Blind QR Code Steganographic Approach Based upon Error Correction Capability

Yin-Jen Chiang[1], Pei-Yu Lin[2], Ran-Zan Wang[1] and Yi-Hui Chen[3]
[1] Department of Computer Science and Engineering, Yuan Ze University
135 Yuan-Tung Rd., Chung-Li 32003, Taiwan
[e-mail: s1006015@mail.yzu.edu.tw, rzwang@saturn.yzu.edu.tw]
[2] Department of Information Communication, Yuan Ze University
135 Yuan-Tung Rd., Chung-Li 32003, Taiwan
[e-mail: pylin@saturn.yzu.edu.tw]
[3] Department of Applied Informatics and Multimedia, Asia University
500 Lioufeng Rd., Wufeng, Taichung 41354, Taiwan
[e-mail: chenyh@asia.edu.tw]
*Corresponding author: Pei-Yu Lin

Received July 14, 2013; revised September 25, 2013; accepted September 21, 2013; published October 29, 2013

Abstract

A novel steganographic QR code algorithm, which not only coveys the secret into the widely-used QR barcode but also preserves the readability of QR content and the capability of error correction, is presented in this article. Different from the conventional applications for QR barcode, the designed algorithm conceals the secret into the QR modules directly by exploiting the error correction capability. General browsers can read the QR content from the QR code via barcode readers; however, only the authorized receiver can further reveal the secret from the QR code directly. The new mechanism can convey a larger secret payload along with adjustment of the QR version and error correction level. Moreover, the blind property allows the receiver to reveal the secret without the knowledge of the embedded position of modules. Experimental results demonstrate that the new algorithm is secure, efficient and feasible for the low-power QR readers and mobile devices.

Keywords: QR barcode, steganography, wet paper code, error correction capability

This research was supported by the National Science Council, Taiwan, under contract No. NSC102-2221-E-155-035-MY3. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

http://dx.doi.org/10.3837/tiis.2013.10.012

1. Introduction

With the widespread use of scanners and mobile devices, barcodes [1-3] provide common applications with clever integration of the Internet and the real world, such as product identification, business transactions and corporate marketing. The barcode forms use one-dimensional (1D) and two-dimensional (2D) symbols. **Table 1** lists the commonly used barcodes. The 1D barcode is composed of different widths of lines and spaces to represent the simple identification of a product. The 2D barcode [4-6] can carry greater storage capacity with various types of content. The error correction ability of the 2D barcode can restore the content if the barcode suffered from becoming dirtied and damaged.

Table 1. The conventional barcodes

One-dimensional barcodes		
Code 128	EAN-13	ISBN
 	 0 346388 000004	 9 780346 388000
Two-dimensional barcodes		
QR code	PDF417	Data Matrix

Barcodes are convenient for automatic systems; nevertheless, there exists a potential risk in security. For a barcode with private content, one can easily reveal the content through the use of barcode readers and mobile devices. To ensure privacy, the content is usually stored in a back-end database. A browser can read the web link via a barcode reader and then connect to the website of a back-end database. The qualified browser with the right access could successfully login to the database and then retrieve the private content [7]. Nevertheless, the web link of the back-end database exposes the secret content to risk and attracts intruders' attention.

Recently, many studies have focused on providing barcode applications. In general, the applications can be classified into three categories: the image hiding [8-11], the watermarking [12-15], and the visual cryptography [7, 16, 17] techniques. The image hiding schemes [8-11] convert the secret to a QR code tag and then embed the secret QR tag into a cover image. These approaches can be regarded as the conventional image hiding technique; however, they are incapable of providing the feasibility of hiding/reading the secret into/from the QR code tag directly.

On the contrary, the watermarking schemes [12, 13, 15] embed the watermark into the QR code image by utilizing the transforms, such as the discrete cosine transform (DCT), discrete wavelet transform (DWT) and discrete Fourier transform (DFT). Nevertheless, the computational load of the transform operation is complex and heavy. Considering the low-power mobile devices and QR readers, the computational complexity of the designed processes should be as low as possible for the mobile device applications.

Different from the conventional hiding and watermarking schemes, Gao and Sun [14] embed the watermark into the width of rows and columns of QR code. The scheme is simple and of low complexity, and can be applied to the low power readers. The watermark could hardly be computed while the width of rows and columns of QR code suffered from distortion. Therefore, to extract the watermark from the distorted QR code, the scheme needs additional bilinear interpolation transform, morphological repair and BCH(15, 5) error correction. Moreover, the embeddable watermark capacity is relatively small.

Based on the observation of the related QR schemes, the proposed mechanism aims to conceal the secret into a QR code directly rather than through the schemes [8-11], and to provide an efficient and feasible secret application for the low-power barcode readers [12, 13, 15]. In order to preserve the original QR content but also carry a larger secret payload than related works, the designed mechanism exploits the QR feature to convey the secret into QR code modules based on the concept of wet paper code [18, 19]. Besides, the proposed blind steganography approach is secure in that the general browsers can read the QR content from the QR code. This leads to reducing the security risk of the secret and only the authorized user can reveal the secret from the QR code directly.

The rest of the article is organized as follows. Section 2 introduces the related works and observations. The proposed blind steganography QR code mechanism is presented in Section 3, followed by the demonstration and performance comparisons are analyzed in Section 4. Finally, conclusions are made in Section 5.

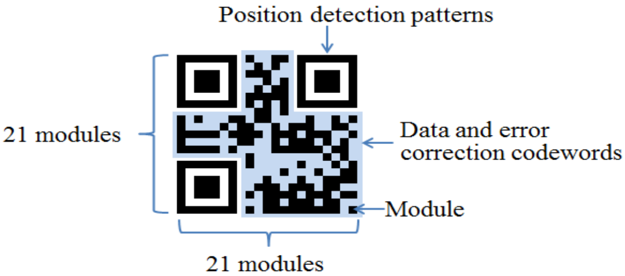

Position detection patterns
21 modules
Data and error correction codewords
Module
21 modules

Fig. 1. QR code with version 1, content: “YZU”

2. Prior Works

The QR code (quick response code) has been widely applied to provide information access via mobile devices. The major structure and error correction of QR code will be briefly introduced in Section 2.1. Additionally, the concept of the adopted WPCs (wet paper codes) will be described in Section 2.2.

2.1 The Technology of QR Code

QR code (quick response code) [4-6] is a type of matrix barcode (two-dimensional barcode) developed by Denso-Wave company in 1994. The content is encoded into binary format and represented as modules (square dots) in the QR code tag. The dark module and white module mean a binary one and zero, respectively. **Fig. 1** depicts an instance of the QR code symbol.

The QR code standard specifies 40 versions, from the smallest 21×21 modules (version 1) up to 177×177 modules (version 40) in size. Each version has four error correction levels (L, M, Q and H) that are user selectable, as listed in **Table 2**. The error correction capability can restore data if the QR code is dirty or damaged [20]. The highest level of error correction used—up to 30% of the data codewords—can be damaged and still be retrieved. Here, a codeword refers to eight modules in a unit that constructs the data area [6].

Table 2. Error correction capability of QR barcode

Error level	Error correction capability, % of codewords (approx.)
L (Low)	7 %
M (Medium)	15 %
Q (Quartile)	25 %
H (High)	30 %

Table 3. Maximum character storage capacity

Version	Error correction		Blocks	QR Content		
	Level	Codewords		Codeword per block	Total Codewords	Total Bits
1	L	7	1	19	19	152
	M	10	1	16	16	128
	Q	13	1	13	13	104
	H	17	1	9	9	72
20	L	224	3 5	107 108	861	6,888
	M	416	3 13	41 42	669	5,352
	Q	600	15 5	24 25	485	3,880
	H	700	15 10	15 16	385	3,080
40	L	750	19 6	118 119	2,956	23,648
	M	1,372	18 31	47 48	2,334	18,672
	Q	2,040	34 34	24 25	1,666	13,328
	H	2,430	20 61	15 16	1,276	10,208

Table 3 lists the maximum data capacity under different error correction levels in versions 1, 20 and 40. The higher the rate of error correction, the more errors can be accommodated, but the data that can be stored is relatively less. According to the different versions of QR code, the stored data will be divided into several blocks. The error correction codeword can be generated corresponding to the individual data blocks for ensuring the capability of error correction. For instance, in version 20-L, there are a total of eight blocks (i.e., 3+5). The storage data will be divided into eight blocks, with three blocks containing 107 data codewords and five blocks containing 108 data codewords (3×107 codewords + 5×108 codewords = 861 data codewords). Also, the total of 224 error correction codewords in QR code will be separated into eight blocks to guarantee the restoration capability for corresponding data blocks.

2.2 Wet Paper Codes (WPCs) Algorithm

The concept of wet paper codes (WPCs) can be regarded as "writing on wet paper" [18, 19]; that is, paper contains some wet regions (unchangeable) and dry regions (changeable). Intuitively, only the dry areas of paper can be written on, while on the contrary, one cannot write on the wet areas of paper. The WPCs thereby solve the problem of writing on paper with wet/dry regions.

Fridrich et al. [18, 19] proposed a steganography algorithm by utilizing the WPCs to embed secret bits into the least significant bit (LSB) of a host image without the pre-shared knowledge of embedding positions between the sender and the receiver. Assume that O is a grayscale host image with n pixels, $O=(p_1, p_2, \ldots, p_n)$ and S is the secret with m bits. All of the pixels in O can be treated as two types: the dry pixels (*changeable*) and the wet pixels (*unchangeable*). To begin, the sender selects k dry pixels in O; that is, there are k dry pixels and $n-k$ wet pixels, $k\subset n$.

Let b be a $1\times n$ vector by consisting of the LSB of all pixels p_i, $b=(b_i \mid b_i=\text{LSB}(p_i), i=1, 2, \ldots, n)$. The secret S is aimed to be embedded into O by modifying b_i with the dry pixels. The dry bit (changeable pixels) b_i can be altered and the wet bit (unchangeable pixels) b_i cannot be changed. The b is modified to b' to comply with (1).

$$Db'^{\mathrm{T}} = S^{\mathrm{T}}, \tag{1}$$

where D is a pseudo-random $m\times n$ binary matrix generated by a secret key and "$^{\mathrm{T}}$" denotes matrix transposition.

The b' can be solved by a linear equation and (1) can be rewritten as

$$DV^{\mathrm{T}} = S^{\mathrm{T}} - Db^{\mathrm{T}}, \tag{2}$$

where V is a $1\times n$ non-zero vector, $V=b'-b$, $V=(v_i \mid v_i =\{0, 1\}, i=1, 2, \ldots, n)$. In (2), k elements v_i in V are unknown and the remaining $n-k$ elements v_i in V are zeros. Hence, the $n-k$ elements of v_i ($v_i = 0$) from V and the corresponding columns from D can be removed. The formula (2) can be reduced and then forms a new equation:

$$D'V'^{\mathrm{T}} = z. \tag{3}$$

The D' is a binary $m\times k$ matrix from D, V' is an unknown $1\times k$ vector from V, and $z = S^{\mathrm{T}} - Db^{\mathrm{T}}$. Finally, the k values of V' can be obtained by computing $\text{INVE}(D')\times z$, where $\text{INVE}(\cdot)$ is denoted as an inverse function. Afterward, the k unknown values of b' can be achieved by $V'+b$ with the corresponding k values.

The stego image O' thereby can be obtained by replacing the LSB of pixels p_i with the modified b_i'. To extract the secret S, an authorized receiver with the secret key can generate the matrix D and then decode S by multiplying D and the LSB of pixels in O' as (1). The advantage of WPCs is that the sender can freely choose the dry elements in O that are not revealed to the receiver or attacker. Without the knowledge of the embedded positions (dry pixels), the authorized receiver still can extract S. Thus, WPCs can satisfy the benefit of public key steganography [18, 19].

Researches [21, 22] have proposed related steganographic methods based on WPCs. However, the linear equations' solvability with a large unknown matrix of WPCs would lead to impractical performance. The computational complexity is relatively heavy in the embedding process. Based on the observations of WPCs, the properties of arbitrary selection positions and unshared knowledge of WPCs are utilized in the proposed mechanism. To reduce the cost of linear equations solvability, the proposed method considers the block structure of QR code. The computational complexity can be reduced. The designed scheme introduced in Section 3 is efficient, practical and fits the requirements for steganographic QR barcode.

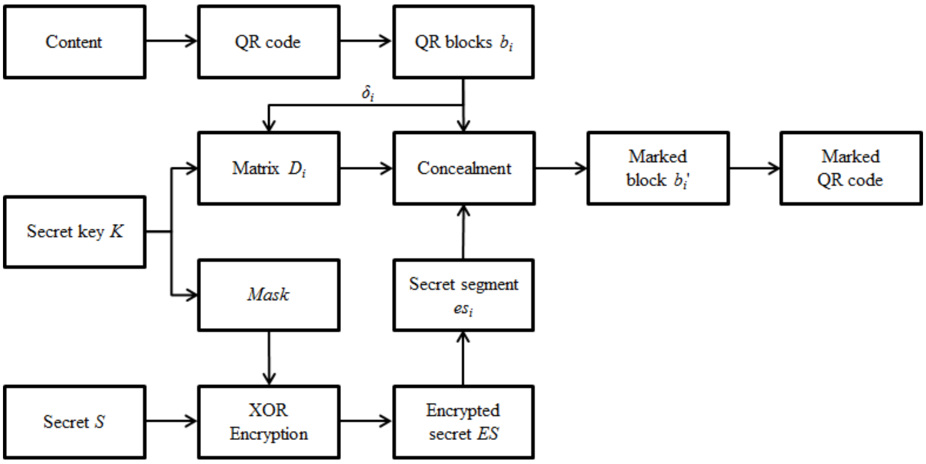


Fig. 2. The architecture of the proposed system

3. The Proposed Scheme

Inspired by the error correction capability of the QR code, this article aims to provide a blind secret communication via the QR code among mobile devices. The feasible application of the proposed scheme for generating the marked QR code and blindly extracting the secret information is discussed below.

3.1 Steganographic QR Code Procedure

Given a cover QR code that is generated with regular content (as depicted in **Fig. 1**) and secret *S*, the proposed scheme can conceal *S* into the cover QR code without degrading the readability of the content. The flowchart of the concealment processes is shown in **Fig. 2**.

Measurement Phase

As mentioned in Section 2.1, the QR code algorithm divides the content into the required number of blocks to enable the error correction algorithms to be processed. Assume that the QR code consists of n blocks $\{b_i\}_{i=1}^{n}$ and the size of block b_i is q modules. Based on the QR code core algorithm, the error correction capacity is less than half the number of error correction codewords. The secret capacity is in accordance with the error correction capacity. For simplicity, let E be the number of error correction codewords. Due to the fact that a codeword consists of eight modules, the maximum embeddable capacity, C, of secret S can be determined as

$$C = \left\lfloor \frac{E}{2} \right\rfloor \times 8 \text{ modules.} \tag{4}$$

In advance and to guarantee the security of the secret, the encrypted result, ES, of S is computed by using the XOR operation as

$$ES = S \oplus Mask, \tag{5}$$

where the *Mask* is a pseudorandom binary stream with length *C* that generated by a random number generator (*RNG*) with a secret key, *K*. The *K* is shared by the sender and the receiver.

To ensure the error correction capability, the *ES* is divided into *n* segments, $ES = \{es_i\}_{i=1}^{n}$. Here, let the length of esi be *p* bits,

$$p = C/n. \tag{6}$$

Each es_i thereby can be embedded into the corresponding block, b_i, by the following concealment phase, i=1, 2, …, *n*.

For instance, for QR version 20-L, as listed in **Table 3**, there are eight blocks in a QR code and the error correction codewords are 224 (that is, E=224). According to (4), we can know that the maximum embeddable capacity of secret $C = \lfloor 224/2 \rfloor \times 8$ =896 modules. The 896 secret modules afterward are divided into eight segments. Each secret segment possesses $p = C/n$ = 896/8 = 112 modules by (6), and can be concealed into the corresponding blocks.

Concealment Phase

Based on the error correction capability of the QR standard, the QR code can resist a certain distortion for the QR data and error correction codewords. As with the property, we conceal the secret into the data and error correction codewords without altering the related position detection patterns for the sake of preserving the restoration of the QR content and the decodability of the QR reader. To avoid distorting the original QR content, the concept of WPCs is utilized. For the sake of convenience, the block, b_i, and secret segment, es_i, are notated as matrix $[b_i]_{1\times q}$ and $[es_i]_{1\times p}$, respectively. Firstly, the sender selects *p* dry modules (changeable elements) in block b_i, $p \subset q$, and the remaining $q–p$ modules of b_i are treated as wet modules (unchangeable elements).

Let the block ID of b_i be δ_i, where each δ_i are mutually exclusive, i=1, 2, …, *n*, and can be assigned by *K*. An $p \times q$ binary matrix D_i is generated by the ID δ_i along with the secret key, *K*,

$$[D_i]_{p\times q} = RNG_K(\delta_i). \tag{7}$$

The dry modules in matrix $[b_i]_{1\times q}$ accordingly can be modified for complying with the following formula,

$$[D_i] \times [b_i']^{\mathrm{T}} = [es_i]^{\mathrm{T}}. \tag{8}$$

The $[b_i]_{1\times q}$ can be rewritten to the marked result $[b_i']_{1\times q}$ based on the linear equations solvability. Note that only the *p* dry modules of $[b_i]_{1\times q}$ can be considered for modification. On the contrary, the $q–p$ wet modules of $[b_i]_{1\times q}$ are unchangeable elements. This can guarantee that, at most, only *p* modules could be altered per block.

In accordance with the *concealment phase* for each block, b_i, and the corresponding secret segment, es_i, i=1, 2, …, *n*, we can obtain *n* marked blocks b_i'. The marked QR code finally can be acquired by consisting of the *n* marked blocks and then communicated/shared to the receiver. From the appearance of the marked QR code, the original QR content still can be preserved. A QR code reader can successfully scan and decode the content from the marked QR code. This helps reduce the attraction of browsers when reading the marked QR code.

For instance, let us simply assume that a block, b_i, has 4 modules (q=4) and the corresponding encrypted secret segment, es_i, is 10 (p=2). First of all, the sender selects two modules of b_i as the dry elements. The matrix, b_i, can be presented as

$$[b_i]^T = \begin{bmatrix} 0 \\ \boxed{1} \\ 0 \\ \boxed{1} \end{bmatrix},$$

where the marked gray elements are denoted as the dry modules, and the rest of the modules are wet. The secret key, *K*, and the block ID, δ_i, are then used to generate a random two-dimensional matrix, $[D_i]_{2\times4}$, by (7),

$$[D_i]_{2\times4} = \begin{bmatrix} 0001 \\ 0100 \end{bmatrix}.$$

By multiplying the matrix $[D_i]$ and $[b_i]$, we have

$$[D_i][b_i]^T = \begin{bmatrix} 0001 \\ 0100 \end{bmatrix} \begin{bmatrix} 0 \\ \boxed{1} \\ 0 \\ \boxed{1} \end{bmatrix}.$$

To comply with (8), the second dry module of $[b_i]$ is changed from “1” to “0”. We can obtain the marked result $[b_i']$ as

$$[D_i][b_i']^T = \begin{bmatrix} 0001 \\ 0100 \end{bmatrix} \begin{bmatrix} 0 \\ \boxed{0} \\ 0 \\ \boxed{1} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = [es_i]^T .$$

3.2 Blind QR Code Extraction Procedure

In the normal scanning conditions, browsers can only decode the content via a QR reader. The authorized receiver, along with secret key, K, not only can extract the content but also can blindly reveal the secret, S, from the marked QR code. The blind extraction allows the authorized receiver to revel the secret without the auxiliary of a host QR code, secret information or other instrument. Besides, based on the advantage of WPCs, the receiver does not need to know the exact embedding positions of the QR code.

For a given marked QR code, the related patterns’ information can be acquired by a QR reader, such as the version and block information. Let there be n blocks $\{b_i'\}_{i=1}^{n}$ in the marked QR code, and the size of b_i' is q modules. Assume that E is the number of error correction codewords corresponding to the marked QR code.

Step 1: Estimate the capacity $C = \left\lfloor \dfrac{E}{2} \right\rfloor \times 8$.

Step 2: Calculate the p value as $p= C/n$.

Step 3: Generate a $p\times q$ pseudo-random binary matrix D_i by the secret key K and the block ID δ_i of b_i',

$$[D_i]_{p\times q} = RNG_K(\delta_i), \tag{9}$$

where PNG_K labeled the random number generator (RNG) with a secret key K.

Step 4: Compute the es_i' by multiplying the D_i and the block b_i',

$$[es_i']^{\mathrm{T}} = [D_i]\times[b_i']^{\mathrm{T}}. \tag{10}$$

Here, the size of es_i' is $p\times1$.

Step 5: Repeat Step 3 and Step 4 for the un-processed blocks, b_j', j=1, 2, …, n and $j \neq i$, until all of the blocks have been processed and then go to step 6.

Step 6: Form the ES' by gathering the secret segments, $ES' = \{es_i'\}_{i=1}^{n}$. Here, the size ES' is $(p\times1)\times n=C$.

Step 7: Create a pseudorandom binary stream, $Mask$, with length C by the random number generator (RNG) with K.

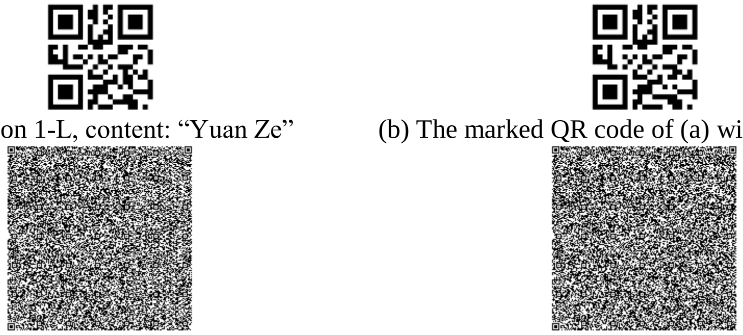
Step 8: Retrieve the secret, *S*, by XOR decryption for the *ES'* and the *Mask*,

$$S = ES' \oplus Mask. \tag{11}$$

The block-based decoding procedure is greatly simplified for implementation and decreased computational complexity. Due to the fact that a QR reader and barcode source library can decode the related format from a QR barcode, the parameters, b_i, n, q, E and C, can be automatically achieved by the QR version and the error correction level of the given QR code. The sender can derive the remaining parameters, *ES*, *Mask*, es_i, p, δ_i and D_i, according to the given secret *S* and key *K*. Hence, the sender and receiver only need to share the key *K*, without auxiliary information. The mechanism with blind extraction process is particularly suitable for the QR code application in mobile devices. Furthermore, the mechanism satisfies the public key steganography purpose and provides secret communication for value-added QR code application. That is, the algorithm can generate specifically-marked QR code to an individual receiver with their private key, *K*, to increase the commercial feasibility of the QR code.

4. Simulation Results and Analysis

In the simulation, the ZXing library with C#.NET language is used to implement the proposed blind QR code steganography mechanism. The ZXing library [23] is an open source library that is often used to read and create a multi-format 1D/2D barcode in varied software development platforms. To evaluate the feasibility of the new approach, two QR codes with Version 1 and Version 40, generated by ZXing, are utilized as the test cover in the simulation. Here, the size of each QR code image is set to 250×250 pixels.



(a) Version 1-L, content: "Yuan Ze"

(b) The marked QR code of (a) with 24 secret bits

(c) Version 40-H, content: "Currently Yuan Ze has five colleges including…"

(d) The marked QR code of (c) with 9,720 secret bits

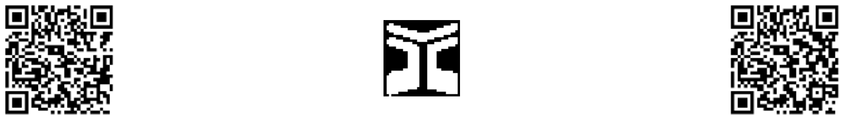
Fig. 3. The results of 1-L and 40-H QR codes

4.1 Applicability

Different types of secret format, including text, binary image and 8-bit color image, are applied to demonstrate the application scenarios. **Fig. 3** exhibits the steganography results of concealing secret text into QR code, Version 1, with error correction level L; and Version 40, with error correction level H. The payloads of secret text are 24 and 9,720 bits, respectively. In the designed algorithm, the embeddable secret capacity is dependent on the version and error correction level of the QR code. From the human eye's perception, the general browsers are senseless with the noise-like two dimensional symbols. They can reveal the QR code content via a QR reader. For example, the browsers can read the content "Yuan Ze" from **Fig. 3**(b); nevertheless, they are incapable of decoding the secret text without the significant key, *K*.

Only the authorized receiver can extract the secret text by decoding and decrypting the marked QR code with *K*. Here, the receiver has no idea about the embedded positions of the marked QR code based on the advantage of WPCs. The designed mechanism offers the blind steganography purpose and reduces the suspicion of browsers.

Aside from the secret text, the sender can select a binary image and an 8-bit color image as the secret form. **Fig. 4** and **Fig. 5** display the marked results of concealing a 16×16 bit binary secret image and a 32×32×8 bit color image into QR codes, respectively. According to the maximum embeddable capacity in (4), the proposed mechanism can dynamically adjust the QR version and error correction level to cope with various sizes of the secret. The higher settings of QR version and error correction level can provide larger secret capacity.

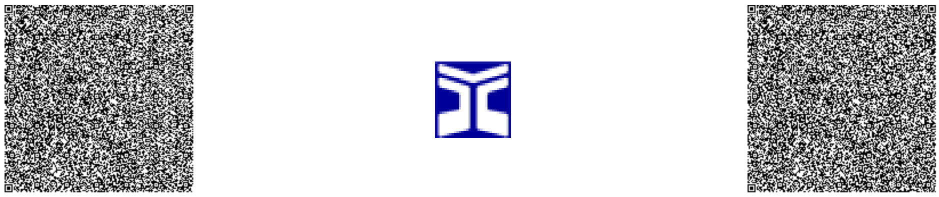


(a) The 4-H QR code

(b) The secret binary image with 16×16 bits

(c) The marked QR code

Fig. 4. The result of 4-H QR code with binary secret image of 256 bits



(a) The 37-H QR code

(b) The secret color image with 32×32×8 bits

(c) The marked QR code

Fig. 5. The result of 37-H QR code with color secret image of 8,192 bits

Table 4. The maximum secret payload, *C*, and the change ratio, *σ*, under different QR versions and error correction levels

Ver.	QR code size (modules)	Error correction level							
		L		M		Q		H	
		C (bits)	*σ* (%)	*C* (bits)	*σ* (%)	*C* (bits)	*σ* (%)	*C* (bits)	*σ* (%)
1	441	24	2.72%	40	4.54%	48	5.44%	64	7.26%
5	1,369	104	3.80%	192	7.01%	288	10.52%	352	12.86%
10	3,249	288	4.43%	520	8.00%	768	11.82%	896	13.79%
15	5,929	528	4.45%	960	8.10%	1,440	12.14%	1,728	14.57%
20	9,409	896	4.76%	1,664	8.84%	2,400	12.75%	2,800	14.88%
25	13,689	1,248	4.56%	2,352	8.59%	3,480	12.71%	4,200	15.34%
30	18,769	1,800	4.80%	3,248	8.65%	4,800	12.79%	5,760	15.34%
35	24,649	2,280	4.62%	4,256	8.63%	6,360	12.90%	7,560	15.34%
40	31,329	3,000	4.79%	5,488	8.76%	8,160	13.02%	9,720	15.51%

Table 4 lists the maximum secret payload of the proposed scheme under different versions and error correction levels of the QR code. For convenience of explanation, we list several versions between the smallest Version 1 (21×21 modules = 441 modules) and the largest Version 40 (177×177 modules = 31,329 modules). Due to the fact that the secret payload, *C*,

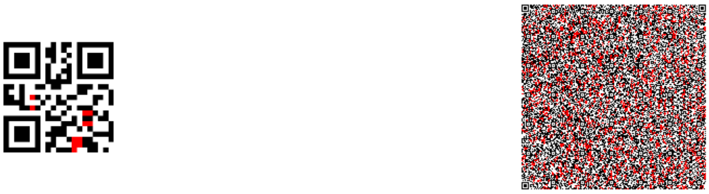
is determined by E in (4), the larger version and error correction level of a QR code we chose, the larger codewords of E we can obtain (as is the case in **Table 3**); hence, the more secret capacity, C, we can hide into a QR code. The designed mechanism takes on the characteristics of the error correction capability of the QR code to achieve the steganography purpose. The minimum and maximum secret payloads are 24 bits and 9,720 bits for versions 1-L and 40-H, respectively.

To evaluate the modified ratio of a marked QR code, the change ratio, σ, is used to ascertain the changed modules of the marked QR code,

$$\sigma = \sum b_{i\_j} \,/\, \text{QR code size}. \tag{12}$$

Here, b_{i_j} stands for the j-th changed module of i-th block, i=1, 2, …, n and $j \subset p$. In general, the amount of the changed modules is half of C, theoretically, as listed in **Table 4**. The theoretical values of σ are 2.72% and 15.51% for the marked 1-L and 40-H QR codes. The practical results of σ are 2.50% and 15.44% for the marked 1-L and 40-H QR codes, as proven in **Fig. 6**. The red dots express the flipped modules, and the corresponding changed modules are 11 and 4,840 modules.

According to the experiments, the designed mechanism alters the half C modules and maintains the remaining half C modules as unchanged for general situations. Thus, the new algorithm not only can preserve the original content of the QR code but also maintains the advantage of half error correction ability theoretically for a marked QR code.



(a) The change ratio: 2.50%, 1-L QR code (b) The change ratio: 15.44%, 40-H QR code

Fig. 6. The change ratio σ for 1-L and 40-H QR codes

4.2 Analysis and Comparison

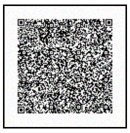
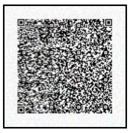
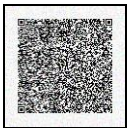
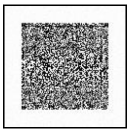
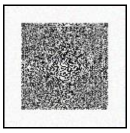
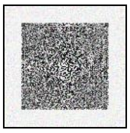
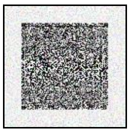
The ability to withstand damage is an important characteristic for the QR code technology. The designed scheme limits the amount of alterable modules by (4) for the sake of guaranteeing the readability of the QR content. Although the modules of the QR code have been changed by the proposed algorithm, the QR content still can be decoded based on the error correction capability. Besides, the marked QR code of the proposed scheme still maintains a portion of error correction capability (as shown in σ) and can be used to resist certain distortions. On the other hand, the new scheme conceals the secret by flipping the QR modules rather than hiding the secret in the pixels of spatial domain [10, 11]; in the coefficients of frequency domain [8, 9, 12, 13, 15]; and in the width of rows and columns of the QR image [14]. Hence, the robustness of the entire modules can be enhanced than that of the related schemes [8-14].

The ability to reveal the QR content and the secret of our designed scheme if the marked QR code suffered from common damages is briefly discussed below.

Noising Addition

The noise is the damage that commonly occurs when QR code is transmitted through the Internet and captured in the real world. To estimate the secret robustness and the QR content readability of the proposed system, the noising attacks, including the Gaussian and the uniform noises, are mounted to the marked QR code. **Table 5** lists the result of adding uniform noise with amounts 5%, 10%, 15% and 20% to the marked QR code, respectively.

Table 5. The revealed results of uniform noising

Uniform Noising	5%	10%	15%	20%
1-L *C*:24 bits				
QR content	readable	readable	readable	readable
Secret	readable	readable	readable	readable
20-H *C*:288 bits				
QR content	readable	readable	readable	readable
Secret	readable	readable	readable	readable
40-H *C*:9,720 bits				
QR content	readable	readable	readable	-
Secret	readable	readable	readable	-

The term "readable" labels data that can be successful decoded. Apparently, the fidelity of marked QR codes is seriously distorted when adding 20% noises; this is especially true for the larger version QR code, which contains high density modules in the same image size. It is obvious that both the QR content and the secret can be extracted for most cases. The designed steganography QR system can work against communication noise for general situations.

Software Rotation Processing

The marked QR code can be successfully scanned in any direction via the QR reader, since the related finder patterns and alignment patterns of the marked QR code have remained unchanged in the proposed algorithm. On the other hand, the image processing software is further adopted to rotate the marked QR code into various angles. In general, the software distorts the image fidelity while rotating the image into 45 and 135 degrees. The modules of a QR code became blurred, especially for the larger QR code version. Hence, the rotation degrees of 45 and 135 by image processing software are a limitation for the general QR code.

Table 6 depicts the 1-L, 10-L and 40-H marked QR code with the rotation degrees of 45, 90, 135 and 270 by image processing software. Both the regular content and the secret can be successfully decoded and read from the upright directions. In the cases of the 45-degree and 135-degree rotations, the modules of 40-H marked QR code are obscured and difficult to decode. Generally speaking, the marked QR code can work against the rotation in much the same way as the functionality of the original QR code.

JPEG 2000 Lossy Compression

A QR code image is usually compressed for the sake of reducing the storage space. The JPEG 2000 lossy compression is mounted to estimate the error correction ability of the marked QR code. **Table 7** displays the compression results of the 1-L and 40-H marked QR code image under various quality factors. As wtih the experiments, the authorized receivers can decode and read both the content and the secret from the compressed QR code. It is obvious that the error correction capability of the marked QR code is practicable and the designed method has sufficient ability to resist the compression attack.

Table 6. The revealed results of the software rotation process

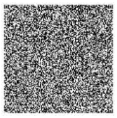
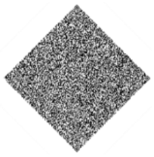
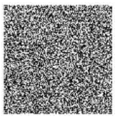
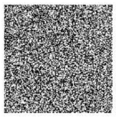
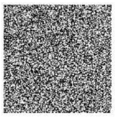
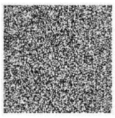
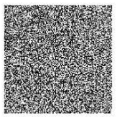
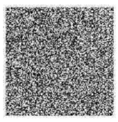
Rotation Degree	45°	90°	135°	270°
1-L *C*:24 bits				
QR content	readable	readable	readable	readable
Secret	readable	readable	readable	readable
10-L *C*:288 bits				
QR content	readable	readable	readable	readable
Secret	readable	readable	readable	readable
40-H *C*:9,720 bits				
QR content	-	readable	-	readable
Secret	-	readable	-	readable

Table 7. The revealed results of JPEG 2000 lossy compression

Quality	100%	80%	60%	20%	1%
1-L *C*:24 bits					
QR content	readable	readable	readable	readable	readable
Secret	readable	readable	readable	readable	readable
40-H *C*:9,720 bits					
QR content	readable	readable	readable	readable	readable
Secret	readable	readable	readable	readable	readable

For a given marked QR code, if an intruder wants to derive the dry modules, the intruder has to try p out of q possible searches for each block via a brute-force attack. Hence, the probability of an intruder successfully learning the embedded positions for a marked QR code is $\left(\begin{matrix} q \\ p \end{matrix}\right)^{n}$. For instance, in the 1-L marked QR code, the q is 26×8 modules (content codewords/block + error correction codewords/block = 19codewords +7codewords) and the p

is 24 modules. The probability of hitting the embedded positions is $\binom{208}{24}$. This shows that the embedded positions are not easily learned.

Table 8. The cryptanalytic attack of the marked QR code

Version	The hitting probability ρ (%)			
	Error correction level			
	L	M	Q	H
1	2^{-24}	2^{-40}	2^{-48}	2^{-64}
5	2^{-104}	2^{-192}	2^{-288}	2^{-352}
10	2^{-288}	2^{-520}	2^{-768}	2^{-896}
15	2^{-528}	2^{-960}	$2^{-1,440}$	$2^{-1,728}$
20	2^{-896}	$2^{-1,664}$	$2^{-2,400}$	$2^{-2,800}$
25	$2^{-1,248}$	$2^{-2,352}$	$2^{-3,480}$	$2^{-4,200}$
30	$2^{-1,800}$	$2^{-3,248}$	$2^{-4,800}$	$2^{-5,760}$
35	$2^{-2,280}$	$2^{-4,256}$	$2^{-6,360}$	$2^{-7,560}$
40	$2^{-3,000}$	$2^{-5,488}$	$2^{-8,160}$	$2^{-9,720}$

Considering the brute-force attack of the encrypted secret stream for a marked QR code, an intruder has to try 2^C possibilities for the secret stream with C bits, as listed in **Table 8**. The hitting probability ρ is from 2^{-24} to $2^{-9,720}$. In addition, an intruder is incapable of identifying the genuine secret information from the 2^C exhaustive results without the knowledge of K. Only the authorized receiver can reveal and decrypt the secret stream by K. The designed scheme is secure against such attacks.

Table 9. Overall comparison between related QR code applications and the proposed method

Methods	[8, 9]	[10, 11]	[12, 13, 15]	[14]	Proposed
Applications	Image hiding	Image hiding	Watermarking	Watermarking	Secret hiding
Embedding domain	Frequency	Spatial	Frequency	Spatial	Spatial
Computational complexity	High	Low	High	Low	Low
Operation upon QR code	No	No	Yes	Yes	Yes
Module-based	No	No	No	No	Yes
Utilizing the QR property	Low	Low	Low	Mid	High
Robustness of secret	Mid	Low	Mid	Low	High
Secret payload	-	-	Limited	Limited	Adaptable, 24~9,720 bits

Table 9 lists the overall comparison between the QR related methods and the proposed scheme. Due to the fact that the QR code is a small image, to embed the secret into a QR code with limited size is inefficient and restricted. Most of articles are designed to embed a secret QR code into a cover image for the image hiding application [8-11], or embed a small watermark into a QR code for protecting the copyright of the QR code [12-15]. To the best of

our knowledge, the secret hiding application of the QR code is limited; the proposed scheme is a novel algorithm to provide the steganography mechanism for conveying the secret information into the QR code directly.

The existing schemes that utilizing the complex image transforms [8, 9, 12, 13, 15] and adjusting the width of rows and columns of QR code [14]. The transform operations of the schemes [8, 9, 12, 13, 15] is complex computation than that of the schemes [10, 11, 14] and the proposed method. Different from existing schemes, the proposed mechanism is based on the characteristic of QR code. The designed mechanism embeds the secret into a QR code by modifying the QR module. This enhances the robustness of the secret when suffering from distortion. The designed scheme can embed the secret payload into a QR code according to the QR version and error correction level. The larger the setting of the QR version and error correction level, the larger secret payload we can embed into a QR code. The designed system is blind, secure, efficient and feasible for low-computation QR readers and mobile devices.

More precisely, Fig. 7 provides the characteristics estimation of the related QR schemes. The magnitudes of the scales (from 0 to 3) are average and concern relative performance evaluation rather than absolute evaluation. The secret payload of image hiding schemes [8-11] is dependent on the size of the cover image and might be relatively large. The image hiding schemes [8-11], the watermarking schemes [12-15] and the proposed secret QR hiding scheme can be targeted for respective applications. In the case of conveying and retrieving the secret upon the QR device, the focus is on decoding efficiency and less deployment cost. The proposed secret hiding scheme that satisfies these essentials can be appropriately utilized in the low-power QR steganography scenario.

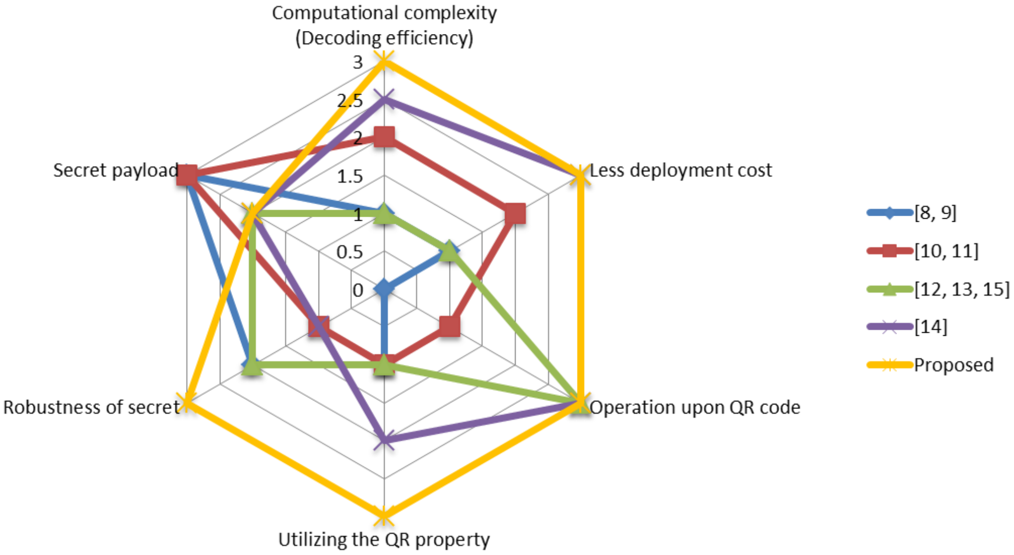


Fig. 7. The characteristics estimation of related QR schemes

5. Conclusion

The designed steganography QR code technique is able to convey about 24-9,720 secret bits into a QR code while preserving the readability of the QR code content and the capability of error correction. Different from the conventional image hiding methods, the new scheme directly embeds the secret into a tiny QR code and exploits the characteristics of the QR code's error correction capability to achieve the steganographic purpose. The general browsers can only read the content via a QR reader. Only the authorized receiver can blind reveal the conveyed secret without the knowledge of the embedded positions (dry pixels). Furthermore, the designed public key steganographic algorithm can generate specifically-marked QR code to an individual receiver with their private, secret key. This provides commercial feasibility for value-added QR code application.

References

[1] T. Sun and D. Zhou "Automatic identification technology — Application of two-dimensional code," in *Proc. of 2011 IEEE International Conference on Automation and Logistics (ICAL)*, pp. 164-168, 2011. Article (CrossRef Link)

[2] D. H. Shin, J. Jung and B. H. Chang, "The psychology behind QR codes: User experience perspective," *Computers in Human Behavior*, vol. 28, no. 4, pp. 1417-1426, 2012. Article (CrossRef Link)

[3] C. Chen, A. C. Kot and H. Yang, "A two-stage quality measure for mobile phone captured 2D barcode images," *Pattern Recognition*, vol. 46, no. 9, pp. 2588-2598, 2013. Article (CrossRef Link)

[4] Psytec QR code editor software, [Online]. Available: http://www.psytec.co.jp/docomo.html

[5] Denso-wave, [Online], Available: http://www.qrcode.com/en/index.html

[6] ISO/IEC 18004, "Information technology Automatic identification and data capture techniques Bar code symbology QR Code," 2000.

[7] J. C. Chuang, Y. C. Hu and H. J. Ko, "A novel secret sharing technique using QR code," *International Journal of Image Processing*, vol. 4, pp.468-475, 2010. Article (CrossRef Link)

[8] C. H. Chung, W. Y. Chen and C. M. Tu, "Image hidden technique using QR-Barcode," in *Proc. of Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2009. Article (CrossRef Link)

[9] W. Y. Chen and J. W. Wang, "Nested image steganography scheme using QR-barcode technique," *Optical Engineering*, vol. 48, no. 5, pp. 057004-01~057004-10, 2009. Article (CrossRef Link)

[10] H. C. Huang, F. C. Chang and W. C. Fang, "Reversible data hiding with histogram-based difference expansion for QR Code applications," *IEEE Transactions on Consumer Electronics*, vol. 57, no. 2, pp. 779-787, 2011. Article (CrossRef Link)

[11] S. Dey, K. Mondal, J. Nath and A. Nath, "Advanced steganography algorithm using randomized intermediate QR host embedded with any encrypted secret message: ASA_QR algorithm," *International Journal of Modern Education and Computer Science*, vol. 6, pp. 59-67, 2012. Article (CrossRef Link)

[12] M. Sun , J. Si and S. Zhang, "Research on embedding and extracting methods for digital watermarks applied to QR code images," *New Zealand Journal of Agricultural Research*, vol. 50, pp. 861-867, 2007. Article (CrossRef Link)

[13] L. Li, R. L. Wang and C. C. Chang, "A digital watermark algorithm for QR code," *International Journal of Intelligent Information Processing*, vo1. 2, no. 2, pp.29-36, 2011. Article (CrossRef Link)

[14] M. Gao and B. Sun, "Blind watermark algorithm based on QR barcode," in *Proc. of Foundations of Intelligent Systems : Proceedings of the Sixth International Conference on Intelligent Systems and Knowledge Engineering*, vol.122, pp. 457-462, 2011. Article (CrossRef Link)

[15] S. Rungraungsilp, M. Ketcham, V. Kosolvijak and S. Vongpradhip, "Data hiding method for QR code based on watermark by compare DCT with DFT domain," in *Proc. of International Conference on Computer and Communication Technologies*, pp. 144-148, 2012.

[16] W. P. Fang, "Offline QR Code authorization based on visual cryptography," in *Proc. of Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp.89-92, 2011. Article (CrossRef Link)

[17] N. Teraura and K. Sakurai, “Information hiding of two-dimensional code by multilayer optical method,” in *Proc. of IEEE 10th International Symposium on Parallel and Distributed Processing with Applications (ISPA)*, pp. 770-777, 2012. Article (CrossRef Link)

[18] J. Fridrich, M. Goljan, P. Lisonˇek and D. Soukal, “Writing on wet paper,” *IEEE Transactions on Signal Processing*, vol. 53, no. 10, pp. 3923-3935, 2005. Article (CrossRef Link)

[19] J. Fridrich, M. Goljan and D. Soukal, “Wet paper codes with improved embedding efficiency,” *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 1, pp. 102-110, 2006. Article (CrossRef Link)

[20] 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)

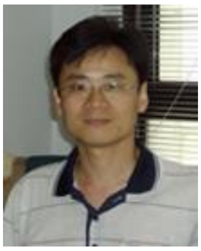
[21] C. C. Chang and Y. C. Chou, “A fragile digital image authentication scheme inspired by wet paper codes,” *Fundamenta Informaticae*, vol. 90, no. 1-2, pp. 17-26, 2009. Article (CrossRef Link)

[22] W. Zhang and X. Zhu, “Improving the Embedding Efficiency of Wet Paper Codes by Paper Folding,” *IEEE Signal Processing Letters*, vol. 16, no. 9, pp. 794-797, 2009. Article (CrossRef Link)

[23] ZXing ("Zebra Crossing"), [Online], Available: http://code.google.com/p/zxing/

Yin-Jen Chiang received the BS degree in computer science and information engineering in 2011 from Chung Hua University, Taiwan. She is currently pursuing her MS degree at the Department of Computer Science and Engineering, Yuan Ze University, Taoyuan, Taiwan. Her research interests include data hiding, secret sharing and image processing.

Pei-Yu Lin received the M.S. and Ph.D. degrees in computer science and information engineering from National Chung Cheng University, Chiayi, Taiwan, in 2004 and 2009, respectively. Since 2009, she has been an Assistant Professor in the Department of Information communication at Yuan Ze University, Chung-Li, Taiwan. Her current research interests include digital watermarking, image protection, data mining and information security.



Ran-Zan Wang received his BS degree in computer science and engineering in 1994 and his MS degree in electrical engineering and computer science in 1996, both from Yuan-Ze University, Taiwan. In 2001, he received a PhD degree in computer and information science from National Chiao Tung University, Hsinchu, Taiwan. He is currently an associate professor in the Department of Computer Science and Engineering at Yuan Ze University, Taiwan. His recent research interests include media security, image processing, and pattern recognition. He is a member of Phi Tau Phi.

Yi-Hui Chen received B.S. and M.S. degrees in information management from the Chaoyang University of Technology in 2001 and 2004, respectively. In 2009, she earned her Ph.D. degree in computer science and information engineering at the National Chung Cheng University. From 2009 to 2010, she worked with Academia Sinica as a post-doctoral fellow. Later, she worked at IBM’s Taiwan Collaboratory Research Center as a Research Scientist. She is now an assistant professor with the Department of Applied Informatics and Multimedia, Asia University. Her research interests include image processing, watermarking, steganography, and XML techniques.