block can be extracted according to the SEL embedding logic traversal. Finally all of these are combined into a complete secret message.

3. Experimental Results

3.1 Image Quality

The proposed method is simulated using Matlab R2018b. Operating environment is CPU: Intel i7 7500U, running memory is 16GB. For experiment, the objective analysis PSNR, SSIM, NPCR, MSE is first used to evaluate the performance of the proposed method. Then we compared our proposed method with Hugo, S-UNIWORD, LSB algorithms in the same indicators with a various payload.

NPCR measures the percentage of different pixels in two images. If the number measured by NPCR is lower, the two images are more similar[24， 26].

Suppose two images x, y whose i , j are the horizontal and vertical indices of pixels in both images. Define an Array $D_{i,j}=0$, if $X_{i,j}=Y_{i,j}$, otherwise $D_{i,j}=1$. The NPCR is defined as[25, 27]:

$$NPCR=\frac{1}{H\times W}\sum_{i,j}D_{i,j}\times 100\% \tag{7}$$

where H, W are the dimensions (size) of the image.

Then, using peak signal-to-noise ratio (PSNR) and structural similarity index (SSIM), we compare the proposed system, STC-LSB, Hugo, S-UNIWORD and LSB.

PSNR is the ratio of the maximum value of an image to the difference between the image and its steganographic version. The larger the ratio is, the less distortion of the stego-image and the better the quality we can obtain[28, 29].

$$PSNR=10\times\log_{10}\frac{(2^n-1)^2}{MSE} \tag{8}$$

where is the bit depth, and the grayscale image used in this paper has a value of 8. MSE is the mean square error, and the quality after image processing is calculated. The most direct

idea is to compare the difference profile between the processed image and the real image, that is, the visibility of errors, and to evaluate the image quality through visual errors. MSE is an indicator based on this simple and direct idea.

MSE represents the mean square error (Mean Square Error) of the current image X and the reference image Y. H and W are the height and width of the image. The calculation formula is as follows：

$$MSE = \frac{1}{H \times W} \sum_{i=1}^{W} \sum_{j=1}^{H} (X_{i,j} - Y_{i,j})^2 \tag{9}$$

The structural similarity index (SSIM) is another tool that can be used to measure the similarities between the original image and the stego image. It ranges from 0 to 1, and 1 means that both images are identical. It is expressed as followed, shown in[24, 30].

$$SSIM = \frac{(2m_o m_s + c_1)(2\sigma_{os} + c_2)}{(m_o{}^2 m_s{}^2 + c_1)(\sigma_o{}^2 + \sigma_s{}^2 + c_2)} \tag{10}$$

Where m , m^2 and σ are the mean, variance and the standard deviation of the image. The subscripts o, s , represent the original and QR code fusion image respectively. σ_{os} is the covariance between both images. The constants c_1, c_2 equal to $c_1 = k_1 L$ and $c_2 = k_2 L$ receptively where $k_1 = 0.01$, $k_2 = 0.03$ and $L = 255$ is the maximum value of the grayscale image. The embedding capacity is the maximum size of the payload that can be successfully embedded in the container. When the embedding rate is 0.1, the results are shown in the table:

Table 1. PSNR, SSIM, NPCR and running time comparison

System	PSNR	SSIM	NPCR	Time(s)
Proposed method	66.3088	0.9998	0.0152	0.2158
Hugo	65.3705	0.9998	0.0188	12.2894
S-UNIWORD	65.8761	0.9999	0.0168	0.5946
LSB	61.1443	0.9993	0.0499	0.3238

It can be seen that the algorithm proposed in this paper has the highest PSNR and the lowest NCPR compared to several airspace steganography algorithms commonly used in the table. At the same time, the running time of the algorithm framework proposed in this paper is also the shortest and has lower complexity.

3.2 Anti-steganography Analysis

To test the anti-steganography analysis of our proposed system, In this part of experiments, we use ZXing to generate 6000 QR code images and use 6000 natural images of BOSSbase1.01[31] to produce 6000 texture-enhanced QR code images and embed random secret bits to these texture-enhanced images from 0.1 to 0.5bpac. Then we use spam686[32] to extract the 686-dimensional features of these images and use Linear classifier[33] to make a classification. The security of steganographic algorithm is evaluated by Minimum average misclassification rate P_E .

$$P_E = \min_{P_{FA}} \frac{P_{FA} + P_{MD}(P_{FA})}{2} \tag{11}$$

P_{FA} is represents probability of false-alarm, P_{MD} is represents probability of missed detection. The larger the P_E, the higher the probability of error detection by steganographic analysis, that is, the stronger the ability of the steganographic algorithm to resist steganographic analysis. It is generally believed that if P_E is greater than 0.4, the detection resistance of the method meets the requirements. The results are shown in the figure.

Table 2. Probability of missed detection comparison

Embedding probability	STC-LSB in 'PROMISE'	Stand-alone STC-LSB	Stand-alone LSB
0.1	0.4580	0.4105	0.1282
0.2	0.3604	0.3045	0.0483
0.3	0.2033	0.1800	0.0275
0.4	0.0810	0.0850	0.0196
0.5	0.0480	0.0455	0.0129

As it can be seen from the results in the table. Under the condition that the embedding rate is 0.1, the method we proposed has a high anti-detection performance and can effectively resist spam686 steganography detection. Under the condition that the embedding rate is 0.1 bpac, the actual number of embedded secret message bits is 16000 bits, which can fully meet the needs of hidden communication. And by using our framework, the anti-steganography detection ability improves comparing with using STC-LSB alone, and small effect achieves on the operating speed of the system.

3.3 System Gain Evaluation

In this part, we analysis the system gains by using the method we proposed, especially in key-space. Key space is the value range of the key. Alvarez et al.[34] suggest that the key space of the encryption system is at least 2^{100} to be safe enough.

3.3.1 Matrix Scrambling

Logistic scrambling key space: The encryption algorithm in this article actually uses the initial key from the initial value of the Logistic project x_0 and the parameter value μ. Since these values are both double-precision real numbers, the maximum accuracy is desirable to be 10^{-15}. And because of the parameter value of the Logistic project $\mu \in (3.6, 4)$. Therefore, the key space of logistic encryption algorithm in this paper is $0.5 \times 10^{15} \times 10^{15}$.

Key sensitivity: The matrix scrambling algorithm used in this article is very sensitive to key changes. When the amount of key change is only $\nabla = 10^{-15}$, the correct QR code information matrix is still not available. It can be seen that even if the key changes slightly, the resulting information matrix is still very different from the original information matrix, and the resulting image cutting site cannot be calculated. It shows that the algorithm has good key sensitivity.

3.3.2 Image Segmentation

After obtaining the split location, SEL embedding logic is added to the system, which makes the embedding scheme of secret information very flexible. Users can choose to embed secret message in any number and order in blocks 1, 2, 3, 4, 6, 7, 8, 9. Key space can be increased

by $A_8^1 \times A_8^2 \times A_8^3 \times A_8^4 \times A_8^5 \times A_8^6 \times A_8^7 \times A_8^8$ when segmenting is added. In summary, the system's overall key space can reach 10^{55}, and far greater than 2^{100}, enough to withstand violent attacks such as exhaustive attacks. In addition, the H-matrix height parameter in the STC hiding algorithm is also part of the key, and calculations are not included here.

4. Conclusion

This paper proposes a novel QR code information hiding framework: PROMISE, image segment information hiding based on the projection matrix of QR code. Experimental results show that the method proposed in this paper has the characteristics of high information hiding capacity, small image distortion, and strong anti-steganographic detection, compared to other QR code image information hiding methods. Furthermore, the key space expands greatly due to the addition of scrambling and segmenting. Even if the carrier is intercepted by the opponent, the secret information cannot be obtained without getting the private key entirely, which ensures the security of the secret information.

Any code scanner can obtain the information content of the QR code, but only authorized users with keys can access hidden secret messages successfully. Meanwhile, with others, the PROMISE framework is NOT isolated so that it could be combined with other algorithms of steganography and cryptography. The framework pioneers the way to use the QR code features to guide image segmentation for information hiding, which greatly enhances the flexibility of embedding secret information and maintains the QR code's readability. In matrix transformation & image segmentation, secret information embedding logic and secure key sharing strategy, future work will be improved and perfected. On the hardware, the whole framework would be applied as the system functions are implemented step by step.

However, there are still some limitations with this method proposed in our paper where SEL that is adopted uses some kinds of simple logistic algorithms. And the secret key uploaded to the server is essential for message extraction. Further work has been carried on about secret information embedding logistic and secret key-free scheme.

References

[1] Information Technology—Automatic Identification and Data Capture Techniques—Data Matrix Bar Code Symbology Specification. International Standard.

[2] Information Technology—Automatic Identification and Data Capture Techniques—PDF417 bar code symbology specification. International Standard.

[3] Information Technology—Automatic Identification and Data Capture Techniques—Bar Code Symbology—QR Code. International Standard.

[4] Q. Y. Wang and H. B. Dong, "Book retrieval method based on QR code and CBIR technology," *Journal on Artificial Intelligence*, vol. 1, no. 2, pp. 101–110, 2019. Article (CrossRef Link)

[5] S. Falkner, P. Kieseberg, D. Simos, C. Traxler and E. Weippl, "E-voting Authentication with QR-codes," in *Human Aspects of Information Security, Privacy, and Trust,Lecture Notes in Computer Science*, Springer, 8533, pp. 149-159, 2014. Article (CrossRef Link)

[6] H. C. Lee, C. R. Dong and T. M. Lin, "Digital Watermarking Based on JND Model and QR Code Features," *Advances in Intelligent Systems and Applications*, Vol. 2, pp, 141-148, 2013. Article (CrossRef Link)

[7] Information Technology—Automatic Identification and Data Capture Techniques—QR Code 2005 Bar Code Symbology Specification. International Standard.

[8] H. Kato, K. T. Tan, D. Chai and Cambridge U. K. C. U.: Barcodes for Mobile Devices. ZXing. http://zxingnet.codeplex.com/, 2010.
[9] M. S. Rewatkar and S. A. Raut, "Survey on Information Sharing Techniques Using QR Barcode," *International Journal on Cryptography and Information Security (IJCIS)*, vol. 4, no. 3, pp. 13–20, 2014. Article (CrossRef Link)
[10] L. P. Yu, C. Y. Hui, L. J. Lin and C. P. Jung, "Secret Hiding Mechanism Using QR Barcode," in *Proc. of the 2013 International Conference on Signal-Image Technology & Internet-Based Systems*, 2013. Article (CrossRef Link)
[11] 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. Article (CrossRef Link)
[12] T. Yuan, Y. Wang, K. Xu, R. R. Martin and S. M. Hu, "Two-Layer QR Codes," *IEEE Transactions on Image Processing*, vol. 28, no. 9, pp. 4413-4428, 2019. Article (CrossRef Link)
[13] Y. Cheng; Z. Fu and B. Yu, "Improved Visual Secret Sharing Scheme for QR Code Applications," *IEEE Transactions on Information Forensics & Security*, vol. 12, no. 9, pp. 2393-2403, 2018. Article (CrossRef Link)
[14] Y. W. Chow, W. Susilo, G. Yang and et al., "Exploiting the Error Correction Mechanism in QR Codes for Secret Sharing," in *Proc. of Australasian Conference on Information Security and Privacy*, Springer, Cham, pp. 409-425, 2016. Article (CrossRef Link)
[15] C. Chen, M. Li, A. Ferreira, J. Huang and R. Cai, "A Copy-Proof Scheme Based on the Spectral and Spatial Barcoding Channel Models," *IEEE Transactions on Information Forensics & Security*, vol. 15, pp. 1056-1071, 2019. Article (CrossRef Link)
[16] L. P. Yu and C. Y. Hui, "QR code steganography with secret payload enhancement," in *Proc. of IEEE International Conference on Multimedia & Expo Workshops (ICMEW)*, IEEE, pp. 1-5, 2016. Article (CrossRef Link)
[17] W. Yan, Y. Yao, W. Zhang, et al., "Privacy-preserving scheme for logistics systems based on 2D code and information hiding," *Chinese Journal of Network and Information Security*, vol. 3, no. 11, pp. 22-28, 2017. Article (CrossRef Link)
[18] G. Ravikanth, K. V. and B. E. Reddy, "Location related signals with satellite image fusion method using visual image integration method," *Computer Systems Science and Engineering*, vol. 35, no.5, pp. 385–393, 2020.
[19] R. Meng, Q. Cui, Z. Zhou, C. Yuan and X. Sun, "A novel steganography algorithm based on instance segmentation," *Computers, Materials & Continua*, vol. 63, no. 1, pp. 183–196, 2020. Article (CrossRef Link)
[20] Y. Luo, J. Qin, X. Xiang, Y. Tan and Z. He, "Coverless image steganography based on image segmentation," *Computers, Materials & Continua*, vol. 64, no. 2, pp. 1281–1295, 2020. Article (CrossRef Link)
[21] Z. Guo and J. Yang, "2-Dimension Projection Feature Extracting Ability Research Based on Image Module," *Computer Simulation*, vol. 27, no. 4, pp. 228-231, 2010. Article (CrossRef Link)
[22] Rongyu Chen, Lili Pan, Yan Zhou and Qianhui Lei, "Image Retrieval Based on Deep Feature Extraction and Reduction with Improved CNN and PCA," *Journal of Information Hiding and Privacy Protection*, vol. 2, no. 2, pp. 9-18, 2020. Article (CrossRef Link)
[23] T. Filler, J. Judas and J. Fridrich, "Minimizing Additive Distortion in Steganography Using Syndrome-Trellis Codes," *IEEE Transactions on Information Forensics & Security*, vol. 6, no. 3, pp. 920-935, 2011. Article (CrossRef Link)
[24] A. K. Sahu and G. Swain, "A Novel n-Rightmost Bit Replacement Image Steganography Technique," *3D Research*, vol. 10, no. 2, 2019. Article (CrossRef Link)
[25] N. El-Fishawy and O. M. A. Zaid, "Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms," *International Journal of Network Security*, vol. 5, no. 3, pp. 241-251, 2007. Article (CrossRef Link)
[26] A. K. Sahu and G. Swain, "Dual Stego-imaging Based Reversible Data Hiding Using Improved LSB Matching," *International Journal of Intelligent Engineering and Systems*, vol. 12, no. 5, pp. 63-74, 2019. Article (CrossRef Link)

[27] S. Li, G. Chen, and X. Zheng, "Chaos-based encryption for digital images and videos," *Multimedia Security Handbook*, vol. 4, pp. 133-167, 2004.
[28] A. K. Sahu and G. Swain, "An Optimal Information Hiding Approach Based on Pixel Value Differencing and Modulus Function," *Wireless Personal Communications*, vol. 108, no. 1, pp. 159-174, 2019. Article (CrossRef Link)
[29] A. K. Sahu and G. Swain, "High Fidelity based Reversible Data Hiding using Modified LSB Matching and Pixel Difference," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 4, pp. 1395-1409, 2022. Article (CrossRef Link)
[30] G. Swain and A. K. Sahu, "A Novel Multi Stego-image based Data Hiding Method for Gray Scale Image," *Pertanika Journal of ence and Technology*, vol. 27, no. 2, pp. 753-768, 2019.
[31] P. Bas, T. Filler and T. Pevný, ""Break Our Steganographic System": The Ins and Outs of Organizing BOSS," in *Proc. of the 13th international conference on Information hiding*, Springer Berlin Heidelberg, pp. 59-70, 2011. Article (CrossRef Link)
[32] T. Pevny, P. Bas, and J. Fridrich, "Steganalysis by Subtractive Pixel Adjacency Matrix," *IEEE Transactions on Information Forensics & Security*, vol. 5, no. 2, pp. 215-224, 2010. Article (CrossRef Link)
[33] R. Cogranne and J. Fridrich, "Modeling and Extending the Ensemble Classifier for Steganalysis of Digital Images Using Hypothesis Testing Theory," *IEEE Transactions on Information Forensics & Security*, vol. 10, no. 12, pp. 2627-2642, 2015. Article (CrossRef Link)
[34] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation & Chaos*, vol. 16, no. 8, pp. 2129-2151, 2006. Article (CrossRef Link)

YIXIANG FANG received the B.Sc. degree from Harbin Institute of Technology, China, in 2009 and the M.S. degree in 2012. And he has been with the faculty of the School of Mechanical and Electronic Engineering, Jingdezhen Ceramic Institute. His current research interests include privacy preservation information hiding, digital forensics and multimedia security.

KAI TU received the B.S. degree from Jingdezhen Ceramic institute and he is currently pursuing M.S. degree in The Pennsylvania State University. His research interests include privacy preservation information hiding, system and network security.

KAI WU is currently pursuing the B.S. degree with Jingdezhen Ceramic institute and he plans to pursue Ph.D. degree in Computer Science in the future. His research interests include data hiding, image processing and information security.

YI PENG received the B.S. degree from Jingdezhen Ceramic institute and he is currently pursuing M.S. degree in Jingdezhen Ceramic institute. Her research interests include steganography, information hiding and image processing.

YUNQING SHI (Life Fellow, IEEE) received the M.S. degree from Shanghai Jiao Tong University, China, and the Ph.D. degree from the University of Pittsburgh, USA. He has been with the New Jersey Institute of Technology, USA, since 1987. He has authored/coauthored more than 300 articles, one book, and five book chapters. He was an Editor of ten books, three special issues, and 13 proceedings. He holds 30 U.S. patents. His research interests include data hiding, forensics and information assurance, visual signal processing, and communications. He is a member of a few IEEE technical committees. He was the Technical Program Chair of IEEE ICME 2007 and IEEE MMSP 2005, the Co-General Chair of IEEE MMSP02, and a Distinguished Lecturer of IEEE CASS. He has been the Co-Technical Chair of IWDW since 2006. He has served as an Associate Editor for the IEEE TRANSACTIONS ON SIGNAL PROCESSING and the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—II: EXPRESS BRIEFS. He serves as an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, and an editorial board member for a few journals.