International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Implementation of QR Code for Sharing Files.

Anjali Pawar, Harmeet Khanuja

Abstract: ***QR code is a quick response code which is used to store information. In QR code, the information is stored in encoded form. To access information present in QR code , we need to decode information with the help of scanner. The information which is present in QR code is accessible to anybody. Private data is not safe in such scenario. This paper presents 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 by 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 higher security to messages and it also provides more flexible access structure. Computational cost of proposed scheme is low.***

Index Terms: Division Algorithm, (k, n) Access, Quick Response Code, Visual Secret Sharing Scheme

I. INTRODUCTION

QR code are used to provide information to customers and other individuals. In recent years, QR codes are used for multiple purposes. QR code are easy to use and having higher storage capacity. QR can store different types of data. QR code is machine readable label that contain information about the item to which it is attached.

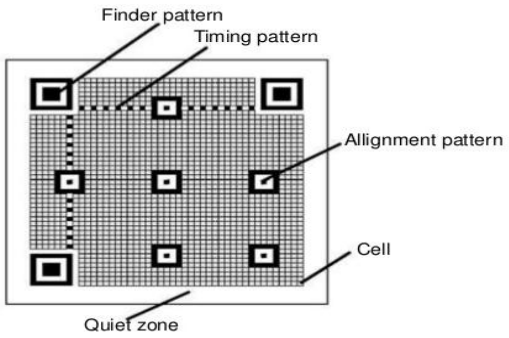

Fig 1. Structure of QR code

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
Anjali Pawar, Department Of Computer Engineering, Marathwada Mitra Mandal's College Of Engineering, Pune.
Harmmet Khanuja,, Department Of Computer Engineering, Marathwada Mitra Mandal's College Of Engineering, Pune..

In above Fig.1 QR code structure is explained. QR code structure consist of position pattern, alignment pattern ,timing pattern ,version information and quite zone. Position patterns detects position of QR code. Alignment pattern helps with orientation when QR code size is exceeding the limit. Timing pattern which is represented by dotted lines is used to determine the size of data matrix. The format information regions contain error correction method. When QR code size is large then alignment pattern helps with orientation. Different versions of QR code are used and version information in Fig.1 detects the version of QR code. Quiet zone is used for scanning purpose. Error correction bits are stored within version information. Actual data is present in data and error correction bits. QR code provides different kind of features which are listed below.

- QR code can handle all type of data
- It can store information in a very small amount of space and it is robust to distortion.
- QR code can be restored if some damage happens to QR code .
- It allows direct labelling on a product.

Visual cryptography secret sharing technology that is used to generate shares. The security provided by visual cryptography is better than traditional system. Secrets are nothing but the QR code which is divided into number of images . Sender specifies the number of secrets and threshold value. After generating secrets sender sends secrets to receiver. But at receiver end, secrets should match with secrets which are present at receiver end. If secrets are of same type then only receiver will get the original data. This method includes simplicity of secret rebuilding. Visual secret sharing method improve the security of existing system.
Motivation: To provide security for private messages in QR code by using visual secret sharing scheme is the main motivation of the work. To improve sharing efficiency of the system. It raises the storage capacity of classical QR code.

II. LITERATURE SURVEY

The paper [1] includes visual secret sharing scheme. Number of shares are generated by using secret sharing scheme. XOR-ing operation is used to combine shares. It provides low computation complexity. Watermarking technique is used which embeds watermark data into image. Shares are nothing but the image of QR code. The paper [2] compares XVCS and OVCS where XVCS stands for XOR based visual cryptographic scheme and OVCS stands for OR based visual cryptographic scheme. OR based operation diminishes the visual quality of image.

In XVCS decoding operation involves stacking. XVCS produces more better image as compare to OVCS. The limitation is that complexity of proposed algorithm increases. The paper [3] uses image code for recognition of image distortion. It presents watermarking technique that uses key for authentication. It includes more information per bit change with error correction capability. Watermark data is more useful and it prevents data removal attack. In paper [4] consist of secret sharing and secret revealing procedure. The proposed methodology uses distributed secret storage system. Secrets are distributed to different participants and they co-ordinate with each other to get original data. Participants are associated with QR tag. In revealing procedure, the procedure verifies participant before revealing secrets.It includes cheater detectability. Authentication is used to verify participant. Need to enhance the security of the QR barcode. The two-level QR code includes two public and private storage levels and they can be used for document authentication [5]. In public level documents are shared using classical QR code. Private levels include QR code which are built by replacing black modules by textual pattern. In private level storage capacity of QR code is increased. Print and scan process produce visible and invisible image structure. It is needed to improve the pattern recognition method. White modules can be replaced by textual pattern which will improve security of QR code . Paper [6] uses secret hiding mechanism and here secrets are embedded into QR tag. For each QR tag key is provided which will be used for extraction of data. Normal QR code reader is unable to retrieve data directly from QR tag. The designed scheme is flexible to hide the secrets into a QR tag. Only the authorized user can get secret. Private key is provided to user to retrieve secret. The paper [7] represents the authentication problem of real - world goods. It selects items on which two dimensional barcodes are printed. 2D-BC consist of white and black images encoding identifier and printed on the goods package. Scanning two -dimensional barcode result in correlation score. Correlational score identifies whether the product is genuine or fake. It requires additional noise to generate fake barcode which is the limitation of proposed scheme.

Issues and challenges in literature survey: In existing system there is no security for private data. The storage capacity of

QR code is also needed to improve. Although encoding and decoding of QR code data is their but by using QR code scanner it is possible to retrieve original data. Protecting confidential data is also challenging. Existing system includes only one level security. Achieving security is challenging in existing system. Segmental loss or symbol damage is possible in QR code. Any user can get the information present in QR codes. QR code are not capable of storing private data. One can get information through scanner in existing system but for private information like bank details, employee details, security is needed.

Limitations of existing system are as below:

- QR codes are not suitable for storing secret data.
- The computational cost is more.

Information stored in a QR code can be easily readable by a camera. It is impossible to classify an originally document in QR code from its copy. Comparison of proposed system with traditional system:

In existing system QR code can store data in kilobytes while the storage capacity of proposed system is increased. In proposed system QR code can store data in megabytes that is around 1 MB.

Classical QR code can gives result with less accuracy while in proposed system multiple iterations are done that produces more accurate result.

In proposed system visual secrete sharing scheme is used to provide security to private document.

In existing system (n, n) sharing method is used. In (n, n) sharing method, n is the share generated in QR code. But as in (n, n) sharing method n shares are compulsory to get the original document. In proposed method, (k,n) sharing scheme is used where k is the minimum number of share required at receiver side. If any one of secret is damaged in proposed system, other secrets can retrieve original document but that is not possible in existing system. Minimum number of secrets are used to produce original document so it will reduces the complexity.

Hence, the computation cost in proposed scheme is low as compare to existing system.

III. PROPOSED METHODOLOGY

An innovative scheme is proposed to enhance the security of QR codes using the XVCS theory. An improved (k, n) sharing method is designed to avoid the security weakness of QR code. In existing system (n,n) sharing method is used.Here ,n is the number of shares generated. Shares are combined in order to get information.

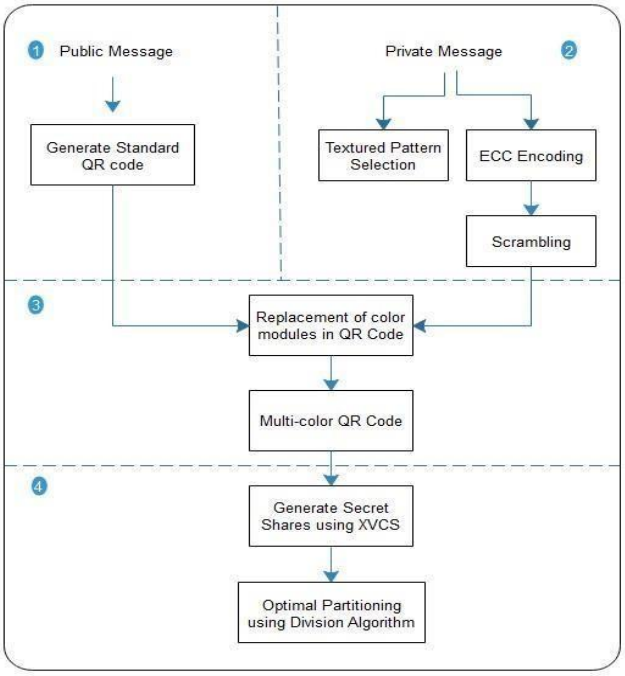

Fig.2 Proposed System Architecture

In (n, n) sharing method, all secrets are needed to get original document. In (k, n) access structure k and n are shares.to get original document. In (k, n) access structure k and n are shares. In (k,n) sharing method k is a threshold. Sender while sending secrets specify value of k and n and then send the secrets to receiver. At receiver side minimum k secrets are needed to get the original document. Algorithm for QR code generation is used where it includes encoding and decoding of QR code data. After getting QR code at sender side ,it will be divided into number of secrets. At receiver end, secrets are collected together to get the original document.

- Enhanced (n, n) sharing method
  In this method, QR code is divided into number of secrets and at receiver end requires all secrets to get the document.
- (k, n) sharing method
  In this method, QR code is divided into number of secrets and at receiver end requires at least k secrets.

A . Architecture

The Fig.2 shows the proposed system architecture of document sharing using QR code. The step first selects either public or private message. If one selects public message then it will create QR code and directly send it to receiver. In public message first it will generate standard QR code and then replacement of color modules will be done and finally generate multicolor QR code . If one select the private message and after selecting textured pattern it will result into QR code. After generating QR code replacement of color modules in QR code takes place. Multicolor QR code is generated after applying color modules. The sender gives the input for generation of secrets and also specify the value of k that is minimum number of secrets required to get original document. At receiver end it requires to combine at least k or more than k secrets but the value should be more than k and less than n.

Advantages of Proposed System:

1.Security is enhanced in proposed system and it provides more flexible access structure.
2.Computational cost is reduced in this system.
3.It includes secure encoding of private data.
4.Instead of (n,n) sharing method Proposed method uses (k,n) sharing scheme where n and k are shares.

Hence ,if any one of secret is destroyed then receiver can use other secret to get the original message which is not possible in existing system.

B. Algorithms

Module 1: Creating QR code
1]Algorithm for Encoding QR code data
Input to QR code is document or text message.

Step 1: Representation of secret message which is document or text into ASCII codes.

Step 2: Conversion of ASCII code to eight-bit binary number.

Step 3: Grouping of four bits together and select suitable letter for that four- bit number.

Step 4: Meaningful sentence formation by
taking letters got in step 3.

Step 5: Omission of relational word, adverb and articles in coding procedure to give adaptability in sentence development.

2]Collect encoded data into matrix and generate QR code
Step 1: Take one matrix and insert all encoded QR code data into matrix.
Step 2: Create buffered image and set all pixels to white.
Step 3. Check M[i,j] value in matrix where M,i,j are matrix ,row and column.
If M[i,j] is not equal to zero then goto step 4 else goto step 5 .
Step 4:Set different color for M[i,j].
Step 5: Generate color QR code.

Module 2: Generating secrets
1]Algorithm for generating secrets
Step1: Take input from above algorithm that is QR code image.
Step 2: Generate polynomial of degree (k-1) where k is threshold which is specified at sender side. Minimum number of secrets are indicated by k.
Step 3: Generate the transformation matrix.
Step 4: XOR image matrix with transformation matrix to produce encrypted image matrix.
Step 5: Send secrets to sender.

Module 3: Combining secrets .
Step 1: Collect all secrets into one array. Construct the polynomial from k secrets where k is threshold.
Step 2: Construct transformation matrix from polynomial.
Step 3: XOR transformation matrix with encrypted image matrix.
Step 4:Get QR code image.

Module 4: Decoding QR code
Algorithm for decoding 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.

IV. RESULTS

Input:
1.Select post type that is private in following case
2.Input private message
3. Specify number of parts to create at sender side and number of parts required to reconstruct the secret.

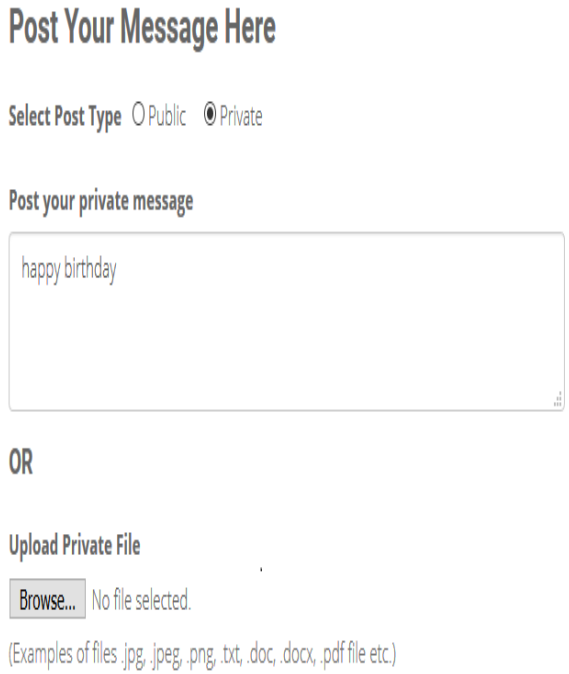

Fig 3. Input private data

Here, Input data is selected privately and after that sender is selecting number of parts and minimum secret required to get original data.

Fig 4. Secrets generated at sender side

Fig 5.Secrets generated at receiver side.

Output:

1.Receiver selects two secrets to get the original private data.
2.After combining two secrets receiver get original private data which is shown in Fig.4

Fig.6 Original private data.

V. CONCLUSION

QR code enhances security by using visual secret sharing scheme. In this system (k,n) sharing method is used instead of (n,n) sharing method where n and k are number of shares. As we are using (k,n) sharing method the computational cost of our work is much smaller than that of the previous studies. It provides more flexible access structure .

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.

AUTHORS PROFILE

Mrs.Anjali Pawar, studying ME in computer engineering at Marthwada Mitra Mandal's College Of Engineering, Pune.Works on QR code to provide security to information.

Prof. Harmeet Khanuja, works as Professor in Marathwada Mitra Mandal's College Of Engineering, Pune.She is pursuing PhD in computer engineering.