Data Hiding under QR Code using Visual Secret Sharing and Advanced Partitioning Based on Specific Relationship

Jyoti Rao, Neeta Chavan

***Abstract:** The Visual Secret Sharing is the technique in which secret information is hidden in the form image which then divided into shares and these shares are used to decrypt the secret information. The number of shares required is given by the creator of the secret. Minimum those many shares are needed in order to decrypt the secret. If a single share is missing then the secret cannot be decrypted. The Quick Response (QR) code gives quick access to the information contained in it. QR code is 2D representation of the barcode which has capability to store information and can be easily read by machine. Due to easy access to the information stored in it, it is necessary to use some encryption or other protection to the data. Proposed approach to visual secret sharing scheme divides a secret QR code into different shares. In addition, the secret message is recovered by using XOR operation of the shares. This can effortlessly be achieved with the use of smartphones or different QR scanning gadgets. Using optimal partitioning methods the decryption of the message is made difficult to the hackers giving additional security to the data. The message accuracy can be checked by comparing the original message with shared message using hashing techniques. Because the QR code are small in size and has high data storage capacity, it is also resistant to damage so that is information is not lost even if some portion of the QR code is damaged it is best image to be used in visual secret sharing. The proposed approach reduces the risk of data transmission attacks.*

***Keywords:** Advanced Partitioning, Hashing, Quick Response code, VSS.*

I. INTRODUCTION

Visual Cryptographic System is the secret sharing scheme in which the secret is printed on different transparencies and by overlying those transparencies the secret is revealed and it can be done easily and very fast. The number of transparencies required is specified earlier and if any of the required transparencies is missing then the secret cannot be revealed [11].

Now a days, the QR code is broadly utilized. In day by day life, QR codes can be used in different scenarios like storing information, links to web pages, authentication and identification. First, the QR code is easy to use computerized Identification technique. Second, QR code has a large storage capacity, anti-damage property, strong, cheap and so on.

The QR code has a one of a kind structure for geometrical correction and high decoding capability. Three position labels are utilized for QR code recognition and direction adjustment. It contain blunder adjustment level and cover design. The code form and error correction bits are put away in the

adaptation data regions. The fame of QR codes is essentially because of the following features:

1. QR code is small in size but has high capacity for data encoding.
2. It can be read in any direction and any scanning device.
3. It is resistant to damage and distortion.

Visual cryptography is another secret sharing innovation. 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 strategy for visual cryptography gave high security prerequisites of the users and ensures them against different security assaults. It is anything but difficult to create an incentive in business applications.

II. LITERATURE REVIEW

The paper [1] gives complete analysis of Visual Cryptographic System based on OR operation and XOR operation and proves how XVCS performs better than OVCS. The contrast obtained using XVCS is higher than OVCS. The divergence obtained from XOR based VCS is times higher than OR based VCS. Advantages are: The secret image can be obtained by overlying the shares easily. And the image obtained in XOR based VCS is more accurate compared with the image obtained from OR based VCS. Contrast obtained of the decrypted image is more and so the quality of decrypted image. In paper [2], author proposed that, to correctly find out the information present in Quick Response code it is important to fix the QR code image and do corrections in it if required.

Revised Manuscript Received on February 20, 2020.
* Correspondence Author

Dr. Jyoti Rao, Department of Computer Engineering, Dr. D. Y. Patil Institute of Technology, Savitribai Phul, Pune University, Pune, India. E-mail: jyoti.aswale@gmail.com

***Miss. Neeta Chavan**, Department of Computer Engineering, Dr. D. Y. Patil Institute of Technology, Savitribai Phule Pune University, Pune, India. E-mail: neetagavande@gmail.com

*Retrieval Number: C5799029320/2020©BEIESP
DOI: 10.35940/ijeat.C5799.029320
Journal Website: www.ijeat.org*

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

So to correct the QR distortion algorithm is given depending on conventional geometric correction. The process involves following steps, first is to locate the exact points of four vertices of the Quick Response code. Then image deformation preprocessing of QR image is done. In second step based on points obtained, geometric correction is carried out. In Third step after correction the binary image is formed based on black and white data blocks of the QR code. This way it increases the application area of QR code.

In paper [3], two levels of storage namely public and private are used which are useful authentication of documents. The usual available storage capacity of QR code is also called as public level storage as it can be read by any scanning device. The private storage level is formed by changing the black modules of the QR code by specific patterns. Due to two storage levels the storage capacity of QR code is more the texture patterns used in this paper are sensitive to Print and Scan operation

In paper [4], The author has used the correction property available in standard QR code for sharing the secret message. The message is encoded into QR code and then divided into shares but these shares are also QR code covered images. Due to cover of QR code on shares it is less appealing for attackers and remain secure. As shares are QR code they can easily read by any scanning device making them easy to use.

This paper [5] propose Advanced cheating prevention mechanism to QR code. First the sender of the image shares the keys with the participants and after sending the share first participant is authenticated by using validation code and key. If any of the participant is dishonest then secret decoding process stops at that point itself. Highest version of the QR code that is version 40 is used in the paper. Advantage is introduced an advanced cheating-prevention visual secret-sharing. Presented approach is tolerant to print and scan operation to protect QR data in real world application.

In paper [6] multiple image visual cryptography (MIVC), optimal grayscale reserving visual cryptography (GRVCS) are studied. Due to shares are transmitted over different media it is possible that they are intercepted and changed before received by the recipients, which make them difficult to interprete so new encryption algorithm called simulated-annealing-based algorithm is used which protect shares from interception. In paper [7], The author has outlined the cheating possibility that can occur while sharing secrets. There are chances that the participant may share fake transparency and cheat other participants. The given approach contrasts from related QR code conspires in that it utilizes the QR qualities to accomplish secret sharing and can oppose the print-and-sweep activity. Advantages are: Reduces the security risk of the secret. Approach is practical. Disadvantages are: Need to improve the security of the QR scanner tag. QR system requires lessening the alterations.

In this work [8], the author has proposed the idea of halftoning the image so that it can be cost effective. Halftoning is the process in which image is appeared in the form of discrete dots instead of continuous dots so that when viewed from the long distance is appears like continuous line. Due to the halftoning image is printed with less ink. The author has used error diffusion method to halftone the image. The secret image is fitted into binary value shares and then these shares are halftoned. The original secret is obtained by overlying the shares. It is less complex and cost effective method.

This paper [9], as the digital copyright protection field is becoming more prominent it is necessary to consider all challenges associated with it. Challenges like geometric attack needs to be tackled as it can hamper image quality and for QR code it can affect it's fast scanning feature. In order to deal with this challenge the author has first used contourlet transform to get the minimum frequency part of the image and divided it into blocks. Then QR code information which is going to be converted into watermark is embedded into less frequency image. The proposed approach increases the robustness of rotation and scaling, also it helps to avoid geometric attacks.

In this paper [10], The author suggests that when creating shares it is necessary that the shares should be user friendly means after overlying they should produce some meaningful secret image so that many efforts data handling can be reduced. For doing this the black and white pixels of an image need to studied and depending on that image portability and allocation plan is given. The proposed method tries to reduce the tradeoff between shares and stack image.

III. PROPOSED METHODOLOGY

In proposed system, an inventive scheme is introduced to increase the security of Quick_Response codes based on advanced partitioning using K-means Clustering algorithm. An existing sharing technique is subjected to loss of security. Therefore, presents partitioning calculations to group all the k-member subsets into a few assortments, in which cases of various subsets can be substituted by just one. The designed approach is to hide the secret into a tiny QR codes as the purpose of visual sharing schema. Only the intended participants with the private key can additionally uncover the covered mystery effectively.

A. Advantages Of Proposed Systems:

- Efficient and Secure embedding of text.
- Increases security using advanced partitioning algorithm.
- Increases the sharing efficiency.
- Increasingly adaptable access structures and high security.
- Processing cost is less.
- Message accuracy can be checked with hashing technique.

Following figure1 shows the proposed architecture of the given approach:

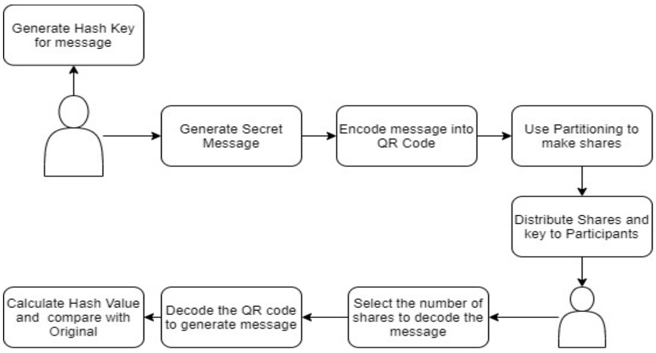
Generate Hash Key for message
Generate Secret Message
Encode message into QR Code
Use Partitioning to make shares
Distribute Shares and key to Participants
Select the number of shares to decode the message
Decode the QR code to generate message
Calculate Hash Value and compare with Original

Fig.1 Proposed System Architecture

Suppose there is situation that some user wants to share some secret to few participants in such a wat that not whole secret is shared but the part of secret is shared with each of them and only few of them are necessary to reveal the secret, in such case it is necessary that shares are made in such a way that even if one or two shares are lost it is not possible to uncover the secret so to achieve this special partitioning method using clustering is used in order to make shares. In order to check if the message received is same as the original one hashing technique is used. First the sender user will generate the secret message which needs to be shared among participants, he will also generate the hash key for it. Secondly he will convert the message into QR code so that message will get covered then for making shares he has to select number of participants. Then the shares will be generated and encoded into small QR codes and shared among participants. After the intended participants received the message share some selected shares will be gathered and the secret is uncovered. At the end the accuracy of the message is checked by obtaining the hash key of the received message if it is same as the one for sent message then it can be assumed that message is sent accurately.

B. Algorithms:

1. Hashing Algorithm:

The MD algorithm is used for authentication of the message. It is a one-way cryptographic function that takes message of any length as input and generate fixed length hash value as output. The output hash value generated is 128 bit key and it is impossible to generate same hash value for two messages, so it gives more secure way for authentication of message. Steps:

- The message digest takes the plaintext of size 512 bits or multiples of 512 bits so we need to convert data to 512 bit size.
- Next step is appending the bits, if plain text is not of size 512 bits then bits are padded at the end so that it becomes multiple of 512 bits.
- Then we have to initialize the buffers which hold the message digest value. Each buffer is of size 32 bits and each digest is of size 128 bits so in all we have to initialize 4 buffers.
- Next each block of plaintext is processed.
- Then output i.e. message digest is generated.

2. K-means clustering:

K-Means Clustering is an iterative, unsupervised algorithm that is used to partition data into clusters based on the similarity present among data points. In this work K-means clustering is used in order to partition the secret message into shares so that it can be distributed to participants. In K-means data is partitioned in such a way that each data point belongs to only one group so as reduce intra-class dissimilarity and increase interclass dissimilarity. In this work for division of message into cluster, a word is compared with center of each cluster and it is then moved to the cluster in which the distance is less from the center.
Steps:

- First select the number of cluster that we want to make as K.
- Then calculate the centroid.
- Randomly select words that are close to the centroid without shuffling words.
- Then cluster mean is calculated.
- Then each word distance is measured from that mean.
- If word’s distance is very less from mean then move to that word to that cluster.
- Otherwise check with the next cluster.
- Re-calculate the center.
- Iterate the procedure till the center doesn’t change.

3. Encoding

- Each letter in the secure message is first converted into its equivalent ASCII value.
- That ASCII value which is 8 bit binary number is then divided into 4 bit number.
- The encoding process is case insensitive.
- The encoding makes the hacker difficult to guess the original message, suppose a meaningful word can be formed by using first letters of the words in the sentence.

4. Decoding

- Each letter of the word is represented as a 4 bit binary number
- Two 4 bit binary numbers are combined to obtain 8 bit binary number.
- From this 8 bit binary number ASCII value is calculated.
- The process is repeated for each word to get the secret message.

IV. RESULTS AND DISCUSSION

Hardware and Software Requirements :Personal Computer with a configuration: Intel (R) Core (TM) i7-2120 CPU @ 3.30GHz, 8GB memory, Windows, MySQL for backend database. It is web based application with JDK 1.9 and Eclipse tool used in designing the application.

Following example illustrates the QR code security with texture patterns by applying the XOR-ing based Visual Cryptography Scheme on QR code for sharing secrets to the receiver. The figure shows the QR code example. The experiment includes two processes encryption process and decryption process.

Results can be explained with the following example:

First the user will generate the secret message along with the hash key for the message and will generate the QR code for it.

Input: Transfer 1 lakh to Sharma

Output:

Fig.2 QR Code

At second step the shares will be generated according to the number of participants selected using specific partitioning technique on the message using clustering method.

Fig.3 Secret Shares generated of given message

Figure 3 shows the secret shares generated of given message.

Third step is to send the shares to the participants according to the criteria used for selecting participants.

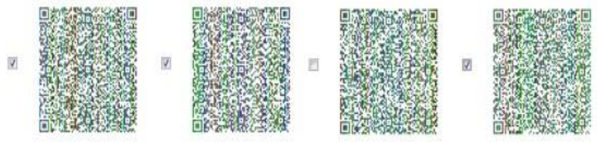

Fig.4 Retrieve the original message using selected shares

At fourth step specific number of shares will be selected and combined to retrieve the original message.

Last step is to check the sent message accuracy using hash key if the original and sent message is correct or not.

Message – Transfer 1 lakh to Sharma

The access structure used in the proposed sharing approach decrease the amount of time for decrypting the secret. It can be shown using following bar chart, which shows the time complexity varies with the length of the message in (k, k) and (k, n) access structure where n is the total number of shares and k is the minimum number of required shares for decrypting the secret.

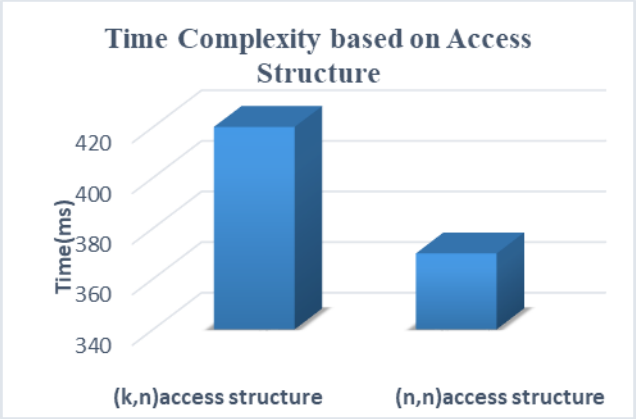

Fig. 4 Time complexity of two access structures

V. CONCLUSION

In this paper, VSS scheme for Quick_Response code applications is used, which makes improvement mainly on two aspects: higher security and partitioning techniques based on specific relationships. In addition, the access structure of (n, n) has been extended to (k, n) by investigating the error correction mechanism of Quick_Response codes. The time requires using (k, n) access structure is less compared to (n, n) access structure which is shown graphically. The message accuracy is checked using Hashing Technique.

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. Wang Xuan, Cao Peng, Feng Liuping, Zhu Jianle, Huo peijun,"Research on Correcting Algorithm of QR Code Image's Distortion "17th IEEE International Conference on Communication Technology 2017.
3. 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.
4. Y W. Chow, W Susilo, G Yang, et al., "Exploiting the Error Correction Mechanism in QR Codes for Secret Sharing," Information Security and Privacy, pp.409-425, 2016.
5. 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.
6. Miss. A. A. Naphade, Dr. R. N. Khobaragade Dr. V. M. Thakare, "Improved NVSS scheme for Diverse Image Media". International Conference on Science and Technology for Sustainable Development, Kuala Lumpur, MALAYSIA, May 24-26, 2016.
7. Y. C. Chen, G. Horng, D. S. Tsai, "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.
8. Z. Wang, G. R. Arce, and G. D. Crescenzo, "Halftone Visual Cryptography via Error Diffusion", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 4, NO. 3, SEPTEMBER 2009.
9. Weijun Zhang, Xuetian Meng, "An Improved Digital Watermarking Technology Based on QR Code" ICCSNT 2015.
10. S. Mohammad Paknahad, S. Abolfazl Hosseini, Mahdi R. Alagheband," User-Friendly Visual Secret Sharing for Color Images Based on Random Grids" International Symposium on Communication Systems, Networks and Digital Signal Processing 2016.
11. M. Naor and A. Shamir, "Visual Cryptography", in Proc. Advances in Cryptology: EUROCRYPT 94, vol. 1995, (950) .

AUTHORS PROFILE

Dr. Jyoti Rao, has total 18 years of teaching experience in Computer Engineering. She is working as Professor in D.Y. Patil Institute of Technology, Pimpri. She is approved Post Graduate Teacher at SPPU. She completed her PhD in 2016 on topic "Novel and efficient Visual Cryptography scheme for privacy protection". Her ME dissertation was in Information security area ie " Security plugin for Outlook" which was BMC software sponsored in year 2008. She worked on Unix, Solaris, Linux in IUCAA during BE project in year 2002.

Miss. Neeta Chavan, is PG student at "Dr..D. Y. Patil Institute of Technology, Pimpri, Pune", affiliated to Savitribai Phule Pune University and will be completing ME(Comp) in 2020. And has completed BE(Comp.Sci.) from P. E. S. College of Engineering ,Aurangabad affiliated to B. A. M. University, Aurangabad.