QR Code Security Using Proxy Re-Encryption for Private Data Shared Barcodes

[1]K.Lakshmi, [2]D.Jeyamanilatha
[1,2]M.E-Applied Electronics, Dept. of ECE, SCAD College of Engineering and Technology, Cheranmahadevi, Tamil Nadu, India

Abstract
A two layer QR Codes for private data sharing using convolutional coder and Proxy Re-Encryption is proposed. In barcodes, as the encoded information is featured to be machine readable only, a human cannot distinguish between a valid and a maliciously manipulated code. While humans might fall for phishing attacks, automated readers are most likely vulnerable to SQL injections and command injections. In this approach both encoding rate and interference level will be optimized with two robust error correction methods. Existing systems uses various techniques like Steganography, DCT, DFT and Secret (N, N)-Threshold QR Code Sharing Approach. But in proposed system convolutional coder is going to be used for encoding the QR Code at the transmitted side and decode the same at the receiver side. To improve the security Proxy Re-Encryption is used. Two single layer QR Codes were taken. One as a input another code is used as guide. Proxy Re-Encryption improves the flexibility of sharing the data between different hosts and also improves security.

Keywords
Barcode, QR Code, Proxy Re-Encryption, Cheater Prevention, Convolutional Code.

I. Introduction

Barcode leads to an easiest way for people labeling a tag on a product so that people can easily identify the content of product itself. Barcodes are basically classified into two types, one-dimensional (1D) barcode and two-dimensional (2D) barcode. The 1D barcodes use different width of lines and spaces to represent data and 1D barcodes put emphasis on "product identification" Whereas the 2D barcodes use symbol types of stacking and matrix to represent data and 2D barcodes put emphasis on "product descriptions". Table 1 shows different types of 1D barcodes and 2D barcodes. Only a few data like product identification is stored in 1D barcode and this is the main disadvantage of 1D barcodes. 2D barcodes are very good in embedding payload, error resistance, data security, and readability also in storage size. 2D barcode can store a lot of information like product descriptions. Including product ingredient, product item, product details, web links, and etc. 2D barcodes are reducing the level of error occurrences and having better error resistance.

1D barcodes having lower security than 2D barcodes. 1D barcodes are very easy to read by scanning the lines and the spaces. However, 2D barcodes are not easy to read a symbol pattern by human eyes. With regard to readability, 1D barcodes must scan along a single directional. If the angle of a scan line does not fit within a range, the data would not be read correctly. To enhance security of data privacy of barcodes, we design a secret sharing technique with Quick Response code (QR code). The technique shares a confidential data into shadows and one shadow is embedded into one carrier tag. Anyone cannot recovery the original secret data from its own share. The secret can be recovered only when the number of shadows is larger than or equal to a threshold.

The proposed technique does not need to connect the back-end database through Internet. Thus, the proposed technique can save much more hardware cost and can reduce the security risks transmission on the open environment. The structure of the QR Code is shown in Fig 1. The outer range is the quiet zone. The upper-left, upper right and left-bottom square areas are used for position detection and pattern separators for positioning. There are six smaller squares which are the alignment patterns. Additionally, the main area, which is colored gray, is the kernel area of data and error correction code. Table 2 shows the reliability of the QR Code.

Table 1: 1D and 2D Barcodes

1D barcodes	Code 39	Code 128	EAN-13	ISBN
2D barcodes	QR Code	PDF417	DataMatrix	Maxi Code

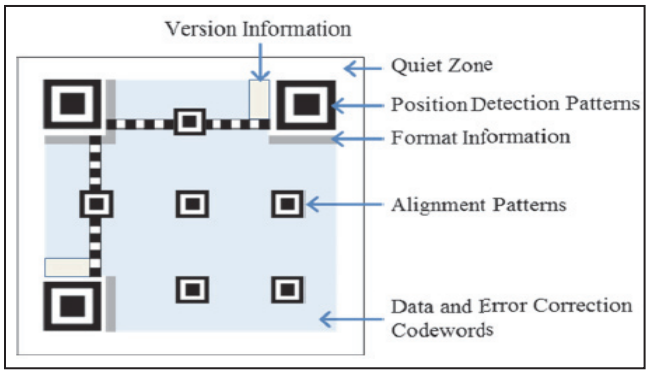

Fig. 1: Structure of QR Code

II. Proposed system

Objective of the proposed technique is to generate a two layer QR Codes for private data sharing using convolutional coder Combining two single layer and then doing proxy re-encryption on two layer QR code will results in high security and low loss. Where the data is transmitted in the form of QR code shown in fig. 3(a) and the QR Code used for guiding the data is shown in fig. 3(b). The encoded QR Code is shown in fig. 3(c). Encoded QR Code is a two layer QR Code. We can also generate multiple layer QR Code.

Table 2: The reliability of QR Code

Error Correction level	Error correction capability,% of codewords (approx)
L(Low)	7%
M(Medium)	15%
Q(Quartile)	25%
H (High)	30%

III. Processing Steps

Following are the processing steps of the proposed system.

1. At the transmitter side, both the QR Codes are converted in to hexadecimal value using MATLAB software. Hexadecimal values are concatenated

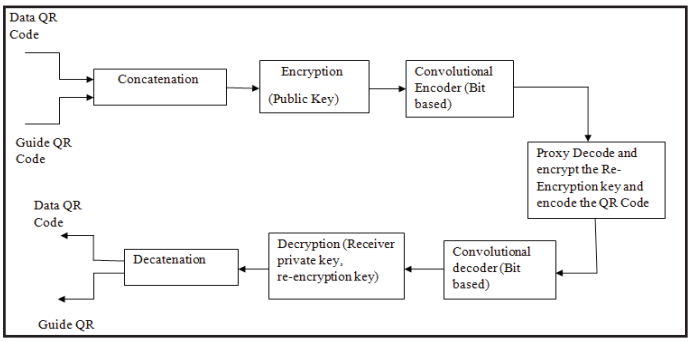

Fig. 2: Block Diagram of the Proposed System

2. Then the concatenated output is encrypted with the help of Public key encryption.
3. The Encrypted output is given as input to the convolutional encoder.
4. In channel, Proxy decoding is done with the two layer QR Code. Decoded data is again encrypted with the Re-encryption key. Proxy decoded and Re-encrypted data is again encoded to a QR code.
5. At the receiver side, two layer QR Code is decoded with the help of convolutional decoder.
6. Decryption is done by using receiver's private key and the re-encryption key.
7. Finally, the decrypted output is decatenated. Data QR Code and Guide QR Code are received at the receiver side with high security and loss.

The fig. 2 shows the block diagram which helps to understand the proposed system

Fig. 3(a): Input QR Code (DATA)

Fig 3(b): Input QR Code (GUIDE)

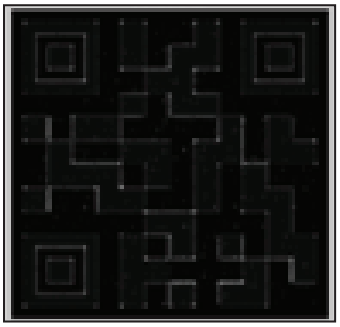

Fig. 3(c): Encoded QR Code

IV. Conclusion

In this project the Security while transferring information from transmitter end to the receiver end is visualized .to achieve high security two layer QR Code and Proxy Re–Encryption techniques are used. QR Code alone provides better security in an image form. Both the Proxy re-encryption and two layer QR Code improves the security to the higher level and leads to fast data transmission. QR Code can also store large amount of data. QR Code received at another end with reduced amount of loss. In future, if we use turbo codes we will get better accuracy and reduction in loss.

References

[1] C. Chen, A. C. Kot, H. Yang,"A two-stage quality measure for mobile phone captured 2D barcode images," Pattern Recognition, Vol. 46, No. 9, pp. 2588-2598, 2013.

[2] Chin-Ho Chung, Wen-Yuan Chen, Ching-Ming Tu,"Image Hidden Technique Using QR-Barcode", Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2009.

[3] D. H. Shin, J. Jung, B. H. Chang,"The psychology behind QR codes: User experience perspective," Computers in Human Behavior, Vol. 28, No. 4, pp. 1417-1426, 2012.

[4] H.C.Huang, W.C.Fang,"Metadata-based image watermarking for copyright protection," Simulation Modelling Practice and Theory, Vol. 18, No. 4, pp. 436-445, 2010.

[5] Hsiang-Cheh Huang, Feng-Cheng Chang, Wai-Chi Fang, "Reversible Data Hiding with Histogram-Based Difference Expansion for QR Code Applications", IEEE Transactions on Consumer Electronics, Vol. 57, No. 2, 2011.

[6] J.C.Chung, 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.

[7] K.Lakshmi Sudha, Kausthob Das, Mahesh Notani, Saisantosh Shridhar,"Reversible Data Hiding using QR Codes for Android", International Journal of Computer Applications, Vol. 97– No.11, 2014.

[8] L. Li, R. L. Wang, C. C. Chang,"A digital watermark algorithm for QR code," International Journal of Intelligent Information Processing, Vo1. 2, No. 2, pp. 29-36, 2011.

[9] N. Teraura, K. Sakurai,"Information hiding of two-dimensional code by multilayer optical method," In Proc. of IEEE 10th International Symposium on Parallel and Distributed Processing with Applications (ISPA), pp. 770-77, 2012.

[10] pei-Yu Lin,"Distributed Secret Sharing Approach with Cheater Prevention based on QR Code", IEEE transaction on industrial informatics, 2015.

[11] S.Dey, K.Mondal, J.Nath, A.Nath,"Advanced Steganography algorithm Using randomized intermediate QR host embedded with any encrypt secret message: ASA__QR algorithm,"

International Journal of Modern Education and Computer Science, Vol. 6, pp. 59-67, 2012.

[12] Suppat Rungraungsilp, Mahasak Ketcham, Virutt Kosolvijak, and Sartid Vongpradhip,"Data Hiding Method for QR Code Based on Watermark by compare DCT with DFT Domain", International Conference on Computer and Communication Technologies (ICCCT'2012) May 26-27, 2012.

[13] Yin-Jen Chiang, Pei-Yu Lin, Ran-Zan Wang, Yi-Hui Chen "Blind QR Code Steganographic Approach Based upon Error Correction Capability", KSII Transactions on Internet and Information Systems, Vol. 7, No. 1, 2013.

K. Lakshmi received B.E degree in Electronics and Communication engineering from P.E.T Engineering college, Anna University, Chennai, India in 2015. At present she is studying M.E degree in Applied electronics from SCAD College of Engineering and Technology, Anna University, Chennai, India. Her research interest includes Digital signal Processing and Digital Image Processing.

D.Jeyamani Latha received her B.E. degree in Electronics and Communication Engineering from Government College, Tirunelveli, India, in 1985, the M.E. degree in Applied Electronics from Karunya University, Coimbatore, India, in 2007. She was a Lecturer with Department of Electronics and communication Engineering, Joe Suresh Engineering College, Tirunelveli, India and SCAD College of Engineering and Technology, Cheranmahadevi, in 2002 and 2004 respectively. She is working now as an Associate professor with Department of Electronics and communication Engineering, SCAD College of Engineering and Technology, Cheranmahadevi from 2007 onwards . Her research interests include digital image processing, wireless communication, microwave engineering and VLSI Design.