Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.488 – 496

RESEARCH ARTICLE

Encryption and Decryption of Data Using QR Authentication System

Atul Hole[1], Mangesh Jadhav[2], Shivkant Kad[3], Swanand Shinde[4]

Information Technology Department, Pune University

Student, Nutan Maharashtra Institute of Engineering and Technology, Pune

Prof. Pramod Patil[5], Assistant Professor, NMIET Pune

[1] atulhole91@gmail.com, [2] mangeshjadhav025@gmail.com,

[3] shivkantkad101@gmail.com, [4] shinde.swanand@gmail.com

Abstract— ***In this paper, we explore how QR codes can be used in education. The low technical barrier of creating and reading QR codes allows innovative educators to incorporate them into their educational endeavors. Security the data is a big problem. And to solve this problem we propose an efficient method to authenticate digital information presents in our documents. If an intruder tries to change the information of the document that intruder cannot do that in QR Code. In this Paper we encrypt the data using encryption Algorithm. The information which is encrypted are entered inside the QR code and QR code will be also printed with the original data of document. Then the data can then be retrieved from the QR code and can be decrypted using decryption algorithm. And finally it can be verified data that are already presents in the document.***

Keywords— ***communication technology; QR Code TM; Encryption; decryption; multimedia; internet***

1. INTRODUCTION

The network security and data encryption is a very important topic in modern communication network. When we send some confidential matter from one client to another client then that data should not be intercepted by someone. The most important fact in data is that it should be original and correct. The authenticity of data is another most challenging fact in management of various types of data in the internet databases. In this paper we mainly study on authenticity of data that can be presents in the Digital Document.

We know that every year lot of Data send and received different sectors, companies and collages from all over the world. At that time there is no any type of method to test the security, authenticity of data from any digital document. Most of the time digital document checking it by human eye but human eye may not function every time a perfect job.

So that's why there is second verification on human eye verification of document. We have introduced a new digital Document. In this new Digital document we can embed the data digitally in QR Code, It means whenever we want to send some message to someone that should be encrypted in such a way that no one can decrypt without knowing the key for the decryption process.

QR (Quick response) Code is a type of 2 dimensional matrixes Barcode. The QR Code will gain more popularity because of its large capacity to hold digital data as well as it can be integrated in any Smartphone. In our new document, we save the various types of data of payment receipt like recipient name, receipt ID, registration number, product name and quantity of product, total amount of product etc. All the data will be embedded in the QR Code are encrypted, and then the QR Codes are printed in the payment receipt. So, next time or in future if the any other person wants to see their data digitally or wants to send their information to any Organization in digital format, then they can just scan the QR Code and decrypt the embedded information and send the authenticated data.

2. LITERATURE SURVEY

2.1. Existing System:

A barcode is an optical machine-readable representation of data relating to the object to which it is attached. A barcode is linear or one-dimensional (1D) code. Later they evolved into rectangles, dots, hexagons and other geometric patterns in two dimensions (2D). Although 2D systems use a variety of symbols, they are generally referred to as barcodes as well. Barcodes originally were scanned by special optical scanners called barcode readers. Later, scanners and interpretive software became available on devices including desktop printers and Smartphone's in industry standards and specifications.

2.2. Proposed System:

We learnt the working of the QR code how it provide security for the data its data capacity the function of the QR code. we understood that traditional Marking system are vulnerable to the many kinds of threats and manipulation but the QR code provide a novel way of providing security to the users information and prevent any kind of attacks on the Digital document. From the survey done on the system we could conclude that it was the need to make robust and dynamic system that would be more reliable and much more convenient to the masses into their day to lives thus revolution the whole Document.

3. METHODS USED

We use MASS encryption algorithm, which was combination of three different cryptographic modules: generalized modified Vernam cipher, KJS and DMASS , for the 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.

3.1. MASS Algorithm for encryption

MASS is a combined symmetric key cryptographic method, which is formed of generalized modified Vernam Cipher, KJS and DMASS symmetric key cryptographic methods. Brief study of the methods used in MASS algorithm is as follows:

3.1.1. Modified Vernam Cipher

Step 1: In this step whole file is divided into different size of small block, and it should be noted that each block size should be less than or equal to 256 byes

Step 2: In second step each byte of blocks of the file is added to the each byte of the blocks of randomized key**.** This operation is also called as normal Vernam Cipher method.

Step 3: While performing normal Vernam Cipher method if the pointer reaches to the end of each block then perform Feedback mechanism.

```
 Ex: ABCD, EFG, HIJKLMN        ←   (File Blocks)
       1234                    ←   (Randomized Key)      If  D+4=D and  Reminder is 4 then
        do  4+E               ← (Feedback mechanism)
```

Step 4: Repeat step 1,2 and 3 till whole file gets encrypted.

Step 5: After performing above mentioned steps merge all blocks of the encrypted file to get final output of this modified Vernam Cipher method.

3.1.2. KJS Algorithm

To perform encryption of the given source file symmetric key method is used in which a random key generator is used for generating the initial key of encryption process. KJS method is basically substitutions method in which take 2 characters from any input file and search corresponding characters in random matrix and store the result in another file. KJS method undergoes multiple encryptions and decryptions.

The random key matrix of order 16x16 is formulated from all characters (ASCII code 0 to 255) in a random order. This randomization of key matrix is done using the some function calls such as cycling (), up shift(), downshift(), left shift(), right shift().These function calls is used to arrange elements of key matrix in random order so that no one can predict the elements of the key matrix. This method is called as modified Playfair method. In Playfair method there is facility of encryption of only Alphabets.

3.1.3. DMASS Algorithm

In this algorithm encryption number and randomization number is calculated by using KJS algorithm.

Step 1: First read 32 bytes at a time from the given input file.

Step 2: Convert 32 bytes into 256 bits and then store it in some 1-dimensional array.

Step 3: Choose the first bit from the 256 bit stream and also the corresponding number(n) from the key matrix. Then interchange the 1st bit and the n-th bit of the selected 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) XORbit(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.

4. Generation of QR Code

To generate a QR code the string of bits are needed This string includes the characters of the encrypted message and the additional bits are added to inform the decoder what type of QR code is used. After generating the strings we generate the error correction code for the QR code . Reed-Solomon is used to generate Error Correction technique .Reed-Solomon codes (RS codes) are non-binary cyclic error correction codes invented by Irving S. Reed and Gustave Solomon.

The generated bit-string and error correction code words are used to generate eight different QR Codes. This different QR code uses a different mask pattern. A mask pattern is used to control and changes the pixels to Light or dark. Then the penalty score is given to different QR codes so that it becomes easy to the decoder to read it. If the encrypted message size becomes more

than 1,264 characters then the characters after these are used separately to generate another QR Code and the process is repeated until and unless the total encrypted message is converted to QR Code.

The method is as followed:

The Encrypted file created using the method MASS is now treated as the input file.

4.1. Algorithm to generate QRCode() :

Step1:

Mode Indicator

There are two types of modes eg:Numeric Mode: 0001, Alpha Numeric: 0010, from that we take the Alphanumeric ie 0010.

Character Count

Character count for Numeric is 10bit long and Alphanumeric is 8bit long .

So lets encode 4 in 8bit long binary

representation 0010 000000100

Encode Data

In Numeric Mode Data is delimited by 3digit and in Alphanumeric

Mode Data is delimited by 2digit

e.g.: Let's take

Ex: “ABCDE123”

AB :: 45*10+11=461	Codeword for
CD :: 45*12+13=553	A=>10
E1 :: 45*14+1=631	B=>11
23 :: 45*2+3=93	C=>12 etc.

Value encoded in 11bit binary as follows
0010 000001000 00111001101 01000101001 01001110111 00001011101

Termination

To terminate add 0000 bits at the end.
Ex: 0010 000001000 00111001101 01000101001 01001110111 00001011101 0000

Encode to Code Word

Then the resultant data is delimit by 8 bit:
00100000 01000001 11001101 01000101 00101001 11011100 00101110 10000
If last data is not in 8 bit form then Padding bits are added:
00100000 01000001 11001101 01000101 00101001 11011100 00101110 10000000.
To complete the capacity we alternatively add ‘11101100’ & ‘00010001’
00100000 01000001 11001101 01000101 00101001 11011100 00101110 10000000 11101100
Decimal representation of the data is as follow:
32 65 205 69 41 220 46 128 236
Decimal Representation: 32 65 205 69 41 220 46 128 236

Step 2:
Reed Solomon Error correcting Code is used in QR Code

Example: A popular Reed-Solomon code is RS(255,223) with 8-bit symbols. Each codeword contains 255 code word bytes, of which 223 bytes are data and 32 bytes are parity. For this code:

n = 255, k = 223, s = 8

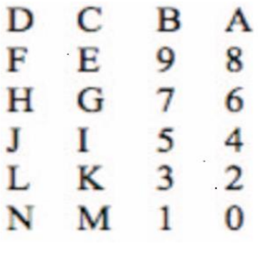
2t = 32, t = 16

The decoder can correct any 16 symbol errors in the code word: i.e. errors in up to 16 bytes anywhere in the codeword can be automatically corrected.

Given a symbol size s, the maximum codeword length (n) for a Reed-Solomon code is n = 2s – 1

For example, the maximum length of a code with 8-bit symbols (s=8) is 255 bytes.
Reed-Solomon codes may be shortened by (conceptually) making a number of data symbols zero at the encoder, not transmitting them, and then re-inserting them at the decoder.

Step 3:
Data Allocation
Step-1: Start the module from lower right corner.
Step-2:We take two modules width then If the left module is blank we move to the left module and put the data and if the left module is not blank we move to the position back.
Step-3:If we are in the left module of the two module then we put data in right module according to the priority of the data modules.
Step-4:Allocation for the upper and the lower we move to the upper blank module.
e.g.: If we have data "89ABCDEF GHIJKLMN" and we put
it in 6*4 matrix.



D	C	B	A
F	E	9	8
H	G	7	6
J	I	5	4
L	K	3	2
N	M	1	0

Step 4:
Mask Pattern
We select from 8 mask pattern
000: (i+j) mod 2 = 0
001: i mod 2 = 0
010: j mod 3 = 0
011: (i+j) mod 3 = 0
100: ((i div 2) + (j div 3)) mod 2 = 0
101: (ij) mod 2 + (ij) mod 3 = 0
110: ((ij) mod 2 + (ij) mod 3) mod 2 = 0
111: ((ij) mod 3 + (i+j) mod 2) mod 2 = 0
"mod" means remainder calculation, "div" means integer divide.

Step5:
Format Information
Step 1:It includes error correcting level and mast pattern indicator in 15bit long.
Step 2:First two bit is error correcting level
01: L OW Error correcting level
00: MEDIUM Error correcting level
11: QUATERL Error correcting level
10: HIGH Error correcting level
Step 3:Next three bit is mask pattern indicator and next 10bit we put error correcting data which is Bose-Chaudhuri-Hocquenghem (BCH).

Step 6:
Generate QR Code Image Library Class is used to generate the image.

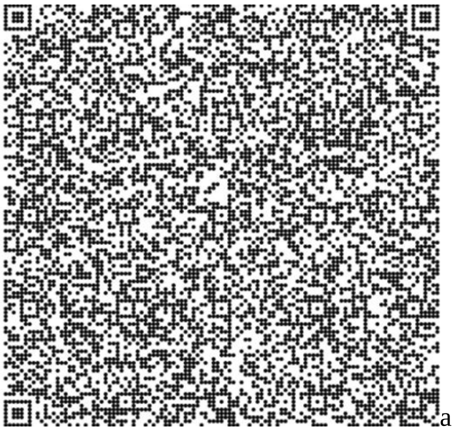
4.2. Algorithm for decode QR Code()

We here follow the reverse process of the above *generateQRCode()* Algorithm to detect the QR Code Image using Library Class [11] and perform error correction using Reed-Solomon technique and get back the encrypted message.

5. Results and Discussion

We choose a Different data to produce the demonstration of the new system that in the following figures.

RESULT 1:



ata

Fig 1: Information in form of Encrypted QR Code

Decryption of Data From QR Code

ABC Electronics Pvt Ltd

At/post-xxxxx, tel – xxxx, dist-pune

Receipt ID-xxxx

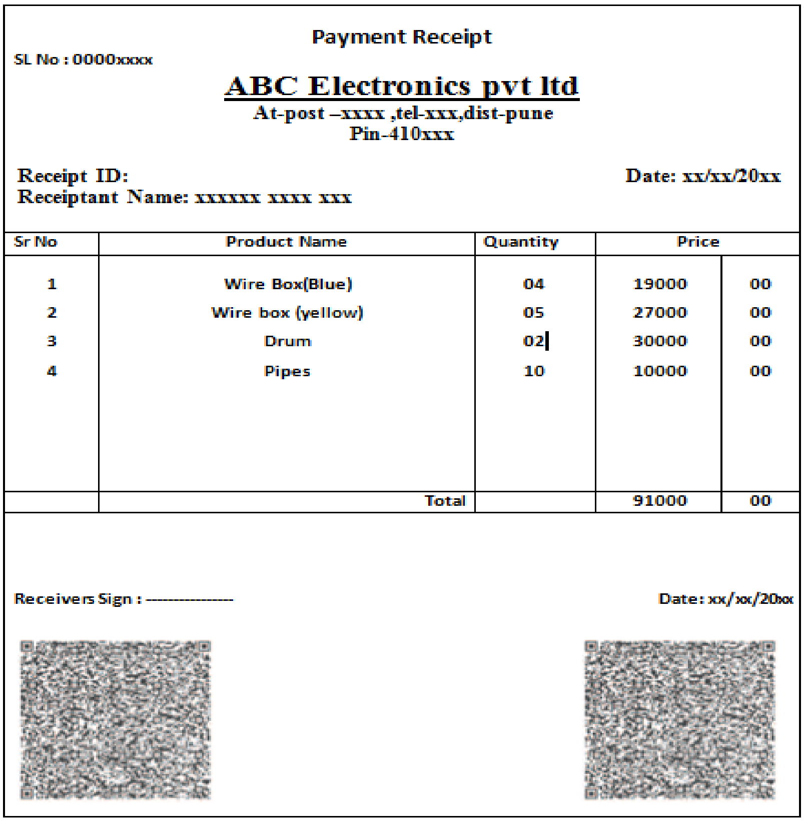
Receiptant Name- xxxxxxx xxxxx

Payment Receipt Date- xx/xx/20xx

Product Name	Quantity	Price
Wire Box (Blue)	04	19000
Wire Box (yellow)	05	27000
Drum	02	30000
Pipes	10	10000
TOTAL		91000

Fig 2: Decrypted Information from QR Code

We have also given a demonstration of our Data in the following figure:



Payment Receipt

SL No : 0000xxxx

ABC Electronics pvt ltd
At-post –xxxx ,tel-xxx,dist-pune
Pin-410xxx

Receipt ID:
Receiptant Name: xxxxxx xxxx xxx

Date: xx/xx/20xx

Sr No	Product Name	Quantity	Price	
1	Wire Box(Blue)	04	19000	00
2	Wire box (yellow)	05	27000	00
3	Drum	02	30000	00
4	Pipes	10	10000	00
	Total		91000	00

Receivers Sign : ---------------

Date: xx/xx/20xx

FIG 3: AN ACTUAL RESULT HAVING THE DIGITAL DATA IN ENCRYPTED QR CODE

RESULT 2:

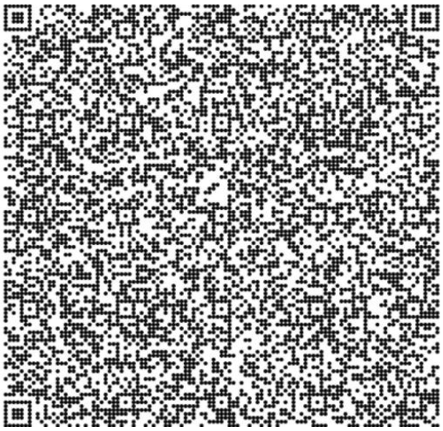
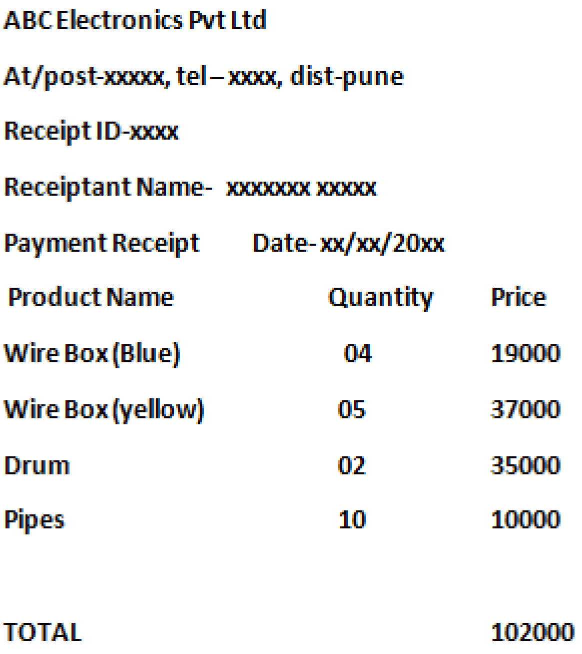


Fig 4: DEF's Information in form of Encrypted QR Code

Decryption of Data From QR Code



ABC Electronics Pvt Ltd

At/post-xxxxx, tel – xxxx, dist-pune

Receipt ID-xxxx

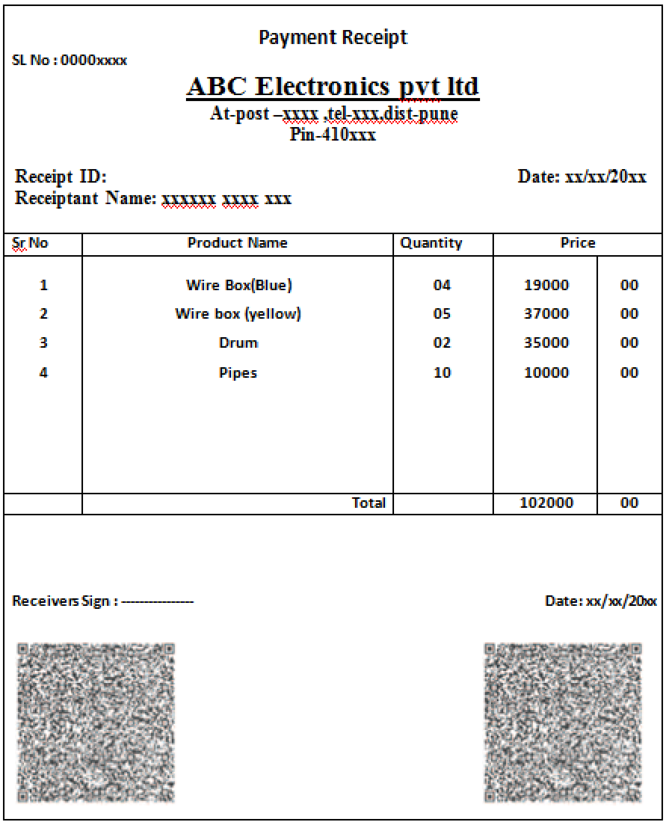
Receiptant Name- xxxxxxx xxxxx

Payment Receipt Date- xx/xx/20xx

Product Name	Quantity	Price
Wire Box (Blue)	04	19000
Wire Box (yellow)	05	37000
Drum	02	35000
Pipes	10	10000
TOTAL		102000

Fig 5: Decrypted DEF's Information from QR Code

We have also given a demonstration of our data in the following figure:



Payment Receipt

SL No : 0000xxxx

ABC Electronics pvt ltd

At-post –xxxx ,tel-xxx,dist-pune
Pin-410xxx

Receipt ID:

Receiptant Name: xxxxxx xxxx xxx

Date: xx/xx/20xx

Sr No	Product Name	Quantity	Price	
1	Wire Box(Blue)	04	19000	00
2	Wire box (yellow)	05	37000	00
3	Drum	02	35000	00
4	Pipes	10	10000	00
	Total		102000	00

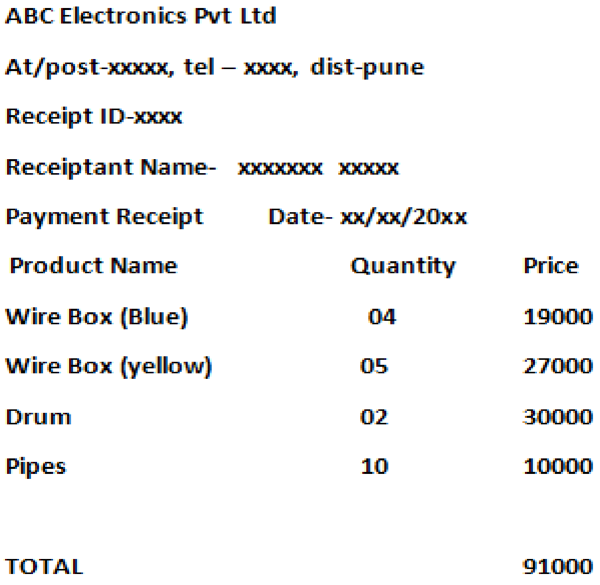
Receivers Sign : ---------------

Date: xx/xx/20xx

Fig 6: An Actual Result having the Digital Data in encrypted QR Code

6. Security analysis

We chose to tampered data and intentionally changed Price obtained by the in only Two Product.



ABC Electronics Pvt Ltd

At/post-xxxxx, tel – xxxx, dist-pune

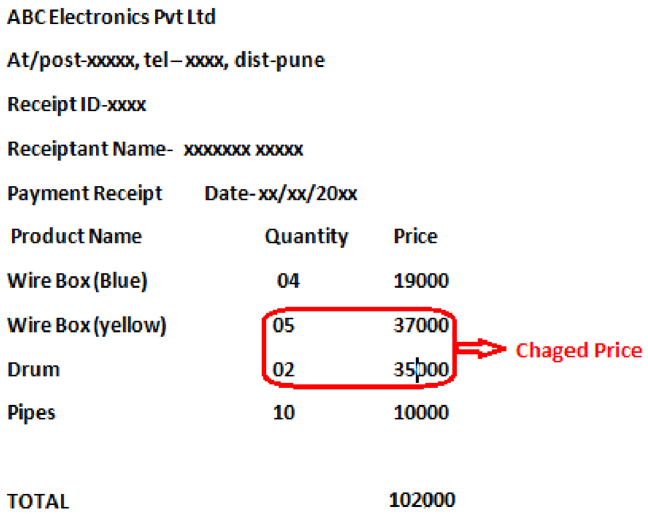
Receipt ID-xxxx

Receiptant Name- xxxxxxx xxxxx

Payment Receipt Date- xx/xx/20xx

Product Name	Quantity	Price
Wire Box (Blue)	04	19000
Wire Box (yellow)	05	27000
Drum	02	30000
Pipes	10	10000
TOTAL		91000

FIG 7: ORIGINAL DATA



ABC Electronics Pvt Ltd

At/post-xxxxx, tel – xxxx, dist-pune

Receipt ID-xxxx

Receiptant Name- xxxxxxx xxxxx

Payment Receipt Date- xx/xx/20xx

Product Name	Quantity	Price
Wire Box (Blue)	04	19000
Wire Box (yellow)	05	37000
Drum	02	35000
Pipes	10	10000
TOTAL		102000

Chaged Price

FIG 8: TAMPERED DATA

Then, we encrypted the data of the tampered receipt. After that, we can frequency analysis of both the encrypted data, and the frequency analysis of both the encrypted data were totally different and no pattern was found among them the encrypted data from embedded QR-code and finally that data to be decrypted using the MASS decryption algorithm..

7. Conclusion

In the present study we have mainly focus on confidential encryption of data hiding and retrieval using QR Code. We know that embedding of data and also retrieval using QR code is very simple. Simply smart phones can be used to extract the encrypted embedded information from QR Code. And finally the data should be decrypted using our MASS decryption algorithm.

References

[1] Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System.
[2] 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.
[3] 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
[4] New Symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm: NeerajKhanna,JoelJames,JoyshreeNath, Sayantan Chakraborty, AmlanChakrabartiand AsokeNath : Proceedings of IEEE CSNT-2011 held at SMVDU(Jammu) 03-06 June 2011, Page 125-130(2011).
[5] N. Johnson and S. Jajodia, "Steganaly- sis: The investigation of hidden information", *Proc. Of the 1998 IEEE Information TechnologyConference*, 1998.
[6] Reed and G. Solomon, "Polynomial codes over certain finite fields", Journal of the Society for Industrial and Applied Mathematics, 8(2):300–304, 1960.