IJMEIT
IGM Publication
International Journal Of Mechanical Engineering And Information Technology
An Official Publication Of IGM Publication

Secure Communication Using Cryptic QR Codes

Authors

Shruti Ahuja, Rajiv Mishra
CBS Group of Institutions, Jhajjar
Email: *shrutiahuja10@gmail.com, mishrarajiv99@gmail.com*

Abstract

Quick Response Code is two-dimensional barcode that stores just about any variety of knowledge. QR codes have gained quality in client advertising as a result of its quick readability and enormous storage capability as compared to the barcodes. QR codes are normally found on websites, product packaging, TV advertisements, posters and newspapers. As the mobile technologies are become increasingly prominent in various parts of the world, so it the process of mobile tagging with Quick Response codes. If any QR code comprises of private information or important data then security risk becomes a major problem. AES it is a symmetric key encryption key technique. When a sender wishes to send some confidential text to a receiver, he can encrypt the QR code using AES algorithm.

Keywords: Barcodes, QR codes, Mobile tagging, AES

Introduction

To decode, users merely require a smart phone and a QR code reader application.

1. Accessing URL's: It saves the users from the hassle of typing the website address. The QR reader application detects the URL and automatically launches the web browser and redirects the users to the website.

2. Triggering Application Launch: Smart phones have a collection of basic functions like contacts, calendar, email, SMS and Internet browsing etc. When a QR code is scanned, it triggers that particular function on the user's device. Like when a QR code comprising of any calendar event is scanned, it prompts the user to launch the calendar and save that particular event as a reminder.

3. Coupons and Marketing: QR code coupons are beneficial in attracting customers by offering then various discounts and potential and marketing promotions simply by using their Smart phones. Customers simply need to scan a QR code and save the coupon image in their Smart phone and can redeem by showing the image while billing to avail discounts.

4. Display information: It is beneficial to the user as he can obtain the information of his interest simply by scanning a QR

code. Information comprised in a QR code can be maps, restaurant menus, images, product information etc.

URL
Text
Email Id
SMS
Contact
YouTube
Wi-Fi
Geo Location

Fig 1.Different nature of QR codes that can be decoded by using QR code reader application

QR CODE Structure

QR code was developed by Denso Wave in 1994. It is a two dimensional matrix symbol .It comprises of data in x and y axis but has no height as it is two dimensional in nature. Figure 1 shows the structure of QR code. It comprises of various zones and each zone has its own function.

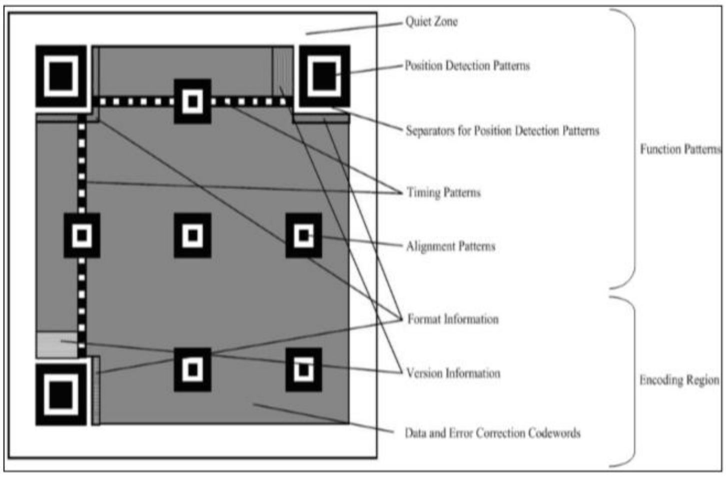


Fig 2. Basic structure of QR code [3]

Features of QR Codes [2]-

Various features of QR codes are as follows:-

1) QR Code holds quiet a greater amount of information than contained in a bar code.

2) It is capable of handling various types of data like Kanji, control codes, binary, numeric, alphabets, and alphanumeric characters.

3) Since QR Code are two dimensional in nature so it takes very less space approximately one – tenth of the traditional barcode in encoding same amount of data.

4) QR Codes are Omni-directional in nature and can be processed at high speed. This is accomplished by using position detection patterns which are located at the three designated corners of the symbol.

5) QR codes are not limited to Computer scanners. Even a smart phone can be used as a QR code reader.

6) QR Codes can be easily decoded by Denso wave. The Denso wave specification is available as Open Source, enabling users to easily encode and decode a QR code using freeware.

How to Create QR Codes

A QR code can be created using few steps as follows:

1. Search for a QR Code Generator: QR code generator can be found either online or can be downloaded as an application in smartphones .Few common QR code generators are QR Stuff, Kaywa and Zxing Project.

2. Content: Type the information to be encoded. QR code can be have any type like URL, text, SMS, contact, Email Id etc. Once the text is entered click on generate code button.

3. Formatting: Once a QR code is generated it can be formatted by using various formatting options like changing its colours or size, overlaying any log, embedding an image inside a QR code etc.

4. Test: Once the QR code is generated one should ensure that it works well. If something is wrong then it needs to be fixed. So it should be tested properly before making it available for public.

5. Publish: After testing the QR code should be saved and can be used in printed media.

Proposed authentication scheme

The user will be able to generate a QR code using text option .Under “Text” option, the user will input some text that needs to be hidden inside the QR code. After that, the user will be prompted for encrypting the QR code. If the user selects “Yes”, he is required to enter password in order to encrypt the QR code. Once the password is inputted, the encrypted QR code shall be generated. If the user selects “No”, the QR code will be generated without a password and displayed on the screen. When a sender wishes to send some confidential text to a receiver, he can encrypt the QR code using AES algorithm .The decryption of the encrypted QR code is feasible only if the receiver knows the right password. AES stands for Advanced Encryption Standard technique , it is a public key encryption algorithm. This algorithm was developed by Belgian cryptographers Joan Daemen and Vincent Rijmen and is based on Rijndael cipher.

AES is efficient in both hardware and software .Also it supports a block size of 128 bits and three key lengths of 128, 192 and 256 bits. AES is not being implemented explicitly, rather the built in API's are performing the task of encrypting the QR codes. It works on 4×4 matrix of bytes, termed as *state*, some versions of Rijndael may have a larger block length and few additional columns in the state. Calculations are mostly performed within a special finite field.

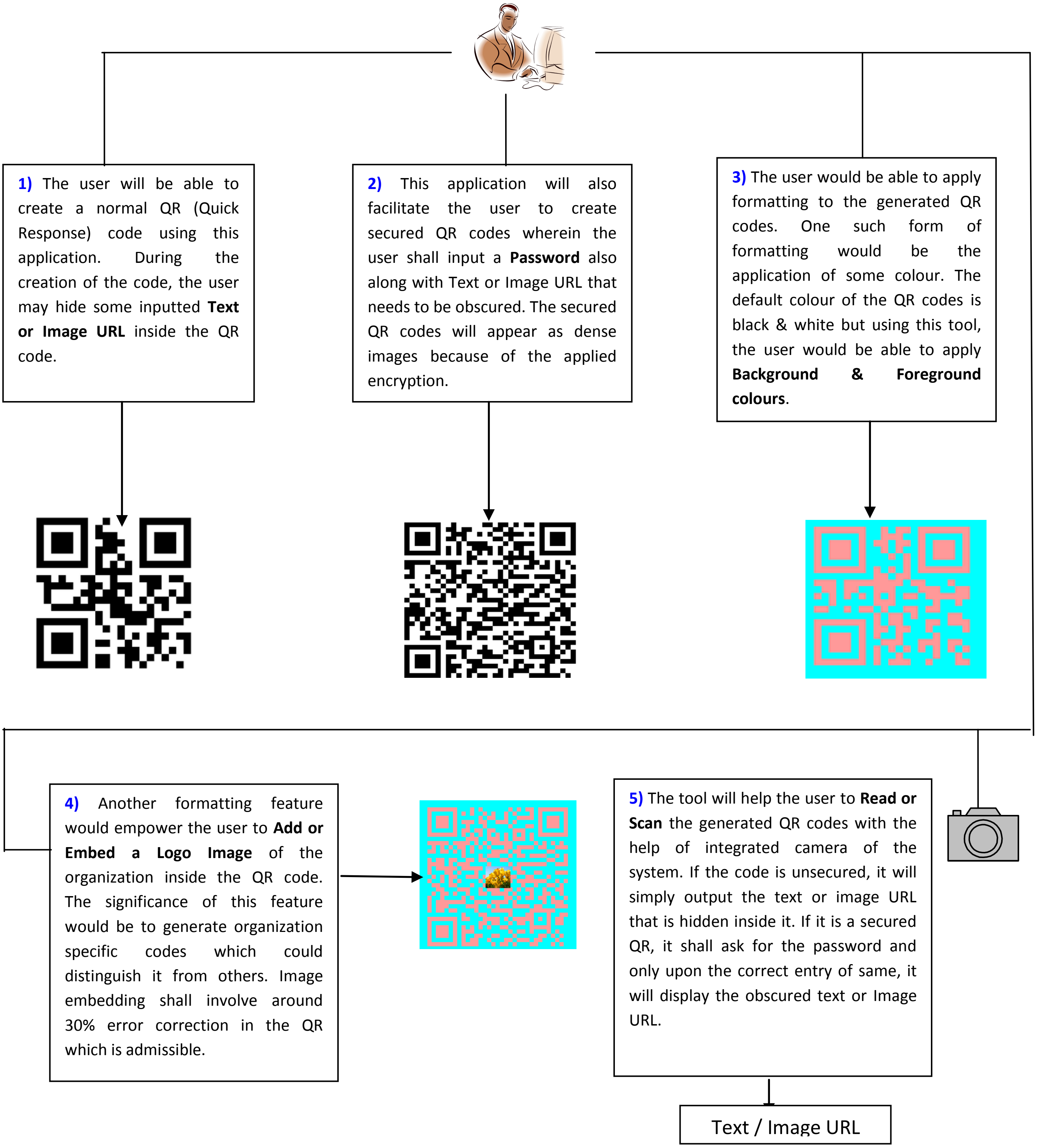
Once a QR code is generated, it will be displayed on the screen as well as saved as an image file at a specific destination folder/directory within the hard drive of the user PC. After the QR code is generated, the user will be able to scan it through the "Scan" option present in the application. If the QR code is encrypted, it will ask for a password for decryption on the PC screen. Once the correct password is inputted, it will show the text or URL that is hidden inside the QR code. But if the QR code is not encrypted, it won't ask for a password and upon "Scan", it will directly show the text or URL hidden inside it.

"QR Customization" options are present in the application namely,

a. Apply Colour
b. Add Logo

a. If the user selects "Background" or "Foreground" button , he would be able to change the colour of the QR code using a multicolour palette. This feature will not make any changes to the data hidden inside the QR code. The user could still scan the QR code perfectly after this customization.
b. If the user selects "Apply Logo", he would browse an image that needs to be embedded inside the QR code so that it is visible as a tiny image in the QR code. This feature too will not make any changes to the data hidden inside the QR code. The user could still scan the QR code perfectly after this customization.

The diagram given below depicts the Workflow of proposed authentication scheme.



1) The user will be able to create a normal QR (Quick Response) code using this application. During the creation of the code, the user may hide some inputted **Text or Image URL** inside the QR code.

2) This application will also facilitate the user to create secured QR codes wherein the user shall input a **Password** also along with Text or Image URL that needs to be obscured. The secured QR codes will appear as dense images because of the applied encryption.

3) The user would be able to apply formatting to the generated QR codes. One such form of formatting would be the application of some colour. The default colour of the QR codes is black & white but using this tool, the user would be able to apply **Background & Foreground colours**.

4) Another formatting feature would empower the user to **Add or Embed a Logo Image** of the organization inside the QR code. The significance of this feature would be to generate organization specific codes which could distinguish it from others. Image embedding shall involve around 30% error correction in the QR which is admissible.

5) The tool will help the user to **Read or Scan** the generated QR codes with the help of integrated camera of the system. If the code is unsecured, it will simply output the text or image URL that is hidden inside it. If it is a secured QR, it shall ask for the password and only upon the correct entry of same, it will display the obscured text or Image URL.

Text / Image URL

Fig. 3 Workflow of proposed authentication scheme

Conclusion

In this paper we have proposed an authentication scheme for sending QR code from sender to receiver. In recent years there has been a steep increase in the number smart phone users. The QR code proves out to be very versatile at the same time beneficial for both sender as well as receiver as in terms of security and exchange of confidential information. AES technique is comparatively stronger against differential, truncated differential, interpolation and Square attacks. Of course, the key length is also very important, especially as the most efficient attack known against Rijndael is the one with an exhaustive key search. It would take around 2^{255} runs of Rijndael in order to find a key 256 bits long. By far AES is one of the most secure way to exchange confidential data.

References

1. The Expectations of Quick Response (QR) Codes in Print Media: An Empirical Data Research Anthology,Ali Probst , UW-L Journal of Undergraduate Research XV (2012)
2. Using Mobile Phones and QR Codes for Formative Class Assessment Hitoshi Susono, Tsutomu Shimomura Faculty of Education, Mie University, Japan, Current Developments in Technology-Assisted Education (2006)
3. A Novel Secret Sharing Technique Using QR Code, Jun-Chou Chuang, Yu-Chen Hu & Hsien-Ju Ko
4. Beyond the simple codes: QR codes in education, Simon So Hong Kong Institute of Education, Proceedings ascilite 2011 Hobart: Concise Paper
5. QR Code – Falling Prey to Malicious Website, Monthly Newsletter – Issue No. 2013-06 , Go safe online
6. QR Code based secure OTP distribution scheme for Authentication in Net-Banking Abhas Tandon,Rahul Sharma, Sankalp Sodhiya,P.M.Durai Raj Vincent .
7. QR Code Essentials,DENSO ADC
8. Context-aware QR-codes ,Dmitry Namiot ,Manfred Sneps-Sneppe ,Oleg Skokov
9. http://www.qrcode-monkey.com/
10. T. Vidas, E. Owusu, S. Wang, C. Zeng, L. Cranor. QRishing: The susceptibility of smartphone users to QR code phishing attacks. In CMU-CyLab-12 (2012), pp. 1–12.