*Advances in Intelligent Systems Research, volume 133*
2nd International Conference on Artificial Intelligence and Industrial Engineering (AIIE2016)

# Secure QR Code Scheme Based on Visual Cryptography

Xiaohe Cao, Liuping Feng*, Peng Cao and Jianhua Hu
Beijing Key Laboratory of Signal and Information Processing for High-end Printing Equipments, Beijing Institute of Graphic Communication, Beijing, China
*Corresponding author

***Abstract*—With the wide application of QR code, the security problem of QR code is serious, such as information leakage and data tampering. In order to solve the QR information security problem, this paper proposed a secure QR code schema based on visual cryptography. The QR code is divided into two share images that can be transmitted separately. The generation of the two share images is based on the pseudo-random matrix, that is, the pixels in the two share images are determined by the corresponding values in the pseudo-random matrix. The two share images can be stacked simply to restore the information. Simulation results show that the QR code image can be well hidden, and it can be restored effectively.**

***Keywords-QR code; visual cryptography; secret sharing; pseudo-random modulation***

## I. INTRODUCTION

In recent years, the QR code is widely used. First, the QR code is easy to be computer equipment identification, for example, mobile phones, scanning guns. Second, QR code has a large storage capacity, anti-damage strong, cheap and so on. Because of the advantages of the QR code, it is used in many areas. Train ticket real-name authentication uses QR code to approve identity. In the supermarket, commodity packaging is now also in the application of QR code to distinguish true or false. Scanning the QR code to pay attention to WeChat public number or download App. Now, QR code is the most popular application. And the mainstream mode of payment is to complete the Alipay or WeChat pay by scanning the QR code. QR code logos are almost full of our lives anywhere. With the wide application of QR code, the security problem of QR code is serious, such as information leakage and data tampering. The coding rules of the QR code are gradually being familiar to the researchers. Some attackers according to the encoding rules forged the same code for the QR code pattern through illegal operation. For example, the pirates can obtain personal information (such as name, ID number) just through the waste real-name system of train tickets, then they can forge a same code pattern ticket with the same encoding to pass the ticket verification. The use of QR code is no longer safe. Therefore, in order to make the QR code authentication more safe and reliable to use, the introduction of new technology is urgently needed. Many researchers are devoted to study the safe and reliable QR code authentication.

S. Khairnar proposed a new authentication scheme for secure OTP(One Time Password) distribution in phishing website detection through EVC(extended visual cryptography) and QR codes[1]. S. Khairnar used extended visual cryptography technique to solve the problem of phishing and done the relevant validation. The method of visual encryption combined with QR code is mentioned more than once. A lot of researchers have done the experiment to confirme the feasibility of this method. M.A. Kute, Ms. Ashvini, and M. D. Deokar described a scheme using the visual cryptography and QR code in their paper[2]. S. Falkner, P. Kieseberg, D. E. Simos proposed an e-voting authentication scheme[3]. This approach is based on visual cryptography as the work frame and also combined with QR codes, focusing on the usability. D Li, Z Liu, and LH Cui proposed scheme for identification photos based on QR Code and Visual Cryptography[4]. The visual cryptography scheme is applied to generate the secret images from the feature values in their research.

Visual cryptography is a new secret sharing technology. It improves the secret share images to restore the complexity of the secret, relying on human visual decryption. Compared with traditional cryptography, it has the advantages of concealment, security, and the simplicity of secret recovery. The method of visual cryptography provided high security requirements of the users and protects them against various security attacks. It is easy to generate value in business applications.

In this paper, we proposed a secure QR code scheme to protect the user's information not be stolen using visual encryption technology. The scheme can be applied in the fields of document management, customs security system, medical medicine and other fields.

The organization of this paper is as follows. In Section II, we explained the basic principles and methods of visual cryptography technology. We proposed the security QR code scheme based on visual cryptography in Section III, and evaluated the performance through experimental results in Section IV. Finally, we concluded this paper in Section V.

## II. VISUAL CRYPTOGRAPHY

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by human visual without the aid of computers [5]. In 1994, M. Naor and A. Shamir firstly introduced visual cryptography and provided their constructions of visual cryptographic solutions for the general k out of n secret sharings problem at their paper[6].

Visual cryptography scheme is a method to encode a secret image into n noise-like shadow images called share images,

and the share images need some processing to reconstruct the secret image[7]. The detailed principle of visual encryption is that the secret image is divided into several share images by cryptographic operations and distributed to different participants. The pixels of each share image appear to be randomly distributed[8]. Decryption is possible by stacking an adequate number of shares. The secret image will be revealed and can be decoded by the human visual system (HVS) on the condition of the absence of any complicated computation or replacement algorithms[7]. Moreover, no knowledge of sophisticated cryptographic techniques is needed for the encryption and decryption processes. However, the secret image will be invisible if the number of stacked shares is less than t. This is so called (t,n)-threshold visual cryptography scheme ((t,n)-VCS)[9].

Consider the simplest two-out-of-two visual threshold scheme where each pixel of the image is encoded into a pair of subpixels in each of the two shares. If the pixel is white, one of the two columns tabulated under the white pixel in Fig. I. is selected. If the pixel is black, one of the two columns tabulated under the black pixel is selected. In each case, the selection is performed by randomly flipping a fair coin, such that each column has equal probability to be chosen. Then, the first two pairs of subpixels in the selected column are assigned to share A and share B, respectively[10]. Now consider the superposition of the two shares as shown in the last row of Fig. I.

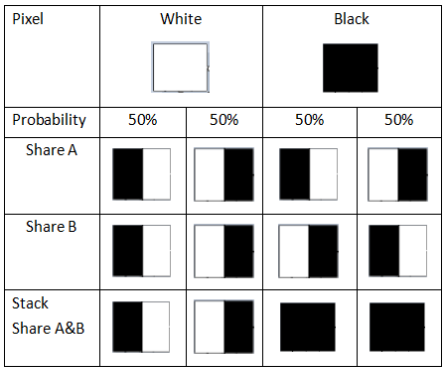


FIGURE I. CONSTRUCTION OF A TWO-OUT-OF-TWOVC SCHEME: A SECRET PIXEL CAN BE ENCODED INTO TWO SUBPIXELS IN EACH OF THE TWO SHARES

The greatest advantage of this decryption process is that it is only through the human vision system. No complex computations and knowledge of Visual Cryptography Scheme is required.

In the visual encryption scheme proposed by Naor and Shamir, share image A pixels in the basic matrix are randomly selected, while share image B pixels are to select the other basic matrix. These two basic matrices are a pair of. The result of their encryption is to generate two gray images, which can not see the original image information of the two images. So the information in secret images can not be obtained.

## III. THE NEW SCHEME OF VISUAL CRYPTOGRAPHY ON THE QR CODE SECURITY

In this section, We will introduce our secure QR code scheme. In order to hide the QR code information, we proposed an improved visual encryption technology based on the existing visual encryption technology to realize the concealment of the QR code pattern. Through this method of encryption, the information hidden in QR code is more difficult to be accessed by forgers. So as to achieve the purpose of hidden information more secure.

The QR code with hidden information is the original secret image, using a special encryption method that pseudo-random matrix combined with visual cryptography algorithm to generate two shared images. Steps are as follows.

### *A. The Collections of the Encoding Matrices $C_0$ and $C_1$*

The two collections of the encoding boolean matrices $C_0$ and $C_1$, respectively, representing a white pixel and a black pixel of the original secret image.

### *B. Generation of a Pseudo-Random Matrix*

Generate a pseudo-random matrix of the same size as the original secret image, which is in the range of 0~3, each value corresponds to the basic matrix of $C_0$ and $C_1$ , respectively.

The basic matrix in $C_1$ is XORed by the basic matrix in $C_0$ and the all-1 matrix.

### *C. Selection of the Basic Matrix*

The pixel matrix of the share image is the basic matrix selected from $C_0$ or $C_1$, but the chosen rule is determined by the participation of the pseudo-random matrix.

*a)* When generating the share image A, the rule as follows: the position of pixel (including white pixels and black pixels) in the secret image are mapped to the corresponding position in the pseudo-random matrix, and then selected the corresponding basic matrix from $C_0$ according to the value in the pseudo-random matrix.

*b)* When generating the share image B, the rule is slightly different when white pixels and black pixels mapped to the pseudo-random matrix.

If the case of white pixel, the rule is as follows: the position of the white pixel in the secret image is mapped to the corresponding position in the pseudo-random matrix, and then the corresponding basic matrix is selected from the $C_0$ according to the value in the pseudo-random matrix.

In the case of a black pixel, the rule is as follows. The position of the black pixel in the secret image is mapped to the corresponding position in the pseudo-random matrix, and the corresponding basic matrix is selected from $C_1$ according to the value in the pseudo-random matrix.

### *D. Reconstructed Secret Image*

In the reconstructed secret image, a white or black pixel in the original secret image is represented by one sub-pixel.

The basic matrices of the collections of the encoding matrices $C_0$ and $C_1$ are as follows:

$$C_0 = \left\{ \begin{bmatrix} 0&1&0&1 \\ 1&0&1&0 \\ 0&1&0&1 \\ 1&0&1&0 \end{bmatrix} \begin{bmatrix} 0&1&1&0 \\ 1&0&0&1 \\ 0&1&1&0 \\ 1&0&0&1 \end{bmatrix} \begin{bmatrix} 1&0&1&1 \\ 0&1&0&1 \\ 1&0&1&0 \\ 0&1&0&0 \end{bmatrix} \begin{bmatrix} 0&1&1&0 \\ 1&0&0&1 \\ 1&0&0&1 \\ 0&1&1&0 \end{bmatrix} \right\}$$

$$C_1 = \left\{ \begin{bmatrix} 1&0&1&0 \\ 0&1&0&1 \\ 1&0&1&0 \\ 0&1&0&1 \end{bmatrix} \begin{bmatrix} 1&0&0&1 \\ 0&1&1&0 \\ 1&0&0&1 \\ 0&1&1&0 \end{bmatrix} \begin{bmatrix} 0&1&0&0 \\ 1&0&1&0 \\ 0&1&0&1 \\ 1&0&1&1 \end{bmatrix} \begin{bmatrix} 1&0&0&1 \\ 0&1&1&0 \\ 0&1&1&0 \\ 1&0&0&1 \end{bmatrix} \right\}$$

The principle of pixel superposition based on AND in this scheme is shown in Fig. II

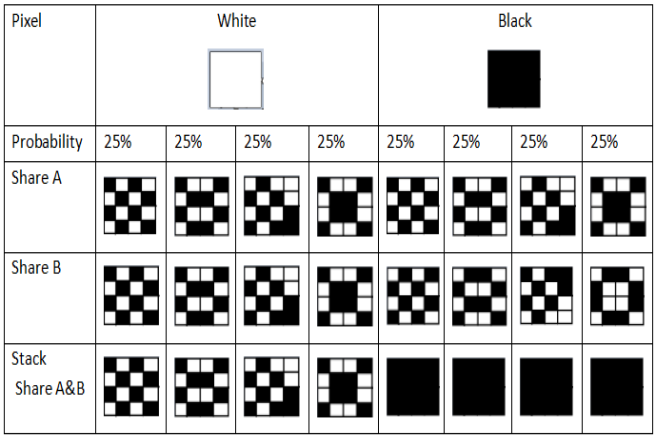


FIGURE II. CONSTRUCTION OF A TWO-OUT-OF-TWO SCHEME OF THIS PAPER: A SECRET PIXEL CAN BE ENCODED INTO TWO SUBPIXELS IN EACH OF THE TWO SHARES

In this scheme, secret share images A and B are generated by using the visual cryptography scheme based on the AND operation. From the basic principle of the visual cipher and the nature of the operation, the two share images A and B can be used to recover the secret image.

The share images generated in this scheme are related to the pseudo-random matrix. Pixels in Share image A are randomly selected from the basic matrix, and the pixels in share image B are also generated from the basic matrix as described above. Even if the basic matrix is obtained by them, the attacker can neither break the encrypt nor obtain the secret information. However, the stacked secret image had a contrast loss compared with the original secret image. A basic matrix replaced a pixel in the original image that caused this phenomenon. This is normal, and it is expected to be the result of the experiment. The size of the share images and the stacked secret image expanded to four times compared with the original image. It also related to the replacement of pixels. Because a pixel of the original image is replaced by a basic matrix of $4\times4$, so the share images and the QR image after overlay recovery would be four times as much as the original secret image.

## IV. EXPERIMENTAL RESULTS AND ANALYSIS

Based on the process described above, we constructed a two-out-of-two visual cryptography experimental scheme. This experiment is based on MATLAB platform. The original image is a 120×120 binary QR image, it is as shown in Fig III. (a).

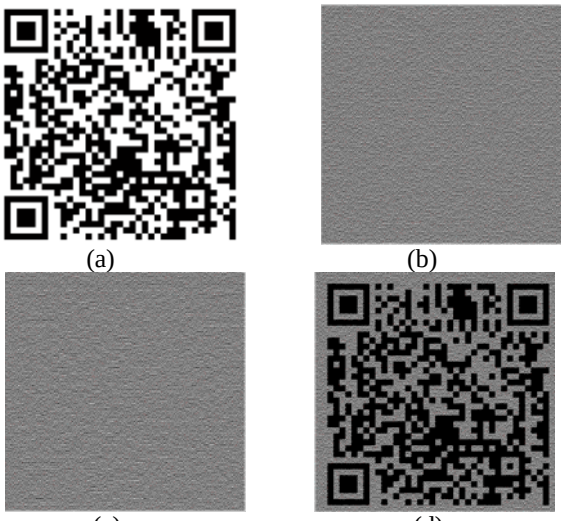


FIGURE III. TWO-OUT-OF-TWO VC SCHEME: (A) THE SECRET IMAGE WAS ENCODED INTO (B), (C) THE TWO SHARES, AND WAS (D) DECODED BY SUPERIMPOSING THESE TWO SHARES WITH 50% LOSS OF CONTRAST. (A) SECRET IMAGE. (B) SHARE A. (C) SHARE B. (D) DECODED IMAGE

Encoding the QR code in Fig III (a) through our scheme, you can get the two shares shown in Fig. the III. (b) and (c), respectively. Superimposing these two shares leads to the output secret as shown in Fig. III. (d). The decoded image is clearly identified, although some contrast loss is observed. Some binary pixels appeared to be “grey” due to the shrinking of the image for layout purpose. The width of the decoded image is fourth that of the original secret image since each pixel is expanded to sixteen subpixels in each share as shown in Fig. II. This effect is referred to as pixel expansion.

Based on the experimental results, this scheme realized the complete restoration of the secret image at the cost of pixel expansion, which only needed two participants to carry a share image.

From the experimental results, the design of the visual encryption of the security QR code scheme is feasible. But this scheme can still be improved to make it more suitable for market applications.

## V. CONCLUSION

In this paper, we proposed a scheme for information prevention using visual cryptography and QR code techniques. We apply the pseudo-random matrix in the visual cryptography in this scheme, and conduct experiments to verify this scheme’s feasibility. Experiments show that this scheme is efficient. And it also show that this scheme is a reliable method through combining visual cryptography with pseudo-random matrix for detecting attacker. It provided better security for QR code.

In view of the operability of the scheme proposed in this paper, we can apply it to the commercial platform. The share image A of the program can be applied to various products. The possibility of information leakage is very small. And the shared image B is retained by the issuing authority, and the original QR code image can be restored when the two images are subjected to the operation. The share images are meaningless images that are random distribution images of black and white pixels. The attacker using mathematical analysis and other means is unable to determine the original secret image at a point of the pixel is black or white. At the same time, the scheme ensured the safe storage of the customer information of the issuing authority.

## ACKNOWLEDGMENT

This paper is supported by the National Natural Science Funds project, No.61370140; Collaborative Innovation Center of Green Printing & Publishing Technology project, No. PXM2016_014223_000025; Beijing Undergraduate science research project, No. 22150116005/033.

## REFERENCES

[1] S. Khairnar, “Anti-Phishing framework based on Extended Visual Cryptography and QR code,” International Journal of Computer Applications vol. 142, May 2016

[2] M.A. Kute, Ms. Ashvini, and M. D. Deokar, "Modern Method for Detecting Web Phishing Using Visual Cryptography (VC) and Quick Response Code (QR code)," International Journal of Engineering Research & Applications vol.5, 2015

[3] S. Falkner, P. Kieseberg, D. E. Simos, et al. “E-voting Authentication with QR-codes,” Human Aspects of Information Security, Privacy, and Trust. 2014, pp.149-159

[4] D Li, Z Liu, and LH Cui, “A Zero-Watermark Scheme for Identification Photos based on QR Code and Visual Cryptography” , International Journal of Security and Its Applications vol. 10, 2016, pp.203-214

[5] P. S. Revenkar, A. Anjum, and W. Z. Gandhare, "Survey of Visual Cryptography Schemes," International Journal of Security & Its Applications 4.vol. 4, 2010

[6] M. Naor and A. Shamir, "Visual cryptography," Lecture Notes in Computer Science vol.950, 1994, pp.1-12

[7] S. Agrawal, "Impact of Error Filters on Shares in Halftone Visual Cryptography," International Conference on Computer Science, Engineering and Applications , 2012, pp.139-148

[8] L. P. Feng , et al. "A halftone visual cryptography schema using ordered dither," vol.9159, 2014, pp.4177-4180

[9] Y.C. Hou，Z.Y. Quan，C.F. Tsai，D.S. Wang, “(3,n)-Visual Secret Sharing Scheme with Unexpanded Shares”. Chinese Journal Of Computers, vol.39, Mar 2016

[10] Z. Zhou, G. R. Arce, and G. D. Crescenzo. "Halftone visual cryptography." Image Processing, 2003 International Conference on IEEE, I-521-4 .vol.1, 2003