Document Sharing Using QR Code With Visual Secret Sharing Scheme

Miss. Anjali Pawar[1]
Department of Computer Engineering
MMCOE, Karvenagar
Pune, India

Prof. Harmeet Khanuja[2]
Department of Computer Engineering
MMCOE, Karvenagar
Pune, India

***Abstract*—QR code stands for quick response code. QR code is used to store information. Anyone can get access to the data present in QR code. They are unsuitable for storing secret data. This paper represents a visual secret sharing scheme to encode a secret QR code into distinct shares. Visual secret sharing scheme is a method of distributing secrete amongst a group of participants. The secret message is recovered with the aid of XOR-ing the shares. Secret message can be generated only when enough number of shares are combined. This provides security for private message using visual secret sharing scheme. Proposed system provides security to private messages and generates QR code. Experimental outcomes discover that the proposed scheme is feasible and computational cost is low. Proposed schemes high sharing performance is likewise recommended in this paper.**

***Index Terms*—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 broadly used. In daily life, QR codes are utilized in an assortment of situations that incorporate information storage, web links, traceability, identification and authentication. QR code are easy to use and having higher storage capacity. QR can store all types of data.

As represented in Fig. 1, the QR code has a unique structure for geometrical correction and decoding. There are three position tags in QR code. Position tags are used for detecting position of QR code. QR code consists of timing pattern which is used to determine the co-ordinate. Furthermore, the format information regions contain error correction level and mask pattern sample. When QR code size is large then alignment pattern helps with orientation. Version information identifies the QR code version that is being used.

Fig. 1. Specific QR Code Structure

TABLE I QR Code Structure Information

Pattern	Description
	Version Information
	Format Information
	Data and error correction keys
	Required Patterns
	Position tags
	Alignment Patterns
	Timing Patterns
	Quiet Zone

Quiet zone is used to differentiate QR code from its surrounding. Error correction bits are stored within version information. Data and error correction keys hold actual data popularity of QR codes is primarily due to the accompanying highlights:

- QR code can handle different type of data.
- It has high storage capacity.
- It allows direct marking on a product.
- It is in small size and robust to geometrical distortion.

Visual cryptography is another new secret sharing technology. It provides better security as compare to traditional technology. At receiver side we get required share only when adequate number of shares are placed together. The condition for share is that shares at senders side should match with shares at receivers side. It has the benefits of concealment, safety, and the simplicity of secret rebuilding. The method of visual cryptography protects QR code against diverse security attacks and provides higher security. It is simple to generate value in enterprise applications. In this paper, proposed system improves security of QR code using visual cryptography.

The paper [10] describes the details about QR code print-and-scan process to retrieve message details at fast rate. The paper [1], [2] studies the details about visual secret sharing and experimental performance analysis on division algorithms for secret sharing schemes on QR codes.

Motivation:

The motivation of work is to provide security for private messages in QR code by using visual secret sharing scheme. It increases storage capacity of classical QR code. The storage capacity can be improved by increasing textured pattern size.

II. REVIEW OF LITERATURE

The paper [1] presents visual cryptography scheme. Secret sharing scheme is used to generate shares. Decoding operation includes XORing of shares. It provides low computation complexity method for decryption process. Shares are image of QR code. It includes reconstruction of secret image.

The paper [2] proves that the contrast of XVCS is 2(k1) times greater than OVCS.XVCS is XOR based visual cryptographic scheme and OVCS is OR based visual cryptographic scheme. The monotone property of OR operation reduces the visual quality of reassembled image for OR-based VCS (OVCS). XVCS uses XOR operation for decoding whereas OVCS uses OR operation for decoding. Advantages of using XVCS is that it can easily decode the secret image by stacking operation. XVCS has better reconstructed image than OVCS. The limitation is that proposed algorithm is more complicated.

The paper [3] presents a visually impaired, key based watermarking technique which embeds a transformed binary form of the watermark data into the DWT domain of the cover image and uses an extraordinary image code for the identification of image distortion. DWT stands for discrete wavelet transform in which DWT coefficients are modified with the data representing watermark. The QR code is inserted into the attack- resistant part of first level DWT area of the cover image and to distinguish malicious interference by an attacker. Advantages are that more information representation per bit change combined with error correction capabilities and it increases the usability of watermark data and maintains robustness against visually invariant data removal attacks.

In paper [4] presents secure and reliable distributed system. The proposed methodology varies from related QR code schemes in that it utilizes the QR qualities to accomplish secret sharing. In this paper, secret sharing procedure and secret revealing procedure are present. Advantages is that it 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. 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 [5]. The public level is the the same standard QR code storage level; therefore, it is readable through any classical QR code utility. The private level is built by using changing the black modules through precise textured patterns. It increases storage capacity of QR code and distinguish the original document from its copy. Print and scan process produce visible and invisible image modification. Advantages are: It increases the storage capacity of the classical QR code. Limitation of this 2LQR code 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 secure the sensitive data, paper [6] investigates the qualities of QR codes to design a secret hiding mechanism for the QR code. Secret information is embedded into data codeword of QR tag. QR code reader is incapable of extracting secret information directly. The designed scheme is feasible to hide the secrets into a QR tag as the motivation of steganography. Only the authorized user with the private key can get the secret. Limitation is that there is need to increase the security.

The paper [7] refers the authentication problem of real - world goods on which 2D bar-codes (2D-BC) are printed.2D-BC is also called as data grid or data matrix .2D-BC consist of white and black images encoding identifier and printed on the goods package. After scanning 2D-BC a correlation score is computed and compared to determine whether the good is genuine or fake. Limitation is that it requires additional noise to generate fake barcode. Generating fake 2D QR code declared as original by QR code reader.

The paper [8] proposes strategy based on Reed-Solomon codes and list decoding for hiding secret information. Storing secret data dependent on bit technique is difficult. If an attacker changes any bit of hidden bits, it is far difficult to recover the secret data. In order to overcome above problem Reed-Solomon codes and list decoding are used in proposed system. Advantage: For attacker hard to discover original data. It provides higher security to secret data.

The paper [9] uses color QR code which is shown on the screen and recorded with camera equipped mobile phones. Proposed system assumes that there is no direct connection between devices. A Proposed technique offers optical information transfer between devices. 4D-codes uses color, height, time and width for encoding purpose. Advantage: Maximizes the data throughput and the robustness of the barcode recognition. Limitation is that data transfer rate is low compare to direct existing techniques.

The paper [10] proposes model for print and scan process. Proposed system uses properties of the undetermined, rescanned image in both the spatial and frequency areas, and after that further examines the adjustments in the Discrete Fourier Transform coefficients. Proposed system extracts invariants from coefficients. Several methods are used in this paper to separate invariants from coefficients. This model examines geometric distortion in print and scan process. Limitation is : Uses watermarking based authentication.

The paper [11] describes the proposed system can hide the secret data into the cover QR code without changing QR code content. Only the legal receiver can encrypt and retrieve the secret from the marked QR code. The secret payload of the designed scheme is alterable. The scheme can bring larger secret into a QR code which depends on QR code version. Advantage: Only the authorized receiver can encrypt and retrieve the secret from the marked QR code. Secret hiding mechanism used for QR code by encrypted payload.

A. Issues and challenges in literature survey:

In existing system security needs to be improved. The storage capacity of QR code is less. Encryption and decryption process is used to secure QR code but through this protecting confidential data is also challenging. Because it includes only

one level security. If we decrypt the data then we can get easily the data . Hence, achieving security is challenging.

A QR code is robust to segmental loss or symbol damage. Any user can access the information in QR codes; therefore, they are incapable of storing secret data. During the past few years, many efforts have been made to place and protect secret messages in QR codes. In existing system, one can get information through scanner but for private messages like bank details, employee details, security is required. QR code is robust to symbol damage.

Advantages of existing systems are as below:

Increase storage capacity of QR code along with differentiate original document.

Limitations of existing system are as below:

- QR codes are unsuitable for storing secret data.
- The computational cost is high.
- Data stored in a QR code is can be easily readable by a camera. It is impossible to classify an originally document in QR code from its copy due to their insensitivity to the Print and Scan process.

In comparison with existing system QR code can store around 255 characters that is in kilobytes while the storage capacity of proposed system is increased. In proposed system QR code can store data in megabytes. Classical QR code can gives result with small number of iterations while in proposed system multicolor QR code performs multiple iterations that produces accurate result .In existing system anyone can directly access QR code. There is no security for private messages in existing system but in proposed system visual secrete sharing scheme is used to provide security to private message .

In existing system (n, n) sharing method is used where n is the share generated in QR code. Shares are required in order to get result. But as in (n, n) sharing method it requires all shares to retrieve message while in proposed system it can use k shares to get result. Proposed system uses (k, n) sharing method where k is the minimum number of share required to retrieve message, k is less than n hence it will require shares which are less than existing system. Hence, the computation cost is low as compare to existing system.

III. PROPOSED 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 into participants. 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.

A. Architecture

The Fig.2 shows the proposed system architecture of document sharing using QR code with visual secret sharing scheme. The step 1 contains the public message directly generates

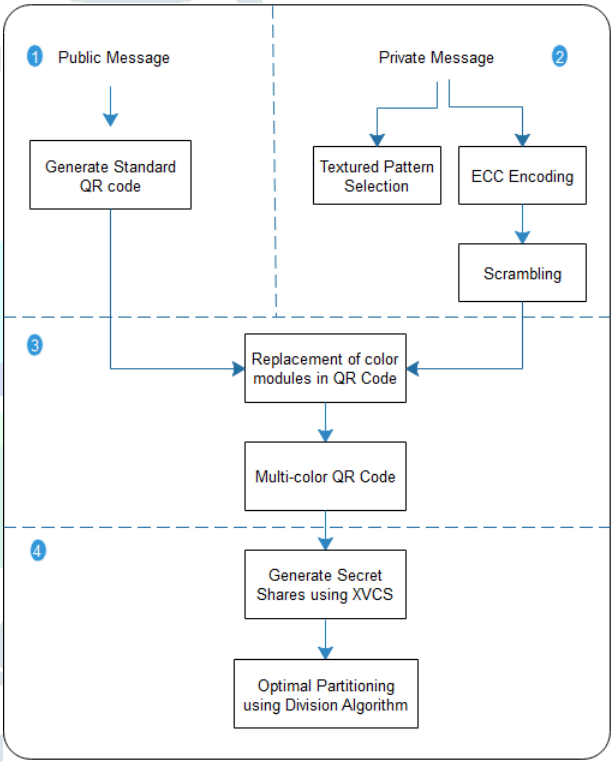

Fig. 2. Proposed System Architecture

the standard QR code. If you select the private message, first select the textured patterns. After applying the same step of generation QR code like, error correction code (ECC) encoding method and after, scrambling method which means one bit of position shifted to another bit position. At third step, apply the color modules using Reed Solomon code. Multicolor QR code is generated. The sender must give the input for generate secret parts at least 2 till maximum 10 size of secret parts. Apply the (k, n) sharing method. The reconstructed parts should be less than or equal to generated secret parts.

After applying the xor-ing based Visual Secret Sharing Scheme (XVCS) algorithm for generation of secret shares which are display like textual code, does not display original message contents. The optimal partitioning using Division algorithm is applied for secrets are generated in QR code format.

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.

B. Algorithms

1. Algorithm for creating QR code.

Encoding:-
Input to QR code is document or text.
Step 1: Representation of each letter in secret message which is document or text into its comparable ASCII codes.
Step 2: Conversion of ASCII code to comparable eight-bit binary number.
Step 3: Division of eight-bit binary number into two parts. Selection of suitable letters comparing to the four-bit parts.
Step 4: Meaningful sentence development by utilizing letters got in step 3.
Step 5: Omission of articles, pronoun, relational word, adverb, was/were, is/am/are, has/have/had, will/ shall and would/should in coding procedure to give adaptability in sentence development.

Decoding Algorithm for QR code
Step 1: First letter in each expression of cover message is taken and represented by corresponding four-bit number.
Step 2: Four-bit binary numbers are combined to get eight-bit number.
Step 3: Get ASCII code for each corresponding eight-bit.
Step 4: Secret message is recovered from ASCII codes.

2. Division Algorithm 2

Input: A collection of all k-participant subsets M_0. Output: Divided collections M_1, M_2, ..., M_d. (d is the number of collections)
Step 1: Let $i \leftarrow 1, d \leftarrow 0$ and go to Step 2.
Step 2: Randomly select a subset Q from M_0 and suppose $Q = \{i_1, i_2, ..., i_k\}$. Let $Q \in M_i$, and go to Step 3.
Step 3: Search the remaining subsets in M_0. If the model above remains solvable when we assume that $Q^j \in M_i$, then let $Q^j \in M_i$. Go to Step 4.
Step 4: Let $M_0 \leftarrow M_0 - M_i$, $d \leftarrow i$, $i \leftarrow i + 1$. If $M_0 \neq \varphi$, go to Step 2; else, go to Step 5.
Step 5: Algorithm ends.

C. Mathematical Model

Let us consider S as a set of document and text to encode in QR code.
S is a set of input, output and functions.

Let I be the set of inputs. Inputs are text and one document.

Let O be the set of outputs where outputs are QR code and list of secret images.

Let F be the set of functions.

Encode , compress ,decode and decompress are the set of functions used. Function encode is used to encode text or document. Function compress is used to compress encoded data Function decode is used to decode compressed data. Function decompress is used to decompress compressed data.

IV. RESULT AND DISCUSSIONS

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.
Input:

Fees: Admission Fees
Total: 5700.0
Name: Shilpa Tandale
Bank Name: Kotak Bank-
5678123323454567-
05/2022-732

Fig. 3. Input Private Message

Output:

Fig. 4. Multi-color QR code

Generate Secrets:

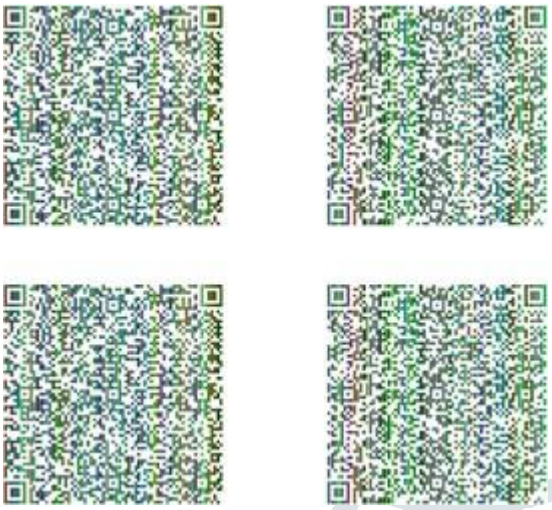

Fig. 5. Shares of private message

Here, n=4,k=3
Reconstruct the secret parts:

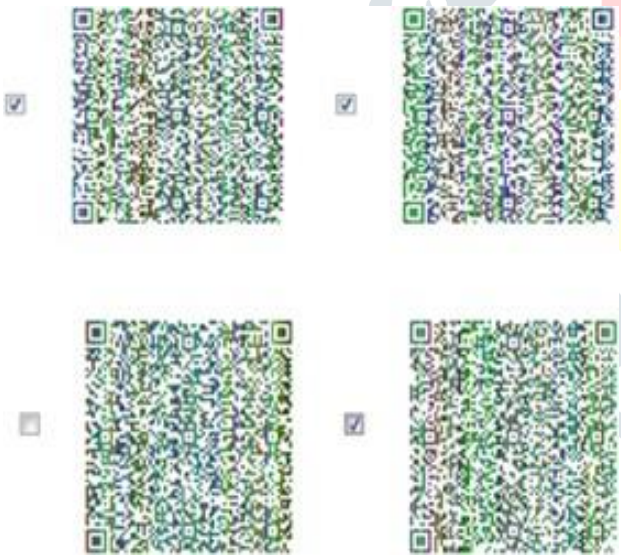

Fig. 6. Selection of shares at receiver

Receiver selects three shares to get original message. After combining three shares and decodes that and gets following original message.
Output:

Fees: Admission Fees
Total: 5700.0
Name: Shilpa Tandale
Bank Name: Kotak Bank-
5678123323454567-
05/2022-732

Fig. 7. Result Private Message

V. Conclusion

Proposed scheme for QR code makes improvement on security. It provides more flexible access structure. Division algorithm reduces the number of shares. Therefore, the computational cost of our work is much smaller than that of the previous studies.

References

[1] Y. Cheng, Z. Fu and B. Yu, "Improved Visual Secret Sharing Scheme for QR Code Applications," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 9, pp. 2393-2403, Sept. 2018.
[2] 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.
[3] 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.
[4] 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.
[5] I. Tkachenko, W. Puech, C. Destruel, et al., Two-Level QR Code for Private Message Sharing and Document Authentication, IEEE Transactions on Information Forensics & Security, vol. 11, no. 13, pp. 571-583, 2016.
[6] 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.
[7] C. Baras and F. Cayre, 2D bar-codes for authentication: A security approach, in Proc. 20th Eur. Signal Process. Conf. (EUSIPCO), Aug. 2012, pp. 1760-1766.
[8] T. V. Bui, N. K. Vu, T. T. P. Nguyen, I. Echizen, and T. D. Nguyen, Robust message hiding for QR code, in Proc. IEEE 10th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIH-MSP), Aug. 2014, pp. 520-523.
[9] T. Langlotz and O. Bimber, Unsynchronized 4D barcodes, in Proc. 3rd Int. Symp., ISVC 2007, Lake Tahoe, NV, USA, Nov. 2628, 2007, pp. 363-374.
[10] C.-Y. Lin and S.-F. Chang, Distortion modeling and invariant extraction for digital image print-and-scan process, in Proc. Int. Symp. Multimedia Inf. Process., 1999, pp. 1-10.
[11] P.-Y. Lin, Y.-H. Chen, E. J.-L. Lu, and P.-J. Chen, Secret hiding mechanism using QR barcode, in Proc. IEEE Int. Conf. Signal-Image Technol. Internet-Based Syst. (SITIS), Dec. 2013, pp. 22-25.