ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Data security in QR code using Steganography

Bhakti Magadum,

M.E. Student, Dept. of Computer Engineering, SKNCOE, Savitribai Phule Pune University, Pune, Maharashtra India

ABSTRACT: Response Code (QR code) is generally used in daily life in present day because it has high capacity encoding of data, damage resistance, fast decoding and other good characteristics. Since it is favour, people can use it to transmit secret information without inspection. This paper, construct a new rich QR code with the help of steganography approach. There are two level of QR which are public and private. The public level is similar to the standard QR code storage level; hence, it is readable by any classical QR code application**.** The private level is developed by hiding the black modules by number of textured pixels, which are fetched form textured patches. This textured patches extracted form cover image. So this new rich QR code helpful for transfer secrete message and verify original message.

KEYWORDS: QR code, double storage levels, private message, document authentication, print-and-scan process, Data embed-ding, reversible, steganography, texture synthesis.

I. INTRODUCTION

Quick response code is a type of two dimensional barcode evolve by Denso-Wave Company in 1994. QR code can transport the text, web link, and phone number. The QR code, Maxicode, Datamatrix code, and pdf417 are widely implemented in daily life. In fact, the QR code has six features like: high capacity encoding of data, small printout size, Chinese/Japanese (kanji and kana) capability, dirt and damage resistance, readable from any direction in 360°, and a structure append feature. The main advantage of a QR code is its versatility. QR codes can be used for anything and everything. They are also helpful for both customers and businesses. For example, a business saves money and advertising costs by distributing a QR code to their website or URL. A customer can scan this QR code and this allows them to store the information for future reference.

Today, 40 QR code versions are accessible with different storage capacities. The smallest QR code version (version V1) has a 21 × 21 module size. It can store 152 bits of raw data at the lowest correction level. The biggest QR code version (version V40) has a 177 × 177 module size. It can store a maximum of 7089 bits of raw data at its lowest correction level. A QR code encodes the information into binary form. Each information bit is represented by a black or a white module.

The error correction capability can reinstate the QR message if the QR code has damaged. QR code becomes popular and give widely business applications via the QR readers and mobile devices. The QR content, however, can be simply decoded by a QR reader. To transmit a QR code with the private information, the security of QR data raises an important problem. The sender usually stores the secret in a back-end database. Browsers can read the web link from the QR code and then connect to the website of the database. Only the authorized user with password can login and retrieve the secret. However, such manner requests that the QR reader needs to be online and exposes the risk of the database.

This paper, construct a new rich QR code with the help of image steganography approach. It has two levels public and private. The public level is similar to the any ideal QR code storage level; hence, it is readable by any ideal QR code reader**.** The private level is developed by hiding the black modules by number of textured pixels, which are fetched form textured patches. This textured patches extracted form cover image. This QR code useful for sharing the private message and verify the original message.

Steganography is the technique of hiding any type of digital media within another any type of digital media. Means steganography is the process of hiding private information in some faultless looking carrier digital file. This carrier digital file may be a text file, HTML, picture file like .bmp, an mp3 file or even a video file, the main point is,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

the insertion of the secret data should not affect the quality of the carrier file. So, the presence of content itself is invisible from the visible of the opponent. Not much mathematics involved here unlike in cryptography. So, cryptography involves the use of mathematics, number theory to hide message. But the secret code is visible to the enemy.

II. RELATED WORK

In [1] authors are consider a good authentication system using 2D-BCs from the point of visible of the opponent. An estimator that he can use to product a fake was proposed and its performance was derived through theoretical results and simulations on real printed and scanned 2D-BCs. While both the model and the tests conducted on real data agree on the general conclusion that Eve's estimation performance increases when collecting 2D-BCs, the slope of the curves, however, differs greatly. In [2] authors has presented a robust scheme to hide secret messages into QR code. The scheme is secure against bit-changed attack and can tolerate more errors than usual. However, the length of secret messages is smaller than the one using existing schemes based on bit algorithm. The algorithm purely uses Reed-Solomon codes to encode secret messages before embedding the outcome message into QR code. In [4] author's contribution in this paper is new, extensive work on modelling the changes that digital images undergo in the print-and-scan process. This paper propose a model for the pixel value distortion, define the RSC-based geometric distortions, analyse the change of DFT coefficients after geometric distortion, and describe methods to withdraw invariant feature vector. In [5] authors has designed secret hiding scheme can carry 24 to 9720 secret bits into a cover QR code and preserve the readability of the QR code content based on the capability of error correction. According to the simulation, the designed scheme is efficient to conceal the secret into a tiny QR barcode and satisfy the steganographic purpose. Only the authorized receiver with private key can successfully retrieve and decrypt the secret. In [7] authors has successfully demonstrated print-scan resilient data hiding methods with potential applications, such as document authentication and image copyright protection. In [9] authors has proposed a reversible steganographic algorithm using texture synthesis. Given a genuine source texture, the scheme can produce a large stego synthetic texture hiding secret messages.

III. PROPOSED SYSTEM

Proposed system based on to create new QR code with the combination of image steganography. The new QR code has two level public and private .Public level creation process is similar to the any ideal QR code creation process. Therefore, it is scan or read by any QR code reader or scanner. The QR code 2D barcode uses Reed Solomon algorithm to add error detection and correction information to input content. The content is represented series of values between 0 and 255(i.e. 8 bit bytes). The encoder add a series of parity bytes.

The private level created by adding pixels on block box and white box. Means, all QR code area is hide by pixels. The pixels are extracted by cover image patches and patches fetched from cover image. The private level created with the help of image steganography using texture synthesis technique. Steganography is the hiding of a digital media (like file, message, image, or video) within another digital media (like file, message, image, or video).Texture synthesis is the operation of filling holes in picture pictures as like inpainting, create a large unique picture and expand small pictures.

There are two method of texture synthesis Pixel and Patch-based texture synthesis. A patch represents a picture block of a source texture where its size is user-defined. This patches fetched from cover pictures. Pixel-based algorithms generate the synthesized image pixel by pixel. This pixels are extracted by cover image patches. The attacker does not attack on QR code because all block and white modules hide by pixels. So they does not add extra bit in QR code to change meaning of secrete message. The new QR code designed for secrete information sharing.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

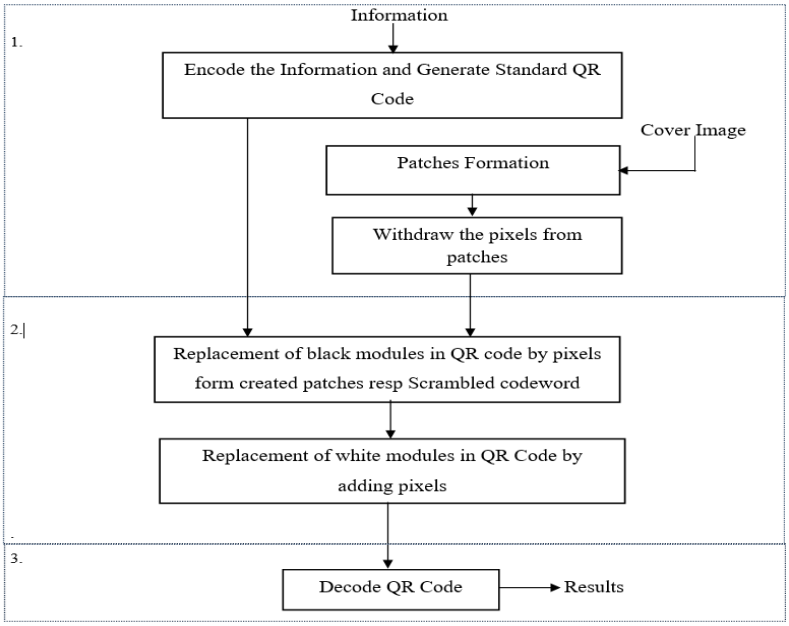

Figure 1: Proposed System Architecture

In above figure 1, block 1 has created one standard QR code. The private message store in this QR code which in encoded form. The Patches Formation module extract number of patches form cover image. In block 2, black and white modules in Standard QR code are replaced by number of pixels which are fetches form patches. Then QR coded hide by cover image. The block 3 make decode process of QR code.

IV. PROPOSED SYSTEM ALGORITHM

A. The standard QR code generation algorithm includes the following steps:

1. First of all, the most optimal mode (numeric, alphanumeric, byte or Kanji) is selected by analyzing the message content.
2. The message contentis encoded using the shortest possible string of bits. This string of bits is split up into 8 bit long data codewords.
3. Then, the choice of error correction level is performed and the error correction codewords using the Reed-Solomon code are generated.
4. After that, the data and error correction codewords are arranged in the correct order. In order to be sure that the generated QR code can be read correctly, the best (for encoded data) mask pattern is applied.
5. After this manipulation, the codewords are placed in a matrix in a zigzag pattern, starting from the bottom-right corner.
6. The final step is to add the function patterns (position tags, alignment, timing, format and version patterns) into the QR code.

V. RESULTS

Proposed system is being implemented module wise:

1. **Hiding secret information (Bank details) in QR image and select .png image for encrypt the QR code.** Zxing library is used to conceal the message in QR code.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

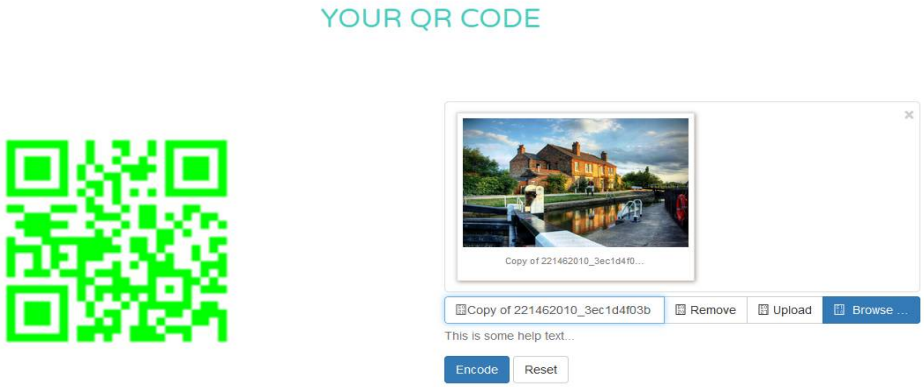

Fig 3: Hiding secret message in QR code.

This module generate a standard QR code which hides private information (Bank details).The private information's are in the encrypted form and this encrypted data stored in Standard QR code. Then select one .png image from browser for encrypt that Standard QR code. This encrypted QR code does not read by any QR code reader.

2. Display Encrypted QR code Image

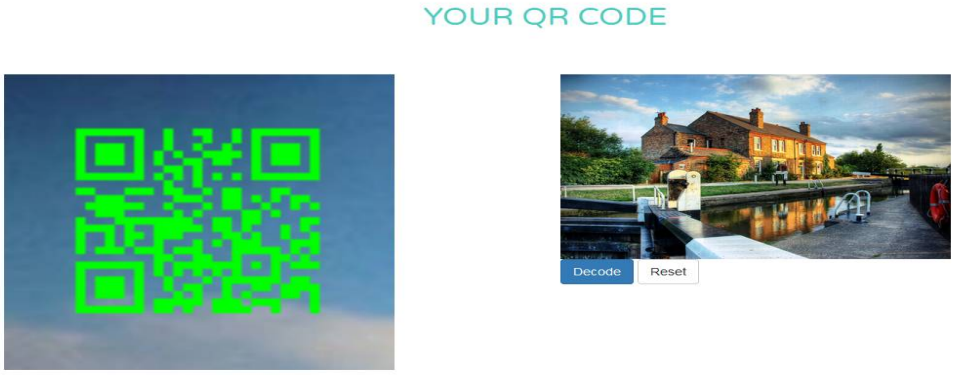

Fig 4: Encrypted QR Code.

This module Display the encrypted QR code Image which is does not read by QR code reader. This module also give the button for decode the encrypted QR code image.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

3. Display Decrpyted QR Code information

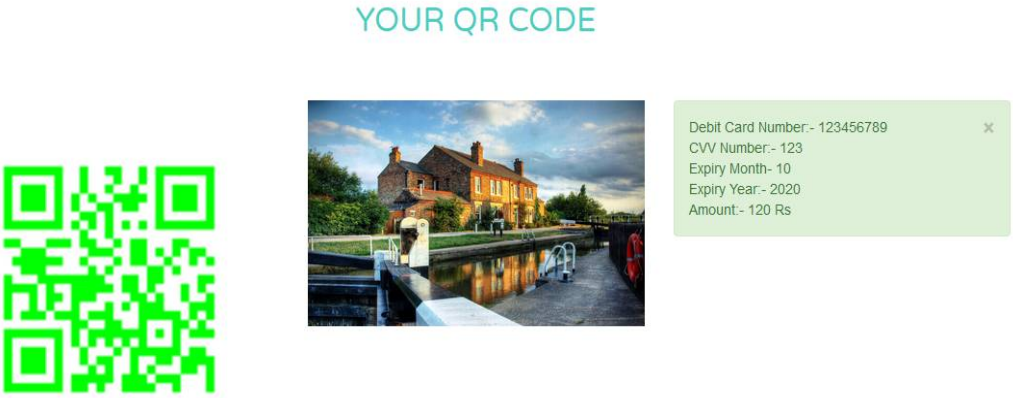

Fig 5: Decrpyted QR Code

This module decrypt the encryped QR coed image, and display private information. This private information storded in encryper form.

VI. EXPECTED RESULTS

Accuracy Range:

Proposed application designed to implement secret information security. This information is concealed using QR image. Furthermore, QR image is composed with patches retrieved from cover image. This measure is used to verify system assure authentication of user information.

Precision and Recall:

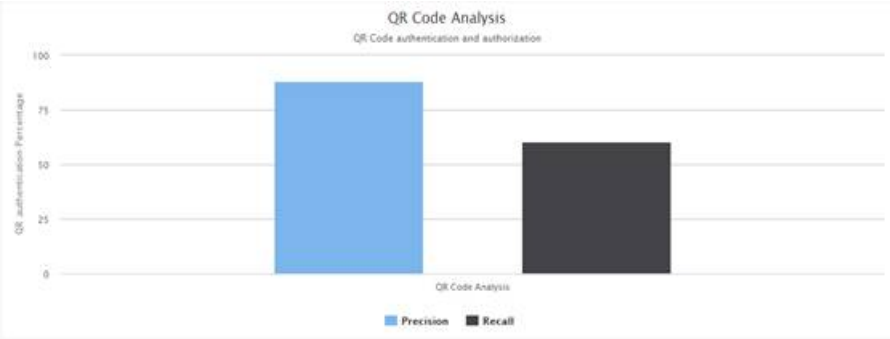

Fig 6:Precision and Recall.

Above bar chart display the result of QR code analysis.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Overhead for QR code encryption and decryption in two level QR Code authentication:

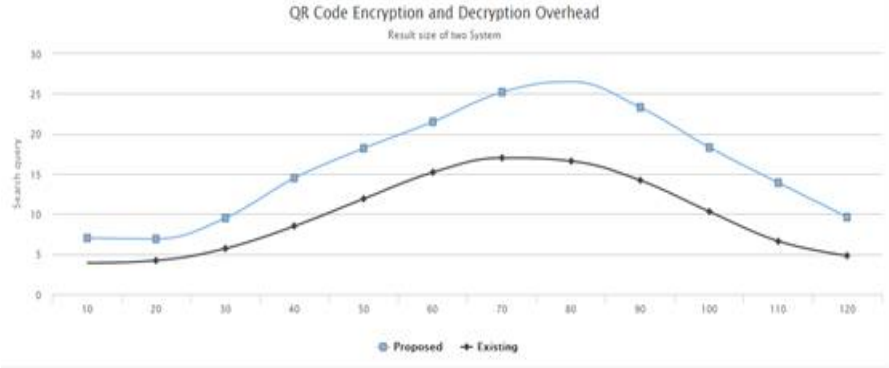

Fig 7: QR Code Encryption and Decryption Overhead.

Above graph display the result of QR code encryption and decryption overhead in QR code authentication.

VII. CONCLUSION AND FUTURE WORK

QR codes can be used for various applications such as business, marketing, education, data security, authentication etc. This paper introduce a new QR code with the combination of image steganography for data security. The new QR code has two level public and private. In public level message encryption process is similar to the any ideal QR code encryption process. The private level created by adding pixels on block box and white box. Means, all QR code area is hide by pixels. The pixels are extracted by cover image patches and patches fetched from cover image. The private level created with the help of image steganography using texture synthesis technique. So this novel QR code enhances the confidentiality and security for secrete message sharing.

REFERENCES

1. C. Baras and F. Cayre, "2D bar-codes for authentication: A security approach," in Proc. 20th Eur. Signal Process. Conf. (EUSIPCO), Aug. 2012, pp. 1760–1766.
2. T. V. Bui, N. K. Vu, T. T. P. Nguyen, I. Echizen, and T. D. Nguyen, "Robust message hiding for QR code," in Proc. IEEE 10th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIH-MSP), Aug. 2014, pp. 520–523.
3. T. Langlotz and O. Bimber, "Unsynchronized 4D barcodes," in Proc. 3rd Int. Symp., ISVC 2007, Lake Tahoe, NV, USA, Nov. 26–28, 2007, pp. 363–374.
4. C.-Y. Lin and S.-F. Chang, "Distortion modeling and invariant extraction for digital image print-and-scan process," in Proc. Int. Symp. Multimedia Inf. Process., 1999, pp. 1–10.
5. P.-Y. Lin, Y.-H. Chen, E. J.-L. Lu, and P.-J. Chen, "Secret hiding mechanism using QR barcode," in Proc. IEEE Int. Conf. Signal-Image Technol. Internet-Based Syst. (SITIS), Dec. 2013, pp. 22–25.
6. M. Querini, A. Grillo, A. Lentini, and G. F. Italiano, "2D color barcodes for mobile phones," Int. J. Comput. Sci. Appl., vol. 8, no. 1, pp. 136–155, 2011.
7. K. Solanki, U. Madhow, B. S. Manjunath, S. Chandrasekaran, and I. El-Khalil, "'Print and scan' resilient data hiding in images," IEEE Trans. Inf. Forensics Security, vol. 1, no. 4, pp. 464–478,Dec. 2006.
8. R. Villán, S. Voloshynovskiy, O. Koval, F. Deguillaume, and T. Pun, "Tamper-proofing of electronic and printed text documents via robust hashing and data-hiding," in Proc. SPIE, vol. 6505, p. 65051T, Feb. 2007.
9. Kuo-Chen Wu and Chung-Ming Wang, *Member, IEEE*, "Steganography Using Reversible Texture Synthesis", Ieee Transactions On Image Processing Vol: 24 No: 1 Year 2015
10. S. V. Voloshynovskiy, O. Koval, F. Deguillaume, and T. Pun, "Visual communications with side information via distributed printing channels: Extended multimedia and security perspectives," Proc. SPIE, vol. 5306, pp. 428–445, Jun. 2004.

BIOGRAPHY

Bhakti Magadumis a M.E Student in the Computer Engineering Department, Smt. KashibaiNawale College of Engineering, Savitribai Phule Pune University, Pune, and Maharashtra, India. She received Bachelor of Computer Science and Engineering (BE) degree in 2015.