Volume 7, Issue 1, January 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on Secret Data Hiding in Quick Response Barcodes

Dini Davis
Department of CSE, Thejus Engineering College,
Vellarakkad, Kerala, India

DOI: 10.23956/ijarcsse/V7I1/0168

Abstract— As the information processing system plays a crucial part in the internet, online information security has become the top priority in all sectors. Failing to provide online information security may cause loss of critical information or someone may use or distribute such information for malicious purpose. Recently QR barcodes have been used as an effective way to securely share information. This paper presents the survey on secret data hiding techniques which can share high security information over network using QR barcode.

Keywords— QR Barcode, Information Hiding, Online information Security.

I. INTRODUCTION

Due to tremendous growth in communication technology, sharing the information through the communication network has never been so convenient. Nowadays information is processed electronically and conveyed through public networks. Such networks are unsecured and hence sensitive information needs to be protected by some means. Cryptography is the study of techniques that allows us to do this. In order to protect information from various computer attacks as well as network attacks various cryptographic protocols and firewalls are used. But no single measure can ensure complete security. Nowadays, the use of internet and sharing information are growing increasingly across the globe, security becomes a vital issue for the society.

Security attacks are classified as passive attacks and active attacks. In passive attacks, attacker monitors network traffic and looks for sensitive information but does not affect system resources. Passive attacks include traffic analysis, eavesdropping, Release of message contents. In active attack, attacker breaks protection features to gain unauthorized access to steal or modify information. Active attacks include masquerade, replay, modification of messages, and denial of service.Therefore, security threats (such as eavesdropping, data modification, phishing, website leaks etc.) force us to develop new methods to counter them. Considering QR barcodes as an effective media of sharing information, many researchers have proposed information/data hiding methods [6,7, 8, 9.] as well as online transaction systems [1,2,3,4,5] using QR barcode. In this paper, we describe different information hiding schemes using QR barcode.

To keep 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 correct access can log into the database and get the confidential data. However, the web link of the back-end database creates a possible risk in which it may attract the intruder's attention. Chuang et al. 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 system is also unable of preventing cheaters in its real world application.

A dependable distributed secret storage system with the QR code can be used in important applications, such as offering secret organization and authorization in e-commerce. Based on our observations, our aim was to design a distributed secret sharing scheme based on the QR barcode, thereby allowing a secret to be split into pieces and shared between individual QR-tag owners to ensure the privacy of the QR data. The secret data can be revealed when qualified QR-tag owners help. Recently, most QRrelated study has used the conventional image hiding method or the conventional 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 unique domain or the frequency domain of a cover image.

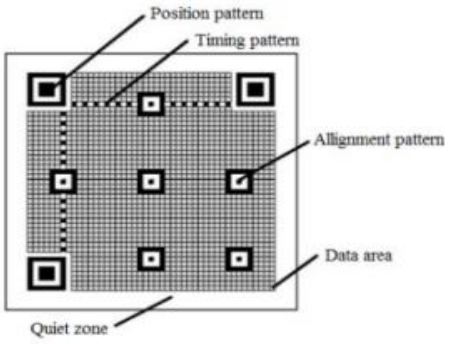

Fig.1: Structure of a QR barcode

Hence, the secret payload of such schemes is equivalent to the QR data. These schemes do not activate on the QR tag directly, so they are unable of allowing the practice of hiding/reading the secret into/from the QR code directly.

II. SECRET INFORMATION HIDING

In this section, we will introduce and analyze the confidential data hiding methods using QR barcodes. Some of the well-known information hiding techniques are Using Hash function, SD-EQR and Using reversible data hiding.

A. Using Hash function

The white and black modules indicate the binary values zero and one, respectively. To achieve the secret communication via the QR code, the proposed scheme conceals the secret into the QR code based on the property of error correction capability. Due to the fact that the error correction capability of the QR code can restore the QR content when it suffered dirty or damaged. Table I lists the error correction capability for the four error correction levels, L, M, Q and H.

1. *Secret hiding* : Given a cover QR code with selected error correction level and the secret information S with l bits, the length of l is determined by the error correction capacity of the QR code as

$$l = \text{floor}(e/2 * 8) \quad \text{.....(1)}$$

Here, e is the number of error correction codewords. To enhance the security of S, the encrypted result, S', of S is processed by the hash function, H, with the private key K,

$$S' = H_K(S) = \{si \mid si = 0/1, i = 1, 2, ..., l\} \quad \text{.....(2)}$$

Based on the error correction capability, S' is aimed to be concealed into the QR content and the corresponding error correction codewords. Let C be the total codewords of the QR content and the corresponding error correction codewords. Since a codeword equals to eight modules in the QR barcode system, there are p modules in C (p = C *8).

The S' thereby is conceals into C according to a random number sequence R. The R with length l are generated by the key K,

$$R = \{ri \mid 1 \text{ ri } p, i = 1, 2, \ldots, l\} \quad \text{.....(3)}$$

Here, ri indicates the element of R, and the value of ri is in the range of [1, p]. For each ri, if the ri-th QR module in C is white and si =1, the ri-th QR module is flipped to black. If the ri-th QR module in C is black and si =0, the ri-th QR module is changed to white. Otherwise, the ri-th QR module keeps unchanged. By hiding the si into the ri-th QR module in C, i=1, 2, …, l, the S' afterward can be hidden in the cover QR code to form the marked QR code. The proposed scheme guarantees that at most l modules in the cover QR code can be altered. According to the error correction capability, the QR content of the marked QR code is decodable for a QR reader. Hence, the new scheme can achieve the steganography purpose to reduce the attention of browsers.

2. *Extraction* : The general browsers can only read the QR content from the marked QR code by a QR reader.

The authorized receiver can retrieve the secret S from the marked QR code by the private key K. The extraction procedure is blind. That is, the scheme can reveal the secret by K without original QR code and auxiliary information. Given a cover QR code, the QR version and the error correction level can be decoded by a QR reader. Let the number of error correction codewords be e, the secret capacity l can be computed as

$$l = \text{floor}(e/2 * 8) \text{ bits.}$$

According to the marked QR code, let C be the total codewords of the QR content and the corresponding error correction codewords. There are p modules in C, p = C8. The random number, ri, with length l thereby can be generated by K. The value of ri is in the range of [1, p], i=1, 2, …, l. Subsequently, the receiver can extract the secret bit, si, from the ri-th module in C, i=1, 2, …, l. Finally, the secret S can be reveal by decrypting si's with the hash function, H, and the private key K. The secret extraction procedure is efficient and low computational complexity. The scheme provides secret communication for value-added QR code application that can be practiced to commonly QR code reader and mobile devices.

B. SD-EQR

Encryption techniques are now a very important research field and, every now and then cryptography scientist are trying to come up with a good encryption technique (algorithm) so that no hacker / intruder can interpret the encrypted message. The modern day cryptographic methods are of two types (i) symmetric key cryptography, where the same key is used for encryption and for decryption purpose and (ii) Public key cryptography, where we use one key for encryption and one key for decryption purpose.

Symmetric key algorithms are well accepted in the modern communication network. The main advantage of symmetric key cryptography is that the key management is very simple. Only one key is used for both encryption as well as for decryption purpose. There are many methods of implementing symmetric key. In case of symmetric key method, the key should never be revealed / disclosed to the outside world other the user and should be kept secure. To deal with this problem we have introduced a new method of generating a code from the entered password, which will act as a key. In this present method the key generated from the password will act as first level of security of the encrypted message.

After doing the first level of encryption to the entered message using the symmetric key, many other several encryption techniques are used to encrypt the message further to increase the level of security, and this will make the job of an intruder or hacker nearly impossible to decrypt the encrypted message. At last the encrypted message will be converted to QR Code(s) and then send to the destination (client). Since maximum storage offered by QR Codes is 1,264 characters of ordinary / ASCII text and is only achieved in Version 40, error correction level H.

For this reason if the size of the encrypted message is larger than 1,264 characters then many other QR Codes are generated containing the encrypted message after 1,264 characters and this method is continued until and unless the entire encrypted message is converted into QR Codes.

The different methods used to encrypt the message after the use of symmetric key for first level of encryption are:

(i) The encrypted message is then treated as a large string and the reverse of the string is generated.
(ii) The reverse encrypted string then extracted bit wise and XOR operation is performed with '1' (one) to those bits.
(iii) This will generate another new encrypted message. Then that encrypted message is converted into QR Code(s).

Since QR Codes are good in hiding the message, that is why it can be used to hide the encrypted message in the QR Code. And now to decrypt the message, first one has to know the key (password) or else the encrypted message will be shown and won't get the real message. After the key is entered to reveal the encrypted message the code will be generated and the encryption technique will be reverse processed to get back the original message.

C. Using reversible data hiding

Reversible data hiding is a new branch in data hiding researches. At the encoder, the data are hidden into original image, and output looks very similar, or even identical, to original image. At the decoder, both the hidden data and the original image should be perfectly recovered. There are two major branches in reversible data hiding; one is the histogrambased scheme, and the other is the difference expansion technique.

1. *Background Descriptions of QR Codes* : The QR (quick response) code is a 2-dimensional bar code, created by Japanese corporation Denso-Wave in 1994. It is also standardized by Japanese Industrial Standards (JIS), with the name JIS-X-0510: 1999 QR Code [2]. QR Codes can be easily seen from web pages, or advertisements in posters or newspapers.
   Users can capture the QR code from the newspaper with the mobile phone camera, and the webpage corresponding to the QR code can be accessed instantly. After encoding, the binary image in square shape 135 is produced. The QR code is inserted into the corner of the original image by removing the pixel values at the lower-right portion of the original image.
   The major purpose for the QR codes is for mobile phone users to link to the web page corresponding to the QR code quickly. Most mobile phones can read this code by using the camera on the phone, then the hyperlink information contained in the QR Codes can be deciphered, and the web page can be displayed on the screen of the mobile phone. In comparison with conventional schemes for accessing the homepages with the mobile phones, users need not type the alphanumeric characters in the URL; by capturing the QR
   Code with the mobile phone camera, the webpage can be shown instantly and lots of time for inputting the alphanumeric characters can be saved. However, the QR code still appears in the original image, and hence the degraded quality of image can be expected.
2. *Message Selection and Generation of QR codes* : At the beginning, we select the URL corresponding to the original image. Next, the QR code is produced by the QR code generator, which is available online [14]. Then, the QR code is prepared to be placed at the corner of the original image. On the one hand, if we add the GPS information into the image, users can access the digital map conveniently. On the other hand, if we add the product information into the image, viewers can make evaluations instantly, and such a product shown in the original image may be purchased online subsequently. There is a wide variety in the selection of messages, and the QR code can be produced accordingly to meet the users' needs.
3. *Integration with Reversible Data Hiding* : Once the size of the QR code is determined, say, 135 ,×135 it is ready to be placed at the bottom-right corner of the original image. Thus, pixels in such a region, consisting of the135 ×135 ×8 bits, should be spread into the rest of the original image for reversible data hiding.

III. COMPARISON

Comparing the three methods of secret hiding in Quick Response barcodes the result can be tabulated as :

Methods	Using Hash function	SD-EQR	Using reversible data hiding
Basic Application	Secret hiding	Secret hiding	Image hiding
Computational Complexity	Low	High	Low
Processing On QR code	Yes	Yes	Yes
Utilizing the error correction capability	Yes	Yes	No
Encryption on Data before embedding into QR code	Yes	Yes	No
Hiding Mechanism	Encrypted data embedded into QR Barcode	Encrypted data embedded into QR Barcode	QR barcode of data embedded into cover image

IV. CONCLUSION

The Quick Response barcodes can be used in confidential data sharing. Some techniques employ traditional information hiding mechanisms like hash functions, SD-EQR and reversible data hiding in conjunction with QR barcodes.

SD-EQR performs generation of code from symmetric key, addition of code with each letter, reversing the encrypted message, XOR-ing the encrypted message, QR code generation and data hiding, decryption etc., and it makes the process complex. In Reversible data hiding the cover image is processed instead of confidential data. So, the effective and less complexive method to share confidential data using Quick Response barcodes is using the hash function to make the data more secure.

REFERENCES

[1] Kaushik S., "Strength of Quick Response Barcodes and Design of Secure Data Sharing System" International Journal on Advanced Computing & Science (IJACSA), Dec 2011.

[2] Kaushik S.; Puri S., "Online Transaction Processing using Sensitive Data Transfer Security Model"4th International Conference on Electronics Computer Technology (ICECT), IEEE, April. 2012.

[3] Suresh Gonaboina, Lakshmi Ramani Burra, Pravin Tumuluru,"Secure QR-Pay System With Ciphering Techniques In Mobile Devices" International Journal of Electronics and Computer Science Engineering.

[4] Jaesik Lee, Chang-Hyun Cho, Moon-Seog Jun,''Secure Quick Response Payment(QR-Pay) System using Mobile Device", Feb 2011.

[5] Sana Nseir, Nael Hirzallah, Musbah Aqel, "A Secure Mobile Payment System using QR Code", 5th International Conference on Computer Science and Information Technology (CSIT), 2013.

[6] Pei-Yu Lin, Yi-Hui Chen, Eric Jui-Lin Lu and Ping-Jung Chen "Secret Hiding Mechanism Using QR Barcode", International Conference on Signal-Image Technology & Internet-Based Systems, 2013.

[7] Somdip Dey, Asoke Nath, Shalabh Agarwal, "Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System", International Conference on Communication Systems and Network Technologies, 2013.

[8] Somdip Dey,"SD-EQR: A New Technique To Use QR Codes in Cryptography" Use of QR Codes In Data Hiding and Securing.

[9] 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

[10] "QR Code, Wikipedia", http://en.wikipedia.org/wiki/QR_code [Online] .

