Mathematical Biosciences and Engineering

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

MBE, 16(6): 6367–6385.
DOI: 10.3934/mbe.2019318
Received: 31 March 2019
Accepted: 11 June 2019
Published: 10 July 2019

Research article

Multiple security anti-counterfeit applications to QR code payment based on visual secret sharing and QR code

Song Wan, Guozheng Yang, Lanlan Qi, Longlong Li , Xuehu Yan*and Yuliang Lu

National University of Defense Technology, No.460 Huangshan Road, 230037, Hefei, China

* **Correspondence:** Email: publictiger@126.com; Tel: +86055186402861.

Abstract: In this paper, we propose a novel mechanism for QR code security anti-counterfeit based on the fusion of visual secret sharing (VSS) and QR code (called VSSQR scheme), which can greatly improve the security of QR code payment. Due to different application scenarios, the background security anti-counterfeit application and the prospects security anti-counterfeit application are shown for QR code payment authentication. The basic idea of the two applications can be characterized as follows. First, two QR code shares that contain the information of the merchant can be generated based on VSSQR scheme with an original secret image. Second, the secret image can be revealed by stacking two QR code shares to obtain the original information. Finally, whether the stacking result is the same as the original secret image or not can determine the authenticity of QR code share used for payment. The analyses show the security of our method. The applications are conducted to show the effectiveness and practicability.

Keywords: QR code payment; visual cryptography application; QR code; anti-counterfeit; security

1. Introduction

Nowadays, with the rapid development of information technology, mobile phones are equipped with more functions, one of which is the mobile payment. Due to its convenience and quickness, mobile payment has been used widely, playing an important role in financial transactions [1–3].

As a two-dimensional barcode, QR code can store large amount of data horizontally and vertically. Since the advantages of the high information density, error correction capability and robustness, the data in QR code can be easily decoded by a QR code reader. QR code has gained popularity rapidly in many applications such as security authentication, payment and so on [4, 5].

Based on this, the third-party payment utilizing QR code is applied more and more widely to the mobile payment market, which is very efficient and convenient for daily life. However, since the technology of QR code is open, it is easy to counterfeit the QR code that represents the merchant's account, which would cause great potential security issues of payment and make huge economic loss. The malicious link encoded by attackers in the QR code also brings serious threats [6, 7]. Security authentication of QR code payment is urgently needed to solve the problem.

Visual secret sharing (VSS), also known as visual cryptography (VC), is a kind of secret sharing scheme [8–12]. The idea of secret sharing scheme is to encode an original secret image into *n* noise-like shares, i.e., shadows or shadow images, where each generated share reveals nothing. Then the secret can only be recovered when qualified shares are combined [13]. In VSS, the secret image could be visually recovered based on the human visual system (HVS) without any computation by stacking a number of shares. VSS [14] could solve the issue of storing secret information in a single carrier which may be lost or damaged easily. However, since each generated share is noise-like, it may cause suspicion and increase the possibility of attracting the attention of possible attackers.

As both of VSS and QR code are composed of white and black dots, the generated shadows can be embedded into the QR code so as to avoid the possibility of attracting the attention. In such a way, the technology of combining VSS and QR code can be applied to many scenes, such as transferring secret message through public channels, security authentication and so on.

Therefore, many researchers proposed relevant schemes about security authentication based on QR code and VSS. Fang [15] proposed an offline QR codes authentication mechanism based on VSS, which can check the authenticity of the QR codes and protect the data. Espejel et al. [16] proposed an identification document authentication system based on QR codes and VSS. The basic idea is to split a binary secret image into two random shares and then encode the generated shares into two QR codes. Stacking the shares decoded from the two QR codes can determine the authenticity. Gayathri et al. [17] presented a QR code authentication protocol based on VSS for protecting ubiquitous multimedia communications. The QR codes that contain the passwords for authentication are encrypted into color share images, which reveal nothing of the secret respectively. The secret password can be recovered by combining the shares. Some other relevant schemes [18–20] on security authentication based on QR code and VSS have been also proposed in recent years.

However, the schemes above just simply combine the techniques of VSS and QR code. If they are applied to the QR code payment, the shadows would be suspected and attacked easily. In addition, there are some other security authentication schemes for QR code payment that combine the techniques of VSS and QR code, which can deal with the issue that the shadows are easy to be suspected and attacked.

Lu et al. [21] proposed multiple schemes for QR code payment based on VSS and QR code, which exploits the XOR mechanism of RS, error correction mechanism of QR code and the theory of VSS. The core idea is as follows. First, an original QR code is encoded into two shadow images based on VSS. Second, the shadows would be embedded into the same background image respectively, and then the results would be inserted into the same carrier QR code by using the error correction mechanism of QR code and the XOR mechanism of RS. Finally, stacking the two carrier QR codes can reveal the original QR code in the corresponding region.

However, from the schemes by Lu et al., the original secret QR code is split into the same size shadows which would be embedded into the carrier QR code and then output the two aesthetic QR codes. To reduce the possibility of suspicion, the two aesthetic QR codes need to be recognized so that the carrier QR code version needs to be greatly bigger than the original QR code version. On the one hand, when one aesthetic QR code needs to be transmitted to the cloud, it would increase the bandwidth of the transmission. On the other hand, the embedding capacity is low.

In this article, two novel applications to QR code payment authentication based on VSS and QR code (VSSQR) are proposed. The proposed applications which deeply integrate the theory of VSS with the error correction mechanism of QR code can greatly improve the embedding capacity and decrease the bandwidth of the transmission. In the proposed applications, the basic idea is as follows. First, based on $(2,2)$ VSSQR scheme, the original secret binary image is shared into two QR code shares, denoted as SC_1 and SC_2. Both of them contain the information of the merchant. Second, SC_1 would be put on the wall or desk of the merchant while SC_2 would be stored in the server and the merchant. Finally, the customer can scan SC_1 with any mobile device and gain SC_2 from the server. The decoding information of SC_1 can preliminarily determine the authenticity of SC_1 and whether the stacking result of SC_1 and SC_2 is the same as the secret image or not can determine the authenticity of SC_1 further.

The main contributions of our article are two QR code payment anti-counterfeit applications based on VSSQR to different scenarios:

a. The background security anti-counterfeit application and the prospects security anti-counterfeit application based on VSSQR scheme are proposed, which have multifactor authentication capacity.

b. As each generated QR code share could be decoded correctly, the security of QR code payment can be improved.

c. The idea is to embed the secret bits generated by VSS from the secret image into the same locations of QR codes in the processing of encoding QRs, which integrates deeply the theory of VSS and the error correction mechanism of QR code. Since only one of the generated QR code share that can be decoded correctly needs to be transmitted to the server, the bandwidth of the transmission would be decreased.

d. The embedding capacity of our proposed applications based on VSSQR scheme can be improved.

The remainder of the paper is organized as follows. The introductions to VSS, QR code and VSSQR are presented in section 2. The applications are described in section 3. Section 4 demonstrates the performance analyses of our applications. Finally, section 5 concludes the paper.

2. Background

2.1. *Visual cryptography*

VSS is first introduced by Naor and Shamir [13]. The core idea is to encode a secret image into a set of n noise-like shadow images (called shares) and stacking qualified shares by OR-operation can reveal the secret image.

In a general (k, n) threshold VSS scheme, the secret image can be divided into n noise-like shares which respectively give no clue about the secret. The secret image could be visually revealed by stacking any k or more shares based on the human visual system (HVS). It would reveal nothing of the secret if the number of shares are less than k. In $(2,2)$ VSS, the secret is encrypted into 2 noise-like shares of the secret image. Even if some contrast loss appears, the recovered image can be recognized clearly [22]. When the light-weight computation device is usable, the secret image could be losslessly revealed by XOR operation [23].

Figure 1 shows the idea of a $(2,2)$ random grid (RG) based VSS. Figure 2 shows an application example of a $(2,2)$ OR-based VCS. Figure 3 shows an application example of a $(2,2)$ XOR-based VSS with light-weight device. It could be seen that the secret image is losslessly recovered and can be recognized as same as the original secret image.

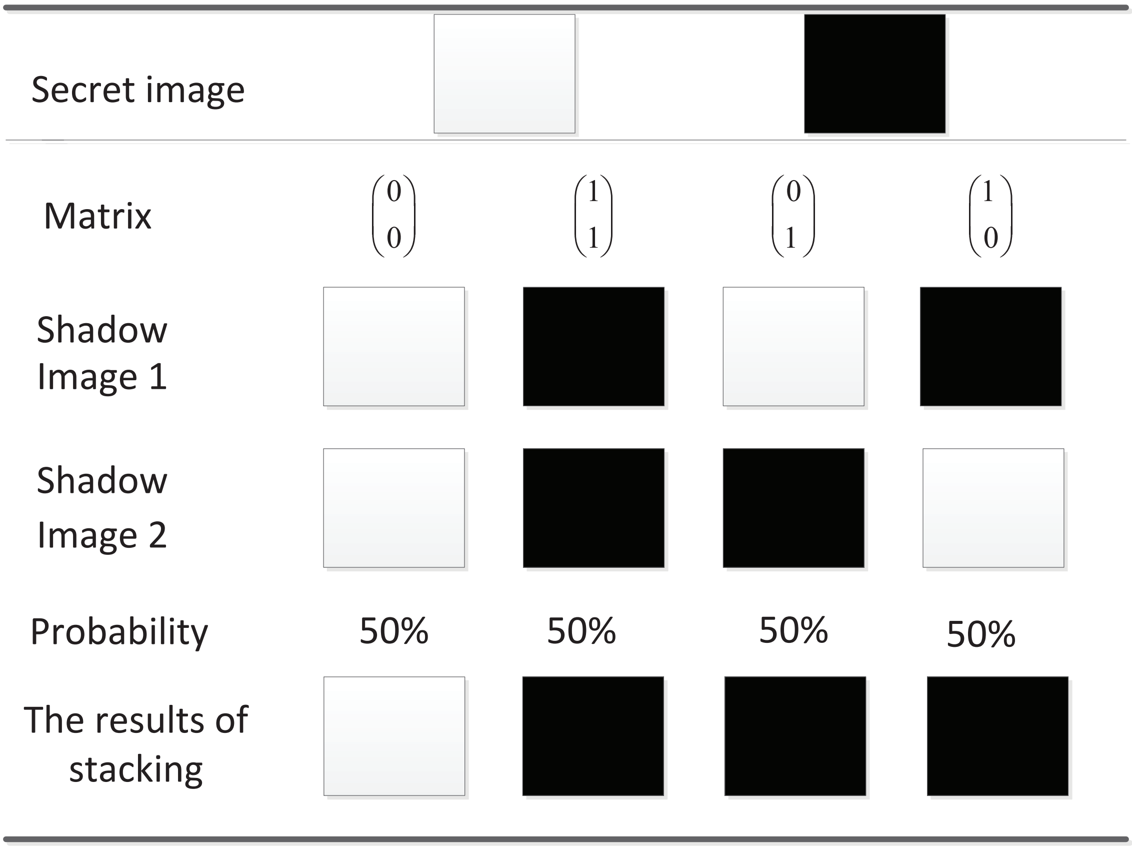

Secret image
Matrix
$\begin{pmatrix}0\\0\end{pmatrix}$
$\begin{pmatrix}1\\1\end{pmatrix}$
$\begin{pmatrix}0\\1\end{pmatrix}$
$\begin{pmatrix}1\\0\end{pmatrix}$
Shadow Image 1
Shadow Image 2
Probability
50%
50%
50%
50%
The results of stacking

Figure 1. The ideal of original (2, 2) RG-based VSS.

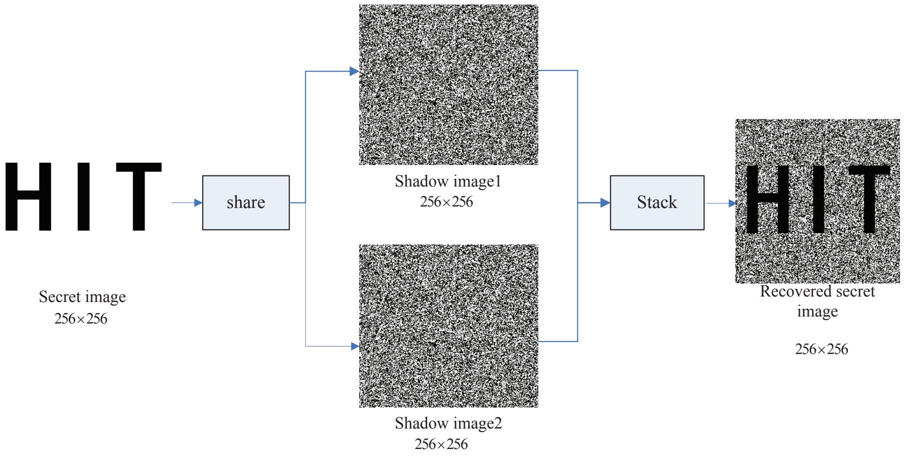


Figure 2. An application example of traditional (2, 2) OR-based VCS. The secret is encrypted into two random shares of the secret image. The recovered image shows the secret image with 50% contrast loss.

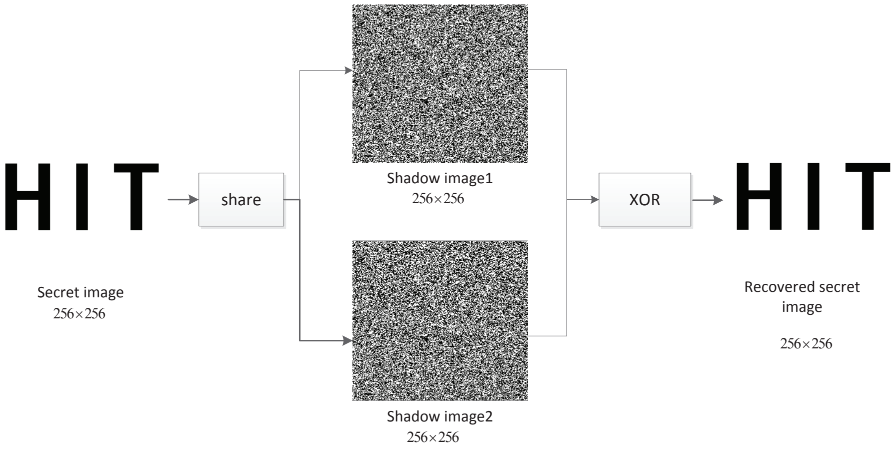


Figure 3. An application example of a (2, 2) XOR-based VCS. The secret is encrypted into two random shares of the secret image. The recovered image shows the secret image recovered lossless.

2.2. *QR codes*

QR code consists of white and black square dotsis and is defined forty sizes versions from version 1 to version 40 [24]. Each QR code is divided into a number of modules and each continuous version is four modules less than the next one. For example, version 9 is made up of 53 × 53 modules while version 10 is made up of 57 × 57 modules. The structure of a QR code version 7 is shown in Figure 4. Each QR code includes three finder patterns that are used to detect the position of the symbol and recognize the QR code. The three finder patterns are located in the upper left, lower left and upper right corner. Each QR code version includes four different error correction levels (L = 7%, M = 15%, Q = 25%, H = 30%). If parts of the QR code are dirty or destroyed, it could also be recovered by the error correction [25, 26]. So, the QR code could also be recognized when embedded with some other information. The recovery capacity of QR codes will be different due to various error correction levels.

2.3. *Visual secret sharing scheme based on QR code (VSSQR)*

VSS based on QR code (VSSQR) is first introduced by Wan [27], which deeply integrates the theory of VSS and the error correction mechanism of QR code. In this paper, (2, 2) VSSQR scheme is used. The idea of VSSQR is to embed the secret bits generated by VSS from a secret bit into the same locations of QR codes in the processing of encoding QRs. The bits of two QR codes are modified in the error correction mechanism so as to generate two QR code shares which include the message of two shadow images. Each share is a valid QR code that could be decoded correctly by any standard decoding software. The secret could be recovered by stacking two QR code shares visually based on HVS. What's more, the secret could be losslessly revealed based on XOR operation if the light-weight computation device is available. Figure 5 shows the generation architecture of VSSQR. To illustrate the efficiency of VSSQR better, we list an example as shown in Figure 6.

Figure 6 shows the results of 17-H (version 17, error correction level H) by (2, 2) VSSQR scheme. The original message of QR_1 is 'Security anti-counterfeit application' while the original message of QR_2 is 'Typical applications to verify the practicability'. Figure 6b,c show the QR code shares that

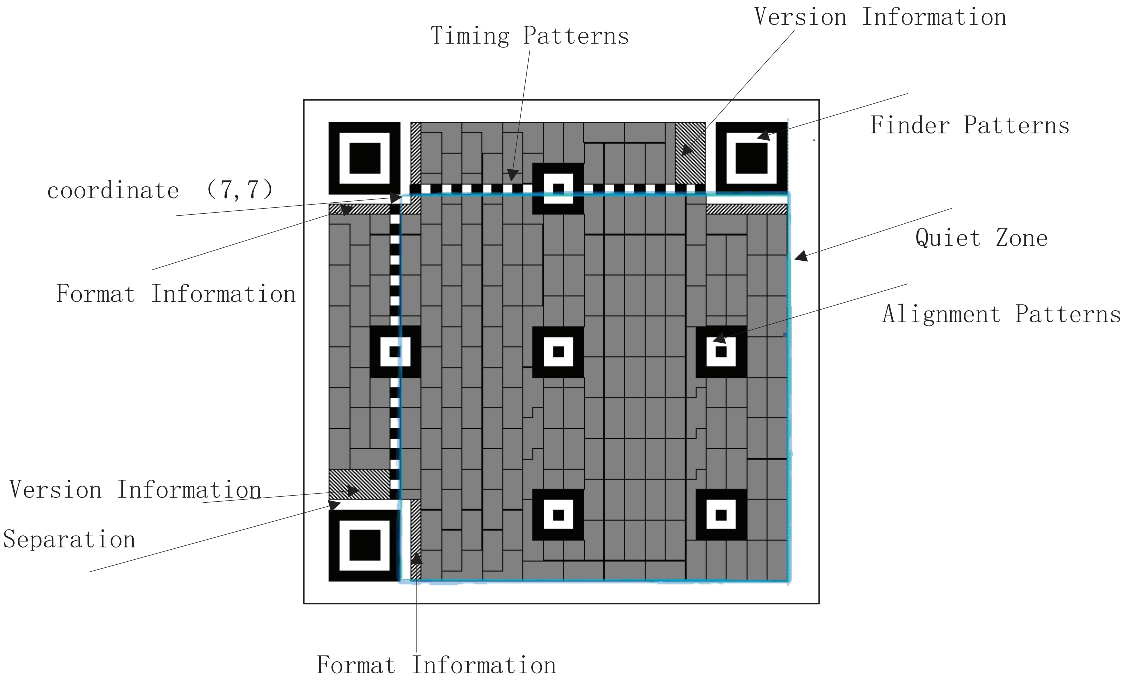


Figure 4. The structure and codewords arrangement for QR code version 7 with error correction level H.

generated by VSSQR scheme, S_1, S_2. Figure 6d,e show the decoding message for S_1, S_2. It can be seen that the shares are valid QR codes that could be scanned and decoded correctly by a QR code reader into the original information. Figure 6f shows the revealed QR code, Sr, which is revealed by stacking two QR code shares. It can be seen that the secret could be seen directly from the revealed QR code. Figure 6g shows the reconstructed QR code, Sr_1, which is revealed by XORing two QR code shares with light-weight computation device. It can be seen that the secret information could be revealed lossless.

3. Applications

In this section, QR code security anti-counterfeit applications according to different payment scenarios are proposed, which can improve the security of QR code payment greatly. We list two typical applications to verify the practicability according to two payment scenarios.

The prospects security anti-counterfeit application and the background anti-counterfeit application can reach the goal, which exploit the technology of VSSQR scheme.

3.1. The background security anti-counterfeit application

In daily life, QR code is more and more popular, and it has been used in the third-party payment. However, since the QR code is easy to be tampered and counterfeited, the QR code payment is becoming more and more insecure. The background security anti-counterfeit application is proposed to solve the issue.

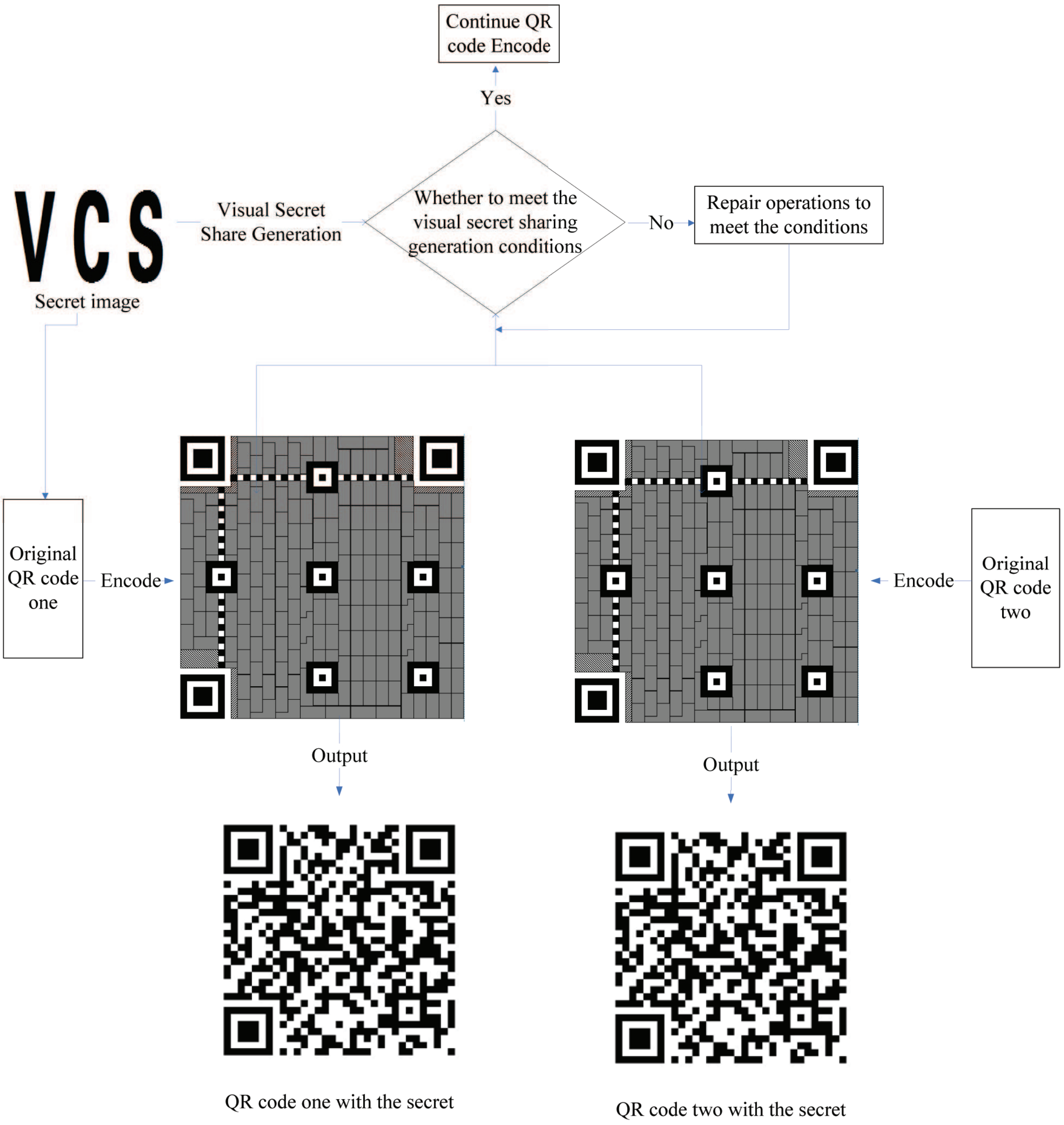
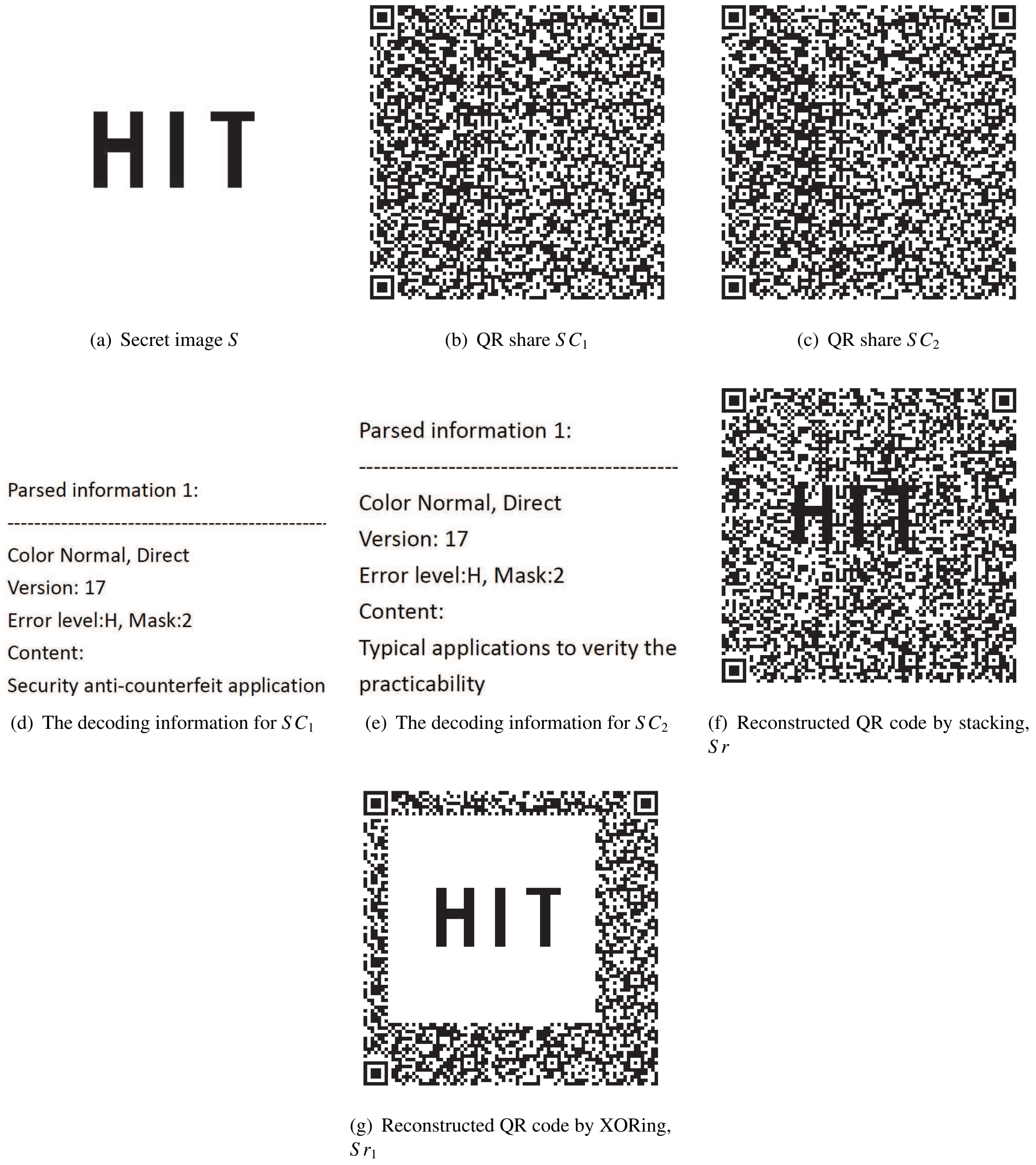

Continue QR code Encode
Yes
VCS
Secret image
Visual Secret Share Generation
Whether to meet the visual secret sharing generation conditions
No
Repair operations to meet the conditions
Original QR code one
Encode
Encode
Original QR code two
Output
Output
QR code one with the secret
QR code two with the secret

Figure 5. The QR code shares generation architecture of the VSSQR scheme.



(a) Secret image S

(b) QR share SC_1

(c) QR share SC_2

```
Parsed information 1:
------------------------------------------------
Color Normal, Direct
Version: 17
Error level:H, Mask:2
Content:
Security anti-counterfeit application
```

(d) The decoding information for SC_1

```
Parsed information 1:
--------------------------------------------
Color Normal, Direct
Version: 17
Error level:H, Mask:2
Content:
Typical applications to verity the
practicability
```

(e) The decoding information for SC_2

(f) Reconstructed QR code by stacking, Sr

(g) Reconstructed QR code by XORing, Sr_1

Figure 6. The results of QR code version 17 with error correction level H by $(2, 2)$VSSQR scheme proposed.

The structure of the background security anti-counterfeit application based on the technology of VSSQR is shown in Figure 7, which can authenticate the identity of QR code payment.

Step 1: The merchant will send an original secret binary image randomly to the relevant technical personnel.

Step 2: The technical personnel generates two QR code shares denoted as S_1 and S_2. S_1 contains a unique identifier ID of the merchant, vendor name and the server link, while S_2 contains the payment link, the unique identifier ID of the merchant and vendor name based on VSSQR scheme with the original secret image.

Step 3: The QR code share S_2 will be stored in the server and the local media of merchant.

Step 4: S_1 would be put on the desk or screen so that the customer can scan it to pay money.

Step 5: The customer would scan and decode the QR code share S_1 by mobile phone with camera.

Step 6: Whether the decoding information is the right or not will determine the authenticity of the QR code share S_1 preliminarily.

Step 7: If the decoding information is wrong, S_1 is faked; otherwise it would be sent to the server. Since the server includes many merchants and stores many relevant QR code shares for different merchant, each QR code share stored in the platform server would contains the unique identifier ID of the merchant and the new generated QR code share will replace the previous one.

Step 8: If this QR code share S_1 is received, the server will try to match another relevant QR code share S_2 and sent it to the customer according the unique identifier ID of the merchant. When the matched QR code share S_2 is received, the customer can stack the two QR code shares by mobile phone. If the stacking result is the same with the original secret image and confirmed by the merchant, the QR code shares S_1 and S_2 are correct and the customer can pay the money by scanning S_2; otherwise, the customer need to contact the merchant to check the information.

In such a way, it can reach the goal of security payment based on the authentication mechanism of QR code. In the proposed application, as the original secret image is distributed randomly which can be changed by merchants each time, so the secret image could not be gained by possible attacker easily. The generated QR code shares are hard to be counterfeited although the decoding information is the same based on VSSQR scheme. So, it can improve the security of payment greatly.

3.2. The prospects security anti-counterfeit application

In the background security anti-counterfeit application, the secret image is decided by merchants. Another application scenario is that the secret image is decided by customers and then the QR code shares would be generated based on VSSQR.

The structure of the prospects security anti-counterfeit application based on the technology of VSSQR as shown in Figure 8. When payment is needed, the authenticity would be verified firstly. Fixed QR code share called S_1 that contains a unique identifier ID of the merchant, the server link, vendor name, is displayed on the screen, and is also stored in the platform server.

Step 1: The customer will scan the fixed QR code share which contains the information of the merchant and the platform server link so as to get the identifier ID of the merchant.

Step 2: If the decoding information, such as the identifier ID of merchant, is correct, the customer would send an original secret image named the identifier ID of the merchant to the platform server by using the server link.

Step 3: The platform server has many merchants and stores corresponding fix QR code shares of

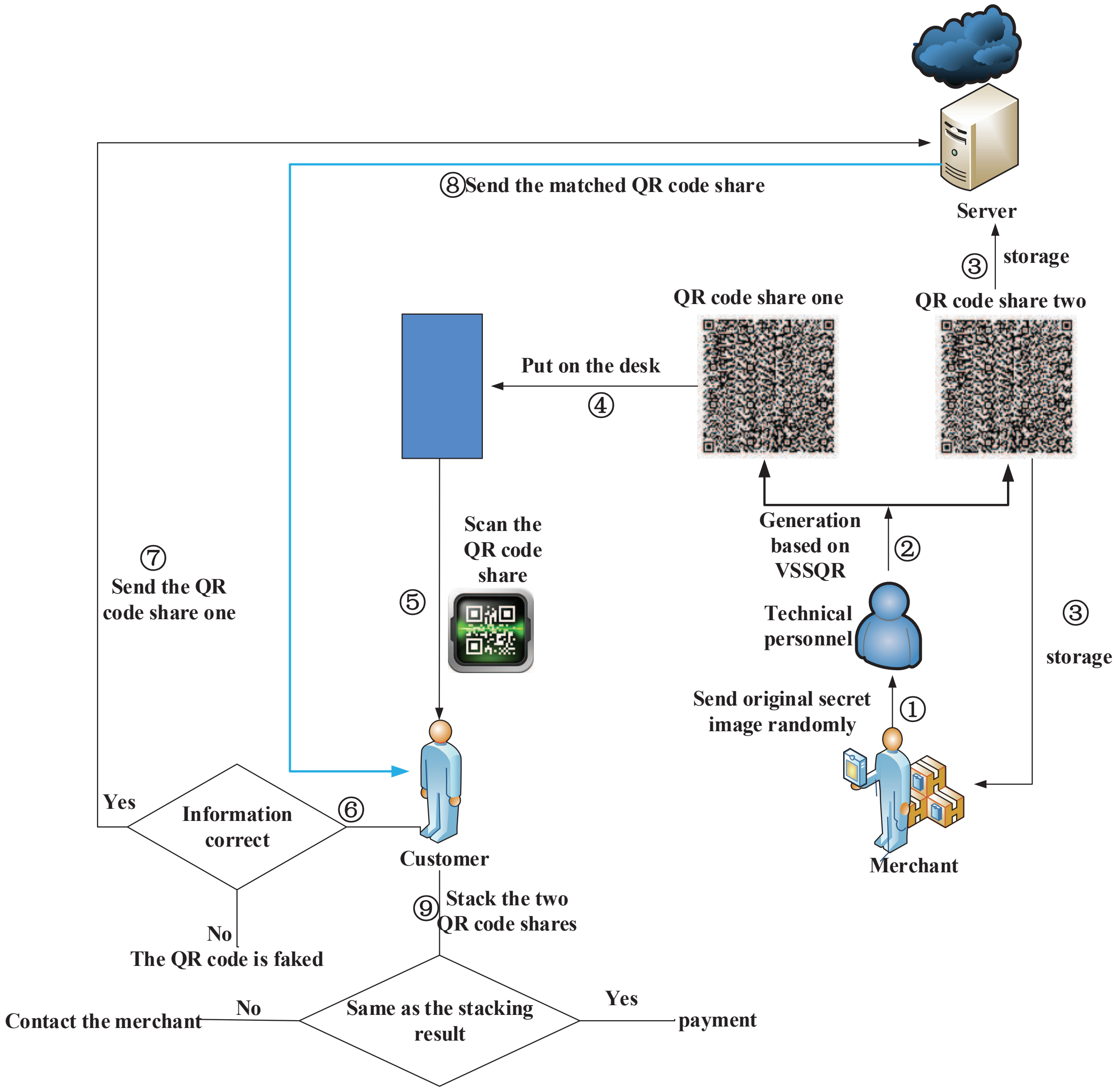


Figure 7. The structure of the background security anti-counterfeit application.

each merchant. Since each merchant ID is unique, the relevant fixed QR code share S_1 would be searched correctly according to the identifier ID of the merchant. Another QR code share S_2 that contains the payment link and the identifier ID can be generated based on VSSQR scheme with the fixed QR code share S_1 and secret image by the platform server.

Step 4: The new generated QR code share S_2, will be sent to the customer.

Step 5: When QR code share S_2 is received, the customer would stack it with the fixed QR code share S_1.

Step 6: If the stacking result is the same with the original secret image, the QR code shares S_1 and S_2 are correct and the customer can pay the money by scanning S_2, else the customer need to contact the merchant to check the information.

There are two-factor authentication mechanism in this application. On the one hand, the merchant can scan the generated QR code share S_1, whether the decoding information is the correct identifier ID or not will determine the authenticity preliminarily. On the other hand, whether the stacking result is the same with the original information or not will determine the authenticity further. So, it can improve the security of payment greatly.

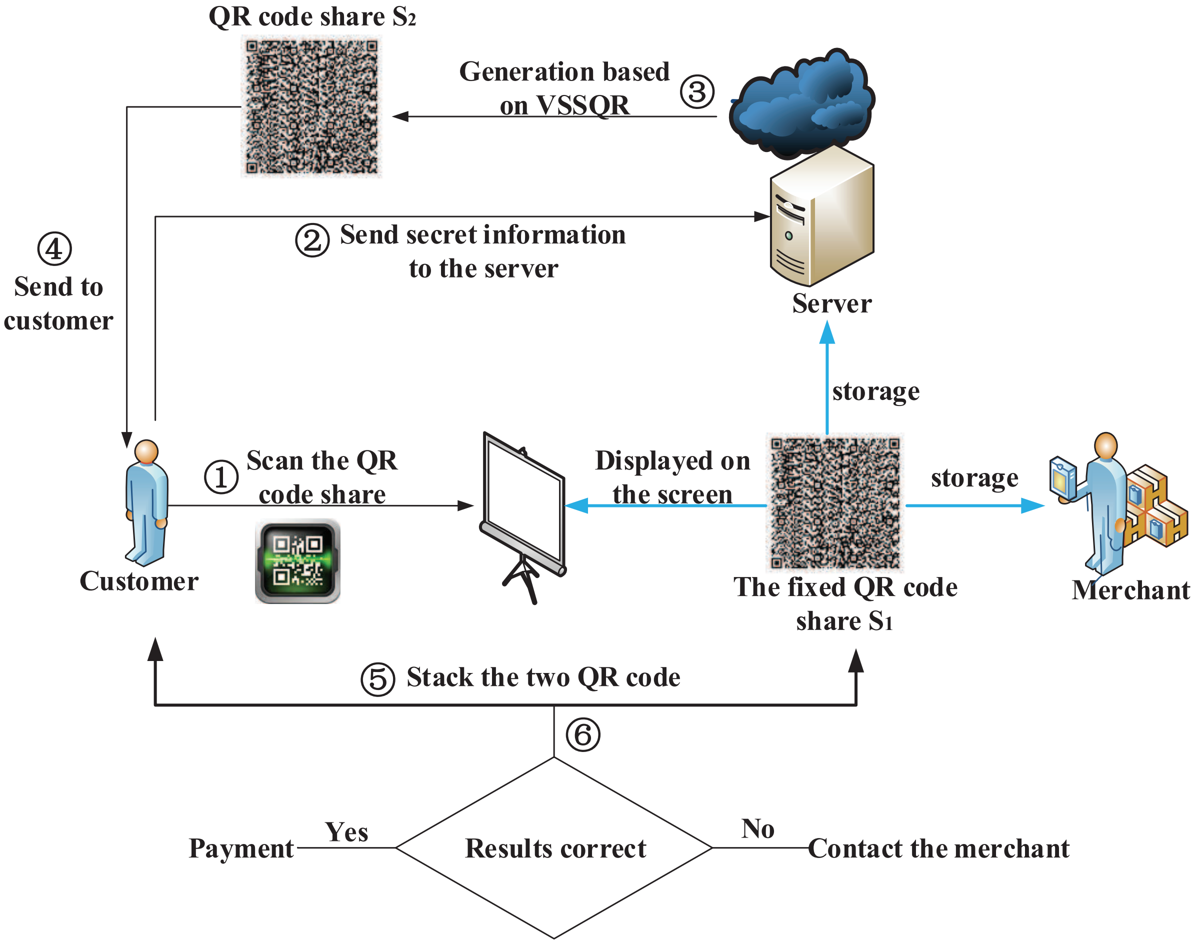


Figure 8. The structure of the prospects security anti-counterfeit application.

4. Performance analyses and comparison

In this section, the security analysis of the proposed applications based on VSSQR is described. To show the effectiveness and practicability of our applications, we compare our applications based on VSSQR scheme with related schemes.

4.1. Security analysis

The core idea of $(2, 2)$ VSSQR scheme is to embed secret information into two QR codes and then generate two QR code shares that could be scanned and decoded correctly by any standard decoding software, which may reduce the possibility of attracting the attention of potential attackers. The secret information can be recovered by stacking two QR code shares. In such a way, the QR code shares will be hard to be counterfeited although the content of each QR code share could be counterfeited easily. So, whether the stacking results of two QR code shares could reveal the secret information or not would determine the authenticity of QR code shares. As the algorithm of VSSQR scheme and the secret information are private, the VSSQR scheme is secure vastly.

In the background security anti-counterfeit application, the original secret image is distributed randomly and the generated QR code shares are also different each time randomly so that it would not be counterfeited by possible attackers easily. As we all know, the secret can be only revealed by stacking two correct QR code shares, if one of them is faked, nothing about the secret can be revealed. Only the QR code share sent from the customer to the server is correct, the stacking result with the matched QR code share selected from the server according to the unique identifier ID of the merchant can be the same with the original secret image. As one of the generated QR code shares is only stored in the merchant and platform server, others could not gain it so that the matched QR code share can be guaranteed, which would improve the security of payment further. So, the security of payment based on the background security anti-counterfeit application can be guaranteed in the application.

In the prospects security anti-counterfeit application, the original secret information is also confirmed randomly by different customers so that the generated QR code share S_2 can be different each time based on VSSQR scheme. Even if another QR code share is fixed, the generated QR code share S_2 is different so that it would not be counterfeited. As we all know, the fixed QR code share S_1 is also stored in the secure server and can be correctly searched according to the identifier ID. Although the fixed QR code share S_1 displayed on the screen can be got by possible attacker, its copy is stored in the server and can be searched with the correct identifier ID that is encoded in the QR code share S_1. Since the copy of S_1 cannot be tampered, security of the generated QR code share S_2 which contains payment link and the correct identifier ID can be guaranteed.

On the one hand, whether the two QR code shares can be correctly decoded the information of the merchant can determine the authenticity preliminarily. On the other hand, Only the two QR code shares are correct, the secret information can be revealed. Therefore, the stacking results can verify the authenticity of QR code shares.

In such a way, if the stacking result is the same with the secret image which is decided by customers randomly each time, the generated QR code share S_2 is correct and we can pay money; otherwise the authenticity of S_1 and S_2 could not be guaranteed. Based on this, other merchants could not counterfeit the payment information of this merchant even if the VSSQR scheme and the platform server are the same according to the identifier ID of the merchant, the QR code payment can be confirmed uniquely so that the security of payment can be ensured.

4.2. Comparison with related schemes

In this section, we compare the proposed security anti-counterfeit applications to QR code payment with Lu et al.'s schemes [21]. Lu et al. [21] proposed three schemes for QR code payment based on VSS and QR code, which exploits the XOR mechanism of RS, error correction mechanism of QR code and the theory of VSS. The core idea is as follows. Firstly, an original QR code is encoded into two shadow images based on VSS. Secondly, the shadows would be embedded into the same background image respectively, and then the generated results would be inserted into the same carrier QR code respectively by using the error correction mechanism of QR code and the XOR mechanism of RS. Finally, stacking the two carrier QR codes can reveal the original QR code in the corresponding region.

In the schemes, the original secret QR code is split into the same size shadows which would be embedded into the same carrier QR code and then output the two aesthetic QR codes that can be decoded correctly. An example of the schemes proposed can be seen as Figure 9. In scheme 1, stacking two QR codes Q_1 and Q_2 can reveal the original QR code which appears in QR code Q_3 as shown in Figure 9c. In scheme 2, stacking two QR codes Q_4 and Q_5 can reveal the original QR code which appears in QR code Q_6 as shown in Figure 9f. In scheme 3, stacking two QR codes Q_7 and Q_8 can reveal the original QR code which appears in QR code Q_9 as shown in Figure 9i. It can be seen that the original secret QR code version is 1 which is 21×21 modules while the carrier QR code version is 5 or 6 and the original secret QR code can be regarded as a logo which is embedded into the carrier QR code.

Our VSSQR scheme is to embed the secret bits generated by VSS from a secret bit into the same locations of QR codes in the processing of encoding QRs. The generated QR code shares can be decoded correctly into the original information and stacking two QR code shares can reveal the original secret image. The stacking result can determine the authenticity of QR code shares. Figure 10 shows the results of QR code version 6 with error correction H by $(2, 2)$ VSSQR scheme. Figure 10a shows the secret image with size of 26×26. The generated QR code shares based on VSSQR scheme that can be decoded correctly are shown in Figure 10b,c. Figure 10d,e show the decoding message for the two generated QR code shares. Stacking two QR code shares can reveal the original secret image, as shown in Figure 10f. If the light-weight computation device is usable, the secret image can be revealed lossless based on XOR operation, as shown in Figure 10g.

Compared with Lu et al.'s scheme, our proposed applications based on the VSSQR scheme have some superior performances as follows, which is concluded in Table 1.

a. The size of the original secret QR code embedded into the carrier QR code by Lu et al.'s is 21×21 while the the size of the secret image embedded into the same carrier QR code based on VSSQR scheme is 26×26. The embedding capacity of our method is bigger than Lu et al.'s.

b. As our applications exploit the VSSQR scheme, the carrier QR code version can be really small, such as 1 or 2. It does not need to be as big as Lu et al.'s. Based on this, when one of the generated QR code shares need to be transmitted to the server, the bandwidth of the transmission would be much smaller than Lu et al.'s.

c. The embedding way of our applications is to generate and embed at the same time while the Lu et al.'s is first to generate shadows and then embed into carrier QR code, which is different. The generated QR code shares have no flaw based on our embedding way while the generated aesthetic QR codes have some flaw in scheme 1 by Lu et al.

Table 1. Comparison with Lu et al.'s scheme.

Schemes	Capacity (carrier QR code version 6)	QR code version limitation	quality
Lu et al.	Secret QR code size 21×21	Yes	With flaws
our method	Secret QR code size 26×26	No	No flaw

4.3. Extensions

The proposed applications based on VSSQR scheme could be extended through the following ways:

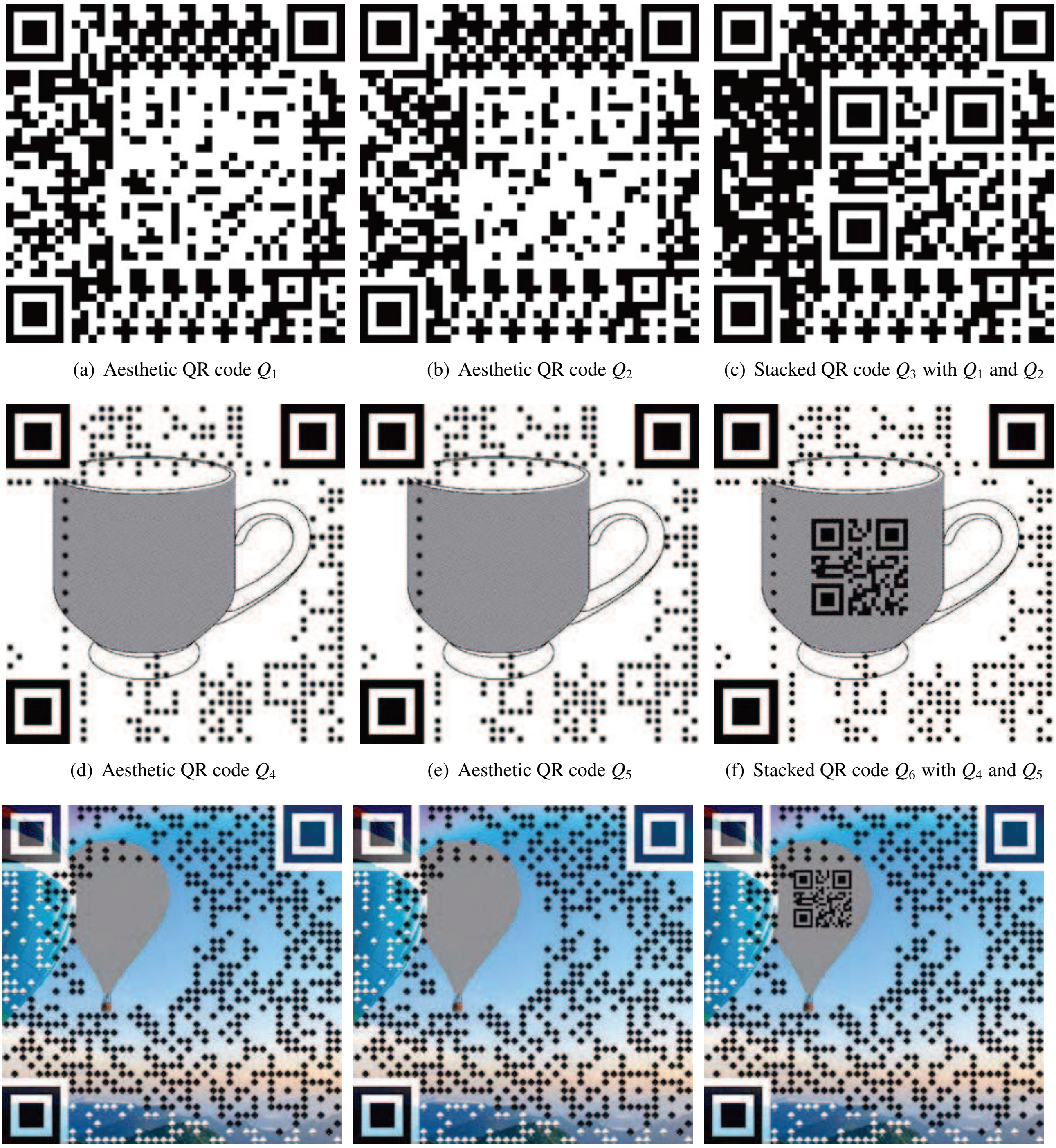
a. Firstly, the secret message including various types of information can be encoded into a secret QR code. Secondly, the secret QR code can be embedded into two cover QR codes to embed the bits corresponding to shares generated by VSS from the secret QR code bit into the same locations of the cover QR codes in the processing of encoding QRs. Finally, each generated QR code share can be decoded correctly by a QR code reader.

b. The secret QR code can be recovered with the generated two QR code shares based on XOR or stacking operation, and can be decoded into the original information. So, whether the decoding information of the recovered secret QR code is the same with original information or not will determine the authenticity of payment.

c. Because of the error correction mechanism of QR code, even if parts of the QR code are dirty or destroyed, it could also be recovered so that can be decoded correctly. In such a way, the recovered secret QR code can contain some errors which could be also decoded correctly by a mobile phone with camera. So, the embedding capacity would be higher. In other words, if the same original secret QR code version need to be embedded, the carrier QR code version based on our extended scheme would be smaller than Lu et al.'s.

4.4. Implementation mechanism

The implementation of our applications needs cooperation with a third-party payment platform, such as Alipay and Wechat Pay, which plays the role of the server in Figures 7 and 8. Our applications seem like an alternative security function that provides the authentication during the payment. The merchant will first decide whether the security function is used or not so that the third-party payment platform can generate QR code in different ways. When the security function is chosen, the platform will communicate with users just as what the server do in our applications.

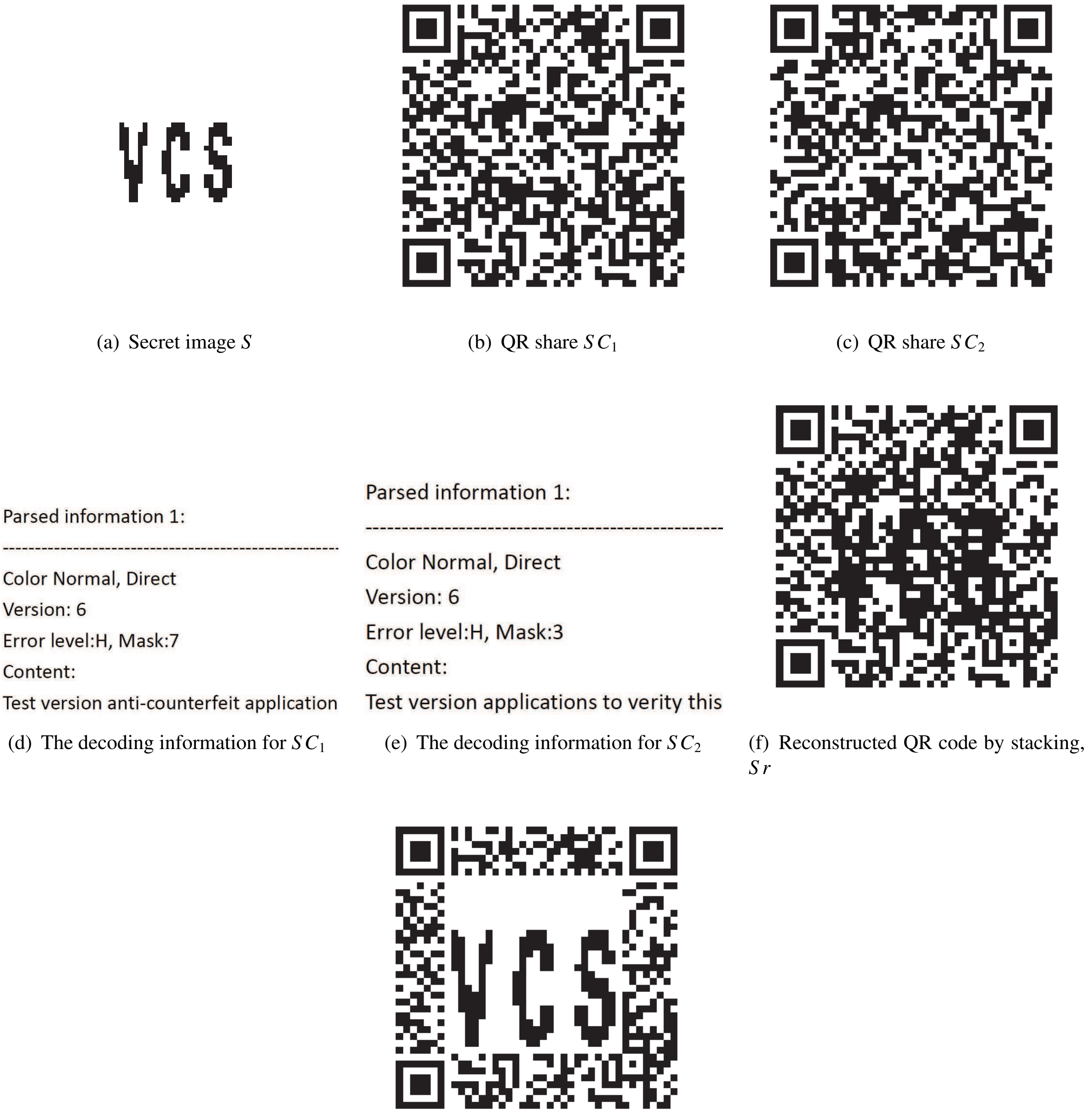


(a) Aesthetic QR code Q_1 (b) Aesthetic QR code Q_2 (c) Stacked QR code Q_3 with Q_1 and Q_2

(d) Aesthetic QR code Q_4 (e) Aesthetic QR code Q_5 (f) Stacked QR code Q_6 with Q_4 and Q_5

(g) Aesthetic QR code Q_7 (h) Aesthetic QR code Q_8 (i) Stacked QR code Q_9 with Q_7 and Q_8

Figure 9. The results of three schemes proposed by Lu et al.



(a) Secret image S

(b) QR share SC_1

(c) QR share SC_2

```
Parsed information 1:
--------------------------------------------------
Color Normal, Direct
Version: 6
Error level:H, Mask:7
Content:
Test version anti-counterfeit application
```

(d) The decoding information for SC_1

```
Parsed information 1:
--------------------------------------------------
Color Normal, Direct
Version: 6
Error level:H, Mask:3
Content:
Test version applications to verity this
```

(e) The decoding information for SC_2

(f) Reconstructed QR code by stacking, Sr

(g) Reconstructed QR code by XORing, Sr_1

Figure 10. The results of QR code version 6 with error correction level H by $(2, 2)$VSSQR scheme proposed.

5. Conclusion and future work

This paper presents multiple security anti-counterfeit applications to QR code payment based on VSSQR scheme that can improve the security of mobile payment greatly. The proposed applications which can be applied to different scenarios integrate theory of VSS with the error correction mechanism of QR code deeply. As the generated QR code shares which contain the information of the original secret image can be decoded correctly by a mobile phone with camera and the original secret image can be only recovered by stacking the two correct QR code shares, the security of QR code payment can be improved vastly. When the payment QR code is faked, even if the decoding information is the same, the stacking result would not be as same as the original secret image so that the security can be guaranteed much. The proposed applications show the effectiveness and practicability. Comparions with related schemes show the superior performances of the proposed applications. How to improve the authentication efficiency of applications will be the further work.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grant Number 61602491).

Conflict of interest

The authors declare that they have no competing interests.

References

1. P. De, K. Dey, V. Mankar, et al., *An assessment of qr code as a user interface enabler for mobile payment apps on smartphones,* Proceedings of the 7th International Conference on HCI, 2015. Available from: https://dl.acm.org/citation.cfm?id=2835977.
2. E. H. Diniz, P. D. A. Jo£o and A. K. Cernev, Mobile money and payment: A literature review based on academic and practitioner - oriented publications (2001 - 2011), *Soc. Sci. Electron. Publ.*, 2011.
3. D. A. Ortiz-Yepes, A review of technical approaches to realizing near-field communication mobile payments, *IEEE Secur. Privacy*, **14** (2016), 54–62.
4. S. Liu, *Anti-counterfeit system based on mobile phone qr code and fingerprint,* 2010 Second International Conference on Intelligent Human-Machine Systems and Cybernetics, 2010. Available from: https://ieeexplore.ieee.org/abstract/document/5590880.
5. P. Subpratatsavee and P. Kuacharoen, Internet banking transaction authentication using mobile one-time password and qr code, *Adv. Sci. Lett.*, **21** (2015), 3189–3193.
6. P. Kieseberg, M. Leithner, M. Mulazzani, et al., *Qr code security,* Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia, 2010. Available from: http://doi.acm.org/10.1145/1971519.1971593.
7. K. Krombholz, P. Frühwirt, P. Kieseberg, et al., *QR code security: A survey of attacks and challenges for usable security,* International Conference on Human Aspects of Information Security,

Privacy, and Trust, 2014. Available from: https://link.springer.com/chapter/10.1007/978-3-319-07620-1_8.

8. M. Naor and A. Shamir, Visual cryptography, *Lect. Notes Comput. Sci.*, **950** (1994), 1–12.

9. J. Weir and W. Q. Yan, *A Comprehensive Study of Visual Cryptography*, Springer Berlin Heidelberg, 2010.

10. C. N. Yang, New visual secret sharing schemes using probabilistic method, *Pattern Recognit. Lett.*, **25** (2004), 481–494.

11. Z. Wang, G. R. Arce and G. Di Crescenzo, Halftone visual cryptography via error diffusion, *IEEE Trans. Inf. Forensics Secur.*, **4** (2009), 383–396.

12. D. Wang, L. Zhang, N. Ma, et al., Two secret sharing schemes based on boolean operations, *Pattern Recognit.*, **40** (2007), 2776–2785.

13. A. Beimel, *Secret-sharing schemes: A survey,* International Conference on Coding and Cryptology, 2011. Available from: https://link.springer.com/chapter/10.1007/978-3-642-20901-7_2.

14. D. Wang, F. Yi and X. Li, On general construction for extended visual cryptography schemes, *Pattern Recognit.*, **42** (2009), 3071–3082.

15. W. P. Fang, *Offline qr code authorization based on visual cryptography,* Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2011. Available from: https://ieeexplore.ieee.org/abstract/document/6079541.

16. A. Espejel Trujillo, I. Castillo Camacho, M. Nakano Miyatake, et al., Identity document authentication based on VSS and QR codes, *Proc. Technol.*, **3** (2012), 241–250.

17. M. Gayathri, A. J. Blesswin and G. S. Mary, An efficient qr-code authentication protocol using visual cryptography for securing ubiquitous multimedia communications, *Indian J. Sci. Technol.*, **9** (2016).

18. N. Buckley, A. K. Nagar and S. Arumugam, Visual secret sharing between remote participants, *Int. J. Comput. Appl.*, **103** (2014), 8–17.

19. S. Nseir, N. Hirzallah and M. Aqel, *A secure mobile payment system using QR code,* 2013 5th International Conference on Computer Science and Information Technology, 2013. Available from: https://ieeexplore.ieee.org/abstract/document/6588767.

20. C. N. Yang, J. K. Liao, F. H. Wu, et al., *Developing visual cryptography for authentication on smartphones,* International Conference on Industrial IoT Technologies and Applications, 2016. Available from: https://link.springer.com/chapter/10.1007/978-3-319-44350-8_19.

21. J. Lu, Z. Yang, L. Li, et al., Multiple schemes for mobile payment authentication using qr code and visual cryptography, *Mobile Inf. Syst.*, **2017** (2017), 1–12.

22. X. Yan, Y. Lu, H. Huang, et al., *Clarity Corresponding to Contrast in Visual Cryptography,* International Conference of Pioneering Computer Scientists, Engineers and Educators, 2016. Available from: https://link.springer.com/chapter/10.1007/978-981-10-2053-7_23.

23. X. Yan, S. Wang, A. A. El-Latif, et al., Visual secret sharing based on random grids with abilities of and and xor lossless recovery, *Multimedia Tools & Appl.*, **74** (2015), 3231–3252.

24.I. Jtc1/Sc, *Information technology—automatic identification and data capture techniques—qr code 2005 bar code symbology specification, ISO/IEC,* 18004 (2015).

25.X. Yan, S. Guan and X. Niu, *Research on the capacity of error-correcting codes-based information hiding,* Iihmsp '08 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008. Available from: https://ieeexplore.ieee.org/abstract/document/4604249.

26.K. Saito and M. Morii, Efficient decoding of QR code using error correcting capability : Decoding method using erasure error correction and the ability, *Tech. Rep. Ieice Isec*, **111** (2011), 79–84.

27.S. Wan, Y. Lu, X. Yan, et al., Visual secret sharing scheme for (k, n) threshold based on qr code with multiple decryptions, *J. Real-Time Image Process.*, 1–16.