Encryption and decryption of data using Quick response code

[1]Vanishree, [2]Sunitha H.S

M. Tech [II year], Assistant Professor
The Oxford College of Engineering, Bangalore, Karnataka, India
Email: [1]swathikasnoor@gmail.com, [2]Sunitha1979_hs@yahoo.com

Abstract:- Steganography method is used to hide the data data to obtained encrypted data and it is not so strong. Visual cryptography scheme is a cryptography technique that allows for the encryption of visual information but this method is complex in computation. DJSSA encryption method uses 65536*256*3 matrix size this may generate in 16777216 ways so in principle it is not possible for anyone to decrypt the encrypted text without knowing the exact key. SDE-QR method is only used for the encryption of the text message, it is not applicable for the encryption of the image. IMAP shows how to build encrypted file systems and secure mail servers, but typically one must sacrifice functionality to ensure security.

To overcome from the all the above problem, digital authentication method can be used. In this paper applying the digital authentication for the marks sheet. In this method the marks obtained by the students is stored in the Quick response code(QR code).The information stored in the QR code is encrypted by using sharing tecqnique method after encryption QR code is printed on the mark sheet of the student and for the decryption also using the sharing technique method.

Keywords— encryption,decryption,QRcode,internet and multimedia

I. INTRODUCTION

Security and authentication of data is a big challenge in present scenario. Here method is proposing to authenticate the digital document like marks sheet. Here work is focusing to authenticity of marks in a printed marks sheet however present method is used for any legal documents. The marks obtained by the students is saved in the QR code which is encrypted by using sharing technique method. After the encryption QR code is printed on the marks sheet if the student wants to send the data to any university they can just scan the QR code and decrypt the embedded information and send the authentic data.

II. RELATED WORK:

Obtain the information like mark sheet ,encrypt this information by using the sharing technique method. The encrypted marks is entered inside the QR code and that QR code is printed with the original data of the mark sheet and this information is transmitted through the channel it is as shown in the figure1 encryption block. Encryption is a process of converting plain text into cipher text in QR code.

At the receiver, receive QR code, decrypt the data by using the sharing algorithm and get the original information. It is as shown in the figure2 decryption block. Decryption is a process of converting cipher text in the QR code into plain text.

Block diagram:

Encryption block

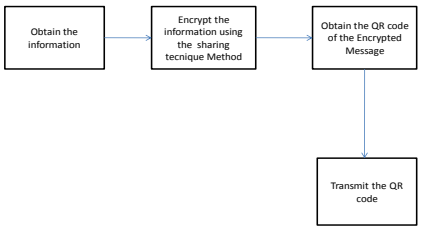


Figure 1:Block diagram for encryption using QR code method.

Decryption block diagram.

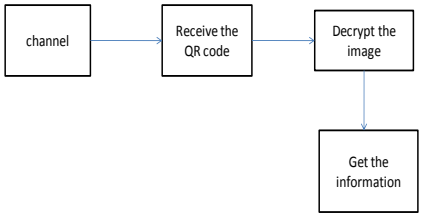


Figure 2:Block diagram of decryption using QR method

A Sharing technique:

The proposed technique designs a secure data transmission scheme based on the secret sharing scheme with QR code. Secret sharing scheme was first proposed by Shamir in 1979 . The main idea of the secret sharing scheme divides a secret into n shadows or called shares. Anyone can not decrypt the original secret from their own share. The secret can be recovered only when any of t out of n shadows (t<=n) are hold together. The framework of the proposed scheme is listed in Figure 3.

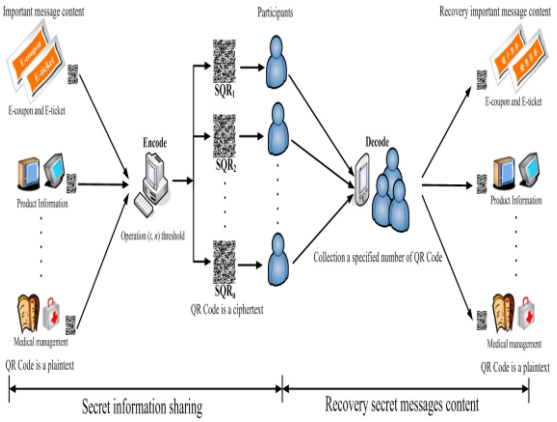


Figure 3:Sharing technique method.

B Encoding of QR Code

Each QR Code symbol consists of an encoding region and function patterns, as shown in Figure4. Finder, separator, timing patterns and alignment patterns comprised function patterns. Function patterns shall not be used for the encoding data. The finder patterns located at three corners of the symbol intended to assist in easy location of its position, size and inclination.

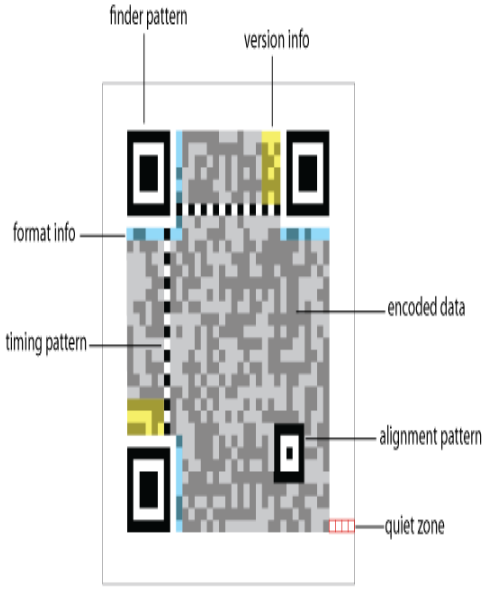


Figure 4:QR code basics

The encode procedure 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 codewords. Then codewords are divided into blocks, and add error correction codewords to each block. All these codewords 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 position of the QR Code. By arranging this pattern at the three corners of a symbol, the position, the size, and the angle of the symbol can be detected. This finder pattern consists of a structure which can be detected in all directions (360□).

b) Alignment Pattern

A pattern for correcting the distortion of the QR Code. It is highly effective 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 easier to detect the central coordinate of the alignment pattern.

c) Timing Pattern

A pattern for identifying the central coordinate of each cell in the QR Code with black and white patterns arranged alternately. It is 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 is arranged in both vertical and horizontal directions.

d) Quiet Zone

A margin space necessary for reading the QR Code. This quiet zone makes it easier to have the symbol detected from among 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 stored (encoded) into the data area. The grey part in Figure 3 represents the data area. The data will be encoded into the 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 corporated for the stored data and the error correction functionality.

f) Linking Functionality of the Symbols

QR Code has a linking functionality which will enable a single symbol to be represented in several symbols by dividing it . A single symbol can be divided into 16 symbols at maximum. The example shown in Figure 4 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 into and in which order that specific symbol would be among

all divided ones. This will enable the entire data to be edited and submitted to the computer regardless of what order the symbols had been read by the reader. By this linking functionality, the QR Code will be able to be printed even if the printing space is not wide enough to have a single QR Code printed.

g) Masking Process

By having special patterns to process masking, QR Code is enabled to have black and white cells well arranged in a balanced order. To accurately finalize the data that had been read, it is necessary to arrange the white and black cells in a well-balanced manner

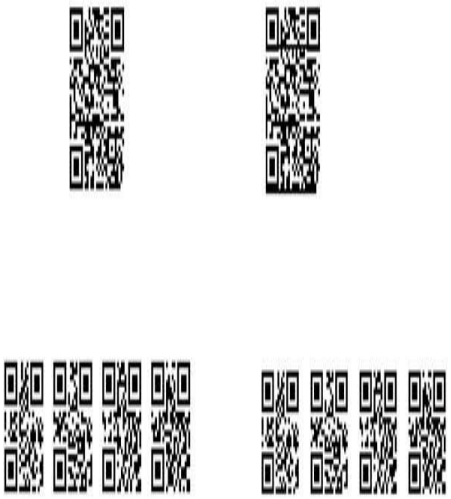


Figure 5:Single QR code is divided into 4 patterns

To enable this, EX-OR calculation will be implemented between the data area cell and the mask pattern (template) cell when encoding the stored data and arranging it into the data area. Then, the number of unique patterns existing and the balance between the white cells and the black cells will be assessed against the data area where the calculation had been implemented. There are eight mask patterns. Assessment will be made for each mask pattern, and the mask pattern with the highest assessment result together with the EX-OR calculation result will be stored into the data area.

h) The Confidentiality of the Code

By making the relationship between the character type and the stored data unique for a special usage, QR Code can be easily encrypted. Unless the conversion table between the character type and the stored data is deciphered, no one will be able to read the QR Code.

i) Direct Marking

QR Code exerts superior readability even for symbols which are directly marked using laser or dot pin markers. For directly marked symbols, the cell shape does not necessarily have to be square as shown in Figure 10. It can also be circular shape. Even if the white part (with high reflectance) and the black part (with lowreflectance) are inverted due to the angle of the illuminating ray, the code can still be read in an accurate manner. It is also possible to read from the back side of the symbol when it is marked upon a transparant material such as glass, etc.

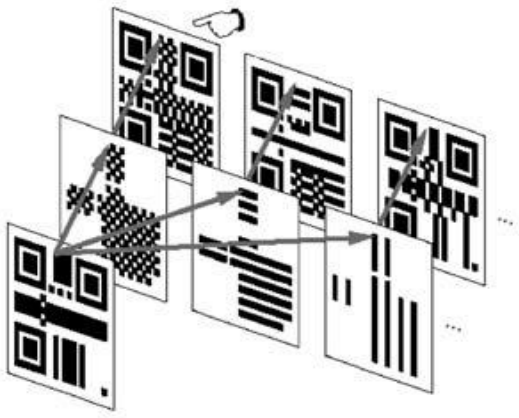


Figure 6.masking pattern

Generation of QR Code:

To create a QR code is 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. QR Codes use Reed-Solomon Error Correction

technique note that in coding theory, Reed- Solomon codes (RS codes) are non-binary cyclic error correction codes invented by Irving S. Reed and Gustavo Solomon. After the generation of bit-string and error correction code words, the resultant data is used to generate eight different QR Codes, each of which uses a different mask pattern. A mask pattern controls and changes the pixels to light or dark ones, according to a particular formula. The eight mask pattern formulas are defined in the QR Code specification, which is referred at the time of mask generation needed for the QR Code generation. Each of the eight QR codes is then given a penalty score that is based on rules defined in the QR specification. The purpose of this step is to make sure that the QR code doesn't contain patterns that might be difficult for a QR decoder to read, like large blocks of same-colored pixels, for example. After determining the best mask pattern, the QR Code, which uses the best mask pattern, is generated and shown as an output. If the size of the encrypted message becomes more than 1,264 characters then the characters appearing after 1,264 characters are used separately to generate another QR

Code and the above mentioned process is repeated until and unless the total encrypted message is converted to QR Code(s).

The method is discussed in details below:

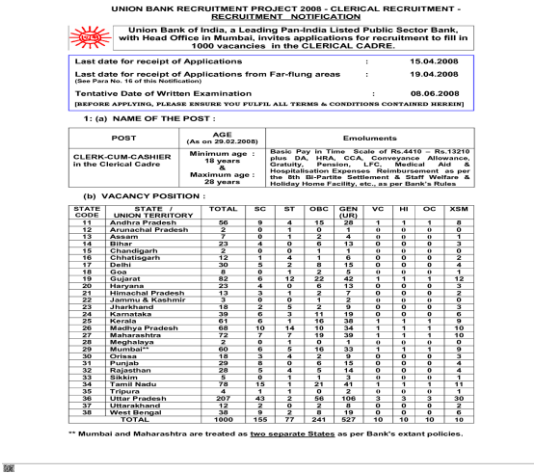
The Encrypted file, which is created using the method

Sharing technique is now treated as the input file and the string is extracted from the file to generate the QR Code.

1: call function file read(output_file)
2: call function generateQRCode (str[])
3: call function delete_file (output_file)

1) Algorithm for generateQRCode() :
a) Step1:
Mode Indicator
e.g.: Numeric Mode: 0001, Alpha Numeric: 0010, Let us choose 0010 for Alphanumeric
Character Count
e.g.: Numeric: 10bit long, Alphanumeric: 8bit long (for version 1-9) Let's encode 8 in 8bit long binary representation 0010 000001000
Encode Data
Numeric Mode: Data delimited by 3digit Alphanumeric Mode: Data delimited by 2digit e.g.: Let's take ABCDE123"AB": 45*10+11=461 "CD":45*12+13=553 "E1": 45*14+1=631 "23": 45*2+3=93 Codeword for A=10,
B=11, C=12 etc. Now the value encoded in 11bit long binary representation. 0010 000001000 00111001101 01000101001 01001110111 00001011101
Termination
Add 0000 at the end to terminate 0010 000001000 00111001101 01000101001 01001110111 00001011101 0000
Encode to Code Word
Result data are delimited by 8bit 00100000 01000001 11001101 01000101 00101001 11011100 00101110 10000 If last data is less than 8bit, pad it with 0 00100000
01000001 11001101 01000101 00101001 11011100 00101110 10000000. We alternatively put '11101100' and
'00010001' until full capacity of the following version 00100000 01000001 11001101 01000101 00101001 11011100 00101110 10000000 11101100
Decimal Representation: 32 65 205 69 41 220 46 128 236
b) Step 2:
Reed Solomon Error correcting Code is used in QR Code
e.g.: For example data, count of error correcting code word is 17g(x)=x17 +α43x16 +α139x15 +α206x14 +α78x13 +α43x12 +α239x11 +α123x10 +α206x9 +α214x8 +α147x7 +α24x6 +α99x5 +α150x4 +α39x3 +α243x2 +α163x +α136
Now polynomial f(x) which coefficients are data code words is divided by g(x)

f(x)=32x25 +65x24 +205x23 +69x22 +41x21 +220x20 +46x19 +128x18 +236x17 ----(i) divided by g(x)
g(x)*(α5)*x8
=α5*x25 +α5*α43*x24 +α5*α139*x23 +α5*α206*x22 +α5
*α78*x21.....
=α5*x25 +α48*x24 +α144*x23 +α211*x22 +α83*x21..... =32x25+70x24 +168x23 +178x22 +187x21.....-----(ii)
Calculate Exclusive logical Sum (i) and (ii)
f(x)'=7x24 +101x23 +247x22+146x21.....
We repeat same logic until this divide calculation is over.
Finally we get R(x).
R(x)=42x16 +159x15 +74x14 +221x13 +244x12 +169x11+239x10 +150x9 +138x8 +70x7 +237x6 +85x5 +224x4 +96x3 +74x2 +219x +61
So we get 32 65 205 69 41 220 46 128 236 42 159 74 221 244 169 239 150 138 70 237 85 224 96 74 219 61
Decoding of QR code:
Perform decoding, decoding process is just reverse of encoding and perform the error correction by using Reed-solomon error correcting code.
IV RESULTS:
Choose details of the students or any legal document, the results are as shown below
Result 1:
Input for sharing technique



UNION BANK RECRUITMENT PROJECT 2008 - CLERICAL RECRUITMENT - RECRUITMENT NOTIFICATION

Union Bank of India, a Leading Pan-India Listed Public Sector Bank, with Head Office in Mumbai, invites applications for recruitment to fill in 1000 vacancies in the CLERICAL CADRE.

Last date for receipt of Applications	:	15.04.2008
Last date for receipt of Applications from Far-flung areas (See Para No. 16 of this Notification)	:	19.04.2008
Tentative Date of Written Examination	:	08.06.2008

[BEFORE APPLYING, PLEASE ENSURE YOU FULFIL ALL TERMS & CONDITIONS CONTAINED HEREIN]

1: (a) NAME OF THE POST :

POST	AGE (As on 29.02.2008)	Emoluments
CLERK-CUM-CASHIER in the Clerical Cadre	Minimum age : 18 years & Maximum age : 28 years	Basic Pay in Time Scale of Rs.4410 – Rs.13210 plus DA, HRA, CCA, Conveyance Allowance, Gratuity, Pension, LFC, Medical Aid & Hospitalisation Expenses Reimbursement as per the 9th Bi-Partite Settlement & Staff Welfare & Holiday Home Facility, etc., as per Bank's Rules

(b) VACANCY POSITION :

STATE CODE	STATE / UNION TERRITORY	TOTAL	SC	ST	OBC	GEN (UR)	VC	HI	OC	XSM
11	Andhra Pradesh	56	9	4	15	28	1	1	1	8
12	Arunachal Pradesh	2	0	1	0	1	0	0	0	0
13	Aasam	7	0	1	2	4	0	0	0	1
14	Bihar	23	4	0	6	13	0	0	0	3
15	Chandigarh	2	0	0	1	1	0	0	0	0
16	Chhatisgarh	12	1	4	1	6	0	0	0	2
17	Delhi	30	5	2	8	15	0	0	0	4
18	Goa	8	0	1	2	5	0	0	0	1
19	Gujarat	82	6	12	22	42	1	1	1	12
20	Haryana	23	4	0	6	13	0	0	0	3
21	Himachal Pradesh	13	3	1	2	7	0	0	0	2
22	Jammu & Kashmir	3	0	0	1	2	0	0	0	0
23	Jharkhand	18	2	5	2	9	0	0	0	3
24	Karnataka	39	6	3	11	19	0	0	0	6
25	Kerala	61	6	1	16	38	1	1	1	9
26	Madhya Pradesh	68	10	14	10	34	1	1	1	10
27	Maharashtra	72	7	7	19	39	1	1	1	10
28	Meghalaya	2	0	1	0	1	0	0	0	0
29	Mumbai**	60	6	5	16	33	1	1	1	9
30	Orissa	18	3	4	2	9	0	0	0	3
31	Punjab	29	8	0	6	15	0	0	0	4
32	Rajasthan	28	5	4	5	14	0	0	0	4
33	Sikkim	1	0	1	1	3	0	0	0	1
34	Tamil Nadu	78	15	1	21	41	1	1	1	11
35	Tripura	4	1	1	0	2	0	0	0	1
36	Uttar Pradesh	207	43	2	56	106	3	3	3	30
37	Uttarakhand	12	2	0	2	8	0	0	0	2
38	West Bengal	38	9	2	8	19	0	0	0	6
	TOTAL	1000	155	77	241	527	10	10	10	10

** Mumbai and Maharashtra are treated as two separate States as per Bank's extant policies.

Figure 7:input image

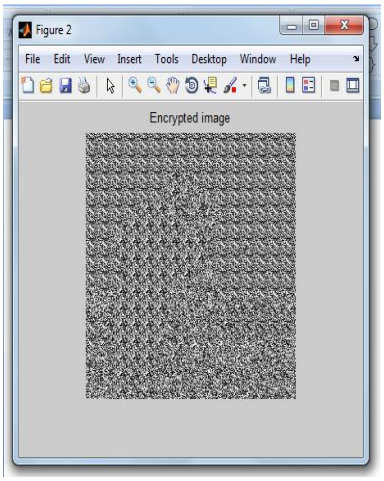


Figure 8:Encrypted document.

Result 2:student information in form of encrypted QR code

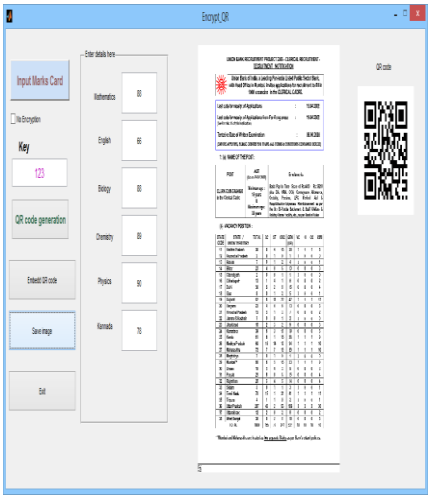


figure 8:Result having the digital data in encrypted QR code

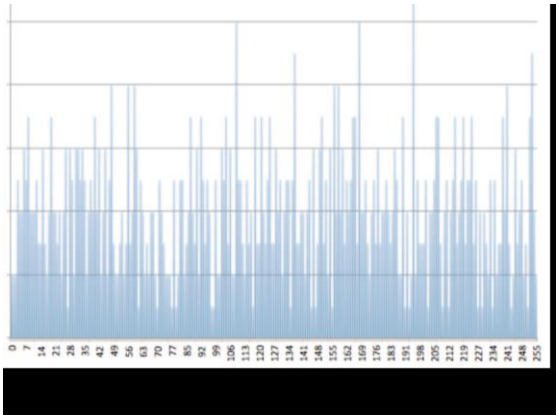


Figure 7:Frequency analysis of encrypted original file

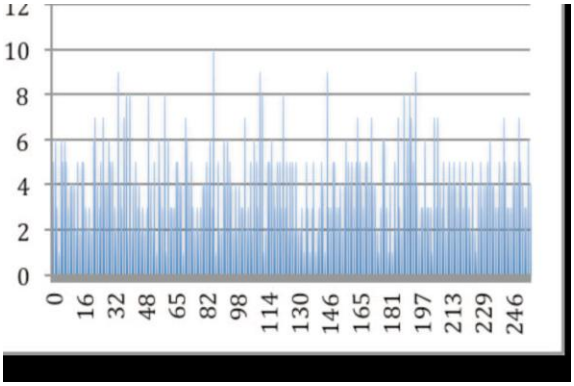


Figure 8:Frequency analysis of tampered data.

Thus, from the frequency analysis (spectral analysis) it is

evident that if the data is tampered then, 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.

CONCLUSION:

In the present work have mainly focus on hiding encrypted in QR code. As we know that data embedding and retrieval from QR-code is very simple issue.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 sharing method.

REFERENCES

[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 Cryptography using Random Key generator: Asoke Nath, Saima Ghosh, Meheboob Alam Mallik: "Proceedings of International conference on security and management(SAM'10" held at Las Vegas, USA Jull 12-15, 2010), P-Vol-2, 239-244(2010).

[3] New Symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm: Neeraj Khanna,Joel James,Joyshree

Nath, Sayantan Chakraborty, Amlan Chakrabarti and Asoke Nath : Proceedings of IEEE CSNT-2011 held at SMVDU(Jammu) 03-06 June 2011, Page 125-130(2011).

[4] Somdip Dey, Joyshree Nath, Asoke Nath, "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] Somdip Dey, Joyshree Nath and Asoke Nath. Article: An Advanced Combined Symmetric Key Cryptographic Method using BitManipulation, Bit Reversal, Modified Caesar Cipher (SD-REE), DJSA method, TTJSA method: SJA-I Algorithm. International Journal of Computer Applications46(20): 46-53, May 2012. Published by Foundation of Computer Science, New York, USA.

[6] Somdip Dey, ”SD-EQR: A New Technique To Use QR CodesTM in Cryptography”, Proceedings of “1st International Conference on Emerging Trends in Computer and Information Technology (ICETCIT 2012)”, Coimbatore, India, pp. 11-21.

[7] Cryptography and Network Security, William Stallings, Prentice Hallof India.

[8] Cryptography & Network Security, Behrouz A. Forouzan, Tata McGraw Hill Book Company.

[9] Reed and G. Solomon, “Polynomial codes over certain finite fields”, Journal of the Society for Industrial and Applied Mathematics,

[10] "ZXING- QR Code Library

"http://code.google.com/p/zxing/ [Online] [Retrieved 2012-02- 09] [12] N. Johnson and S. Jajodia, “Steganaly- sis: The investigation of hidden information”, Proc. Of the 1998 IEEE Information Technology Conference,1998.

[13] Somdip Dey, Kalyan Mondal, Joyshree Nath, Asoke Nath,"Advanced Steganography Algorithm Using Randomized Intermediate QR Host Embedded With Any Encrypted Secret Message: ASA_QR Algorithm", IJMECS, vol.4, no.6, pp. 59-67, 2012. 517

[14] T. Falas and H. Kashani, “Two-dimensional barcode decoding with camera-equipped mobile phones”.

◈◈◈