iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** III **Month of publication:** March 2019

DOI: http://doi.org/10.22214/ijraset.2019.3079

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

Upgraded Optical Secret Sharing Strategy for QR Code Approach

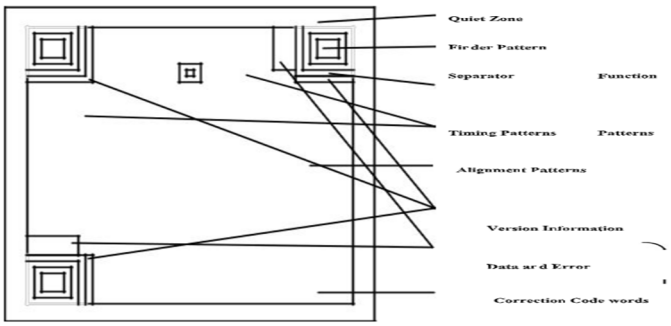
Mrs. S. Hemamalini[1], B. Ahalya[2], S. Sagaya Roshini3
[1]*Associate professor,* [2,3]*UG Student, Department of CSE, Computer Science Department Panimalar Institute of Technology Chennai*

Abstract: ***For Application such as data storage and high speed machine reading Quick Response (QR) code have been widely used. Access to the QR code is given to all those using it; therefore, encoding the information without using the cryptography or some protection algorithm is unsuitable in this paper we propose a visual secret sharing which divides the images into n-shares and decode the image with that n-shares. In Contrast with other techniques the share in our scheme are valid QR codes, by a standard QR reader that can be decoded with some specific meaning, thereby avoiding the raising issue with the potential attacker. By XOR-ing the qualified shares the secret message is recovered, this operation can be easily performed with the android smartphones or other QR code scanning devices. In proposed work, we implemented the AES Algorithm for encryption. To split the encrypted data into several shares, we proposed Division Algorithm.***

Keywords: Division Algorithm, Error Correction Capacity, High Security, (k,n) Access Structure, Quick Response Code, Visual Secret Sharing Scheme

I. INTRODUCTION

Compared with one-dimensional code two-dimensional codes, such as QR codes, offers greater data storage because they allow more wide spread application. The Japanese Denso-wave Company originally designed the QR code and since adopted as a universal standard specification published information transmission channel and this leads to online to offline mode of QR code information transmission channel and this leads to online to offline mode of QR code access into promising trends. According to a QR code is robust to segmental loss or symbol damage [1]. Any user can have the access to the QR code so it is unsuitable for storing the secret information, for the past few years many efforts have been taken to place and protect secret message in the QR code. Among that some scholars has used stenography or watermarking techniques[2].



These studies embed a QR code as a secret into mask image; or treat it as a mask to hide the information. Transformation to one specified domain is required for the secret extraction of both the technique, such as DCT or DWT. A polynomial algorithm was shared in for the secret sharing method, in this the QR codes are conveyed in the form of shadow [3]. In this scheme the QR code is act as a carrier to transfer shadow information and its message is meaningless. The author presented a scheme that resist the print and scan operation and it will easily detect the chapter[4]. For two-level message sharing and document authentication a novel QR code was designed, in this the hash function is performed to decrypt the secret[5]. Compared to the Boolean operations, the computational overhead as all the aforementioned schemes is slightly larger.

As a secret image sharing category, the concept of visual secret sharing scheme was first proposed by Naor and shamir. A secret image is divided in to n shares in (k,n)-VCS, when they are super imposed to human vision any K-share can obtain the secret. No information about the secret image can be revealed if the possession is less than the K-level, Later introduced a special type of VCS, termed the XOR based VCS, in which the recovery process is based

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

II. RELATED WORD

Weir and yan used a QR code to implement share authentication by embedding a QR code as a part of the share. To reduce the influence of secret revelation, a method was proposed in that sought the best embedding region for a given share[7]. In addition a continuous -tone VCS was developed for intended authentication on certain application on smartphone. Due to the meaningless shares of the scheme it is likely to be suspected by the potential attackers when disturbed via a public channel. A (k,n)-VCS with QR code shares are designed in, where the QR code is not the secret image and had to be decoded by the human vision[8]. For intelligent and automatic user experiences QR code are used in most of the cases. This type of schemes become the prefered approach, when the smartphone became popular, because its reconstructed secrets can be directly read by the machine. However the access structure discussed in was limited to (n,n)[9]. When the cover message was similar additionally its secret was influenced. In this paper an innovative Scheme is proposed to improve the security of the QR codes using the XVCS theory. To avoid the security weakness an improved (n, n) sharing method is designed[9]. On this basis, we consider the method for (k,n) access structure by utilizing the (k. k) sharing instance on every k-participant subset respectively. As n increases in this, this approach will require a large number of instance. To classify all the K-participants subset into several collection we further present two require a large number of instance. To classify all the K-participants subset into several collection we further present two division algorithm, in which instance of multiple subset can be replaced by only one. The validity and advantage of the proposed scheme is shown by the experimental result and comparision.

III. EXISTING SYSTEM

A QR code is robust to segmental loss or symbol damage. Any user can access the information in QR codes; therefore, they are unsuitable for storing secret data. During the past few years, many efforts have been made to place and protect secret messages in QR codes. Some scholars have utilized traditional steganography or watermarking techniques [8]-[9]. These studies embed a QR code as a secret into a mask image; or treat it as a mask to hide information. Secret extraction in both techniques requires a transformation to one specified domain, such as DCT or DWT. Regarding secret sharing methods, a polynomial algorithm was presented in[10], where shadows were conveyed in the form of QR codes. In this scheme, the QR code was used as an information carrier to transfer shadow information and its message is meaningless. The authors presented a scheme that resist print and scan operations and detect cheaters. Additionally, a novel QR code was designed for two-level message sharing and document authentication in which a hash function is performed when decrypting the secret. Compared with Boolean operations, the computational overhead of all the fore mentioned schemes is slightly larger. In the Existing system the security to the message that was send is very lesser, anyone can access the information send by the sender. In our proposed system we come along with the solution for the existing security issues, the message send by the sender is under highly level security by using the division and the cryptographic algorithm. Anyone can give access to the QR code, so sending of the private information is not secure through this QR code.

IV. PROPOSED SYSTEM

In this project, an innovative scheme is proposed to improve the security of QR codes. First, an improved (n, n) sharing method is designed to avoid the security weakness of [11]. On the basis, we consider the methods for (k, n) access structure by utilizing the (k, k) sharing instance on every k-participant subset, respectively.

The approach will require a large number of instance as n increases. Therefore, we further present 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.

One significant feature of QR codes in the error correction capability, which allow QR code readers to correctly decode data, even when parts of the symbol are dirty or damaged. The secret message is encoded or encrypted into another form by using AES algorithm.

Then the encrypted message is splits into four shares and stored in different QR code image. Then it will send to the user. In user part, we have to merge all the QR code and by using the QR code scanner, original message is retrieved. The retrieving of the original message is done by merging the QR codes by using the secret key, this secret key is send to the receivers corresponding mail id, and after entering the secret key in the key

Field the user is provided with the message that is send by the sender, through this technique a high security is achieved through the transmission of the message. This security for the transmission is achieved by the Division Algorithm. In the Proposed system the message is transmitted with the high level of security by using the division algorithm.

This Proposed system includes two users 1.Sender 2.Receiver

The sender login to through his registered user name and password and select his receiver from the list of the registered user and send him the message. The receiver who is receiving the message in this phase must connected to the internet so that he can get the respective key to unlock the message. The message from the sender is received as a n-shares of QR code the receiver should merge the QR codes through the respective Algorithm and using his key he will decrypt the message with high level of security.
The registered user can also scan the QR codes to get the Key value, here two division algorithm is used to classify the k-participant subsets into severe, collection.
Third party and malicious user cannot detect the original data.
As described in the figure 1 the sender sends the secret data and that secret message will be encrypted with cryptographic algorithm, the encrypted text is then splited and stored in a n-shares of QR code for better way of security and to avoid the common access of the message. The registered user who want to receive the message login through his user name and password and merge the QR codes send by the user through the cryptographic algorithm, and the receiver scan the QR code using the smart phone.
Both the user need to login to send and receive the message for the better way of security.

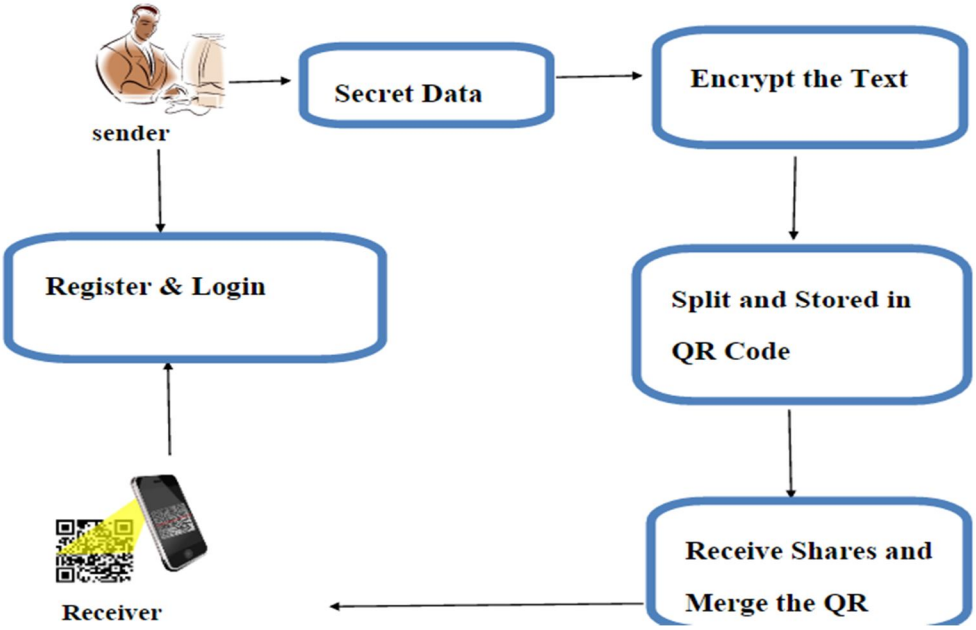


Fig2: Architecture diagram for Encryption and Decryption

V. IMPLEMENTATION OF MODULES

A. *Register & Login*

Data owner has to register by giving all the details. Then Login with correct username and password. If both match, then the owner will be considered as a valid person otherwise invalid person. After login, Owner can able to upload files. Before uploading the files into the cloud, owner has to encrypt the file for security purpose**.**

B. *Sender*

Here user can send message to other user. For security purpose, the secret message should be encrypted and stored in QR Code. By using the Division Algorithm, the secret message is spitted into several parts. By using QR code Scanner we can able to see the Encrypted message. The Spitted message is encrypted and stored in the QR Code with secret key. Select the person to whom the user wants to send the message.

C. *Receiver*

Receiver Login with username and password. User can see the received Secret message in QR Code. The message are spitted and received so user needs to Merge all the QR code images. All the spitted parts are merged and the secret message is hidden in the QR code. All the shares are Merged Together and form New QR Code. Then File key is sent users mail id by using the file key only receiver can view the QR code. To get the original message, Receiver needs to scan the QR code. After Scanning, user gets the original message in Mobile device. By using the mobile device cam QR Scanner, Receiver can able to see the original message.

D. Scanning

The QR code is a type of two dimensional barcode, it encode information in a pattern of black and white squares, corresponding to the 1 and 0 binary bits, the three bullseye square are targeted that allow the Decoding Algorithm to determine if the barcode is rotated, skewed or otherwise distorted based on the camera that is imaging it. This help the decoder accurately read the barcode. The information is encoded in a QR code is usually an internet URL. The scanning of the QR codes is the efficient way of reading the information, thorugh this QR codes the information can be read as soon as possible, during the scanning of the QR code locating the pattern of the QR code is the first process, there are three finding pattern in the QR code and the orientation of the code is also estimated by the scanner. The QR code are detected based on their ratio, the ratio varies from code to code. The code goes through every row and count the number of black and white pixels it encounter. Then it starts verifying the finders pattern, it goes in the way of vertically verifying the pattern and then horizontally verifying the pattern and both the vertical and horizontal verification goes around a ratio test.

E. Division Algorithm

1) Input: C1, C2, , Cn, and S (Each QR code has a blocks).

2) Output: T1, T2, , Tn.

a) Step 1: Let i □ 1, j □ 1, q □ 1, and Tk □ Ck ($1 \leq k \leq n$). Go to Step 2.

b) Step 2: Randomly select a share in which error codewords in block q do not exceed e, and let T represent this share; then, go to Step 3.

c) Step 3: Calculate t □ Tq1 (i, j) □ Tq2 (i, j) □□□ Tqn (i, j). If t □ Sq(i, j), let T(i, j) □□□ T(i, j); else, skip. Go to Step 4.

d) Step 4: Let j □ j + 1. If $j \leq 8$, go to Step 3; else, j □ 1 and go to Step 5.

e) Step 5: Let i □ i + 1. If $i \leq c$, go to Step 2; else, i □ 1 and go to Step 6.

f) Step 6: Let q □ q + 1. If $q \leq a$, go to Step 2; else, go to Step 7.

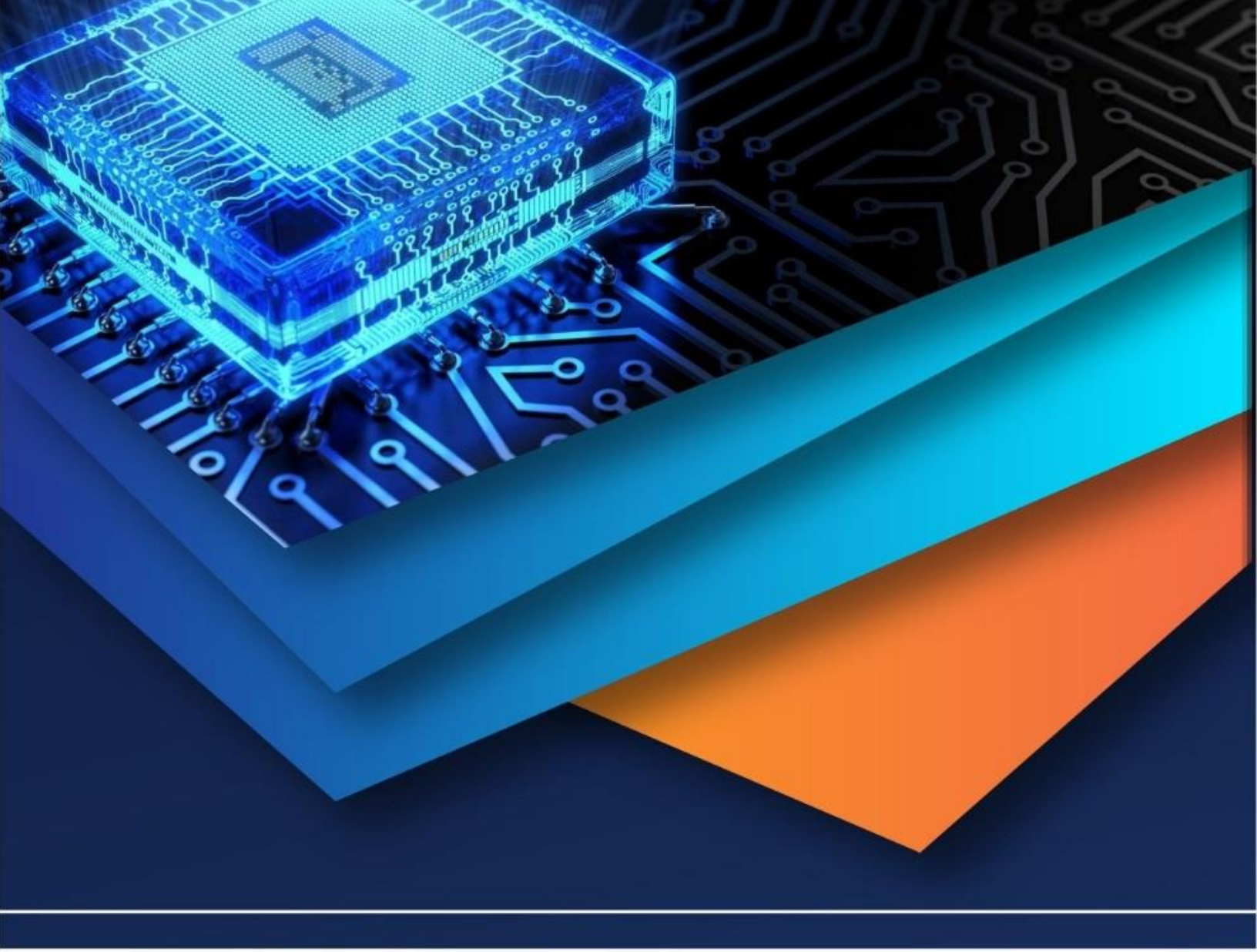
g) Step 7: Algorithm ends.

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. The security weakness of previous work is solved in our paper. 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 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. However, our paper introduces only two feasible partitioning algorithms. According to super graph theory, there may be a deeper relation among those k-participant subsets. Finding this specific relationship and designing an optimal partitioning method remains open problems.

REFERENCES

[1] G. Ateniese, C. Blundo, A. D. Santis, et al., "Visual Cryptography for General Access Structures," Information & Computation, vol. 129, no. 2, pp. 86-106, 1996.
[2] P. Tuyls, H. D. Hollmann, J. H. Lint, et al., "Xor-based visual cryptography schemes," Designs, Codes and Cryptography, vol. 37, no. 1, pp. 169–186, 2005.
[3] Ming Sun, Jibo Si, Shuhuai Zhang, "Research on embedding and extracting methods for digital watermarks applied to QR code images," New Zealand Journal of Agricultural Research, vol. 50, no. 5, pp. 861-867, 2007. QR Code," International Journal of Image-Processing, vol. 4, no. 5, pp. 468-475, 2010.
[4] W. Y. Chen, J.W.Wang,"Nestedimage steganography scheme using QR-barcode technique," Optical Engineering, vol. 51, no. 5, pp. 057004.
[5] F. Liu, C. Wu, X. Lin. "Step construction of visual cryptography schemes," IEEE Transactions on Information Forensics & Security, vol. 5, no. 1, pp.27-38, 2010.
[6] Y. C. Chen, G. Horng, D. S. Tsa "Comment on cheating prevention in visual cryptography," IEEE Transactions on Image-Processing A Publication of the IEEE Signal Processing Society, vol. 21, no. 7, pp. 3319-3323, 2012.
[7] S. Dey, K. Mondal, J. Nath, et al., "Advanced Steganography Algorithm Using Randomized Intermediate QR Host Embedded with Any Encrypted Secret Message: ASA_QR Algorithm," nternational Journal of Modern Education & Computer Science, vol. 4, no. 6, pp. 59, 2012.
[8] 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.
[9] 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
[10] P. Y. Lin, "Distributed Secret Sharing Approach with Cheater Prevention Based on QR Code," IEEE hiding technology for QR codes," Eurasip Journal on Image & Video Processing, vol. 2017, no. 1, pp. 14, 2017.
[11] 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.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY