International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 10 No. 2 Oct. 2014, pp. 433-437

http://www.ijisr.issr-journals.org/

QR Verification System Using RSA Algorithm

K. Naresh[1] and Prathibha N. Pillai[2]

[1]PG Student [CSP], Dept. of ECE,
GVP College of Engineering (A),
Visakhapatnam, Andhra Pradesh, India

[2]Assistant Professor, Dept. of ECE,
GVP College of Engineering (A),
Visakhapatnam, Andhra Pradesh, India

ABSTRACT: Now a days, in data transmission security and authentication are the major challenges. To resolve these problems different techniques are used like cryptography, steganography etc. in the image steganography, we are using two images i.e., cover image and hidden image. The hidden image is sent by put it in the cover image. In the present techniques, only one key is used for both encryption and decryption. So, the users can see the data and also they can modify the content of the data. . Now we are using QR code which represents the hidden image and sent the QR code by encryption and decryption. We proposed a novel algorithm, in which the sender has two keys (public and private keys) and the user is provided with only one key (public key) by using RSA algorithm. Thus, the user can only see the data and he can't modify the data.

KEYWORDS: RSA algorithm, RS code, QR code, Finite fields, steganography.

1 INTRODUCTION

In this age of the digital world, with the progress of technology and continuous growth in digital data, there is a vital need of optimization of data and information presently in the digital world. The authenticity of data is the trickiest issue in management of data in the internet database. In this, we mainly consider the authenticity of security passwords, phone numbers or security information. This process also applied to steganogrphy technique to hide the secret images, route maps. Furthermore, there is no second certification on human eye verification of documents. Keeping this problem in mind, we have introduced a new digital documentation system using QR codes.

QR Code is a type of 2 dimensional matrix barcode, which is more popular than 1-D barcodes because of its large capacity of digital data and it can be readable in any mobile devices. In our new document, we save the essential data like passwords, signature in the QR Code. But, all the data saved in the QR Code, are encrypted, then the QR Codes are printed on the document.

This paper is planned as follows: Section 2 deals with Literature survey. Section 3 describes RSA algorithm. Section 4 deals with RS codes. Section 5 deals with proposed. The results and conclusions are specified in section 6 and 7.

2 RELATED WORK

Algorithms for encoding and decoding the QR codes and data security are existing in the literature. During the years, many have urbanized algorithms for QR codes, a few of them are Somdip Dey [1] proposed a method Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System. Sartid Vongpradhip [2] proposed an algorithm Use Multiplexing

Corresponding Author: K. Naresh

to Increase Information in QR Code. Prathibha.N.Pillai, K.Naresh proposed an algorithm to Improving the Capacity of QR Code by Using Color Technique.

Somdip Dey et al [1] proposed an algorithm Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System, in this algorithm encrypt the mark sheet data using the TTJSA encryption algorithm. In this method, read the 32 bytes data and it converts into bits (256 bits). These bits are XOR with with the key bits, the result bits are replaced with original bits in encryption side. In decryption side these bits are again XOR with key bits we get the original information.

3 RSA METHODOLOGY

In TTJSA algorithm we use same key in the encryption and decryption side. Due to this reason the data can be modified by the other user. To resolve this problem we can use the RSA algorithm. In this algorithm we use different key on both sides. On the encryption side, we use the private key in the same way in decryption side we use a public key.

The RSA cryptosystem is one of the famous security algorithm. In RSA algorithm, there are mainly three steps: key generation, encryption and decryption procedure.

Key Generation:

1. Select the two prime numbers p,q and p≠q.
2. Calculate n= p x q.
3. ϕ(n) calculated as ϕ(n)= (p-1) x (q-1).
4. Select integer e whose gcd (ϕ (n), e) =1, 1 < e < n.
5. Calculated such that Ed-1 is exactly divisible by ϕ (n).
6. Public key (e, n).
7. Private key (d, n).

Encryption process

Plain text --- m
Cipher text C = ((m^e) mod n).

Decryption process

Cipher text --- C
Decipher text D = ((C^d) mod n).
For example, consider p = 5, q = 3. So, ϕ(n) = (5-1)(3-1) = 8.
Therefore, e = 11, d = 3.
Plain text --- 2.
Cipher text C = (2^{11} mod 15) = 2048 mod 15 = 8.
Decipher text D = (8^{3} mod 15) = 512 mod 15 = 2.
D = m.

4 REED SOLOMON CODE

In communication, there is a possibility of occurring either single bit or multiple bit error, but in data storage it is burst errors []. So, we use the Reed-Solomon codes in the data storage. The encoding process of RS code as follows:

- Multiply the non-binary message polynomial m(x) by x^{n-k}
- Dividing $x^{n-k}m(x)$ by g(x) to obtain the remainder b(x)
- Forming the codeword $b(X)+x^{n-k}u(x)$

In the data storage, if the information bits are damaged or distorted can be retrieved by using the RS code decoding process. The steps for decoding of RS code as follows:

Step1: Calculate the syndrome vector.
Step2: Calculate the error location polynomial.
Step3: Calculate the roots of the error location polynomial.
Step4: Calculate the value of the errors, and do the error correction.

5 PROPOSED METHOD

In this paper proposed a new algorithm for Confidential data based on the RSA algorithm. In this algorithm the confidential information is encrypted by using RSA algorithm, then we generate the QR code. The following steps explain the encoding process.

Step 1: enter the confidential information.
Step2: each character is converted into ASCII equivalent, then apply the RSA algorithm for each value with Private key.
Step3: generate the codeword for the given information by using non-binary RS code, due to this if the QR is damaged or distorted it is retrieved.
Step 4: convert the codeword into binary and place these bits in QR pattern.

The decoding process is as follows:

Step 1: read the QR image as the input to the decoding process.
Step 2: eliminate the unwanted bits in QR code(finder patterns) and read the information bits from QR code.
Step 3: convert these bits into decimal and eliminate the parity bytes by using an RS decoding process.
Step 4: apply the RSA algorithm by using Public key to get the original information.

6 EXPERIMENTAL RESULTS AND DISCUSSIONS

In this paper, we focus on the confidential data like password or signatures. For example, consider the confidential information is a password for locker like ABCD1234. By applying the RSA algorithm for this key it is converted into some other format as follows:

A means it's ASCII is 65.

65^11 = 87507831740087890625.

87507831740087890625 mod 15 = 5.

Similarly, convert the all characters by using RSA algorithm. Then we generate codeword for this information by using Reed Solomon code for retrieve the information if the QR is damaged. For generation codeword is done by using simlink in matlab the block diagram as follows:

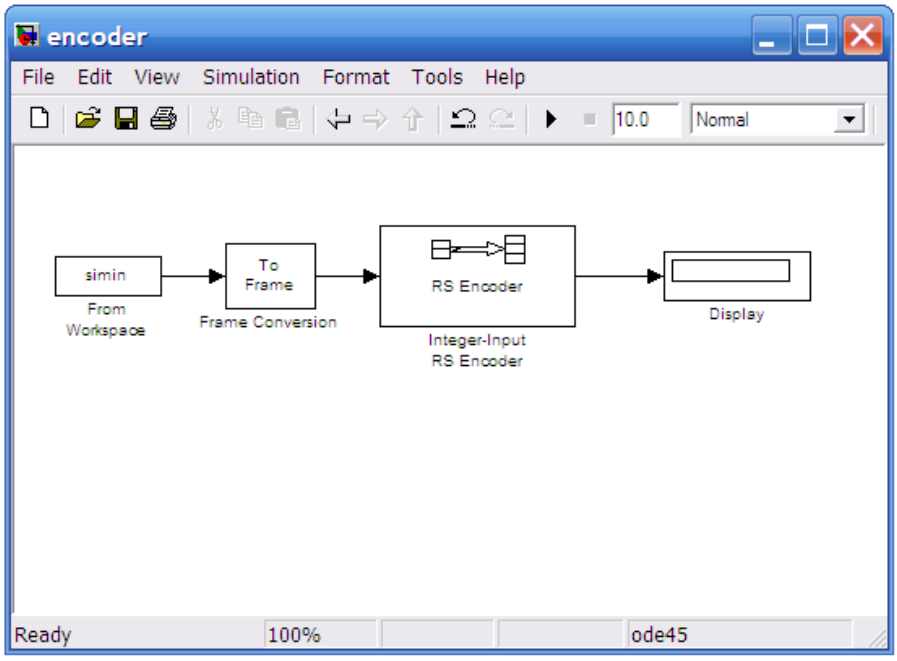

Figure 1: RS encoder diagram using simlink

Figure 2: QR code for given information

Figure 2 shows the QR code for the given information. It contains the codeword of the given information of length 255 because it is a (n, k) encoder. Here n = 255, k=length of message.

In the same way, in decoding side the QR is considered as input image. Read the information bits from the QR code and eliminate unwanted bits like finder patterns. This codeword is given as input to the RS decoder. RS decoder using simlink is shown below.

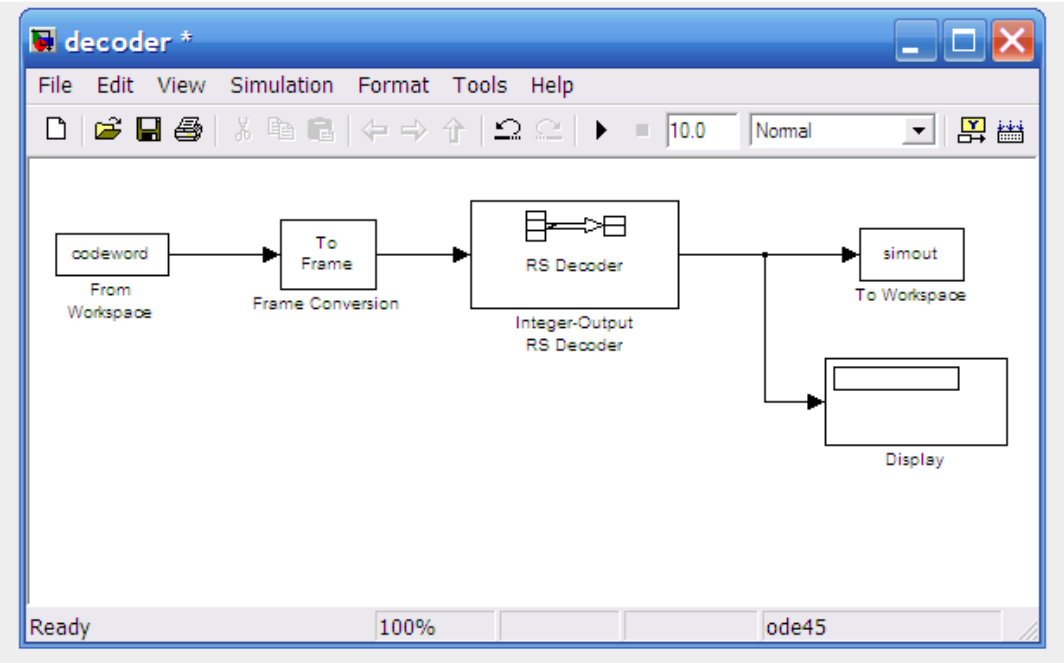

Figure 3: RS decoder diagram using simlink

In figure 3, simout gives the cipher text of the RSA algorithm. Applying the RSA decoding processor for getting plain text or password (ABCD1234).

7 CONCLUSION

In this paper, a new algorithm is implemented for confidential information. As compared with single password secure systems, this method has high security. Due to beauty of RS code if the QR is damaged up to 30% can also be retrieve the information from QR code. This algorithm is also useful in image processing for cryptography and steganography.

REFERENCES

[1] Somdip Dey 'Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System" International Conference on Communication Systems and Network Technologies 2013.
[2] Sartid Vongpradhip 'Use Multiplexing to Increase Information in QR Code'The 8th International Conference on Computer Science & Education (ICCSE 2013) April 26-28, 2013.
[3] Prathibha.N.Pillai, K.Naresh "Improving the Capacity of QR Code by Using Color Technique" ijareeie, Vol. 3, Issue 7, July 2014.
[4] Chun Jin and Jianghong Yuan "Optimization of RS Error-Correcting Decoding Algorithm for QR Code" 5th International Conference on BioMedical Engineering and Informatics, 2012.
[5] Jantana Panyavaraporn, "QR Code Watermarking Algorithm based on Wavelet Transform", 13th International Symposium on Communications and Information Technologies (ISCIT), 2013.