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 6, June 2017

A Survey on Two Level QR Code Authentication Using Image Encoding Technique

Tahemeena Gunjarge, Kailas Tambe

M. E Student, Department of Computer Engineering, ZCOER, Narhe, Pune, India

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

ABSTRACT: The QR code was intended for capacity data and rapid perusing applications. In proposed QR code verification two level stockpiling is utilized, which help to confirm unique substance in QR code. Our proposed work utilizes open and private stockpiling level of record stockpiling. In general society level same standard QR code stockpiling level is investigated; which can be decipherable to any QR cod lucid gadget. The private level is developed by supplanting the dark modules by particular finished patches frame cover picture. It comprises of data encoded utilizing q-ary code with a mistake revision limit. Q-cluster code will build the capacity limit of the QR code, yet in addition to confirm the first report from a duplicate. This verification is because of the affectability of the utilized patches to the print-and-output process. Steganalysis calculation is not liable to overcome our steganographic approach. Third, the reversible ability acquired from our plan gives usefulness which permits recuperation of the source surface. We mesh surface blend process into steganography for concealing mystery in picture.

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

1. INTRODUCTION

To secure the mystery message or information in QR code, QR tag and be decoded by a standard QR code peruser is utilized straightforwardly; proposed work has composed a QR code steganography approach in view of the property of QR standard in this article. To enhance the concealing limit, this framework proposed another data concealing technique for QR codes by utilizing the idea of EMD plot. The proposed plan can disguise higher payload of the classified information into a QR tag by adjusting the QR modules straightforwardly. The QR information of the created checked QR tag, particularly, is intelligible. That is, one can utilize the scanner tag peruser to show the QR information, for example, the URL. The capacity of showing the QR information from the stamped QR tag can lessen the doubts of aggressors and gatecrashers. Just the approved client can additionally extricate the classified mystery from the same produced QR tag by means of standardized identification peruser. The composed approach can fulfill the basics of steganography, mystery insurance and practicality for low power standardized identification perusers and cell phones. QR code has a particular structure for geometrical redress and fast deciphering. Three position labels are utilized for QR code discovery and introduction rectification. At least one arrangement designs are utilized to code disfigurement modification. The module arranges are set by timing designs. Moreover, the arrangement data zones contain blunder amendment level and cover design. The code adaptation and mistake redress bits are put away in the variant data regions.

The ubiquity of QR codes is fundamentally because of the accompanying elements:
•QR code powerful to the replicating procedure,
•It is anything but difficult to peruse by any gadget and any client,
•It has high encoding limit improved by blunder adjustment offices,
•It is in little size and hearty to geometrical contortion.
Be that as it may, those irrefutable preferences likewise have their partners:

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 6, June 2017

1.Information encoded in a QR code is open to each client effortlessly, regardless of the possibility that it is encoded.
2.It is hard to arrange unique substance from copy document content because of print and sweep highlight.

3.It is difficult to recognize an initially printed QR code from its duplicate because of their lack of care to the Print-and-Scan (P&S) process

The proposed two levels QR (2LQR) code contains of: a first level open for any standard QR code peruser, subsequently it keeps the solid attributes of the QR code; and a moment level that enhances the limits and qualities of the underlying QR code. The data in the second level is encoded by utilizing q−ary ($q \geq 2$) code with mistake remedy limits. This data is imperceptible to the standard QR code peruser in light of the fact that it sees the finished fixes as dark modules. Accordingly, the second level can be utilized for private message sharing. Furthermore, on account of finished patches affectability to P&S bends, the second level can be utilized to recognize the first 2LQR code from its duplicates. The Reed-Solomon mistake adjustment code is utilized for information encryption. Subsequently, one of 4 blunder revision levels must be picked amid QR code era.

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 Nc 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

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 6, June 2017

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 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

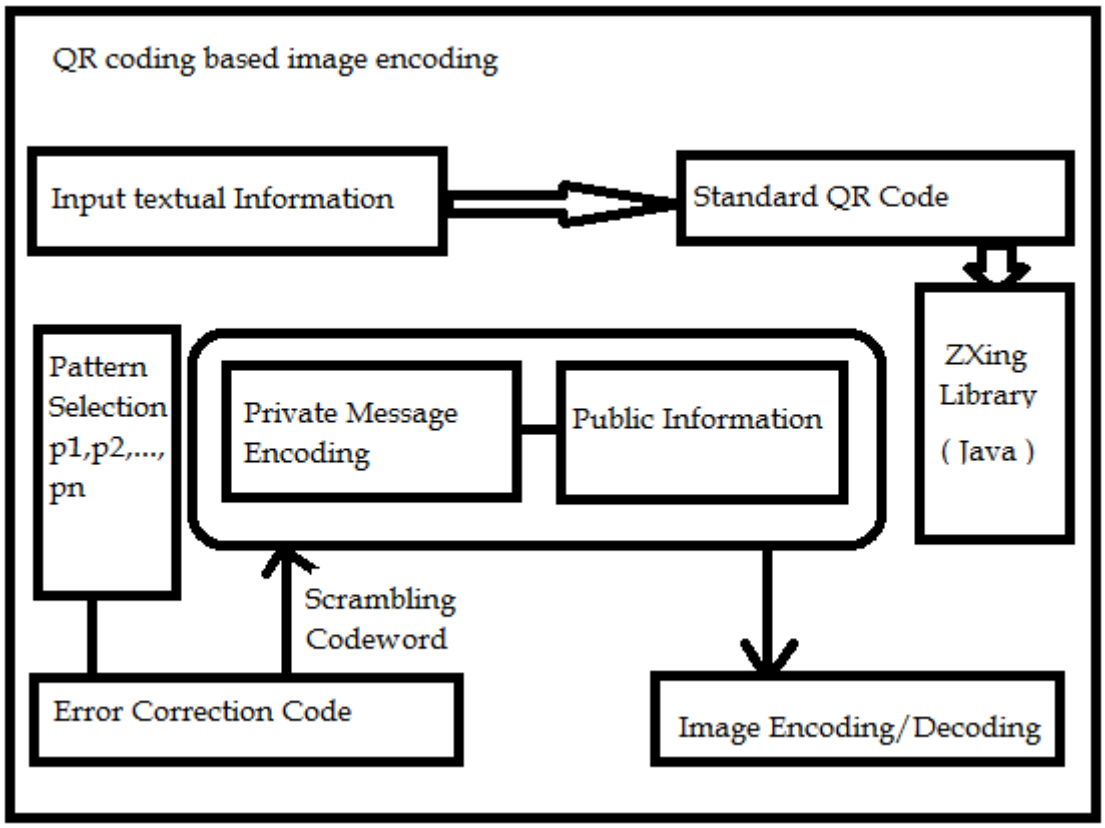

Fig.1:QR code authentication using image encoding mechanism.

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.

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 6, June 2017

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 textured patches are considered as black modules by standard QR code reader. So that private level is hidden to QR code readers, Propose 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. 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.