IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

QR code Authentication System for confidential (digital Mark sheet) Encrypted data hiding and retrieval (Decryption)

Supriya Chavan [1], Sujata Gadakh [2], Gholap Kanchan [3], Sorte Surabhi [4], Prof. D. V. Shinkar [5]

Information Technology, JSPM Bhivarabai Sawant Institute of Tech & Research, Wagholi, Pune, India [1,2,3,4,5]

Abstract: Nowadays, we hear news about fake mark sheets, fake transcripts, fake degree certificates etc. With latest printing and scanning technologies convenient and reasonable available, creating simulated documents have become an easy affair, making it tough to understand between original and the artificial. So it is a very big challenge to provide security and authenticity of digital data. This paper proposes an innovative method to authenticate the digital documents. A advanced method of QR code is introducing here, which grant multiple encryption and decryption of digital data. In this paper, we introduced a new technique, where the resume of a candidate will be encoded in QR [Quick Response] Code in encrypted form, so that if an hacker tries to change the data in the resume then he cannot do that. This is because; the encryption key is unknown to him. Encrypted QR codes are QR codes that everyone cannot scan and access. They are not very typical, since maximum QR codes are used in marketing, and the developers of those codes want them to be accessible by everybody. Protect QR codes can be built that make the scanner enter a password to be able to access the content. We are using TTJSA algorithm method for encryption and decryption purpose. TTJSA is very effective method; we encrypt the mark sheet information using the TTJSA encryption algorithm. The encrypted marks are entered inside QR code and that QR code is also printed with the initial information of the mark sheet. The marks can then be retrieved from the QR code and can be decode using TTJSA decryption algorithm and then it can be verified with marks already there in the mark sheet.

Keywords: QR Barcode, Information Hiding, Encryption Decryption, TTJSA.

I. INTRODUCTION

Quick Response (QR) code is a 2-dimensional matrix barcode; 2D barcodes (a group of barcodes the QR code belongs to) are equivalent to regular, 1-dimensional bar codes as they are e.g. used on the product packaging at the grocery store. However, QR code are able to store more data; they can include over 3000 characters on a very small space. This gained popularity because of its holding large capacity of digital data and it can be integrated in any mobile devices. It can be applied to encrypt data in secure system, banking sector, mobile network. QR code was invented by DENSO CORPORATION in 1994. recognized as AIMI Standard in 1997 and ISO/IEC Standard in 2000. Adapted as an industry-wide standard code by AIAG, JAMA and JTA. High stability by a reader is pursued. QR code is a barcode which is readable by any camera like ,smart phone. They are normally seen as a white square with black geometric shapes. Users point their phones at the QR code, scan it, and then taken to the end data.

QR Codes are two-dimensional bar-code with endless potential for embedded information. The QR code was developed by the automotive zone for tracking item and data associated with the parts. Unlike traditional bar codes commonly used in market, the QR code is capable of storing more information and links to digital media. The QR code is multifaceted and can working as a link or storage system for info. The QR codes are scanned by a digital device and the user is either provided with the information inserted in the QR code or routed to the link associated with the QR code. Link codes are regular but the reach of QR codes is endless and these codes are gaining popularity in retail, web and mobile applications.

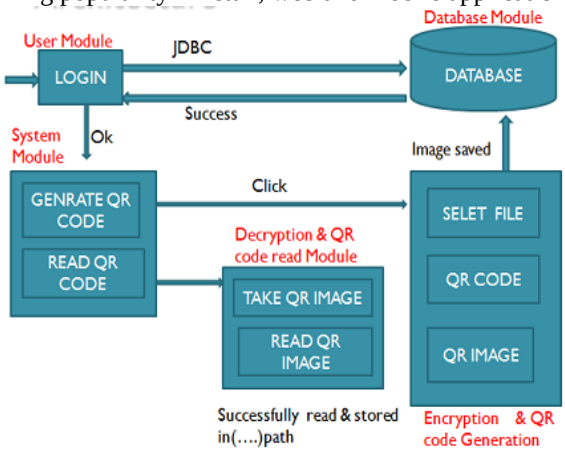

Fig 1 : System Architecture

Encoding of QR Code:
Each QR Code symbol subsist of an encoding region and function patterns, as shown in Fig 1. Finder, separator, timing figure and alignment figure comprised function patterns. Function patterns shall not be used for the encoding data. The finder figures placed at three corners

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

of the symbol intended to assist in easy location of its position, size and inclination.

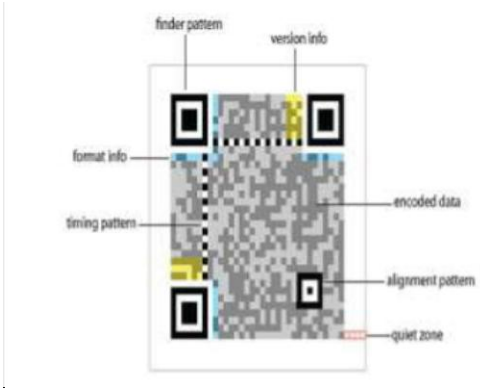

Fig 2 : Encoding of QR code

The encode operation of QR Code including follows steps. Firstly input data is encoded in according to most efficient mode and formed bit stream. The bit streams are divided into code words. Then code words are divided into blocks, and add error correction code words to each block. All these code words are put into a matrix and are masked with mask pattern. Finally function patterns are added into the QR symbol. A QR Code symbol is formed.

a) Finder Pattern
A pattern for detecting the place of the QR Code. By arranging this pattern at the three corners of the size, a symbol, the position, and the angle of the symbol can be detected. This finder pattern consists of a structure can be detected in all the directions (360).

b) Alignment Pattern
A pattern for correcting the distortion of the QR Code. It is highly efficient for correcting nonlinear distortions. The central coordinate of the alignment pattern will be identified to correct the distortion of the symbol. For this purpose, a black isolated cell is placed in the alignment pattern to make it easy to detect the central coordinate of the alignment pattern.

c) Timing Pattern
Pattern for recognizing the central coordinate of each cell in the QR Code with black and white patterns arranged alternately. It used for correcting the central coordinate of the data cell when the symbol is distorted or when there is an error for the cell pitch. It arranged in both vertical and horizontal directions.

d) Quiet Zone
A margin space essential for reading the QR Code. This quiet zone makes it easier to have the symbol detected from the image read by the CCD sensor. Four or more cells are necessary for the quiet zone.

e)Data Area
The QR Code data will be store (encoded) into the data area. The grey part in Figure 3 represents the data area. The data will be encode into binary numbers of 0 and 1 based on the encoding rule. The binary numbers of(0 and 1)will be converted into black and white cells and then will be arranged. The data area will have Reed-Solomon code in corporate for the stored data and the error correction functionality.

f) Linking Functionality of the Symbols
QR Code has a link functionality which will enable a single symbol to be represented in several symbols by dividing it . A symbol can be divided into 16 symbols at maximum. The example shown in Figure 1 is one where a single QR Code is divided into four symbols, and each symbol has an indicator showing how many symbols the original symbol had been divided and in which order that specific symbol would be among

II. LITERATURE SURVEY

a) Hiding of Confidential Information and its Retrieval using Advanced Algorithms and QR Authentication system, Mamtha Shetty.
In this era of digital world, with the evolution of technology, there is an essential need for optimization of online digital data and important information. Nowadays, Security and Authenticity of digital data has become a big challenge. This paper proposes a new method to authenticate the digital documents. A new method of QR code is introduced here, and which allows multiple encryption and decryption of digital data. In this paper, we propose a new method, where the resume of a candidate will be encrypted in QR [Quick Response] Code in encrypted form, so that if an intruder tries to change the data in the resume then he can't do that. It is because; the encryption key is unknown to him. Encryption changes data or information that is usually plaintext by usage of an algorithm so that someone must possess certain knowledge to access it. which is normally called as key. For example, something is encrypted if someone enters a password to access it. Encrypted QR codes are QR codes that everyone cannot scan and access. They are not too common, since many QR codes are used in marketing, the developers of those codes want them to be accessible by everybody. Secure QR codes can make the scanner enter a password to be able to access the content.

b) Confidential Encrypted Information Hiding and Retrieval by Using QR Authentication System, Asoke Nath, Somdip Dey, Shalabh Agarwal.
Now, authenticity and security of data is a big challenge. To correct this problem, we propose an innovative method to authenticate the digital documents .In this paper, we propose a new method, where the marks obtained by a candidate will also be encoded in QR Code TM in encrypted form, so that if an hacker tries to change the marks in the mark sheet then he cannot do that in the QR Code TM, since the encryption key is unknown to him. In this method, we encrypt the mark sheet information with the help of TTJSA encryption algorithm .The encrypted marks are entered inside QR code and that QR code is also printed with the actual data of the mark sheet. The marks can then be retrieved from the QR code and can be

decrypted using TTJSA decryption algorithm and then it can be checked with marks already there in the mark sheet.

c) Encryption and Decryption of Data Using QR Authentication System, Atul Hole1, Mangesh Jadhav2, Shivkant Kad3, Swanand Shinde4.
In this paper, we explore how QR codes can be used in education. The low technical barrier of creating and fetching QR codes allows innovative educators to incorporate them into their educational endeavors. Security the data is a big problem. And to solve this we propose an efficient method to authenticate digital information presents in our documents. If someone tries to change the information of the document that intruder cannot do that in QR Code. In this Paper we are encrypting the data using encryption Algorithm. The information which is encrypted are entered inside the QR code and it will be also printed with the original data of document. Then the data can then be retrieved from the QR code and can decrypt using decryption algorithm. And finally it can be verified data that are already presents in the document.

d) QR Code and Application in India. Suraj Kumar Sahu, Sandeep Kumar Gonnade
This paper examines QR Codes and how they can be composed and scan and then decrypt by a camera. QR code is 2-dimensional barcode used for quick response in promotional and marketing purpose. The paper details about QR code, how QR code is different from barcode, It's Capacity, formation and Error correction code. It's application in India and worldwide.

e) Symmetric key cryptosystem using combination of cryptographic algorithms - Generalized modified Vernam Cipher method, MSA method and NJJSAA method: TTJSA algorithm.
In this paper the authors have introduced a new combined cryptographic method called TTJSA. Nath et al. had already developed some symmetric key methods. In the present work the authors have used two methods MSA and NJJSAA were developed by Nath et al. and have developed a new algorithm, generalized modified Vernam Cipher Method. The above three methods are used in random order on any given plain text for a number of times to get the ultimate cipher text file. In this, authors modified the standard Vernam Cipher Method for all characters (ASCII code 0-255) with randomized keypad, and also introduced a feedback mechanism. The method has been closely monitored on various known plain text and it was found that this method is almost unbreakable.

The present method allows multiple encryption / decryption. This method is an extremely secure block cipher method and it can be applied to encrypt data in Banking sector, Defence system, mobile network etc. The advantage of the present method is that one can use this method on top of any other standard algorithm such as DES, AES or RSA. The method is suitable to encrypt any type of file.

III. RELATED WORK

Encryption and Decryption
In cryptography, encryption is the process of encoding messages (or information) in such a way that hackers cannot read it, but that authorized person can. In an encryption scheme, the message or information is encrypted with the help of an encryption algorithm, turning it into an unreadable cipher text (ibid.). This is normally done with the help of an encryption key, which specifies how the message is to be encoded. Any adversary that see the cipher text should be unable to determine anything about the original message. An authorized person, however, is able to decode the cipher text with the help of a decryption algorithm, that usually requires a secret decryption key, that intruders do not have access to. For technical purpose, an encryption scheme usually requires a key-generation algorithm to randomly produce keys.

In recent world most commonly used encryption technique in QR Codes is DES (Data Encryption Standard), but the method already broken in Different Attack, a method used to cryptanalysis and analyse the algorithm apply for encryption and decryption. So, maximum institutions/organizations use their own methods to encrypt QR Code data. But till now most of those techniques have been hacked or are very less. In this we have tried to implement TTJSA encryption technique, which is unbreakable with common cryptography attack such as Differential attack, known plain text attack or Brute Force method. Now we will discuss TTJSA cryptography algorithm.

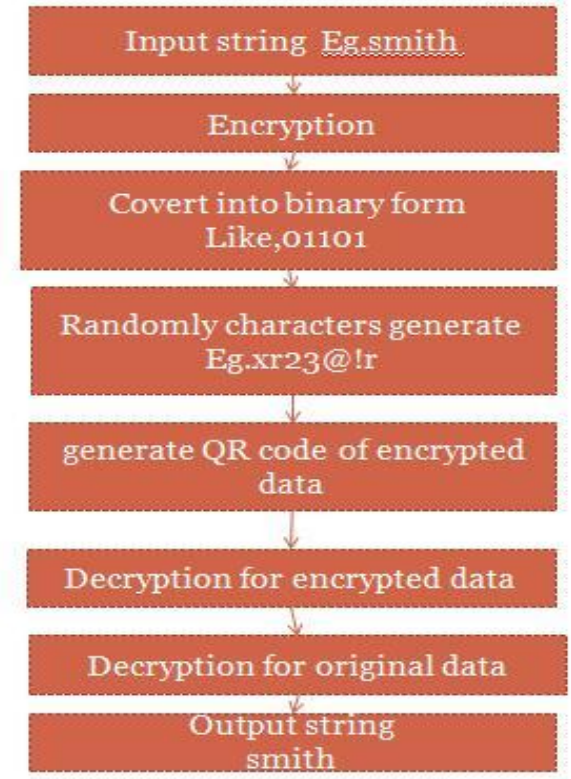

Fig 3.Encryption and Decryption process

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

Need of Encrypted QR Code
One of all the applications that come to mind is to use encrypted QR codes on passports, driver license and other documents or even loyalty cards. Assume that every citizen will have a hidden Id residing in governmental secured database. This hidden Id points in the database to an overt Id printed on the passport together with a name and other personal details. The QR code encrypts a URL and the hidden Id. An inspector scanning the QR code will get from the secured database all information linked with the hidden Id including name, birth date address and more. All the inspector's duty is to compare the received data to that on the passport. With today technology even the image that is on the passport can be sent for comparison.

IV. MOTIVATION

The tremendous growth in internet technology in the last decade has made it a real challenge for a sender to send private data from one computer to another. There is no guarantee that, between a sender and a receiver, there is no one intercepting those private data, provided the data is not encrypted or properly protected. The security of data is now a very important aspect in data communication network. If we send any confidential or important message from one computer to another via internet, then, a hacker might intercept that confidential/important message. So we are proposing a system that can be useful to increase Security and Authenticity of digital data.

V. ALGORITHM

TTJSA for Encryption Purpose of the Embedded Data:
TTJSA is a combined symmetric key cryptographic method, which is formed of generalized modified Vernam cipher, NJJSA and MSA are symmetric key cryptographic methods. Brief study of the methods used in TTJSA algorithm is as follows:

1.Modified Vernam Cipher:
In this method, we break the whole file into different small blocks (like in Block Cipher system []), where size of each block should be less than or equal to 256 byes. Then we follow these steps:

Step1: Perform usual Vernam Cipher method with the block of randomized key i.e. each byte of blocks of the file + each byte of the blocks of randomized key.

Step 2: If the pointer points the end of each block then after performing Vernam Cipher method, pass the remainder of addition of the last byte of the file block along with the last byte of key to the next file block and add the remainder with the first byte of the that file block. (This mechanism is called feedback mechanism)

Step 3: Perform Step 1 and Step 2 till the whole file is encrypted and repeat this step for random number of times. After performing the all the above steps, we again merge the blocks of the encrypted file and thus we get the final encrypted output of this modified Vernam Cipher method.

2.NJJSAA Algorithm:
The encryption number (=secure) with randomization number (=times) is calculated according to the method given in MSA algorithm [2].

Step 1: Read 32 bytes at a time from the input file.
Step 2: Convert 32 bytes into 256 bits and store it in some 1- dimensional array.
Step 3: Choose the first bit from the bit stream and also the required number(n) from the key matrix. Interchange the 1st bit and the n-th bit of the bit stream.
Step 4: Repeat step-3 for 2nd bit, 3rd bit...256th bit of the bit stream
Step 5: Perform right shift by one bit.
Step 6: Perform bit(1) XOR bit(2), bit(3) XOR bit(4),...,bit(255) XOR bit(256)
Step 7: Repeat Step 5 with 2 bit right, 3 bit right,...,n bit right shift followed by Step 6 after each completion of right bit shift.

3.MSA Encryption and Decryption Algorithm:
Nath et al. [2] proposed a symmetric key method where they have used a random key generator for discovering the initial key and that key is used for encrypting the given source file. MSA method is basically a substitution method where we use 2 characters from any input file and then search the corresponding characters from the random key matrix and save the encrypted data in another file. MSA method provides us multiple encryptions and multiple decryptions. The key matrix (16x16) results from all characters (ASCII code 0 to 255) in a random order. The randomization of key matrix is done using function calls:
Step-1: call Function cycling()
Step-2: call Function up shift()
Step-3: call Function downshift()
Step-4: call Function left shift()
Step-5: call Function right shift() How the above functions will work is discussed in detail by Nath et al[1]. The logic of these functions is to make elements in a square matrix in a random order so that nobody can predict what will be the closest neighbour of a particular element in that matrix. This method is basically modified Play fair method. In Play fair method one can only encrypt Alphabets but in MSA one can encrypt any character whose ASCII code from 0-255 and one can use multiple encryption here which is not possible in normal Play fair method.

VI. RESULT AND EVALUATION

System Evaluation
We conducting our evaluation experiment to encrypt QR code using TTJS algorithm I represent the methodology of QR code that provide the encoding and decoding capacity also use the stenography then calculate the following result;

1. Integration of QR code resolve the capacity problem and store the max data as compare other conventional barcode. The QR code save the data both direction vertical and horizontal. So it can increase the limit of storing the data. Mostly the QR code stores the numeric, alphanumeric, binary (8bit) data.

2. The QR code increases the security of data or information. When we want to send any massage or personal data then encode the data in QR code and then send it to the receiver so it can be very confusions for access the data because we can see only the QR code image but not data.

3. Integrate the two QR code image. The first QR image as a cover images another can be use the actual data. When integrate the QR image encode any data and now encode the data which will be very secure now encrypt and integrate using stenography. Now if we want access the data then firstly steno decrypt the QR code and find the data. If we want to send any other data or information like; audio clip, video clip, word file etc; then we can use the stenography encryption and decryption and integrate the data and encrypt now embed the data now send to the receiver side.

4. The QR code is to much user friendly because the data can be access only single scan by using the smart phone. If we want to read the data from the QR code image then we can use the smart phone using the android application and scan the QR code image by capturing in camera and scanning the image and find the data.

5. The QR code can use in magazine, newspaper etc and encrypted QR code can also be used in driving license, shopping card etc.

VII. CONCLUSION

With the analysis of all these three algorithms using various formats of images we conclude that the Vernam method is more acceptable for encrypting the images or data. Comparing, TJJSA Hiding of Confidential Data or information and its Retrieval by using Advanced Algorithms and QR algorithm as it has the larger PSNR value and Less MSE value it is less considered for the encrypting of any information.

REFERENCES

[1]. Mamtha Shetty “Hiding of Confidential Data and its Retrieval using Advanced Algorithms and QR Authentication system” (Nov – Dec. 2014).
[2]. Asoke Nath, Somdip Dey, Shalabh Agarwal, “Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System- (2013 International Conference on Communication Systems and Network Technologies)
[3]. Suraj Kumar Sahu, Sandeep Kumar Gonnade, “QR Code and Application in India” (International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-2, Issue-3, July 2013)
[4]. Symmetric key cryptosystem using combined cryptographic algorithms - Generalized modified Vernam Cipher method, MSA method and NJJSAA method: TTJSA algorithm “ Proceedings of Information and Communication Technologies (WICT), 2011 “ held at Mumbai, 11th – 14th Dec, 2011, Pages:1175-1180.
[5]. "QR Code, Wikipedia", http://en.wikipedia.org/wiki/QR_code [Online] [Retrieved 2012-02-09]
[6]. Cryptography and Network Security, William Stallings, Prentice Hall of India.
[7]. Cryptography & Network Security, Behrouz A. Forouzan, Tata McGraw Hill Book Company.

DOI 10.17148/IJARCCE.2016.5424