Anti-fake Technology of Commodity by Using the QR Code Application

Dharamvir[1], Ashwini D[2], Apula S[3] , Hibu Tabyo[4], BhimSen Singh[5]

[1] Asst. Professor ,[2,3,4,5] MCA Final Year
[1,2,3,4,5] Department of MCA, The Oxford College of Engineering , Bengaluru , Karnataka , India – 560068
Corresponding Author – [1]dhiruniit@gmail.com

Abstract—

QRCode are often used in the raw materials trading. One of its main idea is covering credible authentication information to avoid the customerbuying produced products. This Research Papers gives an extinct idea how the QRcode Security system interacts with a customer and it helps us to know the relation on the server and the QRCode data. It is necessary to encrypt the QRCode by using the RSA secure-ID software token and DES Algorithm. And by Comparing these procedures for the QR security Code, by using the DES and RSA algorithms, it displays the way how the expends of preceding goods are increasing, which is ultimately can be used in the anti-fake identification as expectation. Furthermore, this insight helps us in decrypting the QRCode and key storage of how it is introduced in the maintenance and development and with the textbook which are written and handled as a relationship of Client and Server on this research. The way and process of how the anti-fake technology detection is working, can be viewed or seen from its brands or by its specialist co-op's side or service providers side, and it is been used for detecting that when a same acquirers or identifiers coded in the QRCode are repeated many times within the specific time periods or Geographic Regions.

Keywords-QR code,Cryptography,RSA, DES.
DOI Number:10.14704/nq.2022.20.8.NQ44533 **NeuroQuantology 2022; 20(8): 5062-5072**

1.INTRODUCTION

The presence of QRcode completely tackled the necessity of containing more data than standardized tag and can be compacted supportively. It is broadly utilized in different regions like portable installment, site investigating and hostile to counterfeit.

The faking items is a difficult inquiry, in retail industry as well as in hardware producing industry. Offenders get the legitimate data of protected item by utilizing illicit methodology and produces the flawed item to the costumers, which makes them unignorably adversity between the two clients and the Makers.

A couple of makers will abuse the QRcodes irreproducible by using a novel covering framework for printing them. Considering the QRcode, this has been effectively applied in enemy who are duplicating the industry, this paper is being mostly loos at the part of the best approach to scramble the information of the QRcode, however by not simply doing with the QRcode.

This paper is proposed a possible method to encode the QRcode, the RSA and DES were used to utilized to scramble the plaintext. With the help of portable applications and the attempt data set, clients simply need to check the QRcode and the application moves the information to the data set and then the data set will return the input. At that point the

clients can get a clear progression of veritable data of that item. But basically, while we expanding the trouble of decoding, this paper likewise looks at the impact of the scramble/unscramble effectiveness while utilizing distinctive encoding way.

2.QR CODE and ANTI-FAKE

2.1 The introduction to QRcode

The introduction to QRcodeabbreviates (Quick Response Code) is a kind of 2-dimensional matrix symbol, which is developed based on the bar code. One- dimensional bar code records information in the horizontal direction, but it can only represent numbers and letters. Besides, itcan not be used in mobile app due to its small storage capacity [1].

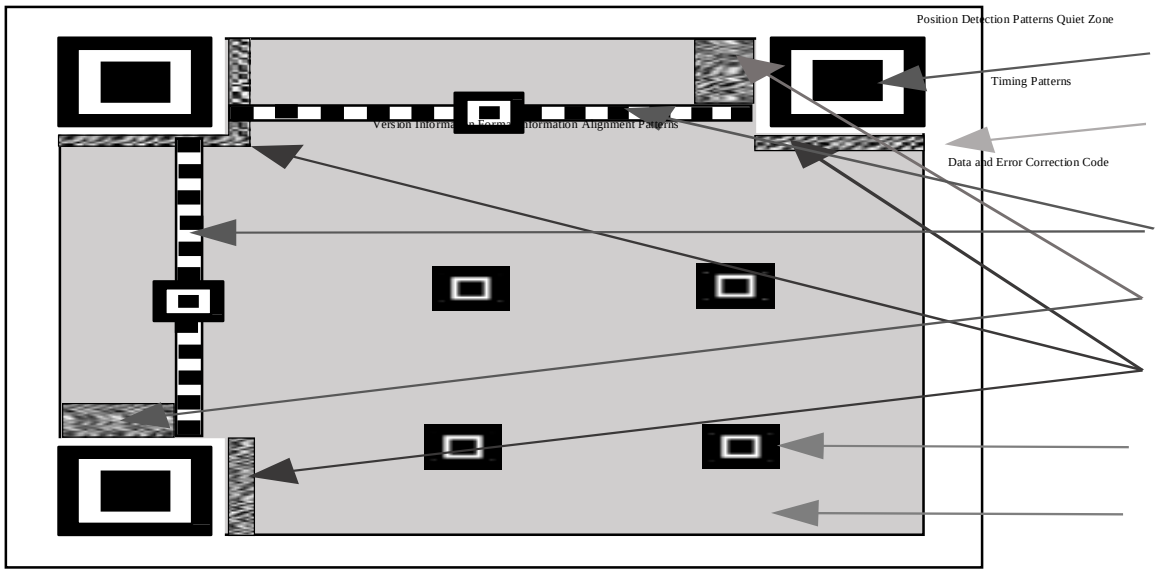

Figure 1. An illustration of QRcode with System Model

An illustration of QRcode is displayed in figure 1, QRcode is comprises of position in the example's recognition as patterns detection (large square), alignment pattern (small square), two timing patterns (the line which is alternating the white and the black-cubes), the Area for format and version information, the area for storage data and a blank quiet zone around it.

The minimum(min) size for the QRcode is 21*21 modules, while the Data Matrix is havingaeven much more space-efficient for minimizing size of 10*10 modules [2]. Resulting in the Reed-Solomon error correction, the data will still be able to be read accurately even if a part of QRcode is damaged. QRcodes have 4 error correcting-levels, L is for (7%), M is for (15%), Q is for (25%), H is for (30%) and the higher-level means area of damaged allowed is larger.

2.2 QRcode Reading andanti-fake

QRcode Reading and anti-fake in a standard QRCode, the corners are estimated and marked so that it is so convenientwhere the code that is inside is scannedaccordingly [3]. The objects with different colors will reflect visible light with different wavelength. While camera is scanning the QRcode, mobile phone will automatically use the image binarization to process the QRcode that wants to be used. Then it will do the widened activity and it obtains the outline of the QRcode through the enlarged image.

A gray-scale value calculation formula is used to get a standard binarization image.

After all these works are done, mobile phone will then do the grid sampling and checks to pixels on each node and determine whether it is "1"-black or "0"-white. This will produce an original binary value image of the QRcode that has been scanned, then it will work with the data correction of the captured image and it works on the decoding development. The raw data will be transferred to actual data according to the logic decoding rules.

QRcode itself can not be anti-counterfeiting, it works like the following. The manufacturers assign a unique QRcode to each and every product, then the customers will use the mobile phone to scan the QRcode. The verification will be done by the computer and then the result will be returned to the customers. The specific scheme will be discussed in part IV.

3.RSA and DES

3.1 Overview of RSA

RSA is an algorithmic encryption asymmetric-key. It was proposed by the professor R. I. Rivest in 1978, A. Shamir and M. Adleman in MIT. RSA is an exponent function which is based on a large prime factoring integer, which is considered to be a one-way trap-door function. This function is also called as “trap door”is because it is easy to compute the inverse functions once a certain “trap door”data’s is known. The reason in which these are called “one way” is because in one-direction they are very easy to compute but by the same way they are very difficult to compute in another [4].

The plaintext and ciphertext are considered to be an integer from (0 to n-1) in RSA(Usually the size of n is 1024).

1) **Generating pri-pub key pair**

a. First two prime integer p and q(each 1024 bits) are selected, which q ⍰ p.

b. Compute the modulus n = q * p

c. Compute e (public exponent) by calculating

$$e * d = 1 mod (p-1) * (q-1),$$

which is the multiplicative inverse of the d[4].

d. Hence the keys of public is n , e and the keysof private is n, d**.**

3.1.2Decryption andEncrypting-

Encryption and Decryption is used to encrypt the plaintext, firstly the plaintext is represented as positive integer M. Then public key n, e is used to calculate,

$E(M) = M^{e} \ (mod\ of\ n)$ and the sender will send receiver.$E(M)$ toreceiver.

$D(E(M)) = E(M)^{d} \ (mod\ of\ n)$ $M$the plaintext from integer M.Then he/she can extract the plaintext from integer M.

3.2Overview ofthe DES

DataEncryptionStandardisan accomplishment of a CipherFeistel. The DES is using the Feistel structure of Sixteen-rounds. The block size of each Feistel Structure is for 64-bit. However, the critical length of the Feistel Structure is for 64-digit, A DES has a powerful key-length of fifty-six pieces, since the eightround of the sixty-four pieces of a key are not utilized by the calculation of encryption (work is used to checking the bits value only). A DES General Structure is summed up in the accompanyingeg –

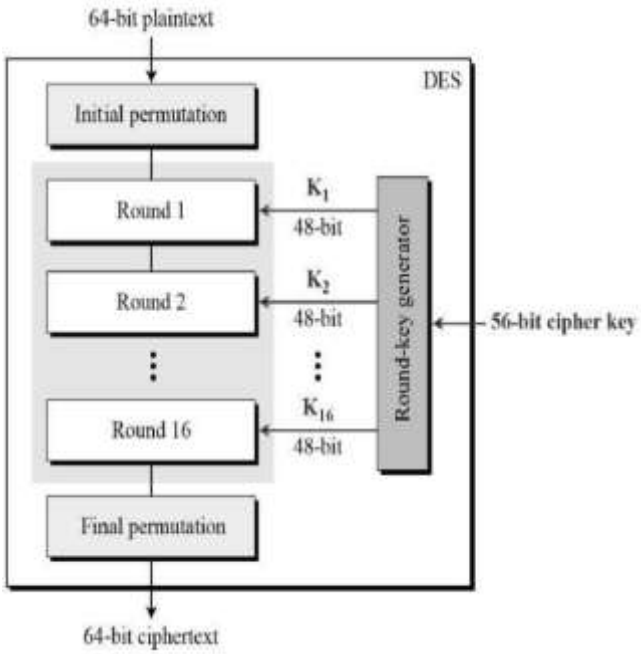

Figure 2.DES GENERAL STRUCTURE

Data Encryption Standard in view of the Feistel-Cipher, everything necessary to determine is used with –

- Round Work
- Scheduling of Key
- Any extra handling − that is Permutation-final and permutation-initial.

3.2.1 **Initial Permutation and Final Permutation-**

The Final permutation and Initial permutations are a forward sort of boxes of permutation(P-boxes) thatis the converse oneothers. There is no importanceof cryptography inDES. The starting permutations and finalpermutations isdisplayed asfollow-

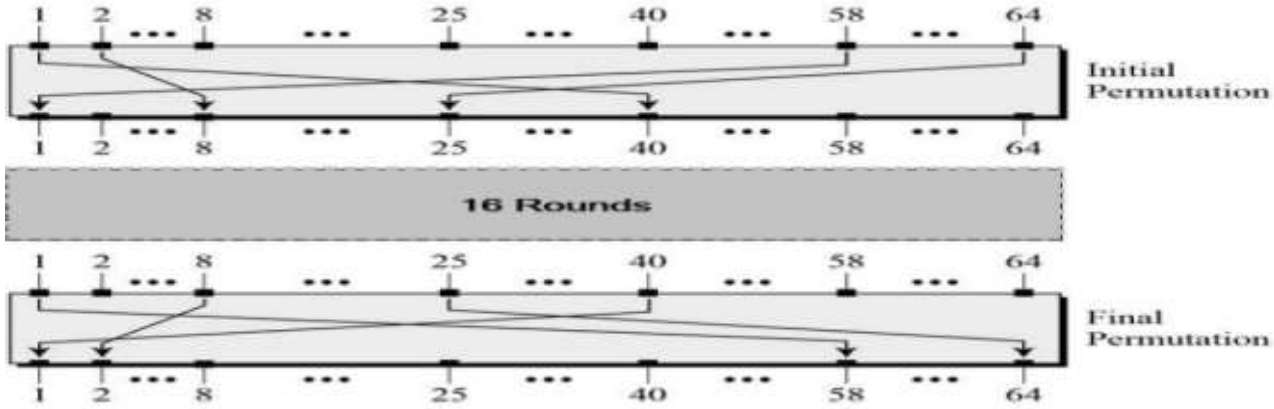

Figure 3.Final Permutation and Initial Permutation

3.2.2 Round Work

The fundamental piece of this code is the Data-Encryption Standardwork, the f. A DES workwill apply a 48piece key to the right-most 32bitkey to produces the output of 32bitkey.

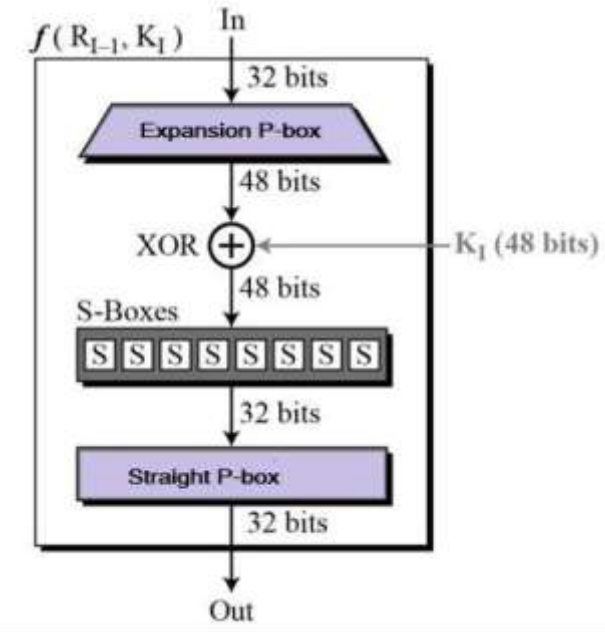

Figure 4. Work of Round Key

- **EPS-Permutation-Box of Expansion** –Hence, the Input of right is having thirty-two-bits and the round work ishaving forty-eight-bit, first we needto expand the right contribution to forty-eight-pieces. The Permutation-logic is pictographically portrayed in the following eg-

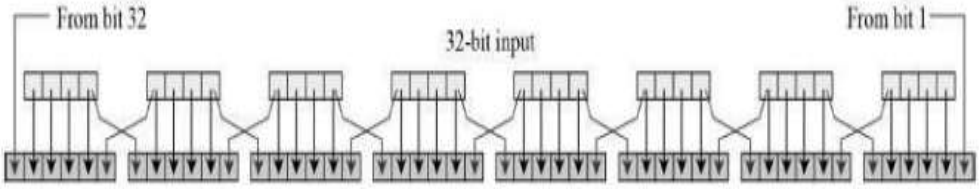

Figure 5.Permutation Logic

Apictographically depicted logic of permutations is basically depicted as a table in the detail of DES which is delineated as displayed in the underneath table-

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

Figure 6.Basic Logic of Permutation

- **Whitener[XOR] –**Later thepermutation development, the DES workson adevelopment of XOR on the extended right segments and even with the roundkey. In this operation we only use the round key.
- **Substitution-Boxes(S-Boxes) –** It carries out the

real-mixing that means a confusion. Data-Encryption Standard uses a (8 S-boxes), where each of the boxes have with a input of 6-bit and a output of 4-bit. By referring the following eg-

- The rule of a S-box is illustrated in the below picture−

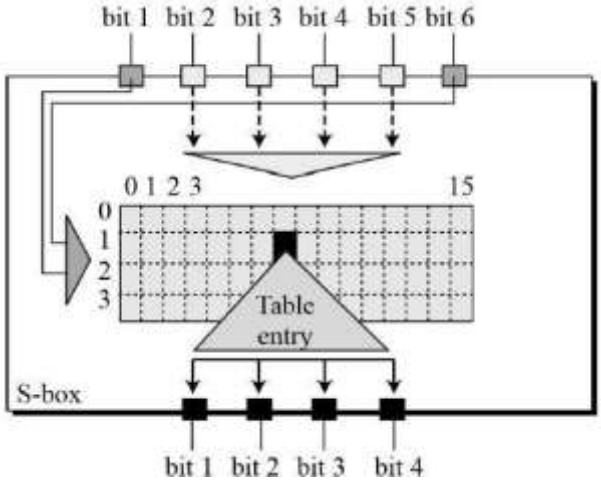

Figure 7.Rule of a S-box

- In total, there're of eightS-box tables. That is having output of-all the eightS-boxes,it is combined into a thirty-two-bit section.
- **Permutations in Straight** –Thethirty-two-pieces output of an S-boxesis then oppressed to the straight-change with a given decide that is displayed in the accompanying example:

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

Figure 8.Basic Example of Straight Permutation

3.2.3Generation of keys.

A generator of roundkeys makes a 16 48-bitkeys short of every 56-pieces of cipherkey. The course of age of a key is portrayed in the accompanying eg−

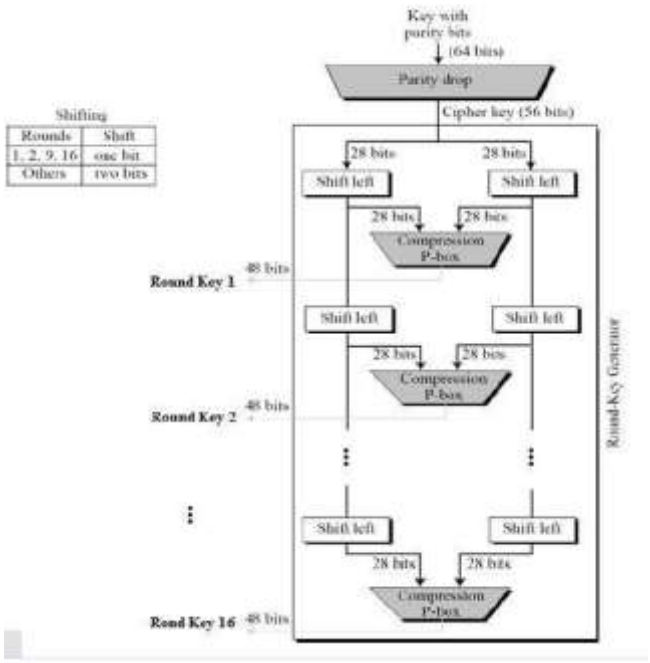

Figure 9.Generation Of Keys

TheParity drop logic, Compression, and Shiftingof Permutation-box is disposedin the Data-Encrypt Standard depiction.

3.2.4**Data-Encrypted Standard Analysis-**
Itfulfills the properties of boththe desired blocks ofcipher. The 2features which makes the cipher-block very strong is-

- **Effect of Avalanche** –A little changes in the plain-textsresults avery remarkable change in figure text.
- **Completeness** − Each piece of the figure text depends upon various pieces of the unencrypted text.

Overamostlatest couples of year, crypt analysis hasfound some shortcoming in the DES, the keys that're selected is known as the powerless keys. Then the keys that are powerless can be kept away from.

4. QRCODE WORKING SCHEME

4.1Encrypting and Generating

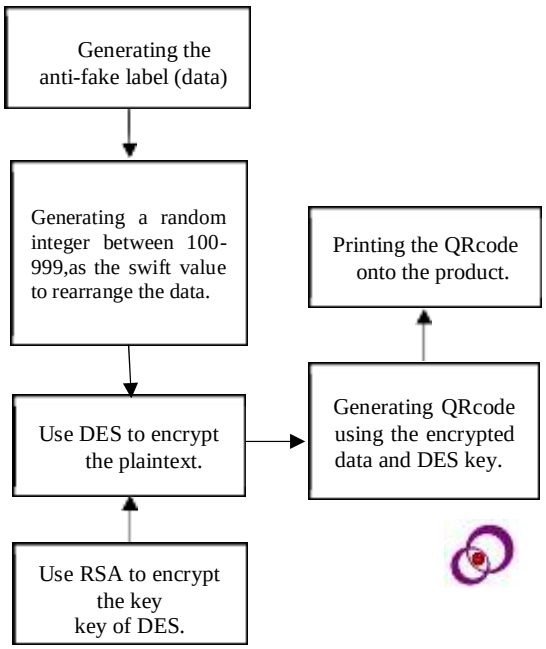

Figure 10. Decrypting and Encrypting

As shown in figure, the data will firstly be rearranged. This paper used PRNG to generate a integer between 100-999, thenswifttheoriginaldataaccordingtothecharactersheet.The main purpose is to avoid the chosen-plaintext attack. Although theanti-fakinglabelofmostoftheproductisusuallyanunique serial number, there will still have many same substrings between different serial numbers. This attack is allowing us to recovering the full key of QRCode in under 2-hrs with 8FPGAs (the tests that were completed on a VIRTEX1000 bg560-4) utilized in the equal[5]. The swift value will be written after the serial number and they will be encrypted altogetherlater.

Before going to the next part, both DES and RSA are already implemented by programmer in different computer languages and easy to get by downloading corresponding packages. JAVA is used to be the encryption engine.

DESisusedtoencrypttheplaintextsandthefigure text that bethefrontpartoftheQRcodedata.SincetheDESisnolonger secured,inordertomakesurethatthecipher textisunbreakable during product's service period (the large machineries like mechanical arm andTBM have service period form a month to several years). The key will be encrypted again by RSA and then it will be the latter part of QRCodedata.

Combining the both cipher text and the encrypted key together as shown in figure. QRCodes will be created and printed on to the cover of products. DES key, private key and public key are all automatically generated by computer. Figure shows an example of QRCode.

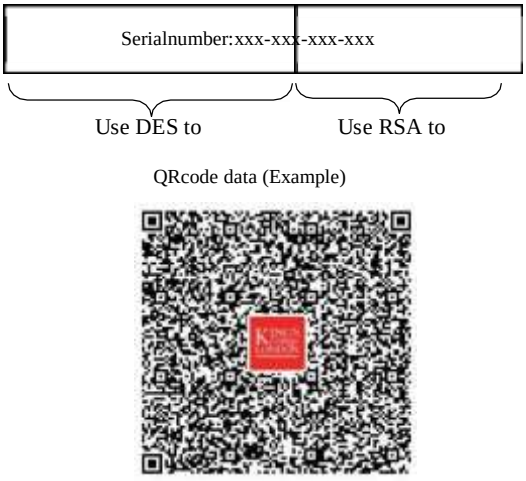

Figure 11. QRCODE

4.2 Key storage

In reality, the company will store the keys in their own database for online verification. Like any information, a data-base system should run on a perfect operating system and dependable equipment, and that is to be protected against attacks over the network[6]. Here an assumption is made that when scanned data is submitted through

browser the data information'sshould be remainedconfidentialontheway that it is been workingtothewebserver,even with theapplication-server, and with the Backend DB-server[7] and-it needed a secure connection in-between any users and then finally the database of QRCode is been developed[8].

Textbookisusedtosimulatethedatabaseinacompany.The encrypted DES keys, private key and public key will be stored in different textbooks once the QRcode is generated. These keys will be used when decryptingdata.

As displayed in figure, when client filters the QRcode, the information of the customers will be transferred to Server.Then the computer-systemwill attempt to decode the given DES-key that is utilizing a rundown of keys of private fromthe DB. If QRCode success, keys of DES will be then capitulated to the DataBase that willmatching with a rundown of a DES-keys. The keys once that are been given is matched with the servers, the computersystems will then begin to decode the ciphertext. Then all given decoded data will be thencoordinated with a progression of chronicno's and the results that are been received will be returned to customer's application.

4.3 Decrypting

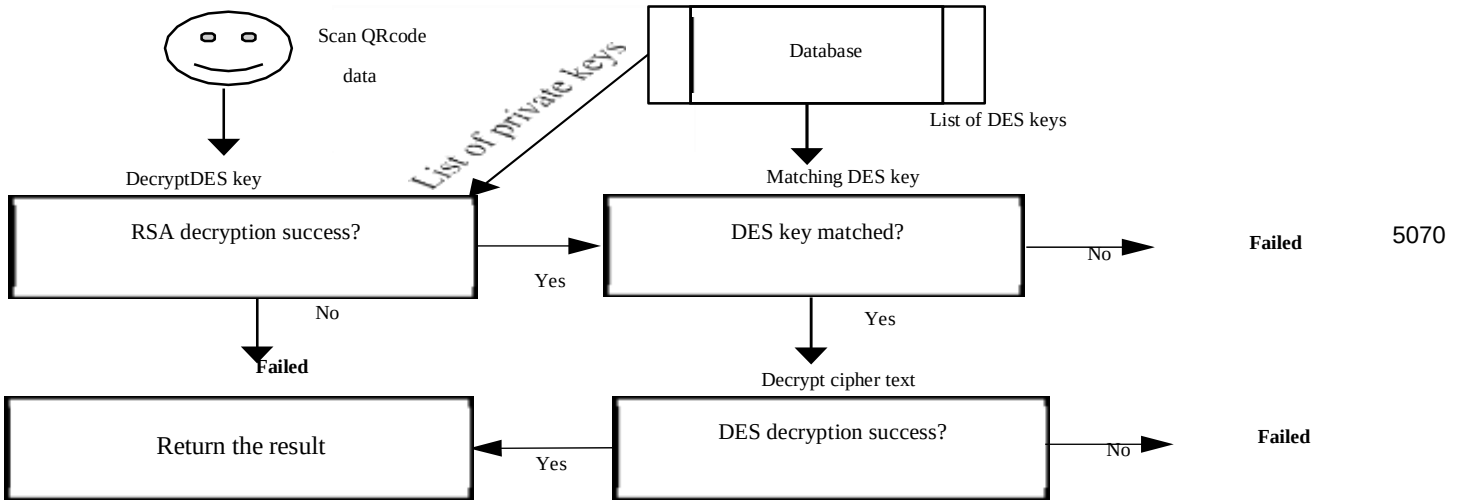

Figure 12. Decrypting scheme
(**Failed** means the product is fake)

4.4 Testing Efficiency

The paper designed an experiment to compare the efficiency of proposed scheme, which is producing the one thousand QRcodes in a row and each time the serial number is unique. The encryption performance of the proposed scheme is compared with RSA and DES and all the situations were done by JAVA (version 12.0.1) in a computer of Intel i7 8750H CPU of 4.1Ghz and 32GB RAM 2400mhz. Each circumstance is performed 20 times and computes the average**.**

Asshowninfigure,encryptingthedatawithRSAtakes3 times more than using DES and 2 times more than using proposed scheme. The scheme encrypts dataeffectively.

Method	QRCode Size	Key Length	Encryption time(s)(avg)
1.RSA	29kb	1024bits	69.267
2.DES	27kb	56bits	22.452
3.Scheme	48kb	1024/56bits	39.484

*e*ISSN1303-5150

Figure 13. Generating 1000 QRcodes

AlthoughusingDEStakestheshortesttime,butthesecurity of data can not be guaranteed. The proposed scheme`s encryption time is 43% faster than using RSA and the data is under the same security requirement. The only difference is that the size of QR code increased, since anadditional encrypted key is after the cipher text, but the size is still within the acceptable range. The efficiency of decryption is not discussed. Since decryption happens on the side of customer, usually only several QRcodes (most of the time only one) will be submitted for verification. The typical home computer can do the decryption in few seconds or evenless.

In this paper, a detailed scheme of QRcode producing, scanning and verifying is proposed for the customer easy use. The customer can verify the QRcode helpfully and the verifying process is totally automatic. A QRcode encryption techniques for commodity to anti-faking is also proposed. The proposed method achieves the strong encrypting protection and is more efficient than the classic encrypting method like RSA.

But since the situations under experiment like network connection, the security of database are ideal so if these cure of database can not be guaranteed, the encryption will be meaningless.

5.CONCLUSION

Figure 14. Over Complex QRcode (Example)

Also, the paper only considered the case of text encryption, QRcode could also be used for encrypting sound and image. The document size of the QRcode increments generally when the length of the plaintext increments, the efficiency of the encoding QRcode will be reduced and the generated QRcode will be excessively mind boggling to be scanned. (As shown in figure 8) The maximum length of the plaintext that the proposed scheme can be encrypt that is around 260 chars.

The following research will focus on the advancing the content of the QRcode, building the scanning application and the database. QRcode hostile to faking will be additionally concentrated on later on work.

6.REFERENCES:

[1] T.Sun, D.Zhou, IEEE International Conference on Automation and Logistics (ICAL)- Automatic identification technology-Application of two-dimensional code, 164-168, 2011.

[2] T.Falas, H.Kashani, 2007 “Two-Dimensional Bar-Code Decoding with Camera- Equipped Mobile Phones,” Fifth Annual IEEE International Conference on the Pervasive Computing and Communications-Workshops (PerCom Workshops 2007), 19-23 March, White Plains, New York, USA, IEEE, 2007.

[3] J.Rouillard, 2008, “Contextual QR Codes”, Computing in the Global Information Technology, The Third International Multi-Conference on IEEE, 2008.

[4] R.L.Rivest, A.Shamir, Adleman.L, 1978 “A method for obtaining digital signatures and public-key cryptosystems,” Communications of the Acm, 21(2):120-126, 1978.

[5] E.Biham, 1999,1267, “A Fast New DES Implementation in Software,” Lecture Notes in Computer Science, 1267, 1999.

[6] G.Rouvroy, F.X.Standaert, J.J.Quisquater, et al. "Efficient uses of FPGAs for implementations of DES and its experimental linear cryptanalysis," IEEE Transactions on Computers, 52(4):473-482, 2003.

[7] U.M.Maurer, 2004 "The Role of Cryptography in Database Security," Proceedings of the ACM SIGMOD International Conference on Management of Data, Paris, France, June 13-18, ACM, 2004.

[8] He.J, and M.Wang, 2002 "Cryptography and relational database management systems," Proceedings 2001 International Database Engineering and Applications Symposium, IEEE, 2002.