IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CRYPTOGRAPHY BY USING QR CODE ENCRYPTION AND DECRYPTION METHOD

[1]Kishor kumar, [2]Rajkumar, [3]Vipin
[1]Scholar
[1]NIT kurukshetra

ABSTRACT

The QR code cryptography with a password and sends it to the required hiding the information QR code. Securing and hiding personal confidential information has become a challenge in these modern days. Due to the lack of security and confidentiality, there are chances that forgery of the confidential information or unauthorized access of a system can cause a big margin loss to a person or a system. At present, confidentiality is maintained in old ways and for that reason, there are possibilities that the confidential information might get forged or hacked. Personal confidential information can be securely shared with the expected person and the person can verify the information by checking its authenticity. Similarly, confidential information can also be kept securely hidden and used to meet a specific purpose like getting access privilege of a secured system and the system can validate the confidential information by checking whether the person is authorized or the information is valid. QR codes are being used increasingly to share data for different purposes. Ininformation communication, QR code is important because of its high data capacity. However, most existing QR code systems use insecure data format and encryption is rarely used. A user can use secure QR code technology to keep information secured and hidden.

Keywords: cryptography, encrypt, confidential, secure, QR code.

1 INTRODUCTION

Nowadays, it is almost impossible to secure and hide personal confidential information like system credentials, Automated Tray Machine(ATM) Card PINs, Ticket Passenger Name Record(PNR), etc., which can be easily hacked and used for unauthorized purposes. Such hacked information can cause huge loss to a person. At present, personal information confidentiality is done by the person's own manual unsecured way and there are chances that the information is not completely secured and hidden. Advanced Encryption Standard (AES) algorithm for legal document data hiding, message hiding, etc. [1-5]. However, these methodsdo not consider cases

when personal confidential information needs to be shared securely. Quick Response (QR) codes [6] are being used increasingly to share data for different purposes such as authentication, verification, etc. [7-8]. The popularity of QR code is because of its high data capacity, error correction capability using Reed-Solomon error correction algorithm [9], fast decoding, etc. However, most existing QR code systems use insecure data format and encryption is rarely used [10]. It is possible to use secure QR code technology to keep his important sensitive information perfectly secured at all times, without the information gets leaked to outside world. Cryptographic algorithms like AES, Data Encryption Standard (DES), Rivest, Shamir, Adleman (RSA) etc., can be used to make a QR code system secure [11-13].

1.1 Problem Statement

Hacking personal confidential information has become a significant problem these days. Persons are facing privacy threat and financial losses as a result of unauthenticated and unauthorized information. So, hiding and securing personal confidential information hasbecome a serious need; so, an effective and uniform process need to be designed and implemented for verifying the authenticity of personal confidential information as well as for authorizing the personal confidential information.

1.2 Motivation

In order to get rid of being forged personal confidential information, there is a need to verify and validate personal confidential information which is may be presented by a person like national citizen, job seeker, representative, passenger, audiences, etc. Providing an efficient and uniform process for prospective persons, institutions, companies or organizations toverify and validate personal confidential information will ensure that all personnel are truly verified and validated. This will prevent financial and productivity losses that are incurred dueto incorrect information. Using a web application, having verification and validation features for checking personal confidential information authenticity and validity, will be fast, effective, efficient and affordable. Lack of such an application motivated us to build a web based application for securing confidential information using QR code.

1.3 Objectives

The objective of this work is to design and implement a secure QR code system that can be used for authenticity and confidentiality of personal sensitive information. To achieve this objective, the project has set the following goals:

- To propose infrastructure for the system.
- To analyze the security strength in comparison of existing conventional ways.

2 BACKGROUND

This chapter gives an overview of QR code technology and also provides the background information regarding the concepts of cryptography and the consecutive sections discuss about the concept of RSA algorithm and digital signature.

2.1 QR CODE

Quick Response (QR) code as shown in Figure 2.1 is a barcode standard developed by Japanese company Denso Wave in the 1990s. Compared to traditional 1D (1-dimensional) barcodes, QR codes are 2D (2-dimensional), allowing for a greater amount of information storage. QR code consists of a black square pattern on white background and it contains information in the vertical direction as well as the horizontal direction. QR codes have a wide variety of uses.

Figure 2.1: A Sample QR Code

2.1.1 QR Code Structure

Figure 2.2 shows QR structure regarding code version information, format information, data and error correction areas, required patterns (position detection pattern, alignment pattern and timing pattern) and quiet zone. QR Codes are 2-dimensional, which results in them having a square filled with data. Besides data, there are certain identifiers helping the code being read correctly. The most common QR Code type is model 2, which is broken down in the following information identifiers:

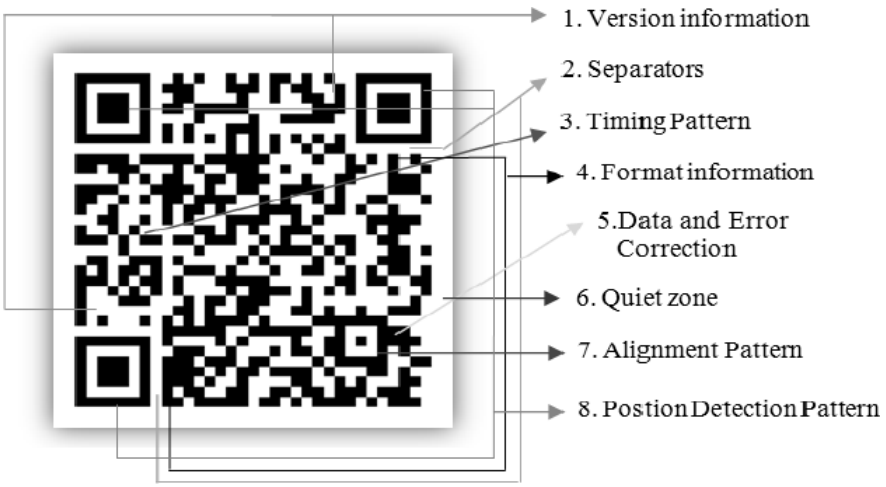


Figure 2.2: QR Code Structure [14]

Version and format information are important for the scanning device to know what kind of data to expect. QR codes have symbol versions from 1 to 40. It determines the data capacity of the code. So the more the data stored, the bigger the size of the QR code. Meanwhile, the data can be slightly damaged or missing and still be readable. This dependson the error correction level being used when writing the code. Rotation of QR Codes is possible whichever direction we may like. This is a courtesy of the position patterns (squares with dots in the middle) that allow the code to be read from any direction in 360 degrees. Meanwhile, the alignment patterns are used to assist in navigation of larger codes and the timing patterns are used to determine the size of modules. The quiet zone requires a margin ofat least 4-module worth.

2.1.2 Error Correction

QR codes have available functionality to restore data if the message is corrupted or damaged. There are four levels of Error Correction possible for QR codes. Level L, the lowest Error Correction rate, can reconstruct a damaged message with up to 7% corruption. Level Q, the highest Error Correction rate, will reconstruct a message containing 30% corruption. Level M, which has an error tolerance of 15%, is the most commonly used level. Error Correction is implemented according to the Reed-Solomon algorithm [9]. Reed-Solomon is a non-binary cyclic error correction method initially designed to reduce communication noise for artificial satellites. The error correcting method is capable of performing corrections in data at the byte level, which has come in handy products such as CDs, Blue-Ray Discs, and QR codes. A fundamental part of the way QR codes work is that the more data we put into them, the more rows and columns of modules will be introduced into the QR code to compensate for the increased data load. As the error correction level increases, this means there will also be an increase in the number of rows and columns of modules required to store the original dataplus the increasing amount of backup codeword. This is shown in Figure 2.3 – the QR code becomes denser as the error correction increases from Level L to Level H, even though the QR codes contain exactly the same information. Quite conveniently, there is also 2 modules down in the Bottom left-hand corner of every QR code that display what the error correction level used in that QR code. Becomes denser as the error correction increases from Level L to Level H even though the QR codes contain exactly the same information. Quite conveniently, there is also 2 modules down in the bottom left-hand corner of every QR code that display what the error correction level used in that QR code.

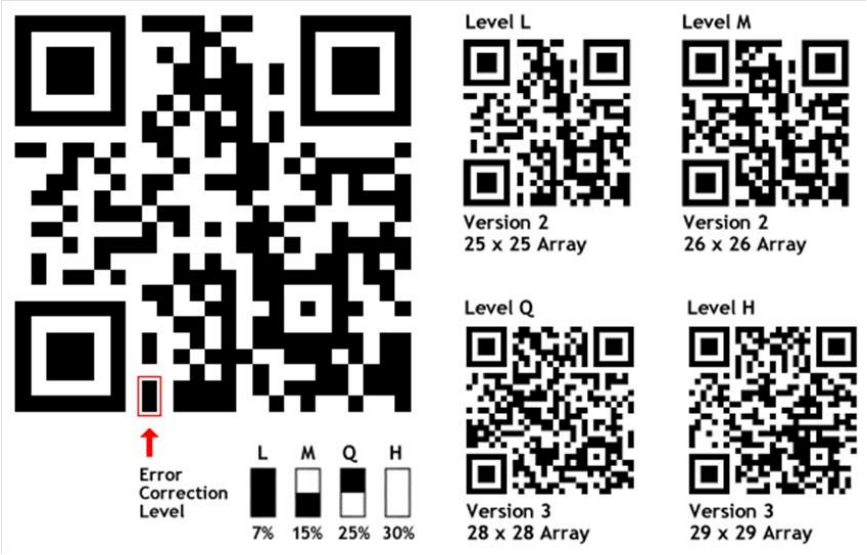


Figure 2.3: QR Code being Error Correction Level Used [15]

2.1.3 Uses of QR Code

- It can be used to share a video or any wepage link.
- It can link a social networking function such as 'Like' button of any page on Facebook.
- It can be used in visiting cards and products to include information such price, address, etc.
- It can be used to locate places

2.1.4 Generation and Scanning of a Simple QR Code

It gives a simplified description of the standard process of generating a QR code from a provided message and scanning the code with a smart phone or a comparable device When provided a message string, the encoder converts the message into a byte string interleaved with general QR header information, error correction bytes, and a masking element.

This modified byte string is then converted to a 2-dimensional matrix of 1's (white) and zeroes (black) which can be synthesized into an image. When this image is scanned by a QR code reader, the byte string is retrieved and converted to the intended message, viewable by the person who initiated the scan.

2.1 Cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of the third parties called adversaries. Cryptography is done by following two basic steps: encryption and decryption.

- Encryption is converting the original information into unreadable cipher information by using a key (or in other words set of rules).
- Decryption is converting back the cipher information into the originalinformation

by using a key (or in other words set of rules). By these two steps, cryptography protects the information while sharing it with others so that only desired person can access thedata.

2.2.1 Types of Cryptographic Algorithms

Cryptographic algorithm can be classified in several ways. On the base of number of keys used to encrypt and decrypt, cryptographic algorithm can be classified into the following:

- Symmetric Cryptography or Secret Key Cryptography (SKC)
- Asymmetric Cryptography or Public Key Cryptography (PKC)
- Hash Function

2.2.1.1 Symmetric Cryptography

Symmetric Cryptography, also known as Secret key cryptography, uses a single keyfor both encryption and decryption process during the communication.

As shown in Figure 2.4, symmetric cryptography follows these steps:

1. The sender converts the plain text into cipher text by using a private key (shared secret key).

2. The sender sends the cipher text to the recipient.
3. At the receiver end, the cipher data is converted back into plain text using the same private key.

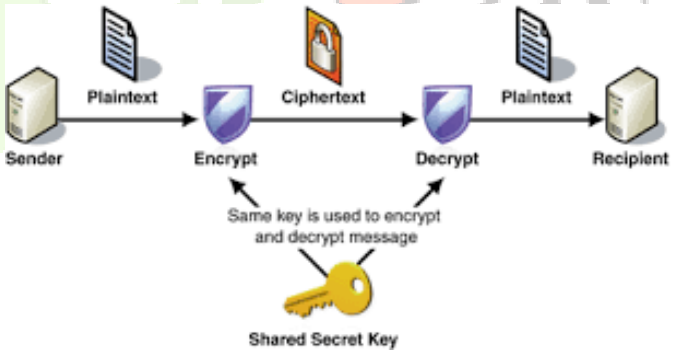
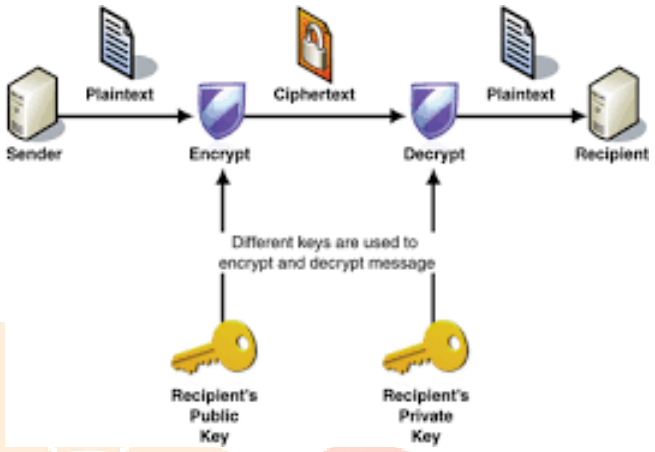


Figure 2.4: Symmetric Cryptography [16]

In this type of cryptography, it is obvious that the private key must be shared between the sender and the receiver before the transfer of data. Sharing the key is the difficult part.

2.2.1.2 Asymmetric Cryptography

Asymmetric cryptography, also known as Public Key Cryptography, uses two different keys, namely private key and public key, for encryption and decryption process respectively. Public key is generally used to encrypt the data and the public key is distributed openly to anyone who needs to communicate with the recipient. And, the private key is used to decrypt the encrypted data in the receiving end.



2.5 Asymmetric Cryptography[16]

As shown in Figure 2.6, the Asymmetric cryptography follows these steps:

1. The sender converts the plain text into cipher text by asymmetric encryption algorithm using the public key of the recipient.

2. The cipher data is transferred to the recipient.

3. The receiver converts back the cipher text into plain text by asymmetric decryption algorithm using the private key that corresponds to the public key used by the sender.

The most commonly used asymmetric algorithm is the RSA algorithm. PKC is used in digital signatures, key management purposes and for facilitating non-repudiation.

2.2.1.3 Hash Functions

In Figure 2.7, a hash function, H, is a transformation that takes a variable-size input m and returns a fixed-size message digest string, which is called the hash value h, that is,

$$h = H(m).$$

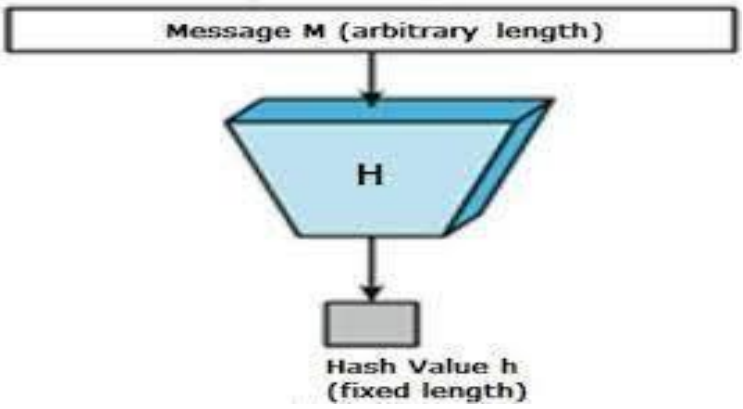


Figure 2.6: Hash Functions [17]

A hash function H is said to be one-way that means if a hash value h is given, thenit is computationally infeasible to find some input x, such that,

$$H(x) = h.$$

The reasons for using hash function or message digest in digital signature are as follows:

- For efficiency: The signature will be much shorter and hence, will be faster.
- For compatibility: A hash function can be used to convert an arbitrary input into the fixed format.
- For integrity: Without the hash function, the original message has to be separated into small blocks to use the signature scheme. Hence, there would be a lot of signed blocks. This can be prevented using the hash function.

2.2.2 RSA Algorithm

RSA algorithm is used in two important scenarios, Public key encryption and digital signature. This algorithm is considered to be one of the most secured algorithms because it uses large integers as the keys to perform the encryption and decryption. It takes years to findthe factors of the keys which make the system secure.

The RSA algorithm works in three steps:

1. RSA Key generation
2. Encryption and
3. Decryption

2.2.2.1 RSA Key Generation

RSA algorithm uses two different keys: public key and private key. Usually, public key is used to encrypt the data and private key is used to decrypt the data. The public key is distributed to everyone and the private key is kept secret. Both private key and public key is generated by the receiver. In RSA algorithm, the key is generated in the following steps:

1. Two integer prime numbers p and q are chosen randomly. These number should have similar bit length.
2. N is the product of the chosen prime numbers p and q, that is,

$$n = pq.$$

3. Now, n is used to generate both public and private keys. φ (n) is generated where, φis Euler's totient function, that is,

$$\Phi (n) = \varphi (p)\, \varphi (q) = (p - 1)(q - 1).$$

4. Choose an integer e, which is public key exponent, such that e and φ(n) are co- prime, that is,

$$\text{Gcd } (e, \varphi (n)) = 1$$

5. Private Key exponent d is generated using the Euclidean algorithm, that is,

$$d \cdot e \equiv 1 \pmod{\varphi (n)}.$$

The public key consists of the modulus n and the public (or encryption) key exponent e. The private key consists of the modulus n and the private (or decryption) key exponent d, which must be kept secret. p, q, and φ(n) must also be kept secret, because they can be used to calculate d.

2.2.2.2 Encryption

After generating the public and private key, the receiver publishes the public key (n, e). The encryption on the sender's side follows these steps:

1. The original message M is converted into an integer m, such that,

$$0 \leq m < n$$

2. Then, the integer m is encrypted to the cipher text c by using the padding scheme, that is,

$$C \equiv m^e \pmod{n}.$$

3. Then, the encrypted cipher text is sent to the receiver.

2.2.2.3 Decryption

The receiver decrypts the cipher text c into the original message m using the private key exponent d by reversing the padding scheme, that is,

$$M \equiv c^d \pmod{n}.$$

2.2.3 RSA Key Length

When we talk about the key length of an RSA key, we are referring to the length of the modulus, n, in bits. A key length of 512 bits is no longer considered that secure although cracking it is still not that trivial task but it is faster than both key lengths 1024 and 2048. A key length of 2048 bits is considered to be very slow for generating a big cipher. Thatis why, 1024-bit key length was our choice to preserve a secure encryption with sort of acceptable execution time, and cipher's length.

2.2.4 Security of RSA

Obviously, the longer a number is, the harder is to factor, and so the better the security of RSA. As theory and computers improve, large and large keys will have to be used. The disadvantage in using extremely long keys is the computational overhead involved in encryption/decryption. RSA's future security relies solely on advances in factoring techniques.

2.2.5 Digital Signature

Digital signature is an electronic signature used to authenticate digitally transferred data and to ensure that the content of the message or the document sent has no changes as shown in Figure 2.8. Digital signature cannot be imitated and can be time stamped automatically, avoiding the chances of the sender to repudiate it later. Digital signature of the digital certificate- issuing authority is also included in the digital certificate, so it is possible tocheck the originality of the certificate by anyone. Digital signature has same value as the physical signature on paper. It uses asymmetric cryptography to encrypt the data, providing reason to believe that the data was send by the claimed sender. The digital signature provides four main characters for the data sent which are given in the following sections.

2.2.5.1 Confidentiality and Privacy

Data is encrypted; the confidentiality and privacy of the data is confirmed.

2.2.5.2 Authentication

The identity of the sender is ensured by the digital certificate. So, the receiver can verify identity of the sender.

2.2.5.3 Integrity

Digital signature ensures that the data is not tampered during the transfer.

2.2.5.4 Non – Repudiation

It ensures the authenticity of the sender. The false denial of the sender is also not possible.

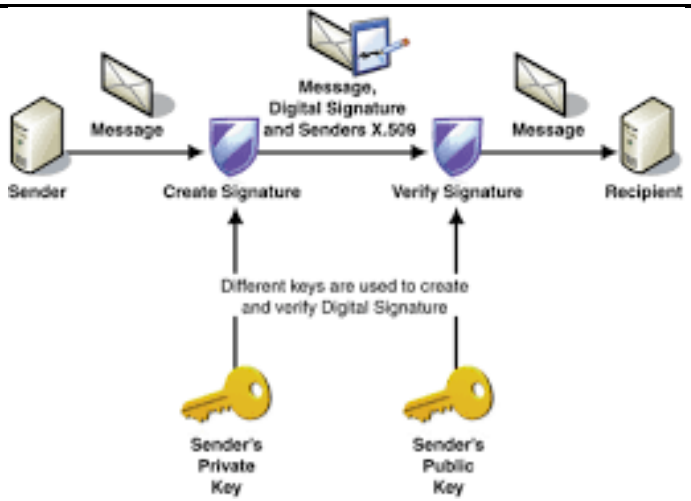


Figure 2.7: Digital Signature [18].

Digital signature is one of the concepts in public Key Infrastructure; the information or the identity of the user is tied to the public key. The digital certificate is signed by the Certification Authority (CA) that provided it, to ensure trust in the signed data. Digitalsignature software became a powerful business tool in recent years. It provides ability to sign online. Documents, contracts, different kinds of form, tax filing can be signed online. This technology is secure, robust, and efficient, and saves all parties time, money, and hassle.

2.2.6 Signing and Verification in Digital Signature

Digital signature uses asymmetric cryptography to encrypt the data. We can split the process into two parts: signing by the sender and verification by the receiver. Figure 2.8 explains the signing and verification part of the digital signature. The digital signature for the data is generated in two steps:

1. Generation of the message digest: The message digest is generated using hash algorithm. This gives a binary message of the original message.

2. The generated message digest is encrypted by the sender's private key. The encrypted message digest is known as the digital signature.

Both the original data and the digital signature are sent to the receiver. Verificationon the receiver end is done by the following steps:

1. Receiver receives original data with the digital signature.

2. The digital signature is decrypted by using the sender's public key to get the hash data that is the message digest; let it be message digest 1.

3. The original data is converted into message digest using the same hashing algorithm used by the sender; let it be message digest 2.

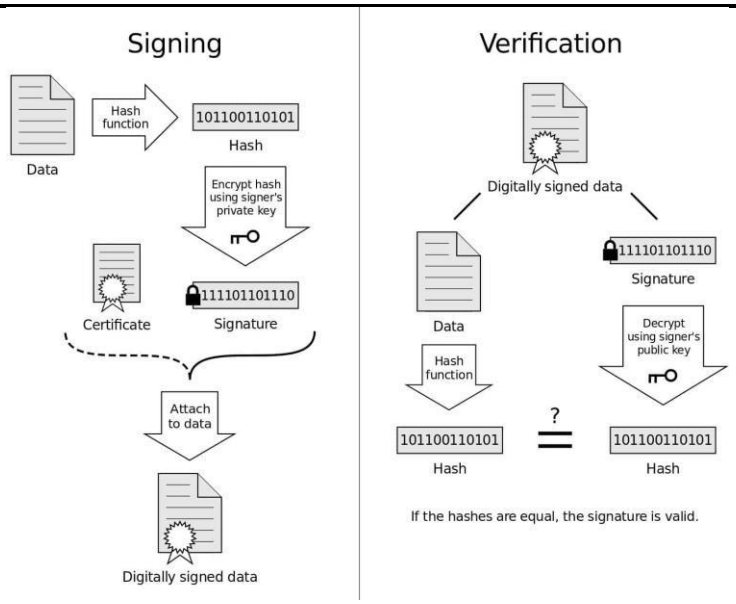


Figure 2.8: Signing and Verification of Digital signature [19].

The message digest 1 and message digest 2 are compared as following:

- If they match each other, then the received data is not been tampered.
- If they don't match each other, then the message has been changed after the data is send by the sender.

This provides the authenticity and integrity for the document transferred.

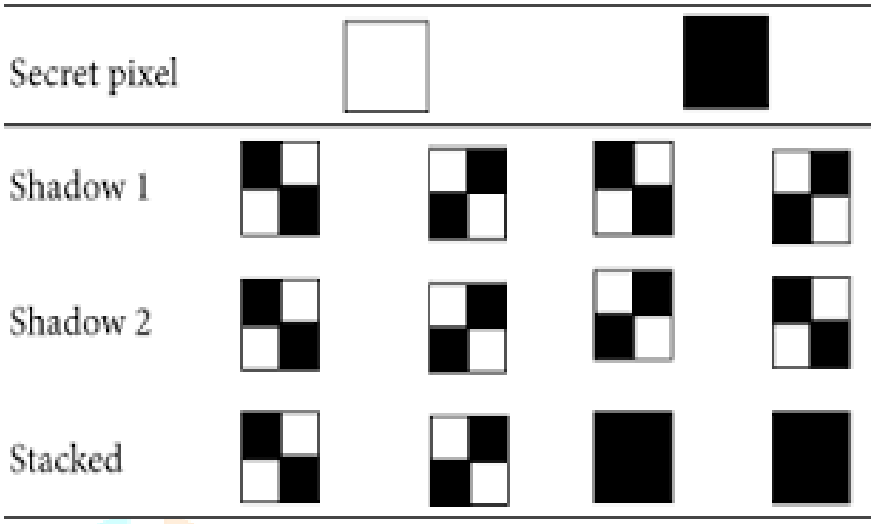
2.3 Visual Cryptography

Visual cryptographic scheme (VCS) is a generalization of secret sharing and was first proposed by Naor and Shamir in 1995 in their scheme [14]. An original halftone image isdivided into shared images and each shared image is printed on a transparent film, such that any films stacked together can restore the original image. However, for the case with lessthan films, the original image cannot be restored. This program mainly uses the human visualsystem of color approximation principle. Therefore, the secret image restoration can beimplemented by a simple film superposition without any password calculation.

Each pixel of the images is divided into smaller blocks. There is always the same number of white and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks.In Figure 3 a pixel is divided into four parts, and it has two different states. If the pixel is white, it can be divided into two blocks and each block has a black pixel and a white pixel.

When the secret image is split, the block is randomly filled into two shadows. When the two blocks are superimposed together, gray blocks appear to simulate the white pixels. If the pixelis black, the two blocks are complementary. When the two blocks are superimposed, they present black pixels. Thus, shadow images that are split by secret image become a chaotic maps and no

information can be inferred from the secret image. Secret images can be restoredwhen the two shadows overlay. Moreover, the stacking process does not require any calculations.



2.9 visual cryptography

2.4 Summary

In this chapter, we have discussed about the QR code in detail in a way that how it is structured, how QR Code negotiates with the error it may face depending on different circumstances and how it is generated. However, conventional standard QR Code generation does not include any kind of security features. It just encodes a plain text into a QR Code and in turn a QR Code reader can read the QR Code and can see the plaintext after the text being decoded. From this chapter, we have also discussed cryptography especially about the RSA key generation algorithm as well as encryption and decryption mechanism in RSA public key cryptography. We have also discussed about the fact that how the message is digitally signed and verified with the help of hash algorithm and RSA algorithm.

3 LITERATURE REVIEW

In this chapter we have discussed about some researches done in this field – their contribution and the mechanisms used to improve the systems. Some of the notable works are:

3.1 Embedded qr-code

In this “mainly focus on confidential encrypted data hiding in QR Code. As we know that data embedding and retrieval from QR-code is very simple issue. Simply a smart phone running on Android or iOS or any other new generation of mobile OS, can be used to extract the encrypted data from embedded QR-code and finally that data to be decrypted using the TTJSA decryption algorithm.

3.2 Encrypt and Decrypt

Hiding of Confidential Data and its Retrieval using advanced Algorithms and QR Authentication system. A smart phone running on Android or iOS or any other new generation of mobile OS, can be used to extract the encrypted data from embedded QR-code and finally that data to be decrypted using the TTJSA decryption algorithm. They have used three types of algorithms to Encrypt and Decrypt the data or any type of information. With theanalysis of all these three algorithms using different formats of images we conclude that the Vernam method is more acceptable to encrypt the images or data.

3.3 RSA cryptographic algorithm

An innovative method to prevent forgery of data like personal confidential information. Here, we designed and implemented a SQRC system for sharing personal confidential information with the help of RSA cryptographic algorithm. It replaces sensitive information on paper documents with encrypted QR codes. The SQRC system can be applied to a range of real- world applications that involve sensitive information sharing.

3.4 encrypted in mobile

Anti-phishing technique using mobile to provide higher level security to the user. Nowadays, the User can access the data from various website through different local computers but that data is not secure because there could be a fake website. In this the Two-Level Security by generating two QR codes one on website and another on user's mobile phone. Intruder cannot obtain the user's personal information because user data is encrypted in mobile device. Servercan check the Uses authentication information on computer and mobile device. Only authorized user with password can only login and retrieve the personal data and secretinformation. Aim of developing this technology is to provide scalability, flexibility for secure communication between mobile device and un-trusted computer.

3.5 One time password

In the new authentication scheme for secure OTP(One Time Password) distribution in phishing website detection through EVC(extended visual cryptography) and QR codes. He used extended visual cryptography techniques to solve the problem of phishing and did the relevant validation.

3.6 Image encryption

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by human visualwithout the aid of compute.

3.7 Analysis

This is the second phase of methodology which involves analyzing the requirements of the system or what the system is expected to do. Analysis helps to reveal important information like what environment was needed to develop and test the application, what parameters that needed to be in place for the successful development and what exactly does the client want. Inthis phase of methodology, we reviewed different kind of sources of information which includes journals, books, academic articles and related research work, which helped to identify the current techniques, used for ensuring information confidentiality and gave idea regarding that how verification and validation of QR code can be achieved by means of personal confidential information authentication and authorization. In this phase, we also studied requirement specifications: functional requirements, non-functional requirements, development tools and technologies requirements and system requirements.

3.7.1 Fact Finding Techniques

System analysis starts with data collection. Several appropriate and effective techniques are used to collect data in order for us to define and specify user's requirements, which is also known as requirement determinations. Below are the elaborations of techniques and method being used.

3.7.2 Existing System Review & Literature Review

Existing system review is important to know the features in the current familiar system. Existing system is evaluated and analyzed to know it's strengthen and weaknesses. From the evaluation, good features is captured and implemented in our proposed SQRC system.

Literature review is important to let us know the concepts of how the QR codes can be used securely as to verify (authentication) and validate (authorization) personal confidential information for our proposed SQRC system. The literature review will be done continuouslyin the future in order to get more and more important information to build the effective and efficient system.

3.7.3 Related Research

Books related to QR code and cryptography were read in order to deepen understanding on the field cryptographic algorithm. Data and information gathered from library research is much more reliable and help better understanding of the development of system. Search for the articles which are used in literature review.

3.7.4 Functional Requirements

Functional requirements capture the intended behavior of the system. This behavior may be expressed as services, tasks or function that the system is required to perform. In software engineering, a function also is described as a set of inputs, the behavior and outputs. Functional requirement may be calculations, technical details, data manipulation and processing and other specific functionality that show how the use cases are to be satisfied. Below are the minimum

functional requirements and the descriptions of the modules:

A. Administrator Module

There are administrative functionalities for the administrator. A user with administrator status can manage and operate some important features exclusively. Administrator can have access of the full system up to the ground level.

B. User Registration Module

This module allows users to register his/her account into the system.

C. Login Module

Administrator and user have to login before they can access the functionalities of the system.

D. Forget Password Module

The purpose of forgot password module provides hints for the user to recall back their password.

E. RSA Key Generation Module

This module helps to generate RSA keys, Private Key and Public Key as a pair. Key sizecan be set while key generation. These keys are stored as XML format in the server machine. Public Key is used for encryption and Private Key is used for decryption. This mechanism is applied in QR Code Validation (Authorization) module. On the other hand Private Key is used for encryption in terms of digital signing and Public Key is used for decryption in terms of digital verification of QR Code (Authentication).

F. QR Code Generation Module

With the help of the QR Code Generator, a QR Code can be generated within few minutes in three simple steps. In step one, confidential information are provided and theseare intended to be encrypted in the generated QR Code. In step two, some important parameters: encryption key, error correction level, encoding type, version and block size are provided and optionally color and logo can be selected to provide a unique look. Finally, in third step, after generating the QR Code, it is displayed on the screen and can be downloaded.

G. QR Code Decoding Module

It is intended to upload a QR Code which has already been generated/provided and then, decode operation is performed to get both the encrypted and decrypted confidential information. In QR Code Decoding procedure, it decrypts those QR Code which are encrypted with the RSA Public Key whereas decryption is done with the RSA Private Key.

H. QR Code Verification (Authentication) Module

Aims of this module is to verify a QR Code, which is already provided/embedded on a

document. Verification is done by giving its ID/URL, which is also available with the QR Code in the document, and it is checked that whether the corresponding QR Code is available on the server side for which the ID/URL was given. Other than searching by giving the ID/URL, we also have an option of uploading the QR Code itself to be verified. The mechanism we used is RSA digital signing and verification algorithm.

I. QR Code Validation (Authorization) Module

Purpose of this module is to validate a QR Code, which is already provided/embedded on a document; by scanning the QR Code, we can get the validation result. Other than scanning the QR Code, we also have an option of uploading the QR Code to be validated. The mechanism we used in the validation process is RSA public key encryption algorithm.

J. Contact Us Module

The contact module facilitates the user of the system to view the contact information in order to contact with the system authority and also can submit a message for the concerned people.

3..8. Non-Functional Requirements

Non-functional requirements include constraints and qualities. Qualities are properties or characteristics of the system that its stakeholders care about and hence will affect their degree of satisfaction with the system. Constraints are not subject to negotiation and, unlike qualities, are (theoretically at any rate) off-limits during design trade-offs.

There are few issues needed to be considered when developing system which includes:

A. User Friendly Interface and Human Factors

The design of user interface should be user friendly and easily understandable for end users. The icon applied in the system must be unambiguous and consistent for the system. It is required to show successful message after performing actions such as QR Code generation, verification, and validation to notify user. Similarly, a friendly error message should also be displayed to notify the user in case of failure. Look and feel of an application should be considered to attract the users as they enjoy using attractive applications due to their appealing design.

B. Performance

The system must able to process QR Code generation, decoding, verification and validation reasonably fast to reduce the performance time. The system must provide reliable and accurate information/result for user based on their input. It is important to have ability to recover as fast as possible if the system breaks down.

C. Response Time

The response time should be within a reasonable interval time where all the desirable information should be available to users at any point in time. User should not be kept waiting for a long time for the results.

D. Robustness

System must be able to handle unexpected error and echo back with proper responses. Effective error handling and error message will be displayed if any unexpected error occurs

E. System Modification

The system must be modifiable in the future to a more advance versions. Some extra function can be built into the system in the future.

F Security

The system is able to perform authentication to verify user's identity using the username and password during the login session. This is to prevent the disclosure information to unauthenticated user. System administrator has full control over the options available in the system.

G Reliability

The system should be reliable and shall not cause unnecessary downtime. The application system, software and hardware shall be reliable and shall not cause unnecessary and unplanned downtime of the overall environment.

Table 1

COMPARATIVE STUDY

Literature Reference no.	Year of Publication	Title	Classification Approach	Performance
1	2013	An Encryption Method for QR Code Image Based	International Journal of Security and Its Applications	The system obtains an accuracy of 85%
2	2017	QR Code Watermarking Algorithm Based on DWT and Counterlet Transform for Authentication	DWT	The approach achieved 60% accuracy.
3	2017	Image Steganography and Data hiding in QR Code.	Cryptography Method is used.	The accuracy obtained by the system on the QR code is 88.6%,
4	2018	QR Code Based Image Steganography	Steganography algorithm	The approach achieved 90.88% of accuracy.
5	2018	Fake and Real Massaging at the Same Time with QRCode in Web Services for Different Users	Security and Communication Network	The accuracy obtained by system is 85%,
6	2019	Region Identification and Decoding Of Security Markers Using Image Processing Tools	QR Code is used	The accuracy of QR code is 98 and 92.5 percent, respectively.
7	2020	QR steganography A Threat to New Generation Electronic Voting Systems	Image Encryption and Decryption	The system obtains an accuracy of 85%.

4 CHALLENGES

4.1 Security Awareness Challenges

Determined that there are significant differences in how Internet users perceive privacy challenges and security vulnerabilities. Their findings alongside with the differences in consumer acceptance of QR codes amongst different nationalities suggest that people have different concerns regarding security vulnerabilities when interacting with QR codes. A detailed understanding of the intercultural differences would significantly contribute to the scientific community in order to enhance awareness raising tools and support the adoption of successful security enhancements worldwide.

4.2 QR Code Requirements:

In this section, we identify security requirements to secure the QR coding scheme. We consider coding scheme improvements as invariant to the QR code reader application.

4.3 Visual QR Codes:

In case of an attack scenario (as described in Section 3) visual QR codes significantly support the user in detecting modified or replaced QR codes in urban spaces. The more complex the theme, the harder it becomes for an attacker to modify QR codes in an unobtrusive way. To make it more expensive for an attacker to replace the original QR code (e.g. in billboard advertising), we suggest to investigate the impact of complex color schemes embedded into the color scheme of the whole advertisement on the user's ability to detect malicious modifications.

4.5 Digital Signatures:

In other domains, digital signatures have proven to be an effective means to improve security as shown in [17]. Therefore, we recommend placing emphasis on the integration of digital signatures in the QR code standardization to verify the originator of the code and to thereby check if the QR code has been modified. A digital signature significantly complicates QR code based attacks as the attacker needs to modify the checksum and the verification process accordingly. However, the increased amount of data to encode reduces the area to encode actual data. Furthermore, QR code readers have to be adapted 8 in a way to verify the digital signatures and to indicate whether the verification was successful, similar to SSL. We suggest developing the integration of digital signatures in order to propose a specification update.

4.6 Service Layer Requirements:

The challenges highlighted in this section place emphasis on securing the QR code reader application and are intend to harden secure QR codes. The overall purpose of service layer improvements is to enrich the security features embedded in the QR codes themselves and to determine whether the user's decision is necessary to obviate a malicious code.

4.7 Masking:

The distribution of black and white modules in a specification-compliant QR code follows a specific pattern. This pattern is determined by the mask that is used to specify whether or not to change the color of the considered module. Due to its robustness provided by the error- correcting Reed-Solomon codes, a certain degree of corrupt pixels does not have a negative impact on decoding the QR code. The higher the deviation from an even distribution of black and white modules is, the higher the probability that the QR code is modified. A detailed analysis on the trade-off between error rate and security would be beneficial in order to use masking aspects to secure reader software.

4.8 Malicious URL Detection:

In general, there are different approaches to successfully distinguish potentially malicious URLs from benign ones. However, shortened URLs can be used by an attacker to obfuscate malicious URLs

4.9 Content Preprocessing: In case of shortened URLs or redirects, simply displaying the encoded content does not provide enough information for the user to determine whether the encoded content is malicious is the need for usable content preprocessing tools.

4 IMPLEMENTATION

5.1 QR code generator

This system component allows the admin to enter details of personal confidential information to generate the QR code for that specific entry of confidential information. This QR codeholds a unique number to be identified as if it refers only that specific entry of confidential 50 information of a particular person. To generate a QR code admin must enter security key as per encryption requirement along with the some necessary constraints like error correction level, encoding type, version and block size. Besides, admin can optionally select color and logo for the sake of look and feel of a QR code. Finally, after generated, a QR code is stored into the database/files and can also be downloaded and printed, if required.

5.2 QR Code Download

After generation of a QR code it can be downloaded with any of the following formats: JPG, 51 PNG, GIF or BMP

5.3 QR Code Decoder

For web view and mobile responsive view respectively, allows users to decode a QR code which was printed on a personal confidential legal document . The QR code decoder providesuploading option through which the QR code is uploaded after taking a snapshot of it from thedocument and then, upon decoding operation begins, the decoder analyses the QR code that was uploaded and hence displaying the information as encoded (encrypted information) and decoded (plain text information).

5.4 QR Code Verification

for web view and mobile responsive view respectively, allows users to verify a QR code which was printed on a personal confidential legal document. The QR code verifier takes the QR code ID or URL as input which is used to query the database. The QR code verifier also provides the QR code uploading option through which the QR code is uploaded after taking the image of it and then, the verifier analyses the QR code that was uploaded and hence gives the result about

whether it is verified or not; if verified, it displays the information which was intended to be shared with confidentiality. There are essentially three options for verifying a QR code: QR code ID(a unique ID which is entered to verify a QR code. If the QR code with the given ID is found then it is said to be that the QR code labeled with the ID is verified), QRcode URL(a unique URL address which is entered to verify a QR code. If the QR code with the given URL address is found then it is said to be that the QR code labeled with the URL is verified), and QR code Image(a unique QR image which is uploaded to be verified itself. Ifthe QR code image is found to be matched with the existing one then it is said to be that the QR code image is verified).

5.5 QR Code Validation

The interface, for web view and mobile responsive view respectively, allows users to scan a QR code which was printed on a personal confidential legal document. In QR code validation scheme, the QR Code scanner uses the webcam and 54 analyses the QR code that was pointedto the webcam and hence, gives the result about whether it is validated or not; if validated, it displays the information which was intended to be authorized. The QR code Validation also provides QR code uploading option through which the QR Code is uploaded after taking the image of it and then, the Validation analyses the QR code that was uploaded and hence gives the result about whether it is validated or not; if validated, it displays the information which was intended to be authorized

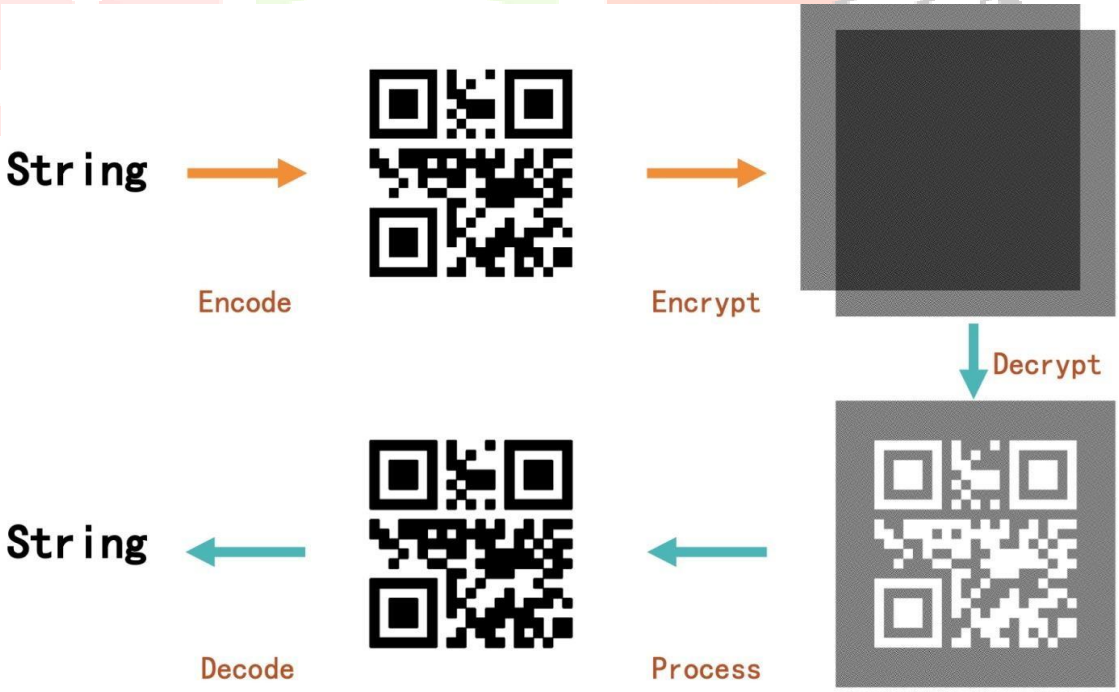


Fig .3.1 QR code encryption and decryption.

5 TOOLS AND TECHNIQUE

6.1 Web Technologies

A quick and simple overview about some of the basic web technologies which are used in our project are described as below.

6.1.1 HTML/HTML5 - Hyper Text Markup Language, one of the oldest and widely used web programming language. It's used to create the basic elements of websites using what is called of 'tag'. There are lots of tags in existence which can be useful to display different kind of information. HTML5 is a new version of HTML that extends the amount of tags that exist.

6.1.2 CSS - Cascading Style Sheet, used to customize the websites visual elements like size, font, color, position and so on. It acts as a complement for HTML technology separating the visual aspects from the HTML tags. This is a very powerful tool and there are a lot of different ways that CSS styles can be used to render websites.

6.1.3 JavaScript - This is a client side script programming language that can dynamically usethe HTML data. JavaScript is not related with Java, but can be used with Java web solutions. JavaScript code runs in the browser (client- side). Most interactive elements of websites these days are driven using JavaScript.

6.1.4 jQuery- jQuery is a JavaScript development framework. It essentially allows us to write less JavaScript code to achieve the same level of functionality. It also improves the performance and compatibility of this JavaScript code in older web browsers.

6.2 Python

Visual cryptography implementation of string/QR code encoding/decoding, and image visua cryptography encryption/decryption. All functions can be used individually or as a pipeline. Base on QR code, the project can encrypt/decrypt any string type messages. Also it can use visual cryptography feature solely to encrypt/decrypt images.

7 CONCLUSIONS AND FUTURE SCOPE

7.1 Conclusion

In modern days, the usage of data is increasing and the ways of forging data is increasing as well. Authenticity and validity of data is a very important issue nowadays. This project presents an innovative method to prevent such forgery of data like personal confidential information and ensures the authenticity and validity of the confidential information. Information,especially confidential information. It replaces sensitive information on paper documents with QR Codes and let only the registered user decode it with our system. In our solution, there are three types

of decoding procedure naming QR Code Decoder, QR Code Verification and QR Code Validation. The SQRC system can be applied to a range of real- world applications that involve sensitive information. Throughout the project development work, we focused on QR Code generation part, QR Code decoding part, QR Code verificationpart, QR Code validation part and also RSA Key generation part, learnt about different attributes of 2D codes, especially QR Code and also learnt about cryptography, especially asymmetric cryptography like RSA public key cryptography and RSA digital signature. Then,we performed testing the system following the possible test cases and got the expected results as these were required by the proposed system. By using the web application, secure encrypted QR Code can be generated and then, this QR code can be decoded by means of confidential information verification.

7.2 Future Work

The limitations of the proposed solution have indicated the following areas as recommendations for future work:

1. Our proposed system is fairly targeted to the web based solution even though it has mobile view responsiveness. So, in future, this system can be developed as a mobile based application to meet the expectation of the mobile community and current technology trends.

2. In the future we try to implement the for single QR CODE it can uses the multiple ways:

When QR CODE read the machine can read the human face then it confirm the person face from the database and automatically detected money from their account.

ANNEXURE I:

Contribution of Each Student Kishor kumar, Dharavath Raj Kumar and Vipin Rathore we all three were involved in report writing paper. We divided research papers from various conferences and journals among three of us, and after discussion, we chose 25 papers that suited our issue. Vipin Rathor collected the different types of datasets from college or other sources. Kishor Kumar and Dharavath Raj Kumar work on the module of feature extraction and Vipin Rathore work on the Neural Network classification technique. Kishor kumar, Dharavath Raj Kumar, Vipin Rathore, we all three authors studied and implemented the Cryptography.

References

[1] Dey, S., Nath, A., Agarwal, S., "Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System" , International Conference on Communication Systems and Network Technologies, DOI 10.1109/CSNT.2013.112, 2013.

[2] Shetty, M., "Hiding of Confidential Data and its Retrieval using Advanced Algorithms and QR Authentication system", IOSR Journal of Electrical an Electronics Engineering (IOSR-JEEE) e-ISSN: 2278-1676, p-ISSN: 2320-3331, Volume 9, Issue 6 Ver. II, PP 01-05 www.iosrjournals.org, Nov – Dec. 2014.

[3] Gupta, N., Mokashe, N., Parihar, M., "QR code: A safe and secure method of authenticating legal documents", International Journal of Engineering Research and General Science Volume 3, Issue 1, ISSN 2091-2730, January-February, 2015.

[4] Bhavar, S., Jadhav, J., Kulkarni, N., Patil, K., "Authenticate Message Hiding in QR Code Using AES Algorithm", International Engineering Research Journal (IERJ) Volume 2 Issue 1 Page 367-369, ISSN 2395-1621, 2016.

[5] Satyanarayana1, T. Assoc. Professor, Swathi2, G., "Secure QR Code for Anti- Phishing System Using Mobile", International Refereed Journal of Engineering and Science (IRJES) ISSN (Online) 2319-183X, (Print) 2319-1821 Volume 2, Issue 12, PP.78-81, December 2013.

[6] "QR Code Tutorial", http://www.thonky.com/qr-code-tutorial/[last accessed on2021].

[7] "SQRC (Secret-function-equipped QR Code)".

https://www.denswave.com/en/adcd/product/software/sqrc/sqrc.html [last accessed on 2021].

[8] "Encrypted QR Codes and Parts of a QR Code", http://www.qrcodestickers.org/qrcode-articles/encrypted-qr-codes.html [last accessed on 2021].

[9]"Reed SolomonCodes

"https://www.cs.cmu.edu/~guyb/realworld/reedsolomon/reed_solomon_codes.html[last accessed on 2021].

[10] "ZXING- QR Code Library", http://code.google.com/p/zxing/ [Online] [Retrieved 2021].

[11] "Encrypted QR Codes: Share secret messages", secret-messages/ [last accessed on 2021].

[12] Stallings, W., "Cryptography and Network Security: Principles and Practice", 5th Edition, Published by Pearson Education, Inc., publishing as Prentice Hall.

[13] Kak, A., "Public-Key Cryptography and the RSA Algorithm", [Online], Available: https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture12.pdf [last accessed on2021].

[14] http://www.qrcodeshowto.com/what-is-a-qr-code/qr-code-specifications-with-pictures/ [last accessed 2021].

[15] https://blog.qrstuff.com/2011/12/14/qr-code-error-correction [last accessed on 2021].

[16] https://conormclaughlin04.wordpress.com/security/ [last accessed on 2021].

[17] https://digitalsignaturescertificates.wordpress.com/2021/steps-involved-in-obtaining-digital-signature-certificates/ [last accessed on 2021].

[18] https://blog.mailfence.com/how-do-digital-signatures-work/ [last accessed on 23-04-2021]

[19] https://www.tutorialspoint.com/cryptography/cryptography_digital_signatures.htm.