Efficient Scheme for Secret Hiding in QR Code by Improving Exploiting Modification Direction

Peng-Cheng Huang[1], Yung-Hui Li[2], Chin-Chen Chang [3] and Yanjun Liu[4]

[1] Xiamen University of Technology, Department of Computer Science,
No. 600 Ligong Rd., Xiamen, China, 361024
[e-mail: HuangPengCheng@xmut.edu.cn]

[2] National Central University, Department of Computer Science and Information Engineering,
No. 300, Zhongda Rd., Zhongli District, Taoyuan, Taiwan, 32001
[e-mail: yunghui@gmail.com]

[3] Feng Chia University, Department of Information Engineering and Computer Science,
No. 100, Wenhwa Rd., Seatwen, Taichung, Taiwan, 40724
[e-mail: alan3c@gmail.com]

[4] Feng Chia University, Department of Information Engineering and Computer Science,
No. 100, Wenhwa Rd., Seatwen, Taichung, Taiwan, 40724
[e-mail: yjliu104@163.com]

*Corresponding author: Chin-Chen Chang

Received July 26, 2017; revised October 1, 2017; revised November 14, 2017; accepted December 12, 2017; published May 31, 2018

Abstract

QR codes as public patent are widely used to acquire the information in various fields. However, it faces security problem when delivering the privacy message by QR code. To overcome this weakness, we propose a secret hiding scheme by improving exploiting modification direction to protect the private message in QR code. The secret messages will be converted into octal digit stream and concealed to the cover QR code by overwriting the cover QR code public message bits. And the private messages can be faithfully decoded using the extraction function. In our secret hiding scheme, the QR code public message still can be fully decoded publicly from the marked QR codes via any standard QR Code reader, which helps to reduce attackers' curiosity. Experiments show that the proposed scheme is

http://doi.org/10.3837/tiis.2018.05.024 **ISSN : 1976-7277**

feasible, with high secret payload, high security protection level, and resistant to common image post-processing attacks.

Keywords: Secret hiding, QR code, exploiting modification direction

1. Introduction

With the development of information technology, QR code [1] has been widely used to deliver and receive interested information in the realm of e-commerce, m-commerce, entertainment industry and social network. The original framework of QR code aims to embed the machine-readable message with error tolerance. As we know that the QR code standard is a public patent, so the QR code message can be read directly by any standard QR code reader. Such intrinsic nature of QR code will result in privacy issues when the sender wants to deliver private messages using QR code to the receiver. Take hospital medical care as an example, it is a good practice to use QR code to record patient information for better management. However, as shown in **Fig. 1**, anyone can read the patient's private information which is stored in the QR code by standard QR code reader. Such mechanism enhances the risks of the patient's private information being leaked. In order to protect the private messages, the traditional way [2] is to store the private messages in the database in the cloud, and the QR code only embeds the URL that links to the database. Only the user with the right access permission can log in to the database and retrieve the private messages [3]. However, the exposed URL that links to the back-end database will attract the intruder's attention, which incubates a potential risk.

Fig. 1. One practical scenario of general QR code in medical care

In recent years, many researchers proposed new methods for this purpose using data hiding technique. Again, let's take medical care as an example. As shown in **Fig. 2**, with the help of data hiding technique, the patient's private information will be encoded into a cover QR code, and the general QR code reader can only decode the public message of cover QR code which is a meaningless patient's serial number. However, with the private key, the special QR code reader can read not only the patient's serial number but also the patient's detail

information. In such a way, we can reduce the risk of the leakage of the patient's personal information.

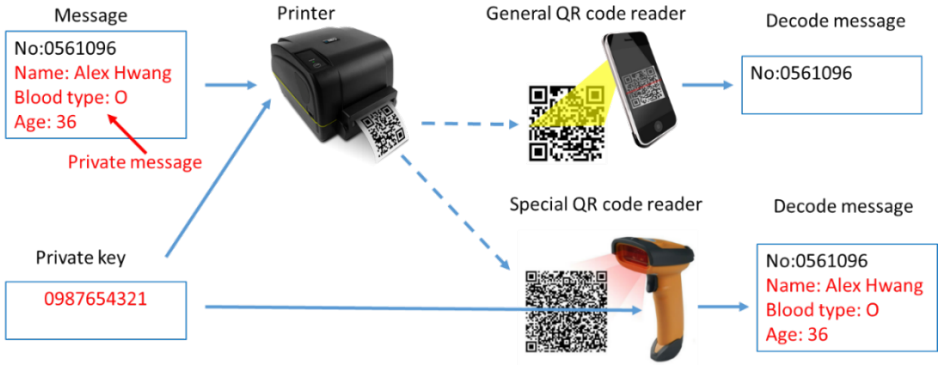


Fig. 2. One practical scenario of the QR code with data hiding ability.

In recent years, some researchers start to use the pattern recognition technique to embed and extract the private messages under the cover QR code. Teraura et al. [4] designed an information hiding scheme to hide the private message in each QR code module with different patterns. Here, a module represents a bit of information in the QR code. Their method treated each QR code module as a cell, which is further segmented to be a 3*3 subcell or 5*5 subcell. The patterns of different subcells represent different information. In order to improve the accuracy of private message extraction, their method exploited Hamming code to correct the errors when some subcells in the QR code were wrongly decoded. However, these subcells may be recognized as white module with the standard QR code decoding processing, so how to correctly identify these subcell's patterns still remains a challenge in their scheme. Tkachenko et al. [5] presented a new rich QR code which has public and private storage levels. The public storage level of this two-level QR code stored QR code public message, which could be decode by any general QR code reader. The private level was used to share private message by replacing the QR code black modules with special textured patterns. The private message was firstly encoded in a q-ary notational system, and q kinds of textured patterns were used to represent these q numbers. Using a special QR code reader, the receiver could correctly extract the private message from the two-level QR code. However, how to improve the correct rate of pattern recognition of these textured pattern is a critical issue in their scheme.

Some researchers start to use the data hiding technique and the QR code error correction mechanism to embed and extract the private messages under the cover QR code. According to the standard of QR code, it employs Reed-Solomon code [6] to correct the errors when a portion of QR code was defaced or some QR code modules were wrongly decoded. The eight consecutive bits of QR code message constitute a codeword, each of which will be the coefficients of the message polynomial in Reed-Solomon code encoding, and the corresponding error correction codewords will be generated. A single codeword error always

needs two codeword error correction codes to correct it in the QR code decoding procedure.

Chiang et al. [7] designed a blind QR code steganographic scheme to embed the private message into the cover QR code randomly by exploiting the wet paper codes algorithm [8]. An additional secret key was used to generate a pseudorandom binary bits stream to mask with the secret bits stream in order to guarantee the security of the secret message. This secret key was shared among the sender and receiver. With the error correction capacity of QR code, QR code reader can decode the QR code public message, but the private message can only be retrieved by the authored user. The private message payload is limited by the cover QR code version and its error correction level. However, the wet paper codes algorithm is an average distribution of probability models. All the secret bits will be evenly distributed in the data codewords of the cover QR code. This means that most data codewords of QR code will have a bit of error, it will lead to these data codewords to be an error codeword. So the number of error codewords will be larger than the QR code error correction capacity, and the decoding procedure will fail. The details of the private message capacity will be discussed in Section 4.3. In order to guarantee their scheme can work, the capacity of secret message should be far less than the estimated value in [7].

To improve the robustness of secret hiding scheme, Bui et al. [9] designed a robust secret hiding scheme to encode the secret message bits stream by applying Reed-Solomon codes before embedding process and recover the lost secret bit by applying List Decoding [10] in extraction process. It is worth mentioning that this scheme encoded the private message with redundant information by applying Reed-Solomon code before embedding them into the QR code. These redundant information messages formed the so-called error correction codes which need to take up some storage space, so the private message payload would be smaller than Chiang et al.'s scheme.

Lin and Chen [11] proposed a QR code data hiding scheme to hide each two secret message bits in a module pair by exploiting modification direction (EMD) [12]. But their scheme did not consider the overflow and underflow problem in the embedding process. To increase the private message payload, Lin et al. [13] designed another QR code steganographic scheme to hide private message in cover QR code using LSB matching revisited embedding algorithm. The experimental results showed that the average private message payload would be a little bit higher than the previous research. However, these two schemes built a pool which contains all the module pairs at the beginning of secret embedding process, then used a secret key to randomly pick up one or two module pairs from the pool, and embedded the secret bits in these module pairs. The operation is similar to the wet paper codes algorithm mentioned earlier, embedded the secret bits into the data codewords of cover QR code randomly. These secret bits will be evenly distributed in the data codewords of the cover QR code, this will cause these two schemes to face the same situation as Chiang et al.'s scheme. There are too many error codewords in the QR code data codewords, more than its error correction capacity, and the QR code decoding process may

fail. In order to ensure that those schemes can work, the secret payload will be less than expected.

To overcome the shortcoming of these secret hiding scheme, we propose a new efficient and feasible QR code secret hiding approach to conceal the secret message bits by improving exploiting modification direction. The new approach embeds the secret message bit stream by modifying the QR code module in sequence to avoid excessive consumption of QR code error correction capacity, and it meets the requirement of the security and robustness for the QR secret hiding system. The generated marked QR codes have high robustness when suffered from noise and blur, and the secret payload is enhanced.

This paper is organized as follows. The technique of QR code and exploiting modification direction are introduced in Section 2. The proposed secret hiding scheme with secret payload enhancement will be presented in Section 3. Section 4 presents the simulation result and the performance of the proposed scheme. Finally, Section 5 presents the conclusions and future works.

2. Preliminary

2.1 The Technology of QR Code

QR code was invented by a Japanese company named Denso Wave in 1994. The QR code consists of an array of nominally square module arranged in an overall square pattern, and the black and white square module represent the digits one and zero, respectively. **Fig. 3** shows the basic structure of the QR code, such as the version information, format information, data codewords, error correction codewords, position detecting patterns, alignment patterns, timing patterns and the quiet zone.

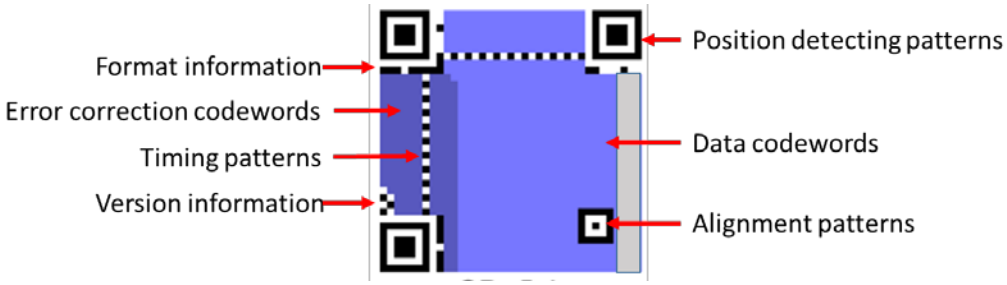


Fig. 3. Structure of a QR Code symbol

The QR code standard provides a total of 40 different versions of the storage density structure. The first version of QR code has 21 × 21 modules, and its length and width are increased by 4 modules when the version increased by 1. The largest version of QR code has 177 × 177 modules. QR code has the ability of fault tolerance, which can still be decoded even if portions of the QR code were destroyed or damaged. To achieve fault tolerance, the

QR code standard offers four user-selectable error correction levels for each version, as listed in **Table 1**. For instance, level H of error correction allows recovery of 30% of the codewords. Here, the codeword is a unit in the QR tag that is equal to eight modules.

Table 1. Error correction levels

Error Correction Level	Recovery Capacity % (approx.)
L	7
M	15
Q	25
H	30

Table 2 briefly presents the storage capacity of different error correction levels and versions of QR code. For example, in the version 20-H, there is a total of 1085 codewords, of which 700 are error correction codewords (leaving 385 data codewords). The 700 error correction codewords can correct 350 misdecodes or substitution errors, i.e. 350/1085 or 32.3% of the symbol capacity.

Table 2. Capacity of different versions of QR code.

Versions	Error Correction Level	Number of Data Codewords	Number of Error Correction Codewords
1	L	19	7
	M	16	10
	Q	13	13
	H	9	17
20	L	861	224
	M	669	416
	Q	485	600
	H	385	700
40	L	2,956	750
	M	2,334	1,372
	Q	1,666	2,040
	H	1,276	2,430

2.2 Exploiting Modification Direction

As we all know, a group of n pixels has $2n$ kinds of possible ways of modification when only one pixel is modified by increasing or decreasing by 1 each time. Considering the case in which no pixel value is changed, there are $(2n+1)$ possible ways of modification. Take advantage of this principle, Zhang and Wang [12] proposed a steganographic embedding method by exploiting modification direction (EMD) to hide each secret digit in n cover pixels. In the secret embedding phase, the EMD method firstly converted the secret message

into a stream digits in a $(2n+1)$-ary notational system, then pseudo-randomly permuted all the cover pixels using a privacy key, and divided them into groups, each of them with n pixels. The grayscale values of each pixel group was denoted as $p_1, p_2, \cdots, p_n$, and the weighted sum could be calculated by the extraction function f modulo $2n+1$.

$$f(p_1, p_2, \cdots, p_n) = \left[\sum_{i=1}^{n}(p_i \cdot i)\right] \ mod(2n+1). \tag{1}$$

For a group of n pixels, when the secret bit s to be embedded is equal to the weighted sum f of that pixel group, there is no need to change in this pixel group. When $s \neq f$, calculate $d = s - f \ mod \ (2n+1)$, then one pixel value would be modified by Formula (2) , as shown in the following.

$$\begin{cases} p'_d = p_d + 1, & if \ d \leq n \\ p'_{2n+1-d} = p_{2n+1-d} - 1, & if \ d > n \end{cases}. \tag{2}$$

In the extraction phase, the secret bit can be easily retrieved by calculating the extraction function f of stegoimage pixel group, as shown in Formula (1). With the application of the EMD embedding method, the PSNR value of stego-image would be larger than fifty, and the embedding rate R up to $\log_2^{(2n+1)}/n$.

Many researchers [14, 15] started to use the EMD method to hide secret in the cover image. The experiments showed that the EMD method had a great help in increasing the secret payload and improving stego-image quality.

3. The Proposed Scheme

The proposed scheme is a QR code steganographic method with high secret payload by improving exploiting modification direction. It contains secret embedding procedure and secret extraction procedure. **Fig. 4** shows the flowchart of secret embedding procedure. In this proposed scheme, the secret message bits are hided and extracted by using the improving EMD method, the extraction function is defined as the sum of the first digit multiplied by one and the second digit multiplied by three modulo eight, as shown in Eq. (3). This is the major difference from those extraction functions in Zhang and Wang's scheme [12] (as shown in Eq. (1)) and Lin and Chen's scheme [11].

$$f(x_1, x_2) = x_1 \times 1 + x_2 \times 3 \ (mod \ 8). \tag{3}$$

With the new extraction function, the secret message bits are easy to hide into the cover QR code and extract from marked QR code. Moreover, the proposed scheme has a high

secret payload while keeps the marked QR code readable, and is able to avoid the overflow and underflow problems.

3.1 The embedding procedure

Suppose that S is the secret message bits stream to be embedded, and a private key k is used to permute the secret message to be a pseudo-random message s'. The cover QR code stores meaningful messages, such as public message or an URL. The secret message will be concealed into the cover QR code by improving EMD method, and a meaningful marked QR code will be generated. The meaningful marked QR code will help to reduce the attention of attacker. The flowchart of embedding procedure is listed as follows:

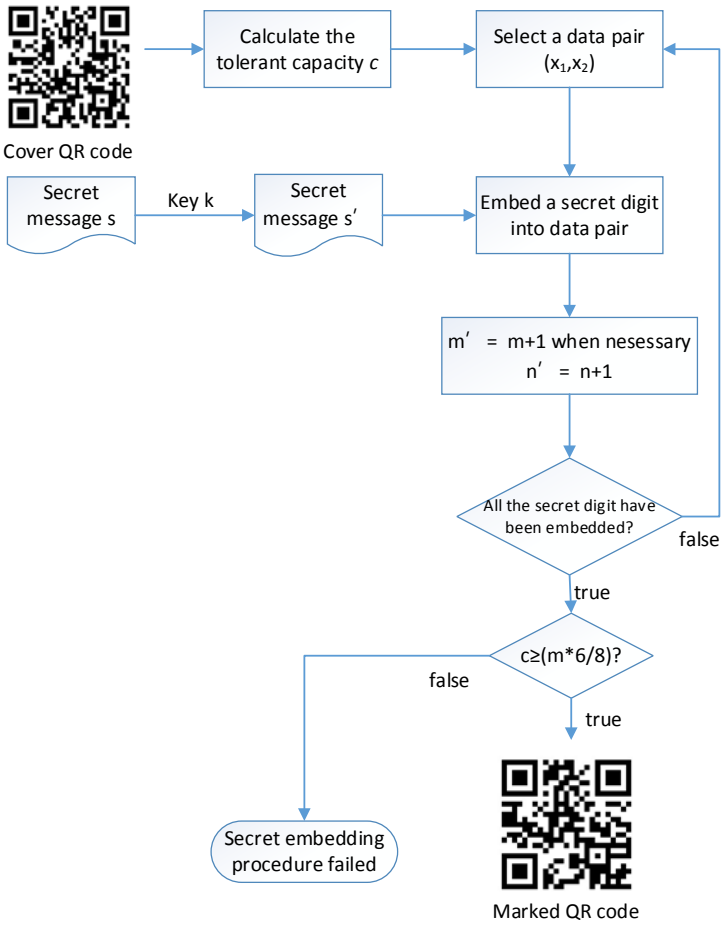


Fig. 4. The flowchart of secret embedding procedure

Step 1) convert the secret message into a stream of secret digits in an 8-ary notational system. A digit in 8-ary notational system is very easy to transform into a 3-bit value in a binary system. Then pseudo-random permuted all the secret digits using a privacy key k.

Step 2) calculate the tolerant capacity, c, of secret message bits for the cover QR code. QR

code employs Reed-Solomon code to enable the symbol to withstand damage without loss of data. According to the feature of Reed-Solomon code, two error correction codewords (ECC) could correct one codeword's error, here, the codeword is a unit in the QR code that is equal to eight modules. The capacity c is defined as

$$c = \left\lfloor \frac{ecc}{2} \right\rfloor, \tag{4}$$

here, ecc is the number of error correction codewords in the cover QR code. Obviously, the value c is dynamically changed with the cover QR code version and its error correction level. According to the QR code specification, QR code versions of 1-L, 1-M, 1-Q, 1-H, 2-L, 3-L use some error correction codewords as misdecode protection codewords, that will sacrifice the QR code error correction capacity, so the actual capacity of those version of QR code will be a little bit less than $\lfloor ecc/2 \rfloor$.

Step 3) transform the message of cover QR code into binary bit stream.

Step 4) sequentially pick two 3-bits length cover QR code message bit stream, and denote them as x_1 and x_2, where x_1 and x_2 stand for the value of the first and second 3-bits length message stream, respectively. Finally, let them be a data pair (x_1, x_2).

Step 5) calculate the weight sum of the data pair (x_1, x_2) by performing the extraction function f as shown in Eq. (3).

Step 6) sequentially pick up a secret digit s in 8-ary notational system, and then compare s with f. Use a counter, denoted as m, to record the number of times the data pair was modified. If s is equal to $f(x_1, x_2)$, there is nothing to change in the data pair (x_1, x_2). When $s \neq f(x_1, x_2)$, the data pair will be modified according to Eq. (5), and the counter m is updated as m+1.

$$\begin{cases} x_1' = x_1 + 1 & if\ s = f(x_1 + 1, x_2) \\ x_2' = x_2 + 1 & if\ s = f(x_1, x_2 + 1) \\ x_1' = x_1 \text{-} 1 & if\ s = f(x_1 \text{-} 1, x_2) \\ x_2' = x_2 \text{-} 1 & if\ s = f(x_1, x_2 \text{-} 1) \\ x_1' = x_1 + 1, x_2' = x_2 + 1 & if\ s = f(x_1 + 1, x_2 + 1) \\ x_1' = x_1 \text{-} 1, x_2' = x_2 \text{-} 1 & if\ s = f(x_1 \text{-} 1, x_2 \text{-} 1) \\ x_1' = x_1 + 1, x_2' = x_2 \text{-} 1 & if\ s = f(x_1 + 1, x_2 \text{-} 1) \\ x_1' = x_1 \text{-} 1, x_2' = x_2 + 1 & if\ s = f(x_1 \text{-} 1, x_2 + 1) \end{cases}, \tag{5}$$

here, all the operations in Eq. (5) are in the Galois Field GF(8). That will effectively avoid the overflow and underflow problems. **Table 3** shows the changes of the data pair $(5, 2)$ when embedding the secret digits 0-7 in it, and **Table 4** shows the changes of data pair $(0, 7)$ when embedding the secret digits 0-7 in it. Note that the data pair $(0, 7)$ is very easy overflow or underflow when embedding a secret digit in it, the operations in the GF(8) will help to avoid these situation.

Step 7) use another counter, denoted as n, to count the secret digits embedded by this proposed scheme. After Step 6, the counter n is updated as $n+1$.

Step 8) repeat the Steps 4 to 7 under the condition that the tolerant capacity $c \geq (m \times 6 \div 8)$ until all the secret digits have been embedded completely.

When the embedding procedure is finished, the secret digits are successfully hided in the cover QR code message area, and a new message bit stream for marked QR code is produced. Then, the marked QR code tag will be generated by replacing the QR code message with new message bit stream in sequence. The proposed scheme can guarantee that at most c codewords of cover QR code will be modified. This means the number of data codewords modified by embedding procedure is limited within the scope of marked QR code error correction capacity, so the marked QR code public message can still be read by any general QR code reader. The meaningful public message read from the marked QR code helps to reduce uninvolved user's curiosity.

Table 3. The changes of data pair $(5,2)$ when hiding secret digits 0-7 in it

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

Table 4. The changes of data pair $(0,7)$ when hiding secret digits 0-7 in it

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

3.2 The extraction procedure

Note that the marked QR code is meaningful, its public message can be read by any standard QR code reader. So, the extracted meaningful marked QR code data messages can help to reduce other people's curiosity while they are scanning this QR code. At the same time, the private message of marked QR code can also be easily extracted with the help of extraction function f (as shown in Eq. 3) and a private key k by a special QR code decoder. The secret message extraction procedure is listed as follows:

Step 1) read the original message from the marked QR code, and convert them to be a digit stream in 8-ary notational system.

Step 2) partition the first two digits as a data pair $\left(x_1', x_2'\right)$, then extract a secret digit by applying Eq. (3).

Step 3) after one secret digit extraction, remove this data pair $\left(x_1', x_2'\right)$, and update the secret digit number counter n as $n-1$.

Step 4) repeat the Step 2 to 3, until the secret digit number counter n is decreased to 0. That means all the secret digits are extracted completely.

Step 5) the secret message will be retrieved by reversing the permutation operation with the privacy key k.

Step 6) with the help of Reed-Solomon error correction code, the pubic message of marked QR code still can be decoded by general QR code reader.

4. Simulation Results and Analysis

The QR code secret hiding approach is implemented by python programming language under the simulation environment. Some experiments were performed from the lowest version to the highest version of error correction level of QR code. **Fig. 5** shows the results of the proposed scheme for a QR code, whose version is 1 and error correction level is L. According to the standard of QR code, version 1-L QR code can tolerate 2 codewords errors maximally. The cover QR code is a meaningful QR code with public message "fcu.edu.tw". The proposed scheme embeds a secret number 29 into the cover QR code with the improved EMD method to produce a new data codeword for marked QR code, and overwrites the first 12 bits of data codewords with those new data codewords in sequence, and the corresponding marked QR code will be generated, as shown in **Fig. 5(b)**. This operation will cause the marked QR code to have 12 bits errors, which are equal to $\lceil 12/8 \rceil = 2$ codewords errors. This two error codewords are equal to the version 1-L QR code's maximal error correction capacity, which is 2 codewords. So the public message "fcu.edu.tw" of the marked QR code still can be successfully decoded by any standard QR code reader. At the same time,

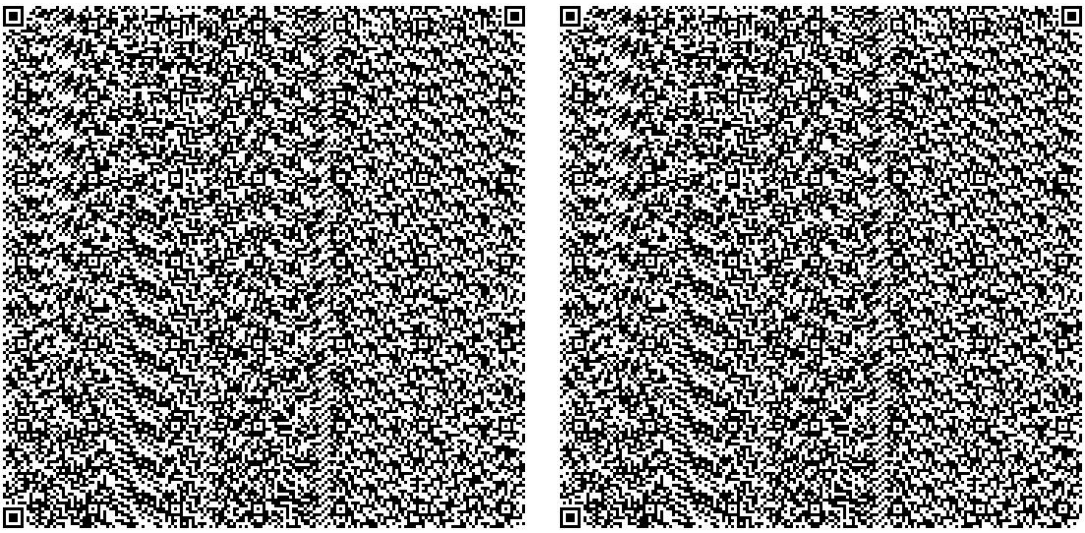
the private message “29” also can be extracted by a special QR code decoder. **Fig. 6** shows the results of version 10-M QR code after embedding secret message number 1866. And **Fig. 7** shows the results of version 40-H QR code after embedding secret message number 119475.

(a) (b)

Fig. 5. Example for version 1-L QR code; (a) the cover QR code with public message “fcu.edu.tw”, (b) the marked QR code embedded with secret number: 29

(a) (b)

Fig. 6. Example for version 10-M QR code; (a) the cover QR code with public message “fcu.edu.tw”, (b) the marked QR code embedded with secret number: 1866



(a) (b)

Fig. 7. Example for version 40-H QR code; (a) the cover QR code with public message “fcu.edu.tw”, (b) the marked QR code embedded with secret number: 119475

4.1 Storage capacity of the proposed scheme

The proposed scheme converts the secret message and original QR code data codewords in the 8-ary notation system, and hides the secret digits into a data pair within the scope of QR code error correction capacity. According to the secret embedding procedure, an octal secret number is hidden in an octal data pair, it means that six bits of data codewords are used to hide three bits of secret message. The maximal secret hiding capacity is limited to the QR code error correction capacity. So the storage capacity of the proposed scheme is equal to $\lfloor r \times 8/6 \rfloor \times 3$, here, r is the QR code error correction capacity. According to the specification of QR code, the error correction capacity of version 1-L QR code is the smallest, the corresponding value of r is equal to 2. The maximum value of r equals to 1215 in the version 40-H QR code. So it is easy to figure out that the scope of secret payload is in the range of [6, 4860], which is adjustable depending on the version and error correction level of cover QR code. **Table 5** shows the secret message payload for different versions and error correction levels of cover QR code.

Table 5. The secret message payload of the proposed scheme

Versions \ Error correction levels	Secret payload (bits)			
	L	M	Q	H
1	6	15	24	30
5	51	96	144	174
10	144	258	384	447
15	264	480	720	864
20	447	831	1200	1398
25	624	1176	1740	2100
30	900	1623	2400	2880
35	1140	2127	3180	3780
40	1500	2742	4080	4860

4.2 Robustness of the proposed scheme

In the real world applications, when the digital QR code is scanned in the absence of sufficient light conditions, it usually suffers from several image degradation factors, such as noise, blur, print-and-scan (P&S) and so on. These factors can be considered as a kind of image attack. Although the image after being attacked is visually similar to the original image, but in fact the image quality has degraded significantly. **Fig. 8** shows the results of the marked QR codes in **Fig. 6(b)** suffered from Gaussian noise (M=0, V=0.10), salt & pepper noise (d=0.10), speckle noise (v=0.10), Poisson noise, Gaussian blur (σ = 1) and print and scan process, respectively. In the print-and-scan attack module, the marked QR code was

printed in 600dpi with the HP LaserJet 500 color M551 printer, and then scanned in 200 dip with HP LaserJet M2727nf scanner. The P&S process always causes image pixel distortion and geometric distortion, because it involves digital-to-analog and analog-to-digital conversion process.

The term “Readable” labels the QR code public message that can be successful read by any standard QR code reader. The term “Decodable” labels the QR code secret message that can be successfully decoded by the special QR code reader.

Although the fidelity of the marked QR code was seriously distorted after suffering from various attacks, the public message of these marked QR codes after the attack still could be read by any standard QR code reader. Moreover, the secret message 1866 could be decoded successfully. It demonstrates that the proposed secret hiding scheme is tolerant to the common attack and practically usable in the real-world applications.

Attack types:	Gaussian noise (M=0, V=0.10)	Salt & pepper noise (d=0.10)	Speckle noise (v=0.10)
Results:			
Public message:	Readable	Readable	Readable
Secret message:	Decodable	Decodable	Decodable
Attack types:	Poisson noise	Gaussian blurring (σ = 1)	Print-and-scan process
Results:			
Public message:	Readable	Readable	Readable
Secret message:	Decodable	Decodable	Decodable

Fig. 8. Results of the marked QR code in **Fig. 6(b)** after image degradation processes

4.3 Comparison and Discussion

At present, QR code is very popular with the development of 4G and the popularity of smart phones. Researchers start to focus on hiding secret data in QR code by applying data

hiding technology to deliver secret message. This research mainly concerns how to improve the secret payload under the condition that keeping the cover QR code readable. The readable meaningful QR code public message will help to reduce the attacker's curiosity. Most of the research exploit the error correction mechanism of QR code to recover the hiding secret message by modifying portion of cover QR code data modules.

Chiang et al.'s scheme treated all the bits of QR code data codewords as a one-dimension matrix, and employed the wet paper codes algorithm to randomly hide the secret message bits in data codewords of the cover QR code within the scope of QR code error correction capacity $c = \lfloor ecc/2 \rfloor$. Here a codeword is equal to eight bits and ecc is the number of error correction codewords. According to the technical specification of QR code, QR code employs Reed-Solomon code to correct the errors when a portion of QR code was defaced or some QR code modules were wrongly decoded. A codeword error always needs two error correction codewords to correct it. For instance, assume we want to encode the string "HELLO WORLD" in alphanumeric mode as the public message with QR code version 1 and error correction level M. The corresponding data codewords encoding results are as follows:

00100000 01011011 00001011 01111000 11010001 01110010 11011100 01001101 01000011 01000000 11101100 00010001 11101100 00010001 11101100 00010001

Converting those binary numbers into decimal codewords, we get

32, 91, 11, 120, 209, 114, 220, 77, 67, 64, 236, 17, 236, 17, 236, 17.

These codewords will be the coefficients of the message polynomial in Reed-Solomon code encoding, then the ten error correction codewords will be generated:

196, 35, 39, 119, 235, 215, 231, 226, 93, 23.

These ten error correction codewords can correct five data codewords errors at maximum. The QR code decoding procedure will fail when there are more than five data codewords errors in the QR code. Chiang et al.'s scheme calculated the error correction capacity $c = \lfloor 10/2 \rfloor = 5$ codewords which was up to 40 bits, the secret bits and authentication stream bits would replace the 40 bits of QR code data codewords by applying the wet paper codes algorithm. However, the wet paper codes algorithm uses probability models of average distribution. These 40 bits would be evenly distributed in the cover QR code data codewords. In the above example, it would lead to more than five data codewords to be modified, which means the QR code decoding procedure would fail because the number of errors is greater than the QR code error correction capacity. Under this secret message concealing strategy, the maximum secret payload of Chiang et al.'s scheme in version 1-M cover QR code would be reduced to 5 bits rather than 40 bits. So the secret payload of Chiang et al.'s scheme will equal to the error correction capacity of cover QR code. According to the specification of QR code, the scope of secret payload of Chiang et

al.'s scheme will be in the range of [2, 1215], which is much less than what they claimed in [7].

Lin and Chen's schemes [11] [13] tried to hide secret message bits by exploiting modification direction, and using LSB matching revisited embedding algorithm. However, these two schemes built a pool which contain all the module pairs at the beginning of secret embedding process, then used a secret key to randomly pick up one or two module pairs from the pool, and embedded the secret bits in these module pairs. The operation is similar to the wet paper codes algorithm mentioned earlier, which embedded the secret bits into the data codewords of cover QR code randomly. These secret bits will be evenly distributed in the data codewords of the cover QR code, this will cause these two schemes to face the same problem as Chiang et al.'s scheme. The number of error codewords in the QR code data codewords would be too many, more than the error correction capacity of QR code, and the QR code decoding process may fail. In order to ensure that those schemes can work, the secret payload will be less than expected. Similar to Chiang et al.'s scheme, the scope of secret payload of Lin and Chen's schemes [11] [13] will be in the range of [2, 1215].

The proposed scheme hides the secret message digits into the data codewords of cover QR code by improving the exploiting modification direction, and produce a new data codewords for marked QR code, then adopts a simple strategy to conceal these new data codewords for the marked QR code, which overwrites the front of continuous data codewords of the cover QR code with in sequence. This strategy ensures that the number of errors are within the scope of error correction capacity of the cover QR code. As shown in **Table 5**, the secret payload of the proposed scheme is in the range of [6, 4860], which is three times more than Chiang et al.'s scheme and Lin and Chen's schemes [11] [13]. **Table 6** shows the comparisons of secret payload between the proposed scheme and the existing work for QR code versions of 1-L, 10-L, 20-M, 30-Q, 40-H.

Table 6. The secret payload of the proposed scheme compared with related schemes

QR code versions	Chiang et al.'s scheme [7]	Lin and Chen's schemes [11] [13]	the proposed scheme
1-L	2	2	6
10-L	48	48	144
20-M	277	277	831
30-Q	800	800	2400
40-H	1215	1215	4860

5. Conclusions

In this paper, a new secret hiding scheme was proposed by investigating the technology of EMD and QR code. The proposed scheme explores the QR code error correction capability to

provide the steganography, robustness and adjustable secret capacity for the secret hiding mechanism. Experiments show that the proposed scheme is feasible, with high level of security, and resistant to common image-processing attacks. For the future work, we will try to investigate the Isomorphic characteristics of the Reed-Solomon code used by QR code technique to improve the secret payload.

References

[1] Denso Wave Inc. "QR Code Standardization," 2003. Article (CrossRef Link).

[2] J. Z. Gao, L. Prakash, and R. Jagatesan, "Understanding 2d-Barcode Technology and Applications in M-Commerce-Design and Implementation of a 2d Barcode Processing Solution," in *Proc. of Computer Software and Applications Conference, 2007. COMPSAC 2007. 31st Annual International*, Vol. 2, pp. 49-56, Aug. 2007. Article (CrossRef Link)

[3] L. Bi, Z. Feng, M. Liu, and W. Wang, "Design and Implementation of the Airline Luggage Inspection System Base on Link Structure of QR Code," in *Proc. of Electronic Commerce and Security, 2008 International Symposium on*, pp. 527-530, 2008. Article (CrossRef Link)

[4] N. Teraura, and K. Sakurai, "Information Hiding in Subcells of a Two-Dimensional Code," in *Proc. of 2012 IEEE 1st Global Conference on Consumer Electronics (GCCE)*, pp. 652-656, Oct. 2012. Article (CrossRef Link)

[5] 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 Transactions on Information Forensics and Security*, Vol. 11, No. 3, pp. 571-583, 2016. Article (CrossRef Link)

[6] I. S. Reed, and G. Solomon, "Polynomial Codes over Certain Finite Fields," *Journal of the Society for Industrial and Applied Mathematics*, Vol. 8, No. 2, pp. 300-304, 1960. Article (CrossRef Link)

[7] Y.-J. Chiang, P.-Y. Lin, R.-Z. Wang, and Y.-H. Chen, "Blind QR Code Steganographic Approach Based Upon Error Correction Capability," *KSII Transactions on Internet & Information Systems*, Vol. 7, No. 10, pp. 2572-2543, 2013. Article (CrossRef Link)

[8] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, "Writing on Wet Paper," *IEEE Transactions on signal processing*, Vol. 53, No. 10, pp. 3923-3935, 2005. Article (CrossRef Link)

[9] T. V. Bui, N. K. Vu, T. T. Nguyen, I. Echizen, and T. D. Nguyen, "Robust Message Hiding for Qr Code," in *Proc. of 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, pp. 520-523, Aug. 2014. Article (CrossRef Link)

[10] P. Elias, "Error-Correcting Codes for List Decoding," *IEEE Transactions on Information Theory*, Vol. 37, No. 1, pp. 5-12, 1991. Article (CrossRef Link)

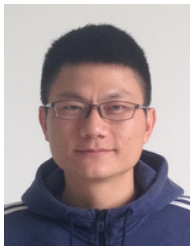
[11] P.-Y. Lin, and Y.-H. Chen, "QR Code Steganography with Secret Payload Enhancement," in *Proc. of 2016 IEEE International Conference on Multimedia & Expo Workshops (ICMEW)*, pp. 1-5, Jul. 2016, Seattle, USA. Article (CrossRef Link)

[12] X. Zhang, and S. Wang, "Efficient Steganographic Embedding by Exploiting Modification Direction," *IEEE Communications Letters*, Vol. 10, No. 11, pp. 781-783, 2006. Article (CrossRef Link)

[13] P.-Y. Lin, and Y.-H. Chen, "High Payload Secret Hiding Technology for QR Codes," *EURASIP Journal on Image and Video Processing*, Vol. 2017, No. 1, pp. 14, 2017. Article (CrossRef Link)

[14] S.-Y. Shen, and L.-H. Huang, "A Data Hiding Scheme Using Pixel Value Differencing and Improving Exploiting Modification Directions," *Computers & Security*, Vol. 48, pp. 131-141, 2015. Article (CrossRef Link)

[15] X.-T. Wang, C.-C. Chang, C.-C. Lin, and M.-C. Li, "A Novel Multi-Group Exploiting Modification Direction Method Based on Switch Map," *Signal Processing*, Vol. 92, No. 6, pp. 1525-1535, 2012. Article (CrossRef Link)



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. 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.

Yan-Jun 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.