International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

A Secured Quick Response (QR) Code Method with Fuzzy Encoding of Secret Message

Dr. Siddhartha Choubey[1], Nidhi Chandel[2]

[1, 2]Department of Computer Science and Engineering, Faculty of Engineering and Technology
Shri Shankaracharya Technical Campus, Junwani, Bhilai, District-Durg, Chhattisgarh-490020, India

Abstract: ***Now a day everywhere Digital formation is involved. all people are use to technology in daily life but the excess use of technology safety is also more important. Quick response code is the process that high quality features such as stored high capacity information in small coded from and embed the secret information. The cryptography technique is used for hiding secret message, the process at the sender side to encode the original message in to any coded from and at receiver side the decoded the original message. Hiding original message is based on bit technique so it is chance to modification attack .if attacker change any bit such as adding a new bit or change the bit then it is some problem arise to recover the original message. In this paper, we propose the a scheme based on Cyclic Redundancy Check and list the decoding to overcome this problem we also conduct our solution by analyzing the complexity, security, experiment.***

Keywords: QR code; Cyclic Redundancy Check; cryptography; encryption; decryption; encode; decode; error correction code;

1. Introduction

In the range of data innovation huge measure of advancement are predominately striking give fast changes. One of these fast enhancements in the information innovation in the current years is QR Code or Quick Response Code. QR (Quick Response) code [1] is a lattice standardized identification or two dimensional code which was produced by Toyota backup Denso- Wave division. These QR code initially utilized by Denso-Wave for vehicle commercials. It's initially utilized for following vehicle make. Aside from alternate frameworks quick coherence and relatively extensive capacity limit helps QR code from other security related information stockpiling codes. The encoding and deciphering of information in QR code is done at rapid. Data can be encoded in vertical and level heading. As it has two dimensional stockpiling regions, along these lines it holding up a few hundred circumstances of information other than the conventional standardized tag framework which store information in prior time. Scanner tag (Figure 1) can just store information in just a single bearing.QR codes are these days dominating in commercials and gadget data stockpiles in advanced hardware, for example, cell phones, portable workstations and so forth [2]. QR code quickly increased universal prominence and its utilization turns out to be high. Broad selection of QR code is expected capacity limit and it is broadly utilized as a part of Japan in light of the fact that QR codes have the capacity to store Kanji images. The essential component of QR code (Figure 2) is depicted by the way that it radically accelerates the stream of data where individuals can get to/view either computerized promotions, a declarations in the road or shopping center or in a site or contact stockpiling data which they could effortlessly store and use for different applications.

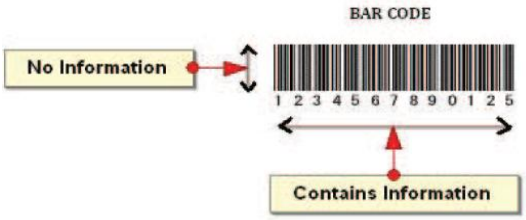

Figure 1: Bar Code (One Dimensional)

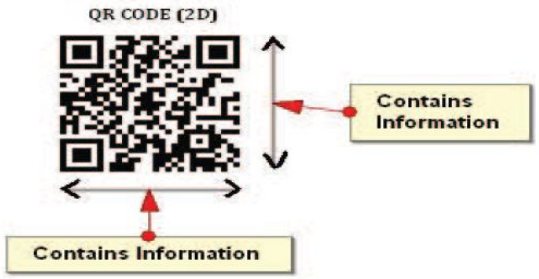

Figure 2: QR Code (Two Dimensional)

Since QR code is so prevalent, some secret data could be exchanged by means of it. The authors [2], [3], [4] investigated the properties of each QR code before installing it into this one. On the off chance that they need to insert a secret message into QR code, they will encode it first. From that point forward, they misuse the structure of QR code which code they need to utilize. It requires investment, hazards, and can't get the secret message straightforwardly from this QR code. Lin et al. [1] watched and proposed a novel plan to tackle this issue. The thought to shroud secret messages into QR code is to utilize the blunder redress ability. This thought is initially proposed by Lin et al. [1]. As a matter of first importance, they encode the secret message sm by utilizing a common key K and get EK(sm). From that point forward, they implant each piece of EK(sm) into QR code. Their first drawback is that in the event that any piece of EK(sm) is harmed, it is difficult to recoup sm from QR code. The second drawback is that if an assailant does not change any piece of EK(sm) but rather includes some additional blunder values into QR code, they can't

recuperate their secret message. To the best of our insight, every single past system utilized bit installing plan to insert secret messages into QR code. It is so defenseless against the change assault, i.e. an assailant changes any piece of secret messages. We propose utilizing Cyclic Redundancy check for error correction.

Our Contribution: Our main contribution is to propose algorithms that hide a secret message into QR code. The secret message is invisible to attackers and secure against modification or damage attack. We analyze them under complexity and security aspects, and conduct these algorithms by experiments.

Outline of the paper: The rest of this paper is organized as the following. Section II present problem identification. Section III describes the methodology. Section IV presents the result. The last section summarizes the key point and mention future scope.

2. Problem Identification

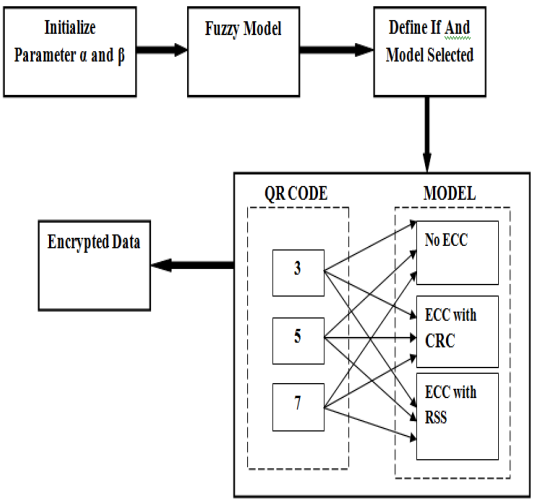

Figure 3: The implementation model

Above fig show the implementation of FUZZY logic in QR model which will describe below.

(a) First of all the two parameter are initialize α and β. Where α = confidentially and β = security fall.

(b) Then the fuzzy logic is applying. where Fuzzy logic means the logic includes 0 and 1 as extreme cases of truth (or "the state of matters" or "fact") but also includes the various states of truth in between so that, for example, the result of a comparison between two things could be not "tall" or "short" but ".38 of tallness.

(c) Next process is defining value of α and selects which model select with QR version.

(d) In this there are three version of QR code such as 3, 5, 7 and the three model which show No ECC (Error Correction Code), ECC with CRC(Cyclic Redundancy Check) at last ECC with RSS(Reed Solomon Code).the version and model selection both are deepened on user choice.

- If user wants to less security and pass the message then select the NO ECC.
- If user wants to medium security and pass the message then select the ECC with CRC where CRC at least detect the error.
- And if user wants to medium security and pass the message then select the ECC with RSS where RSS detect and also correct the error.

(e) After that user encrypted the data.

3. Methodology

Algorithm 1:
x(0,1) and y= (0,1)
if α = x and β= y ,where x= low value and y = low value
then
model is initial.
if α = x and β= y ,where x= medium value and y = low value
then
model intermediate
if α = x and β= y ,where x= high value and y = low value
then
model is expert
if α = x and β= y ,where x= low value and y = medium value
then
model is initial.
if α = x and β= y ,where x= medium value and y = medium value
then
model intermediate
if α = x and β= y ,where x= high value and y = medium value
then
model is expert
if α = x and β= y ,where x= low value and y = high value
then
model is initial.
if α = x and β= y ,where x= low value and y = high value
then
model intermediate
if α = x and β= y ,where x= low value and y = high value
then
model is expert

Algorithm 2: Hiding Secret message in to QR code with CRC.

INPUT: A massage m that can be encoded by a QR code QRC and a Secret Message Sm of length S_k

OUTPUT: QR code contains m and Sm.

Step1: use of QRC to Encode the message m. where α= medium value Choose Sn (no of String) s.t. $S_k < Sn < T$

Step 2: Choose a secret generator polynomial g1(x) for [S_{n1}, S_{k1}]-Reed-Solomon code (denote RSS). Use RSS to encode the message Sm and get M1=(m_{11} m_{12}…..$m_{1_{sn\,1}}$).

Step3: Choose B integers n_{11}, . . . ,n_{1B} s.t.: $0 \leq n_{1i} \leq t_i$ and $\sum_{i=1}^{B} n_{1i} = S_{n1}$. Let us define $n_{10} = 0$.

Step 4.: Choose arbitrary n_{1i} positions of m_i, i = 1, . . . ,B. Assume that there are $m_{i\,j1}$,$m_{i\,j1}$, . . . $m_{ij_{n1i}}$ and $1 \leq j_1 < j_2 < . . . < j_{n1} \leq n_i$.

Step5: Replace m_{ij_x} by. $m_{1(x+n_{10}+\cdots+n_{1(i-1)})}$, x=1,2, . . . ,n_{1i}.

Algorithm 3: Hiding Secret message in to QR code with RSS.

INPUT: A massage m that can be encoded by a QR code QRC and a Secret Message Sm of length S_k
OUTPUT: QR code contains m and Sm.
Step1: use of QRC to Encode the message m. where α= high value Choose Sn (no of String) s.t. $S_k < Sn < T$
Step2: Choose A secret message polynomial generator g2(x) for [S_{n2} , S_{k2}]- Cyclic Redundancy check (denoted CRC). Use CRC to encode the message Sm and get M2= (m_{21} m_{22}…..$m_{2_{sn\,1}}$).
Step3 : Choose B integers n_{21}, . . . ,n_{2B} s.t.: $0 \leq n_{2i} \leq t_i$ and $\sum_{i=1}^{B} n_{2i} = S_{n2}$. Let us define $n_{20} = 0$.
Step4: Choose arbitrary n_{1i} positions of m_i, i = 1, . . . ,B. Assume that there are $m_{i\,j2}$,$m_{i\,j2}$, . . . $m_{ij_{n2i}}$ and $1 \leq j_1 < j_2 <$. . .$< j_{n2} \leq n_i$.
Step5: Replace m_{ij_x} by. $m_{2(x+n_{20}+\cdots+n_{2(i-1)})}$, x=1,2, . .n_{2i}.

Algorithm 4: Decoding QR code and getting the Secret message using decoding method and
Error correction (CRC) and Error correction &detection (RSS) method.

INPUT: QR code contains the secret message m and the secret message sm.

OUTPUT: m and Sm.
Step 1. Use QRC to decode QR code, then get the message m and error values.
Step 2. Combine the error values to get the secret message M2.
Step 3. Using Decoding and Error Correction method.
- If α= low value then No ECC.
- If α= medium value then CRC.
- If α= high value then RSS.

4. Result

In this section QR code is secure the message but it is depend on user choice(0,1) if user wants to secure the message then put the value of alpha and beta is high. The value of alpha beta and model is shown in figure 4,if any changes in value of alpha and beta the graph is also change.

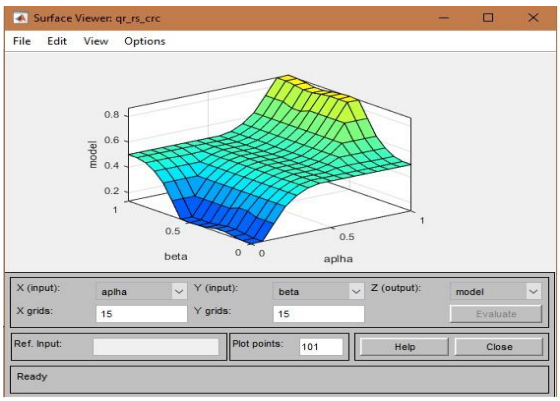

Figure 4: Graph of alpha beta and model

5. Conclusion

We have presented a robust scheme to hide secret messages in to QR code. Our scheme is secure against bit- changed attack and can tolerate more error than usual. However, the length of secret message is smaller than the one using existing scheme .In our scheme to encode the secret message before embedding the outcome message into QR code. The outcome message probably is decoded.

6. Scope for Further Work

Our further work is more survey on this problem and find the algorithm to help the reside the problem .Description of a pattern language to describe patterns .It should be possible to describe patterns in the pattern language via the GUI tool and then automatically generate the requisite code to match the pattern.

References

[1] Akhil N.V., Athira Vijay Deepa S kumar, kerala India Qr code Security using proxy Re Encryption , IEEE2016
[2] Mansanori KIKUCHI, Masaaki FUJIYOSHI and Hitoshi KIYA, Tokyo: A new color QR Code forward compatible with the standard QR code decoder.
[3] Thach V. Bui* , Nguyen K. Vu.*, Thong T.P. Nguyen*, Isao Echizen and Thuc D. Nguyen*.Tokyo Japan, Robust Message hiding for QR code, 2014 Tenth International Conferences on intelligences Information Hiding And Multimedia Signal Processing, IEEE 2014.
[4] Satid Vongpradhip , Suppat Rungraungsilp, Bangkok, Thailand : QR Code invisible Watermarking in frequency domain, IEEE2011
[5] Lin, Pei-Yu, Yi-Hui Chen, Eric Jui-Lin Lu, and Ping-Jung Chen. Secret Hiding Mechanism Using QR Barcode. In Signal-Image Technology & Internet-Based Systems (SITIS)2013International Conference on, pp.22-25IEEE, 2013
[6] Y. Liu, J. Yang, And M. Liu, "Recognition Of Qr Code With Mobile Phones," In Control And Decision Conference, 2008. Ccdc 2008. Chinese. Ieee, 2008, Pp. 203–206.
[7] D. Pintor Maestre, "Qrp: An Improved Secure Authentication Method Using Qr Codes," 2012.
[8] F. Aloul, S. Zahidi, And W. El-Hajj, "Two Factor Authentication Using Mobile Phones," In Computer Systems And Applications, 2009. Aiccsa 2009. Ieee/Acs International Conference On. Ieee, 2009, Pp. 641– 644.
[9] Chen, Wen-Yuan, And Jing-Wein Wang. Nested Image Steganography Scheme Using QR-Barcode Technique. Optical Engineering 48, No. 5(2009): 057004-057004.
[10] Chung, Chin-Ho, Wen-Yuan Chen, and Ching-Ming Tu. Image hidden technique using QR-barcode. In Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP'09. Fifth International Conference on, pp. 522-525. IEEE, 2009.
[11] Huang, Hsiang-Cheh, Feng-Cheng Chang, And Wai-Chi Fang. Reversible Data Hiding With Histogram-Based Difference Expansion For QR Code Applications. Consumer Electronics, IEEE Transactions On 57, No. 2 (2011): 779-787.
[12] Iso/Iec 18004:2006. Information Technology – Automatic Identification And Data Capture Techniques – Qr Code 2005 Bar Code Symbology.

[13] S. Narayanan, "Qr Codes And Security Solutions," International Journal Of Computer Science Andtelecommunications, Vol. 3, No. 7, Pp.69–71, 2012.
[14] 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. Acm, 2010, Pp. 430–435.
[15] C. Y. Law, W. W. S. So, and, "Qr Codes In Education," 2010.
[16] G. Starnberger, L. Froihofer, And K. M. Goschka,¨ "Qr-Tan: Secure Mobile Transaction Authentication," In Availability, Reliability And Security, 2009. Ares'09. International Conference On. Ieee, 2009, Pp.578– 583.
[17] http://www.qrcode.com