

Efficient secret sharing scheme with cheater identification based on QR code

Peng-Cheng Huang^{1,2}, Chin-Chen Chang², Yung-Hui Li^{3,*}, Yanjun Liu²

¹Department of Computer Science and Technology,
Xiamen University of Technology, Xiamen 361024, China,
[e-mail: pc4hpc@gmail.com]

²Department of Information Engineering and Computer Science,
Feng Chia University, Taichung 207, Taiwan
[e-mail: alan3c@gmail.com]

³Department of Computer Science and Information Engineering,
National Central University, Taoyuan 320, Taiwan
[e-mail: yunghui@csie.ncu.edu.tw]

* Corresponding author: Yung-Hui Li

*Received November 23, 2018; revised March 16, 2019; accepted April 5, 2019;
published October 31, 2019*

Abstract

Secret sharing is an effective way of protecting secret messages. However, the traditional secret sharing schemes are considered meaningless due to malicious people attention which might raise risks. To overcome the weakness, this paper presents an effective secret sharing scheme with the functionality of cheater identification, based on meaningful QR code. The secret message will be split and concealed in the padding region of cover QR codes with the assistance of Latin square and it can be completely restored when all the involved participants cooperate. The concealing strategy exploits the characteristic of Reed-Solomon (RS) code to ensure the strong robustness of generated QR code pseudo-shares. The meaningful QR code pseudo-shares help to reduce the curious of unrelated persons. Some experiments were done to evaluate the performance of proposed scheme. The results showed that the proposed scheme is feasible, efficient and secure compared to the other existing schemes. It also achieves a higher secret payload and maintains stronger robustness.

Keywords: Secret sharing, cheater identification, QR code, Reed-Solomon code, Latin square

This study was funded by the NSFC (grant number 61672442 and grand number 61872436), the Fujian NSF (grant number 2016Y0079 and grand number 2016J01327), the Quanzhou Science and Technology Plan Project (grant number 2017G030).

1. Introduction

Secret sharing (SS) schemes were invented by Shamir and Blakley independently in 1979 to protect the highly sensitive messages and has been extensively studied in recent years. In a typical (t, n) -threshold secret sharing scheme, the sensitive message divided into n shares and assigned to n involved participants. The sensitive message would be successfully reconstructed only when any t or more than t involved participants cooperate. The reconstruction process will fail when combination is fewer than t shares. Through this way, the sensitive message is protected. There are many well-known secret sharing schemes, such as Shamir's SS [1], Blakley's SS [2] and Azimuth-Bloom's SS [3], but the sharing of these schemes are considered meaningless due to malicious people's interest, which leads to the potential risk. To overcome this type of weakness, many researchers studied the secret sharing schemes in which the sensitive information are encoded into meaningful image shares [4-11]. The meaningful image shares helped effectively to reduce malevolent people's attention.

With the development of smart phone and Internet of Things (IoT), QR codes severed as interactive medium and widely used in various fields, such as mobile payment, marketing, production tracking and many others. QR code has a characteristic of faster readability and higher storage compared to one dimensional barcode. Therefore, researchers start to study the secret sharing schemes based on QR code.

In 2010, Chuang et al. [12] firstly proposed a (t, n) -threshold secret sharing scheme based on QR code. The scheme employed the concept of Shamir's SS to divide the secret message into n secret shares, and generated n shadows in the form of QR code by concealing these secret shares as the public message of QR codes. In the secret recovering procedure, any t out of n QR codes can be used to recover secret message by the Lagrange polynomial interpolation. However, for QR code as a public patent, the secret shares as the public of QR code would cause security issues. Anyone can decode the secret share with general QR code reader. The cheater can easily forge a fake QR code with secret share read from a real QR code shadow. Unfortunately, this fake QR code is treated as a valid shadow in the secret revealing process which lead to secret message leakage.

To enhance system security, Lin [13] exploited the QR code error correction capacity by proposing an (n, n) -threshold secret sharing scheme. Lin's scheme employed the technology of wet paper code [14] to randomly embed both the secret share and authentication message in cover QR codes. This randomly embedding strategy would produce a lot of QR code error codewords, and reduce the error correction capacity. The generated QR code pseudo-shares are still valid unless the error correction capacity bankrupt. The meaningful QR code pseudo-shares reduce malevolent people's attentions with the help of the cheater detection function which makes it difficult to forge a fake QR code pseudo-shares. Chow et al. [15] and He et al. [16] proposed two QR code secret sharing scheme to improve the security of Chuang's scheme. Their schemes employed the symmetric encryption algorithm to encrypt shares before embedding shares into the meaningful cover QR codes. The encrypted shares embedding strategies of these two schemes are also based on QR code error correction capacity. Huang et al. [17] utilized the concept of Sudoku puzzle and Shamir's SS to propose a (t, n) -threshold secret sharing scheme with the functionality of cheater prevention. This scheme converted the secret shares into Sudoku digit stream and sequentially replaced them with the data codewords of cover QR codes. The byte-based embedding strategy produces

minimum errors for QR code decoding. The secret payload would be much higher than that of Lin's scheme with randomly embedding strategy. At the same time, Huang et al.'s scheme embedded the secret key along with secret share in the cover QR code. The participants do need to hold the additional secret embedding keys but just the QR code pseudo-shares.

Noting that all these four schemes exploited the redundancy check mechanism of QR code to recover the errors caused by secret embedding process, but there are still several flaws in this kind of schemes. Firstly, the secret payload is limited by the error correction capacity of cover QR code. Secondly, the secret shares embedding strategy would reduce the QR code error correction capacity, so the generated QR code pseudo-shares became vulnerable to withstand image attacks, such as noising, fouling, print-and-scan processing. Therefore, the robustness of the QR code pseudo-shares is poor.

Furthermore, both Lin's scheme and Huang et al.'s scheme implemented the functionality of cheater prevention. First, in the secret revealing procedure, the cheater identification process is performed to detect and identify the malicious participants. Only through the valid verification of QR code pseudo-shares and secret keys, the secret retrieval process would be performed to reconstruct the secret message. This creates difficulty for malicious people to forge a fake QR code pseudo-shares. However, both the cheater prevention mechanisms are defective. The cheater detection functionality of Lin's scheme is available only when the dishonest participant provides a real secret key and a fake QR code pseudo-shares. All the participants' secret key together served as an input to generate the authentication stream, so the cheater detection would fail when the dishonest participant provides a fake secret key. But for Huang et al' scheme, the authentication message depends on secret keys extracted from two sequential QR code pseudo-shares, so the functionality of cheater detection of Huang et al' scheme is available only when the condition $t = n$ is satisfied.

Taking the above-mentioned flaws of existing works into consideration, we propose a new (n, n) -threshold secret sharing scheme with cheating prevention based on QR code. The proposed scheme divides the secret message into n secret shares, and disguises them as a series of coordinate position information of Latin square to prevent from leakage. The disguised shares along with authentication message will be embedded in the padding region of cover QR codes by utilizing the XORed characteristic of Reed-Solomon code. Finally, the generated QR code pseudo-shares will be distributed to involved participants. In the secret construction procedure, the legitimacy of QR code pseudo-shares will be verified before secret constructing to prevent secret message from being illegally acquired. Experimental results showed that the proposed scheme is feasible, efficient and keyless, also the generated QR code pseudo-shares can resist common image attacks such as noising, blurring, fouling, damaging and so on. Comparison with existing works demonstrates the proposed scheme achieves a much higher secret payload.

The organization of this paper is as follows: Section 2 briefly introduces the technology of QR code and Latin square, especially the XORed characteristic of Reed-Solomon code. Section 3 presents the secret sharing procedure and the secret construction procedure of the proposed scheme. Section 4 shows the performance of the proposed scheme, including secret payload, security analysis and robustness analysis. It also conducts the comparisons with existing works. Section 5 concludes this paper.

2. Preliminary

This section briefly introduces the technology of QR code and Latin square, especially the XORed characteristic of RS code.

2.1 The technology of QR code

A standard QR code consists of black and white modules that randomly arranged into a square. It always contains data codewords, error correction codewords and functional patterns. The QR code standard provides 40 user-selectable versions and 4 different error correction levels for each version. QR code employs the Reed-Solomon error correction mechanism to ensure its decodability even if it suffered from different kind of attacks. According to the QR code specification, two codewords of error correction code can correct one codeword's error. Russ Cox [18] pointed out that two RS codes with the same length of data codewords and error correction codewords can be XORed. The result of XOR operation is still a valid RS code. It means that one RS code can be derived from two other RS codes. For instance, assume that two RS codes A and B consist of 8 bits data and following 4 bits error correction code. The XOR operation result C shown in Table 1 is still a valid RS code.

Table 1. An XOR operation result of two RS codes

RS codes	Data codewords	Error correction codewords
A	0011 0101	1001
B	1000 1000	0101
C	1011 1101	1100

From another point of view, assume that we try to flip the 1st bit and 5th bit data codewords of RS code A, we can construct a data codewords 10001000 whose data bits are all zero except the 1st bit and 5th bit, and generate the corresponding error correction codewords by using Reed-Solomon algorithm and add them to the tail of data codewords to form RS code B. The result C will be derived by XORing RS code A with RS code B. The XOR operation not only flipped the 1st bit and 5th bit of RS code A, but also kept the result C to be a valid Reed-Solomon code.

Noting that the content of QR code is combination of several RS codes. Utilizing the XOR characteristic of RS code, we can flip any bits of data codeword of QR code, but without scarifying the error correction capacity of QR code.

2.2 Latin square

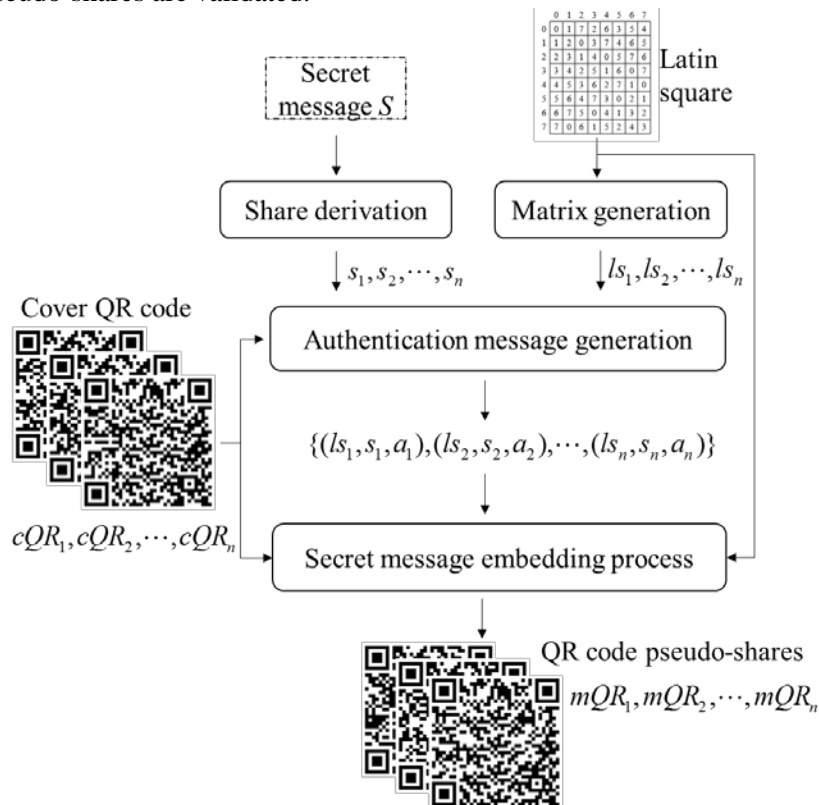
Latin square, introduced by Leonhard Euler is an $n \times n$ size of array filled with n different symbols. Each symbol only occurs once in each row and each column. According to [19], the number of possible solutions of an $n \times n$ Latin square is growing exponentially. Table 2 is the example of 8×8 sized Latin square with eight numbers from 0 to 7. The total possible solutions of an 8×8 Latin square are $108,776,032,459,082,956,800 \approx 1.09 \times 10^{20}$ [20]. We take advantage of this feature to disguise the secret shadow message into Latin square matrix coordinates in our proposed secret sharing procedure described in Section 3.1, to satisfy the requirement of security and reversibility.

Table 2. An example of 8×8 Latin square

	0	1	2	3	4	5	6	7
0	0	1	7	2	6	3	5	4
1	1	2	0	3	7	4	6	5
2	2	3	1	4	0	5	7	6
3	3	4	2	5	1	6	0	7
4	4	5	3	6	2	7	1	0
5	5	6	4	7	3	0	2	1
6	6	7	5	0	4	1	3	2
7	7	0	6	1	5	2	4	3

3. The proposed scheme

Based on the XORed characteristic of RS code and the technology of QR code, we design a new (n, n) -threshold secret sharing scheme to protect secret message with meaningful QR code pseudo-shares. Fig. 1 illustrates the flowchart of secret sharing procedure of the proposed scheme. There is a dealer and n participants in the proposed scheme. In the secret sharing procedure, the dealer is responsible for secret shares derivation, authentication message generation and message embedding in cover QR code. In the secret revealing procedure, firstly the dealer verifies the legitimacy of QR code pseudo-shares that provided from n participants to prevent cheater, and then reconstructs the secret message when all the QR code pseudo-shares are validated.

**Fig. 1.** The flowchart of secret sharing procedure of the proposed scheme

Noting that data bits in the padding region of QR code is useless and meaningless, the proposed scheme tends to embed the secret share s_i and the authentication message a_i in the padding region of the cover QR code with the assistance of Latin square. Fig. 2 illustrates the composition of RS code within QR code of the proposed scheme.

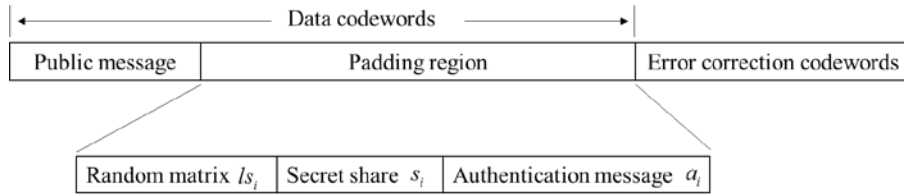


Fig. 2. The composition of RS code within QR code of the proposed scheme

3.1 (n, n)-threshold secret sharing procedure

Assume that there is a secret message S to be shared among n participants, who held n cover QR codes marked as $cQR_1, cQR_2, \dots, cQR_n$, respectively.

Step 1 Generate $n-1$ random secret shares s_1, s_2, \dots, s_{n-1} of the same length as S . Then derive secret share s_n by XORing S with these secret shares s_1, s_2, \dots, s_{n-1} .

$$s_n = s_1 \oplus s_2 \oplus \dots \oplus s_{n-1} \oplus S. \quad (1)$$

where \oplus denotes the exclusive-or (XOR) operation.

Step 2 Randomly choose a Latin square LS with size of 8×8 as secret shares embedding key. Then generate $n-1$ random matrices $ls_1, ls_2, \dots, ls_{n-1}$ with the same size as Latin square LS , all elements of these matrices are in the range of $(0, 7)$. Finally, derive the last matrix ls_n by XORing Latin square LS with those random matrices $ls_1, ls_2, \dots, ls_{n-1}$.

$$ls_n = ls_1 \oplus ls_2 \oplus \dots \oplus ls_{n-1} \oplus LS. \quad (2)$$

Step 3 Read public message pm_i and RS code rs_i of the cover QR code cQR_i .

$$\Gamma(cQR_i) = \{pm_i, rs_i\}, \quad (3)$$

where $1 \leq i \leq n$ and $\Gamma(*)$ denotes QR code reading function. According to the length of public message of cover QR code, the scope of padding region can be easily deduced. The secret share and the authentication message will be embedded in padding region of cover QR code as shown in Fig. 2. The upper bound of secret payload is determined by the length of padding region.

Step 4 Convert secret share s_i to be octal digital stream $\{d_1, d_2, \dots, d_k\}$. Convert the corresponding message in cover QR code padding region to be octal digital stream $\{p_1, p_2, \dots, p_m\}$. Sequentially pick up two padding digits as a group (p_j, p_{j+1}) . According to Section 2.2, each symbol only occurs once in each row and each column of Latin square, select a group (r_j, c_j) in row p_j or column p_{j+1} of Latin square matrix LS to learn a value equal to d_j by mapping the row r_j and the column c_j at Latin square matrix LS . Both r_j and c_j are in the range of $[0, 7]$. The searching strategy reduces the bit number need to flip in Step 7. The less data bits are flipped in cover QR code, the less noticeable changes QR code pseudo-share will have. This process can be described as Eq. (4):

$$d_j = M((r_j, c_j), (p_j, p_{j+1})), \quad (4)$$

where $1 \leq j \leq k$ and $M(*)$ is Latin square matrix mapping function based on (p_j, p_{j+1}) . So the secret digit d_j is well disguised as (r_j, c_j) which is the coordinate of Latin square matrix. For instance, suppose we choose Latin square matrix LS shown in **Table 2** as embedding key, the secret digit d_j is 4, and it will be embedded in padding region which contain two digits 3 and 5. We group them to be (3, 5) as (p_j, p_{j+1}) , then select (r_j, c_j) in row 3 or column 5 of LS to meet the condition $d_j = LS(r_j, c_j)$. It easy to find out that $4 = LS(3, 1)$, thus we just need to flip one bit in (3, 5) to be (3, 1) in order to embed secret message 4 based on Latin square matrix LS .

Repeat the mapping process until all the octal digital bits $\{d_1, d_2, \dots, d_k\}$ are camouflaged. Finally, we will get the disguised message $s'_i = \{(r_1, c_1), (r_2, c_2), \dots, (r_k, c_k)\}$ for secret share s_i . **Step 5** Derive the authentication message a_i by hashing the cover QR code public message, random matrix ls_i and the disguised secret share s'_i .

$$a_i = H_{ls_i}(pm_i, ls_i, s'_i), \quad (5)$$

where $1 \leq i \leq n$ and $H_{ls_i}(\cdot)$ is the one-way hash function with key ls_i .

Step 6 Packet the message $\{ls_i, s'_i, a_i\}$ to be embedded into a message stream m_i in order by

$$m_i = pm_i || ls_i || s'_i || a_i, 1 \leq i \leq n. \quad (6)$$

Step 7 Derive the bit locations $bits$ in the data codewords of cover QR code that need to be flipped to embed m_i by comparing message stream m_i with RS code rs_i of cover QR code.

$$bits = P(m_i, rs_i), \quad (7)$$

where $1 \leq i \leq n$ and $P(\cdot)$ denotes the bit comparison function.

Step 8 According to bit location $bits$ and the length of RS code rs_i , we can construct a new RS code whose data codewords all are zero except the locations in $bits$. We can utilize the XORed characteristic of RS code demonstrated in Section 2.1 to embed message $\{ls_i, s'_i, a_i\}$ in cover QR code padding region by XORing the RS code rs_i with this new RS code.

$$rs'_i = \Lambda(bits, rs_i), \quad (8)$$

where $1 \leq i \leq n$ and $\Lambda(\cdot)$ is the RS code construction and updating function. rs'_i is the result after updating operation, it is still a valid RS code.

Step 9 According to QR code specification [21], the final RS code rs'_i will be encoded into a QR code pseudo-share mQR_i .

$$mQR_i = E(rs'_i), \quad (9)$$

where $E(\cdot)$ denotes the standard QR code encoding procedure.

Step 10 Repeat **Step 3** to **Step 9**, until all n QR code pseudo-shares $\{mQR_1, mQR_2, \dots, mQR_n\}$ are generated. Then assign them to each n participants, respectively.

By exploiting the XORed characteristic of RS code, the embedding results are still a valid RS code. So the proposed secret sharing scheme does not scarify any error correction

capacity of the generated QR code pseudo-shares mQR_i , which means the generated QR code pseudo-shares mQR_i maintains strong robustness. Moreover, the involved participants do not need to hold any additional secret embedding key but just the QR code pseudo-shares.

3.2 Secret revealing procedure

Assume that QR codes $\{\overline{mQR}_1, \overline{mQR}_2, \dots, \overline{mQR}_n\}$ are the secret pseudo-shares provided from n participants.

3.2.1 Cheater identification phase

Step 1 Extract the RS code \overline{rs}_i in the QR code pseudo-share \overline{mQR}_i by using standard QR code decoding process.

Step 2 Extract the public message \overline{pm}_i , the random matrix \overline{ls}_i , the secret share \overline{s}_i and the authentication message \overline{a}_i from RS code \overline{rs}_i .

Step 3 Recalculate the authentication message \overline{a}'_i .

$$\overline{a}'_i = H_{\overline{ls}_i}(\overline{pm}_i, \overline{ls}_i, \overline{s}_i), \quad (10)$$

where $H_{\overline{ls}_i}(\ast)$ is the one way hash function with key \overline{ls}_i .

Step 4 Verify the legitimacy of the QR code pseudo-shares by comparing \overline{a}_i with \overline{a}'_i . If both have the same value, it indicates that the QR code pseudo-shares \overline{mQR}_i is legal.

Otherwise, the QR code pseudo-shares \overline{mQR}_i will be considered as fake. It indicates that the i^{th} participant is a cheater.

Step 5 Repeat **Step 1** to **Step 4** until all the n participants' legality is verified. If more than one participant is considered as a cheater, the secret reconstruction process will be terminated immediately. Only when all the n participants pass the honesty and trustworthiness verification, the secret construction process will be authorized to perform.

3.2.2 Secret reconstruction phase

Step 1 Construct the Latin square \overline{LS} with size 8×8 from the random matrices $\{\overline{ls}_1, \overline{ls}_2, \dots, \overline{ls}_n\}$.

$$\overline{LS} = \overline{ls}_1 \oplus \overline{ls}_2 \oplus \dots \oplus \overline{ls}_n. \quad (11)$$

Step 2 Sequentially group six bits of the secret disguised message bit stream \overline{bs}_i as an octal data pair $(\overline{r}, \overline{c})$. Using **Equation 6**, extract all the digits of secret share \overline{s}_i by mapping the row \overline{r} and the column \overline{c} in the Latin square \overline{LS} . Finally, we can derive the secret shares $\{\overline{s}_1, \overline{s}_2, \dots, \overline{s}_n\}$ from the n QR code pseudo-shares $\{\overline{mQR}_1, \overline{mQR}_2, \dots, \overline{mQR}_n\}$.

Step 3 Construct the secret message \overline{S} from the secret shares $\{\overline{s}_1, \overline{s}_2, \dots, \overline{s}_n\}$.

$$\overline{S} = \overline{s}_1 \oplus \overline{s}_2 \oplus \dots \oplus \overline{s}_n. \quad (12)$$

4 Simulated results and analysis

4.1 An example of the proposed scheme

To evaluate the practicality of the proposed (n,n) -threshold QR code secret sharing scheme, a piece of software was developed in Python language and used to encode and decode QR code pseudo-shares. The QR codes with version 5 and error correction level L were selected as cover QR codes. Fig. 3(a)-(c) show three normal QR codes with public message “www.fcu.edu.tw”, “www.google.com”, “www.xmut.edu.cn”, respectively. Latin square as shown in Table 2 was selected to be the secret shares embedding key. 2010110704 is the secret message to be shared, it was divided into three secret shares and embedded in the padding region of the cover QR codes with the help of Latin square. Take the cover QR code cQR_1 for example, the version 5-L cQR_1 contains 108 data codewords and 26 error correction codewords according to the QR code specification. The public message “www.fcu.edu.tw” would be encoded into a bit stream of length 124, so the secret share and the authentication message could be embedded in the padding region with size of $108 \times 8 - 124 = 740$ bits. Fig. 3(d)-(f) list the corresponding QR code pseudo-shares of Fig. 3(a)-(c) after sharing the secrets message “2010110704”. These QR code pseudo-shares would be shared and assigned to 3 involved participants. It is necessary to mention that, the involved participant does not need to hold an additional key beside a QR code pseudo-shares.

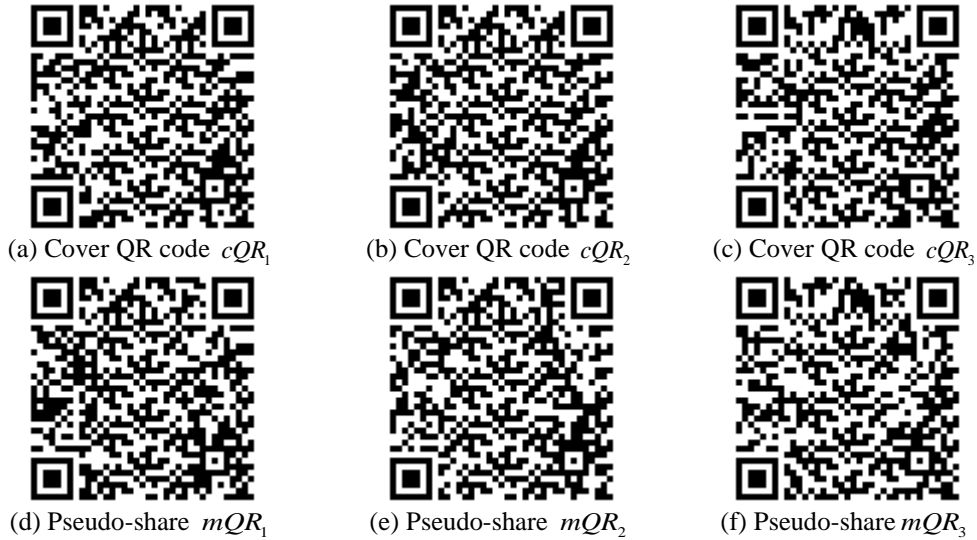


Fig. 3. (3, 3)-threshold secret sharing of the proposed scheme for QR code version 5-L

For QR code consists of the noise-like modules, the QR code pseudo-shares are difficult to draw people’s attentions and identify the abnormal areas. Furthermore, the QR code pseudo-shares are still valid and could be decoded by any QR code standard reader. For example, the public message of QR code pseudo-share mQR_1 is “www.fcu.edu.tw”, which is the same as the public message of cover QR code cQR_1 . The meaningful QR code pseudo-shares help to further reduce people’s curiosity. If the malicious participant tries to forge a QR code pseudo-share with the same public message in order to steal the secret message, the cheater identification process of the proposed scheme can detect the authenticity of QR code pseudo-share before reconstructing secret message. In this way it effectively prevents secret

from leakage. Only when all the QR code pseudo-shares pass the cheater detection process, then the secret reconstruction process will be authored to be performed.

4.2 Storage analysis

The proposed scheme divides secret message S into n secret shares, and then embeds them into the padding region of cover QR code with the assistance of Latin square matrix. In order to achieve the functionality of keyless and cheating prevention, the proposed scheme also embeds some additional information such as random matrix and authentication message in the padding region together with secret share. These three kinds of information are packaged into order as shown in Fig. 2. Hence, the secret payload of the proposed scheme is determined by a number of factors: the length of data codewords, the length of cover QR code public message, the length of random matrix and the length of authentication message.

























Note that random matrix is the size as Latin square matrix. Its size would be $(8 \times 8 \times 3 = 192)$ bits. Authentication message is the hash value of front portion of data codewords. Its length depends on hash algorithm chosen. For ease of calculation, we assume that the length of hash digest is 64 bits. In a specific version of a QR code, the length of the data codewords is deterministic. In this case, the secret payload is determined by the length of public message, and it approaches to maximum when the length of cover QR code public message approaches 0. It is easy to infer that the length of the data codewords of the cover QR code should be greater than $(192 + 64 = 256)$ bits. According to the QR code specification, version 2-L is the minimum version available for the proposed scheme. Table 3 lists the secret payloads for QR code with different QR versions and different error correction levels. It is easy to find out that, the secret payload is adjustable, within the range of (16, 23392) bits.







Table 3. The secret payload of the proposed scheme

Versions Error correction level	Secret payload of the proposed scheme								
	1	2	3	4	5	10	20	30	40
L (7%)	0	16	184	384	608	1,936	6,632	13,624	23,392
M (15%)	0	0	96	256	432	1,472	5,096	10,728	18,416
Q (25%)	0	0	16	128	240	976	3,624	7,624	13,072
H (30%)	0	0	0	32	112	720	2,824	5,704	9,952

4.3 Robustness analysis

During capturing, the quality of digital QR code image is also affected by light conditions. Lack of sufficient light creates the noises added to QR code image which seriously degrade the quality of QR code image. These noises are considered as a kind of attacks and decrease the success rate of the QR code decoding process. The first four rows of Fig. 4 showed the results of the QR code pseudo-share in Fig. 3(d) after suffering from varying degrees of noising and blurring attacks.

Gaussian noise	(M=0, V=0.10)	(M=0, V=0.20)	(M=0, V=0.30)	(M=0, V=0.40)
Attack results:				
Public message:	Readable	Readable	Readable	Readable
Secret message:	Decodable	Decodable	Decodable	Decodable
Pepper & salt	V=0.10	V=0.20	V=0.30	V=0.40
Attack results:				
Public message:	Readable	Readable	Readable	Unreadable
Secret message:	Decodable	Decodable	Decodable	Undecodable
Speckle noise	V=0.10	V=0.20	V=0.30	V=0.40
Attack results:				
Public message:	Readable	Readable	Readable	Readable
Secret message:	Decodable	Decodable	Decodable	Decodable
Gaussian blur	($\sigma=0.5$)	($\sigma=1$)	($\sigma=1.5$)	($\sigma=2$)
Attack results:				
Public message:	Readable	Readable	Readable	Unreadable
Secret message:	Decodable	Decodable	Decodable	Undecodable
Fouling	4% area	5% area	6% area	Two 3% area
Attack results:				
Public message:	Readable	Readable	Readable	Readable
Secret message:	Decodable	Decodable	Decodable	Decodable
Damage	4% area	5% area	6% area	Two 3% area
Attack results:				
Public message:	Readable	Readable	Readable	Readable

Secret message:	Decodable	Decodable	Decodable	Decodable
Fig. 4. The results the QR code pseudo-shares in Fig. 3(d) after suffering common attacks				
Rotation degree:	45°	90°	135°	
Results:				
Public message:	Readable	Readable	Readable	
Secret message:	Decodable	Decodable	Decodable	
Rotation degree:	180°	225°	270°	
Results:				
Public message:	Readable	Readable	Readable	
Secret message:	Decodable	Decodable	Decodable	
Fig. 5. The results the QR code pseudo-shares in Fig. 3(d) under the rotation attacks				

QR codes are also usually printed on paper media, such as magazine, billboard, tickets, which frequently defaced. The last two rows of **Fig. 4** showed the results, that the QR code pseudo-share in **Fig. 3(d)** suffers from varying degree of fouling and damage attacks. **Fig. 5** shows the experimental results of the proposed method under the rotation attacks. The term “Readable” means that the public message of QR code pseudo-share still can be decoded, vice versa. And the term “decodable” means that secret share in QR code pseudo-share can be successfully extracted, vice versa. From **Fig. 4** and **Fig. 5** we can see that the shares can still be extracted, although the QR code pseudo-shares suffered serious attacks. The results shown in **Fig. 4** and **Fig. 5** illustrate that the generated QR code pseudo-shares of the proposed scheme has a strong robustness.

4.4 Security analysis

Considering the cheating situation, a malicious participant tries to provide a fake QR code pseudo-shares to cheat other involved participants. Noting that the proposed scheme embeds authentication message within the QR code pseudo-shares. The authentication message is the one-way hash function value of public message, random matrix, and the disguised secret share. Any bit changed in the data codewords of QR code pseudo-share results in a new hash value recalculated in cheater identification process, and the recalculated hash value will not equal to authentication message extracted from the QR code pseudo-shares. This makes the fake QR code pseudo-shares unable to pass the cheater identification process.

Considering the security of secret share, it is disguised as Latin square matrix coordinate information and embedded in the padding region of cover QR code. In order to correctly extract secret information, we need to reconstruct Latin square matrix from random matrices

$\{ls_1, ls_2, \dots, ls_n\}$. As the total number of possible solutions of an 8×8 Latin square are $108,776,032,459,082,956,800 \approx 1.09 \times 10^{20}$, so the possibility of one guess is $1/1.09 \times 10^{20} = 9.17 \times 10^{-19}$. It is nearly impossible for malicious participants to successfully extract the secret share.

If less than n participants correctly construct the secret message, the possibility is $1/2^{len_{dc}}$, which is nearly impossible, here len_{dc} is the length of data codewords of QR code pseudo-shares. For example, the possibility of hitting the secret message in version 5-L QR code is $1/2^{864}$. Only, when all the n participants provide real QR code pseudo-shares, the secret reconstruction process will be allowed to perform, and the secret message can be successfully revealed.

The above analysis demonstrates that the proposed (n, n) -threshold secret sharing scheme achieves high security.

4.5 Comparisons

So far, the research of secret sharing based on QR code is still not much. Table 4 lists the overall comparisons between exiting schemes and the proposed scheme.

For the secret shares embedding mechanism, Chuang et al.'s scheme treats the shares as the QR code public message, Lin's scheme, Chow et al.' scheme, He et al.' scheme and Huang et al.' scheme embeds the secret in the RS code in the cover QR code by exploiting the QR code error correction capacity. The proposed scheme hides the shares in the padding region of cover QR code based on the XORed characteristic of RS code, it would not reduce the error correction capacity of cover QR code.

For the functionality of cheating prevention, except the Chuang et al' scheme, all these schemes implement the cheater prevention mechanism. However, the cheater identification function of Lin's scheme would fail when one of the participants provide a fake embedding key. The cheating detection function of Huang et al' (t, n) -threshold secret sharing scheme rely on two adjacent QR code pseudo-shares, and it is available when condition $t = n$ is satisfied. In the proposed scheme, the cheater identification process on each QR code pseudo-share does not rely on any additional data. The reliability of the cheater identification will be much higher than others schemes.

Table 4. The comparison of the proposed scheme with exiting schemes

Functionality	Chuang et al.'s scheme	Lin's scheme	Chow et al.'s scheme	He et al.' scheme	Huang et al.'s scheme	The proposed scheme
Secret embedding mechanism	Without embedding process	Error correction capacity	Error correction capacity	Error correction capacity	Error correction capacity	XORed characteristic of RS code
Utilization of ECC	No	Yes	Yes	Yes	Yes	No
Need key to extract share	No	Yes	Yes	Yes	No	No
Cheating prevention	No	Yes	Yes	Yes	Yes	Yes

Cheater identification	No	It depends	Yes	Yes	It depends	Yes
Security	Low	High	High	High	High	High
Robustness	High	Low	Low	Low	Low	High
Time complexity	$O(n \log^2 n)$	$O(n)$	$O(n \log^2 n)$	$O(n \log^2 n)$	$O(n)$	$O(n)$
Secret payload	Number of data codewords	Adjustable 3~1,215 bits	Adjustable 16~9,620 bits	Adjustable 16~9,620 bits	Adjustable 20~9,620 bits	Adjustable 16~23,392 bits

The QR code pseudo-share of Chuang et al.' scheme can be easily forged; it has poor security. Lin's scheme utilized the wet paper code to randomly embed the shares in cover QR code. Both Chow et al. scheme and He et al.'s scheme encrypted shares using symmetric encryption algorithm. Both Huang et al.'s scheme and the proposed scheme camouflage secret share as coordinate information. The possibilities of successfully extracting the secret share in the QR code pseudo-share of these five schemes are negligible, thus, their securities are high.

In terms of robustness of the generated QR code pseudo-share, Chuang et al.'s scheme generated QR code pseudo-shares by treating secret share as QR code public message. The generated QR code pseudo-shares still maintains the full error correction capacity, the robustness is strong. Lin's scheme, Chow et al.'s scheme, He et al.' scheme and Huang et al.'s scheme employ QR code error correction capacity to embed shares. The shares embedding process would reduce the error correction capacity of cover QR code, the robustness of generated QR code pseudo shares would be weakened. However, the proposed scheme exploits the XORed characteristic of the RS code to embed the secret shares into the QR code without scarifying the error correction capacity. As listed in the Fig. 4, the generated QR code pseudo-shares of the proposed scheme can resist common QR code image attacks. The robustness of the proposed scheme is much stronger compared to Lin's scheme and Huang et al.'s scheme.

In the aspect of computational complexity, suppose that these schemes generate n QR code pseudo-shares. The main operations of Chuang et al.' scheme, Chow et al.'s scheme, He et al.' scheme and Huang et al.' scheme are the secret shares derivation based on Shamir's SS, According to [1], their computational complexity is $O(n \log^2 n)$. The proposed scheme and Lin's scheme directly divided secret message into n pieces, and embedded them in the spatial domain of cover QR code, the corresponding computational complexity is $O(n)$. The low computational complexity of the proposed scheme is highlighted.

In the aspect of secret payload, the randomly embedding strategy of Lin's scheme results have too many error codewords in the QR code, the secret payload is dramatically reduced, it is in the range of [2, 1215] bits. The QR code error correction capacity determines the secret payload of Chow et al.'s scheme and He et al.'s scheme, their payloads are in the range of [16, 9620] bits. At the same time, beside the secret share, Huang et al.'s scheme also embedded many side information to implement the cheating preventions function and embedding key reconstruction. This side information occupied storage capacity, and the secret payload of Huang et al.'s scheme is in the range of [20, 9620] bits. Table 5 shows the secret payload of the proposed scheme compared to the exiting schemes with different QR code versions and different error correction levels.

Table 5. The comparison of secret payloads between exiting schemes and the proposed scheme

Versions	Error correction level	Lin's scheme	Chow et al.'s scheme	He et al.' scheme	Huang et al.'s scheme	The proposed scheme
1	L	2	16	16	0	0
	M	4	32	32	0	0
	Q	6	48	48	0	0
	H	8	64	64	0	0
2	L	4	32	32	0	16
	M	8	64	64	0	0
	Q	11	88	88	0	0
	H	14	112	112	0	0
7	L	20	160	160	0	992
	M	36	288	288	0	736
	Q	54	432	432	0	448
	H	65	520	520	60	272
20	L	112	896	896	436	6,632
	M	206	1,648	1,648	1,204	5,096
	Q	300	2,400	2,400	1,940	3,624
	H	350	2,800	2,800	2,340	2,824
40	L	375	3,000	3,000	2,540	23,392
	M	686	5,488	5,488	5,028	18,416
	Q	1,020	8,020	8,020	7,700	13,072
	H	1,215	9,620	9,620	9,620	9,952

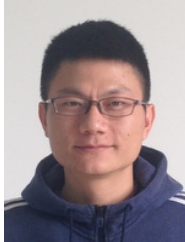
5. Conclusions

This paper utilized the XORed characteristic of RS code to propose a keyless (n, n) - threshold secret sharing scheme. The secret shares camouflage as the coordinate position information of Latin square matrix and embedding in the padding region of cover QR code. The meaningful generated QR code pseudo-shares help to reduce the people's attentions. Some experiments were done to evaluate the performance of the proposed scheme. The proposed scheme is highly secure and cheater identifiable. It has a higher secret payload and maintain a stronger robustness than exiting schemes. In the future, we will try to investigate the reversible data hiding technology to further improve the secret payload.

References

- [1] A. Shamir, "How to Share a Secret," *Communications of the ACM*, Vol. 22, No. 11, pp. 612-613, 1979. [Article \(CrossRef Link\)](#).
- [2] G. R. Blakley, "Safeguarding Cryptographic Keys," in *Proc. of the 1979 National Computer Conference*, Vol. 48, pp. 313-317, Jun. 1979. [Article \(CrossRef Link\)](#).
- [3] C. Asmuth, and J. Bloom, "A Modular Approach to Key Safeguarding," *IEEE transactions on information theory*, Vol. 29, No. 2, pp. 208-210, 1983. [Article \(CrossRef Link\)](#).
- [4] S. Zhai, F. Li, C.-C. Chang, and Q. Mao, "A Meaningful Scheme for Sharing Secret Images Using Mosaic Images," *IJ Network Security*, Vol. 17, No. 5, pp. 643-649, 2015. [Article \(CrossRef Link\)](#).
- [5] C.-C. Lee, H.-H. Chen, H.-T. Liu, G.-W. Chen, and C.-S. Tsai, "A New Visual Cryptography with Multi-Level Encoding," *Journal of Visual Languages & Computing*, Vol. 25, No. 3, pp. 243-250, 2014. [Article \(CrossRef Link\)](#).

- [6] A. A. A. El-Latif, X. Yan, L. Li, N. Wang, J.-L. Peng, and X. Niu, "A New Meaningful Secret Sharing Scheme Based on Random Grids, Error Diffusion and Chaotic Encryption," *Optics & Laser Technology*, Vol. 54, pp. 389-400, 2013. [Article \(CrossRef Link\)](#).
- [7] C.-C. Chang, Y.-H. Chen, and H.-C. Wang, "Meaningful Secret Sharing Technique with Authentication and Remedy Abilities," *Information Sciences*, Vol. 181, No. 14, pp. 3073-3084, 2011. [Article \(CrossRef Link\)](#).
- [8] P.-Y. Lin, and C.-S. Chan, "Invertible Secret Image Sharing with Steganography," *Pattern Recognition Letters*, Vol. 31, No. 13, pp. 1887-1893, 2010. [Article \(CrossRef Link\)](#).
- [9] D.-S. Tsai, G. Horng, T.-H. Chen, and Y.-T. Huang, "A Novel Secret Image Sharing Scheme for True-Color Images with Size Constraint," *Information Sciences*, Vol. 179, No. 19, pp. 3247-3254, 2009. [Article \(CrossRef Link\)](#).
- [10] C.-C. Chang, Y. Liu, and H.-L. Wu, "Distortion-Free Secret Image Sharing Method with Two Meaningful Shadows," *IET Image Processing*, Vol. 10, No. 8, pp. 590-597, 2016. [Article \(CrossRef Link\)](#).
- [11] K.-H. Lee, and P.-L. Chiu, "Digital Image Sharing by Diverse Image Media," *IEEE transactions on information forensics and security*, Vol. 9, No. 1, pp. 88-98, 2014. [Article \(CrossRef Link\)](#).
- [12] J.-C. Chuang, Y.-C. Hu, and H.-J. Ko, "A Novel Secret Sharing Technique Using QR Code," *International Journal of Image Processing (IJIP)*, Vol. 4, No. 5, pp. 468, 2010. [Article \(CrossRef Link\)](#).
- [13] 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. [Article \(CrossRef Link\)](#).
- [14] J. Fridrich, M. Goljan, and D. Soukal, "Wet Paper Codes with Improved Embedding Efficiency," *IEEE Transactions on Information Forensics and Security*, Vol. 1, No. 1, pp. 102-110, 2006. [Article \(CrossRef Link\)](#).
- [15] Y.-W. Chow, W. Susilo, J. Tonien, E. Vlahu-Gjorgievska, and G. Yang, "Cooperative Secret Sharing Using Qr Codes and Symmetric Keys," *Symmetry*, Vol. 10, No. 4, pp. 95, 2018. [Article \(CrossRef Link\)](#).
- [16] C.-W. He, P.-Y. Lin, and C.-Y. Lin, "Secret Sharing Application for Two-Dimensional Qr Barcode," in *Proc. of 2018 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)*, pp. 1-2, 2018. [Article \(CrossRef Link\)](#).
- [17] 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*, vol. 77, no. 19, pp. 25275-25294, 2018. [Article \(CrossRef Link\)](#).
- [18] R. Cox, "Qart Codes," 2012 [Online]. Available: <http://research.swtch.com/qart>, Dec. , 2017.
- [19] J.-y. Shao, "A Formula for the Number of Latin Squares," *Discrete mathematics*, Vol. 110, No. 1-3, pp. 293-296, 1992. [Article \(CrossRef Link\)](#).
- [20] N. Sloane, "A002860: Number of Latin Squares of Order N; or Labeled Quasigroups," *On-Line Encyclopedia of Integer Sequences*, 1964. [Article \(CrossRef Link\)](#).
- [21] D.-W. Inc., "QR Code Standardization," 2003 [Online]. Available: www.qrcode.com/en/about/standards.html, 24 Nov. , 2017.



Peng-Cheng Huang is a lecture at the Xiamen University of Technology. He received his BS degree from Xiamen University of Technology in 2007, the MS degree in Computer Architecture from the Fuzhou University in 2010. He is currently pursuing the Ph.D. degree from the Feng Chia University. His current research interests include multimedia security, image processing, Internet of thing.



Chin-Chen Chang is a professor in Feng Chia University. He received the BS degree in Applied Mathematics in 1977 and the M.S. degree in Computer and Decision Sciences in 1979, both from the National Tsing Hua University, Taiwan. He received the Ph.D. degree in Computer Engineering in 1982 from the National Chiao Tung University, Taiwan. He is the author of more than 900 journal papers and has written 36 book chapters. His research interests include computer cryptography, data engineering, and image compression.



Yung-Hui Li is an assistant professor in National Central University. He received his BS degree from National Taiwan University in 1995, the M.S. degree from University of Pennsylvania in 1998, and the Ph.D. degree from the Language Technology Institute, School of Computer Science, Carnegie Mellon University in 2010. He is the author of more than 30 conference and journal papers and has written five book chapters. His current research interests include image processing, machine learning, pattern recognition and biometric recognition.



Yanjun Liu received her Ph.D. degree in 2010, in School of Computer Science and Technology from University of Science and Technology of China (USTC), Hefei, China. She has been an assistant professor serving in Anhui University in China since 2010. She currently serves as a senior research fellow in Feng Chia University in Taiwan. Her specialties include E-Business security and electronic imaging techniques.