

# Improved data hiding in QR code using visual secret sharing with advanced partitioning

Neeta Chavan<sup>1</sup>, Prof.Dr.Jyoti Rao<sup>2</sup>, Dr. Swat Nikam<sup>3</sup>,  
Department of Computer Engineering

Dr. D. Y. Patil Institute of Technology, Pimpri, Pune, Maharashtra, India.

[neetagavande@gmail.com](mailto:neetagavande@gmail.com)<sup>1</sup>, [jyoti.aswale2020@gmail.com](mailto:jyoti.aswale2020@gmail.com)<sup>2</sup>, [swanikam147@gmail.com](mailto:swanikam147@gmail.com)<sup>3</sup>

*Abstract—As the information travels from one point to another there are chances of information loss or corruption during transmission also the integrity and authenticity of the information are important points that need to be considered. For this we proposed an approach that hides secret information under QR Code which is then divided into parts and sent to the receivers in the form of shares and by using XOR operation the shares are merged to get the secret. The method of encrypting the visual information into an image so that the decrypted information appears as an image is known as Visual Cryptography [11]. QR codes are easy to read, cheap, distortion resistant and also hold more information than traditional barcodes. But as the information stored in QR codes can be easily read, it is essential to use some type of protection mechanism or encryption while storing the data into QR code [12]. The proposed approach ensures data security and data integrity by hiding the data under QR code and data authenticity is checked by hashing technique.*

*Index Terms—Hashing, Partitioning Algorithm, Quick Response code, Visual secret sharing scheme.*

## I. INTRODUCTION

### Visual Cryptography:

Visual Cryptography is a technique in which visual information is encoded into secret image so that the secret information hidden under image can be found only after using some decryption process on that image [11]. The first best known visual Secret Sharing was proposed by Adi Shamir and Moni Naor in 1994. To demonstrate it they first broken down the secret image into different shares and only the one who has all those shares could decrypt the image, if any one of the shares was missing then it is not possible to decrypt the secret image. This is called as  $(n,n)$  Secret Sharing Schemes, where  $n$  is the total number of shares of the image and all  $n$  out of  $n$  are required to decrypt the image [13]. There are many variations of this schemes.  $(k,n)$  Secret sharing means  $k$  out of  $n$  shares are required to decrypt the image, where  $(k \leq n)$ . Minimum  $k$  or more shares are required to decrypt the secret.

### QR Code:

QR code means Quick Response code is a 2D representation of the barcode which gives fast retrieval to the data stored in it. The fig shows structure of the QR code.

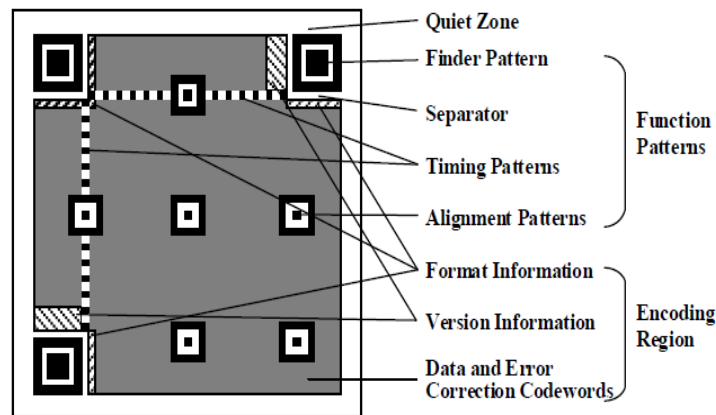


Fig.1 The symbol structure of QR code version 7

As shown in the figure the QR code is a square shaped box which is separated by a border. The three rectangular blocks at the three corner and squares along diagonal are called as data alignment blocks which help to read data from QR code in any direction. The dotted black and white lines are called as timing pattern which tells the size of QR code, how much data a QR code can hold. Version information tells the information about the version of the QR code. There are 40 versions of the QR code, bigger is the version more the data QR code can hold. The figure shows version 7 of the QR code. Data and error correction pattern help to recover data from QR code in case if it is damaged.

Some characteristics of QR Code:

1. Relatively high capacity for encoding of data.
2. Small print out size
3. Stores variety of datatypes including kanji, kana
4. Dirt and damage resistant
5. Readable from any direction in 360degree
6. Structured appending features

## II. REVIEW OF LITERATURE

In paper [1], the author has proposed the visual secret sharing scheme using QR codes with  $(n, n)$  Threshold scheme, here the image is encoded into QR code and these QR codes are split into parts which are then shared among the participants and the required number of participants are necessary to decode the secret otherwise image cannot be decoded. The secret image can also be decoded by stacking the QR shares one above the other. The advantage of this method is that the image can be reconstructed without any loss.

In paper[2], the author has first examined various flavors of secret sharing schemes then put forward two variants for the same, firstly the grey code technique is used to create shares of the secret and then XOR operation is used to recreate the secret from the shares. Proposed approach can be used in cryptographic algorithm for secret sharing.

This paper [3] the author has proposed new algorithm in order to increase the security of visual cryptography. A new algorithm called CISEA is proposed for creating the shares of the secret image. A compliment image is used in order to hide the secret image and then the shares are produced from that

complimentary image. The proposed algorithm provides an additional layer of security to the secret as compared to the traditional watermarking method.

In the paper [4], the author has used the potential of visual secret sharing for authentication and copyright protection. The binary image which is having secret data can be used to make parts of the secret which is then used to authenticate copyright owner by overlying the parts one above another.

paper [5] proposes advanced conning avoidance instrument to QR code. First the sender of the picture imparts the keys to the members and subsequent to sending the offer first member is confirmed by utilizing approval code and key on the off chance that any of the member is untrustworthy, at that point mystery interpreting process stops by then itself. Most noteworthy adaptation of the QR code that is variant 40 is applied in the paper.

In paper [6] The capacity of QR code is increased by introducing color QR codes. As traditional black and white QR code can hold data of multiple types including text, images, web-links, etc. The black and white QR code hold 1bit in each module but the color QR code with 16 different colors can hold 4-bit data. The decoding of QR code is relatively simple and be done using any scanning devices. For this the author has used 8-megapixel camera and the application was developed on android phone. The disadvantage of using color QR code is that, over a period the color of the QR code may fade away for example red may turn into pink which could result in wrong decoding of the message.

In paper[7], the author has proposed visual secret sharing scheme using QR codes, the shares made for secret are also tiny QR codes that contain some portion of secret, when these shares are stacked one above another secret is revealed. As the secret parts are also QR codes they are less likely to be get attacked by the attackers and the information security is achieved during the data transmission. The author has used  $(k, n)$  based threshold scheme to reconstruct the secret.

In paper[8], the author has proposed extended visual cryptographic technique. Because the traditional visual cryptography technique suffers the security issues the extended approach is proposed. In which by dithering halftone technique the time is reduced for generating halftone images and also the quality of secret image is also enlightened which improves security as well as the processing.

In paper[9], the author has focused on security features of the QR code in many real life applications and further secured transmission of data over communication channel. QR code is nothing but 2D barcode which can store more information than traditional barcode. It has self built in error correction mechanism which is useful for correcting the missing information. The amount and type of data varies as per usage. Any weblinks, text, images can be stored in the QR codes.

In paper[10], the author has used visual secret sharing scheme with QR codes. As QR codes are readable and store more information therefore it becomes essential to give some protection to the information stored in it, for that QR codes are used to make meaningful shares which are less likely to be attacked by hackers. Two division algorithms are used which tries to give more security and increase sharing efficiency.

### III. PROPOSED SYSTEM

A new approach is introduced to improve the security of QR codes using enhanced division method. Because the data in the QR code is subjected to attacks due to easy readability it becomes necessary to use some type of additional security to it. Clustering technique used in the proposed system makes it more secure during data transmission as the shares are made by randomly clustering the words into groups. Following diagram shows the flow of the process.

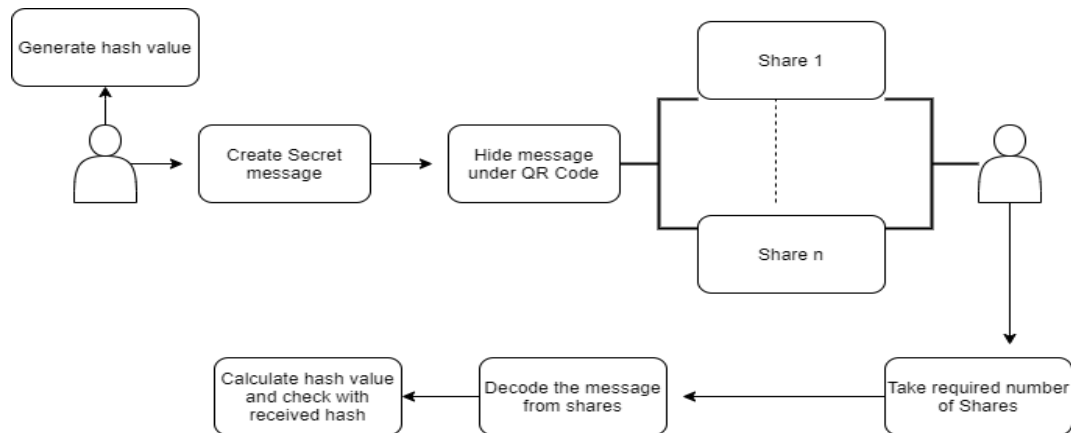


Fig.2 System Diagram

#### Algorithms

##### 1. Hashing:

The MD calculation is utilized for validation of the message. It is a single direction cryptographic capacity that accepts any length message as information and create constant length hash an incentive as yield. The yield hash produced is 128 piece key and it is difficult to create same hash an incentive for two different texts, so it gives safer route for confirmation of texts.

Steps:

- A MD calculation is a hash work that takes a piece grouping of any length and creates a piece arrangement of a fixed little length.
- The yield of a message digest is considered as an advanced mark of the information.
- MD5 is a message digest calculation creating 128 pieces of information.
- It utilizes constants inferred to geometrical Sine work.
- It circles through the first message in squares of 512 pieces, with 4 rounds of tasks for each square, and 16 activities in each round.
- Most present day programming dialects gives MD5 calculation as implicit capacities

##### 2. Encoding and Decoding of Data into and from the QR code:

Steps:

- Every character in the secret text is transferred to the corresponding ASCII value.
- This ASCII number is converted to the corresponding binary 8 bit representation of the data.
- This 8 bit value is divided into the 4 bit parts and stored into the QR code's code-word while encoding.
- While decoding two four bit parts are combined to form the binary eight bit data.
- From that binary eight bit value ASCII number is calculated and from that ASCII value corresponding character is found out.

### 3. Partitioning:

The traditional division algorithm divides the sentence into groups with each group containing the words which are adjacent to each other in the original sentence. Such division makes it easy for hackers to guess the message if any one share is lost. But the proposed clustering method will try to divide the message words into clusters in which words are randomly selected.

K-Means Clustering is an iterative, unaided calculation that is utilized to segment information into groups dependent on the likeness present among information focuses. In this work K-implies grouping is utilized so as to parcel the mystery message into shares with the goal that it very well may be dispersed to members. In K-implies information is parceled so that every information point has a place with just one gathering so as diminish intra-class uniqueness and increment interclass divergence. In this work for division of message into group, a word is contrasted and focal point of each bunch and it is then moved to the bunch in which the separation is less from the inside.

Steps:

- Give the quantity of bunch an incentive as k.
- Randomly pick the k group focuses .
- Calculate mean or focal point of the group
- Calculate the separation between each word to each group community
- If the separation is close to the middle at that point move to that bunch.
- Otherwise move to next bunch.
- Re-gauge the inside.
- Repeat the cycle until the inside doesn't move.

## IV.RESULTS AND DISCUSSION

The experiment includes two processes encryption process and decryption process. To check the efficiency of the proposed system we have developed a web application with java and MYSQL to support database. Apache Tomcat server is used as application server.

### Sender's side:

The secret message is generated by sender who also generates hashcode for the message and send to receiver both the message and hashcode. Following snapshots show the working of the process:

Enter message, number of parts to create, enter the number of parts required to reconstruct the secret and specific user participants.

Select Post Type  Public  Private

Post your private message

visual secret sharing schema



Enter the number of parts to create:

4

(Integer at least 1.)

Enter the number of parts required to reconstruct the secret:

3

(Integer at least 1, no more than number of total parts.)

neha mehra

Fig.3 Sender generating message and creating shares.

The message shares and hash code is sent to the receivers, the one who is having all the required number of shares is able to decrypt the message.

Shares are generated using advanced partitioning technique i.e. k-means clustering

List of Secrets



Send

Fig.4 Sender generated shares of QR code

**Receiver Side:**


View Message:


Private Friend Messages


Profile Pic	Name	Date	Required Parts	Show
	neeta gavande	2020-07-06 08:52:15.0	3	<a href="#">View</a>


Fig.5 Receiver gets the message shares

Select required parts:

Profile Pic	Name	Date	Required Parts
	neeta gavande	2020-07-06 08:52:15.0	3










Fig.6 Receiver selects required number of shares.

Decode Message:

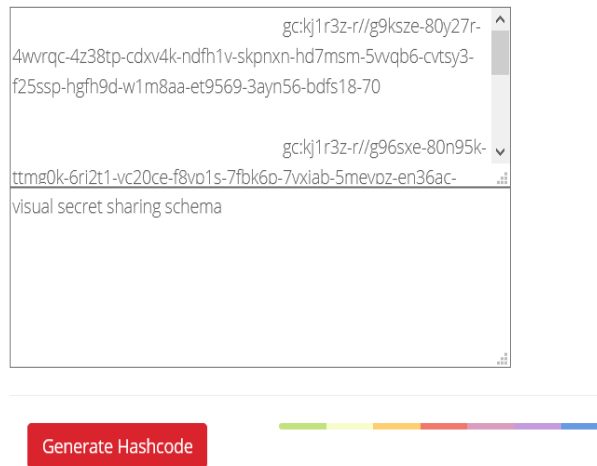


Fig.7 Receiver decodes message and generates hashcode.

The hashcode generated by receiver is used to check the message integrity and authenticity of the sender. Below graph shows the encoding and decoding speed of the existing versus proposed system.

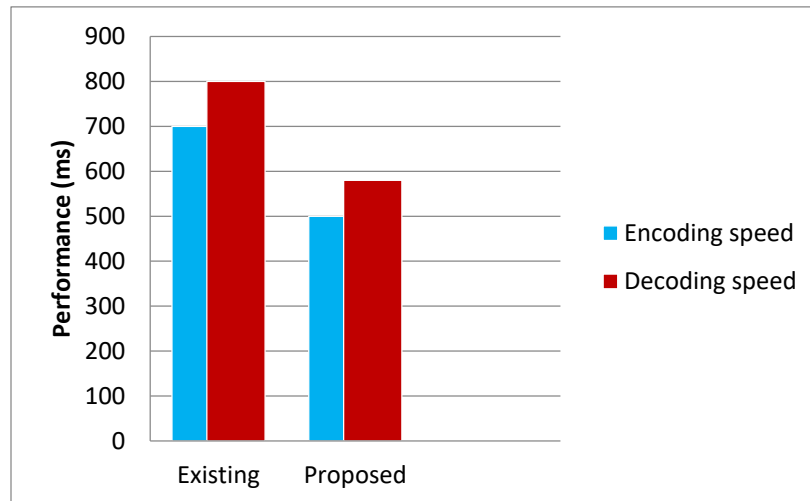


Fig.8 Encoding and Decoding speed comparison

The time taken by the proposed system is compared with the existing system and shows that the time taken by (k, n) sharing scheme is less compared to the (k, k) sharing scheme.



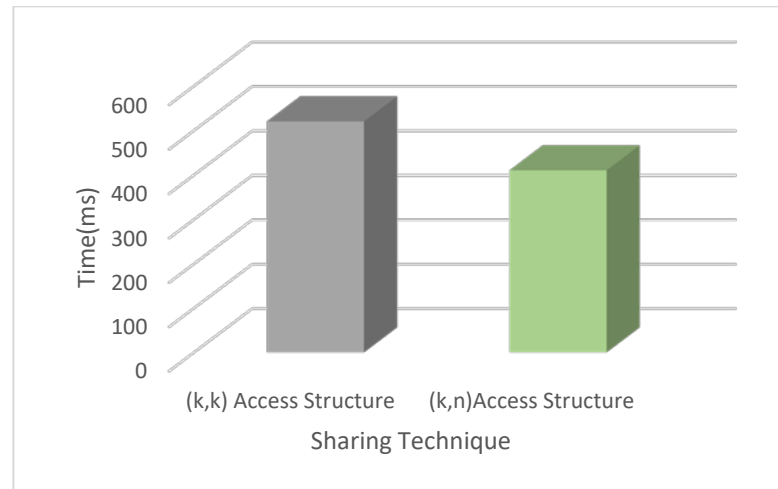


Fig.9 Time Complexity

## V. CONCLUSION

In proposed system, the security of the Visual Secret Sharing Scheme is improved with respect to partitioning technique. The  $(n,n)$  access structure is changed to  $(k,n)$  which in turn increases the security during transmission and reduces risk of single point of failure as in case of  $(n,n)$  access structure because in  $(n,n)$  if single share is missing or corrupted then the whole decryption process stops. Hashing technique used makes it easier to verify the accuracy and authenticity of the message. The processing cost is very less as QR codes are cheap. Self-error correction mechanism available in QR codes make them popular for encryption decryption processes.

## REFERENCES

- 1] Kesheng Liu, Song Wan, Longdan Tan, Chao Chang, Jinrui Chen, Xuehu Yan “Visual Secret Sharing Scheme for Color QR Code”, IEEE 3<sup>rd</sup> International Conference on Image, Vision and Computing (ICIVC), 2018.
- 2] A. Sreekumar, M. P. Deepika “Secret sharing scheme using gray code and XOR operation”, Second International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2017.
- 3] Govind Kumar Jha, Himanshu Sharma, Neeraj Kumar “Enhancement of security in visual cryptography system using cover image share embedded security algorithm (CISEA)”, International Conference on Computer and Communication Technology, 2011.
- 4] Yuh-Yih Lu, Hsiang-Cheh Huang, Jiun Lin “Visual Secret Sharing for Copyright Protection and Authentication of Color Images”, Third International Conference on Robot, Vision and Signal Processing (RVSP), 2015.
- 5] P. Y. Lin “Distributed Secret Sharing Approach with Cheater Prevention Based on QR Code”, IEEE Transactions on Industrial Informatics, 2016.

- 6] Nutchanaad Taveerad “DEVELOPMENT OF COLOR QR CODE FOR INCREASING CAPACITY”, 11<sup>th</sup> International Conference on Signal-Image Technology & Internet-Based Systems, 2015.
- 7] Xuehu Yan, Song Wan, Lintao Liu, Yuliang Lu “Visual Secret Sharing Scheme with (k, n) Threshold Based on QR Codes”, 12<sup>th</sup> International Conference on Mobile Ad-Hoc and Sensor Networks (MSN), 2016.
- 8] Vishnu Kumar Kaliappan, M. Desiha “Enhanced efficient halftoning technique used in embedded extended visual cryptography strategy for effective processing”, International Conference on Computer Communication and Informatics (ICCCI), 2015.
- 9] S. Subhitsha, K. Saranya, R.S. Reminaa “Modern applications of QR-Code for security”, IEEE International Conference on Engineering and Technology (ICETECH), 2016.
- [10] Zhengxin Fu, Bin Yu, Yuqiao Cheng ”Improved Visual Secret Sharing Scheme for QR Code Application” ,IEEE Transaction on Information Forensics and Security,2018
- 11][https://en.wikipedia.org/wiki/Visual\\_cryptography](https://en.wikipedia.org/wiki/Visual_cryptography)
- 12] Jyoti Rao, Neeta Chavan, ”Data Hiding under QR Code using Visual Secret Sharing and Advanced Partitioning Based on Specific Relationship” International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-3, February, 2020
- 13]M. Naor and A. Shamir, “Visual Cryptography”, in Proc. Advances in Cryptology: EUROCRYPT 94, vol. 1995, (950).