Information Hiding Using Qr Code

Iswaryah.G, Ramachandran.A

ABSTRACT: There are various types of information's are transferred within mile seconds so these information's have to be secure .there are different types of algorithm are used for both for securing of data and also for transmission of data.in this paper we use QR Code for the secure transmission of data. Data can be of any type for example image, text, audio or video and even most of the money transaction is made through the QR Code, etc…In this paper, we are going to talk about how to share big organized companies sensitive information or data can be securely transferred using the QR Code .The sensitive information like auditing files of a company.

1 INTRODUCTION:

In this paper, we proposed an idea for sharing the sensitive information through the QR code. In this paper we first encrypt the sensitive information using the Advanced Encryption Standard, then the encrypted file is then hidden or again encrypted using the QR code, then send it to the user who is going to scan and download the file. First, the user will scan the QR code and the encrypted file will be download than can be decrypted using the reverse process of the Advanced Encryption Standard algorithm

1.1 QR CODE:

QR code is Quick Response code which is of type two dimensional bar code . It is formed in the form of a matrix of dots. It can be scanned using a QR Code scanner or with the Smartphone camera [1]. QR Code is generally used for any purpose in these days like transferring files, documents, audios, videos, etc… so the next generation level transaction like UPI (Unified Payment Interface) money transfers and sharing most sensitive information through the QR Code The QR code was initially invented to keep track of the manufacturing company where the vehicle part is manufactured so that it can be easy to identify the parts if it is missing. In the year 1994 Toyota subsidiary, Denso Wave created the QR code .The idea of creating a bar code makes the creation of QR code because the bar code can hold only twenty alphanumeric characters but QR code can store more data than that. Nowadays QR code is used more than tracing the vehicle parts .QR code is used more in smart phones and also in other fields from tracking manufacturing vehicle parts to simple scans to pay our bills in the restaurant and mainly attracted by the Smartphone user to scan and easy to go. Using the API (Application Program Interface) the user created the QR code. Customized QR code can be created like logo, users can innovate their own type of QR code The QR code is similar to other cryptography systems. It consists of an encoder to change the original data or text into encrypted form and a decoder to convert the encrypted form into the original text .

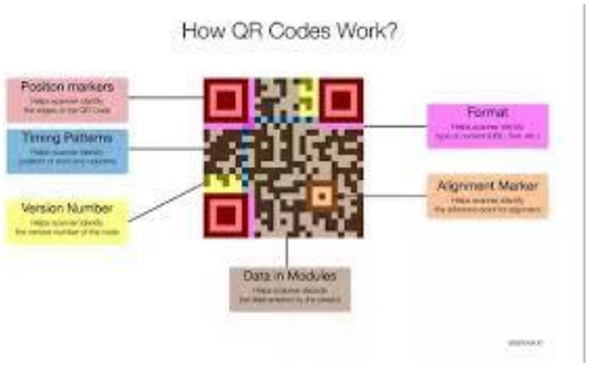
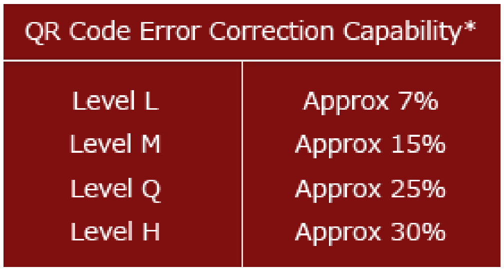


Figure 1.1 *outline structure of QR code*

ERROR CORRECTION:

[3]The data will be encrypted and decrypted, during that process is an error has occurred during the decryption we have to recover the error and get the data back. QR code uses an algorithm to recover error that is the Reed Solomon error correction algorithm. QR code has the capability to restore data if it has been damaged or code is dirty .there are four error-correcting levels that are provided for the user to choose based on the type of data they are going to encrypt .the four error-correcting algorithms are chosen by the user based on the operating environment. Increasing the level of the error correction capability in which the intern increases the size of data stored in the QR code. There are different levels of the QR code to select a specific error correction level many factors have to be considered .the factors to be considered as the operating environment and the size of the QR code.[3] Level Q and H are used for the factory environment; the error correction recovery capacity is in between 25%-30%. The next level of error correction is Level M is most widely used, the error correction capacity of Level M is 15% and the last Level L which is used in the cleaner environment with huge amount of data, the error correction capacity of this level is 7%.increase in the capacity of error correction which in turn increase the amount of data that are added to the QR code.



QR Code Error Correction Capability*	
Level L	Approx 7%
Level M	Approx 15%
Level Q	Approx 25%
Level H	Approx 30%

Figure 1.2 *levels of error correction*

- *Iswaryah. G is currently pursuing master's degree in computer science and engineering in B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, India. E-mail: sharukhrahman.sr@gmail.com*
- *Dr. Ramachandran. A , B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, India. E-mail: msg2chandran@gmail.com*

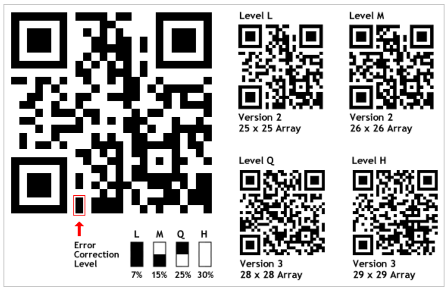


Figure 1.3 *Error correction structure*

1.2AES ALGORITHM:

AES stands for Advanced Encryption Standard. [5]Advanced Encryption Standard is used for encrypting large data, and Advanced Encryption Standard is more secure than the other algorithm used for encryption. AES is a block cipher utilized as an encryption technique. AES was created by Daemen and Vincent Rijmen both were a Belgian cryptographers. Rijnded cipher was the base idea behind the development of the Advanced Encryption Standard. The encryption block size is fixed in Advance Encryption Standard like 128-bit, 192-bit, and 256-bit encryption block. These secure encryption keys are created because of the Brute force attack during 2006 which made 56-bit RC5 key powerless.

1.2.1ENCRYPTION:

Encryption is a process of changing the original text (plain text) into encrypted text (cipher text).In AES the encryption can be divided into three parts. In the first part of the encryption process Add round key, the second part comprises Sub Bytes, Shift rows, Mix columns and Add round key. The third part of the encryption process comprises of Sub bytes, Shift rows and Add round key

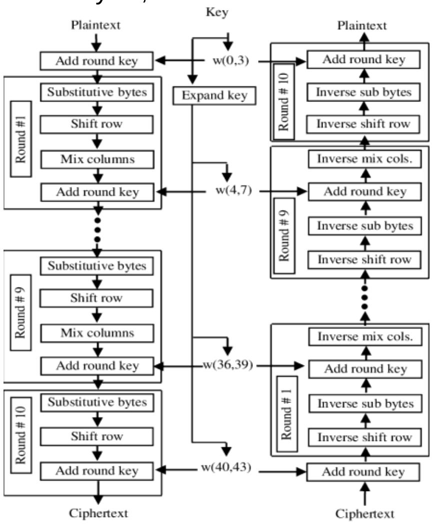


Figure 1.2.1 *AES Encryption*

In Advance Encryption Standard has some specification, the plaintext is the input and then the input is put through the number of transformation rounds that convert the plaintext. The final output after applying all the transformation comes to the output called cipher text. The transformation rounds as follows:

1. One hundred twenty eight -bit keys for ten rounds
2. One hundred ninety two -bit keys for twelve rounds
3. Two hundred fifty six-bit keys for fourteen rounds

Sub Bytes

In sub byte part of Advance Encryption Standard comprises of splitting the input data (plaintext) or information into bytes and moving each through a substitution box or S-box. The Advanced Encryption Standard S-Box is implemented based on inverse multiplication.

Shift Rows

The row is moved one by one the shift row is the next operation that is done in the Advance encryption standard. The one hundred twenty-eight bit of internal state of the cipher is moved in each row. Each row in Advanced Encryption Standard is a standard representation of the internal state, which is of 4*4 matrix's where each cell lies of a byte [5]. In a column, the bytes are placed in matrices form from left to right. In the operation of shift rows, each of those rows is moved left by some amount, the rows are numbered and the starting cell is numbered as zero. The top row of the matrix is not shifted at the wall, the next one.

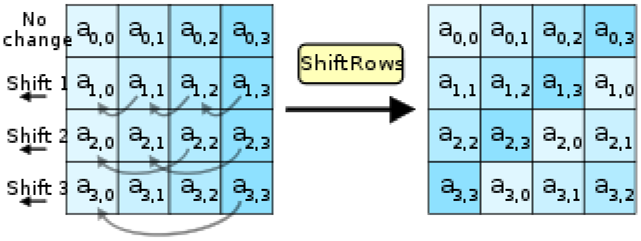


Figure 1.2.2 *Shift rows*

Mix Columns

The next phase of the Advance Encryption Slandered is mix columns. The mix column part provides the diffusion by mixing the input rounds, similar to shift rows the mix column also do some operations like splitting the matrix by column instead of rows

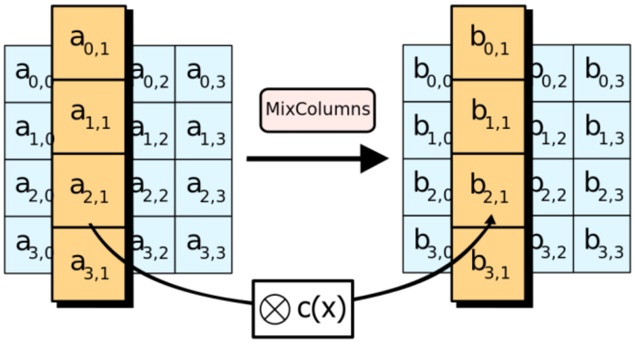


Figure 1.2.3 *Mix Columns*

Add Round Key

The next part of the Advanced Encryption Standard is Add Round Key. In this part of the encryption, the round keys are directly operated. The input to this part of encryption is based on the round key.

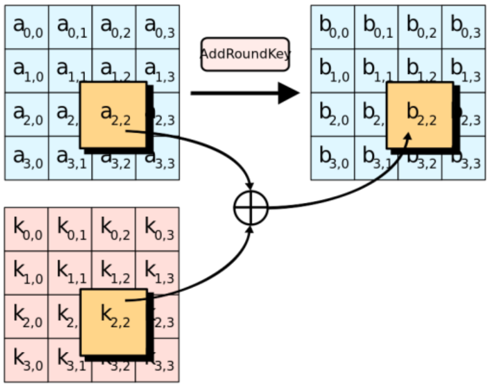

AddRoundKey
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
$k_{0,0}$ $k_{0,1}$ $k_{0,2}$ $k_{0,3}$
$k_{1,0}$ $k_{1,1}$ $k_{1,2}$ $k_{1,3}$
$k_{2,0}$ $k_{2,1}$ $k_{2,2}$ $k_{2,3}$
$k_{3,0}$ $k_{3,1}$ $k_{3,2}$ $k_{3,3}$

***Figure 1.2.4** Add round key*

1.2.2 DECRYPTION:

The decryption process in Advanced Encryption Standard is the same as the encryption but the difference is the decryption is a reverse process .the decryption process also contains operations like shift rows, mix columns, add sub bytes and add round key.

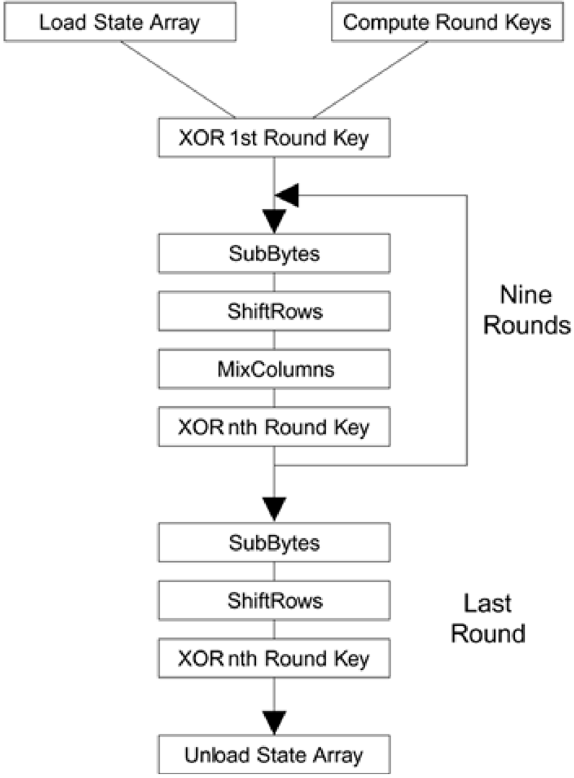


***Figure 1.2.2.1** Decryption*

The decryption process is similar but it is the opposite of the encryption process.

CONCLUSION:

The conclusion is we can use these in the ATM, government sectors for secret data transmission and it mainly focused on the auditing sectors, because in auditing the data are still stored in the hard disk or pen drive .we can implement this in cloud so that the data auditing files can be stored and transmitted using the cloud technology, which in reducing many things including the resources.

REFERENCES

[1] Sumit Tiwari," An Introduction to QR Code Technology" Published in: 2016 International Conference on Information Technology (ICIT)

[2] Dong-Hee Shin, Jaemin Jung, Byeng-Hee Chang "The psychology behind QR Codes: User experience perspective", Science Direct, Computers in Human Behavior 28 (2012) pp 1417-1426.

[3] QR Code, http://www.QR code.com/en/

[4] Babitha M.P. ; K.R. Remesh Babu, "Secure cloud storage using AES encryption" Published in: 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)

[5] Shrivathsa Bhargav, Larry Chen, Abhinandan Majumdar, Shiva Ramudit, 128-bit AES decryption, CSEE 4840, 2008