International Journal of Computer Engineering in Research Trends
Multidisciplinary, Open Access, Peer-Reviewed and fully refereed
Research Paper Volume-5, Issue-12, 2018 Regular Edition E-ISSN: 2349-7084

Overview of Visual Secret Sharing Schemes for QR Code Message

Komal S. Patil[1*], Suhas B. Bhagate[2], Dhanashri M.Kulkarni [3]

[1]*Department of Computer Science, D.K.T.E. Society's Textile and Engineering Institute, Ichalkaranji, India*
[2]*Department of Computer Science, D.K.T.E. Society's Textile and Engineering Institute, Ichalkaranji, India*
[3]*Department of Computer Science, D.K.T.E. Society's Textile and Engineering Institute,Ichalkaranji, India*

e-mail: komal.patil6596@gmail.com, suhas.bhagate@gmail.com, kulkarni.dhanashri@gmail.com.

Available online at: http://www.ijcert.org

Received: 19/Dec/2018, Revised: 21/Dec/2018, Accepted: 28/Dec/2018, Published: 04/Jan/2019

Abstract:- The Quick Response (QR) code was designed for storing information and high-speed reading applications. With the wide application of QR code, the security problem of a QR code is severe, such as information leakage and data tampering. The QR code contains a secret message. To solve the QR information security problem, this paper proposed visual secret sharing schemes for QR code message. Invisible secret sharing scheme the QR code message is divided into several parts called shares, which separately reveals no knowledge about the QR code message. By stacking two or more shares one another, QR code message can be revealed and visually recognized. It improves the security of the data transmission and also improves the clarity of a secret image.

Keywords: Visual Secret Sharing Scheme, QR code, Progressive Visual Cryptography Scheme.

1. Introduction

Visual cryptography is one of the secret sharing techniques. Moni and Adi Shamir originally invented it in 1994 [1]. Visual cryptography deals with hiding the information in images, in such a way that it can be decrypted by human vision. The secret image is encrypted into n number of shares, and the hidden image can be reconstructed from any k or more shares are stacked together ($k \leq n$).

Quick Response (QR) code is generally used for data storage and high-speed machine reading. QR code is two dimensional (2D) barcode developed by Denso-wave Company in 1994 [2]. The main use of QR code is to store a large amount of data on a small size. In day-to-day life, QR code is used in the variety of scenarios, including information storage, web links, phone number, traceability, identification, and authentication. The 1D barcodes can store a maximum of 20 alphanumeric digits, while the QR codes store around 7089 numeric characters and around 4296 alphanumeric characters. Information stored in the QR code can be accessed by anyone, so it needs to provide security using cryptography or other protection technique.

QR code conveys information through the arrangement of dark modules and light modules. Module refers to the black and white dots that make up the QR code. The QR code consists of two main parts, the encrypting region, and the function patterns. Function pattern is the shape that must be placed in the specific area of the QR code to ensure that the QR code scanner correctly recognizes and orients the code for decoding. There are four different types

 https://doi.org/10.22362/ijcert/2018/v5/i12/v5i1202

of function patterns i.e. finder pattern, separator, timing patterns and alignment patterns. The encrypting region consists of data that represents version information, format information, data and error correction code words. There are 40 versions (1-40) and 4 error correction levels (L, M, Q, and H) of QR code are defined. Each QR code version has a data capacity, depends on the amount of data, character type, and error correction level. Data is encoded as a bit stream, which is divided into a sequence of codewords. The length of each code words is 8 bit. The code words are divided into a number of error correction blocks, based on QR code version and error correction level. The QR code employs error correction mechanism that allows correct decoding of the message even if some part of the symbol is dirty or damaged.

Visual secret sharing mechanism is used to secure the QR code message so that the data privacy during data transmission can be enhanced. The secret QR code message is divided into a number of shares by the hidden sharing mechanism, and secret QR code message can be recovered when the minimum two or number of shares are stacked together.

2. Related Work

MoniNaor and Adi Shamir proposed visual cryptography scheme [1]. The primary purpose of the visual cryptography scheme is to encrypt a secret image into some shares. Confidential information cannot be revealed with a few shares. All shares are necessary to combine to show the mysterious image. In (2, 2) Visual Cryptography Scheme, an original image is divided into 2 shares. Both the shares are required to be superimposed to reveal the secret image. Anyone, having only one share will not be able to reveal any secret information. In (k,n) scheme, if any k recipients stack their transparencies together, then a secret message is revealed visually. On the other hand, if only k −1 recipients stack their transparencies, they are not able to obtain any information about the secret message. The main drawback of (k,n) visual cryptography scheme approach is, it requires at least k shares to recover the hidden message.

Wen-Yuan Chen et al, proposed image processing and QR code techniques that can be used to construct nested steganography scheme [3]. Steganography technique hides the secret data into the cover image, so any other people cannot discover the confidential data. There are two types of data (text and image) is serve as confidential data. In the embedding process, the working flow divided into three parts. The upper portion can be text data encoding process that converts text into 2D barcode pattern and then embeds into the cover image. Middle part can be face image embedding process. Lower portion creates the cover image for secret data embedding. At starting text data taken as input and generate the QR code, then regular area moving (RAM) can be used for moving redundancy. The chaotic mechanism provides hashing of secret data to enhance the security. On cover image, a DCT is used to convert an image from the spatial domain to the frequency domain for robustness. The IDCT returns cover image to the spatial area from the frequency domain; then secret data embedding is complete. In decoding secret data, the extraction algorithm is used that extracts the text and image. The problem of this approach is it requires some other operations such as chaotic inversion or calculation of correlation coefficients which are computationally expensive.

Li Li, Rui-Ling Wang, Chin-Chen Chang proposed a digital watermarking algorithm for QR code [4]. Digital watermarking is a fascinating topic in current research related to the security field. This technology combines 2D Barcode with a digital watermark. Digital watermarking is an information security and protection technology. The basic idea is to embed the watermark signal in the secret image and detect the watermark signal by a specific technique. Watermark signal contains an electronic signature, date, audio, text or digital works. This hidden information can also be extracted from printed or scanned images. The digital watermark method is used for the QR Code. The watermark technology is used to embed the invisible watermark into the QR code image. After embedding the watermark, the DCT IF coefficients are compared. To prevent the overflow of the QR Code in the DCT domain of the image, QR image needs fuzzy processing and be added noise too. In order to resist image distortion after print and scan operations, the watermark is repeatedly embedded. The watermark is extracted by using the two maximum membership degree of the fuzzy pattern recognition without the original image.

J. C. Chuang, Y. C. Hu, H. J. Ko proposed method that shares confidential secret data [5]. Secure data transmission scheme based on the secret sharing scheme with QR code. Shamir first proposed secret sharing scheme in 1979. The main idea of the secret sharing scheme divides a secret into *n* shadows or called shares. The shadows that are generated are embedded in each QR code tag. The secret data

can be recovered only when any t out of n shadows ($t \leq n$) are stacked one another. In the decoding process to recover secret data, the Lagrange polynomial interpolation technique can be used. A secret sharing mechanism is used to improve the security and data privacy of the QR code and also provides high security during data transmission but it requires high computational complexity for decryption. This technique can be applied to some applications such as electronic tickets, airline luggage inspection, medical e-health system, and other fields.

Xiaohe Cao, Liuping Feng, Peng Cao and Jianhua Hu proposed Secure QR Code Scheme Based on Visual Cryptography [6]. With the broad application of QR code, the security problem of the QR code is serious, such as information leakage and data tampering. To solve the QR information security problem, the secure QR code schema based on visual cryptography technique is used. The QR code is divided into two share images that can be transmitted separately. The generation of the two share images is based on the pseudo-random matrix, that is, the corresponding values determine the pixels in the two share images in the pseudo-random form. The two share images can be stacked merely to restore the QR code information. QR code information prevention using visual cryptography and QR code techniques. It applies the pseudo-random matrix in this scheme and verifies scheme's feasibility. It shows that this scheme is efficient and also indicates that this scheme is a reliable method through combining visual cryptography with the pseudo-random matrix for detecting the attacker. It provided better security for the QR code.

Yang-Wai Chow, Willy Susilo, et al., a proposed QR code for secret sharing approach exploits the error correction mechanism inherent in the QR code [7]. One of the problems of storing secrets in a single information carrier is that it is easily damaged or lost. The secret sharing mechanism distributes and encodes information about the mystery in some shares. Each share is constructed from QR code and each share itself a valid QR code. The secret message can be recovered by combining the information contained in the QR codeshares. Individually, the shares reveal no information about the secret. The (n,n) secret sharing scheme used to as QR code secret sharing (QRCSS), which exploits the error correction redundancy in the QR code structure. The QR code containing a secret message, it distributes and encodes into n number of shares, and hidden message is recovered only all n shares are stacked together. The main advantages of this paper are to reducing attracting the attention of potential attackers, and while improving the secret image, users do not need any computing devices. The hidden image is revealed without any loss in visual quality also it requires low computational complexity for decryption. This approach has low security, and it has limited to (n,n) scheme.

Yuqiao Cheng, Zhengxin Fu, Bin Yu proposed an improved visual secret sharing method for QR code [8]. It encodes secret QR code into multiple shares. Each share is a valid QR code. The hidden message can be recovered by stacking QR code Shares in one another. Secret sharing overcomes the problem of storing a secret in a single information carrier, which can be easily lost or damaged. The security weakness can be solved by extending the access structure from (n,n) to (k,n). In (k,n) secret sharing scheme, the secret message has to be divided into n shares, where $n>1$ shares should be created and k shares are required to reconstruct the secret QR code message, where $k \leq n$. Even k-1 shares cannot recover the secret message. It provides high security and more flexible access structure. The computational cost is much smaller than other approaches.

Young Cheng, Hou and Zen-YuQuan proposed progressive visual cryptography with unexpanded shares [9]. The basic (k,n) threshold visual cryptography scheme is to share a secret image with n participants. The secret image can be recovered while stacking k or more shares obtained, but we will get nothing if there are less than k pieces of shares being overlapped. On the contrary, progressive VC can be utilized to recover the secret message gradually by superimposing more and more shares. If we only have a few pieces of shares, we could get an outline of the secret image; by increasing the number of the shares being stacked, the details of the hidden information can be revealed progressively. The progressive VC can improve the clarity of a secret image step by step by stacking more and more shares. The pixel unexpanded progressive VC solves the main problem such as a leak of confidential information, pixel expansion, and lousy quality of recovered images.

3. Proposed Work

In earlier steganography and watermarking techniques were used to secure the QR code message. Transformations such as DCT or DWT are required in both techniques, but these transformations require more time and the computational cost is also expensive. The proposed

system describes different visual secret sharing schemes for securing the QR code message. In (2,2) visible secret sharing scheme, the secret image is divided into two shares. Both shares are required to recover the hidden message. Individual stock cannot improve the secret image. In (2,n) visual secret sharing scheme, the secret image is divided into n shares. Any two shares are required to recover the mysterious image. Therefore wasting of space is a drawback of this technique because if any two stocks can recover the secret image, no other stocks are required. In (n,n) visual secret sharing scheme, the hidden image divided into n shares. To recover mysterious image, all n shares are required. The disadvantage of this scheme is that less than n stocks cannot recover mysterious image. In (k,n) visual secret sharing scheme, divide the mysterious image into n shares. To recover mysterious image any k shares out of n shares is required. The less than k shares cannot improve the secret image. The value of k is in between two ton. The main drawback of (k,n) visual cryptography scheme approach is, it requires at least k shares to recover the secret message. So, as compared to the (k,n) visual cryptography, progressive visual cryptography is lessen strict because in that minimum 2 or more shares can reveal secret information progressively. All of the above limitations are resolved using a progressive visible secret sharing scheme.

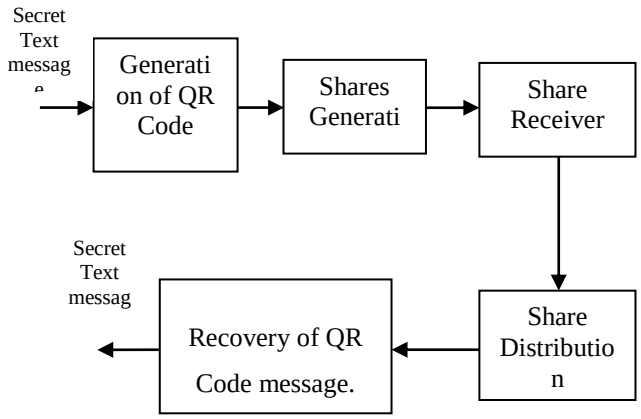

Figure1. System architecture

Figure 1 shows the system architecture of the proposed system. It takes secret text message as input and generates the QR code of secret text message using a QR code generator. The generated QR code is divided into different shares. The share generation algorithm is used for share generation. The generated shares can be watermarked using a watermarking algorithm. i.e Each share is superimposed with a cover image to generate a meaningful share. Each share is a valid QR code, and it distributes to different participants. The shared receiver receives the shares from each participant. Secret text message in the QR code reveals progressively by stacking at least 2 or more and more shares. If there are only a few pieces of shares (more than the 2 shares) then the outline of the secret image can be obtained; by increasing the number of the shares being stacked, the details of the hidden information can be revealed progressively.

4. Conclusion

In today's world security of data is very important. To protect the confidential data, we need some security techniques. Visual secret sharing schemes provide an effective and efficient way of providing security to QR code message. In this paper briefly reviewed the literature survey of visual secret sharing schemes for QR code message. All schemes are good to provide security to QR code message, have their advantages and disadvantages. These schemes require more time and also for recovering the secret message at least k shares are needed. Therefore, Progressive visual secret sharing scheme is used to secure the secret QR code message.

References

[1] M. Naor and A. Shamir, "*Visual Cryptography*", in Proc. Advances in Cryptology: EUROCRYPT 94, vol. 1995, (950) pp. 1–12.

[2] International standard ISO/IEC 18004, "*Information technology Automatic identification and data capture techniques Bar code symbology QR Code*", Reference number- ISO/IEC 18004:2000(E), First edition 2000-06-15.

[3] W. Y. Chen, J. W. Wang, "*Nested Image Steganography Scheme using QR-barcode Technique*", Optical Engineering, vol. 51, no. 5, pp. 057004, 2009.

[4] L. Li, R. L. Wang, C. C. Chang, "*A Digital Watermark Algorithm for QR Code*", International Journal of Intelligent Information Processing vol. 2, no. 2, pp. 29-36, 2011.

[5] J. C. Chuang, Y. C. Hu, H. J. Ko, "*A Novel Secret Sharing Technique using QR Code*", International Journal of Image-Processing, vol. 4, no. 5, pp. 468-475, 2010.

[6] X. Cao, L. Feng, P. Cao and J. Hu, "*Secure QR Code Scheme Based on Visual Cryptography*", 2nd International Conference on Artificial Intelligence and Industrial Engineering, vol. 133, 2016.

[7] Y W. Chow, W Susilo, G Yang, "*Exploiting the Error Correction Mechanism in QR Codes for Secret Sharing*", Information Security and Privacy, pp.409-425, 2016.

[8] Yuqiaocheng, Zhengxin Fu, Bin Yu, "*Improved Visual Secret Sharing Scheme for QR Code Application*", IEEE Transactions on Information Forensics and Security,2018.

[9] Young cheng, Hou and Zen-YuQuan, "*Progressive Visual Cryptography with Unexpanded Shares*", IEEE Transactions on Circuits and Systems for Video Technology, 2011.

