Encrypted QR Code

Jiahui Cui and Basar Koc
{jcui, bkoc}@stetson.edu

Problem

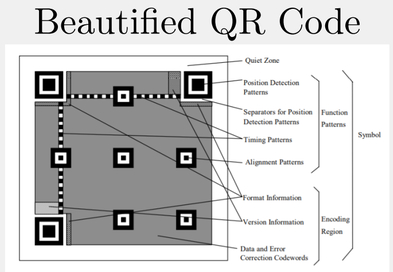
The quick response (QR) code is a matrix barcode that can be used to store various type of information. Because of its fast reacting feature, QR codes have been widely used in many fields. Some of them require authentication and privacy. Using the QR code in such systems has a disadvantage, that is standard QR code does not provide any security.

Solution

In this study, we present a new technique for the encryption and decryption of QR codes. The proposed technique applies a Feistel-like encryption scheme to the QR code and provides security at the expense of a negligible time without any compression.
Our proposed coding scheme starts by re-fragmenting the information and changes every bit to hide the source information by employing a Feistel-like encryption algorithm, then shuffle the order of all segments.The complete encryption algorithm repeats the steps above 10 rounds. Our decryption algorithm only cost about one third time of the encryption process on average.

QR Code

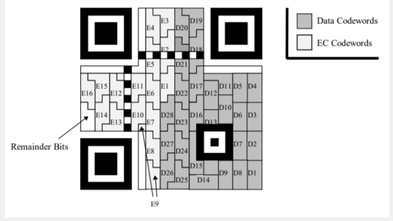
Beautified QR Code



QR Code Structure

QR code is a machine-readable two-dimensional image that can carry up to 4296 Alphanumeric characters or 2953 8-bit (Byte) information.

Functional Pattern is to help scanner quickly recognize the QR code.



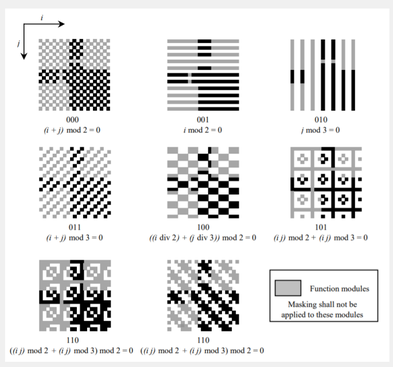
Encoding Region

The Encoding Region consists of data and Error Correction Code (ECC).

Error Correction Level	Recovery Capacity % (approx.)
L	7
M	15
Q	25
H	30

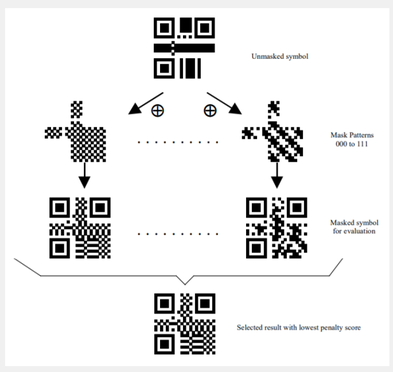
Error Correction

ECC would recover corrupted data.



Mask

Masks make black and white squares evenly distributed in the QR Code.

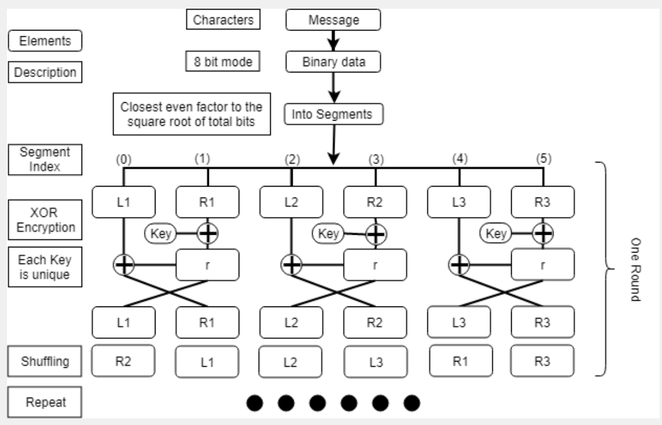


Select Mask

Choose the mask with lowest penalty score for final QR Code.

Scheme

Scheme Process

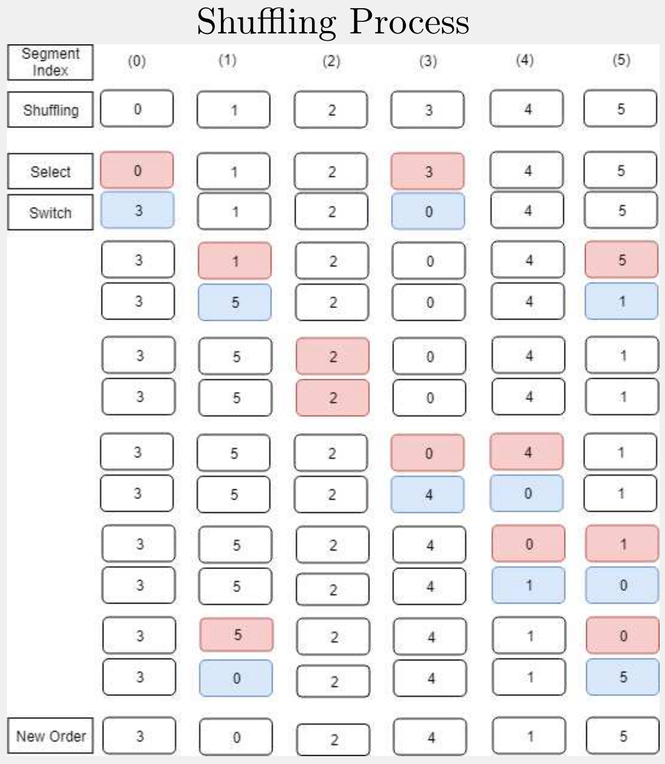


Shuffling Numbers

Shuffling

Keys		110101101		001001010		111000111	
Decimal	|2^6-Decimal|	429	365	74	10	455	391
Mod 6	Mod 6	3	5	2	4	5	1

Shuffling Process



Key Selection

1	0	0	1
0	1	1	1
1	1	0	1
0	0	1	1

Create a 4×4 binary matrix, then select a initial value and store it as the most significant bit.

1	0	0	1
3	2	1	1
4	X	0	1
5	6	7	1

Using formula $n^2 \ mod \ modulo$ where $n = i + j$, $modulo$ is a primary number,get a random number(R).

1	0	0	1
0	1	1	1
1	1	0	1
0	0	1	1

Using $R \ mod \ 8$ calculate the location of next bit.

1	0	0	1
0	X	1	1
1	1	0	1
0	0	1	1

Increment n by 1, for the rest of the bits.

3	2	1	1
4	X	0	1
5	6	7	1
0	0	1	1

Repeat the process above.

Experimental Result

We tested our proposed encryption and decryption technique using Google's open-source ZXing ("zebra crossing") multi-format 1D/2D barcode image processing library. The following figures show the encrypted QR codes. The tested messages and scanning results are given in Table I.

Fig: Encrypted QR codes (a)(b)(c)

TABLE I: QR code scanning results

	Original Message	Scanning Result
(a)	Hello IEEE	‡sÂS©Y4Kô
(b)	http://www.ieee-security.org	î #XrøÜR ^vc/{'Kô|çèA
(c)	The QR code itself does not have any security components so it is easy to cause information leakage.	ôKóDh_šœ˜ÌôP šcIØÙÙþXCMž ÕE¡1^v<H¸º) æl9>ª(¸ÁE^ ŒÅ6ŸMÄíðÌØ[S™»Ë£ZÎ'ó7Jq á]\•,\¶

1: Encrypted message from WeChat

Key Strength

- 10 character message as an example.
- 40 bits key per round (half of the message)
- 10 rounds by default totally 400 bits key.
- 2^{400} possibility to brute force.

References

[1] ISO/IEC 18004:2000 - Information Technology - Automatic Identification and Data Capture Techniques - Bar Code Symbology - QR Code, 2000

[2] P. Kieseberg, M. Leithner, M. Mulazzani, L. Munroe, S. Schrittwieser, M. Sinha, and E. Weippl, "QR code security," In Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia (MoMM '10) ACM, New York, NY, USA, 430-435.

[3] [Online]. Available: https://github.com/zxing/zxing