Secret Data Hiding Into Images and Retrieval from Images Using QR Codes

Shruthi. K. Mathad
Research Scholar, Dept of EC&E,
GMIT Davanagere, India.
Email id: mathadshruthi@gmail.com

Shivakumar. B. R
Asst. Professor, Dept of EC&E,
GMIT Davangere, India.
Email id: shivkumarbr@gmail.com

***Abstract*—now, security and authenticity of data is a big challenge. To solve 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 be encoded in QR Code in encrypted form, so that if an intruder tries to change the marks in the mark sheet then he cannot do that in the QR Code, because the encryption key is unknown to him. In this method, we encrypt the mark sheet data using the TTJSA encryption algorithm. The encrypted marks are entered inside QR code and that QR code is also printed with the original 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 verified with marks already there in the mark sheet.**

Keywords- communication technology; QR Code; encryption; decryption.

I. INTRODUCTION

In this era of digital world, with the evolution of technology and un-ending growth in digital data, there is an essential need of optimization of online data and information present in the digital world. The most important issue in data is that it should be original and correct. The authenticity of data is the most challenging issue in management of data in the internet database. In the present study we mainly focus on authenticity of marks in a printed mark sheet. However the present method can be applied to any other legal documents also. We know every year billions of students pass and have passed from different schools, colleges and Universities all over the world. At the same time there is no scientific method to test the authenticity of data from any printed document. Mostly we depend on checking by human eye where human eye may not function always perfect. Moreover there is no second verification on human eye verification of document. Keeping this problem in mind, we have introduced a new digital mark-sheet system. In our new mark-sheet system, we will be embedding the data digitally in form of QR Code [1][2], which is itself encrypted, so that the marks obtained by the student cannot be tampered, and the data embedded in the mark-sheet can be only decrypted and read from our decryption program. In this way, we do not have to increase our digital space or add new servers to our already existing system just because to save more marks record of students.

QR Code [4][6] is a type of 2 dimensional matrix barcode, which gained popularity because of its large capacity to hold digital data and it can be integrated in any mobile devices. In our new mark-sheet system, we save the essential data of each student in the QR Code, like the student’s name, roll number, registration number, semester and year of study, marks obtained in different subjects and grades secured. But, all the data saved and embedded in the QR Code, are encrypted, and then the QR Codes are printed in the mark-sheet of the student. So, in future if the student or any other person wants to see their marks digitally or wants to send their academic information to any University or Organization in digital format, then they can just scan the QR Code and decrypt the embedded information and send the authentic data.

II. METHODS USED

We use TTJSA [1] encryption algorithm is an amalgamation of three different cryptographic modules: generalized modified Vernam cipher [1], NJJSA [2] and MSA [3], for then encryption purpose of data in the QR Code. After encrypting the data, we embed the data in the QR Code using a set of different protocols and ultimately generate the encrypted QR Code. We discuss the procedure elaborately in the following sections.

A. TTJSA for Encryption Purpose of the Embedded Data

TTJSA [1] is a combined symmetric key cryptographic method, which is formed of generalized modified Vernam cipher, MSA and NJJSA symmetric key cryptographic methods. Brief study of the methods used in TTJSA algorithm is as follows:

1) Modified Vernam Cipher

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

Step1: Perform normal 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 reaches the end of each block then after performing Vernam Cipher method, pass the remainder of the addition of the last byte of the file block with the last byte of the 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 until the whole file is encrypted and repeat this step for random number of times.

After performing the aforementioned steps, we again merge the blocks of the encrypted file and thus we get the final encrypted result of this modified Vernam Cipher method.

2) NJJSAA Algorithm

The encryption number (=secure) and randomization number (=times) is calculated according to the method mentioned 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 in some 1-dimensional array.

Step 3: Choose the first bit from the bit stream and also the corresponding number (n) from the key matrix. Interchange the 1st bit and the nth bit of the bit stream.

Step 4: Repeat step-3 for 2nd bit, 3rd bit...256-th 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

It is a symmetric key method where they have used a random key generator for generating the initial key and that key is used for encrypting the given source file. MSA method is basically a substitution method where we take 2 characters from any input file and then search the corresponding characters from the random key matrix and store the encrypted data in another file. MSA method provides us multiple encryptions and multiple decryptions. The key matrix (16x16) is formed from all characters (ASCII code 0 to 255) in a random order. The randomization of key matrix is done using the following function calls:

Step-1: call Function cycling()

Step-2: call Function upshift()

Step-3: call Function downshift()

Step-4: call Function leftshift()

Step-5: call Function rightshift()

The idea of these functions is to make elements in a square matrix in a random order so that no one can predict what will be the nearest neighbor 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 apply multiple encryptions here which are not possible in normal Playfair method.

B. Generation of QR Code

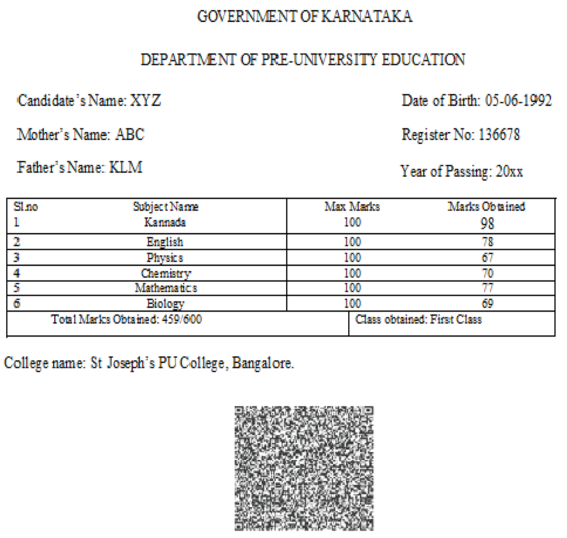
To create a QR code we are using a java library called ZXing. Zebra Crossing (ZXing) is an awesome open source library that one can use to generate / parse QR Codes in almost all the platforms. QRGen is a good library that creates a layer on top of ZXing and makes QR Code generation in Java. To create a QR code is we first create a string of data bits. This string includes the characters of the original message (encrypted message in this case) that you are encoding, as well as some information bits that will tell a QR decoder what type of QR Code it is. After generating the aforementioned string of bits, we use it to generate the error correction code words for the QR Code.

C. Algorithm For Decode QR Code

We here follow the reverse process of the above *generate QR Code ()* Algorithm to detect the QR Code Image using ZXing library class and get back the encrypted message.

III EXPERIMENTAL RESULT

We choose a student of anonymous name and produce the demonstration of the new mark-sheet system of that student in the following figures.



GOVERNMENT OF KARNATAKA

DEPARTMENT OF PRE-UNIVERSITY EDUCATION

Candidate's Name: XYZ
Date of Birth: 05-06-1992
Mother's Name: ABC
Register No: 136678
Father's Name: KLM
Year of Passing: 20xx

Sl.no	Subject Name	Max Marks	Marks Obtained
1	Kannada	100	98
2	English	100	78
3	Physics	100	67
4	Chemistry	100	70
5	Mathematics	100	77
6	Biology	100	69
Total Marks Obtained: 459/600		Class obtained: First Class	

College name: St Joseph's PU College, Bangalore.

Figure 1: Marks sheet having the Digital Data in encrypted QR Code.

The QR code that is present on marks sheet contains all details of the student such as name of the candidate, register no, college name, year of passing and marks of the respective subject. These data can obtained back by decrypting the data using decryption algorithm. If any intruder tries to change the data present in the QR code then it results in tampered output the encrypted data of the tampered file will be very different from the encrypted data of the original one. And by comparing the frequency analysis of the two encrypted data, it can be verified whether the data is authentic (original) or not.

IV. ACKNOWLEDGMENT

With great pleasure and gratefulness, I extend my deep sense of gratitude to Mr. Shivakumar. B. R, Asst. Prof, GMIT, Davanagere for giving me an opportunity to accomplish my dissertation under his guidance and to increase my knowledge. Lastly I wish to thank my HOD Prof. D. Basavalingappa and Principal Dr. S.G. Hiremath GMIT, Davanagere for my dissertation successful. Thank You

V. CONCLUSION AND FUTURE SCOPE

In our present work the capacity of holding data in a QR code is comparatively small, in future the capacity of QR code can be increased. And in the present work we have mainly focus on confidential encrypted data hiding in QR Code. As we know that data embedding and retrieval from QR-code is very simple issue. Since TTJSA is used for encryption, this method can be used to encrypt any type of message or file (picture, video, audio etc.) and send it to the receiver safely or the method can also be used to store important data or information safely. The inclusion of QR Code adds an extra level of security to the encrypted message and the receiver can access the original message very quickly. Simply a smart phone running on Android or iOS or any other new generation of mobile OS, can be used to extract the encrypted data from embedded QR-code and finally that data to be decrypted using the TTJSA decryption algorithm.

REFRENCES

[1] 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.

[2] 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.

[3] New Symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm: NeerajKhanna,JoelJames,JoyshreeNath, SayantanChakraborty, AmlanChakrabarti and AsokeNath : Proceedings of IEEE CSNT-2011 held at SMVDU(Jammu) 03-06 June 2011, Page 125-130(2011).

[4] SomdipDey, JoyshreeNath, AsokeNath, "An Integrated Symmetric Key Cryptographic Method – Amalgamation of TTJSA Algorithm, Advanced Caesar Cipher Algorithm, Bit Rotation and Reversal Method: SJA Algorithm", IJMECS, vol.4, no.5, pp.1-9, 2012.

[5] SomdipDey, JoyshreeNath and AsokeNath. Article: An Advanced Combined Symmetric Key Cryptographic Method using Bit Manipulation, Bit Reversal, Modified Caesar Cipher (SD-REE), DJSA method, TTJSA method: SJA-I Algorithm. *InternationalJournal of Computer Applications46(20):* 46-53, May 2012. Published by Foundation of Computer Science, New York, USA.

[6] "QR Code, Wikipedia", http://en.wikipedia.org/wiki/QR_code [Online] [Retrieved 2012-02-09]