Tech Science Press

Journal on Big Data
DOI:10.32604/jbd.2021.018618
Article

A Secure Visual Secret Sharing Scheme with Authentication Based on QR Code

Xinwei Zhong[*], Lizhi Xiong and Zhihua Xia

Nanjing University of Information Science & Technology, Nanjing, 210044, China
[*]Corresponding Author: Xinwei Zhong. Email: 846111780@qq.com

Received: 14 March 2021; Accepted: 01 April 2021

Abstract: With the rise of the Internet of Things (IoT), various devices in life and industry are closely linked. Because of its high payload, stable error correction capability, and convenience in reading and writing, Quick Response (QR) code has been widely researched in IoT. However, the security of privacy data in IoT is also a very important issue. At the same time, because IoT is developing towards low-power devices in order to be applied to more fields, the technology protecting the security of private needs to have the characteristics of low computational complexity. Visual Secret Sharing (VSS), with its features of safety and low computational cost, can fully meet the requirements of communication security in IoT. Therefore, a VSS scheme with QR code (VSS-QR) was proposed and has been applied to some extent. In VSS-QR, the secret is shared into a series of shares. These shares are usually common QR codes, which cannot cause the attention of the attacker. However, if there is dishonesty among participants, the secret cannot be recovered, which will lead to VSS-QR cannot be widely used due to its inadequate security. In this paper, we propose a visual secret sharing scheme with authentication based on QR code (VSSA-QR). Both the reconstructed secret QR code and shares can be verified whether they are forged by attackers. The above-mentioned operations conveniently are performed on low-power QR scanning devices. Not only does the proposed scheme prevent some dishonest participants or attackers from cheating, but also prevent all participants from conspiring. In addition, the payload is the QR code itself, which is higher than other schemes. Theoretical analysis and experiments prove that the proposed scheme is effective.

Keywords: QR code; visual secret sharing; low computational complexity; authentication

1 Introduction

With the commercialization of 5G network, a growing number of data in daily life will be digitized. At the same time, as people pay more attention to the privacy data, the security of the privacy data has become a very important topic. In traditional data security schemes, secret data is usually kept by only one person. If the data is lost or maliciously tampered with, the secret cannot be recovered. Therefore, in some situations, the secret can be distributed to a series of people for preservation. In 1979, Shamir [1] and Blakley [2] came up with the concept of secret sharing (SS) to address this problem. In SS, the secret is encoded into an array of shares, which are also referred to as shadows. Because of the security and convenience of SS, it has attracted extensive attention from researchers. After that, Shamir et al. [3] proposed Visual Secret Sharing (VSS) scheme in 1994, which applied SS to the binary images. In VSS, the qualified shares can be stacked to reveal the original secret. Because of its low computational cost, VSS can be applied to low-power devices so that it can be applied to more fields. Recently, researchers have made some achievements in VSS. In particular, Shen et al. [4] designed a VSS scheme for Machine-to-

Machine (M2M) communications with the Latin square to ensure that the transmission of information in M2M is secure and efficient. Tuyls et al. [5] proposed an XOR-based VSS (XVSS) scheme, in which the secret data is retrieved by XOR operation. The method improves the recovered image quality, and the computational cost is slightly increased. Since Internet of Things (IoT) was proposed, Quick Response (QR) code has become a very important cover in our daily life. Thus, the concept of the combination of QR code and VSS will inevitably become a hot research trend.

QR code, one of the most popular covers in our daily life, was first developed by Japanese company in 1994 [6]. Nowadays, it has become a very common coding method on mobile devices due to its convenience in reading and writing and error correction capability. Besides, compared with the traditional bar code, QR code can not only store more data, but also represent more types of data. Thus, QR code can be applied to more fields, such as mobile payment, login, information retrieval, etc. However, since QR code is generated by the universal standard published by ISO, anyone can get the message stored in the QR code easily. For this reason, there will be a lack of security for privacy when passing a QR code containing the privacy on a public channel [7–8]. To solve this problem, more and more researchers have proposed their solutions. At first, some researchers utilize the traditional watermarking or steganography [9] to embed QR code into the common covers. In this kind of methods, a common image and QR code are regarded respectively as a cover image and a secret image. QR code is stored into the covers, more precisely, it is embedded into the spatial domain [10] or frequency domain [11–12] of the covers. Thus, the capacity of these schemes is the payload of the QR code. But these methods don't directly use the nature of the QR code itself. In addition, it is a solution that the privacy is stored in the QR code with watermarking methods. Li et al. [13] designed a median coefficient comparison scheme by which the watermark is embedded into the intermediate frequency Discrete Cosine Transform (DCT) coefficients of the carrier QR. In this method, only data matrix with small capacity can be stored into covers. In [14], Rungraungsilp et al. embedded a watermark into QR code by combining DCT with Discrete Fourier Transform (DFT). However, these transform operations are computationally expensive, and the restored watermark is distorted to some extent. Considering the low-power barcode devices, the computational complexity of the QR code scheme should be minimized.

Since SS scheme was proposed, an increasing number of researchers began to apply SS scheme to QR code. Unlike the conventional watermarking or steganography mentioned above, the characteristics of QR code are fully utilized. In particularly, a (k, n) QR code SS scheme was first investigated by Chuang et al. [15]. They planned to share a secret message into n meaningless shares through a (k, n) secret sharing algorithm [16]. Then the corresponding QR codes can be generated based on these shares. When k qualified QR codes are collected, the secret message can be reconstructed by Lagrange interpolation method. But there is a flaw in this plan. For the common QR codes, it is suspicious to store these meaningless or odd messages. Afterwards, Chow et al. [17] proposed a (n, n) VSS with QR code. In their research, the secret QR code is shared into a list of shares by utilizing the error correction capacity of the QR code. Each generated share is a common QR code, which can reduce the possibility of being attacked by attackers in transmission. But most of the secret can be revealed by less than n shares, if the public information of cover QR code are similar with each other. For the sake of overcoming this defect, Cheng et al. [18] investigated a new sharing method based on VSS theory to solve this problem. However, if the share forged by the attacker is involved in the recovery process, the recovery process will be invalid. Therefore, Lin [19] proposed a (n, n) SS scheme to prevent cheating. In her research, the secret stream is firstly split into n shares with the same length. Afterwards, the master key of the authentication algorithm is obtained by the cooperation of the participants and the check code is generated by the authentication algorithm. After that, wet paper code (WPC) algorithm [20] is utilized to embed the share and the check code into the common cover QR code. Only when the attacker uses the fake cover and the real key, can the scheme identify the attacker. However, when a fake key forged by the dishonest participant is involved in the authentication process, the authentication process will be invalid because the master key of authentication algorithm is obtained by all participants' private keys. Besides, because the embedding index of each bit in the shared bit streams is generated by random function and the basic unit of the QR code is a consecutive 8 bits block, the payload of the cover QR codes is not as high as that proposed in this scheme. In fact, the payload ranges from 3 to 1215 bits for different versions of the QR code [21]. What's more, if all participants conspire to compromise the authentication process, in other words, they collaborate with each other to forge *n* private keys and n corresponding stego-QR codes, the authentication process would be compromised. Thus, a forged secret QR code will be obtained to fool other users. Recently, some researchers have found that it is possible to combine Reed Solomon (RS) homomorphism with the redundancy in the data region of the QR code [22–23]. If the data is embedded into the redundancy with RS homomorphism, the error correction capability of the QR code will not be affected. However, the payload of the above schemes is determined by the length of public message stored in the cover QR codes. In addition, validation capability is not taken into account in their schemes, so the stego-QR codes do not have the ability to cheat prevention.

Overall, a well VSS scheme based on QR code needs to meet the following characteristics: 1) high payload, 2) authentication capability, 3) robustness of covers, 4) low computational cost.

For the sake of solving the above issues, we design a secure Visual Secret Sharing scheme with Authentication based on QR code (VSSA-QR). In our scheme, the check code is generated by the check algorithm and the generated check information is embedded into the secret QR code without affecting any function. Then the embedded secret QR code is encoded into a collection of shares, which are very similar with the common QR codes. Therefore, the possibility of being attacked by the attacker can be reduced when these shares are transmitted. After that, the corresponding authentication codes are generated by the check algorithm according to shares and embedded into the shares. Therefore, the authentication system can check the authenticity of the stego-QR codes and the revealed secret QR code. Our contribution can be drawn as follows:

1. The proposed scheme designs a verification capability of the secret QR code, which can prevent some dishonest participants or attackers from cheating as well as preventing all participants from conspiring. In other words, the proposed scheme can prevent the deception that n dishonest participants forge n QR codes to conspire the users.

2. In this scheme, the time complexity of the recovery process is O(1), the time cost of the recovery process can be ignored since the size of QR code is small. Thus, the scheme can be applied to low-power mobile devices.

3. Each share not only does not disclose any secret stored in the secret QR code, but also is a common cover QR code, which can reduce the possibility of being attacked by the attacker. Moreover, the capacity of our scheme is higher than that of some other schemes.

This paper is organized as follows. Section 2 shows the preliminaries. In Section 3, the proposed schemes are shown. In Section 4, experiments are shown. Our conclusion is described in Section 5.

2 Quick Response Code

Quick Response (QR) code has been widely researched because of its error correction capability [17] and Reed Solomon (RS) homomorphism [22,24]. An example of RS homomorphism is illustrated by Tab. 1, assuming that both code1 and code2 are valid RS codes, the result code calculated by XORing code1 with code2 is still a valid RS code. Note that the result RS code does not destroy any function.

Table 1: Example of RS homomorphism

code1	1000100000001000110011001
code2	000000001000100010001000
result code	100010001001100100010001

3 The Proposed Scheme

3.1 Design Concept

For the sake of addressing the shortcomings described in Introduction, we investigate a (*n*, *n*) Visual

Secret Sharing scheme with Authentication based on QR code (VSSA-QR). In VSSA-QR, the authentication bits of shares can identify whether the attacker has tampered with shares and the verification bits in the secret QR code can help us prevent all participants from conspiring. Moreover, the computational complexity of XOR operation is lower than that of the polynomial methods and the time complexity of XOR recovery operation is O(1). In addition, the embedding capacity of our scheme is higher than that of some schemes, which is the secret QR code in itself.

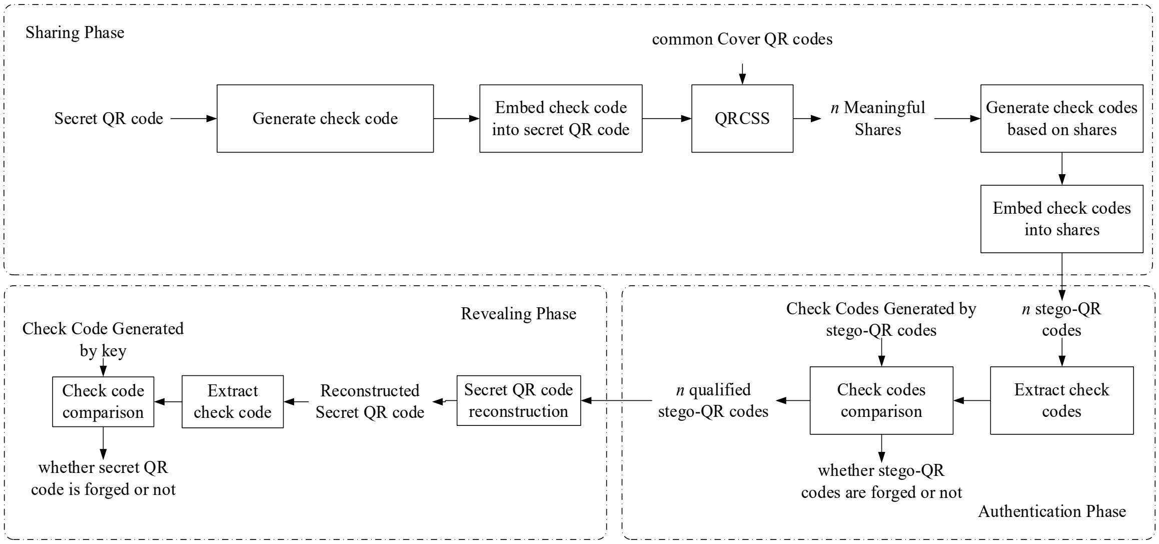

Sharing Phase
common Cover QR codes
Secret QR code
Generate check code
Embed check code into secret QR code
QRCSS
n Meaningful Shares
Generate check codes based on shares
Embed check codes into shares
Revealing Phase
Check Code Generated by key
Check code comparison
Extract check code
Reconstructed Secret QR code
Secret QR code reconstruction
whether secret QR code is forged or not
Check Codes Generated by stego-QR codes
n stego-QR codes
n qualified stego-QR codes
Check codes comparison
Extract check codes
whether stego-QR codes are forged or not
Authentication Phase

Figure 1: The framework of VSSA-QR

Fig. 1 presents the general framework of VSSA-QR. In the sharing phase, the check code is first generated by the authentication function and used to replace the padding codewords in the secret QR code with RS homomorphism. Secondly, the embedded secret QR code is encoded into a series of shares according to QRCSS, which are common QR codes. Then, the check code of the shares is obtained by the authentication function and embedded into the shares to get the final QR codes. In the authentication process, the check code in the stego-QR code is used to judge the authenticity of the stego-QR code. In the reconstruction process, the secret QR code can be revealed by a series of qualified stego-QR codes with XOR operation. Finally, the authenticity of the secret QR code can be judged according to the check code stored in the secret QR code.

3.2 Secret Sharing Procedure

1) Preliminary Phase: It is necessary to embed authentication code VQ in it in line with RS homomorphism to prevent all participants collaborating with each other to cheat before sharing the secret QR code Q. The secret QR code embedded with authentication code will not sacrifice any of its original capability.

Step 1) The payload of the verification code VQ in the secret QR code can be calculated in line with its public message, version, and error correction level.

$$l_{VQ} = 8 \times R - \sum_{j=1}^{m}\left(M_j + I_j + D_j\right) - T \tag{1}$$

where R is the quantity of units (Each unit consists of 8 bits) in the data region, m is the quantity of pieces in the QR code, M_j is the length of the mode indicator in each piece, I_j is the length of the character count indicator in each piece, D_j is the length of the input data characters in each piece, T is the length of the terminator.

Step 2) Because a dealer controls the secret sharing algorithm and reconstruction algorithm, the authentication code VQ is obtained by the authentication function (the authentication function can be random number generator or some other function) in line with the key *MK* owned by the dealer and is utilized to replace the padding codewords in line with to RS homomorphism. In the light of the key *MK*, the dealer can identify whether the secret QR code is forged by a conspiracy of all participants. The authentication code *VQ* of the secret QR code can be obtain by

$$VQ = G(MK) \tag{2}$$

where *G* is a random number generator.

Step 3) Before embedding the authentication code *VQ* into the secret QR code *Q*, padding bits *P* is first calculated by decoding the unmask secret QR code, in which the length of the padding bits *P* is consistent with the length of the authentication code *VQ*. Then, the modified padding stream *MP* can be obtained by XORing of the authentication code *VQ* and the padding bits *P*.

$$MP = XOR(VQ, P) \tag{3}$$

Step 4) Suppose there are a total of R codewords in the data region. $8 \times R - l_{VQ}$ bits zero is added in the front of the modified padding stream *MP* to form a data stream *DS* of the RS code with $8 \times R$ bits. Afterwards, by inputting this data stream *DS* into RS algorithm, a temporary code *NRS* can be calculated. At last, by XORing the temporary code *NRS* with the RS code in the original secret QR code, the result code *FRS* embedding in the secret QR code can be obtained.

$$FRS = XOR(ORS, NRS) \tag{4}$$

2) Share Derivation Phase: The secret QR code embedded with authentication code is denoted as Q'. In this phase, Q' is divided into n meaningful shares $S_i'(1 \le i \le n)$ with n common cover QR codes S_i. Then, the authentication code of the shares is obtained by the authentication function and embedded into the shares to obtain the final stego-QR codes S_i''.

Step 1) The figure for modified codewords L_e in a block of the share is first calculated.

$$L_e = d - c + r + 1 \tag{5}$$

where d represents the minimum number of codewords per block in the secret QR code, which is divided to these shares, c is the quantity of codewords per block, r is the error correction payload of each block.

Step 2) Suppose that the cover QR code has b blocks. This distribution algorithm is proposed in this scheme, which can ensure that any secret cannot be revealed by no more than *n* shares. As is shown in Tab. 2, the *ib*-th ($ib = i \bmod b, 1 \le i \le n$) block of each share is first divided into L_e codewords. '$*$' represents that the value is randomly obtained from distributing the rest of codewords in each block.

Table 2: Number of codewords in each share

	1	2	3	...	$n-1$	n
1	L_e	$*$	$*$	$*$	L_e	$*$
2	$*$	L_e	$*$	$*$	$*$	L_e
...	$*$	$*$	L_e	$*$	$*$	$*$
b	$*$	$*$	$*$	L_e	$*$	$*$

Step 3) Then the remaining codewords *RE* of each block are assigned randomly to the corresponding block of each share. In particularly, the number of the changed codewords per block is not exceeded *r*.

$$RE = d - N_{L_e} \times L_e \text{ where} \begin{cases} N_{L_e} = \lfloor n/b \rfloor + 1 \ (n \bmod b \ge bi, 1 \le bi \le b) \\ N_{L_e} = \lfloor n/b \rfloor \ (\text{others}) \end{cases} \tag{6}$$

where *RE* is the figure for remaining codewords per block, and N_{L_e} is the quantity of L_e in each block.

Step 4) In order to keep attackers or dishonest participants from tampering with the share $S_i'(1 \le i \le n)$ to invalidate the recovery phase, Hash-based Message Authentication Code (HMAC) is used (In the experimental of this paper, the hash function uses SHA-1). At the same time, so as to keep cheaters from compromising the verification phase in the light of the share owned by other participants, the input of hash function needs to be appended with the identification (ID) of the share. Then, the authentication code $V_i(1 \leq i \leq n)$ of the same length as the remainder bits can be obtained by XORing 160bits output of the hash function as shown in the following formula:

$$V_i = XOR < H_K(S_i'||I_{ID}) > \tag{7}$$

where I_{ID} is the identification of the share.

Step 5) The authentication code $V_i(1 \leq i \leq n)$ is embedded into the remainder bits of the corresponding share to get the result QR code S_i''. Note that remainder bits are the redundant bits of the QR code. That is to say, if remainder bits are damaged, it does not affect any function of the QR code.

3.3 Secret Revealing Procedure

Before performing the recovery phase, the stego-QR code needs to be judged whether it has been tampered with by attackers to avoid invalidation of recovery phase. In the authentication phase, the authentication code $V_i'(1 \leq i \leq n)$ can be generated according to the following formula. If V_i' is the same as the authentication code V_i in the stego-QR code S_i'', it means that the QR code is true; otherwise, it means that the QR code is forged by the cheater.

$$V_i' = XOR < H_K(S_i'||I_{ID}) > \tag{8}$$

where I_{ID} is identification of the share.

Then, the secret QR code with authentication code can be restored by XORing the module of each share's encoding region and adding the function patterns. Because the size of the QR code is 21-177, the size of the encoding region is relatively reduced. On the other hand, the time complexity of XORing operation is O(1), so the computational cost of the recovery process is very low. After reconstructing the secret QR code, it is necessary to judge its authenticity. The authentication code VQ can be generated by the following formula according to the dealer's key and is compared to the authentication code VQ' stored in the secret QR code. If the result is false, it is proved that the secret QR code was forged by a conspiracy of all participants; otherwise, the secret QR code is true.

$$VQ' = G(MK) \tag{9}$$

where *G* is a random number generator, *MK* is the key of the dealer.

4 Experiment

In this section, experimental results, embedding capacity, authentication capability, robustness, and overall comparison are respectively elaborated in detail. All experiments were implemented on MATLAB 2018A with i5-7300HQ CPU, 8 GB RAM, and Windows 10. The open-source library of ZXing is utilized to write and read the QR code for experiments.

4.1 Experiment Results

In the experiment, (3, 3) threshold VSSA-QR scheme is taken as an example to explain the experimental results in detail. The secret QR code with error correction level H and version 4 is selected. Since the format of the cover QR code must be consistent with the secret QR code, 4-H cover QR codes are selected. The results of the secret QR code for the (3, 3) threshold VSSA-QR scheme are presented in Fig. 2. As presented in Fig. 2(a), the QR code containing the message "Secret Quick Response Code" is selected as the privacy. The number of padding codewords is 8 for the secret QR code, so the length of embedded verification code is 64 bits. Fig. 2(b) is the secret QR code after storing the verification code in line with RS homomorphism. Although some codewords are damaged as presented in Fig. 2(c), the error correction function of the embedded secret QR code has not been compromised. At the same time, if the verification code is occupied by the damaged part, the verification code can be restored based on the error correction function. In addition, the aesthetic of the secret QR code can be improved by the beautification scheme [25].

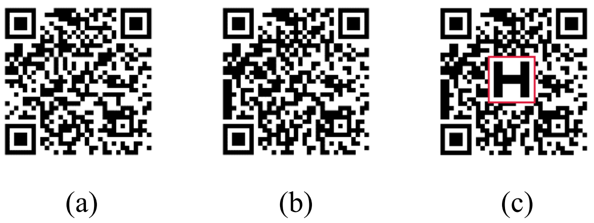


Figure 2: The results of secret QR code for (3, 3) threshold VSSA-QR scheme. (a) Secret QR code, (b) Embedded Secret QR code and (c) Damaged Secret QR code

The experiment results for (3, 3) threshold VSSA-QR scheme are depicted in Fig. 3. The version and error correction level of all QR codes in the result are 4 and H, respectively. The secret QR code embedded with the verification code in the light of RS homomorphism is presented in Fig. 3(a). Figs. 3(b)–3(d) present original cover QR codes with 7bits-remainder bits. Thus, the length of the embedded authentication code is 7. Figs. 3(e)–3(g) present stego-QR codes from the proposed Algorithm 1. These stego-QR codes are common QR codes, which can be read by a scanner according to QR code standard. Fig. 3(h) presents the revealed secret QR code, which was reconstructed by XORing all stego-QR codes. The revealed secret QR code can be verified by the stored authentication code with low computational cost, and the privacy decoded from the recovered secret QR code is consistent with that in the original secret QR code.

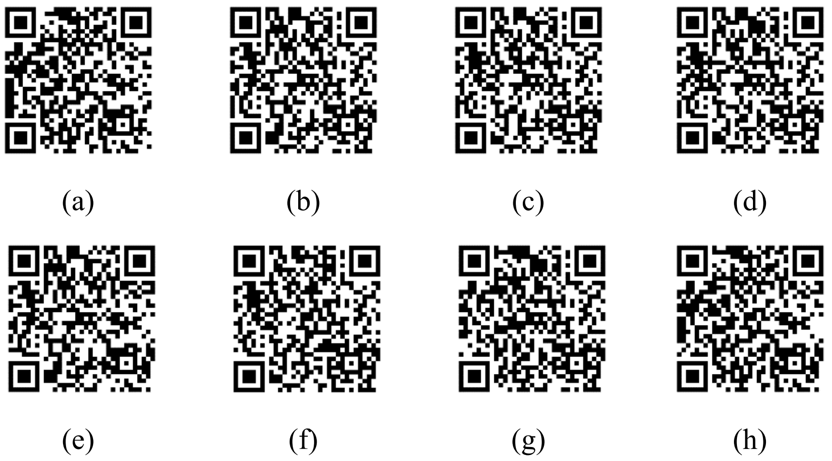


Figure 3: The experiment results for (3, 3) threshold VSSA-QR scheme. (a) Embedded secret QR code, (b) Cover QR code1, (c) Cover QR code2, (d) Cover QR code3, (e) Stego-QR code1, (f) Stego-QR code2, (g) Stego-QR code3 and (h) Reconstruct Secret QR code

4.2 Embedding Capacity

In this part, the embedding payload of our proposed scheme is elaborated in detail and made a comparison with other schemes [15,17–19]. The comparison of embedding capacity is shown in Tab. 3. In Chuang's scheme [15], since the secret is encoded into an array of shares with the same length as the secret and stego-QR codes are obtained in line with the shares, the embedding capacity is the length of the public information stored in the QR code. Specifically, for different versions and error correction levels, the embedding capacity ranges from about 72 to 23648 bits. Note that the generated stego-QR codes in [15] are meaningless, so that it is easy to be noticed by attackers in transmission. In Lin's scheme [19], the actual embedding capacity is 3–1215 bits due to the randomness of embedding algorithm [21]. In Chow [17] and Cheng [18], and our schemes, since the secret QR code is directly shared, the embedding capacity is the secret QR code in itself. Suppose (3, 3) scheme with 4-H QR code is taken as an example. Specifically, the actual embedding capacity of Chuang's scheme is 288bits in the light of QR code standard. In Lin's scheme, the total embedding capacity including authentication code is 32bits, thus the actual payload of the secret is less than 32 bits. In Chow [17] and Cheng [18], and our schemes, since the shared secret is the secret QR code in itself, the embedding capacity is 4-H QR code in itself. Obviously, the embedding capacity in our scheme is higher than that in Chuang and Lin's schemes.

Table 3: Comparison of embedded capacity

Scheme	Embedding capacity	Embedding capacity of (3, 3) scheme with 4-H QR
[15]	the length of the public message stored in the QR code	288bits
[17]	Secret QR code in itself	4-H Secret QR code in itself
[18]	Secret QR code in itself	4-H Secret QR code in itself
[19]	3–1215 bits	Less than 32 bits
Ours	Secret QR code in itself	4-H Secret QR code in itself

4.3 Authentication Capability

In this part, the authentication capability of this proposed scheme is elaborated in detail and made a comparison with other schemes [15,17–19] shown in Tab. 4. In [15, 17–18], since the generated stego-QR codes are not embedded with any authentication code, their schemes have no authentication capability. In Lin's scheme [19], the authentication code is generated not based on the share but based on the participant's key, in other words, if a cheater provides a false key, the verification process will be easily invalid. Thus, the stego-QR codes in Lin's scheme do not have the authentication capability to resist attacks from dishonest participants [21]. In our proposed scheme, the authentication code of the same length as the remainder bits is generated according to the share. Therefore, the length of the authentication code is the length of the remainder bits in the QR code. It can be found that the length of remainder bits is 1-7bits for different versions according to ISO/IEC 18004 standard, so the maximum length of authentication information in stego-QR codes is 7 bits. Suppose (3, 3) scheme with 4-H QR code is taken as an example. Specifically, because the length of remainder bits in the QR code is 7, the payload of authentication code in our scheme is 7 bits.

Table 4: Comparison of authentication capability for Stego-QR code

Scheme	Number of Authentication bits	Authentication bits of (3, 3) scheme with 4-H QR
[15]	0	0
[17]	0	0
[18]	0	0
[19]	0	0
Ours	The length of remainder bits	7 bits

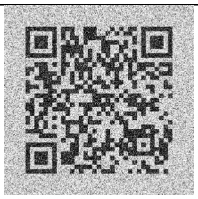
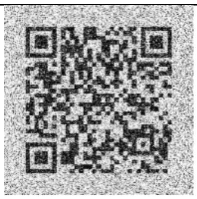
In order to avoid the participants cooperating with each other to forge the secret QR code to cheat the dealer, the verification code is stored in the secret QR code in our paper. Meanwhile, the embedded secret QR code will not affect any function of the original secret QR code. Tab. 5 shows a comparison for the secret with other schemes. As the authentication ability of the secret is not considered in other schemes, the authentication capability in other schemes is not able to resist the collusion attack of participants. In our scheme, the length of the authentication code is determined by the padding region, so the length of the verification code is the length of the padding region. According to different versions and error correction levels of the secret QR code, the maximum length of authentication information is about 5200 bits. Specifically, suppose a 4-H QR code with content "Secret Quick Response Code" is the secret, the length of the authentication code is 64 bits because the length of padding codewords is 8.

Table 5: Comparison of authentication capability for secret

Scheme	Number of Authentication bits	Authentication bits of (3, 3) scheme with 4-H secret QR
[15]	0	0
[17]	0	0
[18]	0	0
[19]	0	0
Ours	$8 \times R - \sum_{j=1}^{m} \left(M_j + I_j + D_j\right) - T$	64 bits

4.4 Robustness

Table 6: Results of 4-H Stego-QR codes after common attacks

Common Attacks	**Gaussian noise:** ***50%***	**Gaussian noise:** ***70%***	**Uniform noise:** ***50%***	**Uniform noise:** ***70%***
Attacked QR code				
Common Attacks	**Gaussian blurring:** ***2 pixels***	**Gaussian blurring:** ***3 pixels***	**Compression: JPEG 2000 70%**	**Compression: JPEG 2000 100%**
Attacked QR code				
Common Attacks	**Rotation:** ***45°***	**Rotation:** ***90°***	**Rotation:** ***135°***	**Rotation:** ***270°***
Attacked QR code				
Content **Secret**	Readable Decodable	Readable Decodable	Readable Decodable	Readable Decodable

Because QR codes are usually published in paper documents or transmitted in public channels, the QR codes with the public message are subject to various common attacks. In daily life, common attacks mainly include Gaussian noise, Uniform noise, Gaussian blur, compression, and rotation. Therefore, the experiments in this section are mainly implemented from these common attacks. Tab. 6 shows the robustness of the stego-QR codes. When the QR code is transmitted, it is easy to be affected by noise. In the noise experiment, stego-QR codes are added with Gaussian noise and Uniform noise at 50% and 70%. In addition, so as to improve the storage payload of the device, the data is usually compressed. Nowadays, JPEG 2000 has become a common compression technology because of its low distortion. Here, stego-QR codes is implemented according to JPEG 2000 with quality factors (Q) of 70% and 100%. Since QR codes are usually read by mobile devices, rotation attacks need to be tested. As shown in Tab. 6, stego-QR codes can still be read normally after these attacks. Meanwhile, secret QR codes can also be reconstructed successfully. It should be noted that the decoded result of the QR code is affected by different lights, mobile devices, and scanners [26].

5 Conclusion

In our scheme, we investigate a (n, n) Visual Secret Sharing scheme with Authentication based on QR code (VSSA-QR). In our proposed scheme, in line with RS homomorphism and remainder bits of the QR code, the authentication capability of the secret QR code and the stego-QR code is realized respectively. Therefore, the proposed scheme not only avoids the deception of individual participants, but also can resist the collusion attack of the participants. In addition, because the recovery of the secret QR code is carried out through XOR operation, the recovery process in our scheme has a lower computational complexity than that in some schemes. The embedding capacity in our scheme is the secret QR code in itself, because the secret QR code is shared directly. Therefore, the embedding capacity is higher than that of some schemes. The experiment results prove the performance of our proposed scheme. In the future work, the scheme will be improved from the following two aspects. First, the authentication capability of stego-QR codes will be further improved to reduce the possibility of cheating the authentication process. Second, the cover QR codes in the scheme will be extended to the artistic QR codes to improve the aesthetics of stego-QR codes.

Funding Statement: This work was supported in part by the Startup Foundation for Introducing Talent of Nanjing University of Information Science and Technology under Grant 2016r055, and in part by the Priority Academic Program Development (PAPD) of Jiangsu Higher Education Institutions.

Conflicts of Interest: The authors declare that they have no conflicts of interest.

References

[1] A. Shamir, “How to share a secret,” *Communications of the ACM,* vol. 22, no. 11, pp. 612–613, 1979.

[2] G. R. Blakley, “Safeguarding cryptographic keys,” *Proceedings of the National Computer Conference,* vol. 48, no. 313, 1979.

[3] M. Naor and A. Shamir, “Visual cryptography,” *Lecture Notes in Computer Science,* vol. 950, no. 9, pp. 1–12, 1994.

[4] J. Shen, T. Zhou, X. Liu and Y. C. Chang, “A novel Latin-Square-based secret sharing for M2M communications,” *IEEE Transactions on Industrial Informatics,* vol. 14, no. 8, pp. 3659–3668, 2018.

[5] P. Tuyls, H. D. Hollmann, J. H. Van Lint and L. Tolhuizen, “XOR-based visual cryptography schemes,” *Designs, Codes and Cryptography,* vol. 37, no. 1, pp. 169–186, 2005.

[6] Information Technology—Automatic Identification and Data Capture Techniques—QR Code, I. I. 18004, 2005.

[7] P. Kieseberg, M. Leithner, M. Mulazzani, L. Munroe, S. Schrittwieser *et al.,* “QR code security,” in *Proc. of the 8th Int. Conf. on Advances in Mobile Computing and Multimedia,* pp. 430–435. 2010.

[8] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu and D. Qiu, “Security of the internet of things: perspectives and challenges,” *Wireless Networks,* vol. 20, no. 8, pp. 2481–2501, 2014.

[9] P. Y. Lin and Y. H. Chen, “High payload secret hiding technology for QR codes,” *EURASIP Journal on Image and Video Processing,* vol. 2017, no. 1, pp. 14, 2017.

[10] H. C. Huang, F. C. Chang and W. C. Fang, “Reversible data hiding with histogram-based difference expansion for QR code applications,” *IEEE Transactions on Consumer Electronics,* vol. 57, no. 2, pp. 779–787, 2011.

[11] C. H. Chung, W. Y. Chen and C. M. Tu, “Image hidden technique using QR-barcode,” in *Fifth Int. Conf. on*

Intelligent Information Hiding and Multimedia Signal Processing, pp. 522–525, 2009.

[12] W. Y. Chen and J. W. Wang, “Nested image steganography scheme using QR-barcode technique,” *Optical Engineering,* vol. 48, no. 5, 2009.

[13] L. Li and R. L. Wang, “A digital watermarking algorithm for QR code,” *Journal of Hangzhou Dianzi University,* vol. 31, no. 2, pp. 46–49, 2011.

[14] S. Rungraungsilp, M. Ketcham, V. Kosolvijak and S. Vongpradhip, “Data hiding method for QR code based on watermark by compare DCT with DFT domain,” in *3rd Int. Conf. on Computer and Communication Technologies,* pp. 144–148, 2012.

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

[16] A. Shamir, “How to share a secret,” *Communications of the ACM,* vol. 22, no. 11, pp. 612–613, 1979.

[17] Y. W. Chow, W. Susilo, G. Yang, J. G. Phillips, I. Pranata *et al.,* “Exploiting the error correction mechanism in QR codes for secret sharing,” in *Australasian Conf. on Information Security and Privacy,* pp. 409–425, 2016.

[18] Y. Cheng, Z. Fu and B. Yu, “Improved visual secret sharing scheme for QR code applications,” *IEEE Transactions on Information Forensics and Security,* vol. 13, no. 9, pp. 2393–2403, 2018.

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

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

[21] P. C. Huang, C. C. Chang and Y. H. Li, “Sudoku-based secret sharing approach with cheater prevention using QR code,” *Multimedia Tools and Applications,* pp. 1–20, 2018.

[22] P. Huang, Y. Li, C. Chang and Y. Liu, “Efficient QR code authentication mechanism based on Sudoku,” *Multimedia Tools and Applications,* vol. 78, no. 18, pp. 26023–26045, 2019.

[23] L. Tan, Y. Lu, X. Yan, L. Liu and X. Zhou, “XOR-ed visual secret sharing scheme with robust and meaningful shadows based on QR codes,” *Multimedia Tools and Applications,* vol. 79, pp. 5719–5741, 2020.

[24] Cox R, Qart Codes. [Online]. Available: http://research.swtch.com/qart. 2012.

[25] S. S. Lin, M. C. Hu, C. H. Lee and T. Y. Lee, “Efficient QR code beautification with high quality visual content,” *IEEE Transactions on Multimedia,* vol. 17, no. 9, pp. 1515–1524, 2015.

[26] D. Munoz-Mejias, I. Gonzalez-Diaz and F. Diaz-de-Maria, “A low-complexity pre-processing system for restoring low-quality QR code images,” *IEEE Transactions on Consumer Electronics,* vol. 57, no. 3, pp. 1320–1328, 2011.