Lin and Chen *EURASIP Journal on Image and Video Processing* (2017) 2017:14
DOI 10.1186/s13640-016-0155-0

EURASIP Journal on Image and Video Processing

RESEARCH Open Access

High payload secret hiding technology for QR codes

Pei-Yu Lin[1] and Yi-Hui Chen[2,3*]

Abstract

Quick response (QR) code has become one of the more popular two-dimensional barcodes because of its greater data capacity and higher damage resistance. The barcode scanners can easily extract the information hidden in the QR code while scanning the data modules. However, some sensitive data directly stored in QR codes are insecure in real-world QR applications, such as the e-ticket and e-coupon. To protect the sensitive data, this paper explores the characteristics of QR barcodes to design a secret hiding mechanism for the QR barcode with a higher payload compared to the past ones. For a normal scanner, a browser can only reveal the formal information from the marked QR code. The authorized user/scanner can further reveal the sensitive data from the marked QR tag. The experiments demonstrate a satisfactory secret payload and the feasibility of the proposed scheme.

Keywords: QR barcode, Secret, Steganography, Error correction capability, Module

1 Introduction

Many multimedia applications, such as labeled street view images [1], video streaming [2], and consumer photos [3], add quick response (QR) codes to help readers to easily distribute and understand some related information. The QR code is a type of trademark barcode with a machine-readable optical label, in which the information of the barcode can be quickly extracted through scanning the label. Recently, the QR code is one of the most popular two-dimensional (2-D) barcodes that consists of black and white square modules [4–6]. With the wide range of matrix modules, the QR code can carry larger data content than the conventional one-dimensional (1-D) barcodes. There are 40 QR versions in the QR code standard [6]. The higher version of the QR code can carry a larger data capacity. For example, the data capacity is 208 modules for QR version 1 and is 29,648 modules for QR version 40. Moreover, the error correction capability of the QR code allows barcode readers to restore the QR data without any loss if the QR code becomes dirty or damaged [7].

With barcode readers, one can obtain the QR data easily and effectively. Nevertheless, the appearance of the confidential data in a QR code raises a security issue. In general, the common approach to protect the confidential data of the QR code is using the back-end database [8]. The QR data only provides the database website link, such as uniform resource locator (URL). An authorized user can login to the database via linking the URL and then achieves the confidential data. Such a mechanism, however, needs to maintain the database, the access control, and the online requirement. The online decoded, moreover, may expose the risks of database attacks.

Recently, the conventional digital secret hiding and watermarking techniques [9–11] are usually adopted to conceal the secret into the host image. The processes embed the secret into the pixels/coefficients and into the spatial/frequency domains of the host image. Such embedding algorithms, unfortunately, are unsuitable for the QR tag [9–15] due to the fact that the embedding schemes treat the QR tag as an image, in which the secret is concealed in the pixel or coefficients of the QR image without considering the characteristics of the QR modules. The decoding processes need further image processing, such as pixel and frequency transformation. The secret is incapable of being extracted by the barcode reader directly. The decoding of the schemes [9–15] limits the real-world applications of QR barcode readers.

To protect the confidential secret of the QR tag and the decoding by a barcode reader directly, we designed a

* Correspondence: chenyh@asia.edu.tw
[2]Department of M-Commerce and Multimedia Applications, Asia University, Taichung 41354, Taiwan
[3]Department of Medical Research, China Medical University Hospital, China Medical University, Taichung 404, Taiwan
Full list of author information is available at the end of the article

secret QR hiding approach based on the property of the QR standard [5, 16] in this article. The proposed scheme can enhance the embeddable secret capacity of the QR tag than that of the related scheme [16]. To increase the hiding payload, this paper considers the characteristics of QR codes to propose a novel data hiding method, which is an extended version of [17]. The proposed scheme can convey a higher payload of the sensitive data for QR tags by modifying the data modules directly. The QR data of the generated marked QR tag, especially, is readable. That is, one can use the barcode reader to exhibit the QR data, such as the URL. The ability of exhibiting the QR data from the marked QR tag can reduce the suspicions of attackers and intruders. Only the authorized user can further extract the confidential secret from the same generated QR tag via the barcode reader. The designed approach can satisfy the essentials of steganography, secret protection, and feasibility for low-power barcode readers and mobile devices.

This paper is organized as follows: related works are briefly described in Section 2. The proposed secret hiding scheme for the QR code is presented in Section 3. The experimental results are shown in Section 4. Finally, conclusions are made in Section 5.

2 Related works

The concepts of the QR barcode [5] and the least significant bit (LSB) matching revisited embedding scheme [18] are briefly introduced in this section.

2.1 QR barcode

According to the QR standard [5], there are 40 versions of the QR tag, and each has four error correction levels, L, M, Q, and H. Table 1 lists the error correction capability of the QR tag. The higher level of error correction represents the QR tag which has the ability to resist larger damage. For instance, level L means that the barcode reader can successfully restore the QR data while the distortion of the QR tag is limited within 7%. Level H indicates that the QR data is decodable by the barcode reader while 30% of the QR tag is damaged.

In general, the binary QR data, such as the URL, is decoded into the corresponding white and black modules. The white and black modules are equal to the binary values 0 and 1, respectively. To achieve the recover ability of QR data, the error correction codewords corresponding to the QR data can be computed [5]. The gray area in Fig. 1 displays the data and error correction codewords of the QR tag. Here, a codeword refers to eight modules.

Table 1 Error correction levels

Error correction level	Recovery capacity (%)
L	7
M	15
Q	25
H	30

Specifically, the QR data with a larger capacity is normally divided into non-overlapping data blocks according to its QR version to withstand damage without loss. The error correction codewords corresponding to each QR data block thereby can be generated individually. For example, the block number is 1 for QR versions 3-L and 3-M, and the block numbers are 2 for QR versions 3-Q and 3-H. That is, the higher QR version and error correction level, the larger number of QR data blocks.

2.2 LSB matching revisited embedding scheme [18]

The image is divided into several groups, and each group is the size of 2 pixels (i.e., p_i and p_{i+1}). Two secret bits, s_i and s_{i+1}, could be hidden in a group. The two secret bits can be extracted according to Eqs. (1) and (2), respectively, where LSB(x) extracts the last significant bit of the x value.

$$s_i = \mathrm{LSB}(p_i). \tag{1}$$

$$s_{i+1} = f(p_i, p_{i+1}) = \mathrm{LSB}(\lfloor p_i/2 \rfloor + p_{i+1}). \tag{2}$$

If the first secret bit (or the second bit) is not equal to the value of $f_1(\cdot)$ function (or the value of $f_2(\cdot)$ function), the pixel p_i must be updated with an embedding algorithm complying with Eqs. (3) and (4).

$$f(p_i - 1, p_{i+1}) \neq f(p_i + 1, p_{i+1}). \tag{3}$$

$$f(p_i, p_{i+1}) \neq f(p_i, p_{i+1} + 1). \tag{4}$$

Embedding Algorithm

Input: a pair of cover image pixels p_i, p_{i+1}; two secret bits s_i, s_{i+1}
Output: a pair of stego-image pixels q_i, q_{i+1}
If $s_i = \mathrm{LSB}(p_i)$
  If $s_{i+1} \neq f(p_i, p_{i+1})$
    $q_{i+1} = p_{i+1} + 1$ or $p_{i+1} - 1$
  else
    $q_{i+1} = p_{i+1}$
  end
  $q_i = p_i$
else
  If $s_{i+1} \neq f(p_i - 1, p_{i+1})$
    $q_i = p_i - 1$
  else
    $q_i = p_i + 1$
  end
  $q_{i+1} = p_{i+1}$
end

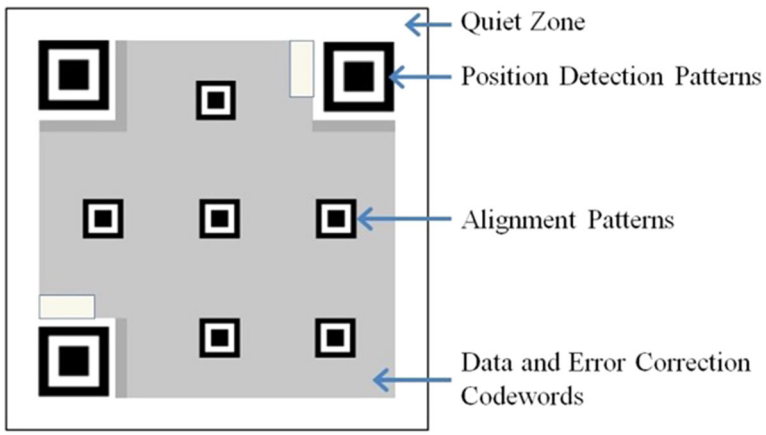

Fig. 1 The modules of a QR code

3 The proposed scheme

The steganography scheme for the QR tag is spilt into a secret embedding procedure and extracting procedure, and their corresponding flowcharts are shown in Figs. 2 and 3, respectively.

3.1 Secret embedding procedure

Given an original QR tag and the confidential secret S, the proposed scheme embeds the secret into the data codewords of the QR tag and retains the remaining unmodified QR regions. The steps are listed below:

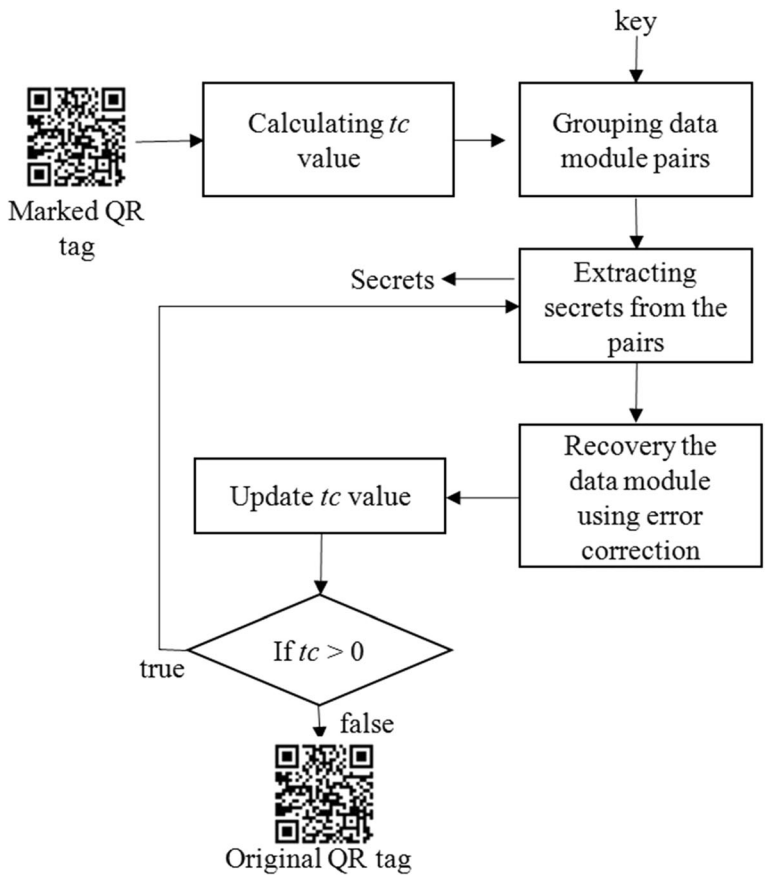

Fig. 2 The flowchart of secret embedding procedures

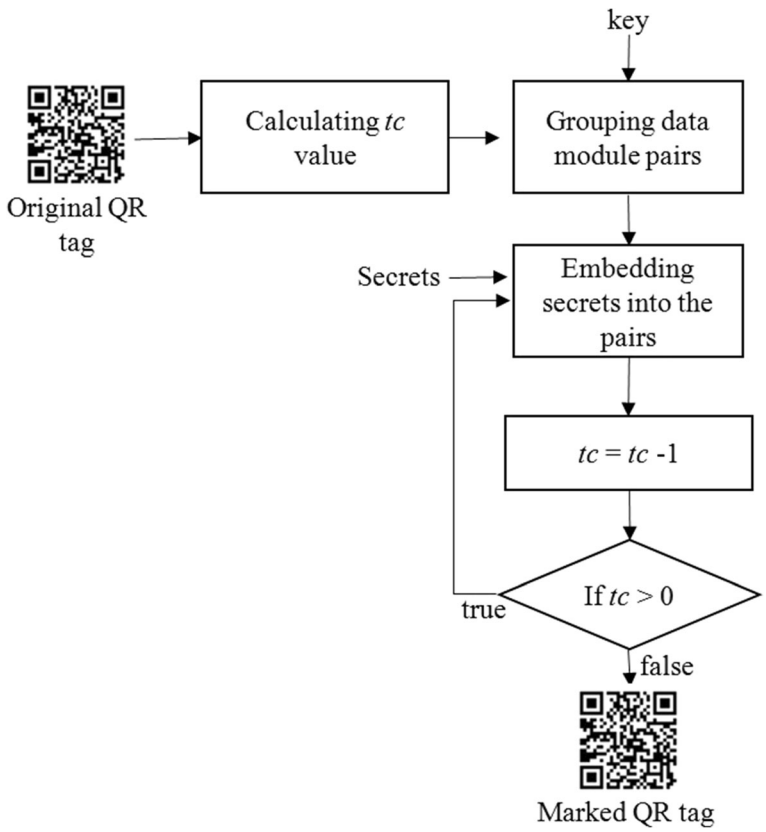

Fig. 3 The flowchart of secret extracting procedure

Step 1. The tolerant capacity, *tc*, of the secret is defined as

$$tc = \left\lfloor \frac{ecc}{2} \right\rfloor \times 8. \quad (5)$$

The value of *tc* is determined according to the QR version and the error correction level of the given QR tag. Here, the value of *ecc* is the number of error correction codewords of the QR tag.

Step 2. The QR data codewords is divided into several pairs, in which two data modules are a pair, and the black data module and the white one are as values 1 and 0, respectively. The pair can be presented as the digit d_i, where d_i is the range of 0 and 3, and be denoted as $\left(d_i^1 \quad d_i^2\right)_2$. Put the digit d_i into a pool.

Step 3. A secret key, *K*, is used to randomly choose two digit pairs, denoted as d_x and d_y from the pool, where $x \neq y$.

Step 4. Four secret bits (denoted as s_1, s_2, s_3, and s_4) are embedded into the digit pairs d_x and d_y with Eq. (6). Here, the $|w|$ function is to get the absolute value of *w*.

$$\begin{aligned} d_x^1 &= s_{1,} \\ d_x^2 &= s_{2,} \\ d_y^2 &= s_{4,} \\ d_y^1 &= |s_3 - \lfloor d_x/2 \rfloor|. \end{aligned} \quad (6)$$

Step 5. Update the corresponding data modules in the QR codes according to the values of d_x^1, d_x^2, d_y^1, and d_y^2 after secret embedding. If the value is 1, the data module is a black one; otherwise, it is a white one.

Step 6. Accumulate the number of the changed data module. That is, if no data modules are changed, keep the *tc* value. If the module is changed from the black module to the white one or white one to black one, the *tc* is updated as *tc*−1. The total changed data module is counted to reduce the *tc* value.

Step 7. Remove the digit from the pool.

Step 8. Repeat steps 3 to 7 until the *tc* value is identical to 0 or the pool is empty.

Step 9. After secret embedding to the QR modules, the proposed scheme produces the marked QR tag.

3.2 Secret extracting procedure

During the secret extracting process, the authorized receiver can extract the secret S from the marked QR code with the secret key K. The detailed extracting steps are listed as follows:

Step 1. Steps 1 to 3 of the secret embedding procedure are applied to this step.

Step 2. A secret key is used to select the digit pairs d_x and d_y from the pool.

Step 3. The secrets can be extracted by using Eq. (7).

$$\begin{aligned} s_1 &= d_x^1, \\ s_2 &= d_x^2, \\ s_4 &= d_y^2, \\ s_3 &= f(d_x, d_y). \end{aligned} \tag{7}$$

Step 4. Find the corresponding data modules of the digit pairs d_x and d_y and then check each of the

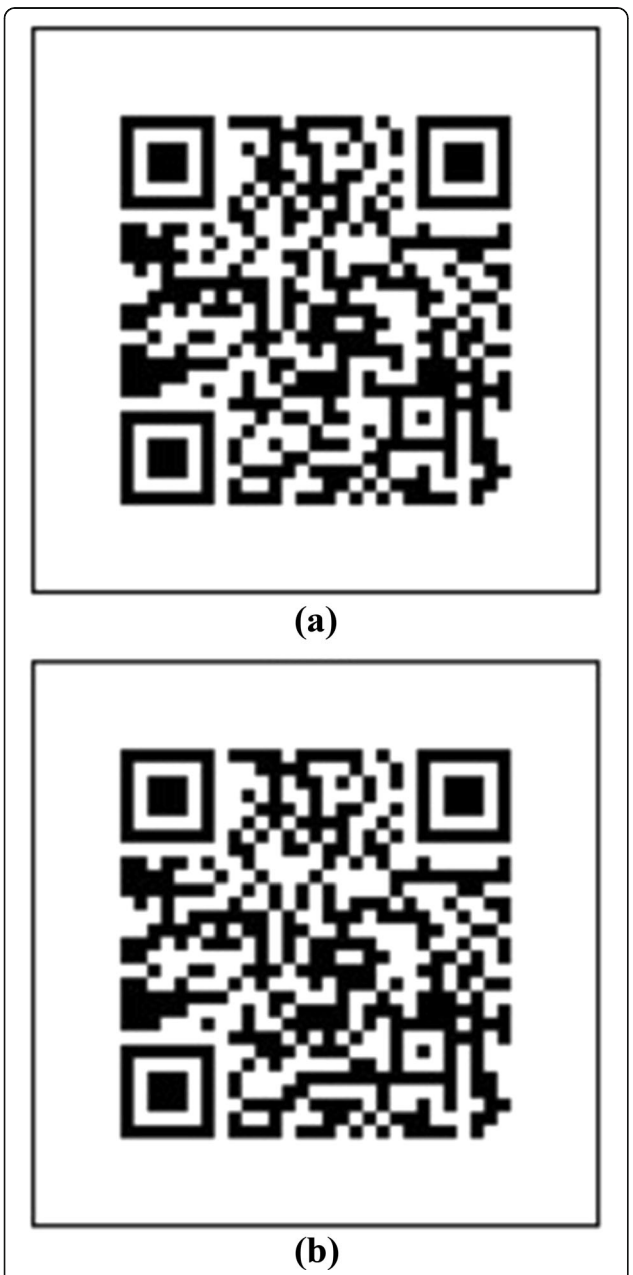

Fig. 4 The results of 3-L QR barcode. **a** The host QR tag with the QR data *EURASIP Journal on Image and Video Processing*. **b** The marked QR tag of **a**

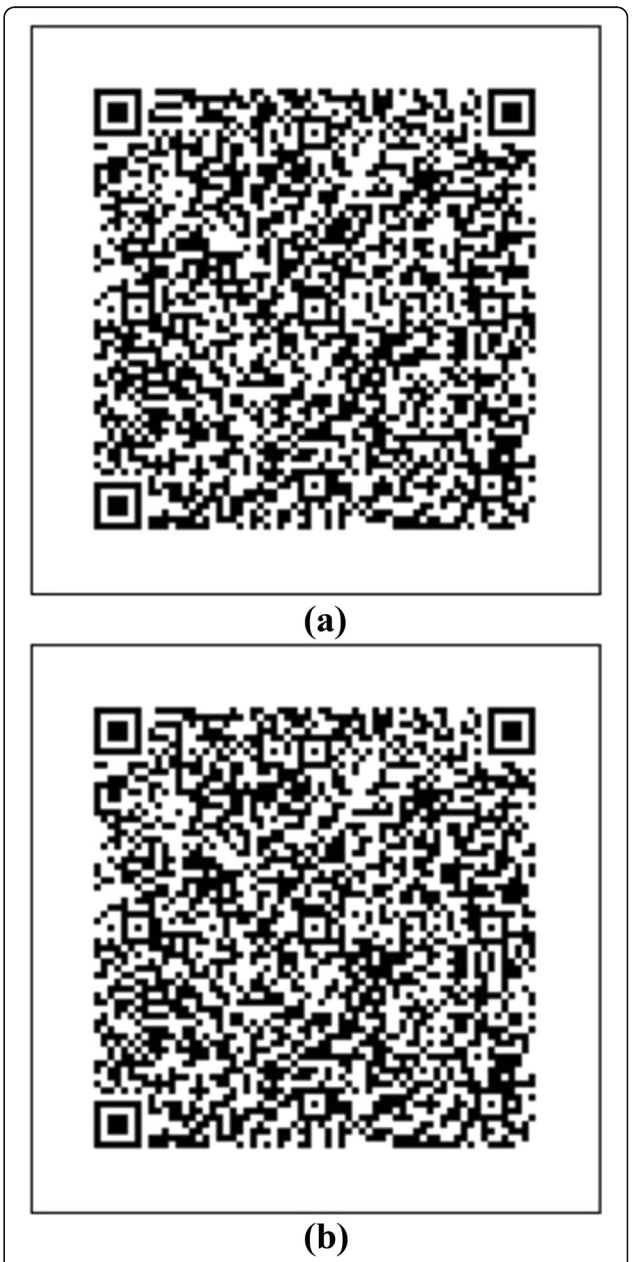

Fig. 5 The results of 12-L QR barcode. **a** The host QR tag with the QR data "HIGH PAYLOAD SECRET HIDING SCHEME FOR QR CODES". **b** The marked QR tag of **a**

four data modules. The corresponding QR code can be recovered by using the error correction. If a module is flipped from the black module to be a white one or from a white one to be black one after the error correction, let $tc=tc-1$. For example, if four data modules are all flipped, $tc=tc-4$.

Step 5. Remove the digit pairs d_x and d_y from the pool.

Step 6. Repeat steps 2 to 5 until tc is equal to 0.

The secret extracting procedure is with a low computation load. The proposed method is feasible to be applied to QR applications. The marked QR codes can be recovered by error correction. Thus, barcode readers can scan the corrected QR codes to extract the information for the users.

4 Experimental results

In a simulation environment, the proposed secret hiding scheme is developed by the ZXing library [19] with C#.NET language. ZXing is an open-source library and is applied to generate the original test QR tag.

The result of the secret embedding procedure is shown in Fig. 4. Figure 4a is the original QR tag with the QR data "EURASIP Journal on Image and Video Processing." Here, the QR version is 3 and the error correction level is L. According to Eq. (5), we can learn that the tolerant capacity of the secret embedding procedure is 24 bits. That is, the new scheme can embed at least 24 secret bits into Fig. 4a. The generated marked QR tag is shown in Fig. 4b by the secret embedding procedure. Figure 4b has the error correction capability for later recovering the error modules.

The pattern of the QR tag is composed of square modules (i.e., white and black dots), which are meaningless to users. That is, the marked QR tag cannot be easily observed by hackers if it is an embedded secret.

With barcode readers, the original QR data can be retrieved from the marked QR tag by the error correction capability. One can obtain the same QR data "EURASIP Journal on Image and Video Processing" from Fig. 4b. The meaningful QR data of the marked QR tag can effectively reduce the attention of general users and intruders.

Figure 5 demonstrates the original QR tag with larger QR data "HIGH PAYLOAD SECRET HIDING SCHEME FOR QR CODES..." The QR version and error correction level of Fig. 5a are 12-L. According to the estimation of Eq. (5), the tolerant secret capacity can be increased and is larger than 384 bits. The corresponding generated marked QR tag is shown in Fig. 5b. Only the authorized receivers with the secret keys can thereby retrieve the corresponding secrets from Figs. 4b and 5b.

Table 2 lists the capacities of the QR data under different QR versions and error correction levels. Table 3

Table 3 The tolerant capacity, *tc*, for different QR versions and error correction levels

QR version	*tc* (bits)			
	L	M	Q	H
1	24	40	48	64
5	104	192	288	352
10	288	520	768	896
15	528	960	1440	1728
20	896	1664	2400	2800
25	1248	2352	3480	4200
30	1800	3248	4800	5760
35	2280	4256	6360	7560
40	3000	5488	8160	9720

Table 2 The QR data payload for different QR versions and error correction levels

QR version	Number of QR data (bit/modules)			
	L	M	Q	H
1	152	128	104	72
5	864	688	496	368
10	2192	1728	1232	976
15	4184	3320	2360	1784
20	6888	5352	3880	3080
25	10,208	8000	5744	4304
30	13,880	10,984	7880	5960
35	18,448	14,496	10,288	7888
40	23,648	18,672	13,328	10,208

Table 4 The average secret capacity under different QR versions and error correction levels, iterations = 100

QR version	Embedded secret capacity (bits)			
	L	M	Q	H
1	50	83	97	72
5	215	396	496	368
10	613	1086	1232	976
15	1088	2024	2360	1784
20	1853	3474	3880	3080
25	2596	4903	5744	4304
30	3735	6752	7880	5960
35	4751	8887	10,288	7888
40	6249	11,445	13,328	10,208

Table 5 The statistical secret capacity under different QR versions and error correction levels

QR version	Statistical secret capacity (bits)			
	L	M	Q	H
1	46	78	94	72
5	205	382	496	368
10	574	1038	1232	976
15	1054	1916	2360	1784
20	1789	3325	3880	3080
25	2492	4700	5744	4304
30	3596	6491	7880	5960
35	4555	8509	10,288	7888
40	5993	10,970	13,328	10,208

shows the tolerant secret capacity *tc*, under different QR versions and error correction levels. The proposed scheme can embed at least the *tc* secret bits into the QR tag. Here, the maximum secret capacity is limited within the QR data payload. For instance, in QR version 1-L, the new scheme can embed at least 24 secret bits into the QR tag (lower bound), and the upper bound of the secret payload is 152 bits.

To demonstrate the performance of the hiding scheme, we generated a random secret stream and then embedded the secret into the selected modules by the random secret key according to the embedding procedure. The average experiment results are listed in Table 4 with 100 embedding iterations. Comparing the secret capacities in Table 3 with Table 4, we can observe that the new scheme can effectively enhance the capacity of embeddable secret. For instance, the original secret capacity is 24 bits in 1-L, and we can enhance and conceal in the average 50 secret bits at the same QR tag.

Table 5 lists the statistical analysis of the embeddable secret capacity under different QR versions and error correction levels. The probabilities of bits 0 and 1 for the secret stream and QR data are 1/2 with normal distribution. According to the experimental results and the statistical results in Tables 4 and 5, the new hiding scheme can achieve a higher secret capacity into a QR tag than the original embedding manner [16].

The number of error correction capability and the QR version are the measure metrics for evaluating the performances of the generated QR tags. The higher setting of the error correction level and QR version, the larger the secret capacity is. Moreover, the proposed scheme can preserve the original QR content by exploring the characteristic of the error correction capability of the QR tag.

Table 6 displays the overall comparison between the related schemes [12–16] and the proposed scheme. Unlike the conventional hiding and watermarking schemes [9–15], the new scheme embeds the secret into the modules of the QR tag directly [16]. Hence, the secret extracting procedure of the proposed scheme is feasible for barcode readers. The new scheme is of low computational complexity and can be applied to mobile device applications.

The secret payload of the proposed scheme is dynamic and can be increased according to the higher settings of QR versions and error correction levels. According to the secret embedding procedure in Subsection 3.1, the designed algorithm can embed more than *tc* secret bits into a QR tag as shown in Table 4. Therefore, the proposed scheme can enhance the embeddable secret payload more than the recent article [16].

5 Conclusions

The proposed secret hiding scheme effectively improves the embeddable secret capacity more than the related QR scheme. Moreover, based on the error correction capability of the QR characteristic, the generated marked QR tag can still preserve the readability of the QR data. According to the experimental analysis, the designed scheme is feasible to hide the secrets into a tiny QR tag as the purpose of steganography. Only the authorized user with the private key can further reveal the concealed secret successfully.

Table 6 Overall comparison between the related schemes and the proposed scheme

Methods	References [12, 13]	References [14, 15]	[16]	Proposed
Applications	Image hiding	Image hiding	Secret hiding	Secret hiding
Embedding domain	Frequency	Spatial	Spatial	Spatial
Computational complexity	High	Low	Low	Low
Operation upon QR code	No	No	Yes	Yes
Module-based	No	No	Yes	Yes
Utilizing the error correction capability	No	No	Yes	Yes
Secret payload	–	–	*tc* bits	Larger than *tc* bits

Acknowledgements
The authors thank the support from the Ministry of Science and Technology, Taiwan. In addition, our gratitude also goes to Michael Burton, Asia University.

Funding
This research was supported by the Ministry of Science and Technology, Taiwan, under contract No. MOST 105-2221-E-155-048, MOST 105-2218-E-155-010, MOST 104-2221-E-468-005, and 104-2221-E-009-109.

Authors' contributions
PL drafted the manuscript and implemented the experiments for verifying the feasibility of the proposed scheme. YC participated in the design of the proposed scheme and drafted the manuscript. Both authors read and approved the final manuscript.

Competing interests
The authors declare that they have no competing interests.

Author details
[1]Department of Information Communication, and Innovation Center for Big Data and Digital Convergence, Yuan Ze University, Chung-Li 32003, Taiwan. [2]Department of M-Commerce and Multimedia Applications, Asia University, Taichung 41354, Taiwan. [3]Department of Medical Research, China Medical University Hospital, China Medical University, Taichung 404, Taiwan.

Received: 3 June 2016 Accepted: 15 December 2016
Published online: 08 February 2017

References

1. TH Tsai, WH Cheng, CW You, MC Hu, AW Tsai, HY Chi, Learning and recognition of on-premise signs (OPSs) from weakly labeled street view images. IEEE Trans Image Process **23**(3), 1047–1059 (2014)
2. HH Shuai, DN Yang, WH Cheng, MS Chen, MobiUP: an upsampling-based system architecture for high quality video streaming on mobile devices. IEEE Trans. Multimedia **13**(5), 1077–1091 (2011)
3. TH Tsai, WC Jhou, WH Cheng, MC Hu, IC Shen, T Lim, KL Hua, A Ghoneim, MA Hossain, SC Hidayati, Photo sundial: estimating the time of capture in consumer photos. Neurocomputing **177**, 529–542 (2016)
4. Psytec QR code editor software, [Online]. Available: http://www.psytec.co.jp/docomo.html
5. ISO/IEC 18004, *Information Technology Automatic Identification and Data Capture Techniques Bar Code Symbology QR Code*, 2000
6. Denso-wave, [Online]. Available: http://www.qrcode.com/en/index.html
7. IS Reed, G Solomon, Polynomial codes over certain finite fields. J. Soc. Ind. Appl. Math **8**(2), 300–304 (1960)
8. JC Chuang, YC Hu, HJ Ko, A novel secret sharing technique using QR code. International Journal of Image Processing **4**, 468–475 (2010)
9. D. Buczynski, (2002-09-05), MSB/LSB tutorial, [Online]. Available: http://www.buczynski.com/Proteus/msblsb.html
10. S Katzenbeisser, FA Petitcolas, *Information hiding techniques for steganography and digital watermarking*. Artech House, Inc. Norwood, MA, USA, 2000
11. XP Zhang, SZ Wang, Efficient steganographic embedding by exploiting modification direction. IEEE Commun. Lett **10**(11), 781–783 (2006)
12. CH Chung, WY Chen, CM Tu, *Image Hidden Technique Using QR-Barcode*. Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2009, pp. 522–525
13. WY Chen, JW Wang, Nested image steganography scheme using QR-barcode technique. Opt. Eng. **48**(5), 057004-01–057004-10 (2009)
14. HC Huang, FC Chang, WC Fang, Reversible data hiding with histogram-based difference expansion for QR code applications. IEEE Trans. Consum. Electron. **57**(2), 779–787 (2011)
15. S Dey, K Mondal, J Nath, 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 **6**, 59–67 (2012)
16. YJ Chiang, PY Lin, RZ Wang, YH Chen, Blind QR code steganographic approach based upon error correction capability. KSII Trans. Internet Inf. Syst. **7**(10), 2527–2543 (2013)
17. PY Lin, YH Chen, *QR Code Steganography with Secret Payload Enhancement*. the 3rd IEEE International Workshop on Mobile Multimedia Computing (MMC), 2016
18. J Mielikainen, LSB matching revisited. IEEE Signal Process Lett **13**(5), 285–287 (2006)
19. Z. Xing ("Zebra Crossing"), [Online]. Available: http://code.google.com/p/zxing/