

Distributed Secret Sharing Approach With Cheater Prevention Based on QR Code

Pei-Yu Lin, *Member, IEEE*

Abstract—QR barcodes are used extensively due to their beneficial properties, including small tag, large data capacity, reliability, and high-speed scanning. However, the private data of the QR barcode lacks adequate security protection. In this article, we design a secret QR sharing approach to protect the private QR data with a secure and reliable distributed system. The proposed approach differs from related QR code schemes in which it uses the QR characteristics to achieve secret sharing and can resist the print-and-scan operation. The secret can be split and conveyed with QR tags in the distribution application, and the system can retrieve the lossless secret when authorized participants cooperate. General browsers can read the original data from the marked QR tag via a barcode reader, and this helps reduce the security risk of the secret. Based on our experiments, the new approach is feasible and provides content readability, cheater detectability, and an adjustable secret payload of the QR barcode.

Index Terms—Cheater prevention, error correction capability, QR barcode, secret sharing.

I. INTRODUCTION

COMPARED with a one-dimensional (1-D) barcode, the two-dimensional (2-D) QR barcode [1]–[3] can store a larger data payload and possesses the capability of correcting errors. The barcode data easily can be decoded and retrieved via an automatic barcode system. However, the lack of security of the barcode with private data creates problems for its real-world application.

In general, to protect the privacy of the barcode data, the data normally are stored in a back-end database, and the barcode shows the web link for the database. Only a browser with the right access can log into the database and obtain the private data [4]. However, the web link of the back-end database creates a potential risk in which it may attract the intruder's attention. Chuang *et al.* [4] proposed a secret sharing scheme for the QR tag to protect the secret barcode data. Unfortunately, the content of the QR tags is meaningless, and the shares can be easily obtained by scanning the QR tags with a barcode reader. The sharing scheme is also incapable of preventing cheaters in its real-world application.

Manuscript received December 11, 2014; revised November 10, 2015; accepted December 18, 2015. Date of publication January 01, 2016; date of current version February 02, 2016. This work was supported by the National Science Council, Taiwan, under contract NSC 102-2221-E-155-035-MY3 and MOST 104-3115-E-155-002. Paper no. TII-14-1372.

The author is with the Department of Information Communication, and the Innovation Center for Big Data and Digital Convergence, Yuan Ze University, Taoyuan, Taiwan (e-mail: pagelin3@gmail.com).

Color versions of one or more of the figures in this paper are available online at <http://ieeexplore.ieee.org>.

Digital Object Identifier 10.1109/TII.2015.2514097

A reliable distributed secret storage system with the QR code can be used in significant applications, such as offering secret management and authorization in e-commerce. Based on our observations, our aim was to design a distributed secret sharing system based on the QR barcode, thereby allowing a secret to be split into pieces and shared among individual QR-tag owners to ensure the privacy of the QR data. The secret data can be revealed when qualified QR-tag owners cooperate.

Recently, most QR-related research [5]–[11] has used the traditional image hiding manner or the traditional watermarking technique without utilizing the characteristics of the QR barcode. The image hiding schemes treat the QR tag as a secret image and then embed the QR image into the special domain [5], [6] or the frequency domain [7], [8] of a cover image. Hence, the secret payload of such schemes [5]–[8] is equal to the QR data. These schemes do not operate on the QR tag directly, so they are incapable of allowing the practice of hiding/reading the secret into/from the QR code directly.

Watermarking schemes [9]–[11] embed a watermark into the frequency domain of a QR image with discrete wavelet transform (DWT), discrete cosine transform (DCT), and discrete Fourier transform (DFT) to protect the copyright of a QR image. The maximum payload of a watermark depends on the size of the QR image. The computational load of the transform operations of schemes [7]–[11] is more complex and heavier than that of the schemes themselves [4]–[6], [12]. Considering low-power barcode devices, the computational complexity of the QR code scheme should be minimized.

Avoiding the conventional schemes, Gao and Sun [12] embedded the watermark into the QR tag by directly adjusting the widths of the rows and columns of the QR module. Nevertheless, the embeddable payload of the watermark was less than that of the related schemes [9]–[11] due to the limitation of the adjustable widths of the rows and columns of the QR modules. The scheme presented in [12] was also incapable of extracting the correct watermark when the widths of the rows and columns of the QR modules were distorted. The result was that the scheme required an additional bilinear interpolation transform, morphological repair and (15, 5) Bose-Chaudhuri-Hocquenghem (BCH) code error correction to help extract the watermark from the distorted QR tag.

The related schemes [4]–[11], however, do not consider and use the characteristics of the QR barcode. The error correction capability of the QR code allows the barcode reader to retrieve the data correctly if portions of the barcode are damaged. In exploring the error correction capability of the QR technique, we designed an efficient and feasible secret QR sharing system to protect the private QR data in real-world applications.

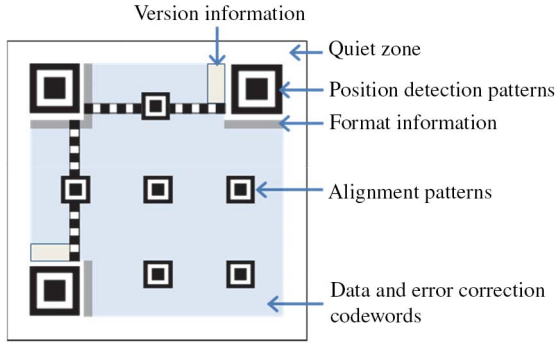


Fig. 1. Basic structure of a QR barcode.

The new system modifies the QR modules directly and can satisfy the essentials of steganography, readability, robustness, security, low computational complexity and feasibility for distributed QR application. To prevent dishonest participants from obtaining the data, the designed sharing scheme can verify cheaters before revealing the shared secret. The generated QR tag can achieve more satisfactory robustness than related QR schemes [9]–[12]. Note that our scheme is not limited to the QR code, because it can be applied to the related 2-D barcodes with error correction capability, such as the PDF417 and data matrix codes.

This paper is organized as follows. Section II introduces the QR barcode technique. The proposed secret QR sharing mechanism is presented in Section III. The sharing simulation and performance comparisons are analyzed in Section IV. Our conclusion is presented in Section V.

II. TECHNOLOGY OF QR BARCODE

The QR barcode (quick response code) is an extensively used 2-D matrix representation that was developed by the Japanese Denso-Wave Company in 1994 [1]–[3]. A QR barcode is constructed of square modules with white and black square dots that represent the digits zero and one. Fig. 1 shows the basic structure of the QR tag, such as the position detection patterns, alignment patterns, format information, version information, and the data and correction codewords. The QR modules are surrounded by a blank, quiet-zone border.

The QR code standard [1] provides 40 QR versions to carry various data payloads. The larger QR version can offer higher data payload. Another significant property of the QR technique is its reliability, which allows the barcode reader to recover data correctly even if portions of the barcode are dirty or damaged. To achieve reliability, the QR code standard offers four error correction levels, i.e., L, M, Q, and H for each QR versions, as listed in Table I. For instance, level H can tolerate approximately 30% of misdecodes or substitution errors in the data and error correction codewords. Here, the codeword is a unit in the QR tag that is equal to eight modules.

Table II briefly presents the data payload and the reliability of various QR versions and error correction levels of the QR standard. According to the QR version and error correction level, the data codewords in the QR tag are segmented and stored into one or more blocks. For instance, the data in QR version 1-L are 152 bits (19 data codewords \times 8 modules)

TABLE I
RELIABILITY OF THE QR BARCODE

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

TABLE II
MAXIMUM CHARACTER STORAGE CAPACITY

Version	Error correction level	Number of error correction codewords	Number of error correction blocks	Number of data codewords per block	Number of data codewords	Number of data 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	6888
	M	416	3 13	41 42	669	5352
	Q	600	15 5	24 25	485	3880
	H	700	15 10	15 16	385	3080
40	L	750	19 6	118 119	2 956	23 648
	M	1372	18 31	47 48	2 334	18 672
	Q	2040	34 34	24 25	1 666	13 328
	H	2430	20 61	15 16	1 276	10 208

and are stored in one block. The data in QR version 40-L are 23 648 bits (2956 data codewords \times 8 modules) and are segmented and stored in 25 blocks (19 + 6), i.e., 19 blocks each of which contains 118 data codewords and six blocks each of which contains 119 data codewords. Then, the error correction codewords that correspond to the data codewords of each block are generated to ensure the error correction capability of the block data.

Obviously, the larger QR version and error correction level can offer higher data payload and reliability. To design an efficient and feasible application for the QR barcode, the proposed scheme exploits the adjustable capacity and error correction feature to achieve readability and secret sharing on QR modules directly.

III. SECRET (N, N) -THRESHOLD QR CODE SHARING APPROACH

Based on the properties of the QR technique, the new scheme designs an (n, n) -threshold sharing system so that the privacy of a secret is provided, making it unavailable to a cheater. In the (n, n) -threshold sharing system, a dealer and n participants exist, where $n \geq 2$. The dealer is responsible for splitting the secret into n marked QR tags, as outlined in Section III-A. Afterward, the n marked QR tags can be distributed to the n corresponding participants. Only the n participants with

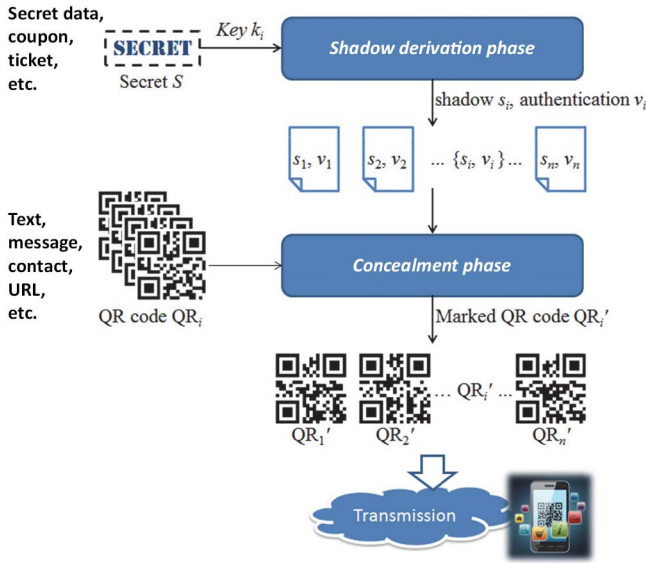


Fig. 2. Architecture of the proposed system.

authorized QR tags are qualified to obtain the shared secret, and no subset of less than n tags can leak any information about the secret (as shown in Section III-B).

The proposed secret sharing with QR code can be applied for value-added barcode applications, such as the distributed secret sharing, e-coupon, and e-ticket. Fig. 2 shows the architecture of the proposed system.

A. Secret Sharing Procedure

Assume that QR_i are the n covers of QR barcodes with the same QR version and error correction level, $i = 1, 2, \dots, n$, and the data of QR_i can be different. That is, the barcode reader can scan and decode diverse data from QR_i . Let S be the private QR data to be protected.

1) Preliminary Phase: According to the QR code core architecture of QR_i , let the number of blocks be b and the number of error correction codewords be E . To share the secret S with cheater detectability, an authentication code V is used to verify the involved participants. Based on the observation of the QR algorithm, the error correction capability is less than half of the number of error correction codewords. Accordingly, the new scheme determines the payloads of S and V dynamically, along with the QR version and the error correction level, as follows.

Step 1) Calculate the value of modifiable capacity C for the given QR barcode as

$$C = \lfloor E/2 \rfloor \times 8 \quad (1)$$

where E is the number of error correction codewords.

Step 2) Evaluate the length of the authentication code V , l_v , according to the QR version and the number of blocks b

$$l_v = (1 + \lfloor \alpha \times \text{QR version} \rfloor) \times b \quad (2)$$

where the parameter α is the strength of cheater detectability. The value of α is a real number that can be adjusted by the dealer, where $0 \leq \alpha < \frac{(C/b)-1}{\text{QR version}}$.

Step 3) Estimate the length of secret S , l_s by

$$l_s = C - l_v. \quad (3)$$

With the preliminary phase, the payloads of secret and authentication code can be learned according to the version and the error correction level of the given QR barcode. This can guarantee that the new algorithm can limit distortion and preserve the readability of the QR content.

For instance, given a QR barcode with version 20-L, as listed in Table II, there are eight blocks in the 20-L QR barcode (i.e., $b = 8$) and the number of error correction codewords E is 224. Hence, the modifiable capacity C equals to $C = \lfloor 224/2 \rfloor \times 8 = 896$ modules. The length of V is $l_v = (1 + \lfloor 0.5 \times 20 \rfloor) \times 8 = 88$ bits, where $\alpha = 0.5$. According to the values of C and l_v , the capacity of S can be derived as $l_s = 896 - 88 = 808$ bits.

2) Shadow Derivation Phase: To derive the secret shadows from S and V , first, the dealer assigns n secret keys k_i for the n corresponding participants $i = 1, 2, \dots, n$. The process of shadow generation is described as follows.

Step 1) Derive the master key K by the participants' secret keys

$$K = \sum_{i=1}^n k_i. \quad (4)$$

Step 2) Generate n authentication streams v_i and the length of v_i is l_v

$$v_i = H_K(k_i), \quad i = 1, 2, \dots, n \quad (5)$$

where $H_K(\cdot)$ is a one-way hash function [13] with the master key K .

Step 3) Generate $(n-1)$ random binary shadows s_1, s_2, \dots, s_{n-1} , with each having the length of l_s .

Step 4) Derive the n th binary shadow s_n with length l_s by the shadows s_1, s_2, \dots, s_{n-1} and the secret S

$$s_n = s_1 \oplus s_2 \oplus \dots \oplus s_{n-1} \oplus S \quad (6)$$

where \oplus denotes the bit stream exclusive-or (XOR) operation.

Hereafter, the dealer can learn n shadows s_i and authentication streams v_i , $i = 1, 2, \dots, n$.

3) Concealment Phase: With exploring the QR code core algorithm, the new coding scheme conceals the (s_i, v_i) within the modules of the data codewords of QR_i only, leaving all other modules of the QR code unchanged.

For the given QR_i , let m be the modules of the QR data codewords and l_m be the length of m . Here, l_m equals the QR data codewords multiplied by eight modules. (A codeword refers to eight modules [1].) For instance, there are 861 QR data codewords in QR version 20-L. Hence, $l_m = 861 \times 8 = 6888$ modules.

Afterward, the (s_i, v_i) are concealed into portions of the m modules of QR_i , $i = 1, 2, \dots, n$, by applying the wet paper codes (WPCs) algorithm [14]. The process is described as follows.

- Step 1) Treat the m modules of the data codewords in QR_i as matrix M_i with the size of $l_m \times 1$.
- Step 2) Select the number of l_s modules in M_i randomly as dry elements, and the remaining number of $(l_m - l_s)$ modules are treated as wet elements $i = 1, 2, \dots, n$. Note that the number of l_s modules is selected evenly from the b blocks to preserve the error correction capability of each block of QR_i , i.e., l_s/b modules are picked up from each block. For instance, if we let $l_s = 808$ and $l_m = 6888$, we thereby select 808 modules randomly as dry elements from the 6888 QR data modules.
- Step 3) Generate the binary matrix D_i with size $l_s \times l_m$ by the key $k_i, i = 1, 2, \dots, n$

$$[D_i]_{l_s \times l_m} = \text{RNG}(k_i) \quad (7)$$

where $\text{RNG}(k_i)$ is a random number generator using the key k_i as the initial seed.

- Step 4) Adjust the l_s dry elements from M_i to M'_i by complying with the following formula:

$$[D_i]_{l_s \times l_m} \times [M'_i]_{l_m \times 1} = [s_i]_{l_s \times 1} \quad (8)$$

where the matrix $[s_i]$ is formed by the shadow s_i with size $l_s \times 1, i = 1, 2, \dots, n$. The modified result $[M'_i]$ can be derived by rewriting or retaining the l_s dry elements in $[M_i]$ based on the solvability of the linear equations.

- Step 5) Regard the l_s modules of M'_i in Step 4 as wet elements, and then select l_v modules randomly from the remaining $(l_m - l_s)$ modules in M'_i as dry elements. Subsequently, the remaining modules $(l_m - l_s - l_v)$ are regarded as wet elements, $i = 1, 2, \dots, n$. Note that the l_v modules also are selected evenly from the b blocks, i.e., l_v/b modules are picked up from each block.
- Step 6) Generate binary matrix D'_i with size $l_v \times l_m$ by the master key K and $k_i, i = 1, 2, \dots, n$

$$[D'_i]_{l_v \times l_m} = \text{RNG}_K(k_i) \quad (9)$$

where $\text{RNG}_K(k_i)$ is a random number generator with the master key K and using the key k_i as the initial seed.

- Step 7) Modify the l_v dry elements in M'_i with symbols M''_i to comply with the formula

$$[D'_i]_{l_v \times l_m} \times [M''_i]_{l_m \times 1} = [v_i]_{l_v \times 1} \quad (10)$$

where the matrix $[v_i]$ is the authentication stream v_i with size $l_v \times 1$. $[M'_i]$ can be rewritten to the modified result $[M''_i]$ based on the solvability of the linear equations.

- Step 8) Learn the marked QR code QR'_i by replacing the m modules in the data codewords of QR_i with the m elements of the results $M''_i, i = 1, 2, \dots, n$.

Subsequently, the marked QR code QR'_i along with the key k_i can be shared and distributed to the involved i th participants $i = 1, 2, \dots, n$.

As we expected, the marked results M'_i of the first level concealment in Step 4 can guarantee that, at most, only l_s modules could be changed. Furthermore, the second level concealment in Step 7 also ensures that, at most, l_v modules could be altered in M''_i . That is, the designed algorithm can limit the distortion within C modules of the given QR code. This leads to the barcode readers being able to scan and decode the data from M''_i successfully. The extracted meaningful QR data help reduce the suspicion of general QR users while they are scanning the QR code. Moreover, browsers and the involved participants are incapable of decoding and extracting the shared secret without sufficient QR'_i and keys.

B. Secret Revealing Procedure

In real-world applications, the capability of detecting cheaters is a significant requirement before the secret data are revealed. In the proposed (n, n) -threshold sharing approach, only sufficient participants with the n -validated QR tags and keys can cooperate to reveal the shared secret. The designed approach can detect dishonest participants and identify who the cheaters are. In addition, the revealing procedure of the proposed scheme is blind, i.e., the authorized participants can extract the secret without the host QR barcode and additional information.

Assume that \overline{QR}_i and \bar{k}_i are the n -provided QR barcodes and keys, respectively, from the involved participants, $i = 1, 2, \dots, n$. By utilizing a barcode reader, the information of the QR version, the error correction level and the related formats can be recognized from \overline{QR}_i immediately. Let E be the number of error correction codewords, and let b be the number of blocks. The detection of cheaters and the extraction of the secret S can be performed by the following phases:

1) Estimation Phase:

- Step 1) Calculate the values of C and m according to the QR barcode core by the definitions, $C = \lfloor E/2 \rfloor \times 8$ and $m = \text{QR data codewords} \times 8$.

- Step 2) Estimate the value of l_v according to the QR version, the number of blocks, and the preshared parameter α

$$l_v = (1 + \lfloor \alpha \times \text{QR version} \rfloor) \times b. \quad (11)$$

- Step 3) Evaluate the value of l_s by

$$l_s = C - l_v. \quad (12)$$

- Step 4) Generate a master key \bar{K} by $\bar{K} = \sum_{i=1}^n \bar{k}_i$.

- Step 5) Reproduce the n authentication streams, \bar{v}_i , each with length l_v by the formula

$$\bar{v}_i = H_{\bar{K}}(\bar{k}_i), i = 1, 2, \dots, n \quad (13)$$

where $H_{\bar{K}}(\cdot)$ is a one-way hash function with the master key \bar{K} .

2) Cheater Identification Phase:

- Step 1) Generate n binary matrixes \bar{D}_i with size $l_v \times l_m$ by $\bar{k}_i, i = 1, 2, \dots, n$

$$[\bar{D}_i]_{l_v \times l_m} = \text{RNG}_K(\bar{k}_i) \quad (14)$$

where $\text{RNG}_K(\bar{k}_i)$ is a random number generator with the master key K , and \bar{k}_i is used as the initial seed.

Step 2) Regard the m modules in the QR data codewords of $\overline{\text{QR}}_i$ as a matrix \bar{M}_i with size $l_m \times 1$, $i = 1, 2, \dots, n$.

Step 3) Obtain the authentication results \bar{v}'_i , according to the formula

$$[\bar{v}'_i] = [\bar{D}_i]_{lv \times lm} \times [\bar{M}_i]_{lm \times 1}, \quad i = 1, 2, \dots, n. \quad (15)$$

Step 4) Verify the genuineness of the provided $\overline{\text{QR}}_i$ and \bar{k}_i by comparing \bar{v}'_i with \bar{v}_i , $i = 1, 2, \dots, n$. If \bar{v}'_i differs from \bar{v}_i , the $\overline{\text{QR}}_i$ is indicated as “tampered” for the i th participant, and the secret revealing procedure will be terminated. Otherwise, if \bar{v}'_i is equal to \bar{v}_i , $i = 1, 2, \dots, n$, the provided QR barcodes and keys are regarded as “validated,” and the secret retrieval phase can be performed in the next process.

3) Secret Retrieval Phase:

Step 1) Construct n binary matrixes \bar{D}'_i with size $l_s \times l_m$ by the key \bar{k}_i , $[\bar{D}'_i]_{ls \times lm} = \text{RNG}(\bar{k}_i)$, $i = 1, 2, \dots, n$, where $\text{RNG}(\bar{k}_i)$ is a random number generator using the key \bar{k}_i as the initial seed.

Step 2) Derive n shadow matrixes $[\bar{s}_i]$, $i = 1, 2, \dots, n$, by performing the binary multiplication as

$$[\bar{s}_i] = [\bar{D}'_i]_{ls \times lm} \times [\bar{M}_i]_{lm \times 1}. \quad (16)$$

Step 3) Compute the secret matrix \bar{S} with the length of $l_s \times 1$

$$\bar{S} = \bar{s}_1 \oplus \bar{s}_2 \oplus \dots \oplus \bar{s}_n. \quad (17)$$

The authenticated participants eventually can disclose the original secret S by regarding the 2-D matrix \bar{S} to 1-D bit stream.

IV. SIMULATION RESULTS AND ANALYSIS

To evaluate the applicability of the proposed scheme, the open source library, ZXing library [15], with C#.NET language was used to generate and decode the multifunction barcode for cross-platform development. The smallest version, 1-L (version 1, error correction level L), and the largest version, 40-H (version 40, error correction level H), are selected as the cover QR barcodes. The size of the generated QR barcode by ZXing is set to 250×250 pixels.

A. Practicability of the Secret QR Sharing

Figs. 3 and 4 show the results of the new scheme for the 1-L and 40-H QR versions in the (3, 3)-threshold sharing system. Note that the designed approach can be applied to the (n, n) -threshold sharing system, while $2 \leq n$. Based on the QR core algorithm, the maximum payload of the data for the 1-L version is 152 bits. Fig. 3(a)–(c) shows the normal 1-L QR barcodes with the data “Yuan Ze,” “YZU IC,” and “info.com,” respectively. With $\alpha = 0.1$, the new approach can conceal 23 secret bits and one authentication bit into the 1-L QR barcode. The

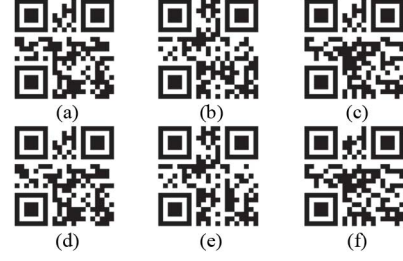


Fig. 3. (3, 3)-threshold sharing of the proposed method for QR version 1-L. (a) Cover QR code 1. (b) Cover QR code 2. (c) Cover QR code 3. (d) Marked QR code of (a). (e) Marked QR code of (b). (f) Marked QR code of (c).

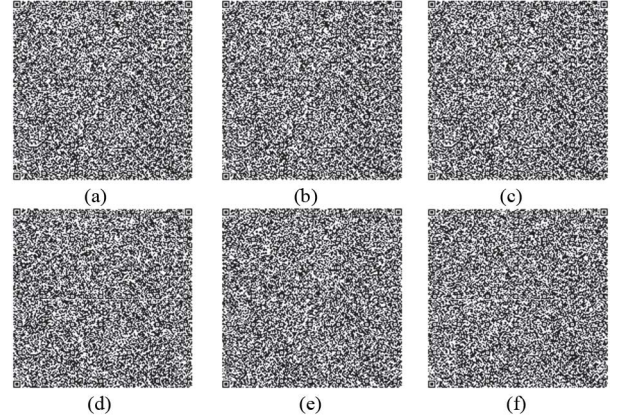


Fig. 4. (3, 3)-threshold sharing of the proposed method for QR version 40-H. (a) Cover QR code 1. (b) Cover QR code 2. (c) Cover QR code 3. (d) Marked QR code of (a). (e) Marked QR code of (b). (f) Marked QR code of (c).

corresponding marked QR codes are listed in Fig. 3(d)–(f). The marked QR barcodes, along with the keys, can be shared and distributed to the individual participants.

Because the QR barcode consists of noise-like symbols, the modification of the marked QR barcode cannot be discerned by the human eyes. With a barcode reader, general browsers can scan and read the QR data from the marked QR code. That is, general browsers can read the content “Yuan Ze” from Fig. 3(d). The meaningful content help reduce the suspicion of the marked QR code from the general QR users. However, general browsers and the involved participants are incapable of extracting the shared secret without sufficient and validated QR barcodes with keys.

Fig. 4(a)–(c) shows the original 40-H QR barcodes with different data (up to 10 208 bits). According to the proposed secret sharing procedure, the new approach can share 9315 secret bits and 405 authentication bits (here, $\alpha = 0.1$) into the QR codes and form the corresponding marked QR codes, as shown in Fig. 4(d)–(f). Considering the readability of the marked QR code, the designed algorithm can satisfy the essentials of steganography and readability by exploring the characteristics of the error correction capability of the QR tag.

The detection and identification of cheaters are essential to prevent fraudulent participants before revealing the secret in the sharing system. According to the cheater identification phase in Section III-B, the involved participants can verify both the provided keys and the marked QR codes with each other.

TABLE III
PAYLOADS OF AUTHENTICATION CODE AND SECRET OF THE MARKED QR BARCODE FOR DIFFERENT α VALUES

Version	α	Error correction levels							
		L (7%)		M (15%)		Q (25%)		H (30%)	
		Authentication (bit)	Secret (bit)	Authentication (bit)	Secret (bit)	Authentication (bit)	Secret (bit)	Authentication (bit)	Secret (bit)
1	0.1	1	23	1	39	1	47	1	63
	1	2	22	2	38	2	46	2	62
5	0.1	1	103	2	190	4	284	4	348
	1	6	98	12	180	24	264	24	328
10	0.1	8	280	10	510	16	752	16	880
	1	44	244	55	465	88	680	88	808
15	0.1	12	516	20	940	24	1416	36	1692
	1	96	432	160	800	192	1248	288	1440
20	0.1	24	872	48	1616	60	2340	75	2725
	1	168	728	336	1328	420	1980	525	2275
25	0.1	36	1212	63	2289	87	3393	105	4095
	1.0	312	936	546	1806	754	2726	910	3290
30	0.1	60	1740	116	3132	160	4640	192	5568
	1	465	1335	899	2349	1240	3560	1488	4272
35	0.1	76	2204	152	4104	212	6148	252	7308
	1	684	1596	1368	2888	1908	4452	2268	5292
40	0.1	125	2875	245	5243	340	7820	405	9315
	1	1025	1975	2009	3479	2788	5372	3321	6399




Without the genuine keys, the derived authentication codes are distinct from the original ones at Step 4 and Step 5 in the estimation phase. In the cheater identification phase, Step 4 can validate the provided QR codes without revealing the secret shadows. Once the provided keys and QR tags are regarded as “validated,” the authenticated participants are allowed to perform the secret retrieval phase.

In order to demonstrate the secret capacity and cheater detectability, Table III lists the amounts of the shared secret and the authentication code for different values of α . The modifiable capacity C is determined by the number of error correction codewords in (1). That is, the higher settings of the QR version and error correction level provide larger capacity for the secret. To cope with the shared secret payload and detectability, the designed scheme can select an adequate QR version and error correction level dynamically to derive the marked QR codes. The maximum secret payload could be 24 to 9720 bits for QR versions 1-L to 40-H, while $\alpha = 0$.

Considering cheater detection, the value of α can be increased to enhance detectability. In the designed system, the scheme offers $(1 + \lfloor \alpha \times \text{QR version} \rfloor)$ authentication bits for each QR block in (2). That is, the new scheme can validate the genuineness of the marked QR code by justifying each QR block. As the definition in (2), there is at least one authentication bit per block for the lower QR version. For the higher QR version, i.e., 40-H, there are 81 QR blocks, and each block contains 41 authentication bits, while $\alpha = 1$.

Considering the common situations of noise, rotation, and print of the QR code in real-world applications, a QR tag should able to withstand various distortions. Statistically, the new scheme modifies $C/2$ modules of the original QR barcode by changing or unchanging the dry modules. That is, the derived marked QR tag can possess the readability of QR data

TABLE IV
MARKED 1-L QR BARCODES AFTER PRINTING AND SCANNING

	Marked QR code 1	Marked QR code 2	Marked QR code
Print and scan			
QR content	Readable		
Secret	Decodable		

and, theoretically, also maintain a portion of the error correction capability.

The print and scan operation for the QR tag is practiced extensively in the commercial magazine, poster, and publication fields. Table IV lists the printed and scanned tags for the marked 1-L QR codes [Fig. 3(d)–(f)]. The marked QR tags were printed by an HP LaserJet M2727 printer with 600 dpi and then scanned with 200 dpi to obtain the digital images without any correction or restoration. The QR data of the three printed and scanned QR tags are readable by a barcode reader. In addition, the QR tags with the validated keys can reveal the shared secret correctly. The designed technique is tolerant of the common print/scan operations to preserve the QR data and the secret shares in real-world application.

Table V illustrates the ability of the marked QR code if the marked QR codes suffered from common processes, such as noise, blur, compression, and rotation. Noise occurs when communicating or capturing the QR tag in the real world. Here, the Gaussian and Uniform noises are added to the marked QR tags at 10%, 30%, 50%, and 70%. Moreover, the compression technique usually is used to compress the QR tag for reducing

TABLE V
RESULTS OF THE MARKED 1-L QR BARCODES AFTER COMMON PROCESSES










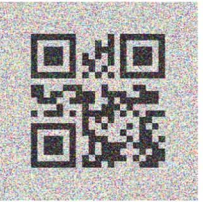















Gaussian noise	Marked QR code				The original QR code, 70%
	10%	30%	50%	70%	
Distorted QR code					
QR content	Readable	Readable	Readable	Readable	Readable
Secret	Decodable	Decodable	Decodable	Decodable	—
Uniform noise	Marked QR code				The original QR code, 70%
	10%	30%	50%	70%	
Distorted QR code					
QR content	Readable	Readable	Readable	Readable	Readable
Secret	Decodable	Decodable	Decodable	Decodable	—
Gaussian blurring	Marked QR code				The original QR code, Radius: 3 pixels
	Radius: 1 pixels	Radius: 2 pixels	Radius: 2.5 pixels	Radius: 3 pixels	
Distorted QR code					
QR content	Readable	Readable	Readable	Readable	Readable
Secret	Decodable	Decodable	Decodable	Decodable	—
Compression	Marked QR code				The original QR code, JPEG 2000, Q = 0%
	JPG, Q = 100%	JPG, Q = 0%	JPEG 2000 Q = 100%	JPEG 2000, Q = 0%	
Distorted QR code					
QR content	Readable	Readable	Readable	Readable	Readable
Secret	Decodable	Decodable	Decodable	Decodable	—
Rotation	Marked QR code				The original QR code, 270°
	45°	90°	135°	270°	
Distorted QR code					
QR content	Readable	Readable	Readable	Readable	Readable
Secret	Decodable	Decodable	Decodable	Decodable	—

TABLE VI
DECODING RESULTS WITH MOBILE DEVICES

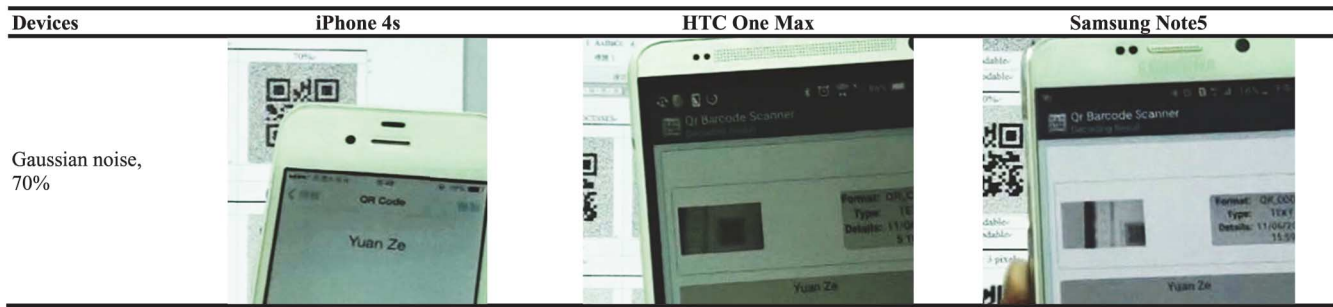


TABLE VII
COMPARISON OF RELATED QR BARCODE SCHEMES

Functionality	[4]	[5]	[6]	[7, 8]	[9-11]	[12]	The proposed scheme
Application field	Secret sharing	Image hiding	Image hiding	Image hiding	Watermarking	Watermarking	Secret sharing
Domain	Spatial	Spatial	Spatial	Frequency	Frequency	Spatial	Spatial
Meaningful of the marked result	No	Yes	Yes	Yes	Yes	Yes	Yes
Operation on the QR code	No	No	No	No	Yes	Yes	Yes
Module-based	No	No	No	No	No	Yes	Yes
Utilizing the error correction capability	No	No	No	No	No	No	Yes
Computational complexity	Low	Low	Low	High	High	Low	Low
Robustness	High	High	Low	Mid	Mid	Low	High
Secret capacity	QR image	QR image	QR image	QR image	Mid	Low	Adjustable, 24~9,720 bits

the storage space. To evaluate the feasibility of the designed scheme under image compression, the JPEG 2000 lossy compression is mounted to the marked QR image with quality factors (Q) of 100% and 0%. The rotation is mounted further to the marked QR tag to estimate the performance of the new scheme with the use of mobile devices and various degrees of scan.

To demonstrate the decodability of the distorted QR tags in Table IV, we used three different mobile devices: 1) an iPhone 4 s; 2) HTC One MAX; and 3) Samsung Note5. The term “readable” in Table IV indicates that the QR data of the distorted QR tag can be decoded correctly by a barcode reader. The term “decodable” denotes that the distorted QR tags with validated keys can reveal the shared secret afterward. It is obvious that the designed steganography QR sharing system is practicable and has sufficient ability to resist noise, blur, lossy compression, and various scan angles. Table VI shows the decoding results of our marked QR codes by the three mobile devices. The QR content “Yuan Ze” can be decoded successfully via the three different mobile devices.

For the sake of comparing the decodability between the original QR code with the designed QR code, the last column of Table V provides the original QR tag (without the secret embedded) when subjected to distortion. Note that the different barcode decoders and environments [16], such as lights, monitors, scales, and mobile devices, could influence the decoded results of the original barcode and our marked QR tag.

B. Comparison and Discussion

Because articles concerning secret sharing on QR barcode are relatively rare [4], to express the functionality of the QR application, Table VII provides an overall comparison of the QR related data hiding schemes, watermarking schemes, secret sharing schemes [4], and the proposed approach. The QR hiding schemes [5]–[8] can be regarded as the conventional image hiding technique that embeds the secret QR image into a cover image. Consequently, the secret capacity of the schemes [5]–[8] is equal to the data of the QR image.

The watermarking scheme [12] adjusts the widths of rows and columns of the QR module to conceal the watermark. Hence, the embeddable capacity and the robustness of [12] is less than that of other schemes [9]–[11]. The computational complexity of schemes [7]–[11] with the frequency domain is relatively greater than that of the schemes [4]–[6], [12] with the spatial domain and the proposed system. Because the selected coefficients of the QR frequency domain are limited, the capacities of [7]–[11] are restricted.

To comply with various secret capacities, the shared secret payload of the proposed approach is adjustable (24–9720 bits) along with an adequate QR version and error correction level. Different from related schemes, the designed approach explores the characteristics of a QR barcode to provide the steganography, readability, robustness, and adjustable secret capacity for the secret sharing mechanism. The new mechanism conceals the secret shares on the QR module directly. Thereby, the modified secret module of the designed approach is more

robust against geometric attacks (as shown in Table V) than the schemes that have modified LSBs and coefficients [5]–[12].

Chuang *et al.* [4] achieved the distributed secret sharing application with a QR tag by using Shamir's (t, n) -threshold system. Their scheme has the same robustness and secret capacity as the QR technique. However, the derived QR tags are meaningless and incapable of satisfying the steganography and readability requirements of the QR content.

C. Security Analysis

Considering the cheating situation, a dishonest participant may offer the genuine key and a fake QR tag to cheat others. Let I be the n authorized participants that can cooperate to reveal the secret S in the (n, n) -threshold secret sharing mechanism. The probability that participants of $I' \subset I$ will correctly reconstruct S is $2^{-\binom{m}{l_s}}$, where $|I'| < n$. The notation $\binom{n}{k}$ is defined as the number of combinations of n distinct things taken k at a time. This guarantees that the participants of I' are hardly able to restore the secret. It is difficult for a fraudulent participant to pass the cheater identification phase with a fake key or a tampered QR tag. The probability that a cheater could successfully hit all of the authentication bits is $2^{-\binom{m}{l_v}}$, which is negligible.

For instance, the probability of hitting the secret with fewer than n participants for the 1-L QR version is $2^{-\binom{152}{22}}$, and the probability for the 40-H QR version is $2^{-\binom{10\ 208}{6321}}$, where $\alpha = 1$. In addition, an intruder is hardly able to identify the genuine secret information from the $2^{-\binom{m}{l_s}}$ exhaustive combinations without the knowledge of n -marked QR tags and keys. The probability that a dishonest participant can fake a valid QR tag to deceive others for the 1-L QR version is $2^{-\binom{152}{2}}$, and the probability for the 40-H QR version is $2^{-\binom{10\ 208}{3321}}$, where $\alpha = 1$. To improve the ability to detect cheaters, the value of the real number α can be increased further according to the system demand, where $0 \leq \alpha < \frac{(C/b)-1}{\text{QR version}}$. This shows that the higher settings of the QR version, error correction level, and α can offer larger number of authentication bits to defend against a cheater. Only the authorized participants can reveal and decrypt the secret stream.

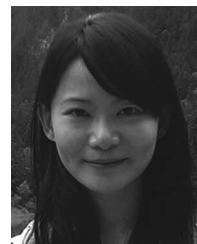
V. CONCLUSION AND FUTURE WORK

Different from the conventional QR application, the proposed approach utilizes the characteristics of QR modules to satisfy the essentials of steganography, readability, robustness, adjustable secret capacity, blind extraction, cheater detection, and identification for the secret sharing mechanism. As demonstrated in this experiment, the new QR sharing system can achieve satisfactory performance when compared to related attempts. Also, the designed algorithm is feasible and can be

applied to the related 2-D barcodes with error correction capability, such as the PDF417 and Data Matrix. In the future, we plan to investigate the Reed–Solomon code of the QR technique to reduce the modifications required and to improve the security of the QR barcode.

REFERENCES

- [1] *Information Technology—Automatic Identification and Data Capture Techniques—Bar Code Symbolology—QR Code*, ISO/IEC 18004, 2000.
- [2] Denso-Wave Inc., “QR code standardization,” 2003 [Online]. Available: <http://www.qrcode.com/en/index.html>
- [3] Psytex Inc., QR code editor software, 2013 [Online]. Available: <http://www.psytec.co.jp/docomo.html>
- [4] J. C. Chuang, Y. C. Hu, and H. J. Ko, “A novel secret sharing technique using QR code,” *Int. J. Image Process.*, vol. 4, pp. 468–475, 2010.
- [5] H. C. Huang, F. C. Chang, and W. C. Fang, “Reversible data hiding with histogram-based difference expansion for QR code applications,” *IEEE Trans. Consum. Electron.*, vol. 57, no. 2, pp. 779–787, May 2011.
- [6] 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,” *Int. J. Mod. Educ. Comput. Sci.*, vol. 6, pp. 59–67, 2012.
- [7] C. H. Chung, W. Y. Chen, and C. M. Tu, “Image hidden technique using QR-Barcode,” in *Proc. 5th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, 2009, pp. 522–525.
- [8] W. Y. Chen and J. W. Wang, “Nested image steganography scheme using QR-barcode technique,” *Opt. Eng.*, vol. 48, no. 5, pp. 057004-01–057004-10, 2009.
- [9] M. Sun, J. Si, and S. Zhang, “Research on embedding and extracting methods for digital watermarks applied to QR code images,” *N. Z. J. Agric. Res.*, vol. 50, pp. 861–867, 2007.
- [10] L. Li, R. L. Wang, and C. C. Chang, “A digital watermark algorithm for QR code,” *Int. J. Intell. Inf. Process.*, vol. 2, no. 2, pp. 29–36, 2011.
- [11] 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. Int. Conf. Comput. Commun. Technol.*, 2012, pp. 144–148.
- [12] M. Gao and B. Sun, “Blind watermark algorithm based on QR barcode,” in *Foundations of Intelligent Systems*, Berlin, Germany: Springer-Verlag, vol. 122, 2011, pp. 457–462.
- [13] H. Martin, P. Peris-Lopez, J. E. Tapiador, and E. San Millan, “An estimator for the ASIC footprint area of lightweight cryptographic algorithms,” *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1216–1225, May 2014.
- [14] Y. J. Chiang, P. Y. Lin, R. Z. Wang, and Y. H. Chen, “Blind steganographic approach for QR code module based upon error correction capability,” *KSII Trans. Internet Inf. Syst.*, vol. 7, no. 10, pp. 2527–2543, 2013.
- [15] ZXing, *Zebra Crossing*, 2015 [Online]. Available: <http://code.google.com/p/zxing/>
- [16] D. Munoz-Mejias, I. Gonzalez-Diaz, and F. Diaz-de-Maria, “A low-complexity pre-processing system for restoring low-quality QR code images,” *IEEE Trans. Consum. Electron.*, vol. 57, no. 3, pp. 1320–13, Aug. 2011.



Pei-Yu Lin (M'10) received the M.S. and Ph.D. degrees from National Chung Cheng University, Chiayi, Taiwan, in 2004 and 2009, respectively, both in computer science and information engineering.

Currently, she is an Associate Professor with the Department of Information Communication, Yuan Ze University, Taoyuan, Taiwan. Her research interests include image protection, data mining, and information security.