Two-Level QR Code for Secured Message Sharing and Document Authentication

Shreya V. Uttarwar[1], Dr. A. M. Bagade[2]

Student, IT Dept, PICT, Pune, India[1]

Associate Professor, IT Dept, PICT, Pune, India[2]

Abstract: The quick response (QR) code was designed for storage information and high-speed reading applications. QR codes are used to create a link between the real world products (tagged with the QR code) and the Internet. A new rich QR code is proposed that has two storage levels: a public level and a private level. The public level can be read by any QR code reading application, while the private level is constructed by replacing the black modules by specific textured patterns. These patterns, do not introduce disruption in the standard reading process and always perceived as black modules by any QR code reader. Thus the private level is invisible to standard QR code readers. It can also be used for document authentication. It consists of information encoded using q-ary code with an error correction capacity which helps to increase the storage capacity of the QR code and to determine the original document from a copy. The sensitivity of the used patterns to the print-and-scan (P&S) process represents this authentication. The pattern recognition method can be used both in a private message sharing and in an authentication scenario. The storage capacity can be notably enhanced by increasing the code alphabet q or by increasing the textured pattern size.

Keywords: Quick Response (QR), two-storage level, Message Sharing, Document Authentication.

I. INTRODUCTION

The QR code was invented for the Japanese automotive industry by Denso Wave Corporation in 1994. The most important characteristics of this code are small printout size and high speed reading process. A QR code encodes the information into binary form. QR code contains black squares organized in a rectangular grid on a white background, which can be read by an imaging device such as a camera. The desired data are extracted from patterns which can be present in both horizontal and vertical components of the image. The QR code has a detailed structure for geometrical correct ion 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. Moreover, the layout information areas include error correction stage and masks pattern. The code version and error correction bits are stored in the version information areas [1].
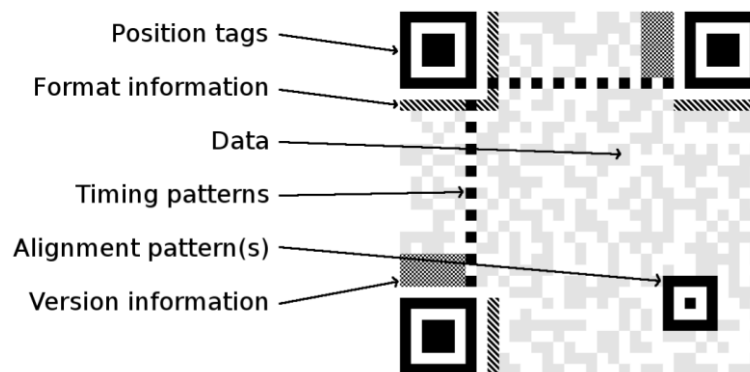

Fig. 1.1 Specific QR code structure consists of position tags, alignment patterns, timing patterns, format information and version information patterns [1].

II. RELATED WORK

According to Zachi Baharav and Ramakrishna Kakarala in "Visually Significant Qr Codes: Image Blending And Statistical Analysis", QR codes are largely used as a means of conveying textual information, such as emails, hyperlinks, or phone numbers, through images which are interpreted using a smartphone camera. This paper indicates how the visually massive QR codes could also be obtained by image blending. This procedure allows images as diverse

as corporate logos and family photographs to be embedded in the code in full color. The purpose of this paper is to describe a statistically analyzed method for blending color images into a QR code to improve its visual significance [2].

Cléo Baras and François Cayre in "2d Bar-Codes for Authentication: A Security Approach" investigates the authentication crisis of actual-world goods on which 2nd bar-codes (2D-BC) were printed and takes the opponent's factor of view. The opponent is assumed to have access to Nc noisy copies of a genuine 2D-BC. A simple estimator of the 2D-BC based on copies averages is proposed, allowing the opponent print a fake 2DBC which aims at being declared as genuine by the system detector. It is proven that the opponent can produce a fake copies that successfully fools the detector with a reasonable number of genuine goods. In this context, an opponent aims at producing a fake 2D-BCs declared as genuine by the detector, whereas the aim of the product manufacturer is to make such a reproduction difficult or impossible. This problem is tackled with a security approach inspired by works in digital watermarking [3].

Anh Thu Phan Ho, Bao An Mai Hoang, Wadih Sawaya and Patrick Bas proposes "Document authentication using graphical codes: reliable performance analysis and channel optimization" to investigate the impact of the channel model for authentication systems based on codes that are corrupted by a physically unclonable noise such as the one emitted by a printing process. The goal of this paper is twofold, firstly, it provides reliable performance measurements of the authentication system based on a Neyman-Pearson hypothesis test. Secondly, the computation of type I and type II errors are used to derive the most favorable channels for authentication [4].

According to Thach V. Bui, Nguyen K. Vu, Thong T.P. Nguyen, Isao Echizen and Thuc D. Nguyen in "Robust Message Hiding for QR Code", To preserve the original content of QR code and embed secret information into it are the two main challenges. Hiding secret information based on it technique is so fragile to modification attack. If an attacker change any bit of hidden bits, it becomes very difficult or impossible to recover the secret information. This paper proposes a scheme to overcome this problem. The main objective 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 [5].

III. PROPOSED ALGORITHM

A rich QR code with a public level and a private level is discussed in this section. Two application scenarios for 2LQR code can be suggested: a private message sharing scenario and an authentication scenario. The main purpose of a private message sharing scenario is the invisible storage and transmission of private information into QR code. In a printed document authentication scenario, QR code aim to verify whether the printed document is an original or a copy. Only the original document (printed by authorities) is considered as an authentic.

- **Public message Mpub:**
The public message Mpub is stored in the standard QR code. The standard QR code generation algorithm includes the following steps.

First of all, the most optimal mode (numeric, alphanumeric, byte or Kanji) is selected by analyzing the message content. The message Mpub is encoded using the shortest possible string of bits. This string of bits is split up into 8 bit long data codewords. Then, the choice of error correction level is performed and the error correction codewords using the Reed-Solomon code are generated.

- **Private message Mpriv:**
The proposed two level 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.
For Private message Mpriv encoding, the private row-bit string is encoded using error correction code (ECC) to ensure the message error correction after the P&S operation. It uses the block codes, for message encoding.

Various shortcomings can be overcome by enriching the standard QR code encoding capacity. This enrichment is obtained by replacing its black modules by specific textured patterns. Besides the gain of storage capacity, these patterns can be designed to be sensitive to distortions due to the P&S process. That do not introduce disruption in the standard reading process, are always perceived as black modules by any QR code reader. Therefore, even when the private information is degraded or lost in the copy, the public information is always accessible for reading.

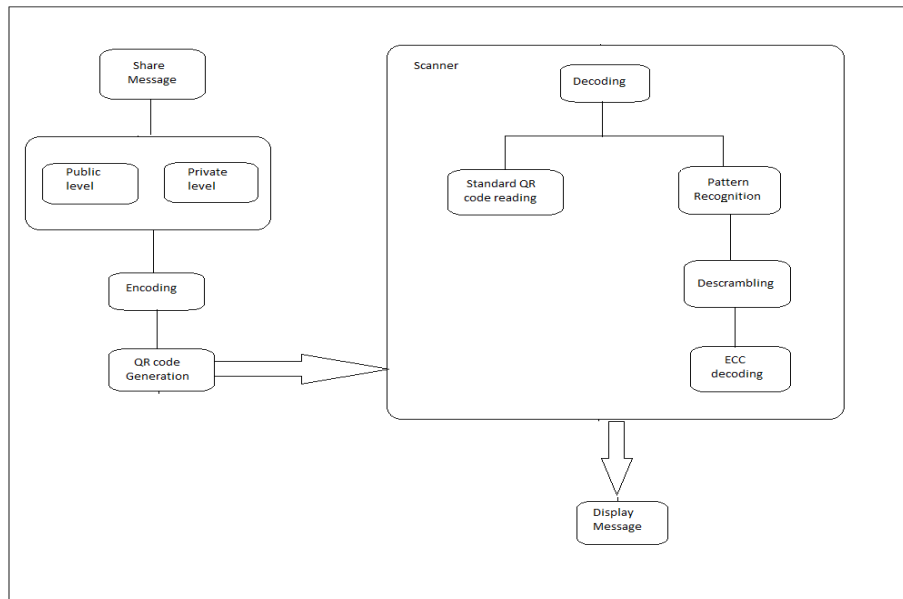The architecture diagram for message sharing can be shown as follows:

Fig 1: Architecture of Message Sharing

- **Document Authentication:**

The advent of the digital age with the Internet revolution has made it extremely convenient for users to access, create, process, copy, or exchange multimedia data. This has created an urgent need for protecting intellectual property in both the digital and the print media. The proposed 2LQR code for document tampers proofing. In addition, due to the specific characteristics of the used textured patterns, the original 2LQR code can be distinguished from one of its copies to ensure document authentication. This functionality has been performed due to the impact of the P&S process, that can be considered as physically unclonable because of both the deficiencies of the physical process and the stochastic nature of the matter [7]. The architecture diagram for message sharing can be shown as follows:
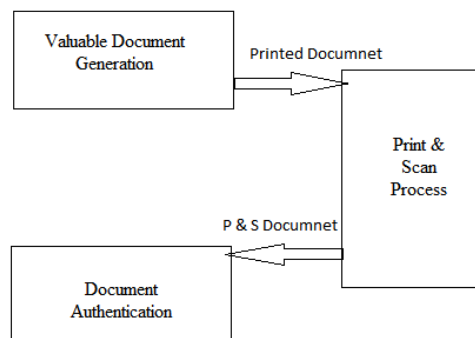

Fig. 2 : Architecture of Document Authentication

- **Two Level QR (2LQR) Code Generation:**

Like the standard QR code, the 2LQR code has the same specific structure, which consists of position tags, alignment patterns, timing patterns, version and format patterns. However, the standard QR code have white and black modules and the 2LQR code have white modules and textured modules instead of black modules. This replacement of black modules by textured modules does not disrupt the standard QR code reading process. But it allows us to have a second storage level, which is invisible to the standard QR code reader. This second level contains the private message, encoded with q-ary ($q \geq 2$) code with error correction capacity. The standard QR code has have white and black modules and the 2LQR code have white modules and textured modules instead of black modules. This replacement of black modules by textured modules does not disrupt the standard QR code reading process. But it allows us to have a second storage level, which is invisible to the standard QR code reader. This second level contains the private message, en with query code with error correction capacity. These textured patterns have specific features and are used for private message private storage in the proposed 2LQR code. In private message sharing scenario, the black modules of these pattern are also replaced by textured patterns.

As shown in Fig.3.3 the input information is the public message, Mpub and the private message Mpriv [1].
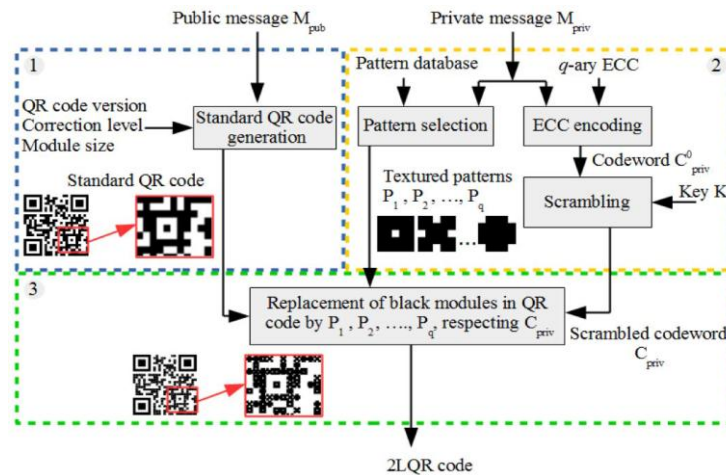

Fig. 3. Overview of 2LQR code generation steps [1]

IV. APPLICATIONS

The quick response (QR) code was designed for storage information and high-speed reading applications. QR codes have come a long way since their creation. Today it have a number of purposes, including transport ticketing, entertainment, commercial tracking, and product labeling/marketing. QR codes being used to send audiences to a website for browsing, to bookmark a webpage, to initiate phone calls, send short messages, send emails, produce links to web URL's, connect to WI-FI networks, access information, get coupons, view videos, purchase items, process orders, advertise products, etc. Application scenarios for 2LQR code are mainly focused on: a private message sharing scenario and an authentication scenario. The main purpose of a private message sharing scenario is the invisible storage and transmission of private information into QR code. In a printed document authentication scenario, it aims to verify whether the printed document is an original or a copy.

V. CONCLUSION AND FUTURE WORK

In this paper a new rich code called two level QR (2LQR) code is proposed. This 2LQR code has two levels: a public level and a private level. The public level can be read by any QR code reading application, while the private level needs a specific application with specific input information. This 2LQR code can be used for private message sharing or for authentication scenarios. The private level is created by replacing black modules with specific textured patterns. These textured patterns are considered as black modules by standard QR code reader. Thus the private level is invisible to standard QR code readers. In addition, the private level does not affect in anyway the reading process of public level.

REFERENCES

1. I. Tkachenko, W. Puech, C. Destruel, O. Strauss, J. Gaudin and C. Guichard, "Two-Level QR Code for Private Message Sharing and Document Authentication", IEEE Transactions on Information Forensics and Security, vol. 11, no. 3, pp. 571-583, 2016.
2. Z. Baharav and R. Kakarala, "Visually significant QR codes: Image blending andstatistical analysis," in Proc. IEEE Int. Conf. Multimedia Expo (ICME), pp. 1–6, Jul. 2013.
3. C. Baras and F. Cayre, "2D bar-codes for authentication: A security approach," in Proc. 20th Eur. Signal Process. Conf. (EUSIPCO), pp. 1760–1766, Aug. 2012.
4. A. T. P. Ho, B. A. M. Hoang, W. Sawaya, and P. Bas, "Document authentication using graphical codes: Reliable performance analysis and channel optimization," EURASIP J. Inf. Secur., vol. 2014, no. 1, p. 9, 2014.
5. 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), pp. 520–523, Aug. 2014.
6. T. Langlotz and O. Bimber, "Unsynchronized 4D barcodes," in Proc. 3rd Int. Symp., ISVC 2007, Lake Tahoe, NV, USA, pp. 363–374, Nov. 26–28, 2007.
7. I. Tkachenko, W. Puech, O. Strauss, C. Destruel and J. Gaudin, "Printed document authentication using two level or code", 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2016.

BIOGRAPHIES

Shreya Vyankatesh Uttarwar is a student of Master of Engineering (M.E.), Information Technology Branch, in Pune Institute of Computer Technology (PICT), Pune.

Dr. A. M. Bagade is a Associate Professor in the Information Technology Department, Pune Institute Of Computer Technology (PICT), Pune. He has received Ph.D. in Computer Science and Engineering.