International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 12th June 2017. Link :
http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-4
Title: Qr Code Based Cheater Prevention For Distributed Secret Sharing Approach.

Volume 06,Issue 04, Page No: 907 – 913.

Paper Authors

*** NEELAM BHAGYA LAKSHMI, VEMU HARINI.**

* Eluru College of Engineering And Technology.

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

QR CODE BASED CHEATER PREVENTION FOR DISTRIBUTED SECRET SHARING APPROACH

***NEELAM BHAGYA LAKSHMI,** VEMU HARINI**
*PG Scholar, Eluru College of Engineering And Technology.
**Assistant professor, Eluru College of Engg And Technology.
bhagya.lakshmi871@gmail.com harinivemu@gmail.com

ABSTRACT:

QR barcodes are used extensively due to their beneficial properties, including small tag, large data capacity, reliability, and high-speed scanning. However, the private data of the QR barcode lacks adequate security protection. In this article, we design a secret QR sharing approach to protect the private QR data with a secure and reliable distributed system. The proposed approach differs from related QR code schemes in that it uses the RSA Cryptographic algorithm to achieve secret sharing. The QR code image is first encrypted using RSA algorithm and transmitted through network. Later the code was reconstructed. Based on our experiments, the new approach is feasible and provides content readability and an adjustable secret payload of the QR barcode.

Index Terms—QR barcode, secret sharing, cryptography, RSA algorithm

I. INTRODUCTION

Barcode provides a convenient way for people labelling a tag on a product so that people can easily and quickly identify the content of product itself. It can be 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, for example, code 39, code 128, EAN-13, EAN-128, ISBN, and etc. As for the 2D barcodes, they use symbol types of stacking and matrix to represent data, such as QR code, PDF417, Data Matrix, Maxi Code, and etc. Table 1 shows different types of 1D barcodes and 2D barcodes. In generally, 1D barcodes put emphasis on "product identification" and 2D barcodes put emphasis on "product descriptions". Because of the limitation of 1D barcode storage, only a few data like product identification is stored in 1D barcode. 2D barcodes are superior to that 1D barcode in embedding payload, error resistance, data security, and readability. In the storage size, 2D barcode can store a lot of information like p duct descriptions, including product ingredient, product item, product details, web links, and etc. For error resistance, 2D barcodes can defence different levels of error occurs.

The security of 1D barcodes is lower 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. However, 2D barcodes get wide ranges of angles for scanning. Thus, 2D barcodes are readability.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

2D Barcodes provide a unique identifier for objects and applications to automatic checkout system, commerce, industry, hospital, and etc. Barcodes are very convenience to automatic systems, but they have data privacy weakness. A reader device with video capture function can read the content from tags directly. When barcodes contain privacy information may result in the risk of security issue. Therefore, the confidential data is often stored in the back-end database. When a reader captures a tag, it only gets a network link from a tag and later connected to the back-end database through the Internet. A user who has access right can login database to retrieve the privacy information.

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

TABLE 1: 1D Barcodes and 2D Barcodes.

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 QR code and encrypt using RSA cryptographic algorithm. The secret can be recovered only when the right receiver receives the encrypted data. 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 rest of this paper is organized as follows. In Section 2, we review the QR code. The proposed technique is described in Section 3. The experimental result analysis and performance is listed in Section 4. Finally, the conclusions are presented in Section 5.

II. QR CODE

The QR code is a kind of matrix symbol, which was developed by the Japanese company Denson-Wave in 1994. Figure 1 shows the basic structure of QR code. They are quiet zone, position detection patterns, separators for position detection patterns, timing patterns, alignment patterns, format information, version information, data, and error correction code words. They are shown in Figure 1.

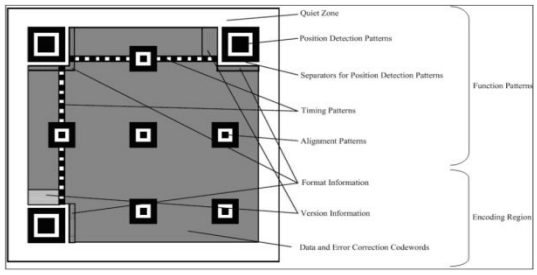

FIGURE 1: The basic structure of QR Code.

The main features of QR code contain large capacity, small printout size, high speed scanning, advanced error correcting, and freedom direction scanning. The overall are summarized as follows.

- High data capacity: QR code can store 7,089 numeric characters and 4,296 alphanumeric characters, and 1,817 kanji characters.
- High speed scanning: A mobile phone with camera function can get the content from a barcode quickly and easily.
- Small printout size: QR Codes carry data on both horizontally and vertically, thus QR codes are better than 1D barcodes in data capacity.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

- Advance error correcting: Even if 50% areas of barcode are damaged, QR codes still can be recognized correctly.
- Freedom direction scanning: The scanning direction of QR code is freedom.

TABLE II
MAXIMUM CHARACTER STORAGE CAPACITY

Version	Error correction level	Number of error correction codewords	Number of error correction blocks	Number of data codewords per block	Number of data codewords	Number of data bits
1	L	7	1	19	19	152
	M	10	1	16	16	128
	Q	13	1	13	13	104
	H	17	1	9	9	72
20	L	224	3 5	107 108	861	6,888
	M	416	3 13	41 42	669	5,352
	Q	600	15 5	24 25	485	3,880
	H	700	15 10	15 16	385	3,080
40	L	750	19 6	118 119	2,956	23,648
	M	1,372	18 31	47 48	2,334	18,672
	Q	2,040	34 34	24 25	1,666	13,328
	H	2,430	20 61	15 16	1,276	10,208

Table II briefly presents the data payload and the reliability of various QR versions and error correction levels of the QR standard. According to the QR Version and the error correction level, the data code words in the QR tag are segmented and stored in one or more blocks. For instance, the data in QR version 1-L are 152 bits (19 data codewordsx8 modules) and are stored in one block. The data in QR version 40-L are 23,648 bits (2956 data codewordsx8 modules) and are segmented and stored in 25 blocks (19+6), i.e., 19 blocks each of which contains 118 data code words and six blocks each of which contains 119 data code words. Then, the error correction code words that correspond to the data code words of each block are generated to ensure the error correction capability of the block data.

Obviously, the larger QR version and error correction level can offer higher data payload and reliability. To design an efficient and feasible application for the QR barcode, the proposed scheme exploits the adjustable capacity and error correction feature to achieve readability and secret sharing on QR modules directly.

III. PROPOSED DESIGN OF SECRET SHARING

The proposed technique designs a secure data transmission scheme based on the secret sharing

scheme with QR code. Secret sharing scheme was developed using RSA cryptographic algorithm. This is a public key encryption which uses public key and private key for encryption and decryption of the given data. The QR code which is to be transmitted is first given to Mat lab code o convert the QR code image to HEX data. The HEX data is then encrypted using RSA algorithm and transmitted within the network. At the receiver end using the receiver private key the HEX data is decrypted and given to mat lab to reconstruct the original QR code. Anyone cannot decrypt the original secret from their own share. The secret can be recovered only when the receiver has his own private key. The above process is listed in Figure 2.

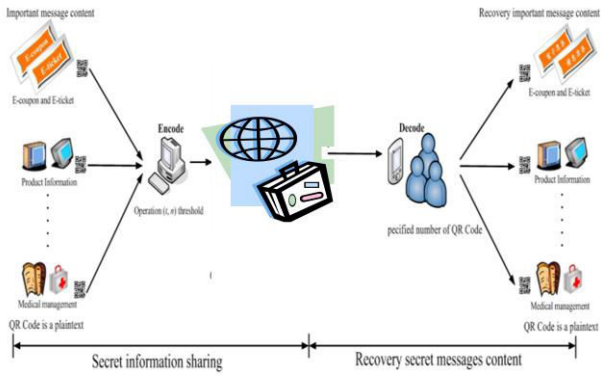

Figure 2 QR code encoding and decoding using MAT Lab and RSA encryption Algorithm

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

➢ RSA ALGORITHM:

In the field of networking, role of network security is immense. In the age of information we need to keep information about every aspect of our live. These information needs to be hidden from unauthorized access (confidentiality), protected from unauthorized change (integrity), and available to an authorized entity when it is needed (availability). Hence the way of keeping the information securely is known as cryptography, [1] which comes from a word with Greek origin, means "secret writing". Many cryptographic algorithms are developed to achieve the above said goal. The algorithms should be such that an opponent cannot defeat its purpose. These algorithms generally consist of some arithmetic operations which are complicated and time consuming. It is because of the fact that these algorithms work with large amount of data either in blocks or simply in streams. Although a single traditional CPU is enough for performing these computations, but for a machine which works as a server in a huge network gets millio of client requests for performing cryptographic operations for them individually. This makes the workload huge. The computational resources may also be limited for example in smartcards, mobile phones, handheld computers, etc. Moreover if the associated network is of high speed, the speed of the necessary cryptographic computations also needs to be taken into account. For example in transmitting audio and video data for cable TV, video conferencing and sensitive financial and commercial data, the speed of the cryptographic module to be embedded, needs to be very high. So from the viewpoint of high speed and throughput, traditional software implementations of these complicated cryptographic algorithms are not efficient in real time applications like ATM, VPN, etc. This forces the system designers to go for hardware implementation of the cryptosystems.

Rivest–Shamir–Adleman (RSA) [3] cryptosystem is a well-known private key cryptosystem whose security comes from the fact that large integers are factorized inefficiently. In this thesis the goal is to design an efficient architecture for modular multiplication and exponentiation operations, which are the main operation of RSA algorithm.

RSA uses two algebraic structures 1) a public ring R = <Zn, +, ×>, 2) a private group G = <Z φ (n)*, ×>. Key generation can be done in the following way:

Two random prime numbers p, q is taken.

System modulus n = pq is calculated.

Euler's totient φ (n) = (p-1) (q-1) is calculated.

A random encryption key is selected such that 1<e< φ (n) and gcd (e, φ (n))=1.

Decryption key d is calculated such that d = e-1mod φ (n).

Publish the public key {e,n}.

Keep the private key {p,q,d}.

To encrypt a message M a sender uses the public key of the recipient and compute thecipher text C as follows:

C = Me mod n

To decrypt a message C the recipient uses his own private key and computes the plain

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

text M as follows:

M = Cd mod n

IV. RESULT ANALYSIS AND PERFORMANCE

This section describes the security and the performance of the proposed scheme. The proposed scheme is based on MAT Lab and AES encryption scheme. The below figure the complete result analysis and performance of the proposed design. Figure 3 gives the encoded data into QR Code. Figure 4.1 gives the simulation results of RSA algorithm encryption. Figure 4.2 gives the simulation results of RSA algorithm decryption. Figure 5 gives the reconstructed QR code from MAT Lab and figure 6 gives the complete encoded text.

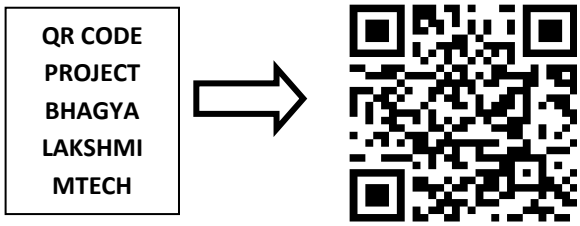

Figure 3

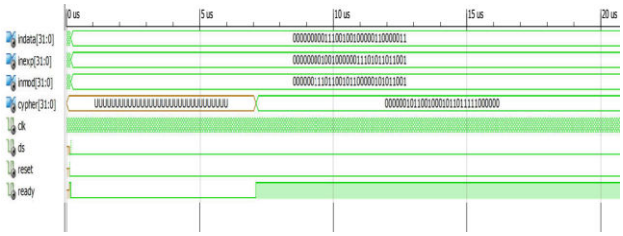

Figure 4.1

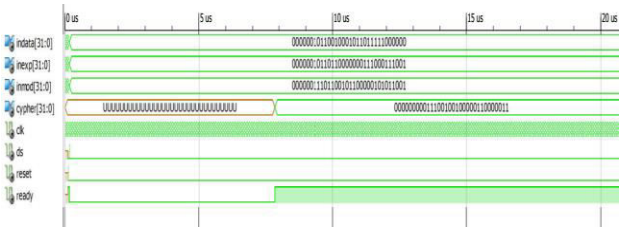

Figure 4.2

Figure 5

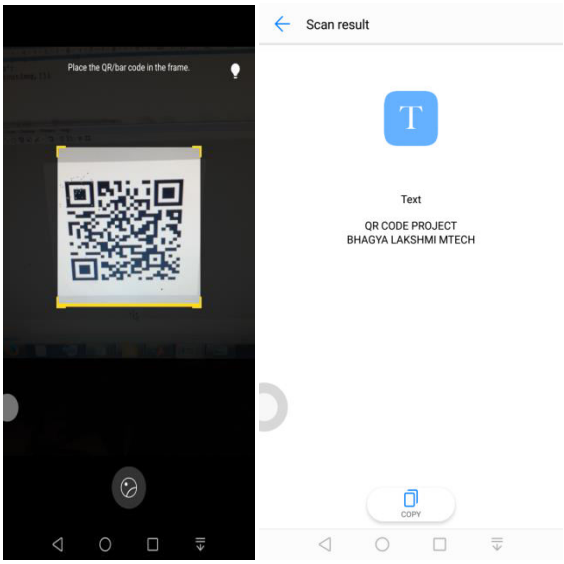

Figure 6 output result on HONOR 5C MOBILE

V. CONCLUSIONS

In this paper, a secret sharing mechanism to enhance the security and data privacy for QR code is proposed. The proposed technique improves data security during data transmission. On the other hand, the proposed technique does not need to establish a back-end database beforehand for contents searching. It direct embeds the secret data into tags therefore the proposed technique can save a lot of hardware cost and software maintenance. The proposed technique can be applied to some applications such as

electronic tickets, airline luggage inspection, medical e-health system, and others fields.

VI. REFERENCES

1. H. S. Al-Khalifa, "Mobile SRS: a classroom communication and assessment service". In Proceedings of the Innovations in Information Technology, United Arab Emirates, 2008.
2. T. Bouchard, M. Hemon, F. Gagnon, V. Gravel, and O. Munger, "Mobile telephones used as boarding passes: Enabling Technologies and Experimental Results". In Proceedings of the 4th Autonomic and Autonomous Systems, Gosier, Guadeloupe, 2008.
3. T. Chen, "The application of bar code forgery - proof technology in the product sales management". In Proceedings of the Intelligent Information Technology Application Workshops, Washington, DC, USA, 2008.
4. U. B. Ceipidor, C. M. Medaglia, and A. Perrone, M. D. Marsico, and G. D. Romano, "A museum mobile game for children using QR-codes". In Proceedings of the 8th International Conference on Interaction Design and Children, Italy, 2009.
5. Y. J. Chang, S. K. Tsai, and T. Y. Wang, "A context aware handheld wayfinding system for individuals with cognitive impairments". In Proceedings of the 10th international ACM SIGACCESS conference on Computers and accessibility, Halifax, Nova Scotia, Canada,2008.
6. N. Fujimura and M. Doi, "Collecting students' degree of comprehension with mobile phones". In Proceedings of the 34th Annual ACM SIGUCCS Conference on User Services, Canada, 2006.
7. T. Falas and H. Kashani, "Two-dimensional barcode decoding with camera-equipped mobile phones". In Proceedings of the Pervasive Computing and Communications Workshops, White Plains, NY, USA, 2007.
8. J. Z. Gao, L. Prakash, and R. Jagatesan, "Understanding 2D-barcode technology and applications in m-commerce – design and implementation of a 2D barcode processing solution". In Proceedings of the Computer Software and Applications Conference, Bejing, China, 2007.
9. T. Kamina, T. Aoki, Y. Eto, N. Koshizuka, J. Yamada, and K. Sakamura, "Verifying identifierauthenticity in ubiquitous computing environment". In Proceedings of the Advanced Information Networking and Applications Workshops, Ontario, Canada, 2007.
10. B. Lingyan, F. Zewei, L. Min, and W. Weining, "Design and implementation of the airline luggage inspection system base on link structure of QR code". In Proceedings of the Electronic Commerce and Security, Guangzhou, 2008.
11. T. Y. Liu and Y. L. Chu "Handheld augmented reality supported immersive ubiquitous learning system". In Proceedings of the Systems, Man and Cybernetics, Singapore, 2008.
12. J. Rouillard, "Contextual QR codes". In Proceedings of the 3rd International Multi-Conference on Computing in the Global Information Technology, Athens, Greece, 2008.
13. S. Reiser and R. Bruce, "Service learning meets mobile computing". In Proceedings of the Annual Southeast Regional Conference, Auburn, Alabama, 2008.

14. A. Shamir, "How to Share a Secret". Communication of the ACM, 22(11): 612-613, 1979.
15. G. Starnberger, L. Froihofer, and K. M. Goeschka, "QR-TAN: Secure mobile transaction authentication". In Proceedings of the Availability, Reliability and Security, Fukuoka, Japan, 2009.
16. Y. L. Yeh, J. C. You, and G. J. Jong, "The 2D bar-code technology applications in medical information management". In Proceedings of the Intelligent Systems Design and Applications, Kaohsiung, Taiwan, 2008.