A Novel Method for Ciphering a Message Based on QR Codes

Basheer N. Ameen* and Sawsan K. Thamer**
*College of Sciences, Al-Nahrain University, Iraq , basher_nahiz@syahoo.com
**Computer Science department,College of Sciences, Al-Nahrain University, Iraq , skt@sc.nahrainuniv.edu.iq

Abstract— In this paper, we have introduced a new data-hiding algorithm, where message is converted to QR code (Quick Response Code). QR Codes are mainly used to carry or store messages because they have higher or large storage capacity than any other normal conventional 'barcodes'. In the present work the authors have introduced the encryption technique by inverting in two special selected areas to generate one ciphered QR code as in sender side. The resulted QR code may be sent to destination or may be saved for future use. In this encryption method authors have used bit-manipulation, byte-reshuffling and generalized this method. The ciphering method used here has been tested on different plain texts and it was found that the method is unbreakable using traditional cryptanalysis techniques like frequency analysis, plain-text attack, Differential attack, Brute-force attack, etc. So that data cannot be easily retrieved without adequate authorization / permission. In this paper, we have introduced a new data-hiding algorithm, where message is converted to QR code (Quick Response Code). QR Codes are mainly used to carry or store messages because they have higher or large storage capacity than any other normal conventional 'barcodes'. In the present work the authors have introduced the encryption technique by inverting in two special selected areas to generate one ciphered QR code as in sender side. The resulted QR code may be sent to destination or may be saved for future use. In this encryption method authors have used bit-manipulation, byte-reshuffling and generalized this method. The ciphering method used here has been tested on different plain texts and it was found that the method is unbreakable using traditional cryptanalysis techniques like frequency analysis, plain-text attack, Differential attack, Brute-force attack, etc. So that data cannot be easily retrieved without adequate authorization / permission.

Index Terms— QR code, cryptography, security.

1 INTRODUCTION

In today's world, security is a big issue and securing important data is very essential, so that the data cannot be intercepted or misused for any kind of unauthorized use. The hackers and intruders are always ready to get through personal data or important data of a person or an organization, and misuse them in various ways. For this reason, the field of cryptography is very important and the cryptographers are trying to introduce new cryptographic methods to secure the data as much as possible. Keep his valuable data like passport information, bank statements, social security number, etc. with himself/herself all the time, but he/she is always afraid of doing so because this information are threatened and can be easily intercepted by outsiders for misuse. We choose another example; a bank manager wants to instruct his subordinates about the process of a huge transaction. If this data is not encrypted properly, then it can be retrieved by a hacker to reverse the transaction process to credit a different account. For this reason, encryption of data and hiding data from unauthentic usage is very important. This problem can be solved by encrypting the data and hiding it in a QR Code [1][2][3], which can be kept with the person all the time and the QR Code scanner with a software, using the method in this paper, can be used to decode with the authentic password the information saved in it.

2 QR CODE

QR code (abbreviated from Quick Response Code) is the trademark for a type of matrix barcode (or two-dimensional barcode) first designed for the automotive industry in Japan. A barcode is a machine-readable optical label that contains information about the item to which it is attached. Four standardized encoding modes (numeric, alphanumeric and byte/binary) could be stored as QR for efficient data store.

The QR Code system became popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard UPC barcodes. Applications include product tracking, item identification, time tracking, document management, and general marketing.[4]

A QR code consists of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging device (such as a camera, scanner, etc.) and processed using Reed–Solomon error correction until the image can be appropriately interpreted. The required data are then extracted from patterns that are present in both horizontal and vertical components of the image.[4]

2.1 Design

Unlike the older, one-dimensional barcodes that were designed to be mechanically scanned by a narrow beam of light, a QR code is detected by a 2-dimensional digital image sensor and then digitally analyzed by a programmed processor. The processor locates the three distinctive squares at the corners of the QR code image, using a smaller square (or multiple squares) near the fourth corner to normalize the image for size, orientation, and angle of viewing. The small dots throughout the QR code are then converted to binary numbers and validated with an error-correcting algorithm.

2.2 Storage

The amount of data that could be stored in the QR code

symbol depends on the data type (mode, or input character set), version (1, …, 40, indicating the overall dimensions of the symbol), and error correction level. The maximum storage capacities occur for 40-L symbols (version 40, error correction level L) as shown in Table (1) [5][6]:

TABLE 1
MAXIMUM CHARACTER STORAGE CAPACITY (40-L)

Input mode	max. characters	bits/char	possible characters, default encoding
Numeric only	7,089	3⅓	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Alphanumeric	4,296	5½	0–9, A–Z (upper-case only), space, $, %, *, +, -, ., /, :
Binary/byte	2,953	8	ISO 8859-1

Here are some samples of QR code symbols:

Level L (Low)	7% of codewords can be restored.
Level M (Medium)	15% of codewords can be restored.
Level Q (Quartile)[7]	25% of codewords can be restored.
Level H (High)	30% of codewords can be restored.

2.3 Error correction

Codewords are 8 bits long and use the Reed–Solomon error correction algorithm with four error correction levels. The higher the error correction level, the less storage capacity. The following table lists the approximate error correction capability at each of the four levels as declared in table (2):

In larger QR symbols, the message is broken up into several Reed–Solomon code blocks. The block size is chosen so that at most 15 errors can be corrected in each block; this limits the complexity of the decoding algorithm. The code blocks are then interleaved together, making it less likely that localized damage to a QR symbol will overwhelm the capacity of any single block.

Due to error correction, it is possible to create artistic QR codes that still scan correctly, but contain intentional errors to make them more readable or attractive to the human eye, as well as to incorporate colors, logos, and other features into the QR code block [8][9].

It is also possible to design artistic QR codes without reducing the error correction capacity by manipulating the underlying mathematical constructs [10].

2.4 Encoding

The format information records two things: the error correction level and the mask pattern used for the symbol. Masking is used to break up patterns in the data area that might confuse a scanner, such as large blank areas or misleading features that look like the locator marks. The mask patterns are defined on a grid that is repeated as necessary to cover the whole symbol. Modules corresponding to the dark areas of the mask are inverted. The format information is protected from errors with a BCH code, and two complete copies are included in each QR symbol that is show in figure (1). [10] BCH code is the abbreviation for (Bose-Chaudhuri-Hochquenghem) code. A multilevel, cyclic, error-correcting, variable- length digital code used to correct errors up to approximately 25% of the total number of digits. Note: BCH codes are not limited to binary codes, but may be used with multilevel phase-shift keying whenever the number of levels is a prime number or a power of a prime number, such as 2, 3, 4, 5, 7, 8, 11, and 13. A BCH code in 11 levels has been used to represent the 10 decimal digits plus a sign digit.

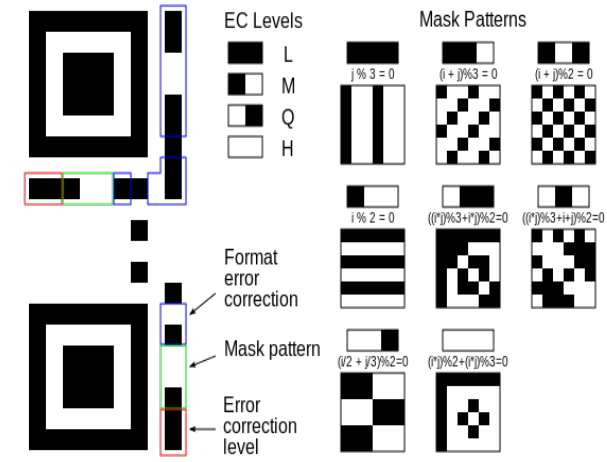

Figure 1: Meaning of format information in QR

The message dataset is placed from right to left in a zigzag pattern, as shown in figure (2). In larger symbols, this is complicated by the presence of the alignment patterns and the use of multiple interleaved error-correction blocks, as shown in figure (3) .

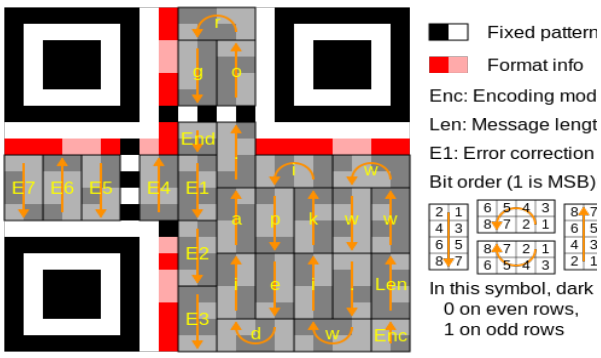

Figure 2: Message placement within a QR

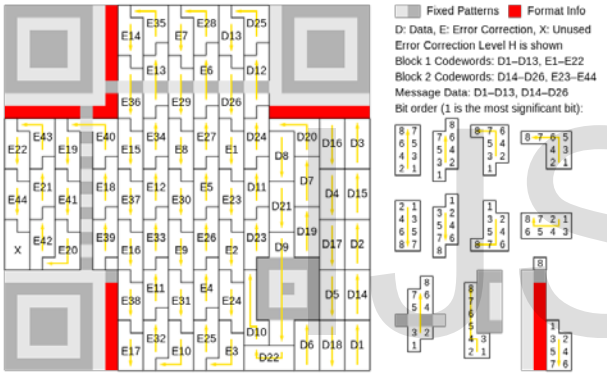

Figure 3: Larger symbol illustrating interleaved

FOUR-BIT INDICATORS ARE USED TO SELECT THE ENCODING MODE

TABLE 1: ENCODING MODES

Indicator	Meaning
0001	Numeric encoding (10 bits per 3 digits)
0010	Alphanumeric encoding (11 bits per 2 characters)
0100	Byte encoding (8 bits per character)
0000	End of message

AND CONVEY OTHER INFORMATION AS SHOWN IN TABLE (3). ENCODING MODES CAN BE MIXED AS NEEDED WITHIN A QR SYMBOL.

AFTER EVERY INDICATOR THAT SELECTS AN ENCODING MODE IS A LENGTH FIELD THAT TELLS HOW MANY CHARACTERS ARE ENCODED IN THAT MODE. THE NUMBER OF BITS IN THE LENGTH FIELD DEPENDS ON THE ENCODING AND THE SYMBOL VERSION AS SHOWN IN

TABLE 2: NUMBER OF BITS PER LENGTH FIELD

Encoding	Ver. 1–9	10–26	27–40
Numeric	10	12	14
Alphanumeric	9	11	13
Byte	8	16	16

TABLE (4).

ALPHANUMERIC ENCODING MODE STORES A MESSAGE MORE COMPACTLY THAN THE BYTE MODE CAN, BUT CANNOT STORE LOWERCASE LETTERS AND HAS ONLY A LIMITED SELECTION OF PUNCTUA-

TABLE 3: ALPHANUMERIC CHARACTER CODES

Code	Character	Code	Character	Code	Character	Code	Character	Code	Character
00	0	09	9	18	I	27	R	36	Space
01	1	10	A	19	J	28	S	37	$
02	2	11	B	20	K	29	T	38	%
03	3	12	C	21	L	30	U	39	*
04	4	13	D	22	M	31	V	40	+
05	5	14	E	23	N	32	W	41	–
06	6	15	F	24	O	33	X	42	.
07	7	16	G	25	P	34	Y	43	/
08	8	17	H	26	Q	35	Z	44	:

TION MARKS, WHICH ARE SUFFICIENT FOR RUDIMENTARY WEB ADDRESSES AS SHOWN IN TABLE (5). TWO CHARACTERS ARE CODED IN AN 11-BIT VALUE BY THIS FORMULA: $V = 45 \times C1 + C2$

3. PROPOSED ALGORITHM

IN OUR APPROACH, NEW DATA-HIDING ALGORITHM IS INTRODUCED. WHERE, ONE QR CODE IS USED AS INPUT, TO OBTAIN ONE QR AS A RESULT. THE QR IS INVERTING IN TWO SPECIAL SELECTED AREAS TO GENERATE ONE CIPHERED QR CODE AS IN SENDER SIDE (ENCRYPTION PROCESS). IN RECEIVER SIDE, THE PROCESS IS REVERSED ONLY BY REPEAT THE PREVIOUS PROCESS BY INVERTING THE SAME TWO SPECIAL SELECTED AREAS IN ENCRYPTED QR (CIPHER); WHERE THE WHITE (DOT) IN QR REPRESENT (1) AND THE BLACK MODULE (DOT) IN QR REPRESENT (0) WHEN INVERTED. THE QR PRODUCED ONE QR IMAGE.

3.1. Algorithm of convert plaintext to QR_code

STEP1: WRITE MESSAGE (TEXT).
STEP2: GENERATE QR CODE FOR THE MESSAGE.
STEP3: SAVE QR IMAGE AS P.

3.2. Algorithm of getting size of dots in QR

STEP1: START.
STEP2: DO LOOP TO GET BEGINNING OF DETECTION PATTERN ON THE TOP LEFT IN QR PLAIN.BMP WITH WIDTH I AND HEIGHT J.
STEP3: DO LOOP TO GET THE ENDING OF DETECTION PATTERN ON THE BOTTOM LEFT IN QR PLAIN.BMP WHIT WIDTH I1 AND HEIGHT J2.
STEP4: CALCULATE THE SIZE OF DOT FROM I,I1 AND J,J2.
STEP5: end.

3.3.Algorithm of Encryption

STEP1: START.
STEP2: LOAD QR IMAGE P.
STEP3: DEFINE CIPHER AS BITMAP FILE WITH DIMENSIONS WIDTH (WD) & HEIGHT (HG).
STEP4: CALL FUNCTION TO PUT P IMAGE IN CIPHER IMAGE EXCEPT TWO IMPORTANT REGIONS.
STEP5: CALL PREVIOUS SUB ROUTINE TO GET FIRST REGION INDICES (I,J).
STEP6: LOOP STATEMENT X=I TO END FIRST REGION
LOOP STATEMENT Y=J TO END FIRST REGION
CIPHER(X)(Y)=NOT(P(X)(Y))
NEXT Y,X.
STEP7: CALL PREVIOUS SUB ROUTINE TO GET SECOND REGION INDICES (I1,J1).
STEP8: LOOP STATEMENT X=I1 TO END SECOND REGION
LOOP STATEMENT Y=J1 TO END SECOND REGION
CIPHER(X)(Y)=NOT(P(X)(Y))
NEXT Y,X.
STEP9: END.

3.4. Algorithm of Decryption

STEP1: START.
STEP2: LOAD ENCRYPTED QR IMAGE C.
STEP3: DEFINE PLAIN AS BITMAP FILE WITH DIMENSIONS WIDTH (WD) & HEIGHT (HG).
STEP4: CALL FUNCTION TO PUT C IMAGE IN PLAIN IMAGE EXCEPT TWO IMPORTANT REGIONS.
STEP5: CALL PREVIOUS SUB ROUTINE TO GET FIRST REGION INDICES (I,J).
STEP6: LOOP STATEMENT X=I TO END FIRST REGION
LOOP STATEMENT Y=J TO END FIRST REGION PLAIN (X)(Y)=NOT(C(X)(Y)) NEXT Y,X.
STEP7: CALL PREVIOUS SUB ROUTINE TO GET SECOND REGION INDICES (I1,J1).
STEP8: LOOP STATEMENT X=I1 TO END SECOND REGION LOOP STATEMENT Y=J1 TO END SECOND REGION PLAIN (X)(Y)=NOT(C(X)(Y))
NEXT Y,X.
STEP9: END.

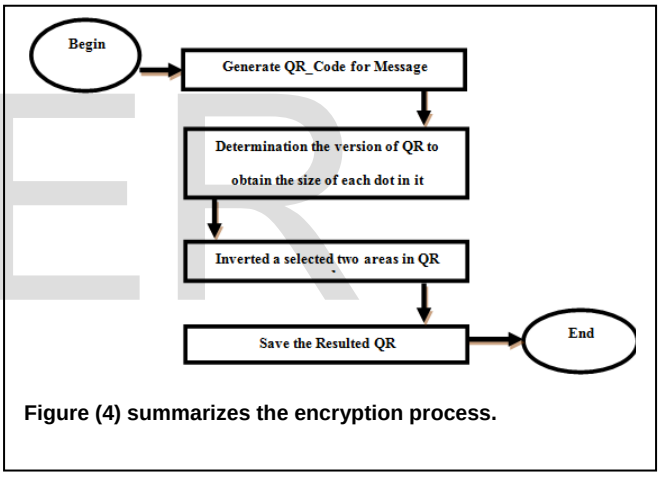

Figure (4) summarizes the encryption process.

Figure (5) summarizes the decryption process.

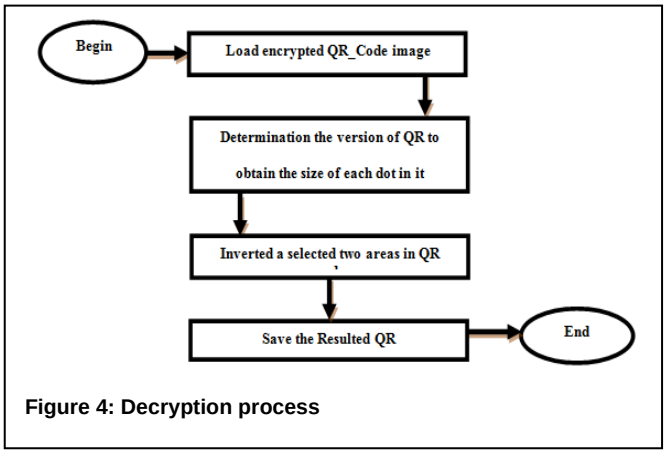

Figure 4: Decryption process

4.TESTING AND RESULT

THE TEST INCLUDES TWO PROCESSES ENCRYPTION PROCESS AND

DECRYPTION PROCESS.

4.1. Encryption Process

FOR EXAMPLE, COSEHO A SECRET MESSAGE "BOOK". FIGURE (6) ILLUSTRATES THE QRS FOR SECRET MESSAGE & THE RESULTED QR OR FINAL QR IMAGE. THE FINAL QR IS UNREADABLE.

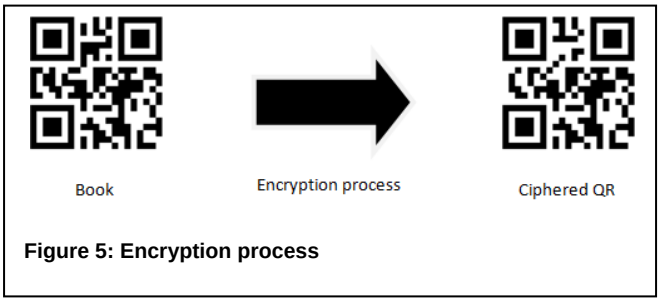

Figure 5: Encryption process

4.2. Decryption Process

THE PREVIOUS EXAMPLE IS USED FOR THE INVERSE OPERATION (DECRYPTION). FIGURE (7) SHOWS THE QR CODES FOR RESULTED QR & SECRET MESSAGE.

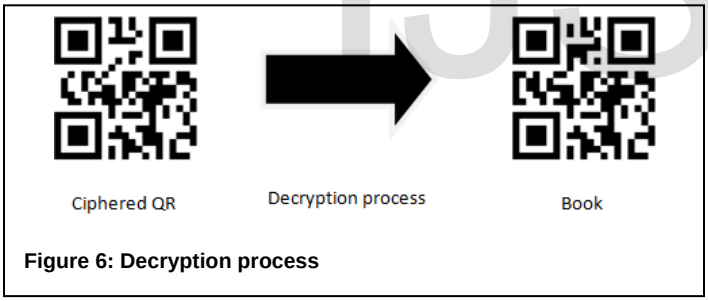

Figure 6: Decryption process

5. CONCLUSION

THIS METHOD COULD BE USED IN LARGE SCOPE. SINCE QR CODES COULD BE USED FOR CONVERTING INFORMATION TO 2D BARCODE (QR CODE), THIS METHOD CAN BE USED TO ENCRYPT ANY TYPE OF MESSAGES OR FILES (NUMERIC, URLS, ALPHANUMERIC AND BYTE/BINARY) AND SEND IT TO THE RECEIVER SAFELY. ALSO, THE METHOD ENABLES THE USER TO STORE IMPORTANT DATA OR INFORMATION SAFELY AS QR. THE INFORMATION COULD BE RETRIEVED EASILY FROM THE QR CODE USING QR READER.

6. References

[1] P. Kieseberg, M. Leithner, M. Mulazzani, L. Munroe, S. Schrittwieser, M. Sinha, et al., "QR code security," in Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia, 2010, pp. 430-435.

[2] S. Dey, S. Agarwal, and A. Nath, "Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System," in Communication Systems and Network Technologies (CSNT), 2013 International Conference on, 2013, pp. 512-517.

[3] . Dey, "SD-EQR: A New Technique To Use QR CodesTM in Cryptography," arXiv preprint arXiv:1205.4829, 2012.

[4] D. Chatterjee, J. Nath, S. Dasgupta, and A. Nath, "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm," in Communication Systems and Network Technologies (CSNT), 2011 International Conference on, 2011, pp. 89-94.

[5] D. Sonawane, M. Upadhye, P. Bhogade, and S. Bajpai, "QR based Advanced authentication for all hardware platforms," International Journal of Scientific and Research Publications, vol. 4, pp. 1-4, 2014.

[6] M. Bajpai and A. P. Agrawal, "INTEGRATION OF 2D SECURE BARCODE IN IDENTITY CARDS: WITH ADDITIONAL SECURITY FEATURES."

[7] O. Sharaby, "Form Meets Function: Extreme Makeover QR Code Edition," ed: Archived from the original on, 2012.

[8] H. Chan, "How to: Make your QR codes more beautiful," Maskable, April, vol. 18, 2011.

[9] R. Cox. (2012). QArt Codes. Available: http://web.archive.org/web/20150321031237/http://research.swtch.com/qart

[10] S. Hore, T. Bhattacharya, and S. B. Chaudhuri, "A Robust Medical Image Authentication Technique using QR Code and DWT," International Journal of Computer Applications, vol. 83, 2013.