Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-6, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

Enhanced Security on 2D Barcode Using Picture Embedding Picode Approach

Ms. Dini Davis[1] & Ms. Soumya P[2]
[1] M.Tech Student, Dept.Of CSE ,Thejus Engineering College, Vellarakkad
[2] Asst. Professor, Dept.Of CSE ,Thejus Engineering College, Vellarakkad,

Abstract*: Two Dimensional barcodes have been widely used as an interface to connect potential customers and advertisement contents. However, the appearance of a conventional 2D barcode pattern is often too obtrusive for integrating into an aesthetically designed advertisement. Besides, no human readable information is provided before the barcode is successfully decoded. Thus an attractive picture embedding 2D barcodes are designed and named it as PiCode. The information processing system plays crucial part in the internet. Online information security has become the top priority in all sectors. Failing to provide online information security may cause loss of critical information or someone may use or distribute such information for malicious purpose. So, Quick Response barcodes have been used as an effective way to securely share information. In order to improve the capacity as well as the security, PiCodes can be used as more effective secure information sharing.*

Keywords: *2D barcode, information sharing, perceptual quality, Quick Response barcodes.*

.

1. Introduction

A barcode is an optical, machine-readable, representation of data; the data usually describes something about the object that carries the barcode. Originally barcodes systematically represented data by varying the widths and spacings of parallel lines, and may be referred to as linear or one-dimensional (1D). Later two-dimensional (2D) codes were developed, using rectangles, dots, hexagons and other geometric patterns in two dimensions, usually called barcodes although they do not use bars as such. Barcodes originally were scanned by special optical scanners called barcode readers. Later applications software became available for devices that could read images, such as smartphones with cameras.

Due to tremendous growth in communication technology, sharing the information through the communication network has never been so convenient. Nowadays information is processed electronically and conveyed through public networks. Such networks are unsecured and hence sensitive information needs to be protected by some means. Cryptography is the study of techniques that allows us to do this. In order to protect information from various computer attacks as well as network attacks various cryptographic protocols and firewalls are used. But no single measure can ensure complete security.

The use of internet and sharing information are growing increasingly across the globe, security becomes a vital issue for the society. Security attacks are classified as passive attacks and active attacks [11]. In passive attacks, attacker monitors network traffic and looks for sensitive information but does not affect system resources. Passive attacks include traffic analysis, eavesdropping, Release of message contents [11]. In active attack, attacker breaks protection features to gain unauthorized access to steal or modify information. Active attacks include masquerade, replay, modification of messages, and denial of service [11].Therefore, security threats (such as eavesdropping, data modification, phishing, website leaks etc.) force us to develop new methods to counter them. Considering QR barcodes as an effective media of sharing information, many researchers have proposed information/data hiding methods [6,7, 8, 9.] as well as online transaction systems [1,2,3,4,5] using QR barcode. In this paper, we describe information hiding schemes using PiCodes. PiCodes are the picture embedding 2D barcode with high capacity and less distortion

2. Background

In this section, the information hiding techniques used in QR barcodes are discussed:

2.1. Using Hash function

Authors of [6] proposed an information hiding method using QR barcode. In this Method, information which is to be transmitted is first encrypted by using hash function, with a secret key K. The key K is known in advance to both sender as well as receiver. After the encryption process; QR code for encrypted information is created and sent over the

network for the receiver. If an intruder were to try to extract the information from QR code, he/she would only be able to read the code with a QR code decoder but would not be able to get the secret information from QR code. Only the authorized user with secret key K can retrieve the secret information from QR code. The scheme is able to encode large amounts of secret information into a QR code based on selection of the QR version and the error correction level. The main disadvantage is that the whole secrecy of this scheme depends on key K. If someone gets the key, this scheme can reveal

2.2. Using TTJSA symmetric key Algorithm

Authors of [7] proposed an encrypted information hiding mechanism using QR barcode. In this method, information which is to be transmitted is first encrypted using TTJSA symmetric key algorithm. For encrypted information, QR code is generated by using QR generator. If an intruder tries to extract the information from QR code then he cannot do that because the cryptographic key is unknown to him. The decryption process is exactly reverse of the encryption process. TTJSA algorithm is free from attacks such as differential attacks, plain-text attacks or brute force attacks.

2.3. SD-EQR

Author of [8] presents a new technique using QR barcode to transfer information securely through public network. In this method, the password is entered along with the information. The secret key generated from the password which acts as the key for encryption process. The process of generating secret key is:
Choose password of any size, but should consist of only ASCII characters (0-255).
• Find the length of the entered password denoted by "L".
• Multiply 'L2' with the sum of the ASCII values of each letter of the word entered in the password to get S.
• Each digit of the S is added with each other. The ultimate sum is the secret key.
This secret key will be added to each character in the text entered in the information and complete the first phase of encryption process. After doing the first level of encryption, many other several encryption techniques are used to encrypt the message further to increase the level of security. At last final encrypted information is encoded into QR code. QR code efficiently handles the 1,264 characters of ASCII text in version 40 with Error correction level H. if encrypted information size is larger than capacity of QR code then other QR code is generated containing encrypted information after 1,264 characters. This method is continued until the whole encrypted information is converted into QR codes. Decryption is actually the reverse process of the encryption.

3. Literature Survey

QR code is an invention of Denso Wave Inc. and has been included in the ISO standard since 2000 [12]. It was created for industrial applications, such as auto-identification and tracking of electronic parts (c.f. [13]). Its pattern is in black and white, and consists of some large fixed patterns which are designed to guarantee detection and decoding robustness. QR code contains three squarish finder patterns located at the top left, top right and bottom left corners, respectively, an alternating black and white timing pattern between adjacent finder patterns, as well as a smaller squarish alignment pattern at the bottom right region [14]. For the high capacity QR code there are more fixed patterns located in the interior region of the barcode. Such fixed patterns are only present in QR codes with a storage being greater than 196 bytes. This is because as the barcode capacity increases, the module alignment accuracy becomes more critical and the fixed patterns can be utilized to improve module alignment.

The direct replacement of data which replaces a portion of the QR code by the embedded image and relies on the error correction capability of the barcode to tolerate the replacement incurred errors. However, the embedding region has to be carefully chosen so as to ensure the decodability of the barcode [15]–[18]. Ono et.al [15] embeds an image into a barcode by replacing part of the encoding region with the image. The replacement region is selected by finding the appropriate scale, angle and position parameters using an optimization approach. Similarly, Samertwit and Wakahara [16] find the best embedding region by further considering the error correction level. Wakahara and Yamamoto [17] develop a picture embedding scheme for QR code with a workable software prototype which is capable of showing the error protection level and the validity of the embedding operation in real time. Lin et. al [18] embed a color image in the barcode by considering some perceptual features, such as the saliency regions of the images.

4. Proposed System

In this section, the proposed PiCode system for secret sharing is described with an emphasis on the novel aspects of the encoding and encrypting algorithms. For the encoding part, the details of the modulation scheme will be presented to illustrate how PiCode preserves the perceptual quality of the embedded image while minimizing the interference of the latter incurred on the modulation waveform.

For the encryption part, the algorithm SHA1for performing hashing is used.

4.1 PiCode Generation

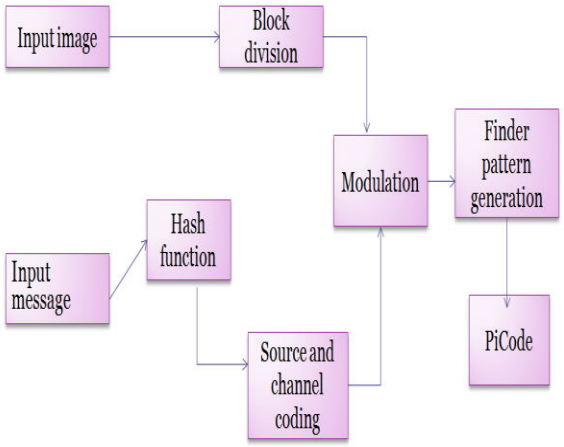

Figure 1: PiCode generation

The PiCode encoding process can be divided into two parts: the input processing and the PiCode generation. In the first part, the input message is converted into a bit stream with source coding and channel coding to improve the efficiency and robustness of the encoded message. The input image is then divided into a 2D grid of image blocks according to the user's input on the number of modules per dimension. Each block consists of k x k pixels. In the PiCode generation part, the pixels in each image block are modified by the proposed adaptive modulation scheme so that each image block conveys a bit '0' or '1'. Finally, a layer of finder pattern of one module wide is added to the exterior of the modulated 2D grid of image blocks to form the PiCode. In the following, we describe the channel coding and the modulation schemes which are essential in balancing the decoding robustness and perceptual quality.

As shown in Figure 1, the proposed modulation scheme divides a module into a block of bi-level pixels. For illustration purpose, the module size is set as 4 x 4 pixels which is the minimum printed/displayed size per module to guarantee theoretical readability. The actual module size is adaptive to the resolution of the embedded image and the number of barcode modules per dimension. The pixels of a module are separated into the inner and outer parts, and the inner part is of size 2 x 2 pixels. If the inner part has a higher intensity, bit '1' is encoded. Otherwise, bit '0' is encoded.

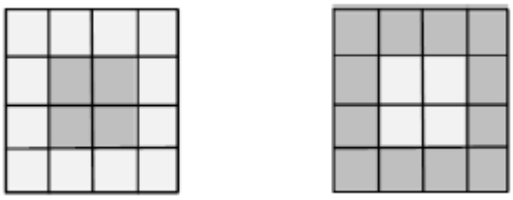

Figure 2: Representation of Bit '0' and Bit '1'

Figure 3 illustrates the steps for PiCode decoding process. First, the captured PiCode image is converted to grayscale and is binarized to facilitate the search for the potential barcode regions which are then checked against the detection criterion. If the check is passed, the four corners are obtained; otherwise, the image will be rejected and the decoding process will be re-initiated with another image frame. Based on the barcode corner locations, the perspective distortion is then estimated and compensated on the graylevel image. For the module alignment step, the region for each PiCode module is obtained based on broken line parts of the finder patterns. The following demodulation process is the reverse of the modulation process by inspecting the intensity differences between the inner and outer parts of each module. The modulated bit in each module is retrieved by the demodulation operation. Finally, the message is obtained by applying channel and source decoding to the demodulated bits. In this part, we mainly cover the corner detection, module alignment and demodulation steps which reflect our major contributions.

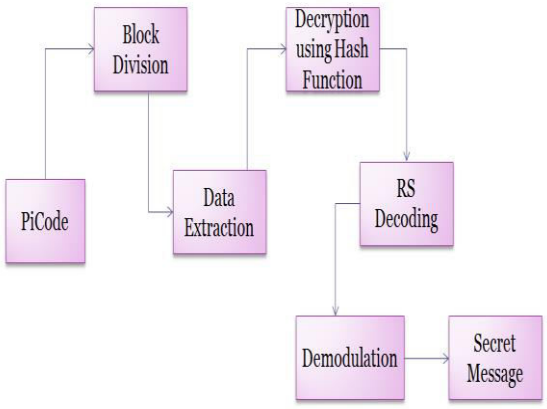

Figure 3 : PiCode Decoding

4.2 Data Encryption

A hashing function called SHA1 algorithm, is used to encrypt the data. SHA1 requires 160 bits or 5 buffers of words as message. The SHA1 algorithm is computed by the given pseudo code

For loop on k = 1 to L
(W(0),W(1),...,W(15)) = M[k]
For t = 16 to 79 do:
W(t) = (W(t-3) XOR W(t-8) XOR W(t-14) XOR W(t-16)) <<< 1
A = H0, B = H1, C = H2, D = H3, E = H4
For t = 0 to 79 do:
TEMP = A<<<5 + f(t;B,C,D) + E + W(t) + K(t) E = D, D = C,
C = B<<<30, B = A, A = TEMP
End of for loop
H0 = H0 + A, H1 = H1 + B, H2 = H2 + C, H3 = H3 + D, H4 = H4 + E
End of for loop
Output:
H0, H1, H2, H3, H4, H5: Word buffers with final message digest

5. Conclusion

PiCodes have a fast decoding robustness and thus it is less secured. QR codes are widely used in secret sharing. To improve the capacity and security a novel picturesque 2D barcode that is, PiCode can be used. PiCode provides one of the best perceptual qualities for the image. The PiCode system is designed with less obtrusive finder patterns to avoid distortions. The high capacity can be got in the picture through adjustment scheme. The encryption algorithm SHA1 keeps the confidentiality of the data. Thus the PiCode can assume a cruicial part in mystery information sharing over the web. Also, more encryption methods can be used to improve security and quality for the PiCode in future.

6. References

[1] Kaushik S., "Strength of Quick Response Barcodes and Design of Secure Data Sharing System" International Journal on Advanced Computing & Science (IJACSA), Dec 2011.
[2] Kaushik S.; Puri S., "Online Transaction Processing using Sensitive Data Transfer Security Model"4th International Conference on Electronics Computer Technology (ICECT), IEEE, April. 2012.
[3] Suresh Gonaboina, Lakshmi Ramani Burra, Pravin Tumuluru,"Secure QR-Pay System With Ciphering Techniques In Mobile Devices" International Journal of Electronics and Computer Science Engineering.
[4] Jaesik Lee, Chang-Hyun Cho, Moon-Seog Jun,''Secure Quick Response Payment(QR-Pay) System using Mobile Device", Feb 2011.
[5] Sana Nseir, Nael Hirzallah, Musbah Aqel, "A Secure Mobile Payment System using QR Code", 5th International Conference on Computer Science and Information Technology (CSIT), 2013.
[6] Pei-Yu Lin, Yi-Hui Chen, Eric Jui-Lin Lu and Ping-Jung Chen "Secret Hiding Mechanism Using QR Barcode", International Conference on Signal-Image Technology & Internet-Based Systems, 2013.
[7] Somdip Dey, Asoke Nath, Shalabh Agarwal, "Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System", International Conference on Communication Systems and Network Technologies, 2013.
[8] Somdip Dey,"SD-EQR: A New Technique To Use QR Codes in Cryptography" Use of QR Codes In Data Hiding and Securing.
[9] H. C. Huang, F. C. Chang and W. C. Fang, "Reversible data hiding with histogram-based difference expansion for QR Code applications," IEEE Transactions on Consumer Electronics, vol. 57, no. 2, pp. 779-787, 2011
[10] "QR Code, Wikipedia", http://en.wikipedia.org/wiki/QR_code [Online] .
[11] Cryptography & Network Security, Behrouz A. Forouzan, Tata McGraw Hill Book Company.
[12] H. Kato, K. Tan, and D. Chai, Barcodes for Mobile Devices. Cambridge University Press, 2010.
[13] H. Kato and K. Tan, "2D barcodes for mobile phones," in International Conference on Mobile Technology, Applications and Systems, Nov 2005, pp. 8–15.
[14] "Information technology – Automatic identification and data capture techniques – QR Code 2005 bar code symbology specification," ISO/IEC 16022.
[15] S. Ono, K. Morinaga, and S. Nakayama, "Two-dimensional barcode decoration based on real-coded genetic algorithm," in IEEE Congress on Evolutionary Computation, June 2008, pp. 1068–1073.
[16] D. Samretwit and T. Wakahara, "Measurement of Reading Characteristics of Multiplexed Image in QR Code," in International Conference on Intelligent Networking and Collaborative Systems (INCoS), Nov 2011, pp. 552–557.
[17] T. Wakahara and N. Yamamoto, "Image Processing of 2-Dimensional Barcode," in International Conference on Network-Based Information Systems (NBiS), Sept 2011, pp. 484–490.
[18] Y.-H. Lin, Y.-P. Chang, and J.-L. Wu, "Appearance-Based QR Code Beautifier," IEEE Transactions on Multimedia, vol. 15, no. 8, pp. 2198– 2207, Dec 2013.