IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 26, 2020, accepted April 30, 2020, date of publication May 6, 2020, date of current version May 20, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2992694

Efficient QR Code Secret Embedding Mechanism Based on Hamming Code

PENG-CHENG HUANG[1,2], CHIN-CHEN CHANG[2,3], (Fellow, IEEE), YUNG-HUI LI[4], (Member, IEEE), AND YANJUN LIU[2]

[1]Department of Computer Science and Technology, Xiamen University of Technology, Xiamen 361024, China
[2]Department of Information Engineering and Computer Science, Feng Chia University, Taichung City 207, Taiwan
[3]School of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou 310018, China
[4]Department of Computer Science and Information Engineering, National Central University, Taoyuan City 320, Taiwan

Corresponding author: Chin-Chen Chang (alan3c@gmail.com)

This work was supported in part by the Natural Science Foundation of Fujian Province under Grant 2018J01571, in part by the Science and Technology Program of Xiamen under Grant 3502Z20183057, and in part by the Open Project of the Key Laboratory of Fujian Universities for Virtual Reality and 3D Visualization under Grant VRTV2019005.

ABSTRACT QR code is designed as machine readable symbol, which is widely used in various fields of life due to its large message capacity and fast decoding speed. However, as a public standard, it will give rise to the security issue when delivering sensitive information with QR code. To overcome this weakness, this paper explores the characteristic of QR code to propose an efficient secret hiding mechanism to protect the sensitive information within QR code. The secret message would be embedded into cover QR code based on (8, 4) Hamming code. The error correction capacity (ECC) of QR code would correct the errors produced in the secret embedding procedure, and the valid marked QR code would reduce people's curious. Compared to the state-of-art works, the proposed scheme achieves a better performance on the aspects of secret payload and embedding efficiency.

INDEX TERMS Secret hiding, QR code, Hamming code, error correction capacity.

I. INTRODUCTION

With the rapid development of mobile communication technology and Internet of things technology (IoT), electronic tag technology has gradually been widely used in all walks of life. Compared with one-dimensional barcode, Quick Response (QR) code has the advantages of large information capacity, high decoding reliability, strong error correction ability, wide range of storage information, high density, high information transmission efficiency, etc. It has been widely used in many fields, such as ID identification [1], advertising [2], warehousing and logistics [3], product traceability [4], e-commerce [5], mobile payment [6], [7], etc. As the core perception technology of Internet of things and the important information entrance of the Internet, QR code has gradually penetrated into various fields of national economy and social life. However, because of the openness of QR code encoding and decoding technology, the sensitive information transmitted by QR code is easy to be stolen, especially in the fields of O2O e-commerce, mobile payment and ID identification. This will cause security issue.

To protect the sensitive information in QR code, many researchers are investigating pattern recognition technology to improve the sensitive information security. Tkachenko *et al.* [8] designed a rich QR code to sharing the sensitive information. Their scheme constructed some special textured patterns to transmit the sensitive message by replacing them with black modules in the cover QR code. The same idea is applied to Erlangga *et al.*'s method [9], their method divided a QR code module into nine sub modules, then embedded the sensitive information by using those sub-module patterns. Although this kind of schemes always achieves a high secret payload, those schemes have two obviously disadvantages. The first one is the generated marked QR code would attract people's attention for its strange appearance. The second one is, those module patterns need to be identified by pattern recognition technology. However, the recognition rate of those module patterns still needs to be improved.

Recently, many researchers start to employ data hiding technology to solve this issue. The main idea of this kind

The associate editor coordinating the review of this manuscript and approving it for publication was Cesar Vargas-Rosales.

of research is embedding the secret message in the space domain of cover QR code, the generated marked QR code would be kept valid because of the fault tolerance of QR code. The valid and meaningful marked QR code would reduce people's attention when delivering in the public channel. Chang *et al.* [10] exploited the Wet Paper Codes algorithm [11] to uniformly distribute secret message in the cover QR code. To enhance the security of secret message embedded in the QR code, Lin *et al.* [12] proposed a new QR code secret hiding scheme to encrypt the secret message before embedding procedure. Then many researchers [13]–[16] study new secret embedding strategies for QR code to further improve the secret payload. However, these methods have low embedding efficiency, which is the average number of secret message bits carried by one bit flipping in the cover QR code. The lower the embedding efficiency, the more bits are modified in the cover QR code to embed a bit of secret message. The greater the difference before and after embedding, the higher the probability of being discovered.

To improve the embedding efficiency, this paper proposes a new secret message embedding scheme to embed sensitive message in the public message of a meaningful cover QR code. The new embedding mechanism designs a data bit flipping rule to hide a hexadecimal secret digit into data codeword based on (8, 4) Hamming code. The fault tolerance of cover QR code would correct the errors caused by the embedding procedure. The valid and meaningful marked QR code would divert people's attention. Experimental result shows that, the proposed secret embedding scheme achieves a high secret payload, and its embedding efficiency is close to 2.9, which is much better than the state-of-art works.

This paper is organized as follows: Section 2 briefly introduces QR code technology and Hamming code. Section 3 presents the state-of-art works. Section 4 presents the proposed secret embedding strategy for QR code based on (8, 4) Hamming code. Section 5 shows the experimental results and the comparison with previous works. Finally, Section 6 makes a conclusion.

II. PRELIMINARY

A. QR CODE TECHNOLOGY

QR code is an effective information transmission medium, it is widely used in product traceability, advertising, mobile payment and other filed. According to the QR code bar code symbology specification [17], QR code is defined into 40 symbol versions and 4 user-selectable error correction level (ECL): L, M, Q and H, it can correct up to 7%, 15%, 25% and 30% error codewords when attacked by defacement, respectively. This is due to the fault tolerance mechanism introduced by QR code standard. QR code employs Reed-Solomon code to realize the fault tolerance, the error correction codewords would be generated by Reed-Solomon code algorithm and added in the tail of QR code data codewords. Normally two error correction codewords could correct one codeword data error. Table 1 lists the fault tolerance of QR code for some specific version and error correction level.

TABLE 1. The error correction capacity of QR code.

Versions-Error correction level (V-E)	Total number of codewords	The number of error correction codewords
1-L	26	7
5-M	134	48
10-Q	346	192
15-H	655	432
20-L	1,085	224
25-M	1,588	588
30-Q	2,185	1,200
35-H	2,876	1,890
40-H	3,706	2,430

B. HAMMING CODE

Hamming codes [18] are a class of linear block codes, they were designed by Bell Labs in 1950 to detect and correct errors when the error rate is low. They have been widely used in digital communication and data storage systems as error control codes. The (n, k) Hamming code is n bits in length, it consists of k data bits and $(n - k)$ parity check bits. The minimum distance of a Hamming code is 3, it implies that Hamming code can detect and correct single-bit error or detect double-bits errors. Take the most basic Hamming code (7, 4) code as an example, (7, 4) Hamming code is 1-bit error correcting linear code which consists of 4 data bits and 3 parity check bits. The bit string $b_1b_2b_3b_4$ gets encoded as $c_1c_2b_1c_3b_2b_3b_4$ with:

$$\begin{aligned} c_1 &= b_1 \oplus b_2 \oplus b_4 \\ c_2 &= b_1 \oplus b_3 \oplus b_4 \\ c_3 &= b_2 \oplus b_3 \oplus b_4. \end{aligned} \tag{1}$$

This three parity check bits could potentially specify not only that an error occurred but also the error bit location. An additional parity bit c_0 can be added at the beginning or at the end of each codeword of (7, 4) Hamming code to derive an extended (8, 4) Hamming code.

$$c_0 = c_1 \oplus c_2 \oplus b_1 \oplus c_3 \oplus b_2 \oplus b_3 \oplus b_4. \tag{2}$$

This way, the minimum hamming distance of the Hamming code is increased form 3, in (7, 4) Hamming code, to 4 in (8, 4) Hamming code. Therefore, the (8, 4) Hamming code has the ability to detect up to 3 errors. It is also called Single Error Correction Double Error Detection (SECDED), and widely used in the computer ECC memory system. Figure 1 illustrates the bit position of the data bits and parity bits for Hamming (7, 4) and Hamming (8, 4) in Venn diagrams.

III. RELATED WORKS

A. LIN et al.'s METHOD

In 2017, Lin *et al.* [15] improved the LSB matching revisited embedding scheme [19] to hide secret message into cover QR code. The secret hiding procedure is outlined below.

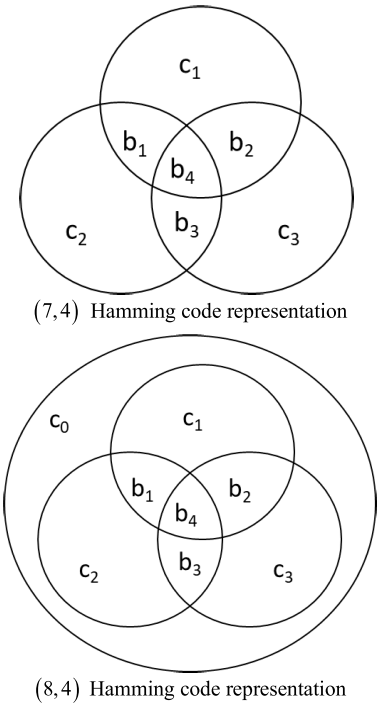


FIGURE 1. The relationship between data bits and parity check bits.

Step 1. Calculate the secret embedding capacity sc for the cover QR code. Generally, $sc = \lfloor n_e/2 \rfloor$, where n_e is the number of error correction codewords of QR code.

Step 2. Divide all the data codewords into several pairs, each pair consists of two modules, then put all of them into a pool.

Step 3. Select two data pairs p_1 and p_2 from the pool with a secret embedding key K.

Step 4. Embed four secret bits (denotes as s_1, s_2, s_3 and s_4) into this two data pair with (3). Then remove these two data pairs from the pool.

$$\begin{aligned} d_1^1 &= s_1 \\ d_1^2 &= s_2 \\ d_2^1 &= s_3 \\ d_2^2 &= s_4 - \lfloor d_1/2 \rfloor . \end{aligned} \tag{3}$$

Step 5. Count the number of modified digits n in Step 4, then renew the embedding capacity sc by $sc = sc - n$.

Step 6. Repeat Step 3 to Step 5, until all the secret message bits are embedded.

B. HUANG et al.'s SCHEME

Exploiting Modification Direction (EMD) [20], which was introduced by Zhang and Wang, is used to increase secret capacity and improve quality of the stego-image while hiding data in cover image. In 2018, Huang *et al.* [16] improved EMD method to propose a QR code steganographic scheme to hide sensitive information in a cover QR code. Their method defines a new secret message extraction function:

$$f(x, y) = x + 3 \times y \ (\text{mod} 8). \tag{4}$$

With the new extraction function, secret message would be embedded into the public message of cover QR code. The embedded procedure is as follows.

Step 1. Calculate the secret embedding capacity sc of cover QR code.

Step 2. Convert the secret message s and the cover QR code data codewords d into octal number sequence $\{s_0, s_1, \cdots, s_n\}$ and $\{d_0, d_1, \cdots, d_m\}$, respectively.

Step 3. Group two octal number from $\{d_0, d_1, \cdots, d_m\}$ in order as a data pair (x, y). Add or substrate the elements of data pair (x, y) in range of 1 to make the value of $f(x', y')$ equal to s_i, and $0 < i < n$.

$$s_i = f(x', y') = x' + 3 \times y' \ (\text{mod} 8). \tag{5}$$

Step 4. Repeat Step 3 until all the secret message s are embedded in the cover QR code, within the limited of secret capacity sc.

In the process of information extraction, the sensitive information will be easily retrieved with the help of extraction function (4). Their method embeds three bits of sensitive information in six bits of public message of cover QR code. Moreover, the secret embedding mechanism of Huang *et al.*'s scheme is based on the error correction capacity of cover QR code, so the amount of secret payload depends on the fault tolerance of cover QR code. The corresponding secret payload is $\left\lfloor sc \times 8/6 \right\rfloor \times 3$, and it's in the range of [12, 4860].

IV. THE PROPOSED SCHEME

This section presents a secret hiding scheme for QR code based on its error correction capacity. The proposed scheme employs (8, 4) Hamming to design a new secret embedding mechanism to improve the secret embedding efficiency, while maintaining a good secret payload.

A. THE SECRET EMBEDDING STRATEGY BASED ON HAMMING CODE

Let H be the parity-check matrix of extended (8, 4) Hamming code, and cw be a codeword of the (8, 4) Hamming code.

$$Hcw^T = \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \varphi \end{bmatrix} \tag{6}$$

where

$$\begin{aligned} \alpha &= c_1 \oplus b_1 \oplus b_2 \oplus b_4 \\ \beta &= c_2 \oplus b_1 \oplus b_3 \oplus b_4 \\ \gamma &= c_3 \oplus b_2 \oplus b_3 \oplus b_4 \\ \varphi &= c_0 \oplus c_1 \oplus c_2 \oplus b_1 \oplus c_3 \oplus b_2 \oplus b_3 \oplus b_4 \end{aligned} \tag{7}$$

If no error is introduced during data transmission, the vector $\begin{bmatrix} \alpha & \beta & \gamma & \varphi \end{bmatrix}^T$ will equal to zero. Suppose $cw + e_i$ is

(a) (b)

FIGURE 2. Example for QR code in version 5-M; (a) the cover QR code; (b) the marked QR code.

received, where e_i is the vector with only one position 1. In other words, one error is made in codeword cw.

$$\begin{aligned}\begin{bmatrix}\alpha & \beta & \gamma & \varphi\end{bmatrix}^T &= H\,(cw + e_i)^T \\ &= Hcw^T + He_i^T \\ &= 0 + h_i \\ &= h_i \end{aligned} \tag{8}$$

where h_i is one column of check matrix H. Suppose two errors are made in the codeword cw, and $cw + e_i + e_j$ is received. The corresponding result $\begin{bmatrix}\alpha & \beta & \gamma & \varphi\end{bmatrix}^T$ will be calculated as following.

$$\begin{aligned}\begin{bmatrix}\alpha & \beta & \gamma & \varphi\end{bmatrix}^T &= H\left(cw + e_i + e_j\right)^T \\ &= Hcw^T + He_i^T + He_j^T \\ &= 0 + h_i + h_j \\ &= h_i + h_j \end{aligned} \tag{9}$$

It equals to the sum of two columns of check matrix H. Since the value of vector $\begin{bmatrix}\alpha & \beta & \gamma & \varphi\end{bmatrix}^T$ from 0000 to 1111 can represent 16 status, we flip one or two bits of the codeword cw into a new codeword cw' to embed a hexadecimal number based on data bit flipping rules. The secret data would also be easily to extract by using (6). The data bit flipping rules is closely related to check matrix H. Table 2 illustrates the data flipping rules based on the check matrix H_1 showed in (10).

$$H_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{10}$$

The flipping operation in the public message of QR code would produce errors during QR code decoding. Thanks to the fault tolerance of QR code, it can still be decoded successfully when the numbers of error codewords is less than its ECC. A meaningful QR code will greatly reduce the possibility of secret information disclosure.

B. THE STEGANOGRAPHIC QR CODE PROCEDURE

Take H_1 as the parity-check matrix of extended (8, 4) Hamming code.

Input: Cover QR code QR_c, Secret message S.

Output: Marked QR code QR_s. The number of hexadecimal secret digit n.

TABLE 2. The data bit flipping rules based on the check matrix.

Data to be embedded	$[\alpha\beta\gamma\varphi]^T$	The bit locations that need to be flipped in the codeword cw
0	0000	unchanged
1	0001	1
2	0010	(1,2) or (3,4) or (5,6) or (7,8)
3	0011	2
4	0100	(1,3) or (2,4) or (5,7) or (6,8)
5	0101	3
6	0110	(1,4) or (2,3) or (5,8) or (6,7)
7	0111	4
8	1000	(1,5) or (2,6) or (3,7) or (4,8)
9	1001	5
10	1010	(1,6) or (2,5) or (3,8) or (4,7)
11	1011	6
12	1100	(1,7) or (2,8) or (3,5) or (4,6)
13	1101	7
14	1110	(1,8) or (2,7) or (3,6) or (4,5)
15	1111	8

TABLE 3. The secret embedding capacity of the proposed scheme.

Version \ ECL	The secret payload			
	L	M	Q	H
1	12	20	26	34
5	52	96	144	176
10	144	260	384	448
15	264	480	720	864
20	448	832	1,200	1,400
25	624	1,176	1,740	2,100
30	900	1,624	2,400	2,880
35	1,140	2,128	3,180	3,780
40	1,500	2,744	4,080	4,860

(a) (b)

FIGURE 3. Example for QR code in version 10-Q; (a) the cover QR code; (b) the marked QR code.

Step 1. Calculate the fault tolerant capacity tc of the cover QR code. Thanks to Reed-Solomon code, the error correction code within QR code could correct errors caused by fouling. According to the characteristic of RS code, two error correction codewords could correct one codeword data error, so the tolerant capacity tc is defined as

$$tc = \lfloor ecc/2 \rfloor, \tag{11}$$

here, ecc denotes the number of error correction code within the cover QR code. It's easy to conclude that the value of tc

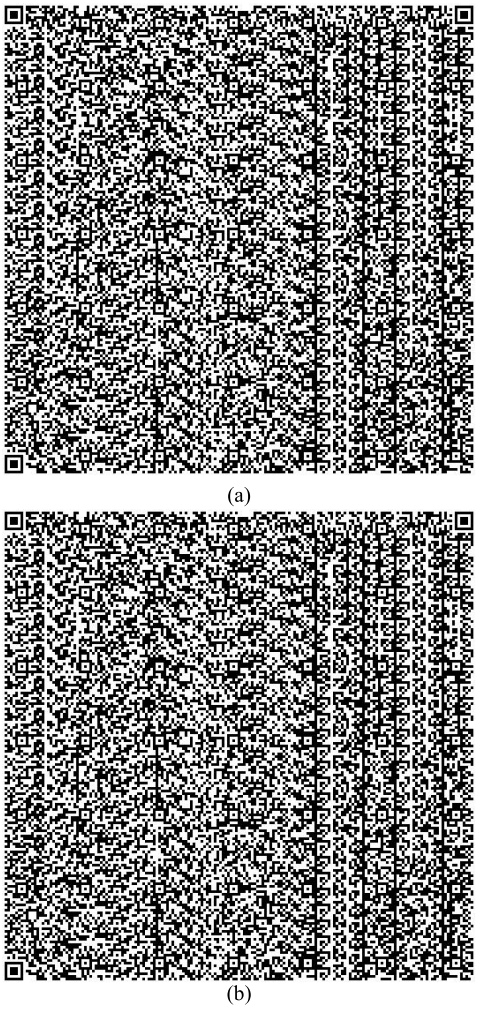


FIGURE 4. Example for QR code in version 40-H; (a) the cover QR code; (b) the marked QR code.

varies with the versions and error correction levels of cover QR code.

Step 2. Transform the secret message S into hexadecimal digit stream $\{s_1, s_2, \cdots, s_n\}$. If $n \leq tc$, then go to **Step 3**. Otherwise, reselect a later version of cover QR code and go back to **Step 1**.

Step 3. Let $i = 1$, where i represents the serial number of hexadecimal secret digit stream.

Step 4. Pick up a data codeword cw_i of cover QR code QR_c, then calculate the vector $\begin{bmatrix} \alpha & \beta & \gamma & \varphi \end{bmatrix}^T$ by using (12).

$$\begin{bmatrix} \alpha & \beta & \gamma & \varphi \end{bmatrix}^T = H_1 cw_i^T \oplus s_i, \tag{12}$$

where $\oplus$ represents the XOR operation.

Step 5. According to the result $\begin{bmatrix} \alpha & \beta & \gamma & \varphi \end{bmatrix}^T$, flip one or two bits in the data codeword cw_i by looking up flipping rules showed in Table 2.

Step 6. $i = i + 1$. If $i \leq n$, then go to **Step 4**. Otherwise, go to **Step 7**.

Step 7. The algorithm ends.

TABLE 4. The secret embedding capacity of the proposed scheme compared to previous works.

Versions	ECL	Lin et al.'s scheme	Huang et al.'s scheme	The proposed scheme
1	L	0	12	12
	M	4	18	20
	Q	4	24	26
	H	8	30	34
20	L	112	447	448
	M	208	831	832
	Q	300	1,200	1,200
	H	350	1,398	1,400
40	L	375	1,500	1,500
	M	786	2,742	2,744
	Q	1,020	4,080	4,080
	H	1,215	4,860	4,860

C. QR CODE EXTRACTION PROCEDURE

Input: The marked QR code QR_s. The number of hexadecimal secret digit n.

Output: Secret message S.

Step 1. Let $i = 1$, $S = \{\ \}$, where i represents the serial number of hexadecimal secret digit stream. S is used to store the secret message.

Step 2. Extract the secret message piece s_i from the data codeword cw_i' of marked QR code QR_s by using formula $s_i = H_1(cw_i')^T$.

Step 3. $S = S \cup s_i$, where '$\cup$' represents the consolidation of sets.

Step 4. $i = i + 1$. If $i \leq n$, then go to **Step 2.** Otherwise, go to **Step 5**.

Step 5. The algorithm ends.

V. EXPERIMENTAL RESULTS AND ANALYSIS

A. SOME EXAMPLES OF THE PROPOSED SCHEME

A program is implemented in Python programming language to access the availability of the proposed secret message embedding mechanism. Some experiments are done in different versions of QR code. Figure 2 shows the result of the proposed scheme with version 5-M QR code after embedding the secret message "1234567890987654321". The cover QR code is meaningful whose public message is "fcu.edu.tw". The secret message will be first converted into 16 hexadecimal digits stream: ('1', '1', '2', '2', '1', '0', 'f', '4', 'b', '1', '6', 'c', '1', 'c', 'b', '1'), then embedded in the first 16 public message data codewords with the proposed QR code secret message embedding mechanism based on (8, 4) Hamming code. There are totally 21 message bits need to be flipped in the embedding procedure. As shown in Table 1, QR code in version 5-M has 48 error correction codewords, this means that it could correct 24 codewords errors. The embedding procedure produces 16 errors codewords, which are within the tolerance range of QR code in version 5-M. And this will guarantee the validity of marked QR code. A valid and meaningful marked QR code will reduce people's curiosity. Figure 3 and Figure 4 show the examples for QR code in

FIGURE 5. The results of marked QR code in Figure 2 (b) after suffering noise attacks.

version 10-Q and version 40-H after embedding secret message "1234567890987654321123456789098765432-1234567890", respectively.

B. THE EMBEDDING CAPACITY OF THE PROPOSED SCHEME

One hexadecimal secret message digit is embedded in one public message codeword of cover QR code based on (8, 4) Hamming code, that is eight bits data hide four bits secret message. The embedding procedure of the proposed scheme ensures the validity of the marked QR code by limiting the number of error codewords within the corresponding fault tolerance of cover QR code. Therefore, the upper bound of secret message embedding capacity of the proposed scheme depends on the level of QR code version V-E. Table 3 lists the secret payload of cover QR code with different versions and different error correction levels.

C. THE EMBEDDING EFFICIENCY OF THE PROPOSED SCHEME

As mentioned in Section 1, the embedding efficiency is defined as the average number of secret message bits carried by one bit flipping in the cover QR code. In the secret embedding process of the proposed scheme, one public message data codeword would be flipped one bit or two bits to embed a hexadecimal secret digit based on (8, 4) Hamming code, one of the data bit flipping rule based on parity check matrix is showing in Table 2. From Table 2, we can see that, only one bit needs to be flipped when embedding an odd hexadecimal secret digit, two bits when embedding an even hexadecimal

secret digit, and zero bit when embedding secret message "0". Suppose that the probability of sixteen hexadecimal secret digits is equal, so the secret message embedding efficiency *ee* of the proposed scheme could be calculated as following.

$$ee = \frac{16 \times 4}{8 \times 1 + 7 \times 2 + 1 \times 0} \approx 2.9. \quad (13)$$

This means that the proposed scheme embeds nearly 2.9 secret bits into cover QR code when modifying one bit in public message codeword of cover QR code.

D. THE ROBUSTNESS OF THE PROPOSED SCHEME

QR code is usually scanned by QR code reader with camera. In the capturing process, lack of sufficient light will introduce noise into the QR code image. This noise will degrade the quality of QR code, and reduce success rate of QR code capturing process. Figure 5 shows the result that marked QR code shown in Figure 2 (b) suffers different level of noise attack, such as salt & pepper, gaussian noise, gaussian blur, speckle noise. The results show that the attacked marked QR codes are still valid, and the embedding secret message can be extracted correctly. It means that the marked QR code of the proposed scheme has a strong robustness against noise attack.

E. THE SECURITY OF THE PROPOSED SCHEME

The proposed scheme embeds secret message in public message of cover QR code based on (8,4) Hamming code. The check matrix H could be considered as a key to embed into cover QR code and extract secret message from marked QR code. Suppose that the adversary knows the secret embedding mechanism of the proposed scheme, and he try to extract secret message by adopting a brute force attack strategy to go through all the possibility of the check matrix H. Therefore, the probability of success for adversary to exact secret message will be bounded by $1/2^{32}$.

F. COMPARISON AND ANALYSIS

The secret hiding schemes for QR code always exploit some kinds of message embedding strategy to conceal the secret message bits in the public message of cover QR code. This research mainly concerns how to improve the secret payload and the embedding efficiency while keeping the marked QR code valid. The valid and meaningful marked QR code will greatly reduce the possibility of secret message being discovered.

As the aspect of secret payload, Lin *et al.*'s scheme embeds four bits secret message bits into two data pairs that randomly selected from a pool. However, this data pair selection strategy will evenly distribute the modified data bits in the cover QR code, it will lead to more error codewords than they expected. The corresponding secret payload would be reduced to between 0 and 1,215. Huang *et al.*'s method improved the EMD method to propose a secret hiding scheme for QR code. Their method embeds three bits of secret message in six bits of public message of cover QR code.

TABLE 5. The flipping number of data pair when hiding secret digits 0-7 in it in the field of GF(8).

Secret digit	The extraction function value	Data pair after being modified	Bits need to be flipped
0	$f(x_1+0, x_2+1)$	(0,0)	3
1	$f(x_1+1, x_2+1)$	(1,0)	4
2	$f(x_1+0, x_2-1)$	(0,6)	1
3	$f(x_1+1, x_2-1)$	(1,6)	2
4	$f(x_1-1, x_2+0)$	(7,7)	3
5	$f(x_1+0, x_2+0)$	(0,7)	0
6	$f(x_1+1, x_2+0)$	(1,7)	1
7	$f(x_1-1, x_2+1)$	(7,0)	6

The secret embedding mechanism of Huang *et al.*'s scheme is based on the error correction capacity of cover QR code, so the fault tolerance determines the upper limit of the secret embedding capacity. The corresponding secret payload is $\lfloor sc \times 8/6 \rfloor \times 3$, and it's in the range of [12, 4860]. The proposed scheme exploits the error correction capacity of QR code to hide the secret message in the space domain of cover QR code. Four secret message bits are embedded in a data codewords, therefore, the scope of secret payload of the proposed scheme is in the range of [12, 4860]. Table 4 lists the secret payload comparison between the proposed scheme and previous works.

As the aspect of embedding efficiency, Lin *et al.*' scheme embeds four bits secret message into four bits data codeword by using (3), the data bits in public message codewords ranging from 0 to 4 need to be flipped for secret embedding. Suppose that the probability of these five cases is equal. Therefore, the embedding efficiency ee_{Lin} can be calculated as follows.

$$ee_{Lin} = \frac{4+4+4+4+4}{4+3+2+1+0} = 2.0 \quad (14)$$

Huang *et al.*'s scheme embeds three bits secret message into six bits data codeword by using improved EMD scheme. The number of flipped bits varies according to different secret bits and different carrier data codeword. Table 5 shows an example to count the number of flipped bits of data pair (0, 7) when embedding secret digits 0-7 in it in the field of GF(8). Therefore, we randomly generated 100 bits of secret message, and then embedded secret message into a version 20-H cover QR code according to the embedding process of Huang *et al.*'s scheme. With 100 embedding iterations, we found out that the embedding efficiency ee_{Huang} close to 1.4. As analyzed in Section 5.3, the embedding efficiency of the proposed scheme is close to 2.9, which is much better than previous two schemes.

TABLE 6. The comparison of previous QR code secret hiding methods with the proposed scheme.

Methods	Lin et al.'s scheme	Huang et al.'s scheme	The proposed scheme
Utilizing the error correction capability	Yes	Yes	Yes
Module-based	Yes	Yes	Yes
Need secret key?	Yes	No	No
The secret payload	Adaptable [0~1,215]	Adaptable [12~4,860]	Adaptable [12~4,860]
The embedding efficiency	2.0	1.4	2.9

Table 6 lists the performance comparison of the proposed scheme with Lin *et al.*'s scheme and Huang *et al.*'s scheme. It can be seen from table 6, the proposed scheme achieves a better performance in secret payload and embedding efficiency aspects.

VI. CONCLUSION

This paper presents a new secret hiding scheme for QR code based on (8,4) Hamming code, the proposed scheme improves the embedding efficiency on the basis of keeping good secret payload. This method can effectively protect the sensitive information in QR code from being discovered while transmitting in the public channel. Although the error correction capacity of QR code keeps the marked QR code valid after embedded secret message, it also limits the upper bound of secret payload. For future work, we plan to invest the linear characteristic of Reed-Solomon code employed by QR code to improve the secret payload.

REFERENCES

[1] J. Cucurull, S. Guasch, A. Escala, G. Navarro-Arribas, and V. Acín, "QR steganography—A threat to new generation electronic voting systems," in *Proc. 11th Int. Conf. Secur. Cryptogr.*, 2014, pp. 1–8.

[2] Y.-Y. Chen, K.-Y. Chi, and K.-L. Hua, "Design of image barcodes for future mobile advertising," *EURASIP J. Image Video Process.*, vol. 2017, no. 1, pp. 1–12, Dec. 2017.

[3] A. Avidan, C. Weissman, and P. D. Levin, "Integration of QR codes into an anesthesia information management system for resident case log management," *Int. J. Med. Informat.*, vol. 84, no. 4, pp. 271–276, Apr. 2015.

[4] L. Tarjan, I. Šenk, S. Tegeltija, S. Stankovski, and G. Ostojic, "A readability analysis for QR code application in a traceability system," *Comput. Electron. Agricult.*, vol. 109, pp. 1–11, Nov. 2014.

[5] Y.-W. Chow, W. Susilo, G. Yang, M. H. Au, and C. Wang, "Authentication and transaction verification using QR codes with a mobile device," in *Proc. 9th Int. Conf. Secur., Privacy, Anonymity Comput., Commun., Storage, SpaCCS*, Zhangjiajie, China, Nov. 2016, pp. 437–451.

[6] J. Gao, V. Kulkarni, H. Ranavat, L. Chang, and H. Mei, "A 2D barcode-based mobile payment system," in *Proc. 3rd Int. Conf. Multimedia Ubiquitous Eng.*, Jun. 2009, pp. 320–329.

[7] J. Lu, Z. Yang, L. Li, W. Yuan, L. Li, and C.-C. Chang, "Multiple schemes for mobile payment authentication using QR code and visual cryptography," *Mobile Inf. Syst.*, vol. 2017, pp. 1–12, Mar. 2017.

[8] I. Tkachenko, W. Puech, C. Destruel, O. Strauss, J.-M. Gaudin, and C. Guichard, "Two-level QR code for private message sharing and document authentication," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 3, pp. 571–583, Mar. 2016.

[9] W. Erlangga and A. M. Barmawi, "Increasing secret data hiding capacity in QR code using 3×3 subcells," in *Proc. Int. Workshop Digit. Watermarking*, 2016, pp. 327–342.

[10] Y.-J. Chiang, P.-Y. Lin, R.-Z. Wang, and Y.-H. Chen, "Blind QR code steganographic approach based upon error correction capability," *KSII Trans. Internet Inf. Syst.*, vol. 7, no. 10, pp. 2527–2543, Oct. 2013.

[11] J. Fridrich, M. Goljan, and D. Soukal, "Wet paper codes with improved embedding efficiency," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 1, pp. 102–110, Mar. 2006.

[12] P.-Y. Lin, Y.-H. Chen, E. J.-L. Lu, and P.-J. Chen, "Secret hiding mechanism using QR barcode," in *Proc. Int. Conf. Signal-Image Technol. Internet-Based Syst.*, Dec. 2013, pp. 22–25.

[13] P.-Y. Lin and Y.-H. Chen, "QR code steganography with secret payload enhancement," in *Proc. IEEE Int. Conf. Multimedia Expo Workshops (ICMEW)*, Seattle, WA USA, Jul. 2016, pp. 1–5.

[14] M. Luo, S. Wang, and P.-Y. Lin, "QR code steganography mechanism with high capacity," in *Proc. Int. Conf. Commun. Problem-Solving (ICCP)*, Sep. 2016, pp. 1–2.

[15] P.-Y. Lin and Y.-H. Chen, "High payload secret hiding technology for QR codes," *EURASIP J. Image Video Process.*, vol. 2017, no. 1, pp. 1–14, Dec. 2017.

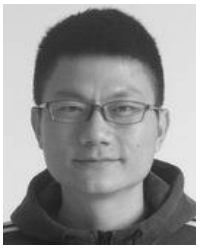
[16] P.-C. Huang, Y.-H. Li, C.-C. Chang, and Y. Liu, "Efficient scheme for secret hiding in QR code by improving exploiting modification direction," *KSII Trans. Internet Inf. Syst.*, vol. 12, no. 5, pp. 2348–2365, 2018.

[17] Denso Wave Incorporated. *QR Code Standardization*. Accessed: May 21 2019. [Online]. Available: https://www.qrcode.com/en/about/standards.html

[18] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 26, no. 1, pp. 96–99, Jan. 1983.

[19] J. Mielikainen, "LSB matching revisited," *IEEE Signal Process. Lett.*, vol. 13, no. 5, pp. 285–287, May 2006.

[20] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," *IEEE Commun. Lett.*, vol. 10, no. 11, pp. 781–783, Nov. 2006.



PENG-CHENG HUANG received the B.S. degree from the Xiamen University of Technology, in 2007, and the M.S. degree in computer architecture from Fuzhou University, in 2010. He is currently pursuing the Ph.D. degree from Feng Chia University. He is currently a Lecturer with the Xiamen University of Technology. His current research interests include multimedia security, image processing, and the Internet of Things.

CHIN-CHEN CHANG (Fellow, IEEE) received the B.S. degree in applied mathematics and the M.S. degree in computer and decision sciences from National Tsing Hua University, Taiwan, in 1977 and 1979, respectively, and the Ph.D. degree in computer engineering from National Chiao Tung University, Taiwan, in 1982. He is currently a Professor with Feng Chia University. He is also the author of more than 900 journal articles and has written 36 book chapters. His research interests include computer cryptography, data engineering, and image compression.

YUNG-HUI LI (Member, IEEE) received the B.S. degree from National Taiwan University, in 1995, the M.S. degree from the University of Pennsylvania, in 1998, and the Ph.D. degree from the School of Computer Science, Language Technology Institute, Carnegie Mellon University, in 2010. He is currently an Assistant Professor with National Central University. He is also the author of more than 30 conference and journal articles and has written five book chapters. His current research interests include image processing, machine learning, pattern recognition, and biometric recognition.

YANJUN LIU received the Ph.D. degree from the School of Computer Science and Technology, University of Science and Technology of China (USTC), Hefei, China, in 2010. She has been an Assistant Professor with Anhui University, China, since 2010. She currently serves as a Senior Research Fellow with Feng Chia University, Taiwan. Her specialties include E-business security and electronic imaging techniques.