A Review On QR Code For Hiding Private Information

Mr.V.V.Panchal[1], Mr.H.B.Torvi[2]

[1] Department of Computer science and Engineering, V.V.P. Institute of Engineering and Technology, Solapur-413004.
[2] Assistant Professor, Department of Computer Science and Engineering, V.V.P. Institute of Engineering and Technology, Solapur-413004.

---***---

Abstract - *The Quick Response (QR) a high speed reading application designed for storage of information. In this paper, we present a new rich QR code that has two storage levels. level one and level two The level one named a public level ,and level two named as private level. The public level is the same as the standard QR code storage level, therefore it is readable by any classical QR code application. The private level is constructed by replacing the black modules by specific textured patterns. It consists of information encoded using q-ary code with an error correction capacity. This allows us not only to improve the security of the QR code, but also increase the storage capacity of QR code and distinguish the original document from a copy.*

Key Words: QR code, two storage levels, private message, data hiding, Watermark, Discrete Cosine Transform, Steganography and Image Fusion

1.INTRODUCTION

The definition of information security given by National Institute of standard and Technology (NIST) says that,” The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.” integrity, which means guarding against improper information modification or destruction, and includes ensuring information non repudiation and authenticity ;confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and availability, which means ensuring timely and reliable access to and use of information. The term information forensics relating to the application of scientific methods and technique to the investigation of crime. For providing security to information, hiding the information in cryptographic from in an image [9].

Quick response Code (QR code) is widely used in daily life in recent years because it has high capacity encoding of data, damage resistance, fast decoding and other good characteristics. [5] QR code (quick response code) is a type of two dimensional barcode developed by Denso-Wave corporation in 1994 [1]. Todays, graphical codes, such as EAN-13 barcode [1], Quick Response (QR) code [3], DataMatrix [2], PDF417, are frequently used in our daily lives. These codes have a huge number of applications including: storage of information (advertising, museum art description), redirection to web link, phone number track and trace (for transportation tickets or brands), identification (flight passenger information, supermarket products) etc. Due to improving the reading speed of 2D-barcodes get the name Quick Response (QR) Code.it is extension of 2D-barcode.it contains data for both horizontal and vertical dimension. The decoding speed of QR code can be 20 times faster than that of other 2D symbols.

2. LITERATURE SURVEY

[4] Robust Message Hiding for QR Code

In [4], QR code is popular for exchange of secret information. The authors analyzed the properties of each QR code before embedding it in to this one. If they want to embed secret message into QR code, they will encode it first. After that, they exploit the structure of QR code which code they want to use. It takes time, risks and cannot get the secrete message directly from this QR code. The Lin et al proposed to hide secret message in to QR code is to use the error correction capability. First of all, they encode the secret message *sm* by using a shared key *K* and get *EK*(*sm*). After that, they embed each bit of *EK*(*sm*) into QR code. Their first drawback is that if any bit of *EK*(*sm*) is damaged, it is impossible to recover *sm* from QR code. The second drawback is that if an attacker does not change any bit of *EK*(*sm*) but adds some extra error values into QR code, they cannot recover their secret message. Their main contributions are 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] Secret Hiding Mechanism Using QR Barcode

In [5] this Paper, a new secret hiding mechanism for QR tag based on the property of QR code. The new scheme exploits the error correction capability to conceal the secret into a cover QR code. Along with the QR version and the error correction level, the designed algorithm can convey larger secret into a cover QR code directly. Besides, the content of the marked QR code is readable. That is, general browsers can read the QR content from the marked QR code for the sake of reducing the risk of attention. Only the validated receiver can decode and encrypt the secret from the marked QR code. The process of the new scheme is efficient and feasible to be applied to the low-power QR readers and mobile devices.

[6] QR Code Using Invisible Watermarking in Frequency Domain

In [6] Digital watermark is a kind of information security and protection technology. Watermarking is mostly similar to steganography in a number of respects. The main idea of steganography is the embedding of secret information into data under assumption that others cannot know the secret information in data. In general, the results of this method are not robust against attacks. The main idea of watermark is to check if the secret information is embedded in data or not and the secret information that is embedded is robust against attacks or edition when it is discovered. The result of this method is more robust than previous method. Watermark is the embedding of information in media for exchange the information within the group. The input to the scheme is the watermark, the cover-data and an optional public or secret key. The key may be used to enforce security that is the prevention of unauthorized parties from recovering and manipulating the watermark. All practical systems employ at a key. In combination with a secret or a public key, the watermarking techniques are usually referred to as secret and public watermarking techniques, respectively. The output of the watermarking scheme is the watermarked data.

This paper uses DCT to embed an image of secret information inside QR Code image. The main arguments for using DCT in watermarking are the following. Embedding rules operating in the DCT domain is often more robust to image compression. Watermarking in the DCT domain offers the possibility of directly realizing the embedding operator in the compressed domain in order to minimize the computation time. The DCT coefficients of the QR Code image and the DCT coefficients of the watermark text (secret information) can be added. In more subtle algorithms, relationships between multiple DCT coefficients can be imposed according to the bit values of the watermark. Furthermore, their quantization can be disturbed according to the watermark bits.

[7] Visually significant QR Codes: Image blending and Statistical analysis

In [7] this paper, a simple method of decoding allows for some latitude in QR code design. If we treat luminance values as normalized to the interval [0, 1], then sensed values in the range [λ,1] are considered white by the decoder, and those in the interval [0,λ] are considered black. Therefore, we may in theory modify the QR code source pixels so that pixels in a white module are transformed from white to any RGB coordinate whose luminance value exceeds λ, without creating a decoding error; similarly, we can modify black modules of the QR source so that their luminance falls below λ. In practice, the luminance sensed by the camera fluctuates due to lighting conditions and noise. Therefore, it is prudent to use upper and lower modification thresholds denoted T_u , T_l, respectively, so that white pixels are modified to have luminance T_u where $T_u > \lambda$, and black pixels to have luminance $T_l < \lambda$. The differences $T_u - \lambda$ and $\lambda - T_l$ provide a margin to reduce decoding error. Below, we analyze statistically the effect of threshold choices on error.

[8] Facial Biometrics for 2D Barcodes

In [8] this paper, focus on the verification problem, in which the system needs to confirm or reject the claimed identity based on the input face, and do not address identification problems (where the input is an unknown face, and the system reports back the determined identity from a database of known individuals). Although computer chips and RFID tags have been previously used for storing biometric information (e.g., Germany introduced its electronic passport containing a chip with a digital photo as biometric identifier [7]), they are not suitable for low-cost solutions, such as those involving paper documents (i.e., paper tickets) rather than smart cards (i.e., pass cards). Compared to computer chips and RFID tags, barcodes have smaller storage capacity and cannot be used as active elements, but they are much cheaper and do not require specialized hardware for retrieving data: indeed, barcodes are inexpensive, passive read-only elements whose content cannot be altered and can be decoded by many ubiquitous and low-cost devices, including smartphones.

The main contributions of this paper are the following. First, they investigate techniques for the extraction of facial characteristics which are not only robust to distortions (such as pose and illumination changes) but also suitable for being embedded into barcodes. This study leads us to identify the most suitable facial features that can be stored in 2D barcodes, while still supporting reasonably good recognition performances. Second, they engineer existing 2D color barcodes in order to increase their data density, so that they can store a sufficient number of facial features and a reasonable cryptographic payload. In particular, they show how to modify HCC2D, the High Capacity Colored 2-Dimensional Barcode so as to increase its data density up to 3,904 bytes per square inch.

3. PROPOSED SYSTEM

In our propose system, a new two level QR code generated, which having two storage levels public and private levels can be used for document authentication. This new generated QR code, called as two levels QR code (2LQR). In the public level is the same as the standard QR code storage level; therefore it is readable by any QR code application. The private level is constructed by replacing the black modules by specific textured patterns. In our system we encrypt the private message which generates the code words . It consists of information encoded using q-ary code with an error correction capacity. That allows us not only to improve the security of the QR code, but also to distinguish the original document from a copy. And increase the storage capacity of QR code.

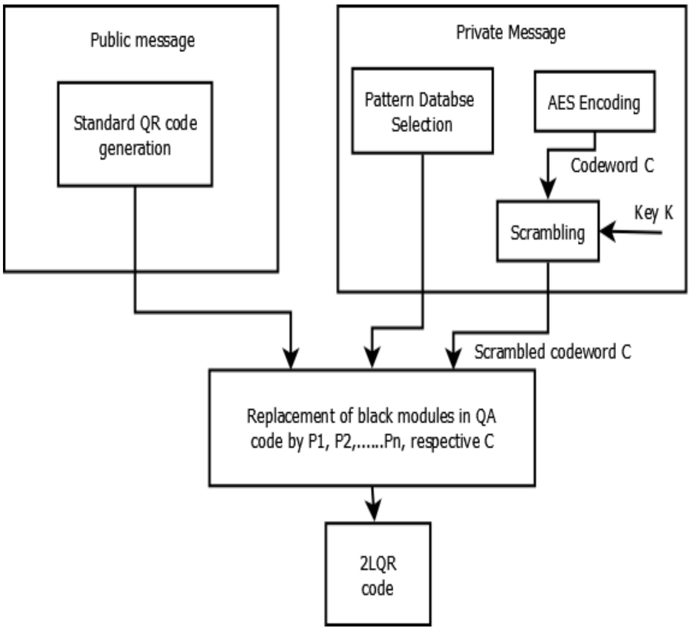
Public message
Standard QR code generation
Private Message
Pattern Databse Selection
AES Encoding
Codeword C
Key K
Scrambling
Scrambled codeword C
Replacement of black modules in QA code by P1, P2,......Pn, respective C
2LQR code

Fig -1: System Architecture

4. CONCLUSIONS

In the proposed system we are going to improve the security and storage capacity of two levels QR code. The public level and private level in the public level public information which is visible to all over and the private level contains private information which can access only authorized user of system. Objective of our project is to increase the storage capacity and improve the security.

REFERENCES

[1] ISO/IEC 15420:2009. Information technology - Automatic identification and data capture techniques - EAN/UPC bar code symbology specification. 2009.
[2] ISO/IEC 16022:2006. Information technology - Automatic identification and data capture techniques - Data Matrix bar code symbology specification. 2006.
[3] ISO/IEC 18004:2000. Information technology - Automatic identification and data capture techniques - Bar code symbology - QR Code. 2000.
[4] Thach V. Bui, Nguyen K. Vu, Thong T.P. Nguyen, Isao Echizen and Thuc D. Nguyen," Robust Message Hiding for QR Code", 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing,pp.520-523.
[5] Pei-Yu Lin, Yi-Hui Chen, Eric Jui-Lin Lu and Ping-Jung Chen," Secret Hiding Mechanism Using QR Barcode", 2013 International Conference on Signal-Image Technology & Internet-Based Systems, pp.22-25.
[6] Sartid Vongpradhip and Suppat Rungraungsilp," QR Code Using Invisible Watermarking in Frequency Domain", 2011 Ninth International Conference on ICT and Knowledge Engineering, pp.47-52.
[7] Z. Baharav and R. Kakarala. Visually significant QR codes: Image blending and statistical analysis. In Multimedia and Expo (ICME), 2013 IEEE International Conference on, pages 1–6. IEEE, 2013.
[8] Marco Querini and Giuseppe F," Facial Biometrics for 2D Barcodes", Proceedings of the Federated Conference on Computer Science and Information Systems pp. 755–762
[9] Richard Kissel" Glossary of Key Information Security Terms", National Institute of Standards and Technology (NIST) May 2013, pp1-222.
[10] J. C. Chuang, Y. C. Hu and H. J. Ko, "A novel secret sharing technique using QR code," International Journal of Image Processing, vol. 4, pp.468-475, 2010.
[11] Lin Liu, "A Survey of Digital Watermarking Technologies", www.ee.sunysb.edu/~cvl/.../Lin%20Liu /ese558report_LinLiu.pdf
[12] Chung, Chin-Ho, Wen-Yuan Chen, and Ching-Ming Tu. *Image hidden technique using QR-barcode.* In Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP'09. Fifth International Conference on, pp. 522-525. IEEE, 2009.
[13] L. Yu, X. Niu, and S. Sun. Print-and-scan model and the watermarking countermeasure. In Image and Vision Computing, volume 23, pages 807–814. Elsevier, 2005.
[14] Geisel, William A. *Tutorial On Reed-Solomon Error-Correction Coding.* (1996).
[15] http://www.qrcode.com/.