International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 06 | June 2019 www.irjet.net p-ISSN: 2395-0072

A Survey: Secret Sharing Approach with Cheater Prevention on QR Code

Sarika Laiphrakpam[1], Mrs. D. B. Gothawal[2]

[1]ME Student, Dept of Computer Engineering, DYPCOE, Pune, India
[2]Faculty, Dept of Computer Engineering, DYPCOE, Pune, India

---

Abstract - *A QR code is the commonly used two-dimensional (2D) barcode which has high encryption and decryption speed; it is not only restricted to error-correction ability, but also can store large information. QR barcode are used considerably because of their beneficial properties, including small tag, large data capacity, reliability, and high-speed scanning. However the limitation of this is it lacks adequate security protection for private or confidential data. A secret QR sharing approach is to protect the private QR data with a secure and reliable distributed system. The QR code schemes use the QR characteristics to achieve secret sharing and can resist the print-and-scan operation. In the system, the secret has been splitted and conveyed with QR tags in the distribution application, and the system can retrieve the lossless secret with the authorized participants. Using a barcode reader, the general browsers can read the original data from the marked QR tags , and helps reduce the security risk of the secret. The systems approach gives a feasible and provides content readability, cheater detectability , and an adjustable secret payload of the QR barcode.*

Key Words: QR barcode, Secret sharing, cheater prevention, QR characteristics

1. INTRODUCTION

QR code (quick response code) is a type of two dimensional barcode developed by Denso-Wave company in 1994 [1]. QR code is a piece of long multilingual text, a linked URL, an automated SMS message, a business card or just about any information can be submerged into the two-dimensional barcode. The QR code system became popular in the automotive industry due to its high-speed scanning, reliability, greater storage capacity compared to standard UPC barcodes and fast readability. A secret QR sharing approach is to protect the private QR data with a secure and reliable distributed system.

- Barcode - a code consist of a group of printed patterned bars and spaces and sometimes numerals that is designed to be scanned and read the information it contain into computer memory.

Fig-1.1 Barcode

Fig -1.2: QR Code

1.1 QR Code

QR code is a two-dimensional code or a matrix barcode that can be reading multiple ways like QR scanners, mobile phones with a camera, and smart-phones.

Fig- 1.3: Overview of QR Code and working.

The QR Code, Information is encoded in both direction i.e. Vertical and horizontal respectively, thus it holds hundred times additional data than a traditional bar.

There are two types of QR Codes.

1. ONLINE CODES
2. It point to an Internet addresses and trigger a client / server interaction that requires an active Internet connection. This involves the access of a mobile website and the sending of an SMS message.

2. OFFLINE CODES

The name itself suggests that these codes do not need an Internet connection. It directly resolved on the phone.

Two-dimensional symbols generally contain much more data mounted on; it is compared with linear symbols and thus requires much longer data processing time and more complex process. Therefore, QR Code has much more consideration for its finder pattern to enable high-speed reading.

QR Codes have overtaken the popularity of classical barcode in many areas. The key fact about typical barcode is that it can hold maximum of 20 digits only, which is overcome by QR code as it can hold up to 7,089 characters.

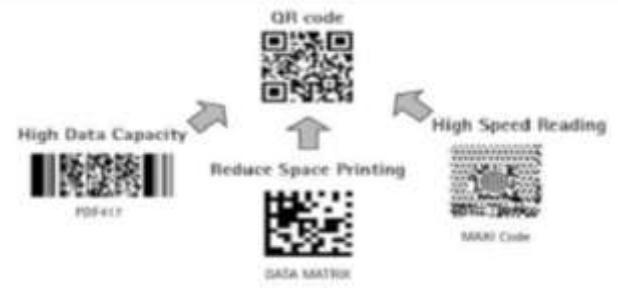

Fig-1.4: - The development of QR code.

QR Codes has the capability to encode same amount of data approximately in one tenth the space of a traditional 1D barcode. A great feature of QR Codes is that they do not need to be scanned from one particular angle, as QR Codes can be read regardless from any position respectively.

The most popular and commercial use for QR Codes is in the telecommunications industry, where the increasing in the adoption of smart-phones seems to be the biggest driver of its popularity. QR Codes seem to be a suitable tool for quick and efficient communication URLs to users.

1.2 Characteristics of QR code

- All-Direction (360^0) High-speed Reading-
  Reading in all directions (360^0) the ratio between black and white among the scan line that runs through the finder patterns is always when seen from any direction among the 360° surrounding it.

- Resistant to Distorted Symbols-
  Symbols often get distorted as soon as they are attached to a curved surface i.e. angled CCD sensor face and the symbol face. To spot this distortion, QR Code has alignment patterns arranged with a regular interval within the range of the symbol.

- Data Restoration Functionality (Resistant to smudged or damaged symbol):-
  QR Code has four different error correction levels 7%, 15%, 25% and 30% that depend on symbol area. The error correction functionality is implemented according to the smudged/damage, and it is utilizing the code which is highly resistant to error.

- Linking Functionality of the Symbols:-
  A single symbol is represented in several symbols on dividing it by using linking functionality. A single symbol can be divided at maximum into 16 symbols.

- High Capacity Encoding of Data:-
  QR Code is efficient to handle all types of data, like numeric and alphabetic characters, Kanji, Kana, Hiragana symbols, binary, control codes and etc. In one symbol up to 7,089 characters can be encoded.

- Small Printout Size:- Since QR Code carries information both horizontally and vertically, QR Code is capable of encoding the same amount of data in approximately one-tenth the space of a traditional bar code.

2. LITERATURE SURVEY

Different from the conventional QR application, the purposed approach utilizes the characteristics of QR modules to satisfy the essential of steganography, readability, robustness, adjustable secret capability, blind extraction, cheater detection, and identification for secret sharing mechanism[1]. The QR sharing system can achieve satisfactory performance when compared to related attempts.

[2] In this paper, a security system for QR codes that guarantees both users and generators security concerns is implemented. The system is reverse compatible with present standards that are used for encoding QR codes. The system is implemented and then tested by using an Android-based smart-phone. The system introduces a small overhead in terms of the delay that is required for integrity verification and content validation.

[3] Security has become extremely important in the digital society. Authentication process should be seriously examined by services that store sensitive information. Most of the users have android smart phones. The Smart phones have good memory size as well as good processing power too. As a mobile phone has become an essential accessory in real life, compared with the traditional key or access card. Sending the authentication by using mobile phones through MMS (Multimedia Messaging Service) allows the user to carry objects but not any extra specific hardware cost. Using QR Code successful authentication can be done.

[4] 2LQR code has two levels: a public level and a private level. The public level can be read by any QR code reading application, while the private level needs a specific application with specific input information. 2LQR code can be used for private message sharing or for authentication scenarios. The private level is created by replacing black modules with Specific textured patterns. These textured patterns are considered as black modules by standard QR code reader. Thus the private level is invisible to standard

QR code readers. In addition, the private level does not affect in anyway the reading process of the public level.

[5] The paper refers the authentication problem of real-world goods on which 2D bar-codes (2D-BC) were printed and we take the challengers view. The challengers are assumed to have access to noisy copies of an original 2D-BC. A simple estimator of the 2D-BC is depends on copies averages is proposed, letting the challengers print a fake 2DBC with as original by the system detector. Performance of the estimator in terms of error probability at the detector side is then derived with respect to Nc and compared with experimental results on real 2D-BC. It is shown that the adversary can produce a fake that successfully fools the detector with a reasonable number of genuine goods. Advantage: Create a fake 2D-BCs declared as genuine by the detector. Disadvantage: Require additional noise to generate fake barcode. Generating fake 2D QR code declared as original by QR code reader.

3. SYSTEM ARCHITECTURE

The system used a secret (n,n)-Threshold QR code sharing approach ,the 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 system, a dealer and n participants exist, where n ≥ 2. [1] So the dealer is responsible for splitting the secret into n marked QR tags. And the n marked QR tags can be distributed to the n corresponding participants. The authorized QR tags with n participants only are qualified to obtain the shared secret, and no subset of less than n tags can leak any information about the secret.[1]

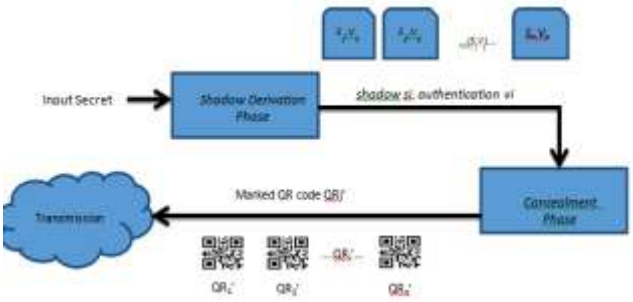

Fig -3.1. Architecture for System

Assume that QR_i are the n covers of QR barcodes with the same QR version and error correction level, i=1, 2, 3…., 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]

Here the input secret data is handled by Shadow Derivation Phase where secret data is split into bundle of 2, first is shadow i.e. s_i and second is authentication v_i and so on. Later this set of (S,V) are pass to the next phase i.e. to Concealment Phase and here QR code is marked and concealed by applying the wet paper codes(WPC)Algorithm and then finally these set of $QR_{n'}$ is send for transmission.[1]

Shadow derivation phase:

Step 1: derive the master key K

Step 2: Generate n authentication streams

Step 3: Generate (n-1)random binary shadows

Step 4: Derive the n-th binary shadow.

A reliable distributed secret storage system with the QR code can be applicable in some applications, such as authorization in e-commerce (like e-coupon and e-ticket) and the distributed secret sharing. Recently, most QR-related research has used the traditional watermarking technique or the traditional image hiding manner without utilizing the characteristics of the QR barcode. These schemes do not operate on the QR tag directly, so they are not capable of the practice of hiding/reading the secret from the QR code directly. In real-world applications, the capability of detecting the cheaters is a significant requirement before the secret data are revealed.

Algorithms

Steganography Algorithm:

1) Creating a QR Code

Step 1: Data Analysis

Step 2: Data EncodinG

Step 3: Error Correction Coding

Step 4: Structure Final Message

Step 5: Module Placement in Matrix

Step 6: Data Masking

Step 7: Format and Version Information

Encoding:-

Representation of each letter in secret message by its equivalent ASCII code.

- Conversion of ASCII code to equivalent 8 bit binary number.
- Division of 8 bit binary number into two 4 bit parts. Choosing of suitable letters corresponding to the 4 bit parts.
- Meaningful sentence construction by using letters obtained as the first letters of suitable words.
- Omission of articles, pronoun, preposition, adverb, was/were, is/am/are, has/have/had, will/shall, and would/should in coding process to give flexibility in sentence construction.
- Encoding is not case sensitive.

Decoding

Steps:

- First letter in each word of cover message is taken and represented by corresponding 4 bit number.

- 4 bit binary numbers of combined to obtain 8 bit number.
- ASCII codes are obtained from 8 bit numbers.
- Finally secret message is recovered from ASCII codes.

ADVANTAGE:

1. The key advantage of the QR code is its versatility.

2. Relatively small in size. These codes are designed small in size than the information they contain.

3. Very quick transfer of information.

DISADVANTAGE:

1. One disadvantage of QR codes and perhaps it is the biggest problem that the lack of familiarity of the QR code among people.
2. Another major disadvantage of a QR code is codes dependability on a mobile device or smart-phone.
3. Security issues. The transfer of data between two devices can always lead to security issues.

4. CONCLUSIONS

Compared with the different conventional QR application, the system utilizes the characteristics of QR modules to satisfy the essential needs of steganography, readability, robustness, secret capacity, blind extraction , cheater detection and identification for the sharing mechanism. Also the QR code security is essential and QR codes are increasingly used in all life fields, this system can protect users' privacy and identity in addition to their smart phone devices. The proposed secure QR code application provides more security level as well as maintains backward compatibility with QR codes that do not incorporate security features. Even if the QR code does not contain digital signature, the application can still verify online contents and malicious contents. However, it will warn the user about that before giving the users the choice to continue or not.

In the future, can extend the work for other barcode types, enhance the implementation and add more security features.

REFERENCES

[1] Pei-Yu Lin" Distributed Secret Sharing Approach with Cheater Prevention based on QR Code" 2016 IEEE.

[2] Raed M. Bani-Hani, Yarub A. Wahsheh, Mohammad B. Al-Sarhan."Secure QR Code System" 2014 IEEE.

[3] Ms. Dhanashree Patil, Mrs. Shanti. K. Guru. "Secured Authentication using Challenge-Response and Quick-Response Code for Android Mobiles" 2014 IEEE.

[4] William Puech, ChristopheDestruel, Olivier Strauss, Jean-Marc Gaudin, and Christian Guichard" Two level QR code for private message sharing and document authentication" 2016 IEEE.

[5] C. Baras and F. Cayre, "2D bar-codes for authentication: A security approach," in Proc. 20th Eur. Signal Process. Conf. (EUSIPCO), Aug. 2012, pp.1760–1766.

[6] T. V. Bui, N. K. Vu, T. T. P. Nguyen, I. Echizen, and T. D. Nguyen, "Robust message hiding for QR code," in Proc. IEEE 10th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIH-MSP), Aug. 2014, pp. 520–523.

[7] Hsiang-Cheh Huang, Feng-Cheng Chang, and Wai-Chi Fang." Reversible Data Hiding with Histogram-Based Difference Expansion for QR Code Applications" 2011 IEEE.

[8] Yang-Wai Chow, Willy Susilo , Joseph Tonien , Elena Vlahu-Gjorgievskaand Guomin Yang" Cooperative Secret Sharing Using QR Codes and Symmetric Keys" Symmetry 2018.

[9] Jun-Chou Chuang, Yu-Chen Hu &Hsien-JuKo." A Novel Secret Sharing Technique Using QR Code" International Journal of Image Processing (IJIP), Volume (4) : Issue (5).

[10] Prof. PallaviTekade , RutujaMhaskar , PriyaSurywanshi , AishwaryaShirgurkar , AniketPanmalkar , Rohit Patil." QR Code Implementation in Car Parking Locator" International Journal of Innovative Research in Computer and Communication Engineering. Vol. 5, Issue 3, March 2017.