




# Efficient QR code authentication mechanism based on Sudoku

Peng-Cheng Huang<sup>1,2</sup> · Yung-Hui Li<sup>3</sup> · Chin-Chen Chang<sup>2</sup>  · Yanjun Liu<sup>2</sup>

Received: 13 November 2018 / Revised: 10 March 2019 / Accepted: 15 May 2019 /  
Published online: 4 June 2019

© Springer Science+Business Media, LLC, part of Springer Nature 2019

## Abstract

QR code is an important means for delivering information which has been widely used in our daily life. As an ISO international standard, the QR code encoding and decoding process are disclosed publicly, thus it is easy to decode a QR code then forge a new QR code with the same QR code public message. It can lead to the problems of information forgery and ease the spreading of fake news. To overcome this weakness, we propose a simple and efficient QR code authentication mechanism to embed the authentication information in the padding region of QR code based on the characteristics of Sudoku and Reed-Solomon code. Different from the previous scheme, the proposed scheme embeds the authentication information without consuming the QR code error correction capacity and is able to achieve a higher embedding capacity. Experimental results show that the proposed scheme has high security, low power consumption and is robust to common QR code attacks.

**Keywords** QR code · Authentication · Sudoku · Reed-Solomon code

## 1 Introduction

With the strength of high information capacity and ease of use, QR code has been widely used in a variety of scenarios, such as information delivering [17, 18], product information tracking [20], mobile payment [15], product marketing [3] and e-ticketing [4]. However, as an ISO international standard, the QR code encoding process and decoding process is opened as public property, thus it is easy to decode a QR code then forge a new QR code with the same

---

✉ Chin-Chen Chang  
alan3c@gmail.com

<sup>1</sup> Department of Computer Science and Technology, Xiamen University of Technology, Xiamen, China

<sup>2</sup> Department of Information Engineering and Computer Science, Feng Chia University, Taichung, Taiwan

<sup>3</sup> Department of Computer Science and Information Engineering, National Central University, Taoyuan, Taiwan

QR code public message. It will open the possibilities for the malicious users to deliver fake news or messages. With the popularity of QR code in our daily life, the possibility of a QR code being attacked is increasing [11, 16]. Authentication technology can be used to enhance the security of QR code by embedding authentication code in the QR code. Taking the QR code invoice as an example, Fig. 1 shows a QR code invoice from 7-Eleven mart. Shopping information such as commodity items is encoded as the public message of QR codes in the invoice. Thus, such a QR code is difficult to prevent the return fraud. Therefore, it will be beneficial to the general public if we can embed a new feature to the QR code to enable anti-forgery to prevent the invoice forgers. One of the effective solutions is to embed authentication code in the QR code of this invoice. If necessary, the authenticity of the invoice can be easily verified by checking the authentication code which is hidden in the QR code.

In recent years, many scholars have studied the QR code authentication mechanisms. Their schemes could be divided into two categories. One is to use the digital watermark technology to authenticate QR code. Sun et al. [23] proposed two kinds of algorithms to embed a random serial number or an image in the high frequency spectrum of QR code image to prevent piracy



Fig. 1 A QR code invoice from 7-Eleven mart

based on discrete wavelet transform. Li et al. [12] proposed a QR code watermarking scheme to embed an invisible watermark into the QR code image based on the discrete cosine transform. Combining with chaos encryption algorithm and singular value decomposition, Qin et al. [21] designed an anti-fake digital watermarking algorithm for QR code by doing three layers wavelet decomposition to the QR code image. When there is a concern on the authenticity of the QR code, the corresponding watermark extraction process of these schemes would be easily performed, and the authenticity of QR code would be verified by checking the extracted watermarks. Obviously, the correct extraction of watermark is the key to their schemes. To improve the reliability of these watermarking algorithms, their schemes always needed high-precision equipment to ensure that the watermark in the QR code could be extracted correctly.

The other category is to employ the data hiding technology [9, 14] to authenticate the QR code. Tkachenko et al. [24] presented a kind of two-level QR code. Compared to the standard QR code, this rich QR code has a private level storage to embed the authentication code in the black modules of the QR code by directly replacing with special textural patterns. Obviously, the design and recognition of those suitable textural patterns always are the critical issues of their scheme. The practicality of their scheme is poor.

To prove the practicality of QR code authentication scheme, Chen [2] proposed another QR code authentication scheme by embedding authentication code in the padding region of QR code. For the public message, Chen's scheme firstly employed Reed-Solomon algorithm to generate the RS code for QR code and fitted them into a QR code. Secondly, he determined the embedding locations in the QR code and generated the authentication code from the public message by exploiting cryptographic algorithm, such as the Universal Message Authentication Code (UMAC) [1] or the Elliptic Curve Digital Signature Algorithm (ECDSA) [13]. In order to improve the success rate of authentication code extraction, he yielded the redundant information for authentication code. Finally, he embedded the authentication code in the front portion of error correction codewords of QR code by directly replacing with authentication code. After masking operation, the stego QR code would be generated. Thanks to the QR code redundancy, the public message of stego QR code could be successfully decoded by any standard QR code reader. If necessary, the authentication code could be extracted with the correct encrypted key. Moreover, the verification process could be performed off-line by authorized users when needed. Experimental results showed that Chen's scheme has a good embedding capacity and achieves a high security level.

However, Chen's scheme has some flaws. The first one is the robustness of the generated stego QR code is poor. His scheme directly replaced portions of the error correction codewords of QR code with authentication code to embed authentication code. The replacement operation would cause a lot of mistakes in the Reed-Solomon code of QR code. In order to decode the QR code, redundant error correction codewords were needed to correct these mistakes. It leads to a decrease in error correction capacity of stego QR code. Thus the stego QR code decoding process might fail when stego QR code was suffered additional attacks, such as defacement or damage. The second weakness is the redundant information for the authentication code not only reduces the embedding capacity of stego QR code, but also reduces the error correction capacity of stego QR code. The last weakness is the cryptograph algorithm for generating and verifying the authentication code still requires heavy computational power. For a battery-powered scanner, such complex algorithm is not preferred.

In this paper, we propose a new QR code authentication scheme to improve these weaknesses. To summarize, this paper has primarily made the following contributions:

- 1) **Higher embedding capacity.** The proposed scheme embeds the authentication code in the padding region of QR code, so the upper bound of the embedded capacity depends on the length of the QR code padding region. Experimental results show that the proposed scheme has higher embedding capacity compared to the state-of-the-art scheme.
- 2) **Stronger robustness.** We exploit the homomorphism characteristics of Reed-Solomon code to update the error correction codes in the authentication code embedding process. Thus, the embedding process does not reduce the error correction capacity. The generated stego QR code maintains a strong robustness against different types of attacks.
- 3) **Lower power consumption.** The proposed scheme encodes the authentication code into Sudoku matrix digits. Compared to authentication code encrypted by the symmetric encryption algorithm or asymmetric encryption algorithm in Chen's scheme, the authentication code embedding process and extraction process of the proposed scheme is dramatically simple and has the benefit of lower power consumption. Moreover, the diversity of Sudoku magic matrix guarantees that the proposed scheme achieves a high security level.

The rest of this paper is presented as follows. We briefly introduced the technology of QR code and Sudoku, especially the QR code generating process in Section 2. In Section 3, we presented the construction of Sudoku expansion matrix and the homomorphism of Reed-Solomon code, then presented the authentication QR code enrollment process and the verification process of the proposed scheme. In Section 4, we provided the simulated results of the proposed scheme, and conducted comparisons with previous schemes. Finally, we made a conclusion in Section 5.

## 2 Background

In this section, we briefly introduce the technology of QR code and Sudoku.

### 2.1 The technology of QR code

Quick Response (QR) code is a kind of two dimension code, which is invented by a Japanese company Denso-Wave [7] in 1994. QR code has a much higher message capacity than the traditional barcode, and it has been a public patent since the corresponding ISO international standard ISO/IEC18004 was approved in 2000 [8]. With the development of Internet of Things (IoT) and the popularity of smartphones in recent years, QR code becomes the most popular two dimensional code in the world, especially in the Southeast Asia.

QR code consists of numerous black and white squares, these squares are called modules. There are forty QR code versions and four user-selectable error correction levels for each version to encapsulate a QR code message. In addition to the data codewords, each QR code also contains error correction codewords and functional patterns such as position detection patterns, timing patterns, version patterns, format information and alignment patterns. Figure 2 shows the structure of QR code in version 2 with error correction level M. The QR code generation process is described as follows.

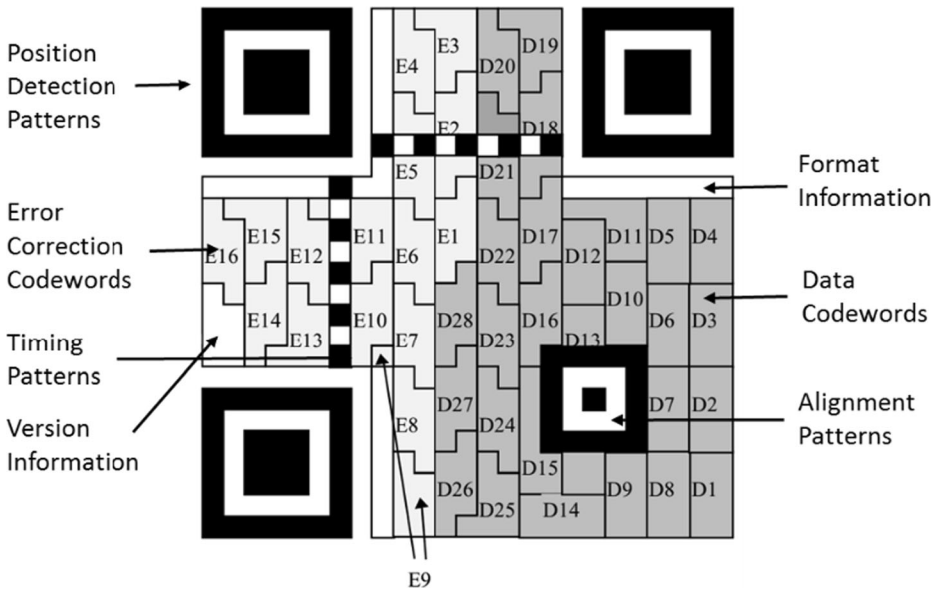


Fig. 2 The structure of QR code in version 2-M

**Step 1)** According to the QR code version and its error correction level, the QR code data codewords  $m$  is divided into  $n$  blocks.

$$m = \{m_1, m_2, \dots, m_n\}. \tag{1}$$

**Step 2)** QR code exploits the Reed-Solomon (RS) code [22] to detect and correct the errors that occurred during QR code decoding when portion of QR code was damaged. Error correction codewords will be generated for each data block  $m_i, 1 \leq i \leq n$ , and appended to the corresponding data codewords.

$$e_i = \mathbb{E}(m_i), 1 \leq i \leq n, \tag{2}$$

where  $\mathbb{E}(\cdot)$  is RS code calculation function. Then  $n$  blocks RS codes are derived.

$$RS = \{rs_1, rs_2, \dots, rs_n\} = \{(m_1, e_1), (m_2, e_2), \dots, (m_n, e_n)\}, 1 \leq i \leq n. \tag{3}$$

**Step 3)** These RS codes will be fitted into a final data sequence  $D$  by taking data codewords and error correction codewords for each RS code block in turn.

$$D = \mathbb{F}(RS), \tag{4}$$

where  $\mathbb{F}(\cdot)$  is QR code data fitting function.

**Step 4)** This data sequence  $D$  will be placed from the lower right corner of the QR code symbol in zigzag order, then masked with one of eight predefined patterns through XOR operation to generate a final QR code tag  $QR$ .

$$QR = \mathbb{M}(D), \quad (5)$$

where  $\mathbb{M}(\cdot)$  is the QR code masking function.

## 2.2 Sudoku magic matrix

Sudoku is a popular logic-based number padding game. The classic Sudoku plate is a  $9 \times 9$  block. It contains nine  $3 \times 3$  sub-blocks. Players need to deduce the numbers on all the remaining empty squares according to the visible numbers on the  $9 \times 9$  Sudoku plate, so that each row, each column and each sub-block ( $3 \times 3$ ) contains all the digits from 1 to 9. Figure 3 shows one of the Sudoku puzzle and its solution.

Sudoku originated in Latin Square, and was developed in the United States in the 1970s. It was renamed as Number Placement and spread to Japan. The Japanese game company Nikoli developed it as a math puzzle game called it Sudoku in 1986. Since 2005, Sudoku puzzle game has become popular in the whole world.

In September 2003, Felgenhauer and Jarvis [6] calculated that there are 6,670,903,752,021,072,936,960  $\approx 6.7 \times 10^{20}$  possible Sudoku solutions. Therefore, the probability of cracking a Sudoku-based encryption scheme by brute-force manner is extremely low. This fact benefits our proposed QR code encryption algorithm and makes it very robust with high security intrinsically.

		6	3	2					5	8	6	3	2	7	4	9	1	
		1				5	3	6	7	2	1	9	4	5	3	6	8	
9	4		6						9	4	3	6	8	1	7	2	5	
		4							1	5	4	7	9	6	8	3	2	
8	7		1	3	4			5	6	8	7	2	1	3	4	9	5	6
							1		3	6	9	2	5	8	1	7	4	
					9			4	7	2	3	5	8	1	9	6	4	7
	1	7	5					2		4	1	7	5	6	3	2	8	9
				7	2	5				6	9	8	4	7	2	5	1	3

(a)
(b)

**Fig. 3** An example of Sudoku. **a** A typical Sudoku puzzle. **b** The solution of (a)

### 3 The proposed scheme

In this section, we describe the proposed algorithm for QR code authentication based on the Sudoku magic matrix and the homomorphism of RS code. we firstly will introduce the construction of the Sudoku expansion matrix, then discuss the homomorphism of Reed-Solomon code, and finally, present the authentication QR code enrollment process and the verification process of the proposed scheme.

#### 3.1 Sudoku expansion matrix

It is not good to directly fill the authentication code with the form of plaintext into the QR code padding region since it is vulnerable to the attacks from the malicious users. With the nature of the extremely high variety of Sudoku, we can design an encryption algorithm which is simple to encode but extremely hard to be cracked. The proposed scheme exploits Sudoku matrix to hide the authentication code into QR code padding region in the form of Sudoku digit. In order to hide the authentication code with higher level of security within the QR code, we propose a modified version of Sudoku matrix, which is described as follows.

Firstly, we choose a Sudoku puzzle, and determine a Sudoku matrix using the digits from 1 to 9. Then subtract 1 from all the digits in the Sudoku block. Figure 4a demonstrates an example of such modified version of Sudoku matrix in Fig. 3b. Finally, a Sudoku Expansion Matrix (SEM) with the size of  $16 \times 16$  is derived by repeating the

4	7	5	2	1	6	3	8	0
6	1	0	8	3	4	2	5	7
8	3	2	5	7	0	6	1	4
0	4	3	6	8	5	7	2	1
7	6	1	0	2	3	8	4	5
2	5	8	1	4	7	0	6	3
1	2	4	7	0	8	5	3	6
3	0	6	4	5	2	1	7	8
5	8	7	3	6	1	4	0	2

(a)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	4	7	5	2	1	6	3	8	0	4	7	5	2	1	6	3
1	6	1	0	8	3	4	2	5	7	6	1	0	8	3	4	2
2	8	3	2	5	7	0	6	1	4	8	3	2	5	7	0	6
3	0	4	3	6	8	5	7	2	1	0	4	3	6	8	5	7
4	7	6	1	0	2	3	8	4	5	7	6	1	0	2	3	8
5	2	5	8	1	4	7	0	6	3	2	5	8	1	4	7	0
6	1	2	4	7	0	8	5	3	6	1	2	4	7	0	8	5
7	3	0	6	4	5	2	1	7	8	3	0	6	4	5	2	1
8	5	8	7	3	6	1	4	0	2	5	8	7	3	6	1	4
9	4	7	5	2	1	6	3	8	0	4	7	5	2	1	6	3
A	6	1	0	8	3	4	2	5	7	6	1	0	8	3	4	2
B	8	3	2	5	7	0	6	1	4	8	3	2	5	7	0	6
C	0	4	3	6	8	5	7	2	1	0	4	3	6	8	5	7
D	7	6	1	0	2	3	8	4	5	7	6	1	0	2	3	8
E	2	5	8	1	4	7	0	6	3	2	5	8	1	4	7	0
F	1	2	4	7	0	8	5	3	6	1	2	4	7	0	8	5

(b)

Fig. 4 Two examples of the modified Sudoku matrices. a An example of the modified Sudoku matrix. b An example of  $16 \times 16$  matrix SEM derived from (a)

pattern of the  $9 \times 9$  matrix until the size  $16 \times 16$  is fulfilled. Figure 4b shows the corresponding SEM derived from Fig. 4a.

In the proposed scheme, the SEM will be shared among users as a kind of encryption key. In order to minimize the storage space of SEM, neither the  $9 \times 9$  matrix nor the  $16 \times 16$  matrix is shared to the users. Instead, the original Sudoku puzzle (an example is shown in Fig. 3a) is shared in a compressed fashion using Huffman encoding [10] or Run-length encoding [19].

### 3.2 The homomorphism of RS code

According to the QR code specification, it employs RS code to detect and correct noise induced errors without loss of data. For RS codes consist of  $a$  bits data message and  $b$  bits error correction code, it can correct up to  $\lfloor \frac{b/8}{2} \rfloor$  codewords data errors. Figure 5 shows the composition of RS code in the QR code. The  $a$  bits data codewords of RS code in QR code always contain two parts:  $c$  bits public message and  $(a - c)$  bits padding message. Note that these  $(a - c)$  bits padding message are meaningless and useless, so it is possible to modify these padding bits to embed the authentication code in the padding region of QR code.

In 2012, Russ Cox [5] found out that two different RS codes with the same parameters  $a$  and  $b$  could be XORed to generate another valid RS code. Such nature can be called the homomorphism of RS code. In this way, we can easily derive a new RS code from the other two valid RS codes.

Based on the homomorphism of RS code, we can modify any bit of padding bits of RS code in QR code and keep the other bits unchanged. Table 1 shows an example. The first row of Table 1 shows a RS code RS0 that satisfies the conditions  $a = 16$ ,  $b = 16$  and  $c = 8$ . Suppose we want to invert the 10th bit and 12th bit of the RS0. We can construct a 16-bit data codewords 0000000001010000 whose data bits are all zeros except the 10th bit and 12th bit, use Reed-Solomon algorithm to generate the 16-bit error correction codewords 1,111,000,010,100,000 and add them to the tail of data codewords to form a temp RS code RS1. Finally, we can derive a result RS2 by XORing RS0 with RS1. The XOR operation inverts the 10th bit and 12th bit of RS0. Most importantly, the result RS2 still is a valid RS code.

This XORing operation does not consume the QR code error correction capacity. It updates the error correction codewords of QR code to maintain its validity. Meanwhile, the public message of QR code still can be decoded by any standard QR code reader. Therefore, the stego QR code appears as if it is a normal QR code for general users. Such characteristics will reduce people’s curiosity.

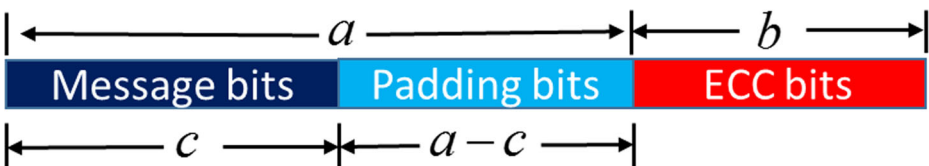


Fig. 5 The composition of RS code in the QR code



**Table 1** An example of homomorphism of RS code

RS0	11000001000101000100000110010100
RS1	00000000010100001111000010100000
RS2	11000001010001001011000100110100

### 3.3 The authentication code embedding procedure

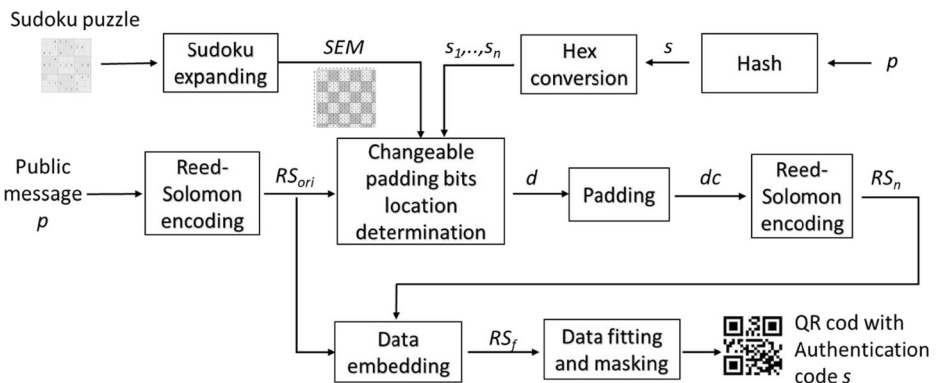
The procedure of authentication code embedding is shown in Algorithm 1. Suppose we want to generate a QR code  $QR_{aut}$  with authentication code  $s$ . The  $QR_{aut}$  public message is  $p$  with a length of  $c$ , and the authentication code  $s$  is the hash value of  $p$ . The QR code enrollment process of the proposed scheme is demonstrated in Fig. 6. The authentication code  $s$  will be hidden in the padding region of QR code in the form of the coordinates in Sudoku expansion matrix  $SEM$ . After confirming the bit location that need to be flipped in the padding region, the procedure will generate a new RS code and XOR it with the original RS code to embed the authentication code  $s$ . The XOR operation will update the QR code error correction code according to the RS code homomorphism. Finally, A stego QR code with authentication code  $s$  is derived.

**Step 1)** Randomly choose a Sudoku puzzle as an embedding key  $k$ , then construct the Sudoku expansion matrix  $SEM$  with size of  $16 \times 16$ .

$$SEM = \mathbb{S}(k, 16), \tag{6}$$

where  $\mathbb{S}(\cdot)$  is the Sudoku expansion matrix construction function.

**Step 2)** Choose a suitable QR code version  $v$  and error correction level  $l$  according to the length of public message  $p$  and authentication code  $s$ , then employ Reed-Solomon algorithm to yield the corresponding Reed-Solomon code  $RS_{ori}$ . Finally, we can obtain the length of data codewords  $a$  and the length of error correction codewords  $b$  of RS code  $RS_{ori}$ .



**Fig. 6** The QR code enrollment process of the proposed scheme

$$\mathbb{RS}(p, v, l) = \{a, b, RS_{ori}\}, \tag{7}$$

where  $\mathbb{RS}(\cdot)$  is the RS code generation function.

**Step 3)** Generate the hash value of public message  $p$  as the authentication code  $s$  by using general hash function such as MD5, SHA-1, SHA-3, SHA-256, and so on, then convert the authentication code  $s$  into novenary digits stream  $\{s_1, s_2, \dots, s_n\}$ , which is a 9-ary numerical system to match the digits in  $SEM$ .

$$\begin{aligned} &\mathbb{C}(\mathbb{H}(p)) \\ &= \mathbb{C}(s) \\ &= \{s_1, s_2, \dots, s_n\}, \end{aligned} \tag{8}$$

where  $\mathbb{C}(\cdot)$  is novenary digit conversion function while  $\mathbb{H}(\cdot)$  is the general hash function.

**Step 4)** Sequentially group eight binary digits from padding region as a hexadecimal data pair  $(x, y)$ , sequentially pick up an authentication code  $s_i$ . Then find  $(x', y')$  which is the closest from  $(x, y)$  to learn the secret digit by mapping the row  $x'$  and the column  $y'$  in the Sudoku expansion matrix  $SEM$ . Finally, replace the data pair  $(x, y)$  with new data pair  $(x', y')$  to hide the authentication code digits  $s_i$ .

$$\mathbb{L}(x, y, s_i) = \{x', y'\}, \tag{9}$$

where  $x, y, x', y' \in [0, F]$ , and  $\mathbb{L}(\cdot)$  is the looking up Sudoku expansion matrix function for the pair  $(x', y')$  near  $(x, y)$  to the matrix  $SEM$  to satisfy the condition  $s_i = SEM(x', y')$ . For instance, suppose that one of the authentication code digit is 1, and 01101010 is the eight bits of padding region message to be embedded. Thus, the corresponding hexadecimal data pair is (6, A). According to the matrix  $SEM$  in Fig. 4b, the value stored at the  $SEM(6, A)$  is 2. Using this cell as the center to search for the closest cell that has a value of 1, we can find three cells:  $1 = SEM(4, 9) = SEM(5, 8) = SEM(7, B)$ . Among them, it is obvious to see that (7, B) is the nearest cell from (6, A). And we shall use the value pair (7, B) to be the new data pair  $(x', y')$ .

**Step 5)** Employ the XOR function to yield an eight-bits binary string  $d_i$  by XORing  $(x, y)$  with  $(x', y')$ . This binary bit string  $d_i$  indicates the changed bits of QR code padding message bits while hiding a novenary authentication code digit  $s_i$  in Step 4.

$$d_i = \mathbb{X}\left((x, y), (x', y')\right), 1 \leq i \leq n, \tag{10}$$

where  $\mathbb{X}(\cdot)$  is XOR operation function. Take the example mentioned earlier,  $d_i = \mathbb{X}((6, A), (7, B)) = \mathbb{X}((0110, 1010), (0111, 1011)) = 00010001$ .

**Step 6)** Repeat Step 4 and Step 5 until all the stream of authentication code digits  $\{s_1, s_2, \dots, s_n\}$  find the corresponding new data pair  $(x', y')$ . Then derive a sequence of  $d_i$  to form a binary data stream  $d$  of length  $8n$ . The bit stream  $d$  marks the changes of padding region of original QR code while embedding all the authentication code  $s$ .

$$d = \{d_1, d_2, \dots, d_n\}. \tag{11}$$

**Step 7)** Note that the  $a$  bits data codewords of RS code in QR code always contain  $c$  bits public message and  $(a - c)$  bits padding message. Therefore we add  $c$  bits ‘0’ in the front of bit stream  $d$  and  $(a - c - 8n)$  bits ‘0’ in the tail of bit stream  $d$  to yield a  $a$  bits data codewords  $dc$ .

$$dc = \mathbb{P}(d), \tag{12}$$

where  $\mathbb{P}(\cdot)$  is the padding function. Figure 7 shows the composition of  $dc$ .

**Step 8)** Use Reed-Solomon algorithm to generate the corresponding error correction codewords  $ec$ . Then add it to the tail of  $dc$  to construct a new RS code  $RS_n$ .

$$RS_n = \{dc, ec\} = \{dc, E(dc)\}. \tag{13}$$

**Step 9)** XOR the RS code  $RS_{ori}$  with the new RS code  $RS_n$  to yield a final RS code  $RS_f$ . According to the homomorphism of RS code described in Section 3.2, the XOR operation will modify the padding region of QR code to hide the authentication code  $s$  and keep the public message of original QR code unchanged. Most importantly, the error correction codewords will be updated, thus the embedding process does not reduce the error correction capacity of QR code.

$$RS_f = \mathbb{X}(RS, RS_n). \tag{14}$$

**Step 10)** The codewords in the final RS code will be placed in a matrix, and a masking process will be executed to distribute black and white modules evenly. Finally, a QR code  $QR_{au}$  with authentication code  $s$  will be generated.

$$QR_{au} = \mathbb{M}(\mathbb{F}(RS_f)). \tag{15}$$

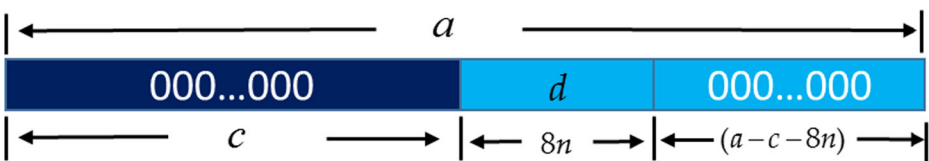


Fig. 7 The composition of  $dc$  which is padded from  $d$

**Algorithm 1** Authentication code embedding

**Input:** The QR code public message  $p$ , its length  $c$ . Sudoku puzzle.

**Output:** The stego QR code  $QR_{au}$  with authentication code.

0	<b>begin</b>
1	Construct Sudoku expansion matrix $SEM$ .
2	Generate the RS code $RS_{ori}$ according to the public message $p$ .
3	$s \leftarrow \mathbb{H}(p)$ .
4	Convert $s$ into a 9-ary digits stream $\{s_1, s_2, \dots, s_n\}$ .
5	<b>for each</b> $s_i \in \{s_1, s_2, \dots, s_n\}$ <b>do</b>
6	Group eight bits in padding region as coordinate $(x, y)$ .
7	Find the $(x', y')$ in $SEM$ satisfying the condition $s_i = SEM(x', y')$ .
8	Calculate $d_i \leftarrow (x, y) XOR (x', y')$
9	<b>end for</b>
10	$d \leftarrow \{d_1, d_2, \dots, d_n\}$ .
11	Pad $c$ bits '0' in the front of $d$ .
12	Construct a new RS code $RS_n$ .
13	Yield a final RS code $RS_f \leftarrow RS_n XOR RS_{ori}$
14	Generate the stego QR code $QR_{au}$ with authentication code $s$ based on $RS_f$
15	<b>end begin</b>

### 3.4 The tamper detection procedure

The procedure of tamper detection is shown in Algorithm 2. Suppose there is an authentication QR code  $QR'_{au}$  that will be validated, and the inspector keeps an authentication code embedding key  $k$ , which is the Sudoku puzzle. Figure 8 illustrated the verification process of the proposed scheme. The authentication code  $s'$  will be extracted from the padding region by looking up the  $SEM$  matrix.  $QR'_{au}$  is authentic only when  $s'$  equals to the hash value of public message of stego QR code  $QR'_{au}$ .

**Step 1)** Use the embedding key  $k$  to construct the Sudoku expansion matrix  $SEM$  as described in Step 1 of Section 3.3.

**Step 2)** Unmask the authentication QR code  $QR'_{au}$ , then extract the public message  $p'$  and the RS code  $RS'$  of  $QR'_{au}$ .

$$\mathbb{R}(\overline{\mathbb{M}}(QR'_{au})) = \{p', RS'\}, \quad (16)$$

where  $\overline{\mathbb{M}}(\cdot)$  is the QR code unmasking function, and  $\mathbb{R}(\cdot)$  is the QR code decoding function.

**Step 3)** Sequentially group eight bits from padding region of  $RS'$  as a hexadecimal data pair  $(x, y)$ , and extract all the authentication code digit  $s'_i$  by mapping the row  $x$  and the column  $y$  in the Sudoku expansion matrix  $SEM$ . Finally, derive a complete authentication code  $s'$ .

$$s' = \mathbb{T}(RS', SEM), \tag{17}$$

where  $\mathbb{T}(\cdot)$  is the authentication code extraction function.

**Step 4)** verify the QR code  $QR'_{au}$  to derive the result  $r$  by comparing  $s'$  with the hash value of QR code public message  $p'$ .  $r = 1$  if they are the same. It means QR code  $QR'_{au}$  is authentic; otherwise, the QR code  $QR'_{au}$  is considered as tempered.

$$r = \mathbb{V}(s', \mathbb{H}(p')), \tag{18}$$

where  $\mathbb{V}(\cdot)$  is the QR code verification function.

**Algorithm 2** Tamper detection

**Input:** The stego QR code  $QR'_{au}$ . Sudoku puzzle.

**Output:** Result  $r$ .

```

0  begin
1  Construct Sudoku expansion matrix  $SEM$ .
2  Extract the public message  $p'$  and RS code  $RS'$  of  $QR'_{au}$ .
3   $s' \leftarrow \mathbb{H}(p)$ .
4  While true do
5      Group eight bits in padding region as coordinate  $(x, y)$ .
6      Extract the authentication code  $s_i \leftarrow SEM(x, y)$ .
7      if it is end of the padding region, then
8          break
9      end if
10 end while
11 Convert the 9ary digits stream  $\{s_1, s_2, \dots, s_n\}$  into binary  $s$ .
12 if  $s = s'$  then
13      $r \leftarrow 1$ 
14 else  $r \leftarrow 0$ 
15 end if
16 end begin
    
```

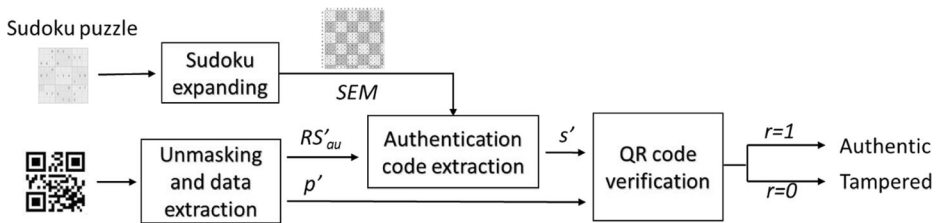


Fig. 8 The QR code verification process of the proposed scheme

## 4 Simulation results and discussion

In this section, we present the performance of the proposed QR code authentication scheme, then discuss the advantages compared to the previous methods.

### 4.1 Experimental results

To evaluate the practicality of the proposed QR code authentication scheme, a piece of software is developed by using python programming language. In our implementation, the Sudoku puzzle of Fig. 3a is selected to be the authentication code embedding key  $k$ , and SHA-1 is selected to be the hash function to yield the authentication code by hashing the QR code public messages. Here we show a QR code authentication example. Figure 9a shows an original QR code of version 5 with default error correction level ‘L’. The public message of the QR code  $p$  is “[www.fcu.edu.tw](http://www.fcu.edu.tw)”. The corresponding authentication code  $s$  is “061e4cdb0cd3fa97aded9aff72e9409850aa0048” which is generated from the SHA-1 hash function. According to the QR code standard, the QR code of version 5-L contains 108 data codewords and 26 error correction codewords, so we could infer that  $a = 108 \times 8 = 864$  and  $b = 26 \times 8 = 208$ . After adding the supplementary information, the public message  $p$  would be encoded to be  $c = 124$  bits binary message stream. With the help of Sudoku expansion matrix  $SEM$  and homomorphism of Reed-Solomon code, the authentication code  $s$  would be converted in novenary digits stream, then embedded into the 124th bit of QR code data message codewords, which is located in the padding region of QR code. Figure 9b shows the authentication result of Fig. 9a. The embedding process would update the error correction code of QR code. Therefore, it did not consume any error correction capacity of QR

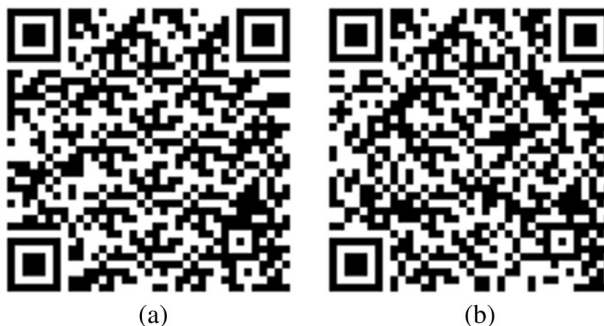


Fig. 9 An example the proposed scheme; a a version 5-L original QR code with public message “[www.fcu.edu.tw](http://www.fcu.edu.tw)”; b the corresponding stego QR code of (a)

code, and the generated QR code remains to have high robustness. Moreover, the public message of QR code is not altered by the embedding process. It still could be fully decoded by any standard QR code reader. However, the authentication code only can be extracted by the authorized person with a correct embedding key  $k$ .

#### 4.2 The embedding capacity of the proposed scheme

According to the authentication code embedding process in the Section 3.3, the authentication code  $s$  would be converted into 9-ary digital stream, then embedded in the padding region of QR code with the help of Sudoku expansion matrix. Thus, the embedding capacity of the proposed scheme depends on the length  $(a - c)$  of the padding region of QR code. Moreover, the length of the padding region depends not only on the version  $v$  and error correction level  $l$  of QR code, but also on the length of public message  $c$  of the QR code. For a certain  $v$  and  $l$  of QR code, the embedding capacity would reach the maximal value only if the length of public message  $c = 0$ . Note that eight bits padding message would be embedded a 9-ary authentication code  $s_i$ . It means that a codeword QR code data message could hide a number of  $\log_2 9$  bits authentication code on average. So the embedding capacity  $ec = \lfloor \log_2 9 \times a \rfloor$ , here  $a$  is the length of data codewords of the cover QR code. Take version 1-L QR code for example, it has 19 data codewords, so the corresponding embedding capacity  $ec = \lfloor \log_2 9 \times 19 \rfloor = 60$ . Table 2 shows the maximal embedding capacity of QR code of the proposed scheme for different versions and error correction levels of QR code under the conditions of the length of QR code public message  $c = 0$ . From the following table we can learn the embedding capacity of the proposed scheme is adjustable within the range of [28, 9370].

#### 4.3 The robustness of the proposed scheme

In the QR code application scenario, very often the QR codes are scanned by different users with different cameras under different lighting conditions. The image quality of captured QR code depends not only on the sensitivity of camera sensors but also on environmental illumination. When there is no sufficient illumination, the image noises become higher. These noises are considered as an attack and they seriously degrade the quality of QR code digital image. Under such attack, the success rate for the QR code decoding will decrease. The first row of Fig. 10 shows the attack results of the stego QR code in Fig. 9b suffered serious noise attack in Matlab, such as Gaussian noise with parameter  $M = 0$  and  $V = 0.15$ , salt and pepper noise with parameter  $d = 0.10$ , speckle noise with parameter  $v = 0.10$ , respectively.

**Table 2** The embedding capacity of the proposed scheme

Versions	The embedding capacity of the proposed scheme(bits)				
	1	10	20	30	40
L	60	868	2729	5499	9370
M	50	684	2120	4352	7398
Q	41	488	1537	3122	5281
H	28	386	1220	2361	4044

In practical application, QR code would be printed on some kinds of paper media. These printed QR code might be defaced even damaged. These factors could be considered another kind of attacks which also reduce the success rate of the QR code decoding. We use the image editing tools to paint and erase the stego QR code to simulate the fouling attack. The second row of Fig. 10 shows the attack results of stego QR code in Fig. 9b defaced by one line, one circle and one star, respectively. The last row of Fig. 10 shows the attack results of stego QR code in in Fig. 9b damaged with different area size.

The term “Readable” represents QR code public message can be read by any QR code standard scanner. The term “Decodable” represents the authentication message in the stego QR code can be successfully decoded by a custom QR code scanner that supports the proposed scheme. The attack results show that the public message of stego QR code still can be decoded correctly despite a serious attack. Moreover, the authentication code embedded in the stego QR code can also be successfully extracted. It demonstrates that the proposed QR code authentication scheme is robust to different types of attacks.










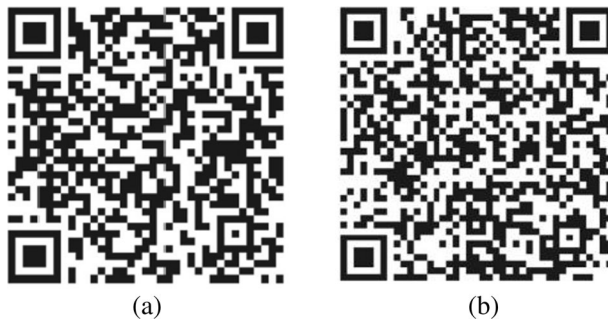
Noising settings:	Gaussian noise ( $M=0, V=0.15$ )	Salt & pepper noise ( $d=0.10$ )	Speckle noise ( $v=0.10$ )
Attack results:			
Public message:	Readable	Readable	Readable
Authentication code:	Decodable	Decodable	Decodable
QR code defacement:	One line	One circle	One star
Attack results:			
Public message:	Readable	Readable	Readable
Authentication code:	Decodable	Decodable	Decodable
QR code damage :	A square with 6% area size	Two squares with 3% area size	One square with 3% area size, the other 4%
Attack results:			
Public message:	Readable	Readable	Readable
Authentication code:	Decodable	Decodable	Decodable

Fig. 10 The results of different types of attacks on the stego QR code of the proposed scheme











**Fig. 11** An example of the QR code authentication patterns from Chen’s scheme [2]. **a** the original QR code with version 5-L; **b** the corresponding stego QR code of (a) with version 6-M

**4.4 The security of the proposed scheme**

The proposed scheme embeds the authentication code in the QR code padding region with the help of SEM. The authentication code embedding process and decoding process is very simple and easy to implement. Obviously, if a malicious user got the embedding key  $k$ (the Sudoku puzzle), he/she would be able to reconstruct the SEM, then easily extract the authentication code from the padding region of stego QR code. Therefore, the

QR code damage:	A square of 6% area size	Two squares of 3% area size	One square of 3% area size, and the other 4%
Attack results:			
	Valid	Invalid	Invalid
QR code defacement	One line	One circle	One star
Attack results:			
	Invalid	Invalid	Valid

**Fig. 12** The robustness of Chen’s scheme

Sudoku is the key to the security of the proposed QR code authentication scheme. Fortunately, as mentioned in Section 2.2, the number of possible solutions to a classical Sudoku is  $6,670,903,752,021,072,936,960 \approx 6.7 \times 10^{20}$ . The probability of a random guess to get the correct key is  $1/6.7 \times 10^{20} \approx 0.149 \times 10^{-20}$ , which indicates that our proposed scheme is very hard to crack. Therefore, the proposed QR code authentication scheme is highly secure.

#### 4.5 Comparison and discussion

In the literature, Chen's scheme [2] employed the symmetric and asymmetric encryption algorithm to generate the authentication code, then embedded these authentication code in the front portion of error correction codewords of the original QR code by replacing those error correction codewords with the authentication code directly. However, such operation would lead to the loss of data codewords in the RS code of QR code and it requires to exploit the error correction capability of the error correct codeword to fix it. In other words, it consumes the error correct codeword of the original QR code and makes it less robust. In order to overcome this defect, Chen's scheme had to generate a higher version of stego QR code than the original QR code requires. Figure 11a shows an example of the original QR code with version 5-L following Chen's scheme. To enhance the robustness of stego QR code, in Chen's scheme, they need to upgrade the version of the QR code to 6-M. Figure 11b shows the result of the corresponding stego QR code. Compared Fig. 11b with Fig. 11a, the upgraded stego QR code has a smaller module size. In consequence, it is highly likely to decrease the successful decoding rate of stego QR code. This problem becomes more serious especially when the QR code version is larger than 20 [25]. However, with the help of homomorphism of Reed-Solomon code, the proposed scheme embeds the authentication code in the padding region of original QR code without sacrificing the error correction capability. Thus, as shown in Fig. 9, the version of generated stego QR code is the same to the original QR code in the proposed scheme.

**Table 3** The embedding capacity compared Chen's scheme with the proposed scheme

QR code versions	Error correction levels	Chen's scheme (bits)	The proposed scheme(bits)
1	L(7%)	0	60
	M(15%)	0	50
	Q(25%)	0	41
	H(30%)	0	28
2	L(7%)	0	107
	M(15%)	32	88
	Q(25%)	56	69
	H(30%)	80	50
40	L(7%)	0	9370
	M(15%)	2488	7398
	Q(25%)	5160	5281
	H(30%)	6720	4044

**Table 4** The comparison of Chen's scheme and the proposed scheme

Schemes	Chen's scheme	The proposed scheme
The way of authentication code generation	Symmetric or asymmetric encryption algorithm	Hash function
Security	High	High
Robustness	Poor	Strong
Power consumption	Mid	Low
Embedding capacity	Adjustable [0, 6720]	Adjustable [28, 9370]

As mentioned above, the authentication code embedding strategy of Chen's scheme would lead to the consumption of the error correction capacity of QR code, and in turn, reduce the robustness of the generated stego QR code. Figure 12 shows the decoding results of stego QR code of Chen's scheme after suffering defacement or even partly damaged. The decoding results show that some of the stego QR codes of Chen's scheme became unable to read. However, as shown in Fig. 10, the public message and the authentication code of the stego QR codes of the proposed scheme still can be decoded and extracted after suffering similar attacks. It demonstrated that the robustness of the proposed scheme is much higher than Chen's scheme.

In terms of authentication code embedding capacity, Chen's scheme utilized the redundancy of error correction codewords to embed the authentication code. Therefore, the secret message embedding capacity depends on the error correction capacity of stego QR code. According to the embedding strategy of Chen's scheme, the version and error correction level of the stego QR code would be 1 higher than the original QR code to maintain the default error correction capacity which can correct 7% of error data codewords in QR code. It is easily inferred that version 2-M is the smallest version that could be used as stego QR code. According to the QR code specification, the error correction capacity of version 2-M QR code is 8 codewords while the error correction capacity of version 2-L QR code is 4 codewords. So the version 2-M stego QR code only has 4 ( $8-4=4$ ) codewords error correction codewords to correct the errors resulted from the embedding process, which is 32 ( $4 \times 8=32$ ) bits length of authentication code. And the version 40-H is the biggest version of stego QR code candidate which could embed 6720 bits of authentication code. In summary, the embedding capacity of Chen's scheme is in the range of [32, 6720]. However, the embedding capacity of the proposed scheme is limited by the length of the padding region of original QR code. Table 3 shows the embedding capacity comparison between Chen's scheme and the proposed scheme. It demonstrates that the proposed scheme has a higher embedding capacity than Chen's scheme for almost every QR code version.

In terms of security, Chen's scheme exploits the symmetric or asymmetric encryption algorithm such as ECDSA to protect the authentication message. It able to achieve high level security. In the proposed scheme, Sudoku is the key to the security of the proposed QR code authentication scheme. As mentioned in Section 2.2, the classical Sudoku has nearly  $6.7 \times 10^{20}$  possible solutions. The probability of one guessing is  $1/6.7 \times 10^{20} \approx 0.149 \times 10^{-20}$ , this is

almost impossible to crack when using Sudoku to encrypt the authentication code in the proposed scheme. So both the proposed QR code authentication scheme and Chen's scheme are highly secure.

In terms of power consumption, compared to the symmetric or asymmetric encryption algorithm used in Chen's scheme, the run time of the proposed authentication code generation method is much shorter than that of Chen's scheme. We implemented both Chen's scheme and the proposed scheme in python programming language, and tested the speed of the authentication extraction procedure in a personal computer respectively. This computer has an Intel Core i5-6200 U CPU and 8GB RAM, and runs with Win 10 operation system. The run time of the embedding procedure and tamper detection procedure of Chen's scheme are 0.727 s and 0.858 s respectively, and the corresponding run time of the proposed scheme are 0.173 s and 0.115 s respectively. It means that the proposed scheme does not require much computational power, and is able to achieve the high level security at the same time. It is more suitable for battery powered QR scanner.

Table 4 shows an overall comparison between Chen's scheme and the proposed scheme. As can be seen from the table, the proposed scheme achieves higher robustness, lower power consumption and higher embedding capacity than Chen's method.

## 5 Conclusions

In this paper, by exploiting the security and reversibility characteristics of Sudoku magic matrix and the homomorphism characteristic of Reed-Solomon code, we propose a new robust QR code authentication mechanism with authentication capacity enhancement to empower the QR code with the ability of secret message embedding and authentication. Experimental results show that the proposed scheme is simpler, more efficient, and less computational intensive compared to the existing algorithm. It can be used for QR code anti-counterfeiting. In the future, we will try to investigate other data hiding technique in order to increase the embedding capacity and further enhance the robustness for resisting various kinds of attacks.

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

## Compliance with ethical standards

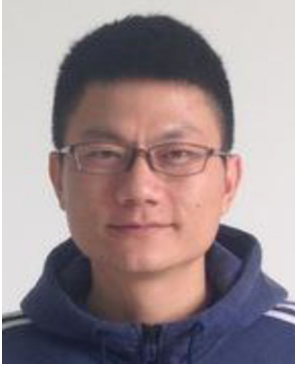
**Conflict of interest** The authors declare that they have no conflict of interest.

## References

1. Black J, Halevi S, Krawczyk H, Krovetz T, Rogaway P (1999) UMAC: Fast and secure message authentication. In: Annual International Cryptology Conference, Springer, pp 216–233
2. Chen C (2017) QR code authentication with embedded message authentication code. *Mobile Networks and Applications* 22(3):383–394
3. Chen Y-Y, Chi K-Y, Hua K-L (2017) Design of image barcodes for future mobile advertising. *EURASIP Journal on Image and Video Processing* 2017(1). <https://doi.org/10.1186/s13640-016-0158-x>

4. Conde-Lagoa D, Costa-Montenegro E, González-Castaño FJ, Gil-Castiñeira F (2010) Secure eTickets based on QR-Codes with user-encrypted content. In: 2010 Digest of Technical Papers International Conference on Consumer Electronics (ICCE). IEEE, pp 257–258
5. Cox R (2012) Qart codes. <http://research.swtch.com/qart>. Accessed Dec 2012
6. Felgenhauer B, Jarvis F (2003) Sudoku enumeration problems. <http://www.afjarvis.staff.shef.ac.uk/sudoku/>. Accessed 23 Nov 2017
7. Inc. D-W (2003) QR code standardization. [www.qrcode.com/en/about/standards.html](http://www.qrcode.com/en/about/standards.html). Accessed 24 Nov 2017
8. ISO B (2005) IEC 18004: 2006. Information technology Automatic identification and data capture techniques QR Code:126
9. Jing P, Su Y, Nie L, Bai X, Liu J, Wang M (2018) Low-rank multi-view embedding learning for micro-video popularity prediction. *IEEE Trans Knowl Data Eng* 30(8):1519–1532
10. Knuth DE (1985) Dynamic huffman coding. *Journal of algorithms* 6(2):163–180
11. Lerner A, Saxena A, Ouimet K, Turley B, Vance A, Kohno T, Roesner F (2015) Analyzing the use of quick response codes in the wild. In: Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services, ACM, pp 359–374
12. Li L, Wang R-l (2011) A digital watermarking algorithm for QR code. *Journal of Hangzhou Dianzi University* 31(2):46–49
13. Li F, Mao Q, Chang C-C (2016) A reversible data hiding scheme based on IWT and the Sudoku method. *International Journal of Network Security* 18(3):410–419
14. Liu M, Nie L, Wang X, Tian Q, Chen B (2019) Online data organizer: micro-video categorization by structure-guided multimodal dictionary learning. *IEEE Trans Image Process* 28(3):1235–1247
15. Lu J, Yang Z, Li L, Yuan W, Li L, Chang C-C (2017) Multiple schemes for mobile payment authentication using QR code and visual cryptography. *Mob Inf Syst* 2017(4356038):12. <https://doi.org/10.1155/2017/4356038>
16. Mazurczyk W, Caviglione L (2015) Steganography in modern smartphones and mitigation techniques. *IEEE Communications Surveys & Tutorials* 17(1):334–357
17. Motahari A, Adjouadi M (2015) Barcode modulation method for data transmission in mobile devices. *IEEE Transactions on Multimedia* 17(1):118–127
18. Nazemzadeh P, Fontanelli D, Macii D, Palopoli L (2017) Indoor localization of Mobile robots through QR code detection and dead reckoning data fusion. *IEEE/ASME Transactions on Mechatronics* 22(6):2588–2599
19. Pountain D (1987) Run-length encoding. *Byte* 12(6):317–319
20. Qian J, Du X, Zhang B, Fan B, Yang X (2017) Optimization of QR code readability in movement state using response surface methodology for implementing continuous chain traceability. *Comput Electron Agric* 139:56–64
21. Qin J, Sun R, Xiang X, Li H, Huang H (2016) Anti-fake digital watermarking algorithm based on QR codes and DWT. *Journal of the Society for Industrial and Applied Mathematics* 18(6):1102–1108
22. Reed IS, Solomon G (1960) Polynomial codes over certain finite fields. *J Soc Ind Appl Math* 8(2):300–304
23. Sun M, Si J, Zhang S (2007) Research on embedding and extracting methods for digital watermarks applied to QR code images. *N Z J Agric Res* 50(5):861–867
24. Tkachenko I, Puech W, Destruel C, Strauss O, Gaudin J-M, Guichard C (2016) Two-level QR code for private message sharing and document authentication. *IEEE Transactions on Information Forensics and Security* 11(3):571–583
25. Tkachenko I, Puech W, Strauss O, Gaudin J-M, Destruel C, Guichard C (2016) Centrality bias measure for high density QR code module recognition. *Signal Process Image Commun* 41:46–60

**Publisher's note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**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.



**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.



**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.



**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.