Technique to Hide Encrypted Data in QR Codes using EK-EQR Algorithm

Neeraj Naik
Department of Computer Engineering
Sinhgad Academy of Engineering
Pune,India

Niraj Kadam
Department of Computer Engineering
Sinhgad Academy of Engineering
Pune,India

Manish Bhalekar
Department of Computer Engineering
Sinhgad Academy of Engineering
Pune,India

ABSTRACT

There are various types of information which being transferred from the known source to required destination. The data that is being transferred can be confidential which should be handled with much care. The transferring of data can be done using various technique and numerous types of algorithms. QR code is one of the technique which can be used to transfer the data with maximum amount of security being involved. In this paper the author present a new technique of data encryption method using QR code. The ideology of this method is to encrypt the data by using the concept of EK-EQR algorithm. This data hiding technique can be used in various government sectors for data transfer.

General Terms

Information, Maximum, Confidential, Technique

Keywords

Encryption, QR Code, EK-EQR algorithm, EQR Algorithm, Data Hiding

1. INTRODUCTION

Quick Response Code, commonly abbreviated as QR code started out as an extension of standard UPC barcode mostly used in retail and production areas. It is a 2-D matrix code that conveys information by the arrangement of its dark and light elements organized in the form of columns and rows.

The QR code itself is simply an array of bits to be identified by scanner. Bits are reserved for the scanner to be able to identify and orient the image. The remaining bits are used for encoding the image and the specific amount of space leftover is dependent on the version of QR code[2] which indicates the number of bits per row/column and the level of error correction which introduces redundancy. Most of the QR codes used today can store information just under 3000 bytes of raw data.

This paper is divided into various Sections:- Section II explains about the related work in the form of block diagram. Section III gives proper description about the generation of QR code and its features whereas in Section IV and V is about the Encryption and Decryption of data using EK-EQR algorithm. In Section VI, the results is being obtained and Section VII and VIII contains the concluding contents of the paper.

2. RELATED WORK

Initially we are using QR code for authentication of identity of user for online transaction. We are hiding user-id in QR code[2]. Identity of user is very sensitive data, so we have to encrypt that data before hiding it in QR code. For this process, we are using EK-EQR algorithm. EK-EQR algorithm stands for Encrypted key – Encrypted QR algorithm. Primarily we are taking DATE factor for key which will be in any format and it will be encrypted by modified EQR algorithm. Once we get key in encrypted form, later it will be used in encryption of user-id. So this process will be double encrypted and cipher data of user-id will change daily as DATE factor is used as key. Now in decryption process, we have to encrypt DATE factor again to get 'key' which will be used for decryption of cipher form of user id.

Block Diagram:

Encryption Block

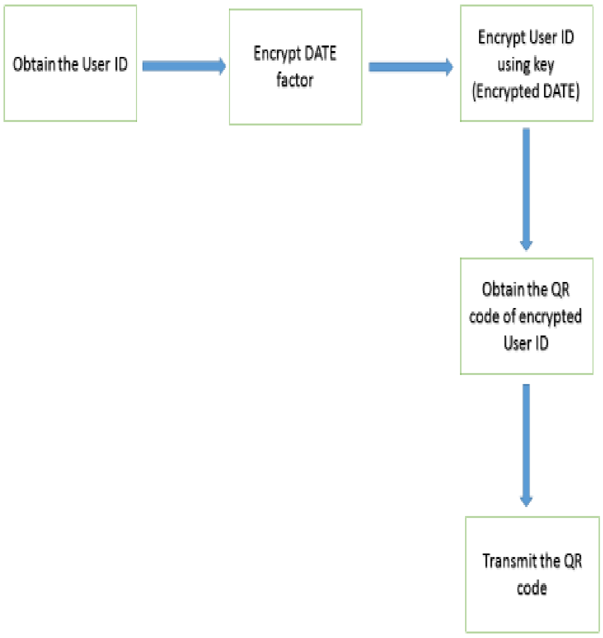

Obtain the User ID
Encrypt DATE factor
Encrypt User ID using key (Encrypted DATE)
Obtain the QR code of encrypted User ID
Transmit the QR code

Figure 1: Block diagram for encryption using QR code method

Decryption Block

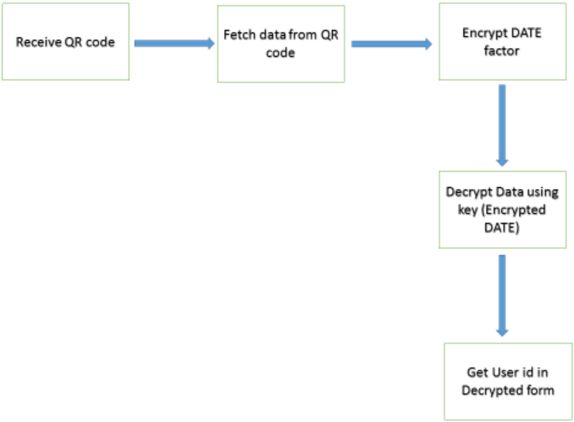

Receive QR code
Fetch data from QR code
Encrypt DATE factor
Decrypt Data using key (Encrypted DATE)
Get User id in Decrypted form

Figure 2: Block diagram of decryption using QR code method

3. QR CODE AND ITS FEATURES

QR code is meant to be read by machines not humans, so there is only a certain amount of information we can interpret by just looking at it. Although each code is different, they contain a few interesting, common features[3].

QR codes are normally encoded in plaintext. A QR code must contain certain parts to be easily decoded. In this section it will show the Anatomy of a QR Code[8]. QR code breaks down in the different parts. There must be the four main squares in a QR code two in the upper corners, one in the lower left corner and a smaller one near the lower right corner which contains information about the alignment pattern. There also must be white space around the outside of the QR code. This is called the quiet zone.

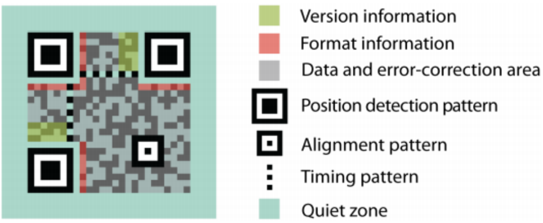


Figure 3: Structure of QR code

Above labelled diagram showing the key features of QR codes, including the finder, timing, and alignment patterns and data cells.

Quiet zone: It is an empty white border that makes it possible to isolate the code from among other printed information.

Finder patterns: Large black and white squares in three of the corners make it easy to confirm that this is a QR code.

Alignment pattern: This ensures the code can be deciphered even if it's distorted or viewed at an angle, printed on a curved surface.

Timing pattern: It runs in horizontally and vertically direction between the three finder patterns and consists of alternate black and white squares. This makes it easy to identify the individual data cells within a QR code and is especially useful when the code is being damaged or distorted.

Version information: There are various different versions of the QR code standard. This information simply identifies which one is being used in a particular code[9].

Data Area: Each individual black or white square that's not part of one of the standard features contains some of the actual data in the code.

3.1 Features Of Qr Code

1. High Encoding Capacity

QR Code is capable of handling hundred times more data than conventional barcode[3]. Conventional barcode has capacity to store maximum 20 digits. In case of QR Code it can store up to 7,089-Numeric, 4,296-Alphanumeric, 2,953-Binary/byte can be encoded in one symbol.

2. Small Size

QR Code[2] stores information in both horizontal and vertical fashion. It is capable of storing the same amount of information in one-tenth the space of a conventional barcode.

3. Dirt and Damage resistant capability

QR Code[10] has four different error correction levels, detailed as follows-:.

- L - Allows recovery of up to 7% damage.
- M - Allows recovery of up to 15% damage
- Q - Allows recovery of up to 25% damage
- H - Allows recovery of up to 30% damage

The error correction level can be selected by the user when he creates the symbol depending on how much damage the QR code is expected to suffer in its usage environment.

4. ENCRYPTION

Encryption changes data or information which is in the form of plaintext through the usage of an algorithm so that someone must possess certain knowledge to access it[1]. This special knowledge is normally called a key. Encrypted QR codes are the codes that cannot be scanned and accessed by every individual. They are not very common, since most QR codes are used in marketing, and the developers of those codes want them to be accessible by everyone.

We are using EQR algorithm for hiding data before encoding in QR code. In this algorithm we are using symmetric key method means same key will be used for encryption and decryption both.

Encryption[6] in EK-EQR algorithm has two steps

1. Encrypt DATE factor.
2. Encrypt User ID with key-encrypted DATE factor

4.1 Encrypt Date Factor

Formula:

A. Creating Key

Let’s take d = today’s date in any format

SD = sum of all digits in date

Assume today’s date is 10/10/2016

So d = 10102016 (you can arrange date numbers in any format to make it more secure)

If you are using text formatted date like 10 October 2016, then use ASCII values of text in d.

Also we can have a private password include in DATE factor.

E.g. DATE factor = 10 abc October 2016

Here password = abc

d = ASCII (10 abc October 2016)

But in current example we are considering d=10102016

SD = 1+0+1+0+2+0+1+6 =11

Now we will generate new number N, where

N =Sum of ((for all single digits from d) d[i] x (SD^2))

SD^2 = 11^2 =121

So, N = 1x121 + 0x121 + 1x121 + 0x121 +2x121 + 0x121 + 1x121 +6x121

N=1331

Now, code = sum of all digits of N

Code = 1+3+3+1 = 8

This code = 8 is key for encryption of DATE factor

B. Convert Date To Unicode
Let d1, d2, d3, d4, d5, d6, d7, d8… be date (10/10/2016) numbers.

Value = (code^2) + i + di

Here 'i' is position of digit in date

Unicode (di) = '&#Value;'

Unicode (1) ='&# (8^2+1+1);' = '&#66;'

Unicode (0) ='&# (8^2+2+0);' = '&#66;'

Unicode (1) ='&# (8^2+3+1);' = '&#68;'

Unicode (0) ='&# (8^2+4+0);' = '&#68;'

Unicode (2) ='&# (8^2+5+2);' = '&#71;'

Unicode (0) ='&# (8^2+6+0);' = '&#70;'

Unicode (1) ='&# (8^2+7+1);' = '&#72;'

Unicode (6) ='&# (8^2+8+6);' = '&#70;'

So all Unicode's generated are '&#66;', '&#66;', '&#68;', '&#68;', '&#71;', '&#70;', '&#72;', '&#70;'

Thus final result is

'BBDDGFHF' this is Unicode form.

This Unicode form of result will be used as "Key"

For encryption of User ID.

4.1.1 Encrypt User Id

Here we are performing EQR algorithm on User ID by using above encrypted key[4].

A. Generate Code From Symmetric Key

Now we already have key "BBDDGFHF" got it by encryption of DATE factor.

Now we have to find out length of key and stored it in 'dlen'

Formula:

Let D1, D2, D3…..Ddlen be key where each Di (i=1 to i=dlen) is a letter of key

N = (for i=1 to i=dlen) (sum of) (Di * (dlen ^2))

Here our key is 'BBDDGFHF'

N = 66*(8^2) + 66*(8^2) +68*(8^2) +68*(8^2) +71*(8^2) +70*(8^2) +72*(8^2) +70*(8^2)

N=80064

Now code = sum of all digits of N

Code = 8+0+0+6+4

Code =18

B. Convert To Unicode

Formula:

Let "L1L2L3L4L5….Ln" be the User ID which we are going to encrypt[4].

Value = Code + ASCII (Li)

Unicode (Li) = '&#Value;' where i=1 to i= n

Now, we have code = 18 from previous method.

Let User ID = 'ABC123'

So after adding code.

Code+ ASCII (A) = 18 +65 =83

Code+ ASCII (B) = 18 +66 =84

Code+ ASCII (C) = 18 +67 =85

Code+ ASCII (1) = 18 +49 =67

Code+ ASCII (2) = 18 +50 =68

Code+ ASCII (3) = 18 +51 =69

So here we have '&#83;', '&#84;', '&#85;', '&#67;', '&#68;', '&#69;'

And final Unicode form result is

'STUCDE" (in Unicode)

C. Reverse Encrypted Data

In this method, to make harder for hacker to interpret data we are going to reverse the encrypted string.

'STUCDE'

Will get converted to 'EDCUTS'

D. Do Ex-Oring Encrypted Data

Now we will perform ex or on encrypted data.

First, we convert it to binary.

01000101 01000100 01000011 01010101 01010100 01010011

After EX OR

10111010 10111011 10111100 10101010 10101011

10101100

Means final encrypted data that we got

º»¼ª«¬

5. DECRYPTION

To decrypt data[6], we have two steps.

1. Encrypt DATE factor
2. Decrypt cipher text using key

5.1 Encrypt Date Factor

We have already seen encryption of DATE factor. We have to follow same procedure. As we are using symmetric key, we need same key for decryption of cipher data. So to create same key we encrypt DATE factor again.

5.2 Decrypt Cipher Text using Key

In decryption procedure[1], we use reverse engineering mechanism so we will get original data. Decryption can be done only using same key which was used at time of encryption. When QR code scanner scans QR to generate encrypted data and then it will process for decryption. Reverse engineering of all steps will leads to original data.

6. RESULTS

Now we summarized full encryption and decryption again.

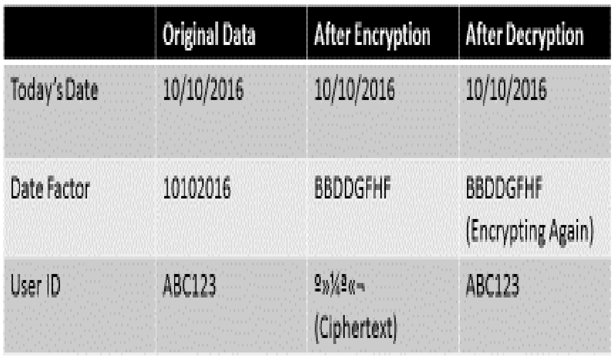
Today’s date: 10 /10 /2016

DATE factor: 10102016

Encrypted DATE factor: ‘BBDDGFHF’

User ID: ‘ABC123’

Encrypted User ID: ‘º»¼ª«¬’



	Original Data	After Encryption	After Decryption
Today’s Date	10/10/2016	10/10/2016	10/10/2016
Date Factor	10102016	BBDDGFHF	BBDDGFHF (Encrypting Again)
User ID	ABC123	º»¼ª«¬ (Ciphertext)	ABC123

So, finally we have successfully developed EK-EQR algorithm.

7. CONCLUSION

In today’s world, due to the development in the technology sector majority of the transactions are being done through online system. QR Code is one of the technique which has various advantages as an information sharing and securing tool. The inclusion of QR Code adds another level of security through data encryption method and the receiver at the other end can access the original data in the QR Code quickly and efficiently by just scanning and decrypting it with the appropriate software. This paper describes the EK-EQR Algorithm in which the data is being hidden into the QR Code by Encryption and Decryption Algorithm with the DATE factor and User ID with key-encrypted. This method has a very large scope. Future scope of this technique is big and can also be implemented in daily life use, but, the use of this technique in reality depends and varies from user to user.QR Code[5] can replace multiple system such as Smart Card, Swipe Cards, Secure way of Transaction, Cash Cards etc. These all Systems require special scanner and Machines for transferring the money. To overcome these weaknesses, QR code techniques introduced into one time password protocol. As most internet users already have smart phones above proposed schemes based on QR code eliminates usage of password verification as well as cost effective solution.

8. REFERENCES

[1] Vanishree and Sunitha,”Encryption and decryption of data using Quick response code”, ISSN (Online): 2347 - 2812, Volume-2, Issue - 3, 2014.

[2] Kevin Peng, Harry Sanabria, Derek Wu and Charlotte Zhu, “Security Overview of QR Codes”, Massachusetts Institute of Technology 6.857 Computer and Network Security,E-Book

[3] Nikita Gupta, Nagesh Mokashe and Mangesh Parihar, “QR code: A safe and secure method of authenticating legal documents,” International Journal of Engineering Research and General Science Volume 3, Issue 1, January-February, 2015.

[4] Somdip Dey, “SD-EQR:A New Technique To Use QR Codes TM in Cryptography”, International Conference on Emerging Trends of Computer & Information Technology (ICETCIT 2012) – India.

[5] Jaesik Lee, Chang-Hyun Cho, Moon-Seog Jun,’’Secure Quick Response Payment(QR-Pay) System using Mobile Device”, Feb 2011

[6] 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.

[7] 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. [

[8] Dante D’Orazlo. Google experiments with new QR-based secure login. The Verge. 17 Jan 2012. Web. 14 May 2014

[9] T. Falas and H. Kashani, “Two-dimensional barcode decoding with camera-equipped mobile phones”.

[10] Eisaku Ohbuchi, Hiroshi Hanaizumi, Lim Ah Hock,” Barcode Readers using the Camera Device in Mobile Phones”, IEEE paper.