

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Two Level QR Code Authentication Using Image Encoding Technique

Tahemeena Gunjarge, Kailas Tambe

ME Student, Department of Computer Engineering, ZCOER, Narhe, Pune, India

Professor, Department of Computer Engineering, ZCOER, Narhe, Pune, India

ABSTRACT: The quick response (QR) code was designed for storage information and high-speed reading applications. In proposed QR code authentication two level storage is used, which help to verify original content in QR code. Our proposed work uses public and private storage level of document storage. In the public level same standard QR code storage level is explored; which can be readable to any QR code readable device. The private level is constructed by replacing the black modules by specific textured patches from cover image. It consists of information encoded using q -ary code with an error correction capacity. Q -array code will increase the storage capacity of the QR code, but also to verify the original document from a copy. This authentication is due to the sensitivity of the used patches to the print-and-scan process. steganalysis algorithm is not likely to defeat our steganographic approach. Third, the reversible capability inherited from our scheme provides functionality which allows recovery of the source texture. We weave texture synthesis process into steganography for hiding secret in image.

KEYWORDS: QR code, two storage levels, private message, print-and-scan, Data embedding, encoding, decoding.

1. INTRODUCTION

To protect the secret message or data in QR code, QR tag and be decoded by a standard QR code reader is used directly; proposed work has designed a QR code steganography approach based on the property of QR standard in this article. To improve the hiding capacity, this system proposed a new information hiding method for QR codes by using the concept of EMD scheme. The proposed scheme can conceal higher payload of the confidential data into a QR tag by modifying the QR modules directly. The QR data of the generated marked QR tag, especially, is readable. That is, one can use the barcodereader to exhibit the QR data, such as the URL. The ability of exhibiting the QR data from the marked QR tag can reduce the suspicions of attackers and intruders. Only the authorized user can further extract the confidential secret from the same generated QR tag via barcode reader. The designed approach can satisfy the essentials of steganography, secret protection and feasibility for low power barcode readers and mobile devices. QR code has a specific structure for geometrical correction and high speed decoding. Three position tags are used for QR code detection and orientation correction. One or more alignment patterns are used to code deformation adjustment. The module coordinates are set by timing patterns. Furthermore, the format information areas contain error correction level and mask pattern. The code version and error correction bits are stored in the version information areas.

The popularity of QR codes is mainly due to the following features:

- QR code robust to the copying process,
- It is easy to read by any device and any user,
- It has high encoding capacity enhanced by error correction facilities,
- It is in small size and robust to geometrical distortion.

However, those undeniable advantages also have their counterparts:

1. Information encoded in a QR code is accessible to every user easily, even if it is encoded.
2. It is difficult to classify original content from duplicate file content due to print and scan feature.
3. It is impossible to distinguish an originally printed QR code from its copy due to their insensitivity to the Print-and-Scan (P&S) process

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

The proposed two levels QR (2LQR) code contains of: a first level accessible for any standard QR code reader, therefore it keeps the strong characteristics of the QR code; and a second level that improves the capacities and characteristics of the initial QR code. The information in the second level is encoded by using q -ary ($q \geq 2$) code with error correction capacities. This information is invisible to the standard QR code reader because it perceives the textured patches as black modules. Therefore, the second level can be used for private message sharing. Additionally, thanks to textured patches sensitivity to P&S distortions, the second level can be used to distinguish the original 2LQR code from its copies. The Reed-Solomon error correction code is used for data encryption. Therefore, one of 4 error correction levels has to be chosen during QR code generation.

II. REVIEW OF LITERATURE

In this paper this system we refer the authentication problem of real-world goods on which 2D bar-codes (2D-BC) were printed and we take the competitors view. The competitors are assumed to have access to noisy copies of an original 2D-BC. A simple estimator of the 2D-BC is depends on copies averages is proposed, letting the competitors print a fake 2DBC with as original by the system identifier. Performance of the of the proposed system in terms of error probability at the detector side is then derived with respect to N_c and compared with experimental results on real 2D-BC. It is implemented that the opponent can create a fake identity that successfully fools the QR code detector with a reasonable number of genuine goods [1]. Storing secret data based on bit technique is so yield to changes to original QR tag attack. If an attacker change any bit of hidden information, it is not possible to regain the secret data. So from this paper, we refer a scheme based on Reed- Solomon codes and List of Decoding mechanism to avoid this problem. We also implements our solution by manipulating the complexity, security, and experiment [2]. A Proposed method gives optical data transfer between public displays and mobile devices based on unsynchronized 4D barcodes. We consider that no direct connection between the devices can exist. Time-multiplexed, 2D color barcodes are displayed on screens and recorded with camera equipped mobile phones. This allows transmitting information optically between both devices [3]. We show properties of the discredited, rescanned image in both the spatial and frequency domains, and then further analyzes the changes in the Discrete Fourier Transform (DFT) coefficients. Based on these properties, we show several techniques for extracting different from the original and scanned images, with potential applications in image watermarking and authentication [4]. We designed a secret hiding technique for QR barcode. The proposed techniques can conceal the important information into the cover QR code without distorting the readability of QR content. That is, general browsers can read the QR content from the marked QR code to reduce attention. Only the authorized receiver can encrypt and retrieve the secret from the marked QR code. The secret payload of the designed scheme is adjustable. The scheme state that the larger secret into a QR code as per to the selection of the QR version and the error correction level [5]. We used high capacity color barcode, which use colors to increase the barcode data density. The identification and recognition of colored modules creates some new and non trivial QR Code vision challenges, such as implementing the color distortions discovered by the hardware equipment that identifies the Print & Scan process [6]. This paper proposes methods to hide information into images that achieve robustness against printing and scanning with blind decoding. The selective embedding in low frequencies scheme conceals data in the magnitude of selected low level discrete Fourier transform coefficients. The differential quantization index modulation scheme embeds information in the phase spectrum of QR codes images by dividing the difference in phase of adjacent frequency locations. A significant contribution of this paper is analytical and experimental modeling of the print-scan process, which forms the basis of the proposed embedding schemes [8]. We propose a novel approach for steganography using a reversible texture synthesis. A texture synthesis process re-samples a little textured image which finds a new texture image with a similar local appearance and arbitrary size. We weave the texture synthesis process into steganography to conceal secret messages. In contrast to using an existing cover image to hide secret messages, proposed algorithm hides the source texture image and embeds secret messages through the process of texture synthesis. This permits user to extract secret data and the source texture from a stego synthetic texture [9]. In this survey, we manage with the problem of authentication and tamper proofing of text documents that can be distributed in electronic or printed forms. We advocate the combination of robust text hashing and text data-hiding technologies as an efficient solution to this problem. First, we consider the problem of text data-hiding in the scope of the Gel'fand-Pinsker data-hiding framework. For illustration, two modern text data-hiding methods, namely color index modulation (CIM) and location index modulation (LIM), are explained. Second, we study two approaches to robust text hashing that are well suited for the

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

considered problem. In particular, both approaches are compatible with CIM and LIM. The first approach makes use of optical character recognition (OCR) and a classical cryptographic message authentication code (MAC). The second approach is new and can be used in some scenarios where OCR does not produce consistent results [10].

III. SYSTEM ARCHITECTURE

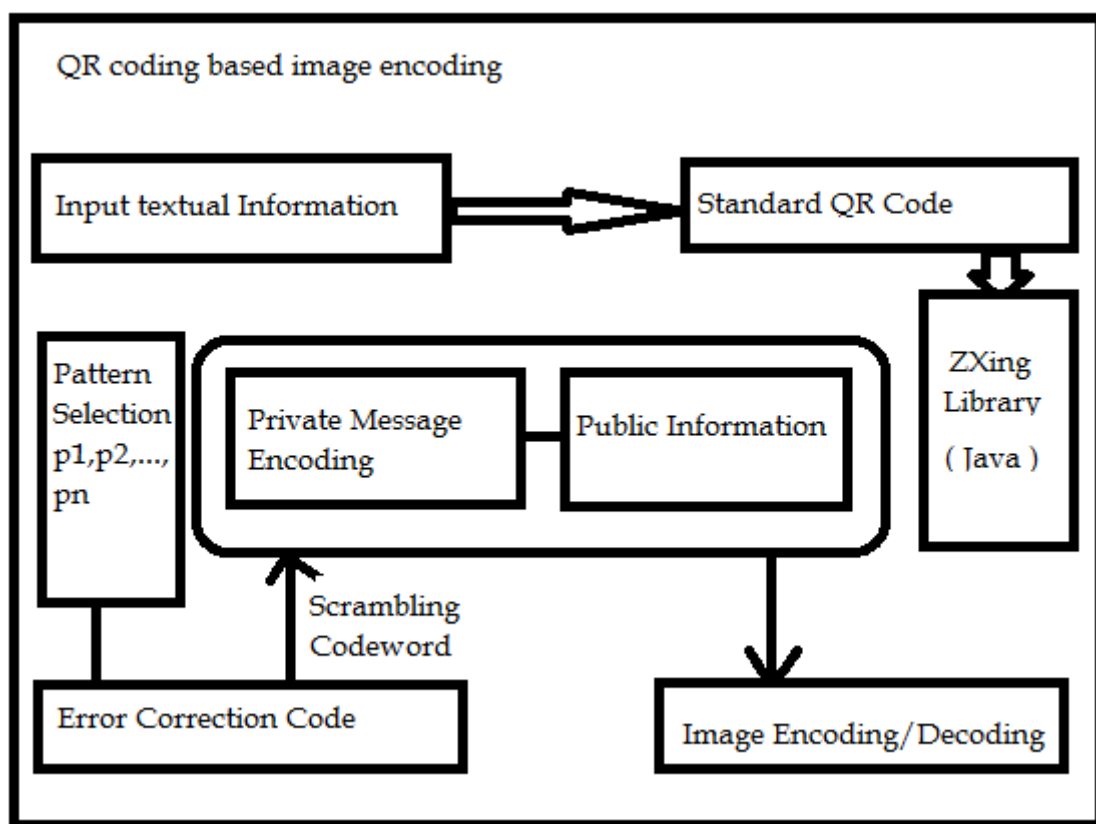


Fig.1:QR code authentication using image encoding mechanism.

The primary problem is to implement an efficient, robust, scalable, and easy to use authentication system. We present and analyze the authentication scheme that combines ownership factors (original content and authentication code) with knowledge factors. The method is based on smart card and optical challenge response solution in which a camera equipped mobile phone is used for the purpose of authentication. The security of the scheme is improved by using a type of knowledge-based authentication challenge to the user's smart phone rather than a code displayed in clear text. This solution has high usability due to its ease of use, easy deployment and cost effectiveness.

IV. SYSTEM OVERVIEW

Proposed system uses two levels QR for data hiding. This 2LQR code has following levels

1. Public level
2. Private level.

The public level QR code can read text or document easily with reader, but the private level needs a specific device with encoded information. This 2LQR code can be used for private message sharing or for authentication mechanism. The private level is created by replacing black modules with textured patches from cover image. These

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

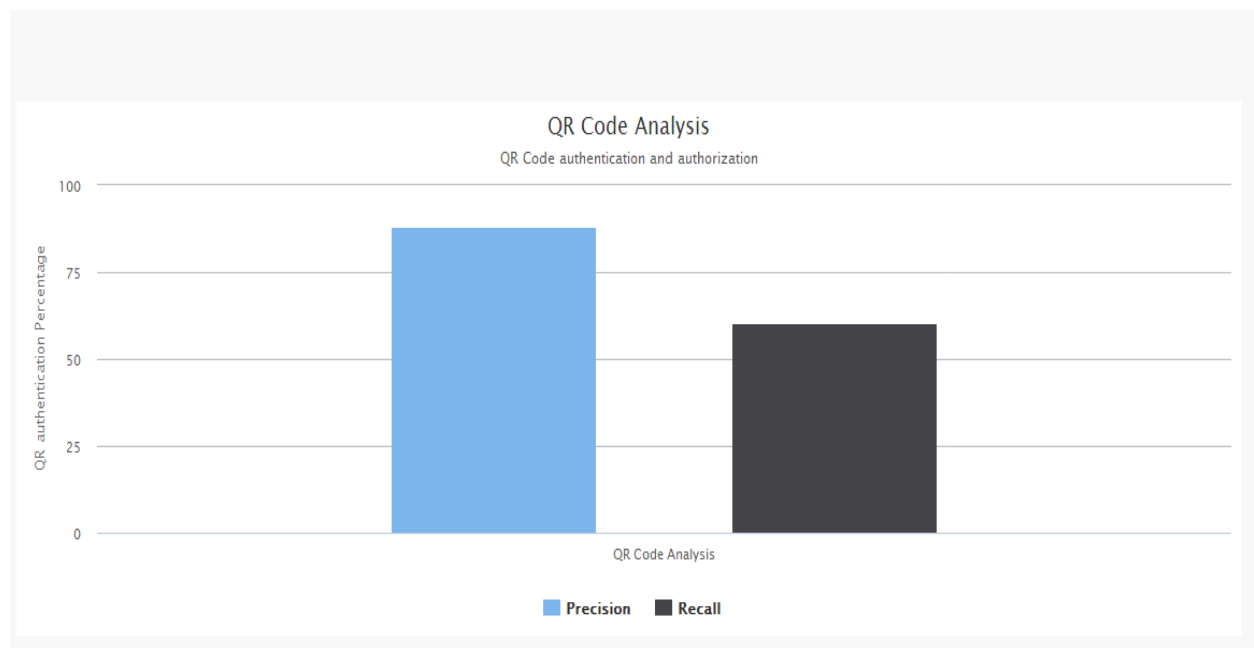
Vol. 6, Issue 7, July 2017

textured patches are considered as black modules by standard QR code reader. So that private level is hidden to QR code readers, Proposed system for private level does not affect in anyway the scanning public data of the public level. The proposed 2LQR code increases the storage capacity of the classical QR code due to its supplementary reading level. The storage capacity of the 2LQR code can be improved by increasing the number of textured patches used or by decreasing the textured patches size. Cover image to hide messages, our algorithm hide the source texture image and embeds secret messages through the process of texture synthesis. This allows us to extract secret messages and the source texture from a stego synthetic texture.

V. EXPERIMENTAL RESULT

1. QR Analysis

QR code analysis with precision shows encoding and recall shows decoding accuracy level. Precision shows QR image encoding uses patches for encryption and Recall is based on index table for cover images patch entries.



2. QR Code authentication Level

Following graph shows QR code analysis for the online recharge system. This graph shows message encoding capacity in QR code image i.e. QR code data encoding scheme to QR image.

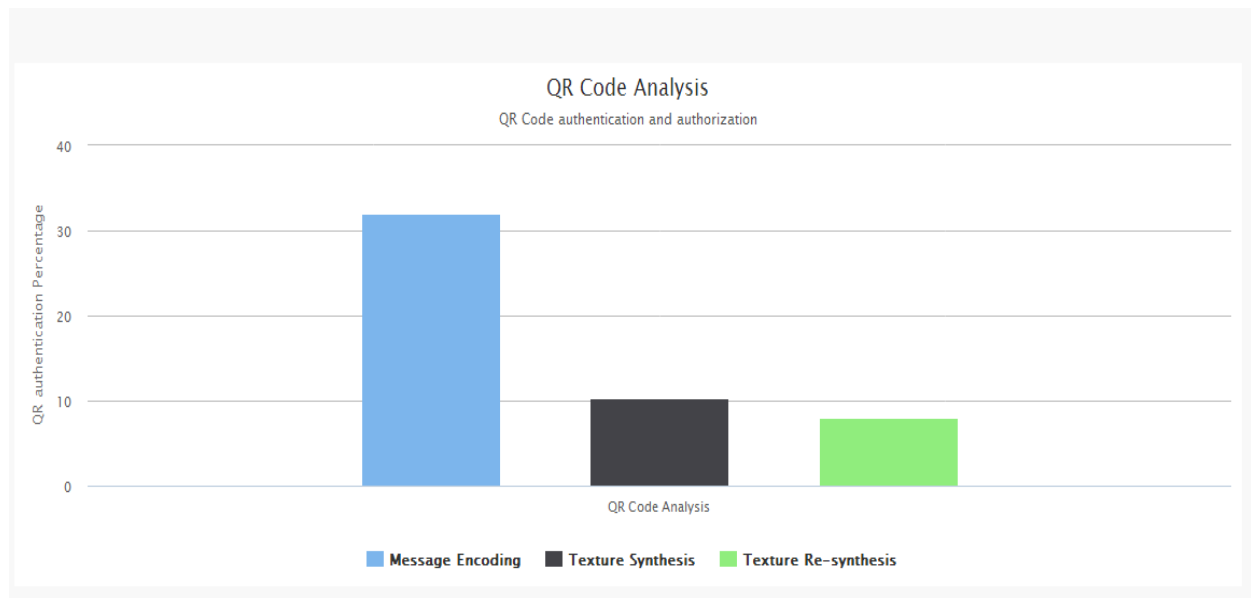
1. Texture Synthesis process shows patches extraction level from cover image for being used as texture pattern for overlapping QR image.
2. Texture re synthesis shows that QR code decoding by reversible texture on cover image by image authentication.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017



VI. CONCLUSION

This 2LQR code can be used for secure private data sharing for authentication mechanism. The private level is created by replacing black modules with specific textured pattern. So that the private level is hidden to QR code readers, we add the private level which does not affect in anyway the reading process of the public level. The proposed 2LQR code increases the storage capacity of the classical QR code due to its supplementary reading level. Proposed system improves standard QR code security by image encoding techniques maintains the readability of the QR code content because of error correction capability. According to the experimental analysis, the designed scheme is feasible to hide the secrets into a tiny QR barcode as the purpose of steganography. Only the author who has private key can successfully obtain the hidden secrets.

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. 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.
10. 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.