Secret Sharing Application for Two-dimensional QR Barcode

Chao-Wei He[1], Pei-Yu Lin[1,*], and Chih-Yang Lin[2]
[1]Dept. of Information Communication, and Innovation Center for Big Data and Digital Convergence, Yuan Ze University, Taiwan
[2]Dept. of Electrical Engineering, Yuan Ze University, Taiwan

***Abstract*-- A secret sharing system based upon two-dimensional QR barcode is proposed in this article. The proposed approach generates shadows in a specific way and utilizes the characteristics of QR code to embed shadows into cover QR codes. Each cover QR code itself is a valid QR code which can be scanned and decoded by a general QR code reader. According to the experiments, the proposed approach can satisfy the content readability of the QR code and can be distributed via public channels without raising suspicion.**

I. INTRODUCTION

Secret sharing is a kind of information sharing method and encryption algorithm. This concept has been put forward by Shamir [1] in 1979, and been known as (t, n)-threshold secret sharing. Dealer generates a group of shadows (or shares) to each participant by the specific way. The secret message cannot be read by a single shadow, yet can be recovered by combining shadows larger than t. After (t, n)-threshold secret sharing scheme been proposed, scholars [2], [4], [5], [11] - [13] have put many kinds of secret sharing methods forward. In the past five years of research, image-based act an important role of secret sharing method. To make shadows not been aware of, when designing image-sharing method, designers must choose the media that can hide shadows.

Chaudhari et al. [2], Sharma et al. [3], Ratnam et al. [4], and Yan et al. [5] use logical connective and pixel expansion to encrypt secret information. Then generate unrecognizable cover images by human vision, which look like noise map. This is the most common method in these five years. Its advantages are multi-constitute and not computationally complex. However, its weakness is low security because easy to get the attention of attackers. Karthikeyan et al. [6], Arun et al. [7], and Wu et al. [8] tried the least significant bit (LSB) or transform color space to get information from secret then changed to shadows, and concealing to pictures. The advantage of methods above is the cover image is meaningful that could cheat attackers. The weakness is the cover image cannot recover secret if via lossy compression.

To achieve image-sharing method, we can also use Quick Response code (QR code) [9] to be the cover image. Research of secret sharing combine QR code has become more important. The commonality of Chiang et al. [10], Wan et al. [11], Lin [12], and Chow et al. [13] is generated a meaning QR code and covered with shadows in the range of error correction capacity. Each cover QR code can be decoded by any standard QR code reader because it would consider shadows as damaged and recovered by error correction mechanism. Due to general QR code reader would not send notifications of errors to users, it can cheat attackers' attention. The weakness is that the resulting QR code is a high version. Technically, it lost the ability of error correction.

This paper introduces a novel approach to secret sharing method. Based on (t, n)-threshold secret sharing scheme, via dealer generates a group of shadows and encoding into QR codes. According to the characteristic of Reed-Solomon code (RS code), this method updates error correction codewords, when embedding shadows. Therefore, this could maintain the ability of error correction and transmit shadows safely. Moreover, QR code can become lower version and error correction level. It can also adjust threshold value and the number of shadows to let participants decide cover QR code format freely. So that it could be widely used in life.

The rest of the article is organized as follows. Section 2 introduces the proposed (t, n)-threshold secret QR code sharing scheme. The demonstration and performance comparisons are analyzed is presented in Section 3. Finally, conclusions are made in Section 4.

II. THE PROPOSED (T, N)-THRESHOLD SECRET QR CODE SHARING SCHEME

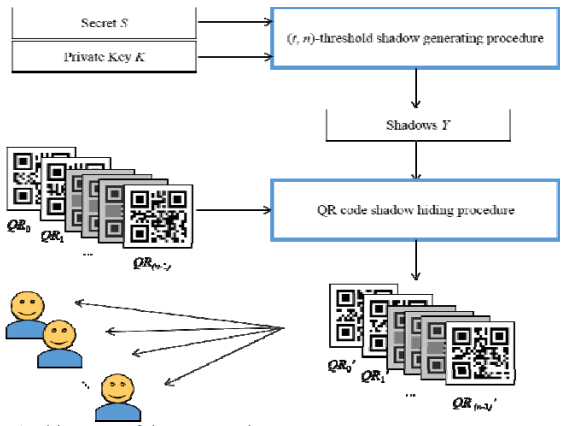

Fig. 1. Architecture of the proposed system

Refer to Fig. 1, the purpose of the proposed method is using (t, n)-threshold shadows generating procedure to realize distributed QR codes. Based on Shamir's secret sharing scheme, by giving the number of n QR codes and private keys, then generate sub-secrets and combine them into shadows by (t, n)-threshold shadows generating procedure

In shadow-hiding part, when encoding QR code, encoder

put content into data codewords and then calculate its error correction codewords. Therefore, we will embed shadows into data codewords. To avoid QR code reader read shadows as damage so that we use Gaussian Elimination to let error correction codewords keep updated, ensure QR codes are readable correctly in damage and be able to hide secret.

III. EXPERIMENTAL RESULTS

Evaluating possibilities of this method, we use C# to build a 2-L QR code embedded with shadows and compare difference modules between this QR code and a normal QR code (refer to Fig. 2). Then, we analyze by security, storage requirement, adjustability, covertness and the ability of error correction and compare with others methods.

(a) A normal QR code (b) The marked QR code of (a) with shadows (c) Difference image between (a) and (b)

Fig. 2. Example of a (*t*, *n*)-threshold secret sharing QR code of the proposed method

A. Ability of error correction

Chiang et al. [10], Wan et al. [11], Lin [12], and Chow et al. [13] cover shadows on the correct module in error correction capacity. Although it still can decode by QR code readers, yet when the real error appears, QR code becomes invalid. Our method updates error correction codewords when embedding shadows. Even if QR codes damaged or been in the poor condition, QR codes keep stable as well.

B. Storage requirement

Chow et al. [13], Chaudhari et al. [2], and Sharma et al. [3] write secret into QR code then transfer into shadows. So that the largest secret capacity is the number of data codewords. For example, Version 2-L is 34 bytes. Chiang et al. [10] and Lin [12] no need to create an extra QR code. These can make shadows hide in QR codes directly. So that the largest secret capacity is the number of error correction codewords. For example, Version 2-L is 5 bytes.

Different from above, secret capacity is adjustable in our method. We reference Shamir's secret sharing scheme, by using the threshold value (*t*) to separate secret into parts. Then encrypt with the private keys and hide shadows in QR codes. Therefore, secret capacity of our method depends on the content of cover QR code, QR version and error correction level. For example, Version 2-L is 31* *t* bytes. In other words, the higher threshold value the more secret capacity.

C. The ability of adjustment

Wan et al. [11] and Chow et al. [13] use visual cryptography to show the secret or to reconstruct QR code by modifying modules. Therefore, it must keep the same version and error correction level. The former generates both high version and error correction level, result in that it is not easy to scan by mobile and webcam. The latter must increase the threshold value at least to 14 in error correction level L. Both of them has been limited in adjustment.

The proposed method generates shadows and recovers secret by simultaneous equations. The dealer is able to decide QR version, error correction level and threshold value by content and needs of participants. In other words, every participant is able to get entirely different QR codes.

IV. CONCLUSIONS

The proposed approach utilizes the characteristics of QR codes and RS code to satisfy the essentials of steganography, readability, adjustable secret capacity, error correctable and covertness for the secret sharing mechanism. As shown in experimental result, it is obvious that the new QR secret sharing system can achieve satisfactory performance compared to related attempts.

REFERENCE

[1]. A. Shamir, "How to share a secret", Communications of the ACM, vol. 22, no. 11, 1979.

[2]. K. R. Chaudhari and S. Patil, "Secure and reliable transmission of chemical molecule structure using QR code and secret sharing," IEEE Computing Communication Control and automation (ICCUBEA), 2016 International Conference, pp. 1-5, August, 2016.

[3]. S. Sharma and V. Sejwar, "Impementation of QR Code Based Secure System for Information Sharing Using Matlab," IEEE Computational Intelligence and Communication Networks (CICN), 2016 8th International Conference, pp. 294-297, December, 2016.

[4]. J. V. Ratnam, P. R. Reddy, and T. S. Reddy, "Design of high secure visual secret sharing scheme for gray scale images," IEEE Wireless Communications, Signal Processing and Networking (WiSPNET), 2017 International Conference, pp. 145-148, March, 2017.

[5]. X. Yan and Y. Lu, "Contrast-improved visual secret sharing based on random grid for general access structure," Digital Signal Processing, vol. 71, pp.36-45, 2017.

[6]. B. Karthikeyan, A. C. Kosaraju, and S. Gupta, "Enhanced security in steganography using encryption and quick response code," IEEE Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference, pp. 2308-2312, March, 2016.

[7]. C. Arun and S. Murugan, "Design of image steganography using LSB XOR substitution method," Communication and Signal Processing (ICCSP), 2017 International Conference, pp. 0674-0677, April, 2017.

[8]. W. C. Wu, K. C. Cheng, and S. C. Yang, "Secret digital images over cloud computing using meaningful secret sharing technique," IEEE Applied System Innovation (ICASI), 2017 International Conference, pp. 889-892, May, 2017.

[9]. ISO/IEC 18004, "Information technology automatic identification and data capture techniques bar code symbology QR Code", 2000.

[10]. Y. J. Chiang, P. Y. Lin, R. Z. Wang, and Y. H. Chen, "Blind steganographic approach for QR code module based upon error correction capability," KSII Transactions on Internet and Information Systems (TIIS), vol. 7, no. 10, pp. 2527–2543, 2013.

[11]. S. Wan, Y. Lu, X. Yan, and L. Liu, "Visual secret sharing scheme with (k, n) threshold based on QR codes," IEEE Mobile Ad-Hoc and Sensor Networks (MSN), 2016 12th International Conference, pp. 374-379, December, 2016.

[12]. P. Y. Lin, "Distributed secret sharing approach with cheater prevention based on QR code," IEEE Transactions on Industrial Informatics, vol. 12, no. 1, pp. 384-392, Feb. 2016.

[13]. Y. W. Chow, W. Susilo, G. Yang, J. G. Phillips, I. Pranata, and A. M. Barmawi, "Exploiting the error correction mechanism in QR codes for secret sharing," Australasian Conference on Information Security and Privacy, pp. 409-425, 2016.