Efficient (k, n)-threshold secret sharing method with cheater prevention for QR code application

Peng-Cheng Huang[1], Ching-Chun Chang[2], Yung-Hui Li[3, 4]*
[1]Department of Computer Science and Technology, Xiamen University of Technology, China
[2] Department of Computer Science, University of Warwick, U.K.
[3]Department of Computer Science and Information Engineering, National Central University, Taiwan
[4]AI Research Center, Hon Hai Research Institute, Taiwan
pc4hpc@gmail.com, ching-chun.chang@warwickgrad.net, yunghui@csie.ncu.edu.tw

Abstract

To protect secret message, secret sharing technique divides it into n shares and distributes them to n involved participants. However, it is hardly to prevent a dishonest participant to cheat other by providing a fake share. To overcome this weakness, this paper presents an efficient (k, n)-threshold secret sharing approach with the functionality of cheater identification using meaningful QR codes. The secret message would be split into k pieces, and used as the coefficients of polynomial function to generate n shares. These shares would be concealed into cover QR codes based on its fault tolerance to generate meaningful QR code shares. The meaningful QR code shares are helpful to reduce the curiosity of unrelated persons when transmitted in public channel. The legitimacy of QR code share would be verified before secret reconstruction to prevent cheater in secret revealing procedure. Some experiments were done to evaluate the performance of the proposed scheme. The experimental results show that the proposed scheme is efficient, highly secure and highly robust, and it also achieves a higher embedding capacity compared to previous methods.

Keywords: Secret sharing, QR code, Fault tolerance, Cheater identification

1 Introduction

Secret sharing is an important research filed of cryptography. It is mainly used in secure multi-party computation, encryption and sharing of information. A secret sharing approach usually consists of the following parts: the secret distributer, secret message, the participants set, access structure, secret derivation algorithm and secret revealing algorithm. In a typical (t, n)-threshold secret sharing approach, a dealer splits secret message into n shares, and distributes them to n involved participants. The secret message could be retrieved only when any group of t or more participants cooperate.

In 1979, Shamir [1] and Blakley [2] designed two different secret sharing approaches by using Lagrange interpolation formula and linear set projection method, respectively. Since then, many researchers have constructed different (t, n)-threshold secret sharing schemes based on different mathematical techniques, such as vector space, Chinese Remainder Theorem [3], lattice [4], bivariate polynomial and so on.

With the development and maturity of mobile communication technology, two-dimensional barcode is becoming more and more popular, and is widely used in industry and business fields [5-12]. Therefore, many researchers began to combine secret sharing approach with QR code technology to generate meaningful shares to enhance the security of shares. The meaningful shares would greatly reduce the people's attention in the process of shares transmission.

Chuang et al. [13] firstly proposed a secret sharing method based on QR code. Their scheme employed Shamir's secret sharing technique to divide secret message into several shares, then treated these shares to be public message of generated QR codes. The aim of their scheme is to protect the data security in data transmission process. As an open standard, QR code message would be easily decoded by any QR code scanner. Hence, this will lead to shares leakage. At the same time, the meaningless content of QR code would attract people's attention.

To reduce the security risk of secret message, Chow et al [14] encrypted the shares using symmetric encryption algorithm before embedding them to cover QR codes. In addition, researchers start to employ data hiding technique [15-18] to embed secret shares into cover QR codes. Lin [19] proposed a (n, n)-threshold secret sharing method based on QR code to enhance the security of shares. Her scheme divided secret message into n shares with XOR operation, then hashed each share with a sharing key to generate the corresponding authentication message. Finally, concealed shares along with authentication message into cover QR codes with the help of Wet Paper Code [20]. In the secret revealing procedure, Lin's scheme verified the legality of each share before secret reconstruction. The secret retrieval phase could be performed only when all n shares are regarded as "validated". The experimental results show the feasibility of Lin's scheme. But the shares verification process of Lin's scheme would be failed when the dishonest participant provides a fake sharing key.

To overcome this weakness, Huang et al. [21] proposed another (n, n)-threshold secret sharing scheme with the functionality of cheater prevention based on Sudoku matrix. Different from Lin's scheme, Huang et al.'s scheme derived the authentication message based on two special keys from pre and post participants, respectively. Then, secret share is concealed along with authentication message into cover QR code by masquerading as coordinate values of Sudoku matrix.

*Corresponding Author: Yung-Hui Li; E-mail: yunghui@csie.ncu.edu.tw
DOI: 10.53106/160792642022012301016

The secret revealing process would firstly verify the validity of authentication message before secret reconstruction. The malicious participant could be easily identified by checking the authentication message with an encrypted key extracted from two adjacent participants. However, this cheater identification mechanism would be failed when more than one participant provides a fake QR code share. Moreover, Huang et al.'s scheme needs to embed much side information to complete the cheater prevention function, which would reduce the embedding capacity of secret message and weaken the robustness of QR code shares.

Taking the above-mentioned flaws of previous works into consideration, we propose a new (k, n)-threshold secret sharing approach with cheater identification for QR code application. The proposed scheme splits secret message into n shares, and embeds the shares along with authentication message into the data codewords of cover QR code by exploiting its fault tolerance capacity. Finally, distributes the generated QR code shares to n involved participants. In the secret construction procedure, the validity of QR code shares will be verified before secret construction to prevent secret message from being illegally acquired.

The main contributions of this paper are as follows.

(1) Higher secret payload: compared with the existed works, the proposed scheme achieves a much higher secret message embedding capacity.

(2) More flexible access structure: the proposed (k, n)-threshold secret sharing scheme is more flexible in comparison with the existed (n, n)-threshold work.

(3) Strong robustness: the generated QR code shares can resist common QR code image attacks, such as fouling, noising, blurring, cropping and so on.

The reminder of this paper is structured as follows: Section 2 briefly introduces Shamir's secret sharing and the QR code technology. Section 3 presents the novel secret sharing scheme for QR code application with (k, n) access structure. Section 4 describes the experimental results of the proposed scheme and provides the comparison with related work. Finally, Section 5 concludes this paper.

2 Preliminary

2.1 The technology of Shamir's secret sharing

Secret sharing technology is an important research content of cryptography and information security. Shamir's secret sharing is introduced by Shamir based on Lagrange interpolation in 1970. The basic concept of (k, n)-threshold Shamir's secret sharing is that the dealer divides secret message s into n shares by exploiting a secret polynomial equation. These shares would be distributed to n participants. The secret message s could be successfully reconstructed when k or more participants cooperate, while the secret reconstruct process would be failed with less than k shares.

In the secret sharing process, to share the secret message $s \in Z_p$, p is a large prime, choose $k-1$ random number $b_1, b_2, \cdots, b_{k-1}$ in $GF(p)$, and let $b_0 = s$. Then, construct the secret polynomial:

$$y = f(x) = b_0 + b_1 x + \cdots + b_{k-1} x^{k-1} \bmod(p). \quad \textbf{(1)}$$

Randomly choose n values $x_1, x_2, \cdots, x_n$ and submit them to the polynomial to yield n shares $(x_1, y_1), (x_2, y_2), \cdots, (x_n, y_n)$. Finally, distribute them to n participants.In the secret revealing process, ,the dealer collects k shares $(x_1, y_1), (x_2, y_2), \cdots, (x_k, y_k)$ from k participants. And derives the following equations:

$$\begin{aligned} b_0 + b_1 x_1 + b_2 {x_1}^2 + \ldots + b_{k-1} {x_1}^{k-1} &= y_1, \\ b_0 + b_1 x_2 + b_2 {x_2}^2 + \ldots + b_{k-1} {x_2}^{k-1} &= y_2, \\ &\vdots \\ b_0 + b_1 x_k + b_2 {x_k}^2 + \ldots + b_{k-1} {x_k}^{k-1} &= y_k. \end{aligned} \quad \textbf{(2)}$$

These operations are in $GF(p)$, the paraments $b_0, b_1, \cdots, b_{k-1}$ could be calculated by using Lagrange interpolation. Obviously, the parament b_0 is the sharing secret s .

2.2 QR code technology

Quick Response (QR) code is the most popular two-dimensional code in the world, it was designed for quickly decoding its content with machine reader by Denso Wave Inc. [22] in 1994. QR code consists of black and white squares. The black module represents information 1, and the white module represents 0. In the four corners, there are small square patterns like "回". These three patterns are used to help the decoding software to locate QR tag. Hence, the data can be read correctly no matter scanning at any angle.

QR code has the characteristics of high message payload and high tolerance. QR code employs Reed-Solomon (RS) code [23] to correct the errors caused by QR code defacement in practical applications. The QR code standard provides 40 versions and 4 error correction levels (ECL) for users to choose from. According to the fault tolerance mechanism of RS code, a codeword error could be corrected by using two error correction codewords (ECC). Thus, the fault tolerance capacity of QR code could be figured out. Table 1 shows the ECC number of QR codes with different versions and different ECL.

Table 1. The ECC number of QR code

Versions	ECL			
	L	M	Q	H
1	7	10	13	17
5	26	48	72	88
10	72	130	192	224
15	132	240	360	432
20	224	416	600	700
25	312	588	870	1050
30	450	812	1,200	1,440
35	570	1,064	1,590	1,890
40	750	1,372	2,040	2,430

3 The proposed scheme

This section presents a (k, n)-threshold secret sharing approach with functionality of cheater identification based on the technology of QR code. Figure 1 illustrates the flowchart

of the proposed secret sharing procedure. In the secret sharing procedure, the dealer is responsible for secret message derivation, authentication message generation, message embedding in cover QR code and QR code shares distribution. In the secret revealing procedure, the dealer would firstly verify the validity of those QR code shares provided by the participants. The cheater would be identified if he or she provides a fake QR code share. The secret reconstruction process would be performed only when k or more participants are verified as honest. No subset of less than k shares can divulge any piece of secret message. In addition, the meaningful generated QR code shares would greatly reduce the curious of unrelated persons.

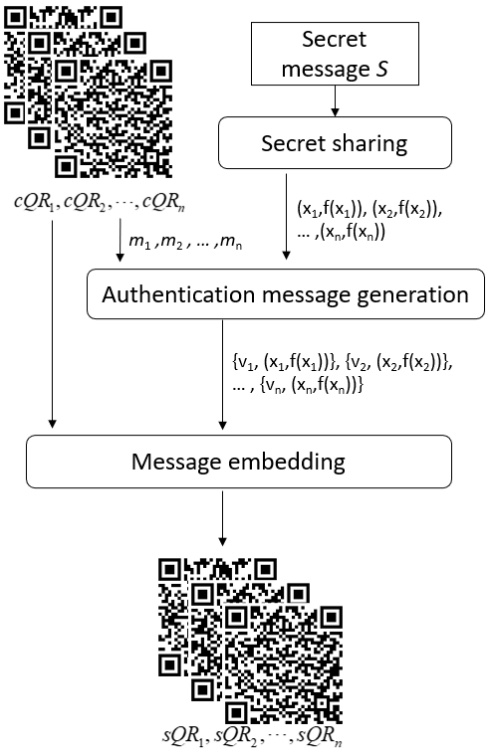


Figure 1. The flowchart of secret haring procedure of the proposed scheme

3.1 The secret sharing procedure

Assume the dealer tries to share secret message S. The dealer splits secret message into n shares based on Lagrange interpolation, and generates authentication message by employing message authentication code. Then the dealer embeds the shares along with authentication message into cover QR codes by using (3,1) Hamming code to generate QR code shares. Finally, the dealer distributes QR code shares to involved participants.

Input: Secret message S, the cover QR code $cQR_1, cQR_2, \cdots, cQR_n$

Output: The QR code shares $sQR_1, sQR_2, \cdots, sQR_n$

Step 1. Split secret message S into n non-overlapping pieces.

$$S = s_0 \| s_1 \| \cdots \| s_{n-1}. \quad \textbf{(3)}$$

Step 2. Determine a prime number p that satisfies the condition $p > s_i$, $i \in [0, n-1]$. Then, generate a polynomial function $f(x)$ with s_i as its coefficients.

$$f(x) = s_0 + s_1 x^1 + s_2 x^2 + \ldots + s_{n-1} x^{n-1} \pmod{p}. \quad \textbf{(4)}$$

Step 3. Generate n random number $x_1, x_2, \cdots, x_n$, and feed them into $f(x)$. Then, we get n shares for each participants as $(x_i, f(x_i))$, $1 \le i \le n$.

Step 4. Decode the public message m_i of cQR_i, derive the verification message v_i by using message authentication code, such as UMAC, HMAC.

$$v_i = MAC(p, m_i \oplus (x_i, f(x_i))). \quad \textbf{(5)}$$

Here, $1 \le i \le n$ and $\oplus$ denotes the XOR operation, the message authentication code takes the prime number p as its cryptographic key.

Step 5. Calculate the fault tolerance capacity ftc of cQR_i. QR code exploits RS code to correct the errors when QR codes are defaced. According to the error correction mechanism of RS code, a codeword error could be corrected by using two error correction codewords, hence, ftc could be calculated as:

$$ftc = \lfloor ecc/2 \rfloor. \quad \textbf{(6)}$$

Here, ecc denotes the ECC number of cQR_i.

Step 6. Join the share $(x_i, f(x_i))$ and the verification message v_i to be the embedding message stream c_i. Transform m_i and c_i into binary bit stream.

$$c_i = (x_i, f(x_i)) \| v_i. \quad \textbf{(7)}$$

Step 7. If $ftc \ge len(c_i)$, go to **Step 8**. Otherwise, go to **Step 12**.

Step 8. Pick up three message bits, denoted them as b_1, b_2, b_3, from m_i in turn. Pick up two message bits, denoted as d_1, d_2 from c_i in turn. Then derive the vector $[\alpha\beta]^T$ by using Formula (8).

$$[\alpha\beta]^T = H \bullet [b_1 b_2 b_3]^T \oplus [d_1 d_2]^T. \quad \textbf{(8)}$$

Here, $\oplus$ denotes the XOR operation, H is the check matrix, and $H = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$.

Step 9. According to the data embedding rules listed in Table 2, flip the message bit b_1, b_2, b_3 based on the vector $[\alpha\beta]^T$.

Table 2. The data embedding rules

$[\alpha\beta]^T$	The location of b_1, b_2, b_3 that needs to be flipped
00	unchanged
01	1

10	2
11	3

Step 10. Repeat **Step 8** to **Step 9**, until all the message bits of c_i are embedded in cQR_i. Then, the corresponding QR code share sQR_i is generated.

Step 11. Repeat **Step 4** to **Step 10**, until all the QR code share $sQR_1, sQR_2, \cdots, sQR_n$ are generated.

Step 12. The algorithm ends.

3.2 The secret revealing procedure

Assume that the dealer receives j QR code shares, $k \le j \le n$. The secret revealing procedure would verify the honesty and trustworthiness of these j participants. Only when all these j participants are verified to be "validated", the secret reconstruction process will be performed. The following is the algorithm of secret revealing procedure.

Input: The QR code share $sQR'_1, sQR'_2, \cdots, sQR'_j$

Output: The secret message S'

Step 1. For a QR code share sQR'_i, read the pubic message m_i.

Step 2. Pick up three message bits $b'_1b'_2b'_3$ of sQR'_i to extract the two bits $d'_1d'_2$ of embedding message c'_i by using Formula (9).

$$[d'_1 d'_2]^T = H \bullet [b'_1 b'_2 b'_3]^T. \quad \textbf{(9)}$$

Step 3. Repeat Step 2, until embedding message c'_i is completely restored.

Step 4. Split c'_i to extract verification message v'_i and share $(x'_i, f(x'_i))$, then calculate the new verification message $\overline{v}_i$ by using Formula (6).

Step 5. Verify both the data integrity and the authenticity of share $(x'_i, f(x'_i))$ by comparing v'_i and $\overline{v}_i$. If the two are not equal, it means the QR code share sQR'_i is a fake one, then the secret revealing procedure will be terminated.

Step 6. Repeat Step 1 to Step 5, until all the shares are extracted. Calculate the parameters $s_0, s_1, \cdots, s_{n-1}$ of polynomial $f(x)$ by using Lagrange interpolation.

Step 7. Reconstruct secret message S by joining $s_0, s_1, \cdots, s_{n-1}$.

$$S = s_0 \,||\, s_1 \,||\cdots||\, s_{n-1}. \quad \textbf{(10)}$$

Step 8. The algorithm ends.

4 Experimental results and comparison

4.1 some examples

We developed an application to evaluate the performance of the proposed (k, n)-threshold secret sharing scheme by using Python program language. Three QR codes with version 5-M were selected to sharing secret message "1234567890" for interpreting the specific case of (3, 3)-threshold secret sharing scheme. The message of these three cover QR codes are "www.bing.com", "www.google.com" and "www.yahoo.com", respectively. The first row of Figure 2 shows these three cover QR codes. The secret message is split into three pieces, $s_0 = 12345$, $s_1 = 678$ and $s_2 = 90$. Then a secret polynomial function could be constructed as $f(x) = 12345 + 678 * x + 90 * x^2 \pmod{18251}$. Therefore, we derive three shares: (1,13113), (6,01402) and (3,15189). Combining with the generated authentication message, these shares were embedded in the data codewords of three cover QR codes, respectively. The second row of Figure 2 shows the embedding results of the proposed scheme. The generated QR code shares are meaningful, the public message of these three QR code shares could be read by any standard QR code scanner. There are 50, 56 and 54 message bits of the three cover QR codes which are flipped in the embedding process, respectively. The last row of Figure 2 shows the difference between the cover QR codes and the generated QR code shares.

Figure 3 shows another example of (2, 3)-threshold secret sharing based on QR code with version 11-L. To share the secret message "1234567890", the new polynomial function is construct as $f(x) = 123456 + 7890x \pmod{131611}$, then generates three shares (1010,64085), (2304,8087) and (11280,22009). The second row of Figure 3 shows the embedding results, and the last row of Figure 3 shows the location of flipping bits of cover QR codes.

4.2 Embedding capacity

The proposed scheme exploits the built-in fault tolerance of QR code to share the secret shadow into cover QR codes. Thus, the error correction capacity of cover QR code determines the upper limit of embedding capacity. According to the message embedding strategy illustrated in Section 3.1, three message bits of cover QR code are used to embed two secret message bits. So, the embedding capacity could be calculated by

$$ec = \left\lfloor \frac{ftc \times 8}{3} \times 2 \right\rfloor = \left\lfloor \frac{ecc/2 \times 8}{3} \times 2 \right\rfloor. \quad \textbf{(11)}$$

Here, *ftc* denotes the built-in QR code fault tolerance capacity, while *ecc* denotes the total number of ECC within cover QR code. Table 3 lists the embedding capacity of the proposed scheme. According Table 3, we observed that the embedding capacity is in the range of [18,6480].

4.3 Embedding efficiency

The embedding efficiency *ee* is defined as the average number of message bits embedded by modifying one module in QR code. According to the message embedding rule showed in Table 2, three bits of data codewords of cover QR code would be flip no more than one bit to embed two secret message bits. There is no message bit needs to be modified when embedding message 0, while only one bit in other cases. Suppose that the probabilities of embedding secret digits 0, 1,

2 and 3 are equal, thus, we can derive the embedding efficiency ee of the proposed scheme using Formula (12).

$$ee = \frac{2+2+2+2}{0+1+1+1} \approx 2.7 . \quad \textbf{(12)}$$

It means that the proposed scheme modifies one module in cover QR code to embed nearly 2.7 bits secret message.

Table 3. The embedding capacity for different version of cover QR code

Versions / ECL	Embedding capacity								
	1	5	10	15	20	25	30	35	40
L (7%)	18	69	192	352	597	832	1,200	1,520	2,000
M (15%)	26	128	346	640	1,109	1,568	2,165	2,837	3,658
Q (25%)	34	192	512	960	1,600	2,320	3,200	4,240	5,440
H (30%)	45	234	597	1,152	1,866	2,800	3,840	5,040	6,480

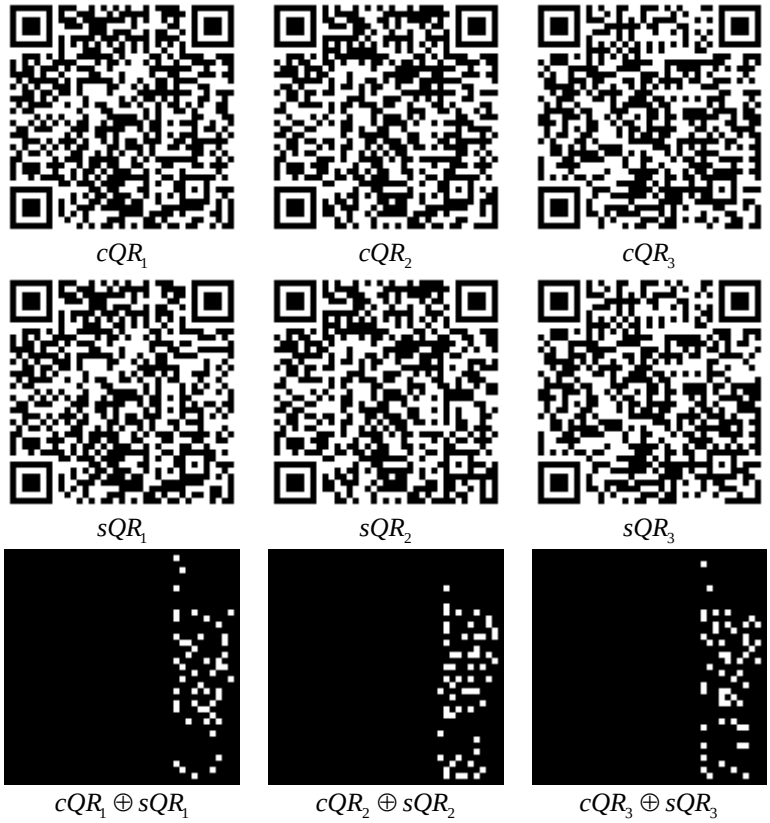


Figure 2. An example of (3, 3)-threshold secret sharing based on version 5-M QR code

4.4 Security analysis

Consider the cheating situation, a malicious participant tries to forge a QR code share to cheat other participants in the secret revealing procedure. Note that the proposed scheme embeds authentication message into the cover QR code, and the authentication message is the hash-based message authentication code generated from the public message of QR code and the share yielded from polynomial function. Thus, a change in any bit of them will produce a brand-new authentication code. Obviously, it would be inconsistent with the authentication message extracted from QR code share. Therefore, the cheater would be identified and the secret reconstruction process would be terminated. The possibility of yielding a new valid QR code share to pass cheater identification phase and successfully extract the secret message is $1/2^{8\times n_{mcw}}$, where n_{mcw} denotes the number of message codewords of cover QR code. For example, the possibility of generating a valid QR code share with version 5-M to match the secret message is $1/2^{1072}$. That is nearly impossible. The above analysis demonstrates that the proposed (k, n)-threshold secret sharing scheme achieves high security.

4.5 Robustness analysis

In practical application scenarios, QR codes are often printed and pasted in the form of paper media. Therefore, it may be subject to a defacement attack. In addition, in the process of QR code scanning by using camera, noise would be introduced to the captured QR code image with insufficient illumination. These two types of attacks that will

reduce the decoding rate of QR code. The first four rows of Figure 4 show the attack results of QR code share sQR_1 in Figure 2 after suffering from Gaussian noise attacks, pepper and salt attacks, speckle noise attacks and Gaussian blur attacks, respectively. The last two rows of Figure 4 show the attack results suffered from fouling attacks and cropping attacks. According to the attack results, we can find that, QR code message still can be read when it is suffered from a certain degrees of noise attacks and defacement attacks. The embedding message of QR code shares could be extracted successfully when suffered from noise attacks. Thus, the attack results of Figure 4 illustrate that the generated QR code shares of the proposed scheme achieve a strong robustness when suffered from common QR code image attacks.

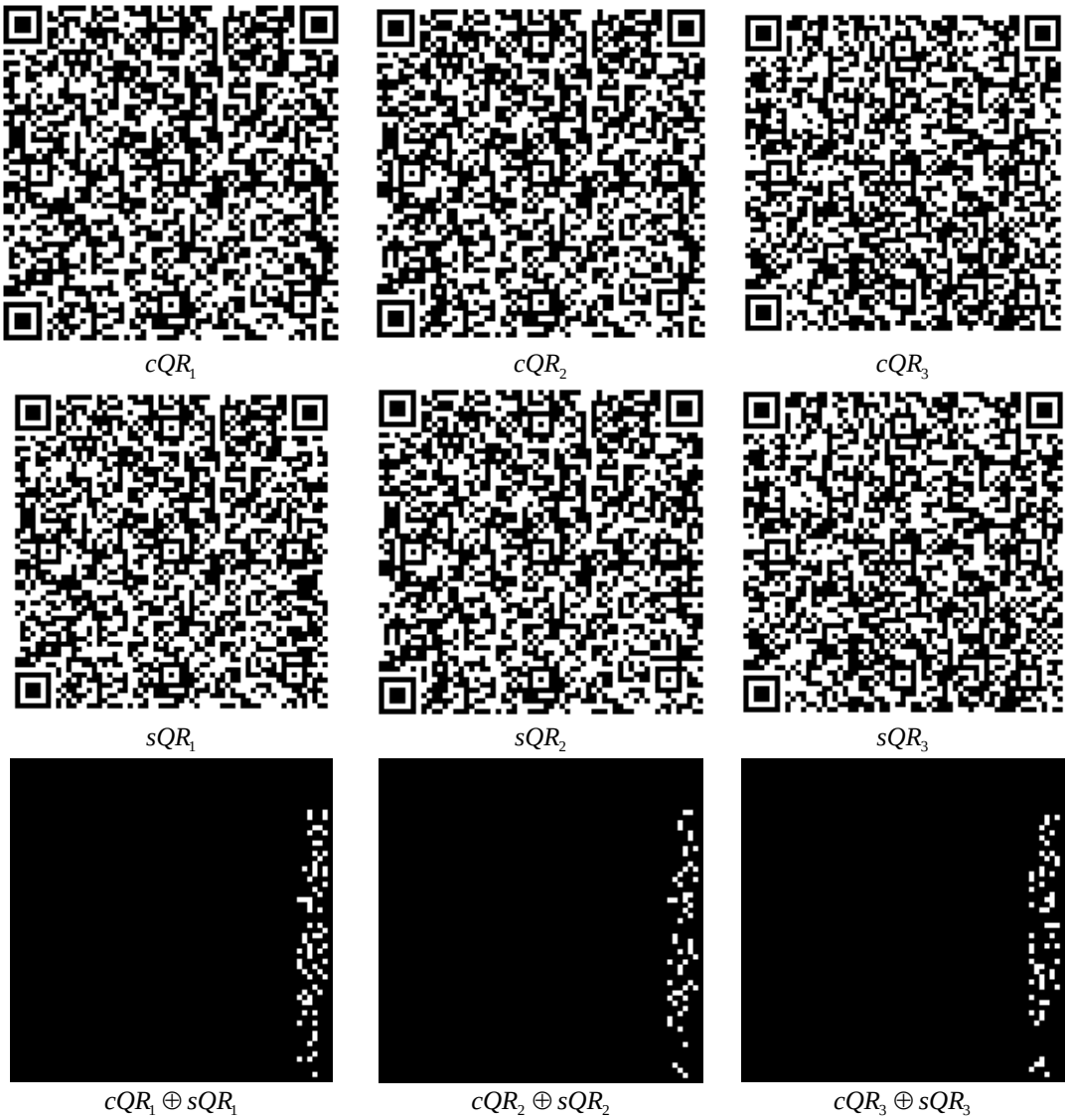


Figure 3. An example of (2, 3)-threshold secret sharing based on version 11-L QR code

4.6 Comparisons

The secret sharing schemes based on QR code always exploit a certain secret derivation mechanism to divide secret message into n shares, then conceal them into n cover QR codes by adopting some kinds of message embedding strategy. Table 4 lists the comparison of the proposed scheme with existing schemes.

These three schemes embed share into cover QR code by utilizing its error correction capacity, which allows the generated QR code shares to still be read by standard QR code scanner. The readable QR code shares are meaningful, and would greatly reduce people's attentions. As the aspect of access structure, both Lin's scheme and Huang et al.' scheme are (n, n)-threshold secret sharing scheme, which means the secret message could be constructed only when all n participants cooperate. Thus, the proposed (k, n)-threshold secret sharing scheme is more flexibly compared to these existed works.

As the aspect of cheater prevention, these three schemes embed additional verification message into cover QR code to verify the validity of participants. However, as analyzed in Section 1, there is a flaw in both Lin's scheme and Huang et al.'s scheme. The cheater identification process would be failed in some cases. The proposed scheme employs the authentication code to verify the integrity of share and legitimacy of participant. Therefore, the cheater would be successfully identified in the proposed scheme.

Gaussian noise	(M=0, V=0.10)	(M=0, V=0.20)	(M=0, V=0.30)
Results:			
Message: Secret:	Readable Decodable	Readable Decodable	Readable Decodable
Pepper & salt	V=0.10	V=0.20	V=0.30
Results:			
Message: Secret:	Readable Decodable	Readable Decodable	Readable Decodable
Speckle noise	V=0.10	V=0.20	V=0.40
Results:			
Message: Secret:	Readable Decodable	Readable Decodable	Readable Decodable
Gaussian blur	(σ=0.5)	(σ=0.75)	(σ=1)
Attack results:			
Message: Secret:	Readable Decodable	Readable Decodable	Readable Decodable
Fouling	Type 1	Type 2	Type 3
Results:			
Message:	Readable	Readable	Readable
Damage	Type 1	Type 2	Type 3
Results:			
Message:	Readable	Readable	Readable

Figure 4. The results the QR code share sQR_1 in Figure 2 after suffering common attacks

Table 4. The comparison of existing schemes

Functionality	Lin's scheme	Huang et al.'s scheme	The proposed scheme
Access structure	(n, n)	(n, n)	(k, n)
Utilize the error correction capacity	Yes	Yes	Yes
Meaningful QR code	Yes	Yes	Yes
Cheater prevention	Yes	Yes	Yes
Cheater identification	It depends	It depends	Yes
Robustness	Poor	Poor	Strong
Security	High	High	High
Embedding capacity	[3,1215]	[0,1822]	[18,6480]

As the aspect of robustness of QR code shares, Lin's scheme consumes almost all the fault tolerance capacity of QR codes, thus, the generated QR code share is difficult to resist defacement attacks. Therefore, the corresponding robustness is poor. At the same time, Huang et al.'s scheme hides much more additional message into the cover QR code to implement secret reconstruction. It consumes much more fault tolerance capacity of QR code, and faces the same situation as Lin's scheme. As analyzed in Section 4.5, the proposed scheme achieves strong robustness. The generated QR code shares could resist common QR code image attacks, such as cutting, noising, and staining.

As the aspect of embedding capacity, Lin's scheme hides secret shares into QR code by using wet paper code. The random embedding strategy of wet paper code would greatly reduce the embedding capacity. The corresponding embedding capacity is in the range of [3, 1215]. On the other hand, Huang et al.'s scheme adopts an embedding strategy based on a 16×16 Sudoku matrix. According to the embedding rules, three secret message bits are disguised as the coordinates of sudoku matrix. Therefore, the corresponding embedding capacity would be in the range of [0,1822]. Obviously, the embedding capacity of the proposed scheme is much higher than two other existing schemes.

5 Conclusions

In this paper, we present a new (k, n)-threshold secret sharing approach with the functionality of cheater identification for QR code based on its build-in fault tolerance capacity. As demonstrated in experiments, the proposed scheme is highly secure and strong robustness, it achieves a higher embedding capacity than previous schemes. it helps to protect the secret message from leaking when transmitting on public channel. For future work, considering the upper limit of message embedding capacity is determined by the QR code built-in error correction capacity, we plan to study the XORed characteristic of Reed-Solomon code to further increase the message embedding capacity.

Acknowledgment

This study was partially supported by the Ministry of Science and Technology of Taiwan under contract no. MOST 110-2221-E-008-081, Fujian Provincial Natural Science Foundation of China (2019J01856), Science and Technology Program of Xiamen(3502Z20183057), open project of Key Laboratory of Fujian Universities for Virtual Reality and 3D Visualization (VRTV2019005), Education and Scientific Research Project of Fujian Province (JT180436, JT180440 and JAT190680), and Scientific Research Project of Xiamen University of Technology (XPDKQ19009). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

[1] A. Shamir, How to share a secret, *Communications of the ACM*, Vol. 22, No. 11, pp. 612-613, November, 1979.

[2] G. R. Blakley, Safeguarding cryptographic keys, *Proceedings of the 1979 National Computer Conference*, New York, NY, USA, 1979, pp. 313-317.

[3] L. Harn, M. Fuyou, C. C. Chang, Verifiable secret sharing based on the Chinese remainder theorem, *Security and Communication Networks*, Vol. 7, No. 6, pp. 950-957, June, 2014.

[4] H. Pilaram, T. Eghlidos, An efficient lattice based multi-stage secret sharing scheme, *IEEE Transactions on Dependable and Secure Computing*, Vol. 14, No. 1, pp. 2-8, January-February, 2017.

[5] T. Chen, K. Ding, S. Hao, G. Li, J. Qu, Batch-based traceability for pork: A mobile solution with 2D barcode technology, *Food Control*, Vol. 107, pp. 1-9, January, 2020.

[6] S. Wan, G. Z. Yang, L. L. Qi, L. L. Li, X. H. Yan, Y. L. Lu, Multiple security anti-counterfeit applications to QR code payment based on visual secret sharing and QR code, *Mathematical Biosciences and Engineering*, Vol. 16, No. 6, pp. 6367-6385, July, 2019.

[7] J. Sun, K. Shrestha, H. Park, P. Yadav, S. Parajuli, S. Lee, S. Shrestha, G. R. Koirala, Y. Kim, K. A. Marotrao, B. B. Maskey, O. C. Olaoluwa, J. Park, H. Jang, N. Lim, Y. Jung, G. Cho, Bridging R2R Printed Wireless 1 Bit-Code Generator with an Electrophoretic QR Code Acting as WORM for NFC Carrier Enabled Authentication Label, *Advanced Materials Technologies*, Vol. 5, No. 2, Article No. 1900935, February, 2020.

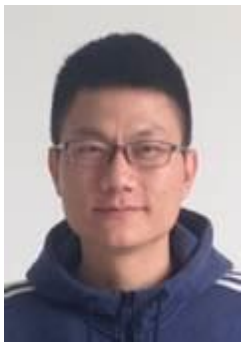
[8] R. Qv, L. Feng, A. Yang, P. Guo, B. Lin, H. Huang, A High Efficient Code for Visible Light Positioning System Based on Image Sensor, *IEEE Access*, Vol. 7, pp. 77762-77770, June, 2019.

[9] S. R. Mogali, R. Vallabhajosyula, C. H. Ng, D. Lim, E. T. Ang, P. Abrahams, Scan and learn: Quick response code enabled museum for mobile learning of anatomy and pathology, *Anatomical Sciences Education*, Vol. 12, No. 6, pp. 664-672, November-December, 2019.

[10] J. Kunhoth, A. Karkar, S. Al-Maadeed, A. Al-Attiyah, Comparative analysis of computer-vision and BLE technology based indoor navigation systems for people with visual impairments, *International Journal of*

Health Geographics, Vol. 18, Article No. 29, December, 2019.
[11] K. Jiang, D. Xu, Z. Liu, W. Zhao, H. Ji, J. Zhang, M. Li, T. Zheng, H. Feng, An invisible private 2D barcode design and implementation with tunable fluorescent nanoparticles, *RSC Advances*, Vol. 9, No. 64, pp. 37292-37299, 2019.
[12] C. Kavitha, S. Sakthivel, An effective mechanism for medical images authentication using quick response code, *Cluster Computing*, Vol. 22, No. S2, pp. 4375-4382, March, 2019.
[13] J.-C. Chuang, Y.-C. Hu, H.-J. Ko, A novel secret sharing technique using QR code, *International Journal of Image Processing (IJIP)*, Vol. 4, No. 5, p. 468-475, December, 2010.
[14] Y.-W. Chow, W. Susilo, J. Tonien, E. Vlahu-Gjorgievska, G. Yang, Cooperative Secret Sharing Using QR Codes and Symmetric Keys, *Symmetry*, Vol. 10, No. 4, Article No. 95, April, 2018.
[15] C.-C. Chang, C.-T. Li, Y.-Q. Shi, Privacy-aware reversible watermarking in cloud computing environments, *IEEE Access*, Vol. 6, pp. 70720-70733, November, 2018.
[16] C.-C. Chang, C.-T. Li, Algebraic secret sharing using privacy homomorphisms for IoT-based healthcare systems, *Mathematical Biosciences and Engineering*, Vol. 16, No. 5, pp. 3367-3381, April, 2019.
[17] C.-C. Chang, C.-T. Li, K. Chen, Privacy-Preserving reversible information hiding based on arithmetic of quadratic residues, *IEEE Access*, Vol. 7, pp. 54117-54132, April, 2019.
[18] C. -C. Chang, Y. Liu, T. S. Nguyen, A novel turtle shell based scheme for data hiding, *2014 tenth international conference on intelligent information hiding and multimedia signal processing*, Kitakyushu, Japan, 2014, pp. 89-93.
[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, February, 2016.
[20] J. Fridrich, M. Goljan, D. Soukal, Wet paper codes with improved embedding efficiency, *IEEE Transactions on Information Forensics and Security*, Vol. 1, No. 1, pp. 102-110, March, 2006.
[21] P.-C. Huang, C.-C. Chang, 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, October, 2018.
[22] Denso-Wave Inc. *QR code standardization*. Available: www.qrcode.com/en/about/standards.html (accessed data: Nov. 24 2020).
[23] R. Cox. *Qart codes*. Available: http://research.swtch.com/qart (accessed data: Dec. 2020).

Biographies



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.

Ching-Chun Chang received his PhD degree from the Department of Computer Science, University of Warwick, UK, in 2019. He was a Marie-Curie fellow and a visiting scholar at Otto von Guericke University Magdeburg (Germany), New Jersey Institute of Technology (USA), Charles Sturt University (Australia) and Deakin University (Australia). He is currently a research fellow at Department of Electronic Engineering, Tsinghua University, China. His research interests include digital watermarking, steganography, secret sharing, applied cryptography, digital forensics, multimedia security, and machine learning.

Yung-Hui Li is an associate 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 70 conference and journal papers and has written five book chapters. His current research interests include AI, deep learning, machine learning, computer vision and biometric recognition.