

A DISTRIBUTED SECRET SHARING SYSTEM WITH REED SOLOMON CODE FOR QR CODE

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE AWARD OF THE DEGREE

OF

MASTER OF TECHNOLOGY
IN
INFORMATION SYSTEM

Submitted By:

Sweta Kumari

(Roll No. - 2K16/ISY/16)

Under the supervision of

Ms. Priyanka Meel

Assistant Professor

Department of Information Technology

Delhi Technological University



DEPARTMENT OF INFORMATION TECHNOLOGY

DELHI TECHNOLOGICAL UNIVERSITY

SESSION: 2016-2018

CERTIFICATE



This is to certify that Ms. **SWETA KUMARI (2K16/ISY/16)** has carried out the major project titled “**A Distributed Secret Sharing Sytem with Reed Solomon Code for QR Code**” as a partial requirement for the award of **Master of Technology** degree in **Information System** by **Delhi Technological University, Delhi**.

The Major project is a bonafide piece of work carried out and completed under my supervision and guidance during the academic session 2016-2018. The Matter contained in this thesis has not been submitted elsewhere for the award of any other degree.

Date:

(Project Guide)

Ms. Priyanka Meel

Assistant Professor

Department Of Information Technology

Delhi Technological University

DECLARATION

We hereby declare that the thesis work entitled “**A Distributed Secret Sharing System with Reed Solomon Code for QR Code**” which is being submitted to Delhi Technological University, in partial fulfilment of requirements for the award of degree of Master of Technology (Information System) is a bonafide report of thesis carried out me. The material contained in the report has not been submitted to any university or institution for the award of any degree.

Sweta kumari

2K16/ISY/16

ACKNOWLEDGEMENT

I express my gratitude to my major project guide **Ms. Priyanka Meel , Assistant Professor** in **Department of Information Technology** at **Delhi Technological University, Delhi** for the valuable support and guidance she provided in making this major project. It is my pleasure to record my sincere thanks to my respected guide for her constructive criticism and insight without which the project would not have shaped as it has.

I humbly extend my word of gratitude to Dr. Kapil Sharma, Head of Department and other faculty members of department of Information Technology for providing their valuable help and time whenever it was required.

SWETA KUMARI

Roll No.: 2K16/ISY/16

M.Tech. (Information System)

Department of Information Technology

Delhi Technological University, Delhi

ABSTRACT

Secret sharing is also called secret splitting refers to methods for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number, of possibly different types, of shares are combined together; individual shares are of no use on their own. QR barcodes are used extensively due to their beneficial properties, including small tag, large data capacity, reliability, and high-speed scanning. This approach differs from related QR code schemes in which it uses the QR characteristics to achieve secret sharing and can resist the print-and-scan operation.

In this study, I utilized the characteristic of Reed Solomon code to detect and correct the errors in the QR module and distribute the secret by using the (N,N) - Threshold Secret Sharing Scheme. The secret can be split and conveyed with QR tags in the distribution application, and the system can retrieve the lossless secret when authorized participants cooperate. General browsers can read the original data from the marked QR tag via a barcode reader, and this helps reduce the security risk of the secret.

CONTENTS

CERTIFICATE	i
DECLARATION	ii
ACKNOWLEDGEMENT	iii
ABSTRACT	iv
LIST OF FIGURES	vii
CHAPTER 1 INTRODUCTION	1-3
1.1 Motivation of study	2
1.2 Our contribution.....	3
1.3 Organization of thesis	3
CHAPTER 2 LITERATURE REVIEW	4-14
2.1 Overview of QR Barcode Technology	4-7
2.2 Overview of Secret Sharing Technology.....	8-12
2.2.1 Shamir’s Secret Sharing Technique.....	9-10
2.2.2 Asmuth-Bloom Secret Sharing Scheme.....	11
2.2.3 Verifiable Secret-Sharing based on Elliptic curves.....	11-12
2.3 Overview of Reed Solomon Code.....	12-14
CHAPTER 3 RESEARCH METHODOLOGY	15-24
3.1. (N,N) – Threshold Secret Sharing Approach	15
3.1.1 Secret Sharing Procedure.....	16-20
3.1.1.1 Preliminary Phase.....	16-17
3.1.1.2 Shadow Derivation Phase.....	18
3.1.1.3 Concealment Phase.....	18-20
3.1.2 Secret Revealing procedure.....	20-22
3.1.2.1 Estimation Phase.....	21
3.1.2.2 Cheater Identification Phase.....	21-22
3.1.2.3 Secret Retrieval Phase.....	22

3.2 Reed Solomon Code	23-24
CHAPTER 4 RESULT AND ANALYSIS.....	25-30
4.1 Generating the shares with threshold value	25-27
4.3 Retrieval of the Secret data.....	28-30
CHAPTER 5 CONCLUSION AND FUTURE WORK.....	31
5.1 Conclusion	31
5.2 Future Work	31
REFERENCES.....	32-33

LIST OF FIGURES

Title	Page No.
Fig. 2.1. Basic Structure of QR Code	4
Fig. 2.2. Threshold Secret Sharing Technique	8
Fig. 3.1. Approach Overview	16
Fig. 4.1. Shows Information about the shares	25
Fig. 4.2. (4,4)-Threshold Sharing Cover QR code	26
Fig. 4.3. (4,4)-Threshold Sharing with all the shares of cover QR code.	27
Fig. 4.4. Showing Result when number of shares less than threshold value	28
Fig. 4.5. When number of shares equal to the threshold value	29
Fig. 4.6. When number of shares more than the threshold value	30

Chapter 1

INTRODUCTION

Secret sharing is a technique in which a secret is distributed among the group of participants. The secret data recovered only when everyone participants shares there shares, independent shares has no meaning. There is different method of secret partaking in one of them there is one merchant and n members. The merchant distribute the shares among the participants. The dealer distribute the shares in a manner that any gathering of t (for threshold) player or additional than t player can recover the secret. But not less than the t-players. This compose framework is called (t,n) – threshold technique (it can also be composed as (n,t) -threshold technique). Only if the players able to satisfy the specific condition than only secret reconstructed from there shares.

Secret sharing technique has the key role of protecting the secret infomation against the lost of information, destroyed and being altered. Secret sharing technique is used for the following :

1. Threshold signature.
2. Threshold cryptography
3. Safe multi party communication
4. Group key management etc.

Secret sharing schemes are best used for the storage of the data that are extreme important and sensitive. For example like encryption keys , code of missile launch and numbered bank account.

QR barcodes are utilized widely because of their gainful properties, containing little tag, expansive information limit, unwavering quality, and fast filtering. Be that as it may, the secret information of the QR scanner tag needs efficient security preservations.

We are using the Reed Solomon code for enhancing the security of the QR barcode. Reed Solomon code is the error correcting code. It is invent to detect the issues for correcting multiple errors. Reed Solomon Code is mainly used for the burst-type errors in the mass storage devices such as :

1. Storing devices (Hard disk drive, DVD, QR code tags)

2. Wireless and mobile communications units.
3. Satellite links
4. Digital TV and Digital Video Broadcasting(DVB)
5. Modern techniques like xDSL

Reed Solomon code is express as $RS(n, k)$ with $r - bit$ symbols. It means that the encoder will take the $k - data$ symbols of size of $r - bit$ each. And add the parity symbols to make the codeword of n symbols. There are total $n-k$ parity symbols of s bits each. The decoder of the Reed Solomon code has ability to correct the error upto t symbols which has the errors in the codeword ,where $2t = n-k$. For the given symbol of size r , the maximum codeword length (n) for a Reed-Solomon code is calculated as $n = 2^r - 1$.

1.1 Motivation of Study

Generally for providing security to the barcode data , store the data at the back-end database. And QR code used to show the link of the data. For obtaining the data we have to access the web browser with the right access detail [4]. Due to using the link for the database create the risk in respect to privacy of the data. Chuang et.l [4] has design a Secret Sharing Scheme for providing security to the barcode data. But unfortunately content of the QR tag does not have any meaning and the data can be easily retrieved by scanning the QR code using a simple barcode reader. A distributed and reliable Secret Sharing System with the QR code is used in the various applications such as : secret management and authorization in e-commerce.

Previously most of the research related to the QR code [5] –[11] these paper used the image hiding and watermarking techniques instead using the QR code features. In the image hiding technique , QR tag is treated as the secret image. And place the QR image into the frequency domain[7],[8] or special domain [5],[6] of the cover image. The data capacity value of these schemes is same as the QR data. In practically these schemes does not implemented directly onto the QR data and also they do not have capability of reading/hiding the secret data into/from the QR code.

For avoiding the conventional scheme Gao and Sun [12] purposed the scheme as,by embedding the water mark into QR tag, by directly adjusting the width of rows and columns of the QR modules. But this schemes fails when we extract the correct water mark and the

width of the rows and columns of the QR module are distorted. Thus this scheme need the additional bilinear interpolation transform and morphological repair.

However , these schemes doesn't use the features of the QR code. QR code ability of correcting the errors make the QR code reader to retrieve the original data correctly even if the QR code portion was damaged. In respect to exploring the ability of the error correction of the QR code we design a secret sharing system with the Reed Solomon code.

Our aim is to design a distributed secret sharing system that to allow a secret to be divided into pieces and shares among the independent QR tag owners. And to ensure the isolation of the QR data. The secret data can be uncovered when authorized QR tag owners collaborate. For enhancing the security of the QR code data we apply the Reed Solomon code for correcting the errors.

1.3 Our Contribution

Our contribution lies in proposing a distributed secret sharing system with the Reed Solomon code for increasing the security of the QR code. We distribute the data into the pieces and each shares is distributed among the authorized participants using the (N,N)-Threshold technique of Secret Sharing scheme. Then ,we apply the Reed Solomon code for the encoding and decoding of the data. Reed Solomon can correct the errors such as noise, erasure and error. Reed Solomon code is used for correcting the burst type errors.

1.4 Organization of thesis

The thesis is organized in various chapters as follows: Chapter 2 gives an overview of the related work of the study that is what is the various research works have been done in this area and how all those work helped in evolution of our study. This includes QR barcode Technology , Secret Sharing Technique. Chapter 3 summarizes the research methodologies used in this thesis. This includes the secret sharing methodology and Reed Solomon Code Technique.. Chapter 4 shows the results and their analysis. And at last the chapter 5 summarizes the research work under conclusion and suggests some future work.

This chapter gives an overview of the research work done with relation to our thesis and is further sub divided into 3 sections i.e. QR code technology , Secret Sharing Technique and Reed Solomon Code Technolog. First section gives the overview of QR code Technology and second section describes the Secret Sharing Technique for QR code.

2.1 Overview of QR barcode Technology

The QR Code stands for Quick Response Code. We uses QR Code for its significance properties we can store massive amount of data into small tags. QR code also have properties like reliability and fast capability of scanning. QR Code uses 2-D matrix representation. QR Code uses four standard encoding means numeric, alpha-numeric, byte and kanji. QR Code made of square module of white and black dots. The black and white dots represent one and zero digit.

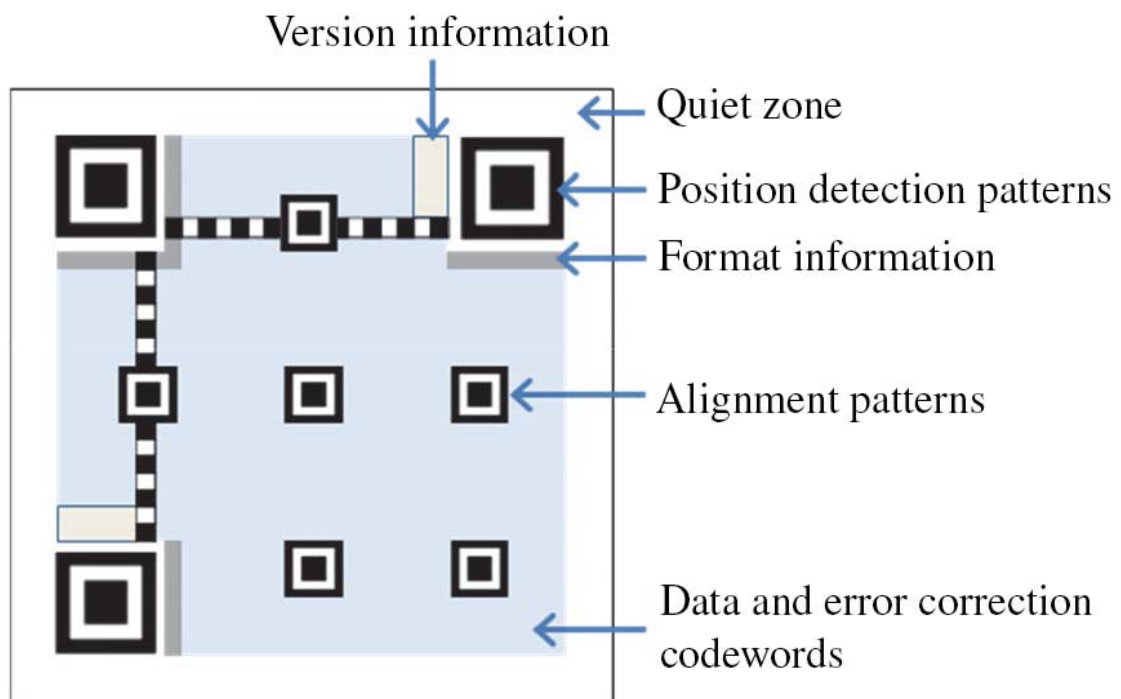


Fig. 2.1 (Basic Structure for QR Code)

Position Detection Pattern:

The three corners of the QR Code are position detection pattern. Position detection patterns are used for detecting the position of the QR Code. Position of the QR Code is detected by the position detection pattern. Position detection pattern allowed the high speed reading. It allows to read QR Code from any direction that enhances the work efficiency.

Alignment Pattern:

The alignment pattern is used for position detection. Alignment pattern used when there is distortion among the modules because of displacement.

Margin:

Margin is the blank area around the QR Code.

Timing Pattern:

White and black modules are alternatively arranged in the way to obtain the coordinate.

Format Information:

It consists of two things one is error correction rate and mask pattern of the code. When code is decoded then format information is the first which is read by first.

Version Information:

It has the information of the version of QR Code. It tells which version of the QR Code is used.

QR Barcode Error -Correction Level and Versions:

The QR Code has four error correction levels i.e L, M, Q and H for each QR version as listed in table - I to achieve reliability. For instance, Level H can tolerate up to 30% of misdecodes or substitution errors in the data and error correction codewords. Here codeword is the unit in the QR tag which is equal to the eight modules.

Error correction level	Error correction capability, % of codewords (approx.)
L (Low)	7
M (Medium)	15
Q (Quartile)	25
H (High)	30

Table 2.1 RELIABILITY OF THE QR BARCOD

The QR Code standard offers 40 QR versions to carry various data payloads. The higher QR version can carry large amount of payload. Other property of QR Code is its reliability which allow barcode reader to recover the data correctly even if the portions of QR Code are dirty or damaged.

Table-II briefly represent the reliability of the various QR versions and error correction level of QR standard. Based to the QR -version and error correction level, the data codewords in the QR tag are segmented and stored into one or more blocks. For instance, the data in QR version 1-L are 152 bits (19 data codewords \times 8 modules) and are stored in one block. The data in QR version 40-L are 23 648 bits (2956 data codewords \times 8 modules) and are segmented and stored in 25 blocks (19 + 6), i.e., 19 blocks each of which contains 118 data codewords and six blocks each of which contains 119 data codewords. Then, the error correction codewords that correspond to the data codewords of each block are generated to ensure the error correction capability of the block data.

Table-II 2.2 QR BARCODE VERSIONS MAXIMUM CAPACITY

Version	Error correction level	Number of error correction codewords	Number of error correction blocks	Number of data codewords per block	Number of data codewords	Number of data bits
1	L	7	1	19	19	152
	M	10	1	16	16	128
	Q	13	1	13	13	104
	H	17	1	9	9	72
20	L	224	3 5	107 108	861	6888
	M	416	3 13	41 42	669	5352
	Q	600	15 5	24 25	485	3880
	H	700	15 10	15 16	385	3080
40	L	750	19 6	118 119	2 956	23 648
	M	1372	18 31	47 48	2 334	18 672
	Q	2040	34 34	24 25	1 666	13 328
	H	2430	20 61	15 16	1 276	10 208

The above table represents the QR code versions with their capability of payload. The above table shows the each version capability of payload with the error correction level of the version. There are basically 40 versions are available of QR code and each version has the four level of error correction. According to the error correction level and version payload capability is defined.

2.2 Overview of Secret Sharing Technology

Secret sharing is a technique in which a secret is distributed among the group of participants. The secret data recovered only when everyone participants shares there shares, independent shares has no meaning. There is different method of mystery partaking in one of them there is one merchant and n members. The merchant distribute the shares among the participants. The dealer distribute the shares in a manner that any gathering of t (for threshold) player or additional than t player can recover the secret. But not less than the t - players. This compose framework is called (t,n) – threshold technique (it can also be composed as (n,t) -threshold technique). Only if the players able to satisfy the specific condition than only secret reconstructed from there shares.

Threshold Secret Sharing Technique :

In the Threshold Secret Sharing Technique set a threshold value such as t . To reconstruct the secret we need the tha atleast t or more shares,less than t shares can not retrieve the original data. This techniques is denoted as the (t,n) or (k,n) secret sharing scheme. Secret Sharing Sharing techniques based on the Threshold are plays the key role in the management of the cryptographic key. Secret Sharing Scheme is good if it has the fair sharing of the secret with information rate. Information rate in the Secret Sharing is the ratio of secret being hidden in the size of each share.

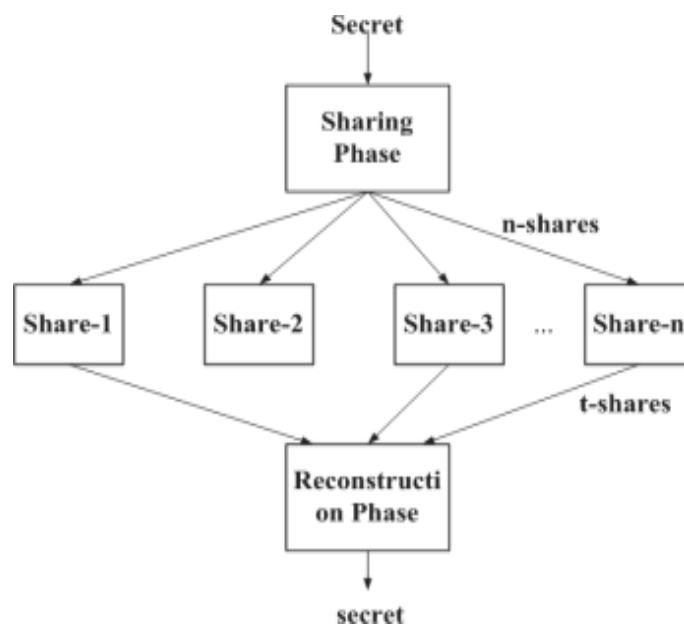


Fig .2.2 (Threshold Secret Sharing Technique)

Secret Sharing Schemes usefull in the following areas:

1. **Cloud Computing Environment:** Using the Threshold Secret Sharing Scheme a key can be distrubted over the various servers. Key can be easily constructed when it is required.
2. **Sensor Networks:** Secret Sharing Scheme is also suggested for sensor network for making the task harder to the eavesdropper where links are reliable to sending the data into the shares.

Hence , we can made the security higher in the above areas by continuously changing the way of construction of the shares.

There are various techniques of Secret Sharing, here we discuss the following techniques of the Secret Sharing :

- 2.2.1 Shamir's Secret Sharing Technique.
- 2.2.2 Asmuth-Bloom Secret Sharing Technique.
- 2.2.3 Verifiable Secret Sharing Scheme based on Elliptic Curves.

2.2.1 Shamir's Secret Sharing Technique :

Modern cryptography used the Secret Sharing technique to dealing with the risk with exposed data in group communication. Shamir's Secret Sharing Scheme comes under the Threshold Secret Sharing technique, according to this scheme shares are obtain from the secret data and distributed among the participants. Secrets are retrived according to the predefined access structure. Shamir's Secret Sharing based on the polynomial interpolation. It is a linear approach. Shamir's Scheme restrict the unauthorized participants from accessing the information of the secret data.

Polynomial Evaluation for the shares generation:

The logic behind the Shamir's secret Sharing Scheme is theoretically simple. Represent the secret data in terms of constant of the random polynomial of degree $(k - 1)$. After that evaluate the polynomial at distinct n - points. Evaluate the polynomial $f(x)$ over the commutative ring R as:

$$f(x) = f_0 + f_1x + \dots \dots \dots f_{k-1}x^{k-1} \quad (1)$$

On the given vector $a = [\alpha_1, \alpha_2, \dots, \alpha_n] \in R^n$. Mapping of polynomial evaluation is defined as :

$$eval(f) = R[x] \rightarrow R^n \quad (2)$$

Result in form of vector as :

$$eval(f) = [f(a_0), \dots, f(a_n)]^T \quad (3)$$

We get the $F_p = [0, 1, \dots, P-1]$ for the given large prime number P . Coefficients for polynomial and vector for polynomial evaluation are taken from the field F_p for the evaluation. Polynomial evaluation of Shamir's scheme done over the field $GF(P)$.

Polynomial Reconstruction:

For the reconstruction Shamir used the Lagrange's interpolation method. Lagrange interpolation formula passes through the k points $(x_0, y_0) \dots \dots (x_{k-1}, y_{k-1})$. The set of basis polynomial $L_j(x_i)$ are constructed of degree n and pass across the k points as:

$$L_j(x_i) = \prod_{j=1, j \neq i}^k \frac{x - x_j}{x_i - x_j} \quad (4)$$

Here ,

$$L_j(x_i) = \{1 \text{ when } j = i \text{ and } 0 \text{ when } j \neq i\} \quad (5)$$

After constructed the basis function we get the $(K - 1)^{th}$ degree of Lagrange polynomial as:

$$f(x) = \sum_{i=1}^k y_i L_j(x_i) \quad (6)$$

In the Shamir's Scheme , the value of x denoting the user and value of y represents the interrelated share's value.

2.2.2. Asmuth-Bloom Secret Sharing scheme:

There are two stages in Asmuth- Bloom Secret Sharing Scheme :

1. Share construction Stage
2. Share retrieving Stage

In the reconstruction phase , we need $k - shares$ from the $n - shares$. At the reconstruction phase we use the Chinese remainder theorem (CRT).

Share Construction Phase:

At this phase take the secret data S , order of the field F , number of users n and the threshold value t and pairwise prime positive integers $n + 1$ as the input for the generation of the shares. At this we get the shares I_1, I_2, \dots, I_n as the output.

Share Retrieving Phase:

Take the shares $I_{k1}, I_{k2}, \dots, I_{kt}$ here ($k_j \in 1, 2, \dots, n$) as the input to retrieve the secret data. For getting the unique solution apply the CRT to the shares as

$$x \equiv I_{i1} \text{ mod } m_{i1}$$

$$x \equiv I_{i2} \text{ mod } m_{i2}$$

$$x \equiv I_{ik} \text{ mod } m_{ik}$$

2.2.3 Verifiable Secret Sharing Scheme based on Elliptic Curves:

Elliptic curve cryptography provide the high security for the smaller key size. Elliptic curves drawn as looping line in (x, y) plan. The genral cubic equation for elliptic curve :

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

Here , $a_1, a_2, a_3, a_4, a_5, a_6 \in F_p$ and P is the prime integer. The above equation of the elliptic curve is over the set F_p . The F_p has the set of solutions $(x, y) \in F_p$. It also include a special point that is '0' which is called as point of infinity. If the feature of the field does not include neither 'two' nor 'three' then the equation -1 can be written by :

$$E: y^2 = x^3 + Ax + B \quad (2)$$

For most of the application we generally use the equation -1 with the following discriminant condition :

$$4a^3 + 27b^2 \neq 0 \quad (3)$$

For performing the Secret Sharing in elliptic curve over the prime field is using the following eq. :

$$y^2 \text{ mod } p = (x^3 + ax + b) \text{ mod } p \quad (4)$$

In the elliptic curve group over the Prime field operations like addition and multiplication are given as follows. Let take points as $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ in the elliptic group $E_p(a, b)$. And let take o be the point at infinity, then their sum $P + Q = (x_3, y_3)$ is given as :

$$x_3 = \lambda^2 - x_1 - x_2 \text{ mod } p$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \text{ mod } p$$

Here , $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ if $P \neq Q$

$$\lambda = \frac{3x_1^2 + a}{2y_1}$$
 if $P = Q$

By using the same addition formula we can obtain the kP multiplication by repeating the elliptic curve addition formula.

2.3 Overview of Reed Solomon Code Technology

Reed Solomon code is the error correcting code technique. It is invented for detecting the issues for correcting burst errors. Reed Solomon code are the most valuable subset of non-binary cyclic error correcting code. It is the most widely used code in various applications. Reed Solomon codes are used in the applications of digital communication and data storing. Reed Solomon code has a systematic approach for detecting and correcting the arbitrary symbol errors. In the Reed Solomon code we add t check symbols to the data, Reed Solomon code can detect up to t erroneous symbols and can correct up to $\lfloor t/2 \rfloor$ symbols.

Reed Solomon code is the error correcting codes. In the Reed Solomon code expendable information is added to the data. So that the original data can be retrieved despite of errors in transmission , storage and at the time of retrieval.

Reed Solomon code encoder takes the block of data and add the extra bit to the data. Errors may occur in the transmission due to the various reasons such as noise and interference. Reed Solomon code decoder process the each block of data to correct the error and to retrieve the original data.

Properties of Reed Solomon Code :

Reed Solomon code has the properties which make it suitable to the burst type errors:

- For the Reed Solomon code it does not matter if multiple bits are corrupted in a single symbol. It will count multiple errors in a single as a unit error. If the data stream is not categorized as a character. Reed Solomon code is the poor choice where a bit stream is not characterized by the error burst.
- “Shortening” is the technique of the Reed Solomon code that produce smaller codes of any desired size from a large code . So that constructor are not to needed the use the actual size of the Reed Solomon code.
- Reed Solomon code for the m symbols has $n = 2^m - 1$ symbols per block. Lets Reed Solomon code for eight-bit symbols has $n = 2^8 - 1 = 255$ symbols per block.
- From the designers point of view it is the best choice to use it for both encoding and decoding tool. It has the capability to deal with the burst errors.

In the Threshold Secret Sharing Technique set a threshold value such as t . To reconstruct the secret we need the at least t or more shares, less than t shares can not retrieve the original data. This technique is denoted as the (t, n) or (k, n) secret sharing scheme. Secret Sharing techniques based on the Threshold are plays the key role in the management of the cryptographic key. Secret Sharing Scheme is good if it has the fair sharing of the secret with information rate. Information rate in the Secret Sharing is the ratio of secret being hidden in the size of each share.

Decoding procedure of the Reed-Solomon can correct errors and erasures. An erasure occurs will take place when the position of an erred symbol is known. A Reed Solomon algebraic decoder can correct up to t errors or up to $2t$ erasures.

When a Reed Solomon code decoder ,decode a codeword then there are three feasible outcomes:

1. If $2s + r < 2t$ (s errors, r erasures) then there is gurantee to recover the original transmitted code word.

Otherwise

2. The decoder will point the fact that it can not retrieve the original data.

OR

3.The decoder can recover the incorrect data and can be mis decode the data without any indication.

This chapter first describes the (N,N)-Threshold Secret Sharing Approach. In the next segment, the Reed Solomon Code technique is described which is used to enhance the security of the QR code by eliminating burst type errors.

3.1 (N,N)- Threshold Secret Sharing Approach :

There are various technique of secret sharing in one of them there is one merchant and n participants. The merchant distribute the shares among the participants. The dealer distribute the shares in a manner that any gathering of t (for threshold) player or extra than t player can recover the secret. But not less than the t players. This type a framework is called (t,n) – threshold technique (it can also be composed as (n,t)-threshold scheme). Only if the players able to satisfy the specific condition than only secret reconstructed from there shares. Secret sharing refers to a technique in which a secret is distributed among the group of participants. The secret can only be retrieved when every one the participants shares there shares, independent shares has no use.

In the (n, n)-threshold sharing system, there is a merchant and n participants, where $n \geq 2$. The dealer will split the secret data into n marked QR tags.

Afterwards the n marked QR tags can be distributed to the n corresponding participants. Only the n participants with authorized QR tags are qualified to obtain the shared secret, and no subset of less than n tags can leak any information about the secret .

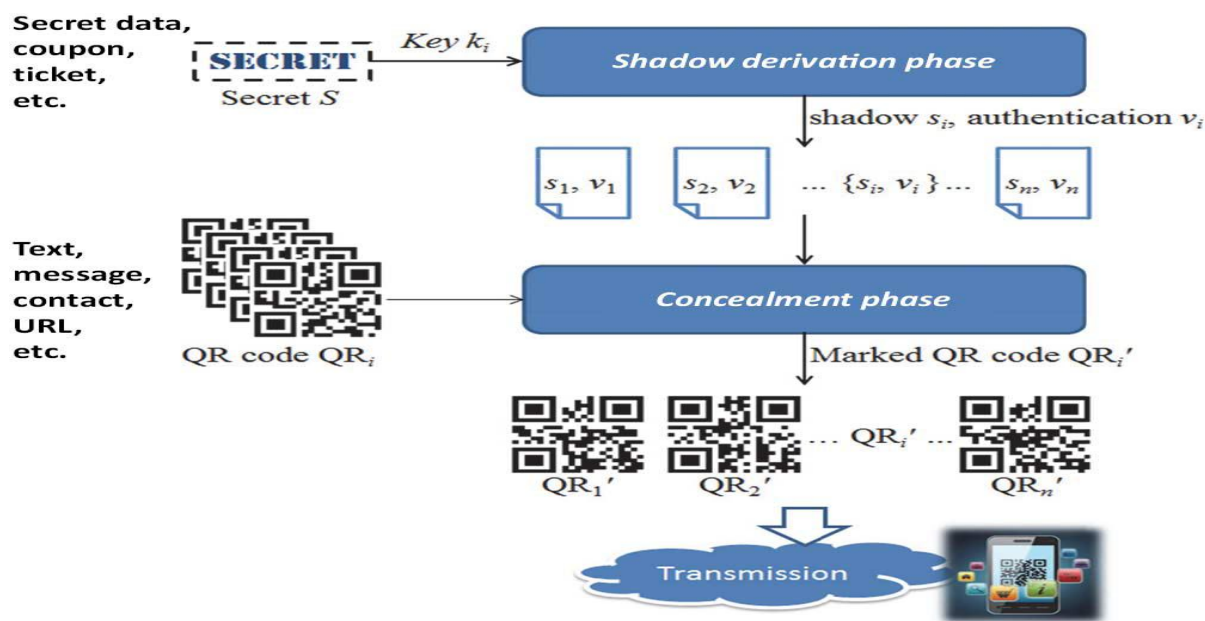


Figure 3.1: Approach overview

There are two steps in procedure:

3.1.1. Secrete Sharing Procedure.

3.1.2. Secrete Revealing Procedur.

3.1.1 Secrete Sharing Procedure :

Let take n covers of QR barcode i.e. QR_i of the same QR version and error correction level, $i=1,2,3,\dots,n$. But the data of QR_i may be different. Barcode reads can scan and decode diverse data from QR_i . Let take S be the private QR data to be protected.

3.1.1.1. Preliminary Phase :

According to the QR code core architecture of QR_i , let the number of blocks b. Count of error correcting codewords be E. To share the secret S with cheater detectability, an authentication code V is used to verify the involved participants. Based on the observation of the QR algorithm, the error correcting capability is less than half of the number of error

correcting codewords. Accordingly, the new scheme determines the payloads of S and V dynamically, along with the QR version and the error correction level as follows.

Step 1: First compute the value of modifiable capacity C for the given QR barcode as:

$$C = \lfloor E/2 \rfloor \times 8 \quad (1)$$

Here E denotes the number of error correcting code words.

Step 2: According to the QR version and number of blocks b compute the length of the authentication code V i.e. l_v :

$$l_v = (1 + \lfloor \alpha \times QR\ version \rfloor) \times b \quad (2)$$

Here α denotes cheater detectability strength. α is a real number it can be adjusted by the dealer, here $0 \leq \alpha < \frac{(C|b)-1}{QR\ version}$.

Step 3: Estimated length of secret S, l_s by

$$l_s = C - l_v \quad (3)$$

The payloads of the secret and the authentication code are computed based on the version and the error correcting level of the given QR Code. This proposed algorithm can bound the distortion and also protect the readability of the QR content.

For example, QR code is given have version 20-L as in table-II 20-L QR code has eight blocks(i.e. $b = 8$) and it has the number of error correction codeword E is 224. Here , modified capacity C equal to $C = \lfloor 224/2 \rfloor \times 8 = 896$ modules. The length of authentication code V is $l_v = (1 + \lfloor 0.5 \times 20 \rfloor) \times 8 = 88$ bits, here $\alpha = 0.5$. Capacity of S is calculated based on the values of C and l_v as $l_s = 896 - 88 = 808$ bits.

3.1.1.2. Shadow Derivation phase:

For deriving the secret shadows from S and V firstly dealer assigns n secrets keys k_i for the n corresponding participants $i = 1, 2, 3 \dots \dots n$. The procedure of shadow age is portrayed as takes after:

Step 1: Using the participant's secret key derive the master keys K .

$$K = \sum_{i=1}^n k_i \quad (4)$$

Step 2: Deriving the n authentication streams v_i with the length l_v .

$$v_i = H_K(k_i), \quad i = 1, 2, 3 \dots n \quad (5)$$

Here, $H_K(\cdot)$ is one way hash function has the master key K .

Step 3: Derive $(n - 1)$ random binary shadows of each length l_s $s_1, s_2, \dots, s_{(n-1)}$.

Step 4: Genrate the n th binary shadow s_n of length l_s from the shadows $s_1, s_2, \dots, s_{(n-1)}$ and secret S

$$s_n = s_1 \theta s_2 \theta \dots \theta s_{(n-1)} \square S \quad (6)$$

Here θ shows the bit stream operation exclusive-or (XOR).

Here dealer have the n shadows s_i and authentication streams $v_i, i = 1, 2, \dots \dots n$.

3.1.1.3. Concealment phase:

By expending the QR Code basic algorithm the new scheme of coding conceal the (s_i, v_i) with the module of the data code words of QR_i while leave the other module of the QR code unchanged.

For the given QR_i let m is the modules of the QR data code words and l_m is the length of m . l_m equals to QR data code word $\times 8$ modules (A code word allude to eight modules).

For example let there are 861 QR data code words in QR data code word in QR version 20-L.

So value of $l_m = 861 \times 8 = 6888$ modules.

Later (s_i, v_i) are covered into parts of the m modules of $QR_i, i = 1, 2, \dots \dots n$ by applying the wet paper codes algorithm. The procedure is described below:

Step 1: Take the m modules of data code word in QR_i as matrix M_i with the size of $l_m \times 1$.

Step 2: Let take the number of l_s modules from the M_i randomly as dry elements, and the left number of $(l_m - l_s)$ are treated as wet elements $i = 1, 2, \dots, n$.

Note number of l_s modules selected from b blocks to maintain the error correction ability of each block of QR_i . So l_s/b modules took from each block.

For example let $l_s = 808$ and $l_m = 6888$ we randomly select 808 modules as a dry elements out of 6888 QR data modules.

Step 3: Derive the binary matrix D_i of size $l_s \times l_m$ using the key k_i , $i = 1, 2, \dots, n$

$$[D_i]_{l_s \times l_m} = RNG(k_i) \quad (7)$$

Here $RNG(k_i)$ is a random number generator who takes the key k_i as initial seed.

Step 4: Now adjusting the l_s dry elements from M_i to \hat{M}_i using the following formula:

$$[D_i]_{l_s \times l_m} \times [\hat{M}_i]_{l_s \times 1} = [S_i]_{l_s \times 1} \quad (8)$$

Here the matrix $[S_i]$ is constructed by the shadow s_i of size $l_s \times 1$, $i = 1, 2, \dots, n$. The modified result $[\hat{M}_i]$ generated by rewriting l_s dry elements in $[M_i]$ according to the solubility of linear equations.

Step 5: According to the l_s modules of \hat{M}_i in step 4 as wet elements. And from the remaining $(l_m - l_s)$ modules in \hat{M}_i took the l_v modules as dry elements. And the remaining $(l_m - l_s - l_v)$ are wet elements, $i = 1, 2, \dots, n$. l_v modules are taken from b blocks. l_s/b modules are taken from each block.

Step 6: Using the master key K and k_i $i = 1, 2, \dots, n$ construct a binary matrix \hat{D}_i of size $l_v \times l_m$

$$[\hat{D}_i]_{l_v \times l_m} = RNG_K(k_i) \quad (9)$$

Here, $RNG_K(k_i)$ is the random number generator. With the master key K and taking k_i as the initial seed.

Step 7: Change the l_v dry elements in \dot{M}_i with the symbols \ddot{M}_i with the formula

$$[\dot{D}_i]_{l_v \times l_m} \times [\dot{M}_i]_{l_m \times 1} = [v_i]_{l_v \times 1} \quad (10)$$

Here , matrix $[v_i]$ is the verification stream v_i of size $l_v \times 1$. $[\dot{M}_i]$ can be rewrite as modified result $[\ddot{M}_i]$ accordingly solvability of linear equations.

Step 8: Take the checked QR code \dot{QR}_i by supplanting the m modules in the data codeword of QR_i with the m components of the outcomes $[\ddot{M}_i]$, $i = 1,2, \dots \dots n$.

Hence , the marked QR code \dot{QR}_i alongside the key k_i can be shared and disseminated to the included i^{th} members, $i = 1,2, \dots \dots n$.

The marked results \dot{M}_i of the first level concealment in step 4 ensures that only l_s modules can be change. In the second level concealment in step 7 guaranteed that l_v modules changed in $[\ddot{M}_i]$. The purposed algorithm control the distortion within the C modules of given QR Code. This enables the barcode readers to scan and decode the data from \dot{M}_i successfully. The extricated important QR information help diminish the doubt of general QR clients while they are examining the QR code. In addition, programs and the included members are unequipped for deciphering and removing the shared secret without adequate \dot{QR}_i and keys.

3.1.2. Secret Revealing Procedure:

In genuine applications, the ability of identifying con artists is a noteworthy prerequisite before the secret data are uncovered. In the proposed (n, n) - edge sharing methodology, just adequate members with the n -approved QR labels and keys can collaborate to uncover the shared secret. The outlined approach can recognize unscrupulous members and distinguish who the con artists are. Furthermore, the noteworthy system of the proposed conspire is visually impaired, i.e., the approved members can remove the secret without the host QR barcode tag and extra data.

Suppose that QR_i and k_i are the n-gave QR standardized identifications also, keys, separately, from the included members, $i = 1, 2, \dots \dots n$. By using a barcode scanner, the data of the QR version, the blunder rectification level and the related configurations can be perceived from QR_i instantly. Let E a chance to be the number of blunder rectification codewords, and let b be the number of squares. The identification of con artists and the extraction of the secret S can be performed by the accompanying stages:

3.1.2.1. Estimation Phase:

Step 1: Based on the QR code compute the values of C and m using the formula $C = C \lfloor E/2 \rfloor \times 8$ and $m = QR \text{ data codewords} \times 8$.

Step 2: Estimating the value of l_v based on QR version, number of blocks and the preshared parameter α .

$$l_v = (1 + \lfloor \alpha \times QR \text{ version} \rfloor) \times b \quad (11)$$

Step 3: Compute the value of l_s using

$$l_s = C - l_v \quad (12)$$

Step 4: Evaluate the master key \hat{K} using $\hat{K} = \sum_{i=1}^n k_i$.

Step 5: Regenrate the n authentication streams \hat{v}_i , each of length l_v using the formula:

$$\hat{v}_i = H_{\hat{K}}(\hat{k}_i), i = 1, 2, \dots \dots n \quad (13)$$

Here, $H_{\hat{K}}(\cdot)$ is the one-way hash function using the master key \hat{K} .

3.1.2.2. Cheater Identification Phase:

Step 1: Produce n binary matrixes \hat{D}_i of size $l_v \times l_m$ using \hat{k}_i , $i = 1, 2, \dots \dots n$

$$[\hat{D}_i]_{l_v \times l_m} = RNG_K(\hat{k}_i) \quad (14)$$

Here, $RNG_K(\hat{k}_i)$ is the random number generator with the master key K and taking \hat{k}_i as the initial seed.

Step 2: Respect the m modules in the QR data codewords of QR_i as a matrix \check{M}_i with measure $l_m \times 1, i = 1, 2, \dots \dots n$.

Step 3: Have the authentication results \check{v}_i using the formula:

$$[\check{v}_i] = [\check{D}_i]_{l_v \times l_m} \times [\check{M}_i]_{l_m \times 1}, i = 1, 2, \dots \dots n \quad (15)$$

Step 4: Confirm the validity of the gave QR_i and \check{k}_i by looking at \check{v}_i with $\check{v}_i, i = 1, 2, \dots \dots n$. In the event that \check{v}_i varies from \check{v}_i , the QR_i is demonstrated as "altered" for the i^{th} member, and the secret uncovering technique will be ended. Something else, if \check{v}_i is equivalent to $\check{v}_i, i = 1, 2, \dots \dots n$, the gave QR barcode and keys are viewed as "approved," and the secret retrieval stage can be performed in the following procedure.

3.1.2.3. Secret Retrieval Phase:

Step 1: Develop n binary matrices \check{D}_i with measure $l_s \times l_m$ by the key \check{k}_i , $[\check{D}_i]_{l_s \times l_m} = RNG(k_i), i = 1, 2, \dots \dots n$ here $RNG(k_i)$ is an irregular number generator utilizing the key k_i as the initial seed.

Step 2: Derive n shadow matrices $[\hat{s}_i], i = 1, 2, \dots \dots n$, by playing out the binary multiplication as :

$$[\hat{s}_i] = [\check{D}_i]_{l_s \times l_m} \times [\check{M}_i]_{l_m \times 1} \quad (16)$$

Step 3: Genrate the secret matrix \hat{S} with the length of $l_s \times 1$.

$$\hat{S} = s_1 \theta s_2 \theta \dots \dots \dots \theta s_n. \quad (17)$$

The verified members inevitably can reveal the unique secret S by with respect to the 2-D matrix \hat{S} to 1-D bit stream.

3.2 Reed Solomon Code:

The fundamental guideline of Reed Solomon Encoding is to modify the first information so it turns into an ideal various of another predefined polynomial called the encoding polynomial. The process in the algorithm form is as follows:

Reed Solomon Encoding Algorithm :

- i. Produce an encoding polynomial
- ii. Now move original data polynomial for making the space for the parity data (shifting of the original data depends on the requirement of the number of error correction bits)
- iii. Now we will divide the modified polynomial by the encoding polynomial and take the remainder value.
- iv. For generating the perfect multiplication of the encoding polynomial we will subtract the remainder from the modified data.

Reed Solomon Decoding :

Reed Solomon decoding is the technique of repairing the data. As there is only one way for the encoding the data using the Reed Solomon Code but for the decoding there are various ways. So there are lots of the decoding algorithms for decoding the data with Reed Solomon code. The decoding process of the Reed Solomon code are generally outlined in the five steps :

- i. Computing the Syndromes Polynomial it allows us to check the characters in respect to which character is corrupted or in error. And also fastly can check for the input message if itself it is corrupted.
- ii. From the syndrome computing the erasure / error Locator Polynomial, it is computed by Berlekamp – massey , it is basically a detector which gives us the exact characters which are corrupted.
- iii. From the syndromes and the erasure/ error locator polynomial compute the erasure / error Evaluator Polynomial , it will evaluate at what level the characters are corrupted that means it helps for computing the magnitude.
- iv. Using the above three polynomial , compute the erasure / error magnitude polynomial this polynomial also known as the corruption polynomial , it has the property that storing the value which is required to subtract from the received message for retrieving the original message or correct message. In this polynomial we remove the

noise and store in the erasure / error magnitude polynomial and we will remove the noise from the original data to renovate it.

- v. Repairing the input message : for repairing the original message we have to subtract the magnitude value from the input data.

Generator Polynomial:

A Reed-Solomon codeword is created utilizing a particular polynomial. All substantial codewords are precisely detachable from the generator polynomial. The general type of the constructor polynomial is:

$$f(x) = (x - \alpha^i) (x - \alpha^{i+1}) \dots \dots \dots (x - \alpha^{i+2t}) \tag{18}$$

Codeword is derived as:

$$c(x) = f(x).i(x) \tag{19}$$

Here , $f(x)$ is the generator polynomial, $i(x)$ is the information block, $c(x)$ is a valid codeword.

Encoding: The $2t$ parity symbols in a systematic Reed-Solomon codeword are given by:

$$p(x) = i(x).x^{n-k} \text{ mod } f(x) \tag{20}$$

Decoding: The received codeword $r(x)$ is the original (transmitted) codeword $c(x)$ plus errors:

$$r(x) = c(x) + e(x) \tag{21}$$

A Reed-Solomon decoder endeavors to recognize the position and extent of up to t errors(or $2t$ erasures) and to adjust the errors or eradications.

4.1 Genrating the shares with threshold value :

For genrating the shares ,at the run time we give the following information :

- i. Number of shares, here gives the information about the total number of shares we want for the secret data (here total number of shares=7).
- ii. Set the threshold value , how many shares are required to redrive the original data (Threshold value set to N=4).
- iii. Now write the secret message which want to share and protect it by providing the password.

```

object?  -> Details about 'object', use 'object??' for extra details.

In [1]: runfile('C:/Users/india/Desktop/project/main.py', wdir='C:/Users/india/Desktop/
project')

Enter Number of shares required(greater than 1) : 7

Enter Number of shares required to recover : 4

Enter your message to share : hi,this is my message to share with QR code

Enter your password : py1
['__add__', '__alloc__', '__class__', '__contains__', '__delattr__', '__delitem__',
 '__doc__', '__eq__', '__format__', '__ge__', '__getattr__', '__getitem__',
 '__gt__', '__hash__', '__iadd__', '__imul__', '__init__', '__iter__', '__le__',
 '__len__', '__lt__', '__mul__', '__ne__', '__new__', '__reduce__', '__reduce_ex__',
 '__repr__', '__rmul__', '__setattr__', '__setitem__', '__sizeof__', '__str__',
 '__subclasshook__', 'append', 'capitalize', 'center', 'count', 'decode', 'endswith',
 'expandtabs', 'extend', 'find', 'fromhex', 'index', 'insert', 'isalnum', 'isalpha',
 'isdigit', 'islower', 'isspace', 'istitle', 'isupper', 'join', 'ljust', 'lower',
 'lstrip', 'partition', 'pop', 'remove', 'replace', 'reverse', 'rfind', 'rindex',
 'rjust', 'rpartition', 'rsplit', 'rstrip', 'split', 'splitlines', 'startswith', 'strip',
 'swapcase', 'title', 'translate', 'upper', 'zfill']
['1-6aabb46f25cb40b052dc7add6025e6ac708339a4f797981daf4c8254ad19237b141dd828d2d4f007',
'2-5264aa2e59fa0f7e51e5f03335949efe45da561199dd6c90cc794498ad2603ee0b138fde1aad5b66']
IPython console  Variable explorer  File explorer  Help

History log
history.py
## ---(Sat Jul 21 20:26:01 2018)---
runfile('C:/Users/india/Desktop/project/main.py', wdir='C:/Users/india/Desktop/
project')
runfile('C:/Users/india/Desktop/project/recover.py', wdir='C:/Users/india/Desktop/
project')

## ---(Sun Jul 22 09:30:17 2018)---
runfile('C:/Users/india/Desktop/project/main.py', wdir='C:/Users/india/Desktop/
project')

Permissions: RW  End-of-lines: CRLF  Encoding: UTF-8  Line: 7  Column: 1  Memory: 58 %

```

Fig. 4.1 Shows information about the shares

The following output screen shows the Cover QR code for the share -1.

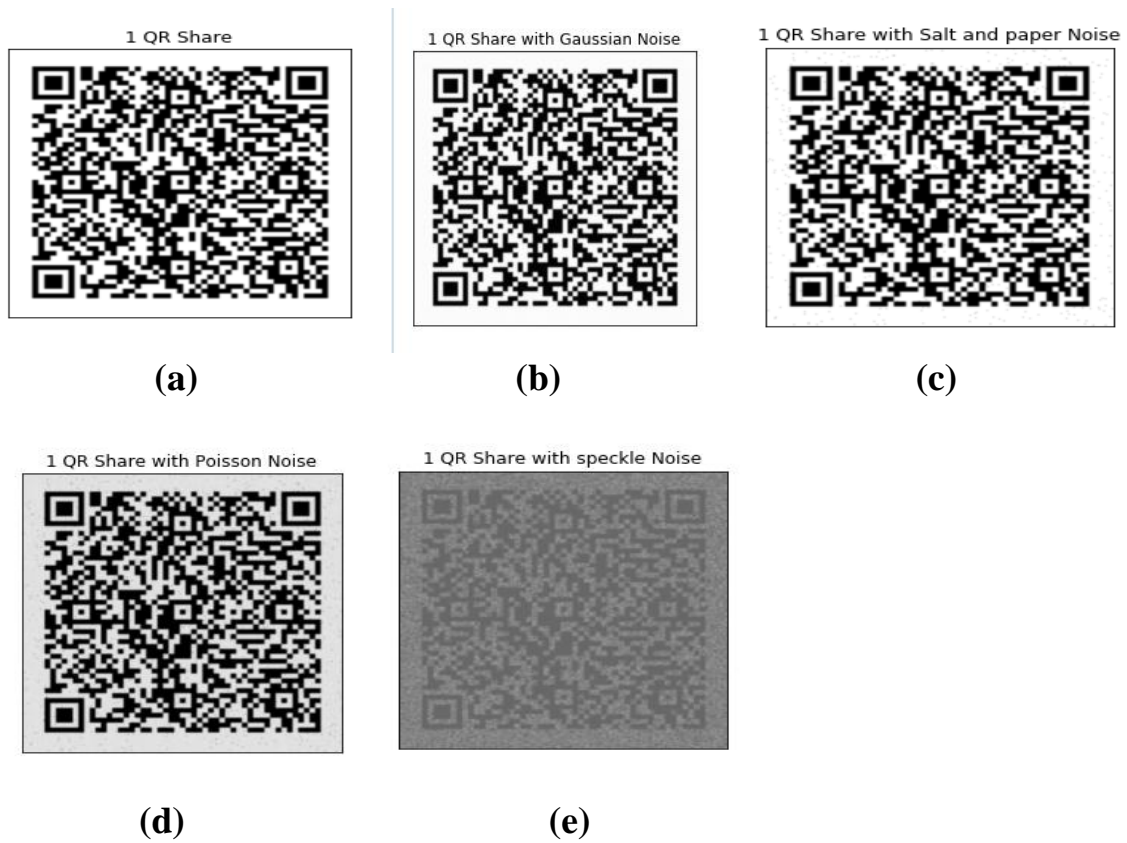


Fig. 4.2 (4-4)-Threshold sharing Cover QR code for share-1 (a) Cover QR image 1. (b) Cover QR image 2. (c) Cover QR image 3. (d) Cover QR image 4. (e) Cover QR image 5

The following output screen shows the all shares of the secret data with the cover QR code for each shares. For the each share of the secret there is cover Qr code with the different noises , Gaussian noise ,Salt and Paper noise, Poisson noise and Speckle noise.



Fig.4.3 (4,4)-Threshold sharing, with all the shares of cover QR code .

4.2 Recovery of the Secret data :

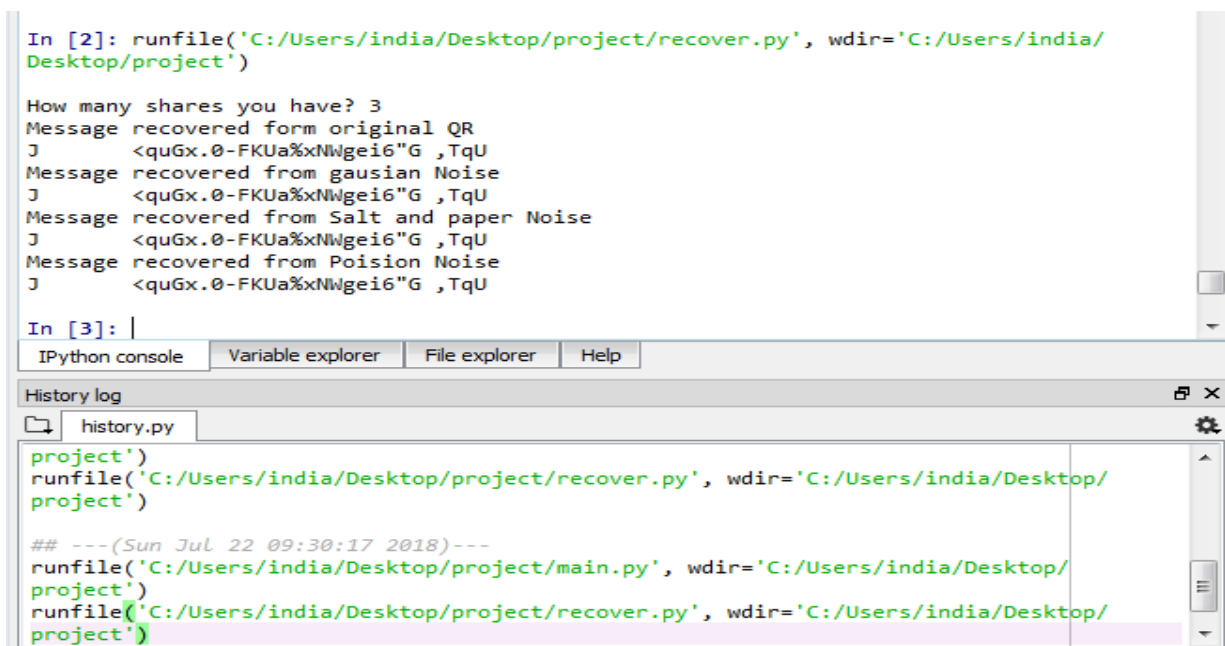
For recovering the original data we need the total number of share equal to the threshold value . Shares less than the threshold value can not retrieve the original data for retrieving the original data . Here for the output there are three cases possible as:

Case-1 : When number of share less than the Threshold value.

Case -2 : When number of shares equal to the Threshold value.

Case -3 : When number of shares greater the the Threshold value.

Case-1 : When number of share less than the Threshold value. (Here, threshold value = 4 and number of shares to recover data = 3)



```
In [2]: runfile('C:/Users/india/Desktop/project/recover.py', wdir='C:/Users/india/Desktop/project')

How many shares you have? 3
Message recovered form original QR
J <quGx.0-FKUa%Nwgei6"G ,TqU
Message recovered from gaussian Noise
J <quGx.0-FKUa%Nwgei6"G ,TqU
Message recovered from Salt and paper Noise
J <quGx.0-FKUa%Nwgei6"G ,TqU
Message recovered from Poision Noise
J <quGx.0-FKUa%Nwgei6"G ,TqU

In [3]: |

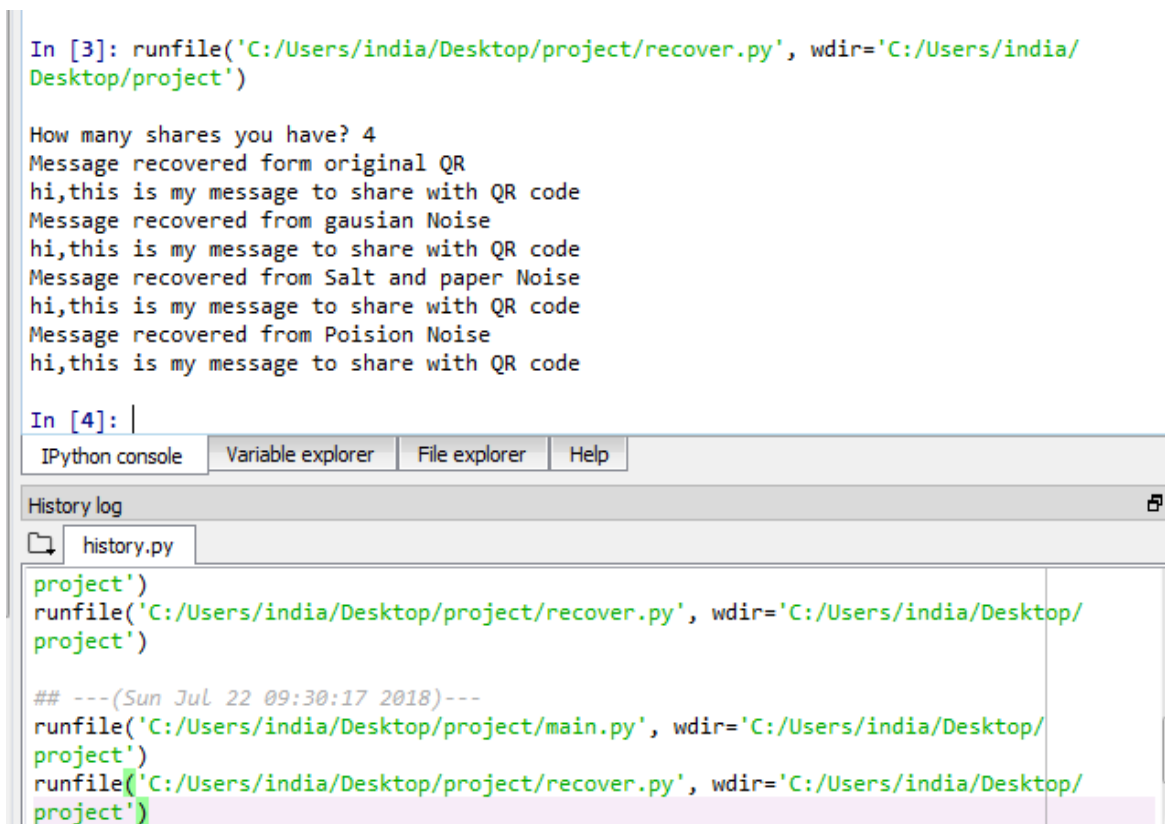
IPython console Variable explorer File explorer Help

History log
history.py
runfile('C:/Users/india/Desktop/project/recover.py', wdir='C:/Users/india/Desktop/project')
## ---(Sun Jul 22 09:30:17 2018)---
runfile('C:/Users/india/Desktop/project/main.py', wdir='C:/Users/india/Desktop/project')
runfile('C:/Users/india/Desktop/project/recover.py', wdir='C:/Users/india/Desktop/project')
```

Fig. 4.4. Showing result when number of shares are less than threshold value

In my output I have set the threshold the value as 4 and here, I am passing the threshold value as 3. For the retrival of the original message atleast 4- shares are required and I have pass the 3 shares, so original message is not recovered :

Case -2 : When number of shares equal to the Threshold value. (Threshold value = 4 and number of shares passing = 4)



```
In [3]: runfile('C:/Users/india/Desktop/project/recover.py', wdir='C:/Users/india/Desktop/project')

How many shares you have? 4
Message recovered form original QR
hi,this is my message to share with QR code
Message recovered from gaussian Noise
hi,this is my message to share with QR code
Message recovered from Salt and paper Noise
hi,this is my message to share with QR code
Message recovered from Poision Noise
hi,this is my message to share with QR code

In [4]: |
```

IPython console Variable explorer File explorer Help

History log

history.py

```
project')
runfile('C:/Users/india/Desktop/project/recover.py', wdir='C:/Users/india/Desktop/project')

## ---(Sun Jul 22 09:30:17 2018)---
runfile('C:/Users/india/Desktop/project/main.py', wdir='C:/Users/india/Desktop/project')
runfile('C:/Users/india/Desktop/project/recover.py', wdir='C:/Users/india/Desktop/project')
```

Fig.4.5 when number of shares equal to the threshold value

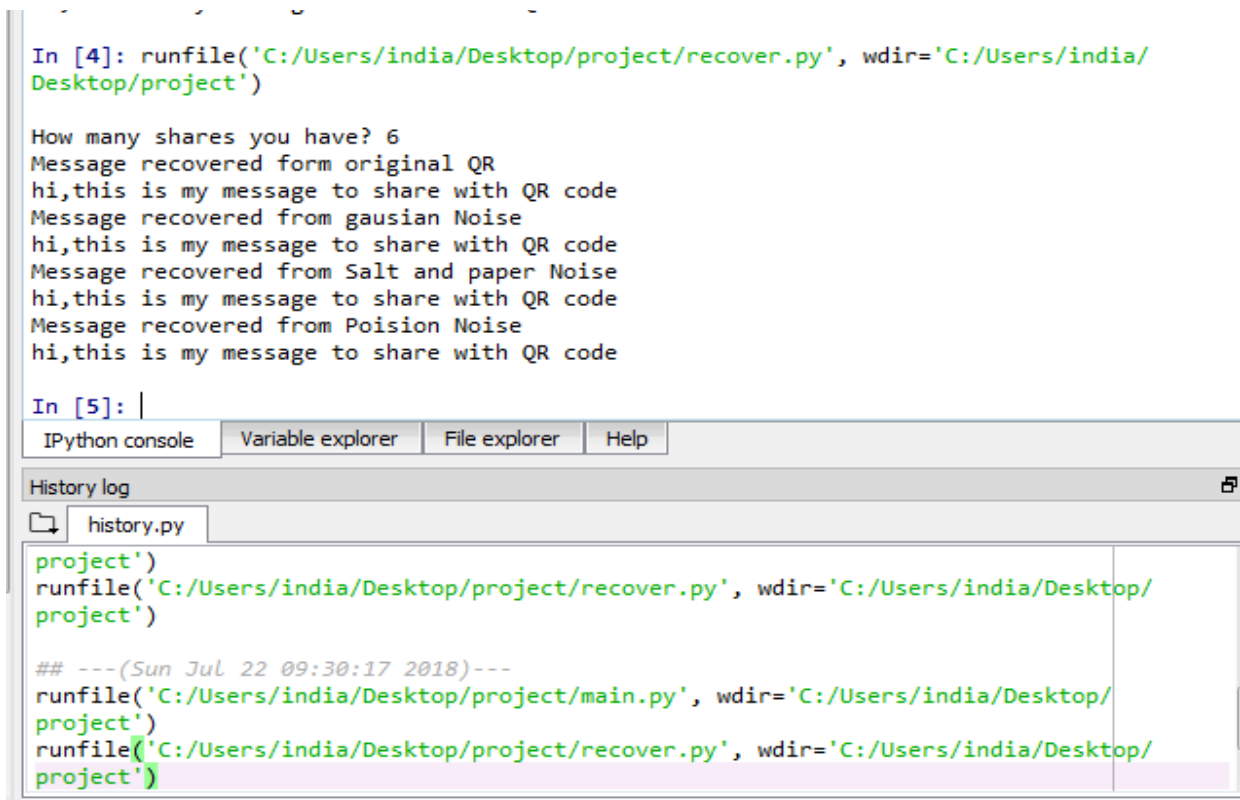
Here, number of shares I have pass is equal to the threshold value i.e 4. So here I have have the number of shares equal to the threshold value the original messge has recovered successfully :

Case -3 : When number of shares greater the the Threshold value. (Threshold value = 4 and number of shares to recover original message = 6)

```
In [4]: runfile('C:/Users/india/Desktop/project/recover.py', wdir='C:/Users/india/Desktop/project')

How many shares you have? 6
Message recovered form original QR
hi,this is my message to share with QR code
Message recovered from gaussian Noise
hi,this is my message to share with QR code
Message recovered from Salt and paper Noise
hi,this is my message to share with QR code
Message recovered from Poision Noise
hi,this is my message to share with QR code

In [5]: |
```



IPython console Variable explorer File explorer Help

History log

```
project')
runfile('C:/Users/india/Desktop/project/recover.py', wdir='C:/Users/india/Desktop/project')

## ---(Sun Jul 22 09:30:17 2018)---
runfile('C:/Users/india/Desktop/project/main.py', wdir='C:/Users/india/Desktop/project')
runfile('C:/Users/india/Desktop/project/recover.py', wdir='C:/Users/india/Desktop/project')
```

Fig.4.6 when number of shares more than the threshold value

For retriving the original data we need the number of shares atleast equal to the threshold value. So thenumber of shares same as the threshold value of greater than the threshold are able to retrieve the original data successfully.

CONCLUSION AND FUTURE WORK

5.1 Conclusion

We can conclude that Reed Solomon code has enhances the security of the QR code with the Distributed Secret Sharing Scheme. Unique in relation to the customary QR applications, the designed approach uses the features of the QR modules to fulfil the fundamentals of readability, steganography, robustness, adjustable secret capacity, blind extraction and also able to identify cheaters for the secret sharing mechanism. Original data can be retrieved even if the some part of the QR code damaged. Reed Solomon code can correct the data if the data is modified by the noise or corrupted. Reed Solomon capable of correcting the errors of the burst type. Hence Reed Solomon code with the (N,N)-threshold Secret Sharing technique enhance the security of the QR code by providing the capability for detecting and correcting the errors.

5.2 Future Work

And as a part of the future work, We can apply the Reed Solomon code with the other secret sharing sharing schemes for the QR code such as Visual Secret Sharing Scheme for the QR code, Shamir's Secret Sharing technique based on polynomial interpolation. Reed Solomon code with these secret sharing technique enhances the security of the QR code. Also will enhance the robustness and readability of QR code.

REFERENCES

- [1]. Pei-Yu Lin, Member, IEEE ,“Distributed Secret Sharing Approach With Cheater Prevention Based on QR Code,” *IEE Transactions on industrial informatics*,(vol. 12, no. 1, february 2016).
- [2]. Monu Verma and Rajneesh Rani, “Strong Threshold Secret Image Sharing Based On Boolean Operation ,” *Communication and Automation (ICCCA2016)*.
- [3]. Shalini I S, Mohan Naik R and Dr. S V Sathyanarayana “A Comparative Analysis of Secret Sharing Schemes with Special Reference to e-Commerce Applications,” on *Emerging Research in Electronics, Computer Science and Technology – 2015*.
- [4]. J. C. Chuang, Y. C. Hu, and H. J. Ko, “A novel secret sharing technique using QR code,” *Int. J. Image Process.*, vol. 4, pp. 468–475, 2010.
- [5]. H. C. Huang, F. C. Chang, and W. C. Fang, “Reversible data hiding with histogram-based difference expansion for QR code applications,” *IEEE Trans. Consum. Electron.*, vol. 57, no. 2, pp. 779–787, May 2011.
- [6]. S. Dey, K. Mondal, J. Nath, and A. Nath, “Advanced steganography algorithm using randomized intermediate QR host embedded with any encrypted secret message: ASA_QR algorithm,” *Int. J. Mod. Educ. Comput. Sci.*, vol. 6, pp. 59–67, 2012.
- [7]. C. H. Chung, W. Y. Chen, and C. M. Tu, “Image hidden technique using QR-Barcode,” in *Proc. 5th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, 2009, pp. 522–525.
- [8]. W. Y. Chen and J. W. Wang, “Nested image steganography scheme using QR-barcode technique,” *Opt. Eng.*, vol. 48, no. 5, pp. 057004-01– 057004-10, 2009.
- [9]. M. Sun, J. Si, and S. Zhang, “Research on embedding and extracting methods for digital watermarks applied to QR code images,” *N. Z. J. Agric. Res.*, vol. 50, pp. 861–867, 2007.

- [10]. L. Li, R. L. Wang, and C. C. Chang, "A digital watermark algorithm for QR code," *Int. J. Intell. Inf. Process.*, vol. 2, no. 2, pp. 29–36, 2011.
- [11]. S. Rungraungsilp, M. Ketcham, V. Kosolvijak, and S. Vongpradhip, "Data hiding method for QR code based on watermark by compare DCT with DFT domain," in *Proc. Int. Conf. Comput. Commun. Technol.*, 2012, pp. 144–148.
- [12]. M. Gao and B. Sun, "Blind watermark algorithm based on QR barcode," in *Foundations of Intelligent Systems*, Berlin, Germany: Springer-Verlag, vol. 122, 2011, pp. 457–462.
- [13]. Shalini I S, Mohan Naik R and Dr. S V Sathyanarayana "A Comparative Analysis of Secret Sharing Schemes with Special Reference to e-Commerce Applications," International Conference on Emerging Research in Electronics, Computer Science and Technology – 2015.
- [14]. Xuehu Yan Yuliang Lu, Canju Lu and Yuxin Chen "Secret image sharing based on error-correcting codes," 2017 IEEE 3rd International Conference on Big Data Security on Cloud.
- [15]. Psytec Inc., QR code editor software, 2013 [Online]. Available: <http://www.psytec.co.jp/docomo.html>
- [16]. H. Martin, P. Peris-Lopez, J. E. Tapiador, and E. San Millan, "An estimator for the ASIC footprint area of lightweight cryptographic algorithms," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1216–1225, May 2014.
- [17]. Y. J. Chiang, P. Y. Lin, R. Z. Wang, and Y. H. Chen, "Blind steganographic approach for QR code module based upon error correction capability," *KSII Trans. Internet Inf. Syst.*, vol. 7, no. 10, pp. 2527–2543, 2013.