Hindawi
Mobile Information Systems
Volume 2017, Article ID 4356038, 12 pages
https://doi.org/10.1155/2017/4356038

Research Article

Multiple Schemes for Mobile Payment Authentication Using QR Code and Visual Cryptography

Jianfeng Lu,[1] Zaorang Yang,[1] Lina Li,[1] Wenqiang Yuan,[1] Li Li,[1] and Chin-Chen Chang[2]

[1]*Institute of Graphics and Image, Hangzhou Dianzi University, Hangzhou 310018, China*
[2]*Department of Information Engineering and Computer Science, Feng Chia University, Taichung, Taiwan*

Correspondence should be addressed to Li Li; lili2008@hdu.edu.cn and Chin-Chen Chang; alan3c@gmail.com

Received 9 December 2016; Accepted 2 February 2017; Published 23 March 2017

Academic Editor: Ching-Nung Yang

QR code (quick response code) is used due to its beneficial properties, especially in the mobile payment field. However, there exists an inevitable risk in the transaction process. It is not easily perceived that the attacker tampers with or replaces the QR code that contains merchant's beneficiary account. Thus, it is of great urgency to conduct authentication of QR code. In this study, we propose a novel mechanism based on visual cryptography scheme (VCS) and aesthetic QR code, which contains three primary schemes for different concealment levels. The main steps of these schemes are as follows. Firstly, one original QR code is split into two shadows using VC multiple rules; secondly, the two shadows are embedded into the same background image, respectively, and the embedded results are fused with the same carrier QR code, respectively, using XOR mechanism of RS and QR code error correction mechanism. Finally, the two aesthetic QR codes can be stacked precisely and the original QR code is restored according to the defined VCS. Experiments corresponding to three proposed schemes are conducted and demonstrate the feasibility and security of the mobile payment authentication, the significant improvement of the concealment for the shadows in QR code, and the diversity of mobile payment authentication.

1. Introduction

With the rapid development of global wireless networks and the growing popularity of mobile devices, such as mobile phones, tablet PCs, and handheld computers, the user's work and daily life become more and more convenient. Mobile payment as a quick payment way is prevalent in some rising markets [1]. Furthermore, QR code, a new technology of information storage, transferring, and recognition, can be decoded by mobile phone anywhere and thus has been widely used in some security sensitive applications [2] such as payments [3–5].

Now QR code payment becomes one of the most mainstream in the mobile payment market. However, there exist some security risks using this means of payment. For example, QR code is stuck on the wall of one shop, which represents the merchant's beneficiary account. There exists no anticounterfeiting function in QR code. Thus, one cheater can tamper with the private data of QR code using his own bank account without any notification. Thus, the funds are transferred to the attacker's account during each subsequent deal. To further decrease the economic loss of the merchants caused by the described behavior and improve the security of mobile payment authentication process for the general customers, the proposed mechanism in this study is applied to practical scenario as shown in Figure 1. Three primary entities are considered: the shop, cloud server, and mobile phone. The QR code carrying the original secret is split into shadow 1 and shadow 2 on the basis of a (2, 2) VCS. QR_1 is the fusion result of shadow 1 and carrier QR code. The generation of QR_2 is similar to QR_1. Moreover, QR_1 is stored in the cloud server while QR_2 is stuck on the wall of the shop. The mobile phone holder photographs QR_2 and then scans QR_2 to acquire QR_1 from the distributed cloud server. Subsequently, the mobile phone simulates the vision characteristic [6] of VCS to stack QR_1 and QR_2. The original QR code is restored and can be accessed by the holder.

QR code presents some significant features, such as small size and the abilities to carry large and various data (such as images, text, symbols, and other types of information). These

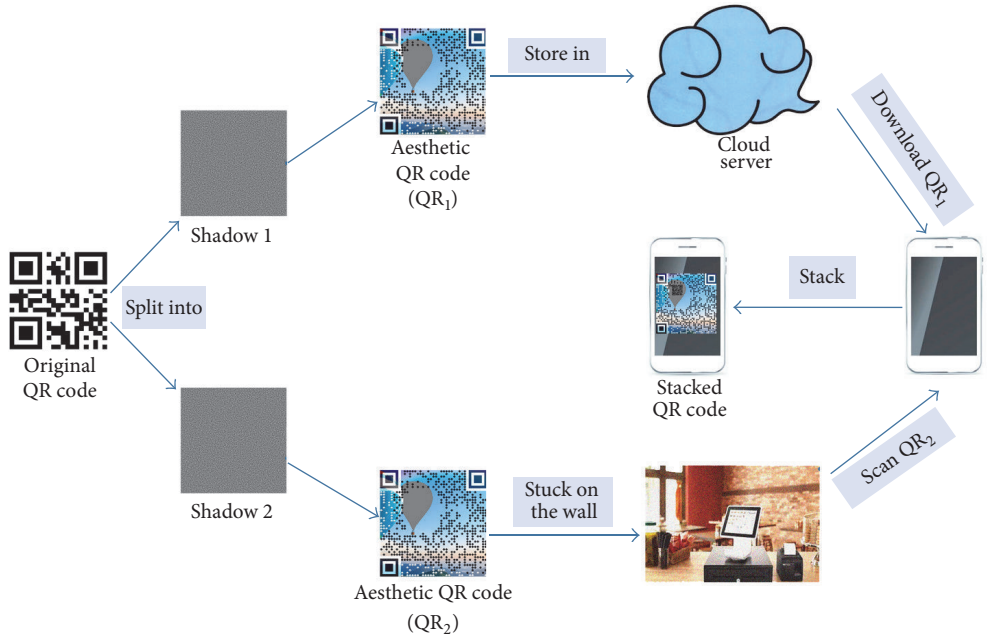


Figure 1: One practical scenario of mobile payment authentication.

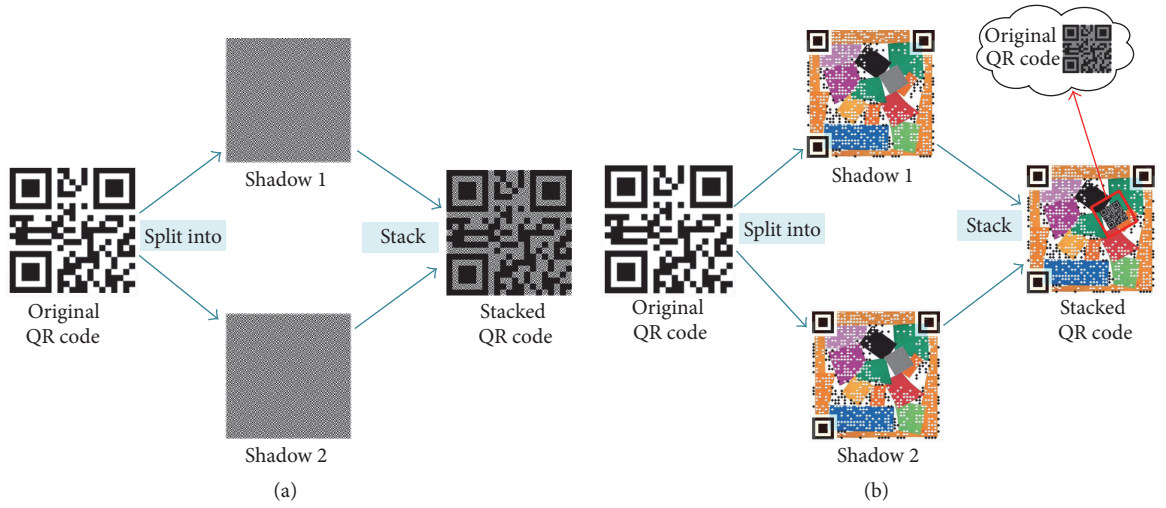


Figure 2: (a) Experiment result of [7]. (b) Our experiment result.

features can make up for the shortcoming of traditional VCS that only decodes a simple image. Therefore, some related researches [8–11] on security authentication based on the combination of QR code and VCS have been conducted in recent years. In these papers QR code is split into several shadows by using VCS since both of VCS and QR code are composed of black and white dots. Besides, VCS used in e-commerce, bank secure login authentication, and so on has been studied [7, 9, 12].

Also, Yang et al. proposed that the split two shadows were stored, respectively, in the mobile client and cloud server to achieve the mobile phone authentication. The two shadows can also be stacked together and the original QR code is restored as shown in Figure 2(a). If the scheme [13] is applied on specific QR code payment, the shadows are only vulnerable.

In this study, the shadows are hidden in an undetectable state using the QR code background fusion on such basis [13]. Specifically, two shadows are respectively embedded into two similar images and the results are fused with two identical carrier QR code by using QR code background fusion strategy. The two fusion QR codes can be stacked precisely since QR code presents the characteristics of automatic identification and independent positioning. The stacked result is the original QR code in carrier QR code [11]. One example of our experiment results is shown in Figure 2(b).

The main contributions of this paper are three schemes with different principles and concealment levels for mobile payment authentication:

(1) In order to make the QR code as holistic as possible after the shadow is embedded, Scheme I operates on the basic unit of QR module and adopts the XOR mechanism of Reed-Solomon (RS). In this scheme the original QR code is split into two shadows using the proposed nonexpansion (2, 2)-VCS; the shadows have the same size with the original QR code.

(2) To decrease the visual difference between the shadow and its surrounding region of the carrier QR code in Scheme I, a two-level fusion strategy with a background image and an aesthetic QR code strategy are proposed in Scheme II. The first-level fusion process is to hide the shadow in the background image and the second is to fuse the carrier QR code with the special region in the fused background image using XOR mechanism of RS.

(3) Scheme II only supports the fusion of binary background image. To achieve better aesthetic effect and concealment, the fusion strategy is adapted between the carrier QR code and extracted regions of interest (ROI) by the error correction mechanism of QR code in Scheme III. Specifically, the saliency map and module layout are used to figure out the saliency values, based on which the appropriate modules are selected as ROI. The obtained ROI is the local region in the background image replaced by the shadow.

The rest of this paper is organized as follows. Section 2 introduces VCS and QR code. The detailed descriptions of the three proposed schemes and their corresponding experiments are given in Section 3. The analysis of authentication security and conclusions are presented in Section 4.

2. Preliminary

2.1. Visual Cryptography. Visual cryptographic scheme (VCS) is a generalization of secret sharing and was first proposed by Naor and Shamir in 1995 in their scheme [14]. An original halftone image is divided into n shared images and each shared image is printed on a transparent film, such that any k films stacked together can restore the original image. However, for the case with less than k films, the original image cannot be restored. This program mainly uses the human visual system of color approximation principle. Therefore, the secret image restoration can be implemented by a simple film superposition without any password calculation.

Each pixel of the images is divided into smaller blocks. There is always the same number of white and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks. In Figure 3 a pixel is divided into four parts, and it has two different states. If the pixel is white, it can be divided into two blocks and each block has a black pixel and a white pixel. When the secret image is split, the block is randomly filled into two shadows. When the two blocks are superimposed together, gray blocks appear to simulate the white pixels. If the pixel is black, the two blocks are complementary. When the two blocks are superimposed, they present black pixels. Thus, shadow images that are split by secret image become a chaotic maps and no information can be inferred from the secret image. Secret images can be restored when the two shadows overlay. Moreover, the stacking process does not require any calculations.

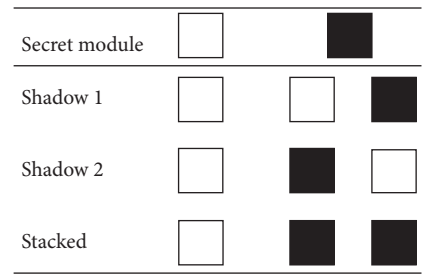


Figure 3: Construction of (2, 2) VCS scheme.

2.2. QR Code

2.2.1. RS Code Encoding Mechanism. The n bits RS code contains k data bits, as parity code for the rest of the word. The QR code is generated by RS code. The generation process of QR code with RS code is presented as follows. Firstly, the length of data region is k in RS code according to the input text; secondly, the input text is encoded based on the encoding rules of RS code; the region filled by those code words are considered as the valid data region, and its length is m. If the code words cannot completely fill the data region, a terminator (0000) is adopted. The padding bits are used to fill the extra data region known as the invalid data region and its length is $k - m$. Moreover, the RS code generates t parity bits according to the k data bits. Finally, the generated RS code combining with the timing pattern and alignment pattern performs XOR operations with mask [15]. Then the standard QR code is generated.

Figure 4 shows the distribution of RS code in the QR code. Pink and green parts are the data region with length of k, and the orange part is the parity region with length of t. The remaining parts are filled by timing pattern and alignment pattern. The pink part is the valid data region with length of m; the green part is the invalid data region with length of $k-m$ after the terminator.

Black and white modules are randomly distributed in QR code, which is a property of QR code. Submodules of VCS are also randomly distributed, but submodule is from image decomposition. Compared with VCS, randomness in QR codes appears natural. Concealment will be better in QR code if we want to hide information.

2.2.2. Construction of PBVM. A series of RS codes can be acquired by Gauss Jordan elimination method [16]. Those RS codes formulate a matrix and its previous section of the matrix is a unit vector matrix. On this basis, the concept of positive basis vector matric (PBVM) is proposed, in which

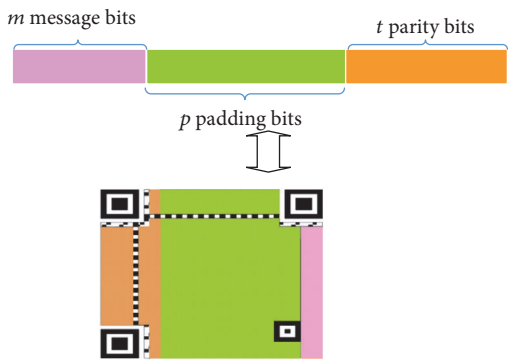


Figure 4: RS code distribution in QR code.

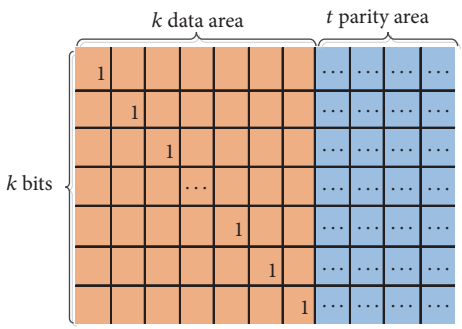


Figure 5: PBVM.

each line is a RS code; the previous k bits are data region and the rear t bits are parity region. The subregion of $k * k$ in the front of the whole matrix is a unit vector matrix (as shown in Figure 5). PBVM is used to modify the data region of RS codes.

2.2.3. XOR Mechanism of RS. According to the literature [16], it is proved that RS code has the features of XOR operation, which means a new RS code can be acquired using two different RS codes by performing XOR operation, and the new RS code still conforms to the standard form. For example, given the following RS codes with data bits $k = 3$ and parity bits $t = 2$, the two RS codes are RS1 = 10010 and RS2 = 01011; then, to perform the XOR operation RS3 = RS1 $\oplus$ RS2 = 11001, it also can be observed that RS3 is also a valid RS code.

2.2.4. Error Correction Mechanism of QR Code. QR code is divided into 40 versions according to the image size. Version 1 consists of $21 * 21$ modules; every following version compared to the previous version increases four modules for each side. In different versions of QR code, each version of QR code has four error correction levels, expressed with L, M, Q, and H; the corresponding error correction capacities are 7%, 15%, 25%, and 30%, respectively. In this paper, we will use error correction mechanism to realize the blend of QR code and background image.

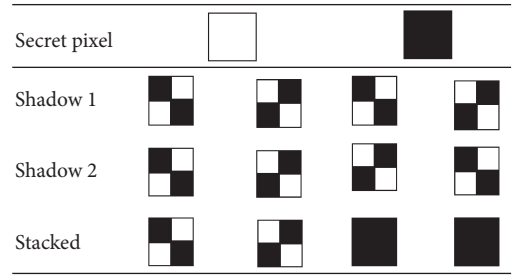


Figure 6: Nonexpansible VCS scheme.

3. Authentication Schemes for QR Code Payment

Because QR code and shadows of VCS are both composed of white/black dots, we can combine VCS with QR code to implement security authentication scheme. Firstly, VCS is used for authentication of QR code. Then security for payment will be further improved if shadow of VCS can be concealed into the QR code undetectably. In order to conceal shadow into QR code, some aesthetic QR code methods are adopted. Sections 3.1, 3.2, and 3.3 introduce some authentication schemes for QR code payment, in which VCS based on QR module, fusion with background image based on XOR mechanism of RS, and error correction mechanism of QR are used, respectively.

3.1. Scheme I Based on QR Module and XOR Mechanism of RS. The original QR code is split into two halftone images as shadows at pixel level. When one shadow is embedded to the carrier QR code directly, the aesthetic QR code is noticeable because of the visual difference of white/black dots. Thus, it is easy to be suspected and then it results in malicious attacks. Therefore, in order to have a better concealment, a new splitting shadows mechanism based on QR code module is designed. The shadow is embedded into the carrier QR code based on XOR mechanism of RS. Figure 6 shows the overall framework, which can be described as follows.

(1) The Generation of Shadows. Considering that the module is taken as the basic unit in QR encoding and decoding, each module of the original QR code is divided into two modules according to the defined rule (Figure 6). If the original QR code module is white, the obtained module pairs must be consistent: both white modules (as shown in the 2nd column in Figure 6). When this pair is stacked, a white module appears. On the other hand, if the original QR code module is black, the obtained module pairs must be complementary (as shown in the 3th and 4th columns in Figure 6). When these complementary pairs are stacked, a black module appears. Each module of the original QR code is handled according to the above defined rules and two shadows are obtained. The two shadows S_1 and S_2 have the same size as the original QR code Q_1. The proposed VCS can provide better concealment for the subsequent fusion process.

Table 1: Results of Scheme I.

Q_3	Q_4	Q_5 (stacked QR code)
		
(1-1)	(1-2)	(1-3)
		
(1-4)	(1-5)	(1-6)
		
(1-7)	(1-8)	(1-9)

(2) The Fusion of Carrier QR Code and Shadows. Given one carrier QR code and shadow S_1, the local region of carrier QR code with the same size as S_1 is modified with XOR mechanism of RS. The related rows in PBVM are obtained if the modules between shadow S_1 and the QR code Q_2 are different. One XOR operation is executed between RS of the module and RS of the carrier QR code to generate a new RS. To insert shadow 1 and shadow 2 into the carrier QR code, the processing steps are described as follows. For each module b_i in shadows 1 or 2, it will be compared with the original module c_i in carrier QR code. If modules b_i and c_i are different, the XOR operation will be executed to change module c_i. Meanwhile, the related rows in PBVM are obtained to generate a new RS in carrier QR code.

After all of the different modules are processed an aesthetic QR code Q_3 is generated. The aesthetic QR code Q_4 is obtained with S_2 in a similar way.

(3) The Stack of QR Code. Then, we stack the two QR codes Q_3 and Q_4. The original QR code Q_1 appears in the stacked QR code Q_5 and can be decoded precisely.

The flowchart of Scheme I is shown in Figure 7. Some experiments are conducted and results are listed in Table 1.

From the front two rows in Table 1, we can find that the modules in the shadow are distinctly different from the surrounding region of the carrier QR code. In order to solve the problem, we need to modify the data region of the original QR code to increase the number of black modules as much as possible. For example, the better result is given in the last row of Table 1.

3.2. Scheme II Based on VCS and Fusion Strategy of Background Image by XOR Mechanism of RS. However, Scheme I has some flaws. For example, there are somewhat differences between the modified region and the surrounding region. Such flaw can cause attackers' suspicion easily and reduce the security of QR code to some extent. So, we propose an improved scheme based on VCS and fusion strategy of background image with XOR mechanism of RS. In Scheme II, the two shadows are embedded into the same background image, respectively. Then, the QR code is fused with the obtained background image based on XOR mechanism of RS. The details are described as follows.

(1) The Generation of Shadows. The QR code Q_1 is divided into two shadows (S_1 and S_2) based on traditional $(2, 2)$-VCS.

(2) Embed Shadows in Background Image. Given a background image (I_1), the two shadows (S_1 and S_2) are, respectively, embedded into I_1. The two background images (I_2 and I_3) are obtained.

(3) Fusion of Background Image and Carrier QR Code. The background images (I_2 and I_3) and the QR code are fused with XOR mechanism of RS. The fusion steps are described as follows. Firstly, background images are grayed using the

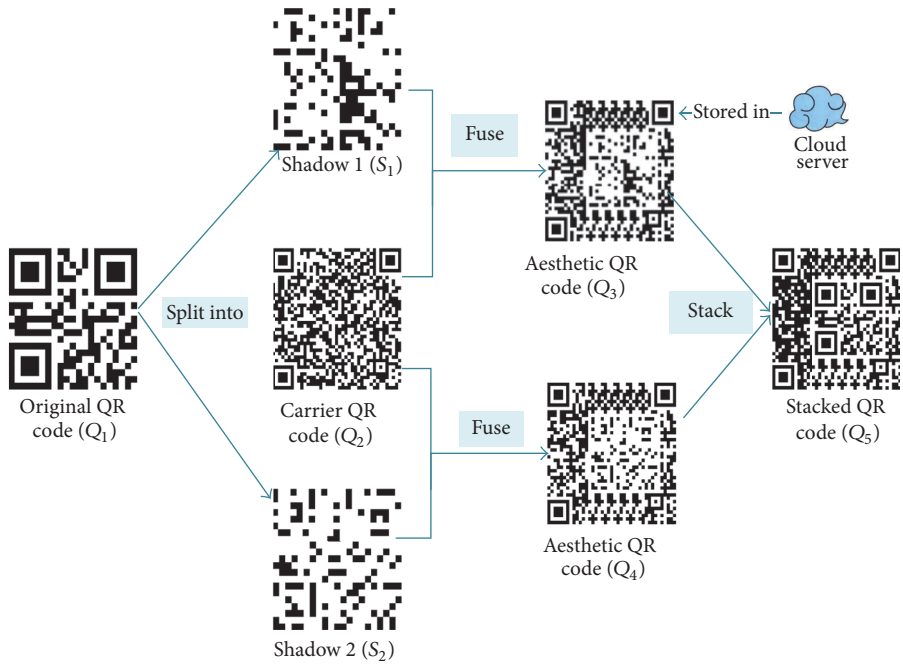


Figure 7: Flowchart of Scheme I.

method of weighted mean and partitioned into several blocks according to the size of QR code module. Secondly, the consistency between every block and its corresponding QR code module is evaluated by comparing their gray value. Then, XOR operation is executed for QR code with PBVM if the comparison result is different. Lastly, the QR code and the background image should be fused. The detailed fusion strategy formula is described as follows:

$$Q = \begin{cases} 0, & T_i < T_0 \cap N_i = 0, \\ -1, & T_i > T_0 \cap N_i = 0, \\ 1, & T_i < T_0 \cap N_i = 1, \\ 0, & T_i > T_0 \cap N_i = 1, \end{cases} \quad (1)$$

where $Q = 0$ represents that the background image that is completely replaced; $Q = -1$ or 1 represents the central region of the specified module which is replaced by the corresponding region of the QR code, and the other region of the specified module is replaced by corresponding region of background image. T_i represents gray average of gray block. T_0 represents binary threshold, which is obtained by Otsu's method. N_i is the module of QR code; $N_i = 1$ represents white block whereas $N_i = 0$ represents black block.

(4) The Stack of QR Code. The two aesthetic QR codes (Q_3 and Q_4) are stacked. The original QR code in the stacked QR code Q_5 appears and can be decoded accurately.

The flowchart of the Scheme II is given in Figure 8. The embedded QR code (Q_2 and Q_3) can be decoded accurately. The small QR code in the fused QR code can be decoded. The secret information can be gained perfectly through decoding the smaller QR code.

For example, when a blank background image is chosen, the result of Scheme II is shown in Figure 9.

From Figure 8, we find that the shadows appear abruptly in the QR code. In this case, the QR code is attacked easily. Thus, the security of QR code is hard to ensure. The selection of background image is crucial. The better results will be tested in Table 2 by selecting some special binary background image.

From Table 2, we find the shadows are hidden with no affection in the binary background images. This scheme has good security and concealment. It is suitable for mobile payment.

3.3. Scheme III Based on VCS and Fusion Strategy of Background Image with Error Correction Mechanism of QR. Scheme II is implemented with XOR mechanism of RS. However, the selected background image is only valid for binary image. In order to enlarge the selectable background image, XOR mechanism adopted in Scheme II is replaced by error correction mechanism of QR code. Thus, Scheme III is designed as shown in Figure 10.

In Scheme III, a color background image is selected. Local region of the color background image is replaced by one shadow as shown in Figure 10. Then, the selected carrier QR code and the modified background image are fused with the method of error correction mechanism. The shadow is hidden in the carrier QR code. It is hard to notice the hidden shadow and the security is enhanced. When two aesthetic QR codes are stacked, the original QR code appears and can

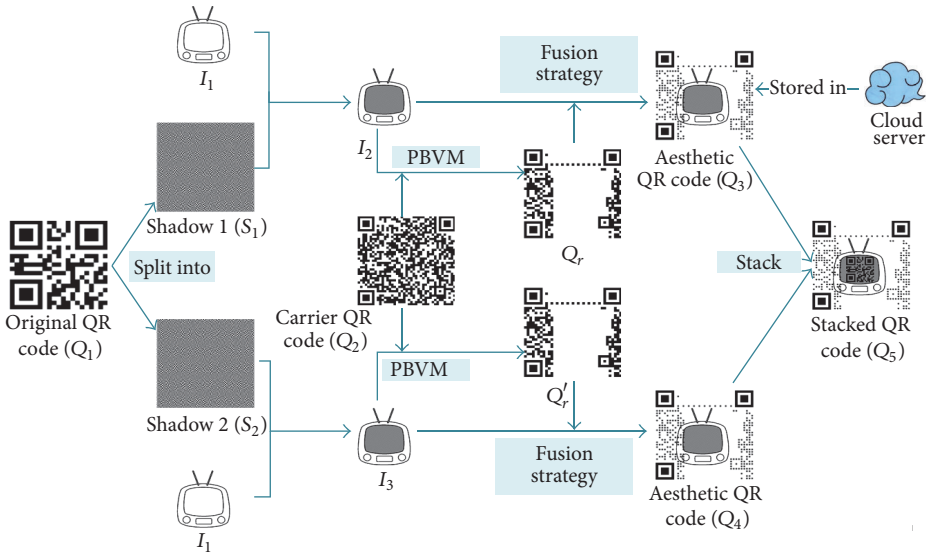


Figure 8: Flowchart of Scheme II.

Figure 9: Simple results of Scheme II: (a), (b), and (c) represent Q_3, Q_4, and Q_5, respectively.

be decoded accurately. The main differences are stated in the second step and the third step compared with Scheme II.

(1) The Generation of Shadows. The QR code Q_1 is divided into two shadows (S_1 and S_2) based on traditional (2, 2)-VCS.

(2) The Selection of Color Background Image. In Scheme III, the background image is selected widely. The color image has rich information, such as texture, color, and shapes, which can be utilized sufficiently to hide the shadows. The region of interest (ROI) in the background image is selected and replaced by the shadows. The modified background image is obtained.

(3) Fusion Strategy of Background Image and QR Code. The error correction mechanism of QR code can be adopted to fuse the modified background image and the carrier QR code. The details are described as follows.

Firstly, the positions of modules of the carrier QR code are marked as module layout. The saliency map is generated according to ROI. The saliency map and module layout are used to figure out saliency values and then sort and select proper modules as changeable regions. The hierarchical module replacement rules are proposed.

Secondly, the binary operation for the modified background image is done. The modified background image is partitioned into blocks as the size of QR code module.

Thirdly, the block in the ROI with the corresponding QR code module is compared. The corresponding module is modified if the comparison result is different. The modification rule is as follows: if the module is white, it is replaced directly by black module. Otherwise, it is replaced directly by white module.

Finally, the third step is repeated for every module in the ROI. The modified background image is fused with the carrier QR code as the method of Scheme II.

Some related experimental results with Scheme III are listed in Table 3. Compared with Scheme II, the background images present a variety of diversity, including grayscale and color images. Due to the rich background images, the shadows are perfectly fused into the background image to further strengthen the concealment of shadow. The attacker would not pay much attention to the fused QR code. Therefore, the

Table 2: Experimental results of Scheme II.

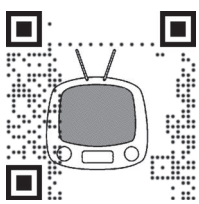
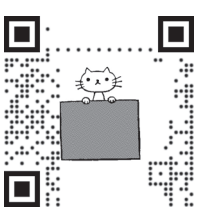
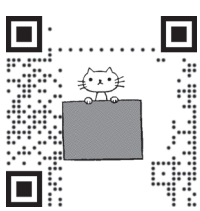
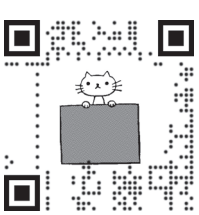
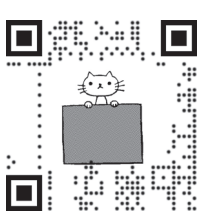
Aesthetic QR code (Q_3)	Aesthetic QR code (Q_4)	Stacked QR code (Q_5)
 (2-1)	 (2-2)	 (2-3)
 (2-4)	 (2-5)	 (2-6)
 (2-7)	 (2-8)	 (2-9)
 (2-10)	 (2-11)	 (2-12)
 (2-13)	 (2-14)	 (2-15)
 (2-16)	 (2-17)	 (2-18)
 (2-19)	 (2-20)	 (2-21)

Table 2: Continued.

Aesthetic QR code (Q_3)	Aesthetic QR code (Q_4)	Stacked QR code (Q_5)
(2-22)	(2-23)	(2-24)

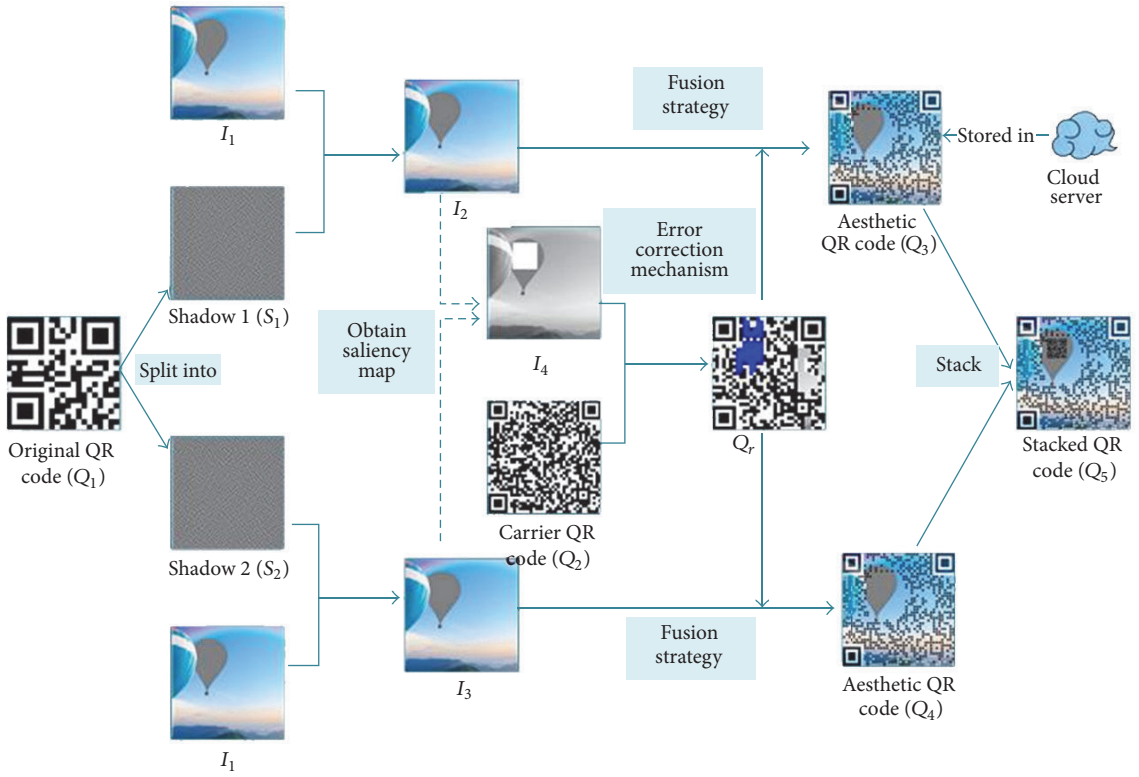


Figure 10: Flowchart of Scheme III.

authentication function can be implemented and the security of mobile payment is ensured.

4. Discussion and Conclusion

Three schemes are proposed in this paper for mobile payment authentication, in which VCS, XOR mechanism of RS, and error correction mechanism of QR code are adopted. The security performance primarily depends on VCS and its construction. Shadows are generated by splitting the original QR code based on VCS and have pseudorandom characteristic similar to noise. It is almost impossible for the attacker to recover the secret information from each individual shadow. Because of the random splitting for each pixel, the secret information cannot be iteratively calculated using the existing technologies, which can be proved using probability theory. The probability of a pixel that is induced in the secret image is 1/3 if only a 2×2 block from a shadow is known. Therefore, the probability of the entire 84×84 of the shadow is estimated to be $(1/3)^{7056}$.

With QR code being used widely for mobile payment, QR code is attacked more frequently. If QR code is replaced or tampered with, it will cause huge economic losses. Thus, the real payment QR code is split to shadows and embedded in a large carrier QR code in the proposed schemes. To increase the uniformity between the shadow and the carrier QR code and improve its concealment of the shadow, the fusion among the shadow, background image, and carrier QR code is executed using XOR mechanism of RS or error correction mechanism of QR code. When the carrier QR code is scanned, it will jump to the Internet web downloading the other carrier QR code. By stacking the two carrier QR codes, the real payment QR code will appear on the mobile.

Table 3: Experimental results of Scheme III.

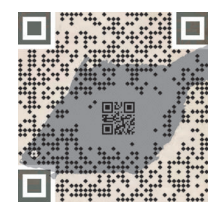
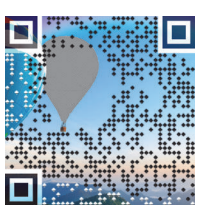
Aesthetic QR code (Q_3)	Aesthetic QR code (Q_4)	Stacked QR code (Q_5)
 (3-1)	 (3-2)	 (3-3)
 (3-4)	 (3-5)	 (3-6)
 (3-7)	 (3-8)	 (3-9)
 (3-10)	 (3-11)	 (3-12)
 (3-13)	 (3-14)	 (3-15)
 (3-16)	 (3-17)	 (3-18)
 (3-19)	 (3-20)	 (3-21)

Table 3: Continued.

Aesthetic QR code (Q_3)	Aesthetic QR code (Q_4)	Stacked QR code (Q_5)
		
(3-22)	(3-23)	(3-24)
		
(3-25)	(3-26)	(3-27)
		
(3-28)	(3-29)	(3-30)

Therefore, our schemes can satisfy the security requirement of QR code payment. As shown in the experiments, the shadows and carrier QR code are mixed to be a uniform object. The application scenarios of the proposed schemes will be further explored in future work.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work was mainly supported by National Natural Science Foundation of China (no. 61370218).

References

[1] D. A. Ortiz-Yepes, "A review of technical approaches to realizing near-field communication mobile payments," *IEEE Security and Privacy*, vol. 14, no. 4, pp. 54–62, 2016.

[2] P. Subpratatsavee and P. Kuacharoen, "Internet banking transaction authentication using mobile one-time password and QR code," *Advanced Science Letters*, vol. 21, no. 10, pp. 3189–3193, 2015.

[3] B. Zhang, K. Ren, G. Xing, X. Fu, and C. Wang, "SBVLC: secure barcode-based visible light communication for smartphones," in *Proceedings of the 33rd IEEE Conference on Computer Communications (IEEE INFOCOM '14)*, pp. 2661–2669, Toronto, Canada, May 2014.

[4] H. Suryotrisongko, Sugiharsono, and B. Setiawan, "A novel mobile payment scheme based on secure quick response payment with minimal infrastructure for cooperative enterprise in developing countries," *Procedia—Social and Behavioral Sciences*, vol. 65, pp. 906–912, 2012.

[5] P. De and J. Eliasson, "An assessment of QR code as a user interface enabler for mobile payment apps on smartphones," in *Proceedings of the 7th International Conference on HCI (IndiaHCI '15)*, pp. 81–84, Guwahati, India, December 2015.

[6] J. M. McCune, A. Perrig, and M. K. Reiter, "Seeing-is-believing: using camera phones for human-verifiable authentication," in *Proceedings of the IEEE Symposium on Security and Privacy*, vol. 4, pp. 110–124, May 2005.

[7] L. Feng and Q. Y. Wei, *Cheating Prevention of Visual Cryptography*, Springer International, Berlin, Germany, 2015.

[8] S. Nseir, N. Hirzallah, and M. Aqel, "A secure mobile payment system using QR code," in *Proceedings of the 5th International Conference on Computer Science and Information Technology (CSIT '13)*, pp. 111–114, March 2013.

[9] N. Buckley, A. K. Nagar, and S. Arumugam, "Visual secret sharing between remote participants," *International Journal of Computer Applications*, vol. 103, no. 2, pp. 8–17, 2014.

[10] A. Espejel-Trujillo, I. Castillo-Camacho, M. Nakano-Miyatake, and H. Perez-Meana, "Identity document authentication based on VSS and QR codes," *Procedia Technology*, vol. 3, pp. 241–250, 2012.

[11] W.-P. Fang, "Offline QR code authorization based on visual cryptography," in *Proceedings of the 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP '11)*, pp. 89–92, October 2011.

[12] C. Chan and C. Lin, "A New Credit Card Payment Scheme Using Mobile Phones Based on Visual Cryptography," in *Intelligence and Security Informatics*, vol. 5075 of *Lecture Notes in Computer Science*, pp. 467–476, Springer, Berlin, Germany, 2008.

[13] C. Yang, J. Liao, F. Wu, and Y. Yamaguchi, "Developing visual cryptography for authentication on smartphones," in *Industrial IoT Technologies and Applications*, vol. 173 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 189–200, Springer International Publishing, Cham, 2016.

[14] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology—EUROCRYPT '94 (Perugia)*, vol. 950 of *Lecture Notes in Computer Science*, pp. 1–12, Springer, Berlin, Germany, 1995.

[15] C. Li, T. Q. Zhang, and Y. Liu, "Blind recognition of RS codes based on Galois field columns Gaussian elimination," in *Proceedings of the 8th International Congress on Image and Signal Processing*, vol. 2015, pp. 836–841, Shenyang, China, 2015.

[16] R. Cox, "Qartcodes," April 2012, http://research.swtch.com/qart.