ELEVATING QR CODE SECURITY THROUGH ENHANCED VISUAL SECRET SHARING

KIRTI T. KAMTHE, Department Of Computer Engineering , Trinity College Of Engineering And Research Savitribai Phule Pune University, India

PRASAD BHOSLE, Department Of Computer Engineering , Trinity College Of Engineering And Research Savitribai Phule Pune University, India

RUTIKA SHAH, Department Of Computer Engineering , Trinity College Of Engineering And Research Savitribai Phule Pune University, India

Abstract

Quick Response (QR) codes have been widely used in applications such as data storage and high-speed machine reading. Anyone can gain access to the information stored in QR codes; therefore, they are unsuitable for encoding secret information without the addition of cryptography or other protection. In this paper, we propose a visual secret sharing scheme to encode a secret QR code into several shares. In contrast with other techniques, the shares in our scheme are valid QR codes that can be decoded with some specific meaning by a standard QR code reader, thereby avoiding raising suspicion in potential attackers. Moreover, the secret message is recovered by XOR-ing the qualified shares, an operation that can easily be performed using smartphones or other QR scanning devices. Experimental results show that the proposed scheme is both feasible and reasonably secure. Our scheme's high sharing efficiency is also highlighted in this paper.

Keywords— QR (Quick Response) Code, healthcare, Health Monitoring, QR Code Technology, Medical Records

I. INTRODUCTION

Quick Response (QR) codes are two-dimensional barcodes that can be used to store a variety of information, such as text, URLs, and contact information. QR codes are widely used in a variety of applications, such as mobile payments, product tracking, and marketing.However, QR codes are also vulnerable to tampering and counterfeiting. To address this issue, researchers have proposed using blockchain technology to improve the security of QR codes.One way to improve the security of QR codes is to use visual secret sharing (VSS). VSS is a cryptographic technique that allows a secret image to be split into two or more shares, such that the secret image can only be reconstructed by combining the shares.Blockchain can be used to improve the security of VSS by providing a tamper-proof way to store the shares. This can help to prevent attackers from tampering with the shares or from forging new shares.The remainder of this paper is organized as follows. Section II introduces some preliminaries concerning our study. The proposed scheme is described in Section III, where contrastive and secure properties are theoretically proved. Experiments and Comparisons are presented in Section IV to illustrate the feasibility of this work and demonstrate how it improves on previous work. Finally, Section V provides conclusions.Modern commercial applications employ QR codes in brand promotion, enriching consumer usage experience, interactive labeling for sharing product information, including promotional videos, web links, etc. In addition, QR codes are integrated with service platforms of governments for the effective delivery of utilization and administrative services to the public. The simplicity of QR code generation and scanning with cheap smart phones and IoT has harnessed their extensive adaptation by commercial and nonprofit organizations [1]. For an example, QR codes allow the consumer to connect to the IoT with a simple smartphone or tablet scan. Having all objects marked with a QR code or barcode means improving the retail environment for consumers because they will be more educated about the item before purchasing, and they will be able to check for an item's availability. On the other hand, they are also susceptible to tampering and duplications for illegal financial benefits and counterfeiting authentic goods [2]. Security investigations have reported huge losses to commercial organizations that are ascribed to the flooding of fake goods carrying authentic QR codes. Several mechanisms have been proposed so far for protecting the QR codes against attacks.

II. RELATED WORK

Secret Image Sharing (SIS) schemes share a secret image as a number of secret shares or shadow images among the participants and recover the secret image, combining sufficient number of shares. Visual Secret Sharing (VSS) and Polynomial-based Secret Sharing (PSS) are the popular SIS approaches. VSS schemes reconstruct the secret image simply stacking the secret shares. These schemes based on the logical XOR operations are characterized by lossy recovery and low visual quality of reconstructed secret images [17]. In the earliest *(k,n)* PSS scheme proposed by Naor and Shamir [18], the secret image is divided into n shares, where at least k out of n shares are required for secret image reconstruction. Though this scheme is secure, it is characterized by storage overheads, as each shadow image is of the size of the secret image. A variant of this scheme proposed by Thien and Lin [19] reduced the size of each shadow image by $1/k$ of the secret image. However, in this method, traces of the secret image are evidenced in the shares and the secret can be reconstructed from insufficient number of shares, forsaking security. Though lossless recovery of secret image is achieved by this method, it suffers from random pixel expansion. Further, other PSS schemes have also been proposed featuring lossless recovery. The scheme proposed by Yang et al. [20] based on polynomials in the Galois Field, exhibits higher computational costs compared to other methods. Similarly, a lossless scheme proposed by Ding et al. [21] also suffers from limitations such as random shape changes, large shadow size and high computational complexity. In a *(k,n)* PSS scheme proposed by Zhou et al. [22], the shadow size is reduced to $1/k - 1$ of the secret image. This method embeds the first $k - 1$ coefficients to reduce the shadow size. A *(n,n)* visual secret-sharing scheme based on XOR operations is proposed in [23], which shares the secret as n meaningful shares among n participants. The authors of this paper claim that this method is superior to conventional methods as the drawbacks such as pixel expansion, alignment of shares for reconstruction, loss of contrast, need for an explicit codebook for construction, etc., are mitigated.

Though creation and recognition of QR codes are simple, incorporating them in the business workflow of enterprises poses severe security risks, as QR codes are vulnerable to copy–paste attacks. A QR code can allegedly be used as an attack vector for threatening the reputation of an organization. Sharing a QR code securely among a group of people as secret shares and recovering the QR code from the shares will be a potential solution to enforce trust among a group of people. The significant difference between sharing images and QR codes is that the QR codes must be decodable after recovery. This requirement imposes a stringent constraint on the implementation of the QR code secret-sharing schemes.

Several attack scenarios such as Cross-Site Request Forgery attack (CSRF) [24], Cross-Site Scripting (XSS) attack [25], social engineering, phishing and pharming attacks can be launched, making minimal changes to genuine QR codes. Various empirical studies on the use of QR code as an attack vector are demonstrated in [26]. In order to prevent these attacks, QR code-sharing schemes must avoid information leakage in the secret shares, making reconstruction difficult. In addition, limitations of conventional secret-sharing schemes such as pixel expansion, memory overheads and computational costs must also be reduced or overcome in these schemes. Further, readability requirements also make QR secret-sharing a challenging task. Hence, there are only very few works in this context, discussed in this section.

Lin [27] proposed an *(n,n)* secret-sharing scheme in which the secret is divided into *n* shadows. Each shadow along with the authentication code is embedded as a pair (s_i,v_i) into the data codewords of each cover QR code QR_i. At the other end, (s_i,v_i) pair is extracted from each QR_i and all the shares are combined to reveal the secret. This scheme verifies the integrity of each share with the verification code, generated using a master key and a hashing function. A *(k,n)* secret-sharing scheme proposed in [28] shares a secret image as *n* QR code shares and provides two approaches for revealing the secret, one by stacking the QR code shares and the other by performing XOR operations. This approach called a VSS-based QR code (VSSQR) scheme, exploits the error correction capabilities of the QR codes to generate QR code shares to share images. The secret image can be revealed by stacking a sufficient number of QR-code shares in low-resource settings. Further, this method also facilitates lossless recovery of a secret image by XOR operations among the shares. In an *(n,n)* secret-sharing mechanism proposed in [29], a secret message is encoded as a secret QR code and shared among *n* participants as QR code shares. The secret message is decoded from the QR code revealed by combining these *n* shares. Similarly, a cooperative secret-sharing protocol proposed in [30], embeds secret messages within QR codes and distributes them to *n* participants such that each QR code carries both public and private information. Public information is readable by conventional QR scanners while the private message is extracted using a symmetric key. This message is then decoded with the private key of a participant to extract the share. These shares are combined to extract the secret messages.

Liu et al. [31] have proposed a (3,3) threshold secret-sharing scheme called the VSS-QR code. This approach encodes the binary QR codes into three color shares and recovers the QR code by stacking them. Yu et al. [32] present a three-level QR coding scheme, embedding sensitive information within a carrier QR code in three steps, revealing only the public information of the carrier at the first layer.

III. OBJECTIVES

This paper is aimed to improve the security of QR codes by making them more tamper-proof and counterfeit-resistant.Traditional QR code security schemes often reveal information about the secret image, even if they are not able to fully reconstruct it. Traditional QR code security schemes can be difficult to scale to support a large number of QR codes.

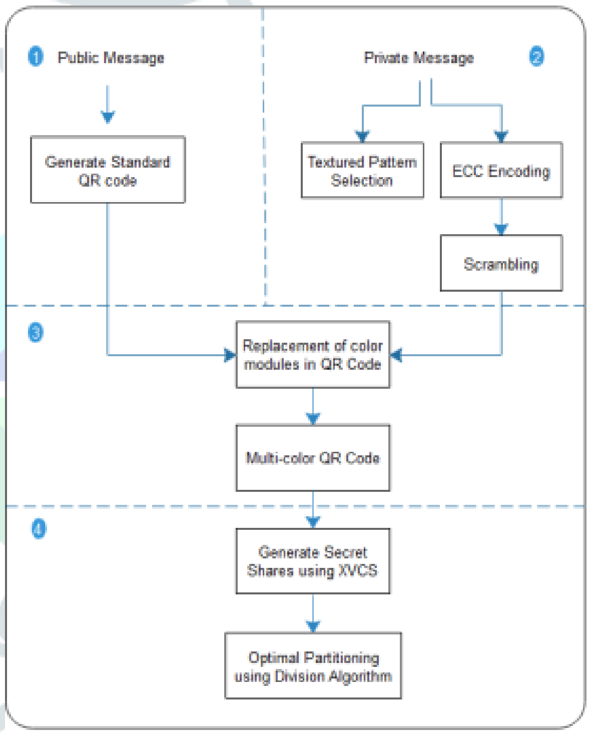
IV. METHODOLOGY

An innovative scheme is proposed to improve the security of QR codes using the XVCS theory. An improved (n, n) sharing method is designed to avoid the security weakness of existing

methods. In (n, n) sharing method, n shares are distributed intoparticipants. Here, all shares are needed to get secret. In an

improved (n, n) sharing method we are taking into consideration (k, n) access method. In (k, n) access structure k and n are shares and at least k shares are required to get secret. This approach will require large number of instances as n increases. Therefore, presents division algorithm to classify all the k-participant subsets into several collections. Division algorithm will reduce number of shares. Algorithm for QR code generation is used where it includes encoding and decoding algorithm for QR code. After creating QR code secret are divided into number of shares at senders side. At receiver end those shares are combined to get access to QR code. Only authorized person will get document as it compares shares at sender side and shares at receiver side. • Enhanced (n, n) sharing method In this method, secrets are distributed amongst the participants and all shares are necessary to get the secret. • (k, n) sharing method

In this method, secrets are distributed among the participants and at least k shares are necessary to get required share. Based on the enhanced (n, n) method, a (k, n) method can be achieved. However, there will be a huge amount of (k, k) instances.


1
Public Message
Private Message
2
Generate Standard QR code
Textured Pattern Selection
ECC Encoding
Scrambling
3
Replacement of color modules in QR Code
Multi-color QR Code
4
Generate Secret Shares using XVCS
Optimal Partitioning using Division Algorithm

Advantages of Proposed System:
1) Secure encoding of document or text.
2) Text steganography for message encoding.
3) Increases the sharing efficiency.
4) Low computational complexity.
5) Higher security and more flexible access structures.
6) Computation cost is less.
7) Synthetic texture for QR code hiding.

V. DISCUSSION

Experiments are done by a personal computer with a configuration: Intel (R) Core (TM) i3-2120 CPU @ 3.30GHz, 4GB memory, Windows 7, MySQL 5.1 backend database and jdk 1.8. The application is web application used tool for design code in Eclipse and execute on Tomcat server. Some functions used in the algorithm are provided by list of jars like zxing jar for QR code generation. .It consist of generation of multicolor QR code using visual secret sharing scheme. The multi-color QR code security with texture patterns by applying the xoring based Visual Cryptography Scheme on QR code for sharing secrets to the receiver. The fig. 4 shows the multi-color QR code .The experiment includes two processes encryption process and decryption process.

VI.CONCLUSION

The blockchain improved VSS scheme is a new technology that can be used to improve the security of QR codes. The scheme works by splitting a secret image into two shares and storing the shares on a blockchain network. This makes it difficult for attackers to tamper with the shares or to forge new shares.Theblockchain improved VSS scheme has a number of benefits over traditional QR code security schemes, including improved security, increased privacy, and improved scalability. However, the scheme also has some challenges, such as cost and complexity.More research is needed to address the challenges of the blockchain improved VSS scheme. However, as the cost of blockchain transactions decreases and blockchain technology becomes more user-friendly, we can expect to see the scheme morewidely adopted in QR code applications.

REFERENCES (CHICAGO STYLE)

[1] Krzysztof Czuszynski, Jacek Ruminski, "Interaction with medical data using QR-codes", 978-1-4799-4714-0/14/$31.00 ©2014 IEEE

[2] Computer Engineering & Informatics Department, Paschou Mersini, EvangelosSakkopoulos, Athanasios Tsakalidis, "APPification of Hospital Healthcare and Data Management using QRcodes", Email: {paschou, sakkopul, tsak}@ceid.upatras.gr

[3] N. Bhuvaneswari, Latha .M, Ranjith .E; International Journal of Advance Research, Ideas and Innovations in Technology, "Doctor Patient Interaction System for Android", @ 2017, www.IJARIIT.com All Rights Reserved.

[4] Chen et al. BioMed EngOnLinehttps://doi.org/10.1186/s12938-019-0674-x, "Collaborative and secure transmission of medical data applied to mobile healthcare", Weimin Chen1,2 ,Zhigang Chen1* and Fang Cui.

[5] W. Song, Y. Lu, X. Yan, *et al.*, "Visual secret sharing scheme for (k, n) threshold based on QR code with multiple decryptions," *Journal of Real-Time Image-Processing*, pp.1-16, 2017.

[6] G. Wang, F. Liu, W. Q. Yan, "2D Barcodes for visual cryptography," *Multimedia Tools and Applications*, vol. 2, pp. 1-19, 2016.

[7] C. N. Yang, D. S. Wang, "Property Analysis of XOR-Based Visual Cryptography," *IEEE Transactions on Circuits & Systems for Video Technology*, vol. 24, no. 12 pp. 189-197, 2014.

[8] 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.