Private Information Sharing using Two Level QR Code

V. V. Panchal
Department of Computer science and Engineering,
V.V.P. Institute of Engineering and Technology,
Solapur-413004

H. B. Torvi
Department of Computer science and Engineering,
V.V.P. Institute of Engineering and Technology,
Solapur-413004

ABSTRACT

The Quick Response (QR) code is widely popular in daily life due to reading high speed application and grater storage capacity of storing information. In this paper, we present a new rich QR code that has two storage levels. Public level and Private level, The level one named a public level ,and level two named as private level. The Private level is designed by replacing the modules using specific textured pattern. It is to be made up or composed by q-ary code with an error correction capacity. This allows us not only increase the storage capacity but also improve the security of QR code. The public level is the same as the standard QR code storage level; therefore it is readable by any classical QR code application.

General Terms

Information Security.

Keywords

QR code, Public level, Private level, AES encryption, Reed-Solomon code document authentication and Data hiding.

1. INTRODUCTION

QR code (quick response code) developed by Denso-Wave corporation in 1994.QR code carry more content such as text, phone number, redirection to web link. Detection of supermarket product, track and trace etc. A QR code uses four standardized encoding modes (numeric, alphanumeric, byte/binary, and kanji) to efficiently store data; extensions may also be used.

The NIST *Computer Security Handbook* [NIST95] defines the term computer security as, "The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)." Security is the mechanism by which information and services are protected from unintended or unauthorized access, change or destruction. Security in networking is based on *Cryptography* (a word with Greek origins, means "secret writing"), the science and art of transforming messages to make them secure and immune to attack [1].

Document prevention is a wide, important and quickly developed area of multimedia security. In today's world challenges are the identifying of fake invoices, bank checks, diplomas, tax forms and other valuable documents. Due to technical improvements in scanning and printing devices, the number of such forgery documents increases. That is why, number of new methods for document authentication have been recommended by multimedia security researchers.[2]In daily lives, DataMatrix [3], EAN-13, PDF417, barcode graphical codes, Quick Response (QR) code [4], are frequently used. Due to improving the reading speed of 2D-barcodes get the name Quick Response (QR) Code. It is extension of 2D-barcode. It contains data for both horizontal and vertical dimension. The decoding speed of QR code can be 20 times faster than that of other 2D symbols.

This paper is having sub sections are as follows. We start with an Introduction, in Section 2 described Related work in QR codes. Proposed system and its system architecture in Section 3. Section 4 defines Methods of 2LQR code. The experimental results in section 5. Finally Section 6 represents conclusions and feature works.

2. RELATED WORK

In [5] this paper, the author Lin et al proposed to hide secret message in to QR code is to use the error correction capability. First of all, they encode the secret message *sm* by using a shared key *K* and get *EK*(*sm*). After that, they embed each bit of *EK*(*sm*) into QR code. If their first variance is the fault of *EK (sm)*, then in the QR code it is impossible to get *sm.* Another drawback is that if an attacker does not change anything else then the QR code adds some extra error value, then they cannot retrieve their secret messages. Their main contribution is to propose a hidden algorithm in a QR code. The secret message is invisible to invaders and it is safe to alter the shuffle or damage. In [6] this Paper, A new secret hiding mechanism for this paper, QR tag based on the property of QR code. New plan cover exploits the error correction capabilities to hide the secret in QR code. Along with the QR version and with the error improvement levels, the design algorithm can express large secrets directly in the secret cover QR code. Only the approved recipient can decode and encrypt the signed QR code. In [7] this paper Barcode has low storage capacity and cannot be used as an active component, but they are too cheap and do not need unusual hardware to retrieve data: Indeed, barcodes are cheap, only readable components whose content cannot be changed and cannot be decoded. Compared to chips and RFID tags, many ubiquitous and low cost devices with smartphones Eases. The main contributions of this paper are the following. First, they investigate techniques for the extraction of facial characteristics which are not only robust to distortions (such as pose and illumination changes) but also suitable for being embedded into barcodes. Second, they engineer existing 2D color barcodes in order to increase their data density, so that they can store a sufficient number of facial features and a reasonable cryptographic payload. In particular, they show how to modify the HCC2D, High Capacity colorful 2-

dimensional barcode so that its density increases to 394 bytes per square inch. In [8] Digital watermark is a kind of information security and protection technology. Watermarking is mostly similar to steganography in a number of respects. The main idea of steganography is the embedding of confidential information into data under assumption that others cannot know the confidential information in data. In general, the results of this method are not robust against attacks. The main idea of watermark is to check if the confidential information is embedded in data or not and the confidential information that is embedded is powerful against attacks or edition when it is recognized. The result of this method is more robust than previous method.

In [9] this paper, a basic method of decoding allows for some latitude in QR code design. If we consider luminance values as normalized to the interval [0, 1], then sensed values in the range [λ,1] are considered white by the decoder, and those in the interval [0,λ] are treated as black. Therefore, we may in theory translate the QR code source pixels so that pixels in a white module are transformed from white to any RGB coordinate whose luminance value exceeds λ, without creating a decoding error; similarly, we can translate black

3. PROPOSED SYSTEM

In this paper our main contribution is that to improve the storage capacity of QR code and its security. For improving the security of QR code as well as well as storage capacity we are going to design a new system, two level QR code, which having two storage levels public and private level can be used for document authentication. This new generated QR code, called as two levels QR code (2LQR). In the public level is the same as the standard QR code storage level; therefore it is readable by any QR code application. The private level is constructed by firstly, private message is get encrypted using AES algorithm and then encrypted message replaced by the modules by specific textured patterns. For improving the security of private level message is encrypted using AES (Advanced Encryption Standard) algorithm. It consists of information encoded using q-ary code with an error correction capacity. That allows to improve the security of the QR code, as well as to differentiate the original document from a copy.

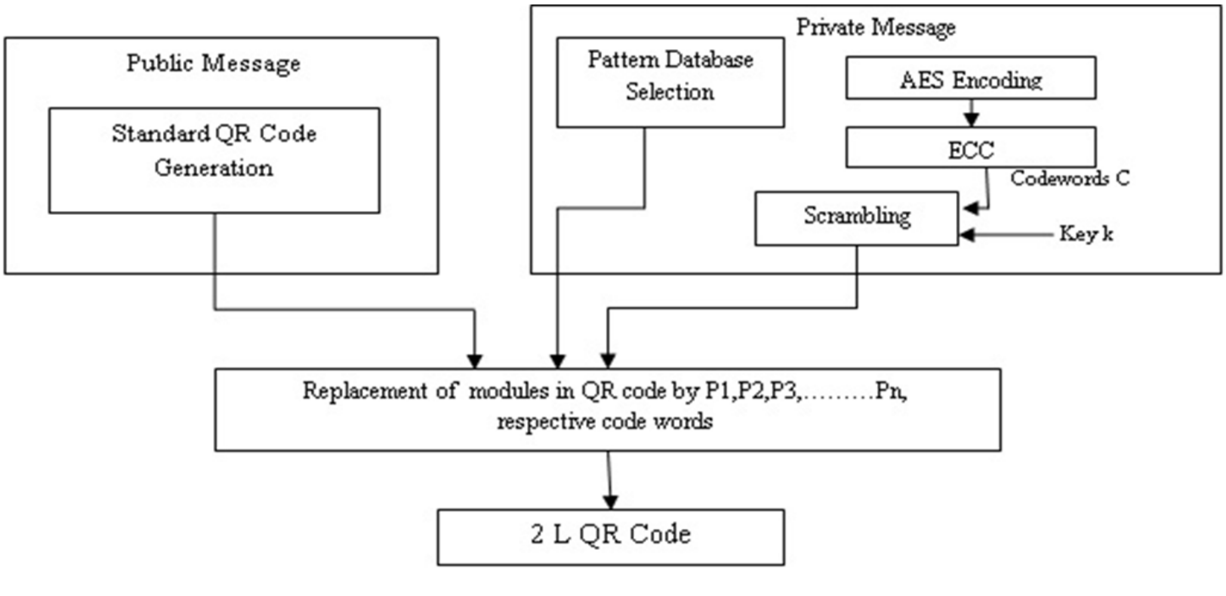

Public Message
Standard QR Code Generation
Private Message
Pattern Database Selection
AES Encoding
ECC
Codewords C
Scrambling
Key k
Replacement of modules in QR code by P1,P2,P3,………Pn, respective code words
2 L QR Code

Fig.1 System Architecture

4. METHODS FOR 2LQR CODE

We define the public M_{pub} and the private M_{priv} messages. The public message is encoded into the QR code using the standard algorithm. In the same way, the private message is encoded first using the AES encryption algorithm and then chosen ECC algorithm. Finally, both QR code with public message M_{pub} and encoded private message are combined in the 2LQR code with two stored messages.

4.1 Public message M_{pub}

Public message M_{pub} (Fig. 1, block 1). The classical generation method is used to store public message. The standard QR code generation algorithm includes the following steps. We, first of all, we analyze the message, select the most optimal mode (numeric, alphanumeric, byte or Kanji) and encode the message Mpub using the shortest possible string of bits. This string of bits is split up into 8 bit long data codewords. Then, we choose the error correction level and generate the error correction codewords using the Reed-Solomon code. After that, the data and the error correction codewords are arranged in the right order. Then, we apply the best (for our data) mask pattern, in order to be sure that the generated QR code can be read correctly. After this manipulation, the codewords are placed in a matrix respecting a zigzag pattern, starting from the bottom-right corner. The last step is to add the operations position tags, alignment, timing, format and version patterns into the QR code.

4.2 Private message M_{pub}

Private message M_{priv}:(Fig.1 , block 2). We have the private message is encode first using the AES encryption algorithm[11], AES allows a 128 bit data length that can be divided into four basic operational blocks. These blocks are treated as array of bytes and organized as a matrix of the order of 4×4 that is called the state. For both encryption and decryption, the cipher start with an AddRoundKey stage. However, before reaching the final round, this output goes through nine main rounds, during each of those rounds four transformations are performed; 1) Sub-bytes, 2) Shift-rows, 3) Mix-columns, 4) Add round Key. In the final (10th) round, there is no Mix-column transformation [3]. Figure 2 shows the overall process. Decryption is the reverse process of encryption and using inverse functions: Inverse Substitute Bytes, Inverse Shift Rows and Inverse Mix Columns. Using AES 128 bit algorithm plain text is converted in to cipher text (C_{aes}m(x)).

Now the generated cipher text (C_{aes}m(x)) using ECC to ensure the message error correction after the P&S operation. We use the block codes, and more precisely cyclic codes (or polynomial generated codes) such as Golay code [10] or Reed-Solomon code, for encrypted message (C_{aes}m(x)) for encoding. Cyclic codes can be defined in matrix form and polynomial form. Any cyclic code C is defined by [n, k, d] parameters, where n is the length of the codeword, k is the number of information digits in the codeword, d is the minimum distance between distinct codewords. The n-k digits in the codeword are called parity-check digits, and in ECCs these digits are used for error detection and correction. The minimum distance d of code C ensures that, up to the (d-1)/2 errors can be corrected by the code C. Let R = A[x]/ (x^n-1) be a polynomial ring over a Galois field A = GF (q). The cyclic code C elements are defined with polynomials in R so that the codeword (C_0,$C_{1........,}C_{n-1}$) maps to the polynomial C_0+C_1x+…..+$C_{n-1}x^{n-1}$, and the multiplication by x corresponds to a cyclic shift.

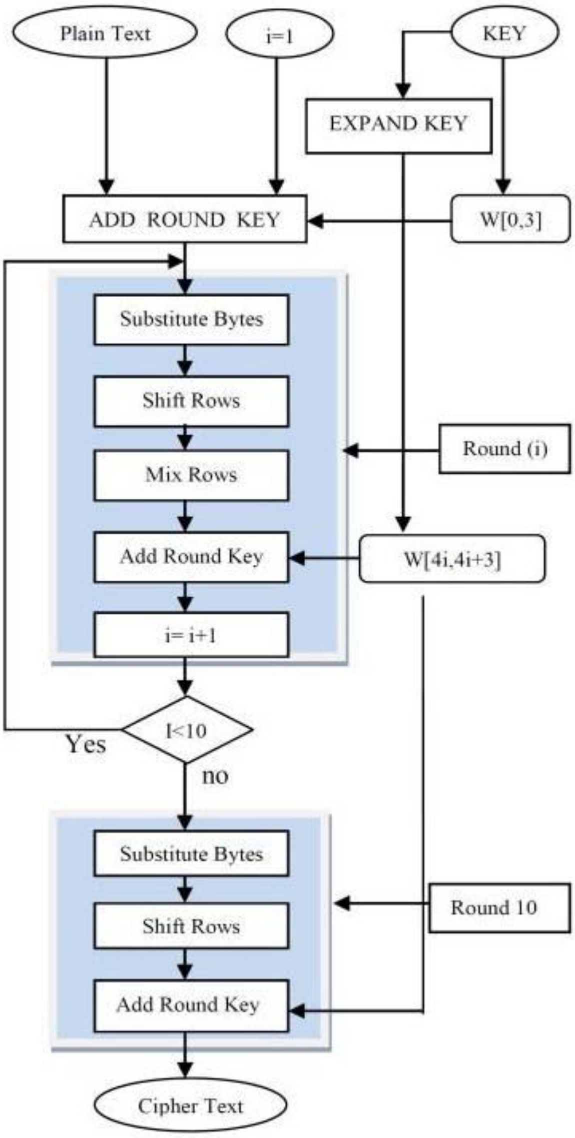


Fig.2 AES (Advanced Encryption Standard) process [11]

The code C is generated by a generator polynomial g(x), which is the code polynomial of the minimum degree in a (n,k) cyclic code C. Therefore, the generator polynomial g(x) is a factor of polynomial x^n-1. Let k informative digits of message be represented by a polynomial C_{aes}m(x), of degree, at most k-1.then the codeword c(x) is the polynomial of the form,

$$c(x)= C_{aes}m(x)g(x) ,$$

$$c(x)= C_0 + C_1 x +\ldots+ C_{n-1}x^{n-1}$$

Therefore, the encoded informative digits are (C_0, C_1,……, C_{n-1}). We encode the private message M_{priv}= (m_1^{priv},…., m_k^{priv}) is using ECC [n , k]. all the M_{priv} is represented in polynomial form m_{priv}(x).then, the polynomial form of the codeword c_{priv}(x)=m_{priv}(x)g(x) is calculated that represent the codeword C_{priv}^0. Then the scrambled codeword are,

$$C_{priv} = (C_0^{priv}, C_1^{priv},\ldots\ldots, C_{n-1}^{priv})$$

5. EXPERIMENTAL RESULTS

Fig.3 shows the public $M_{pub.}$ The public message is encoded into the QR code using the standard algorithm. In the same way in Fig.4 the private message is encoded first using the AES encryption algorithm and after that ECC algorithm. Finally, both QR code are combined in the 2LQR code.

2LQR Code Generation:

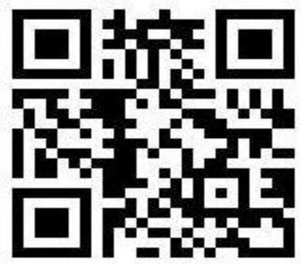


Fig.3 Standard QR code with public message M_{pub}

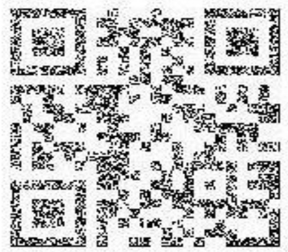
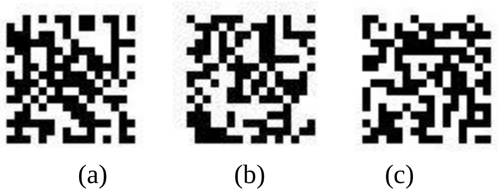


Fig.4 2LQR Code with private message M_{priv}



(a) (b) (c)

Fig.5 Textured Pattern used for private message generation

Table 1. Correlation values for the original patterns P_1, P2, P_3 and its P & S Versions $S_1S_2S_3$

	P1	P2	P3
S1	0.9993	-0.0083	-0.0563
S2	-0.0081	0.9992	0.0406
S3	-0.0563	0.0399	0.9993
min{ei1,ei2}	1	0.9586	0.9586

The private message of 2LQR code is created by encrypting private message using AES technique and then replacing the modules using given texture pattern in Fig. 5.

6. CONCLUSION

In this paper, the proposed system is presented by improving the security and storage capacity of two levels QR code. The public level information which is visible to all over and the private level contains private information which can access only authorized user of system. Objective of our project is to increase the storage capacity and improve the security. In feature work, first will add one more level that is Three Level QR code. And second is to Pattern recognition method Improvement.

7. REFERENCES

[1] Behrouz A Forouzan, "Data Communications and Networking", McGraw-Hill, 4th Edition.

[2] Lu. Tkachenko,w.Puech,O.Strauss and C. Destruet J "Printed Document authentication Using Two Level QR Code", ICASSP) 2016, pp2149-2153.

[3] ISO/IEC 16022:2006. Information technology - Automatic identification and data capture techniques - Data Matrix bar code symbology specification. 2006.

[4] ISO/IEC 18004:2000. Information technology - Automatic identification and data capture techniques - Bar code symbology - QR Code. 2000.

[5] Thach V. Bui, Nguyen K. Vu, Thong T.P. Nguyen, Isao Echizen and Thuc D. Nguyen," Robust Message Hiding for QR Code", 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing,pp.520-523.

[6] Pei-Yu Lin, Yi-Hui Chen, Eric Jui-Lin Lu and Ping-Jung Chen," Secret Hiding Mechanism Using QR Barcode", 2013 International Conference on Signal-Image Technology & Internet-Based Systems, pp.22-25.

[7] Marco Querini and Giuseppe F," Facial Biometrics for 2D Barcodes", Proceedings of the Federated Conference on Computer Science and Information Systems pp. 755–762

[8] Sartid Vongpradhip and Suppat Rungraungsilp," QR Code Using Invisible Watermarking in Frequency Domain", 2011 Ninth International Conference on ICT and Knowledge Engineering, pp.47-52.

[9] Z. Baharav and R. Kakarala. Visually significant QR codes: Image blending and statistical analysis. In Multimedia and Expo (ICME), 2013 IEEE International Conference on, pages 1–6. IEEE, 2013.

[10] B. Sklar. Digital communications, volume 2. Prentice Hall NJ, 2001.

[11] Gurpreet Singh, Supriya " A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security" International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013

[12] Akash Kumar Mandal, Chandra Parakash and Mrs. Archana Tiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE

Students’ Conference on Electrical, Electronics and Computer Science, pp. 1-5, 2012.

[13] 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.

[14] Lin Liu, “A Survey of Digital Watermarking Technologies”, www.ee.sunysb.edu/~cvl/.../Lin%20Liu

[15] /ese558report_LinLiu.pdf

[16] Chung, Chin-Ho, Wen-Yuan Chen, and Ching-Ming Tu. *Image hidden technique using QR-barcode.* In Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP’09. Fifth International Conference on, pp. 522-525. IEEE, 2009.

[17] L. Yu, X. Niu, and S. Sun. Print-and-scan model and the watermarking countermeasure. In Image and Vision Computing, volume 23, pages 807–814. Elsevier, 2005.

[18] http://www.qrcode.com/.

[19] Geisel, William A. *Tutorial On Reed-Solomon Error-Correction Coding.* (1996).