IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 7, Issue 8, August 2019

Enhanced Security of System using Visual Cryptography

V.Rajeswari[1], V.Uthaman[2]

M.Phil[1]

M.C.A, M.Phil., S.E.T[2]

Abstract: Different color patterns of Quick Response (QR) codes, such as RGB, grayscale, and binary QR codes, are widely used in applications. In this paper, we propose a novel XOR-Based Visual Secret Sharing (VSS) scheme using grayscale QR codes as cover images and binary QR code as secret image. First, all the code words of the secret QR code image are encoded into temporary binary QR code images, which are substituted for the second significant bit planes of the grayscale QR code cover images to generate shares. Each share is a grayscale QR code image, which can be decoded by a standard QR code decoder, so that it may not attract the attention of potential attackers when distributed in the public channel. The secret image can be recovered by XORing the code words regions of QR codes which are extracted from the second significant bit planes of the grayscale shares. More importantly, the proposed scheme is robust to JPEG compression, addition of different noises, rotation, resizing, and cropping, which is useful in practice. The effectiveness and robustness of our scheme are shown by the experimental results. The application of QR code is suitable for wireless multimedia data security.

Keywords: QR Codes, (N, N) Threshold XOR-Based VSS, Visual Cryptography

I. INTRODUCTION

Quick Response(QR) code is a kind of two-dimensional matrix codes used widely in all walks of life recently, for the advantages of its speed reading, error correction capability, multiple-format data representing, high capacity compared to one-dimensional codes, and so on. And the application of QR code is suitable for wireless multimedia data security. QR code image is a binary image in general, each pixel in the image has only two possible values or gradation levels, which is represented by Black and White (B&W) or monochrome image. By graying binary QR code image, we can obtain grayscale QR code image. Each pixel of grayscale QR code image takes up 8 bits of storage space. Keeping the most significant bit plane of the grayscale QR code image unchanged and then replacing the other less significant ones with secret bits could implement information hiding in grayscale QR code image.

The main idea of Visual Cryptography (VC) [1], also known as Visual Secret Sharing (VSS), is to split a secret image into numerous shares (also called share images or shadow images). Each share reveals no information on the original secret image separately, and only a specific amount of qualified shares could reconstruct the secret image. The secret image would be lost when storing and transmitting in a single image carrier which could be damaged easily, so that we may fail to extract the secret image. But, VSS can overcome the problem to a certain degree [2].

The threshold-based VSS was first proposed by Shamir [3] and Blakley [4]. Sharing one binary secret image into n corresponding random shares and then distributing them to n participants are the way to share. More than or equal to k shares are superimposed to reveal the secret image visually. However, less than k participants would reveal no information on the original secret image by stacking or inspecting their shares. The advantage of VSS in [1] is that it is easier to recover the secret image by stacking a specific amount of shares using HVS without any cryptographic knowledge and computations. However, the characteristics of pixel expansion and codebook (basic matrices) design may be be problematic in some situations.

Since Kafri and Keren proposed Random Grid (RG)-based VSS [5–7], it has received much more attention, in which the pixel expansion problem is not exist and codebook design is not required. The secret image is shared into noise-like shares with the same size of the secret image. The decryption method is the same as traditional VSS, i.e., stacking. However, the background of the reconstructed image becomes darker and darker when more and more shares are stacked in OR-based VSS (OVSS) based on RG.

XOR-based VSS (XVSS) can solve the problem of RG-based OVSS [8], since the decryption method is to perform XOR operation on the shares with a light weight computational device to reconstruct the secret image. By applying the XVSS, better image contrast and quality can be obtained [6, 9].

Due to the advantage of VSS and QR code, some combinations of them have been proposed by many researchers recently. Jonathan and Yan [12] authenticated the shares using a QR code. Wang et al. [13] proposed a scheme through

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 7, Issue 8, August 2019

embedding QR codes into the best region of given shares to prevent cheating. Chow et al. [11] proposed a (n, n) threshold scheme for cases that n is no less than 3, in which the secret image and cover images are all binary QR codes with the same version and the same level of error correction. Wan et al. [10] proposed a scheme that deeply integrated the QR code error correction mechanism with the theory of VSS and the region shared with the secret image is continuous. Chen et al. [14] proposed a VSS scheme with high security and flexible access structures for QR code applications. Chow et al. [15] investigated a method to distribute shares through embedding them into QR codes cover by a secure way using cryptographic keys. However, robustness is not considered in the above mentioned schemes, which is important in practice. The threshold is greater than 2 in [11], and the problem of image quality uniformity is not taken into account in paper [10].

Nowadays, more and more QR codes are used on mobile phones. A possible scenario to convey secret information securely in the network is described below. It is unsafe to transmit secret information in the public channel without protection, and mobile devices are widely used nowadays. Thus we encode secret information in QR code, which is shared into n different QR code cover images to generate n corresponding shares. Then the shares are transmitted in different channels over a network from one mobile phone to anther mobile phone. When JPG compression and recoding, Gaussian noise and other image attacks occur during the transmission, if the shares are robust to the attacks, secret information would be recovered, while less than n shares cannot reveal any information on the secret image. The decoding results of shares are identical with those of cover images, so they will not come into notice.

The schemes above are not suitable for the scenario. So, we propose a novel robust secret sharing scheme for (n,n) threshold that is not less than 2. This scheme integrates the QR code error correction mechanism with the theory of XVSS, and all the QR codes are with the same version and level of error correction. First, all the code words of a secret QR code image are encoded into n temporary binary QR code images. Then the n temporary binary QR code images are substituted for the second significant bit planes of the grayscale cover QR code images to output n shares. The selection of code words of secret QR code is random and each share can be decoded by a standard QR code reader, which can reduce the likelihood of suspicion and potential attacking. Since the modifications of grayscale QR codes are the second significant bit planes and the error correction mechanism of QR code, the scheme is robust to the conventional image attacks.

The rest of the paper is organized as follows. QR codes and XOR-based VSS are introduced in Section 2. The secret image sharing, recovering algorithm, and analyses are described in Section 3. Section 4 demonstrates the experimental results, comparisons and test. Finally, Section 5 is the conclusion of this paper.

QR Codes

A QR code symbol [17] consists of a square array consisting of square modules, which is developed by Denso Corporation of Japan in September 1994. The standard [16] defines forty versions of QR code versions ranging from version one to version forty. Different versions of QR code are comprised of different quantities of modules. QR code version 1 is made up of 2121 modules. From version 1, each version has 4 modules per side more than the previous version. For example, version 7 is made up of 4545 modules.

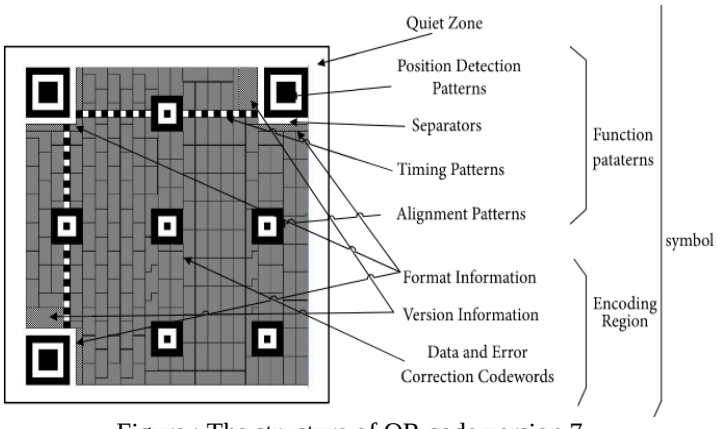

Figure : The structure of QR code version 7

A QR code [16] consists of functional patterns and encoding regions. The encoding region includes data and error correction codewords, format information and version information. The functional patterns consist of alignment, timing, finding patterns, and separation. The amounts of data and error correction codewords and error correction blocks are relying on the version and level of error correction of the QR code. The quiet zone is the blank region around QR code that is important for reading the QR code, encoding input data stream into an array of data codewords with 8-bits length. Error correction codewords also with 8-bits length are generated by using Reed-Solomon error control

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 7, Issue 8, August 2019

algorithm which is added to the back of the data codewords. Depended on the QR version and the level of error correction, data codewords and error correction codes are arranged in different error correction blocks. The level of error correction is divided into four categories: L ~ 7% , M ~ 15% , Q ~ 25%. The higher the level of error correction is, the stronger the error correction ability will be. But, high level of error correction requires larger QR version to encode the same input data stream, since the proportion of error correction codewords is larger than lower level in the same version.

(n,n)Threshold XOR-Based VSS:

The scheme of (n,n) threshold XOR-based VSS is to share a secret image into n corresponding noise-like shares in n participants and each share in every participant is different from each other

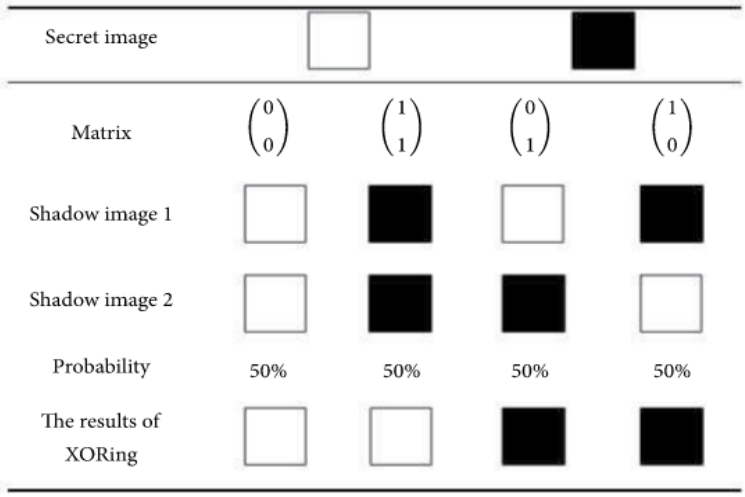

Figure :(2 , 2) XOR-based VSS application

Then, the secret image can recover losslessly only by XORing n shares with a computational device with XOR ability. Less than n participants cannot obtain any information about the original secret image by inspecting or stacking their shares.

II. PROPOSED SYSTEM

In this section, we propose an (n,n) threshold XVSS scheme based on QR code. The secret image is a binary QR code, whose codewords are all shared into the codewords of n different binary QR codes with the same version and level of error correction, where their functional patterns are the same. All codewords of the secret image are shared with the theory of XVSS. Then the n binary QR codes are substituted for the second significant bit plane of n grayscale QR code cover images with the same version and level of error correction to generate n grayscale QR code shares.

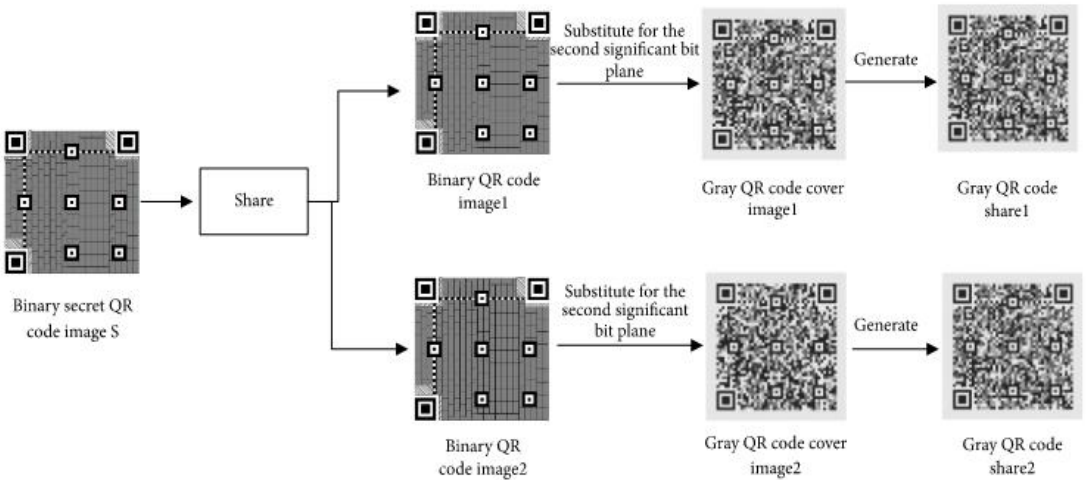

Figure: The idea of the grayscale QR code shares generation in our (2,2) threshold scheme.

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 7, Issue 8, August 2019

The messages in grayscale cover images are different from each other, the grayscale QR code shares can be decoded by a standard QR code decoder. The secret QR code image can be recovered by extracting the secondary significant bit planes of n gray QR code images to generate n binary QR code images firstly and then XORing white and dark modules in the codewords region of n the binary images, adding the functional patterns, version, and format information later. All the codewords can be recovered and the decoding result of the reconstructed secret image is identical with that of the secret image. Since the version and level of error correction of all the QR codes are the same, codewords are at the same position and functional pattern are the same. Taking the (2,2) threshold scheme as an example, Figure 3 illustrates the grayscale QR code shares generation of the proposed scheme. The secret QR code image can be recovered by extracting the secondary significant bit planes of n gray QR code images to generate n binary QR code images firstly and then XORing white and dark modules in the codewords region of n the binary images, adding the functional patterns, version, and format information later. All the codewords can be recovered and the decoding result of the reconstructed secret image is identical with that of the secret image. Since the version and level of error correction of all the QR codes are the same, codewords are at the same position and functional pattern are the same. Taking the (2,2) threshold scheme as an example, Figure 3 illustrates the grayscale QR code shares generation of the proposed scheme.

2.1 The Sharing Phase:

When sharing the secret QR code image into arbitrary binary QR code images, we only encrypt the codewords region while other parts are identical with the binary QR code images, then replace the second significant bit planes of the grayscale QR code cover images with the encrypted binary QR code images. All the QR code images have the same version and level of error correction. The codewords of the secret QR code are divided averagely and shared randomly into n different temporary binary QR code images. The artificial modification of shares is not perceptible. The shares can be decoded by a standard QR code.

2.2 The Recovery Phase:

Base on XORing operation, the data of the recovery QR code image could be lossless. Suppose that n grayscale shares are provided, we can get the pixels in the second significant bit planes from shares to create n binary QR code images. Then we read the version and level of error correction by a QR decoder. We perform XOR operation on the encoding regions of n binary images, after that putting the bits in other regions based on the version and level of error correction. In this way, we can create a QR code image whose message is the same as that of the secret image.

2.3 Analyses:

In this section, we present some theoretical analyses about the properties of our scheme. The grayscale shares are generated by replacing the secondary planes with the binary QR codes in which shared the secret image by Algorithm 1, when a QR code decoder reading the grayscale QR code, thresholding the grayscale image in the first place. The thresholding way in different QR code decoder may be not the same, but the simplest and common one is to set the number of 128 as the threshold, so when remaining the most significant digits of the pixel values in grayscale QR code cover images unchanged, the grayscale shares could be decoded. If the 6 bits behind the secondary bit of each pixel value are changed in the range from 000000 to 111111, the value in the secondary bit will not be changed. So when the last 6 bits are kept in the range from 000000 to 111111 although some noise added, the second significant bit plane replaced with secret image will not be affected, and the secret image can still be rebuilt. Because QR codes have the ability to correct errors, even if the modules are damaged or dirty in the error correction capacity range, the secret QR image could be decoded.

2.4 Image Illustration:

The reconstructed secret QR code image S' performing XOR operation on the codewords region of QR code image in the second significant bit planes of shares, then adding the functional patterns, version and format information together. The shares and the reconstructed secret image could be decoded by a QR code decoder, The decoding result of the reconstructed secret image is identical with that of the secret QR code image.

Result analysis

Figure 1: Qr code

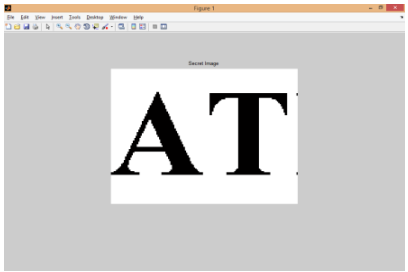

Figure: secrete data

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 7, Issue 8, August 2019

The QR code is generated based on encryption algorithm, secret data generated using visual cryptography

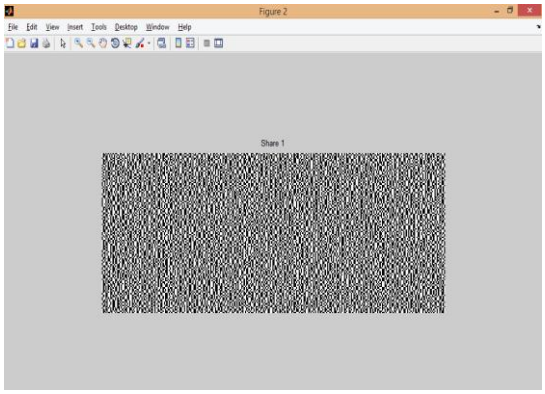

Figure: share 1

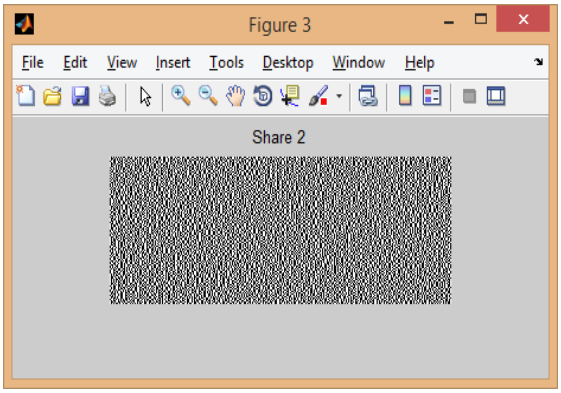

Figure: share 2

III. CONCLUSION

This paper proposed a novel robust VSS scheme applying to QR code. In this scheme, all the codewords of the secret QR code image are split into temporary binary QR codes randomly with the theory of XOR-based VSS, so shares with high image quality and high imperceptibility can be achieved in the end. Each share in our scheme can be decoded by a QR code decoder when distributing via public channels, which would avoid the attentions from potential attackers. Since all the images are QR codes, which have their own abilities to correct errors, and the plane modification is the second significant bit plane of the grayscale image, our scheme is robust to conventional image attacks, such as rotation, JPEG compression, Gaussian noise, resizing and cropping, when reconstructing the secret image, performing XOR operation on the bits of the codewords region in the second significant planes of the grayscale shares and adding the functional patterns, version, and format information together. There are no wrong codewords in the reconstructed secret QR code image, so the message of which is identical with that of the original secret image. The reduction of the size of the shares will be the future work.

REFERENCES

1. M. Naor and A. Shamir, "Visual cryptography," in Advances in Cryptology—EUROCRYPT'94, vol. 950 of Lecture Notes in Computer Science, pp. 1–12, Springer, Berlin, Germany, 1995. View at Publisher · View at Google Scholar · View at MathSciNet
2. C.-N. Yang and D.-S. Wang, "Property analysis of XOR-based visual cryptography," IEEE Transactions on Circuits and Systems for Video Technology, vol. 24, no. 2, pp. 189–197, 2014. View at Publisher · View at Google Scholar · View at Scopus
3. A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612-613, 1979. View at Publisher · View at Google Scholar · View at MathSciNet · View at Scopus
4. G. R. Blakley, "Safeguarding cryptographic keys," in AFIPS, 1979.
5. X. Yan, S. Wang, and X. Niu, "Threshold construction from specific cases in visual cryptography without the pixel expansion," Signal Processing, vol. 105, pp. 389–398, 2014. View at Publisher · View at Google Scholar · View at Scopus
6. X. Yan, X. Liu, and C.-N. Yang, "An enhanced threshold visual secret sharing based on random grids," Journal of Real-Time Image Processing, vol. 14, no. 1, pp. 61–73, 2018. View at Publisher · View at Google Scholar · View at Scopus
7. X. Yan and Y. Lu, "Participants increasing for threshold random grids-based visual secret sharing," Journal of Real-Time Image Processing, vol. 14, no. 1, pp. 13–24, 2018. View at Publisher · View at Google Scholar
8. X. Wu and W. Sun, "Random grid-based visual secret sharing with abilities of or and XOR decryptions," Journal of Visual Communication and Image Representation, vol. 24, no. 1, pp. 48–62, 2013. View at Publisher · View at Google Scholar · View at Scopus
9. P. Tuyls, H. D. Hollmann, J. H. van Lint, and L. Tolhuizen, "Xor-based visual cryptography schemes," Designs, Codes and Cryptography. An International Journal, vol. 37, no. 1, pp. 169–186, 2005. View at Publisher · View at Google Scholar · View at MathSciNet
10. S. Wan, Y. Lu, X. Yan, and L. Liu, "Visual Secret Sharing Scheme with (k, n) Threshold Based on QR Codes," in Proceedings of the International Conference on Mobile Ad-Hoc and Sensor Networks, MSN '17, 2017. View at Scopus
11. 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," in Proceedings of the Australasian Conference on Information Security and Privacy, 2016.
12. J. Weir and W. Yan, "Authenticating Visual Cryptography Shares Using 2D Barcodes," in Proceedings of the 10th International Workshop on Digital Forensics and Watermarking, IWDW '11, pp. 196–210, Springer, Atlantic City, NY, USA, 2011. View at Publisher · View at Google Scholar
13. G. Wang, F. Liu, and W. Q. Yan, Barcodes for Visual Cryptography, Kluwer Academic Publishers, 2016.
14. Y. Cheng, Z. Fu, and B. Yu, "Improved Visual Secret Sharing Scheme for QR Code Applications," IEEE Transactions on Information Forensics and Security, vol. 99, p. 1, 2018. View at Publisher · View at Google Scholar
15. Y. W. Chow, W. Susilo, J. Tonien, E. Vlahu-Gjorgievska, and G. Yang, "Cooperative Secret Sharing Using QR Codes and Symmetric Keys," Symmetry, vol. 10, no. 4, p. 95, 2018. View at Publisher · View at Google Scholar