ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

Improved Visual Secret Sharing Scheme for Multi-Color QR Code Application

Nikita Jalkote[*1], NishaJadhav[*1], Ashwini Kendre[*1], Karishma Khade[*1], Dipali Pawar[*2]

Student, Department of Information Technology, Sinhgad Institute of Technology and Science, Narhe, Pune, SPPU, Maharashtra, India[*1]

Assistant Professor, Department of Information Technology, Sinhgad Institute of Technology and Science, Narhe, Pune, SPPU, Maharashtra, India[*2]

ABSTRACT: The QR code was intended for storage data and fast reading applications. Quick Response (QR) codes were extensively used in fast reading applications such as statistics storage and high-speed device reading. Anyone can gain get right of entry to data saved in QR codes; hence, they're incompatible for encoding secret statistics without the addition of cryptography or other safety. This paper proposes a visual secret sharing scheme to encode a secret QR code into distinct shares. In assessment with other techniques, the shares in proposed scheme are valid QR codes that may be decoded with some unique that means of a trendy QR code reader, so that escaping increases suspicious attackers. In addition, the secret message is recovered with the aid of XOR-ing the qualified shares. This operation which can effortlessly be achieved the use of smartphones or different QR scanninggadgets. Contribution work is, to maximize the storage size of QR code and generating multi-colored QR code. Experimental results show that the proposed scheme is feasible and cost is low. Proposed scheme's high sharing performance is likewise highlighted in this paper.

KEYWORDS: Division algorithm, error correction capacity, high security, (k, n) access structure, Quick Response code, visual secret sharing scheme

I. INTRODUCTION

In recent years, the QR code is widely used. In daily life, QR codes are used in a variety of scenarios that include information storage, web links, traceability, identification and authentication. First, the QR code is easy to be computer equipment identification, for example, mobile phones, scanning guns. Second, QR code has a large storage capacity, anti-damage strong, cheap and so on.

Specific QR code structure

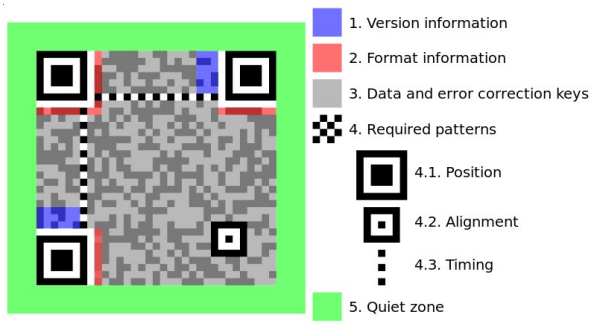

Fig. 1 Specific QR Code Structure

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

As represented in Fig. 1, the QR code has a unique structure for geometrical correction and high speed decoding. Three position tags are used for QR code detection and orientation correction. One or more alignment patterns are used to code deformation arrangement. The module get it together is set by timing patterns. Furthermore, the format information areas contain error correction level and mask pattern. The code version and error correction bits are stored in the version information areas.

The popularity of QR codes is primarily due to the following features:

- QR code robust to the copying process,
- It is easy to read by any device and any user,
- It has high encoding capacity enhanced by error correction facilities,
- It is in small size and robust to geometrical distortion.

Visual cryptography is a new secret sharing technology. It improves the secret share images to restore the complexity of the secret, relying on human visual decryption. Compared with traditional cryptography, it has the advantages of concealment, security, and the simplicity of secret recovery. The method of visual cryptography provided high security requirements of the users and protects them against various security attacks. It is easy to generate value in business applications. In this paper, proposed a standard multi-color QR code using textured patterns on data hiding by text steganography and providing security on data by using visual secret sharing scheme.

II. MOTIVATION

The motivation of the work is to propose the storage capacity can be significantly improved by increasing the code alphabet q or by increasing the textured pattern size. It increases the storage capacity of the classical QR code. It provides security for private message using visual secret sharing scheme.

III. STATE OF ART

The paper proves that the contrast of XVCS is $2^{(k-1)}$times greater than OVCS. The monotone property of OR operation degrades the visual quality of reconstructed image for OR-based VCS (OVCS). Accordingly, XOR-based VCS (XVCS), which uses XOR operation for decoding, was proposed to enhance the contrast. Advantages are: Easily decode the secret image by stacking operation. XVCS has better reconstructed image than OVCS. Disadvantages are: Proposed algorithm is more complicated.

In paper, present a blind, key based watermarking technique, which embeds a transformed binary form of the watermark data into the DWT domain of the cover image and uses a unique image code for the detection of image distortion. The QR code is embedded into the attack resistant HH component of 1stlevel DWT domain of the cover image and to detect malicious interference by an attacker. Advantages are: More information representation per bit change combined with error correction capabilities. Increases the usability of the watermark data and maintains robustness against visually invariant data removal attacks. Disadvantages are: Limited to a LSB bit in the spatial domain of the image intensity values. Since the spatial domain is more susceptible to attacks this cannot be used.

In paper, design a secret QR sharing approach to protect the private QR data with a secure and reliable distributed system. The proposed approach differs from related QR code schemes in that it uses the QR characteristics to achieve secret sharing and can resist the print-and-scan operation. Advantages are: Reduces the security risk of the secret. Approach is feasible. It provides content readability, cheater detectability, and an adjustable secret payload of the QR barcode. Disadvantages are: Need to improve the security of the QR barcode. QR technique requires reducing the modifications.

The two-level QR code (2LQR), has two public and private storage levels and can be used for document authentication . 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. Advantages are: It

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

increases the storage capacity of the classical QR code. The textured patterns used in 2LQR sensitivity to the P&S process. Disadvantages are: Need to improve the pattern recognition method. Need to increase the storage capacity of 2LQR by replacing the white modules with textured patterns.

To protect the sensitive data, paper explores the characteristics of QR barcodes to design a secret hiding mechanism for the QR barcode with a higher payload compared to the past ones. For a normal scanner, a browser can only reveal the formal information from the marked QR code. Advantages are: The designed scheme is feasible to hide the secrets into a tiny QR tag as the purpose of steganography. Only the authorized user with the private key can further reveal the concealed secret successfully.
Disadvantages are: Need to increase the security.

IV. PROPOSED WORK

In this paper, an innovative scheme is proposed to improve the security of QR codes using the XVCS theory. First, an improved (n, n) sharing method is designed to avoid the security weakness of existing methods. On this basis, consider the method for (k, n) access structures by utilizing the (k, k) sharing instance on every k-participant subset, respectively. This approach will require a large number of instances as n increases. Therefore, presents two division algorithms to classify all the k-participant subsets into several collections, in which instances of multiple subsets can be replaced by only one.

- Enhanced (n, n) sharing method
- (k, n) sharing method

Based on the enhanced (n, n) method, a (k, n) method can be achieved if we apply the (k, k) instance to every k-participant subset of the (k, n) access structure. However, there will be a huge amount of (k, k) instances.
Advantages are:

- Secure encoding of document or text.
- Text steganography for message encoding.
- Increases the sharing efficiency.
- VCS is low computational complexity.
- Higher security and more flexible access structures.
- Computation cost is less.
- stego synthetic texture for QR code hiding.

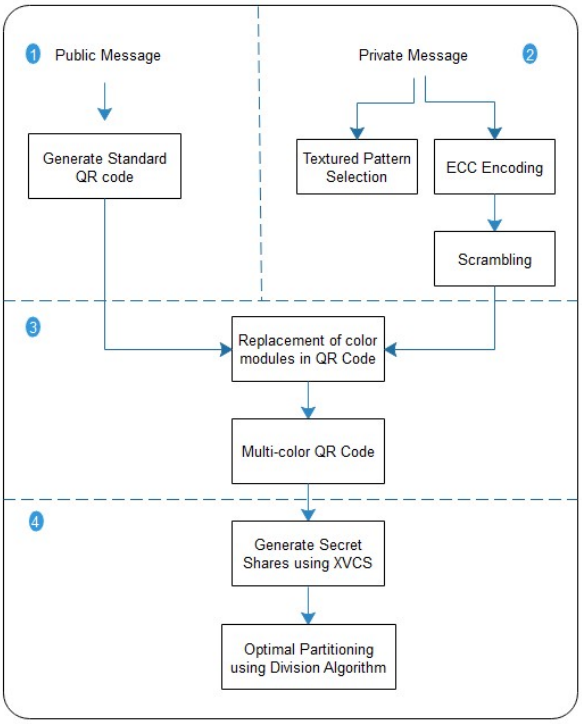

Fig. 2 Proposed System Architecture

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

V. MATHEMATICAL MODEL

Two collections of $n \times 1$ Boolean matrices denoted by C^0 and C^1 consist of an (n, n)-XVCS if the following conditions are satisfied:

) $If\ X = P, then\ \forall B \in C^0(C^1), w(B_P) = 0(1).$

) $If\ X \subseteq P\ and\ X \subseteq P, then\ \forall B \in$

$or\ C^1;\ the\ possibilities\ of\ w(B_X) =$

$w(B_X) = 1\ are\ equal.$

1

2

C^0

$0\ and$

(2)

The first property is contrast, which illustrates that the secret can be recovered by XOR-ing all participant shares. The second property is security, which prevents any k ($k < n$) participants from gaining any knowledge of the secret.

Enhanced (n, n) sharing method

Define two blocks B_1 and B_2 belong to an identical group G if $B_1 = B_2$ is satisfied.

(3)

With above definition, we can divide $T_1^q, T_2^q, \dots, T_n^q$ into several groups $G_1^q, G_2^q, \dots, G_u^q$. For example, to determine whether T_1^q and T_2^q are of a same group, we calculate $T_1^q \oplus T_2^q$. If $T_1^q \oplus T_2^q = 0$, we can conclude that T_1^q and T_2^q are of an identical group, and vice versa. A block different from any other blocks will not be contained in any group.

$T^q(i)$ is said to be responsible for $S^q(i)$ if $T^q(i,j)$ is reversed to share $S^q(i,j)$.

Let $X_{ki} = 1$ denote the case that $T_k^q(i)$ is responsible for $S^q(i)$ and let $X_{ki} = 0$ represent the opposite. A matrix X is constructed by solving (1).

$$X = \begin{bmatrix} \overbrace{x_{11}\ x_{12} \cdots x_{1d}\ 00 \cdots 0}^{c} \\ x_{21}\ x_{22} \cdots x_{2d}\ 00 \cdots 0 \\ \vdots\ \vdots\ \ddots\ \vdots\ \vdots\ \ddots\ \vdots \\ \underbrace{x_{n1}\ x_{n2} \cdots x_{nd}}_{d}\ \underbrace{00 \cdots 0}_{c-d} \end{bmatrix}$$

(4)

$$\begin{cases} \sum_{q=1}^{n} X_{pq} \le r (p = 1, 2, \dots, n) \\ \sum_{q=1}^{d} (X_{iq} | X_{jq}) \ge d - c + r + 1 (T \ne T_j^q \in G_k^q; k = 1, 2, \dots, u)_i^q \\ \sum_{q=1}^{d} (X_{1q} | X_{2q} | \quad nq) = d \\ X_{pq} \in \{0\ 1,\ \} (q = 1, 2, \dots \quad = 1, 2, \dots, n) \end{cases} \quad \begin{matrix} \\ \dots | X \\ , d; p \end{matrix}$$

If n satisfies the condition $n \times r \ge c - r$, there must be a solution to (1) when $d = c - r$. In addition, we can adjust the value of d $(c - r \le d \le c)$ to balance errors between the covers and the reconstructed secret. Based on X, we design a new sharing algorithm.

VI. CONCLUSION

In this paper, we proposed a visual secret sharing scheme for QR code applications, which makes improvement mainly on two aspects: higher security and more flexible access structures. In addition, we extended the access structure from (n, n) to (k, n) by further investigating the error correction mechanism of QR codes. Two division approaches are

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

provided, effectively improving the sharing efficiency of (*k*, *n*) method. Therefore, the computational cost of our work is much smaller than that of the previous studies which can also achieve (*k*, *n*) sharing method. The future work will make the QR code reader for scanned QR code within fraction of seconds.

REFERENCES

[1] 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.

[2] P. P. Thulasidharan, M. S. Nair, "QR code based blind digital image watermarking with attack detection code," *AEU - International Journal of Electronics and Communications*, vol. 69, no. 7, pp. 1074-1084, 2015.

[3] 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, 2016.

[4] I. Tkachenko, W. Puech, C. Destruel, *et al.*, "TwoLevel QR Code for Private Message Sharing and Document Authentication," *IEEE Transactions on Information Forensics & Security*, vol. 11, no. 13, pp. 571-583, 2016.

[5] P. Y. Lin, Y. H. Chen, "High payload secret hiding technology for QR codes," *Eurasip Journal on Image & Video Processing*, vol. 2017, no. 1,pp. 14,2017.