QR CODE STEGANOGRAPHY WITH SECRET PAYLOAD ENHANCEMENT

Pei-Yu Lin[a] and Yi-Hui Chen[b,†]
[a]Department of Information Communication, Yuan Ze University, Chung-Li 32003, Taiwan
[b]Department of M-Commerce and Multimedia Applications, Asia University, Taichung 41354, Taiwan
e-mail: pylin@saturn.yzu.edu.tw; chenyh@asia.edu.tw
[†]Correspondence author: Yi-Hui Chen

ABSTRACT

Different from one-dimensional barcode, QR (quick response) code is a popular two-dimensional barcode due to the fact that it can carry greater data capacity and capable of resisting damage. The content of QR code can be easily revealed by barcode scanners. However, in the real world QR applications, the content could be private information, such as the e-ticket and e-coupon. The QR content should be protected to resist from unauthorized users/scanners. In this article, we explore the characteristic of QR barcode and design a QR barcode steganography mechanism. The private information can be embedded into a cover QR tag with high secret payload. For a normal scanner, a browser can only reveal the cover QR content from the marked QR code. Only the authorized user/scanner can further reveal the private secret from the marked QR tag. According to the experimental, the new algorithm can convey satisfactory secret payload in to a QR tag. The mechanism is efficient and feasible for private QR applications.

Index Terms— QR barcode, secret, steganography, error correction capability, module

1. INTRODUCTION

QR code (quick response code) is one of the popular two-dimensional (2-D) barcodes that consisting of black and white square modules [1-3]. With the wide range of matrix modules, QR code can carry larger data content than the conventional one-dimensional (1-D) barcodes. There are 40 QR versions in QR code standard [3]. The higher version of QR code can carry larger data capacity. For instance, 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 QR code allows barcode readers to restore the QR data losslessly when QR code suffered from dirtied and damaged [4].

With barcode readers, one can obtain the QR data easily and effectively. Nevertheless, the appearance of the confidential data in QR code raises an insecure issue. In general, the common approach to protect the confidential data of QR code is using the back-end database [5]. The QR data only provides the database website link, such as uniform resource locator (URL). An authorized user can login the database via linking the URL and then achieve the confidential data. Such mechanism, however, needs to maintain the database, the access control and the online requirement. The online decoded, moreover, may exposes the risks of database attacks.

Recently, the conventional digital secret hiding and watermarking techniques [6-8] are usually adopted to conceal the secret into the host image. The processes embed the secret into the pixels/coefficients into the spatial/frequency domains of the host image. Such embedding algorithms, unfortunately, are unsuitable for the QR tag [6-12]. Due to the fact that the embedding schemes treat the QR tag as an image, the secret concealed in the pixel or coefficients of QR image and without considering the characteristic of QR modules. The decoding processes need further image processing, such as pixel and frequency transform. The secret is incapable of being extracted by the barcode reader directly. These decoding of the schemes [6-12] limit the real-world applications of QR barcode readers.

To protect the confidential secret of QR tag and be decoded by a barcode reader directly, we designed a QR code steganography approach based on the property of QR standard [2, 13] in this article. To improve the hiding capacity, this paper proposed a new data hiding method for QR codes by using the concept of EMD scheme [8]. The proposed scheme can conceal higher payload of the confidential data into a QR tag by modifying the QR 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 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 QR code is presented in Section 3. Section 4 demonstrates the simulation results and performance. Finally, conclusions are made in Section 5.

2. RELATED WORKS

The concepts of the QR barcode [2] and the EMD scheme [8] are briefly introduced in this section.

2.1. QR Barcode

According to the QR standard [2], there are 40 versions of QR tag, and each with four different error correction levels (L, M, Q and H). As listed in Table 1, the higher level of error correction can resist larger damaged of QR tag. For instance, the level L means the barcode reader can successfully restore the QR data while the distortion of the QR tag is limited within 7%. The level H indicates that the QR data is decodable by barcode reader while 30% of the QR tag is damaged.

In generally, the yellow area of Fig. 1 demonstrates the data and error correction codewords of QR tag. Here, a codeword refers to eight modules. The white and black modules equal to the binary values zero and one, respectively.

Table 1. Error correction levels

Error correction Level	Recovery Capacity %
L	7 %
M	15 %
Q	25 %
H	30 %

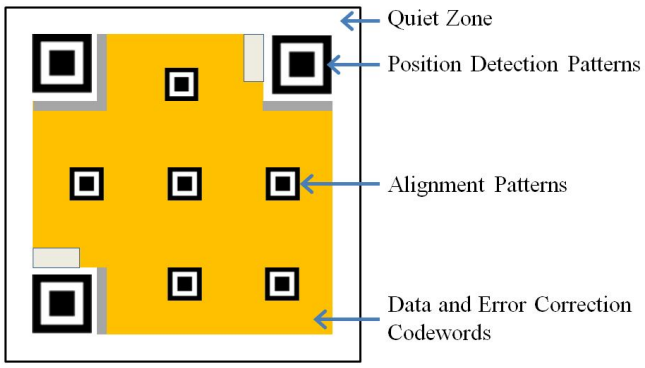

Fig. 1. The modules of a QR code.

2.2. EMD Embedding Scheme

Every w pixels (i.e., p_1, p_2, …, p_w) as a group is to cluster the images into n groups, denoted by g_1, g_2 , ..., g_n. Here, the pixel values in each group can be represented by m digits in a $(2w+1)$-ary notational system [8]. The digit d can be calculated by Eq. (1).

$$d = f(p_1, p_2, \ldots, p_w) = \sum_{i=1}^{w} i \cdot p_i \bmod (2w+1) . \quad (1)$$

If d is not equal to s, ss is computed as $s - d \bmod (2w + 1)$. While ss is more than w, let p_{ss} equal to p_{ss} +1; otherwise, $p_{2w+1-ss}$ equals to original value minus by 1.

3. THE PROPOSED SCHEME

The steganography scheme for QR tag is spilt into secret embedding procedure and extracting procedure.

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 QR regions unmodified. The steps are listed below.

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

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

The value of tc can be dynamically 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 QR tag.

Step 2. Let two data modules be a module pair. Put all the module pairs into a pool.

Step 3. A key is used as random seed to choose a module pair (x_1, x_2) from the pool, where x_1 and x_2 are values of the data modules in the chosen module pair.

Step 4. The digit e is computed with Eq. (2).

$$e = f(x_1, x_2) = (x_1+2x_2) \bmod 4. \quad (3)$$

The z value is computed as $z = s - e$. Next, $|z|$ is transformed to be $(z_1z_2)_2$. If z is larger than 0, x_i is updated as $x_i = x_i+z_i$, for i =1 to 2; otherwise, $x_i = x_i-z_i$.

Step 5. Update the corresponding module values in QR codes according to the changed module pair (x_1, x_2).

Step 6. The digit, denoted n, is used to record the number of module pairs selected for embedding. After data embedding, n is updated as n+1.

Step 7. If no data modules are changed, keep tc value intact. In the second case, if $|z|$ is less than 3 and any data module of the module pair (x_1, x_2) is changed, the tc is updated as tc-1; otherwise, $tc = tc$ -2.

Step 8. Remove the module pair from the pool.

Step 9. Repeat the steps 3 to 8 until tc is equal to 0 or the pool is empty.

By hiding the secret into the QR modules, the proposed scheme finally can generate the marked QR tag. The proposed scheme can guarantee that at most tc modules of QR tag be modified. Therefore, the new scheme can achieve

the steganography purpose and reduce the attention of intruders.

3.2. Secret Extracting Procedure

In the secret extracting process, the authorized receiver can retrieve the secret S from the marked QR code by the private key K. The normal users can only obtain the QR data from the marked QR code by barcode reader. The steps are listed below.

Step 1. The steps 1 and 2 of embedding procedure are applied to this step.
Step 2. A secret key is used to select the module pair (x_1, x_2) from the pool.
Step 3. The secrets can be extracted by using Eq. (2).
Step 4. After secret extracting, n is updated as n-1.
Step 5. Remove the module pair from the pool.
Step 6. Repeat the steps 2 to 5 until n equals to 0.
Step 7. The QR codes can be recovered by using the error correction.

The secret extracting procedure is low computational complexity and efficient. The scheme is feasible to be applied for barcode readers and mobile device for value-added QR applications.

4. EXPERIMENTAL RESULTS

In the simulation environment, the proposed steganography scheme is developed by the ZXing library [14] with C#.NET language. Fig. 2 shows the resultant of the proposed secret embedding procedure. Fig. 2(a) is the original QR tag with QR data "http://icme2016.org". Here, the QR version is 2 and the error correction level is L. According to Eq. (2), we can learn the tolerant capacity of secret is 24 bit. That is, the new scheme can embed at least 24 secret bits into Fig. 2(a). The generated marked QR tag is shown in Fig. 2(b). The pattern of QR tag is composed of square modules (i.e., white and black dots), which are meaningless to users. Generally, the QR tag cannot easily be detected by attackers whether it embeds secret.

Fig. 2(b) has error correction capability for later recovering the error modules while modules are altered during the secret embedding procedure. With barcode readers, the original QR data can still be retrieved by the error correction capability. That is, one can obtain the same QR data "http://icme2016.org" from Fig. 2(b). The steganography of the generated QR tag can effectively reduce the attention of general users and intruders.

Fig. 3 demonstrates the original QR tag with larger QR data "QR CODE STEGANOGRAPHY WITH SECRET PAYLOAD ENHANCEMENT …". The QR version and error correction level of Fig. 3(a) is 12-L. According to the estimation of Eq. (2), the tolerant secret capacity can be increased and larger than 384 bits. The corresponding generated marked QR tag is shown in Fig. 3(b). Only the authorized receiver with key can thereby retrieve the secret from Figs. 2(b) and 3(b).

(a) The host QR tag with the QR data "http://icme2016.org"

(b) The marked QR tag of (a)

Fig. 2. The results of 2-L QR barcode.

(a) The host QR tag with the QR data "QR CODE STEGANOGRAPHY WITH SECRET PAYLOAD ENHANCEMENT …"

(b) The marked QR tag of (a)

Fig. 3. The results of 12-L QR barcode.

Table 1 lists the payloads of the tolerant secret capacity, tc, under different QR versions and error correction levels. According to Table 1, the proposed scheme can embed at

least *tc* secret bits into QR tag. For instance, in QR version 1-L, the new scheme can embed at least 24 secret bits into QR tag (lower bound), and the upper bound of secret payload is 152 bits.

Thus, 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 error correction level and QR version, the larger secret capacity is. Besides, the proposed scheme can achieve the steganography purpose by exploring the characteristic of the error correction capability of the QR tag.

Table 1. The secret payload for different QR versions and error correction levels

QR version	Secret payload, *tc* (bits)			
	L	M	Q	H
1	24	40	48	64
5	104	192	288	352
10	288	520	768	896
15	528	960	1,440	1,728
20	896	1,664	2,400	2,800
25	1,248	2,352	3,480	4,200
30	1,800	3,248	4,800	5,760
35	2,280	4,256	6,360	7,560
40	3,000	5,488	8,160	9,720

Table 2. Overall comparison between the related schemes and the proposed scheme

Methods	**[9, 10]**	**[11, 12]**	**Proposed**
Applications	Image hiding	Image hiding	Secret hiding
Embedding domain	Frequency	Spatial	Spatial
Computational complexity	High	Low	Low
Operation upon QR code	No	No	Yes
Module-based	No	No	Yes
Utilizing the error correction capability	No	No	Yes
Robustness	-	-	High
Secret payload	-	-	Larger than *tc* bits

Table 2 displays the overall comparison between the related schemes [9-12] and the proposed scheme. Unlike the conventional hiding and watermarking schemes [6-12], the new scheme embeds the secret into the modules of QR tag directly [13]. Hence, the secret extracting procedure of the proposed scheme is feasible for barcode readers. The new scheme is 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 larger than *tc* secret bits into a QR tag, as shows in Table 2. Therefore, the proposed scheme can enhance the embeddable secret payload than the recent article [13].

5. CONCLUSIONS

The proposed secret hiding scheme for QR codes can carry higher secret bits than that of the past one as well as preserving the readability of the QR code content because of error correction capability. According to the experimental analysis, the designed scheme is feasible to hide the secrets into a tiny QR barcode as the purpose of steganography. Only the author who has private key can successfully obtain the hidden secrets.

6. ACKNOWLEDGMENT

This research was supported by the Ministry of Science and Technology, Taiwan, under contract No. NSC 102-2221-E-155-035-MY3, MOST 104-3115-E-155-002 and No. MOST 104-2221-E-468-005.

7. REFERENCES

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

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

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

[4] 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.

[5] 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.

[6] D. Buczynski, (2002-09-05), MSB/LSB Tutorial, [Online]. Available: http://www.buczynski.com/Proteus/msblsb.html

[7] S. Katzenbeisser and F. A. Petitcolas, "Information hiding techniques for steganography and digital watermarking," *Artech House, Inc. Norwood*, MA, USA, 2000.

[8] X. P. Zhang and S. Z. Wang, "Efficient steganographic embedding by exploiting modification direction," *IEEE Communications Letters*, vol. 10, no. 11, pp. 781-783, 2006.

[9] C. H. Chung, W. Y. Chen and C. M. Tu, “Image hidden technique using QR-Barcode,” *Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2009.

[10] 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.

[11] 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.

[12] 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.

[13] Y. J. Chiang, P. Y. Lin, R. Z. Wang and Y. H. Chen, “Blind QR code steganographic approach based upon error correction capability,” *KSII Transactions on Internet and Information Systems*, vol. 7, no. 10, pp. 2527-2543, October 2013.

[14] Z. Xing (“Zebra Crossing”), [Online]. Available: http://code.google.com/p/zxing/