International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 05 | May - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Secure Messaging Using Cryptography, Steganography and QR Code

Adinath Sangale[1], Ajinkya Taru[2], Raksha Gupta[3], Vrushali Gandhas[4], Prof. Ratan Deokar[5]

Department of Information Technology,
MET Institute of Engineering Nashik-422203.

Abstract: **Various cryptographic strategies are available for serving the reason of information security over the web, servers and neighborhood systems. In any case, there's persistently ask of more security which may not be meet by such cryptographic calculations alone since of known security assaults and numerical complexity. In this way visualizing the key combination of cryptography and steganography strategies can give the another level of security. Quick Response (QR) codes are utilized broadly due to their advantageous characteristics. It consolidates vigor, significance, botch change capability, colossal information capacity than routine barcodes etc. Hence, in this work, we propose a 3-layered engineering for securing message sharing instrument by utilizing QR code picture in one layer. This designing utilizes the exploratory and key utilize of cryptography and steganography methods. The proposed framework gives the higher level of security on the premise of quantitative and subjective comes about.**

Keywords: **QR code, Steganography, Cryptography, Encryption, Decryption, Cipher text, Private key, Public key, RSA.**

INTRODUCTION:

In this innovative period, advanced communication is considered as helpful way to share data. Cryptography and steganography both work as two lines of defense to guarantee profitable information against adversary.

Cryptography is the craftsmanship of securing information in the midst of transmission. In image steganography, private computerized data is secured up behind progressed picture utilizing specific calculations. QR-code tag is considered as best case of image steganography.

In this paper, three level security approach is displayed, where each level improves the security of the data. In to start with layer, the RSA strategy is utilized to scramble the private message. In moment layer, scrambled advanced message is inserted into the QR barcode and at long last within the final layer, QR barcode image is encoded behind veil picture with the assistance of proposed picture encoding calculation.

This work characterizes the key combination of cryptography and steganography to overhaul the security to progressed information.

OBJECTIVES:

1. To secure beneficial information that are transmitted on the net all the time.

2. To dodge this data from falling into wrong hands.

3. To safely share individual private data and beneficiary ought to be able to confirm the data by checking its realness.

4. To require the all the points of interest of cryptographic calculations image steganography to attain highest level security.

LITERATURE REVIEW:

As we said the supremacy of organize security is extended day by day as the access of data being exchanged over the Internet. This issue pushes the analysts to do various considers to extend the capacity to clarify security issues.

An course of action for this issue is utilizing the advantage of cryptography and steganography combined in one system. Various considers propose methodologies to combine cryptography with steganography frameworks in one system. This Wander has been actualized on the preface of the prerequisites of security i.e. confirmation, privacy, and vigor.

Fatma Mallouli displayed the distinction between RSA and ECC algorithms. He appeared how the cryptographic algorithms works. He separate the algorithms by considering key length, security assault, speed, adaptability, etc. parameters. In this way we centered our work on this and recorded a few work in this segment. [1].

Xin Zhou displayed the RSA cryptosism and public and private key cryptography. Within the proposed framework, they done encryption, unscrambling arrangements that can guarantee security of data and to avoid data from altering. In this way, a comparative kind of approach we proposed where we utilizing hilter kilter cryptography to scramble data and for more security we covering up that scrambled data QR code and scrambling QR code by utilizing picture veiling in steganography. [2].

Sahu and Young man conferred a steganographic system supported component worth differencing (PVD) and LSB. It's focused on on the mistake piece drawback (EBP) and FOBP. The picture is partitioned into pieces with two adjoining pixels. The pieces are part into 3 levels subject to the refinement of component values. The square level and thus the component refinement confirm the implanting capability of the square. Their framework makes strides PSNR and implanting capability. Furthermore, the framework is safe to component qualification bar chart (PDH) examination. [3].

Barrera et.al. upheld a framework that employments QR codes in optical coding as holders. They select QR codes as holders in their framework much obliged to their resistance to squander matter dot commotion. Also, QR codes are clear to check abuse cell phones‟ cameras. At that point comes approximately show up that their system is additional defenseless to commotion compared to ordinary optical encryption. [4].

PROBLEM STATEMENT:

To ensure important data there are different cryptographic and steganographic procedures available to ensure information. Making utilize of QR codes and both cryptographic and steganographic techniques at the same time can make data more secure. Since we have to make use of this techniques and algorithms to develop a most secure message sharing web application.

MOTIVATION:

Data sharing and information security has its claim significance since of expanding assault hones presently days. We are utilizing QR code to secure data since it has various benefits utilizing the combination of cryptography and steganography for overhauled security.

The inspiration behind our work is taking benefits of QR codes as holders to cover up the payload:

A QR code can be displayed as a coded message as well as image.

Usually, the payload degrades the container. But thankfully, the QR code can be up to 50 percent damaged without affecting the message.

A QR code is displayed as a binary picture, which makes it more size-efficient compared to other containers such as colored images.

SYSTEM ARCHITECTURE:

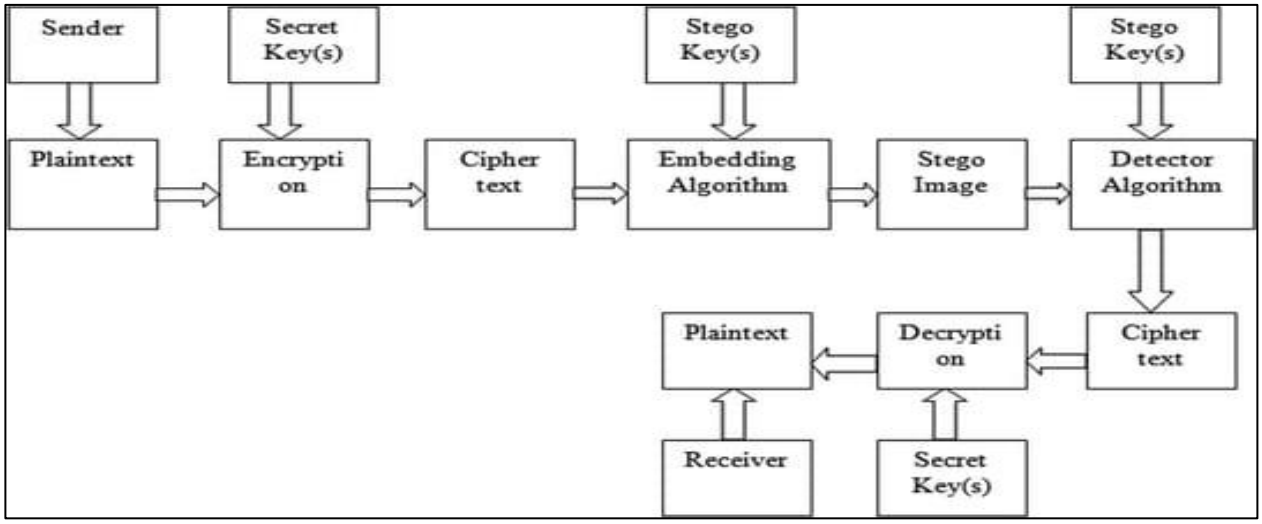


Fig. System Architecture.

Firstly Sender enter message implies that was the plaintext. At that point that content will be scrambled utilizing key so it'll make a cipher text. And after that framework will produce a QR code of that cipher content. At that point picture implanting calculation will apply on that QR to scramble that QR code picture. That will be the stego picture. At the recipients conclusion, get transfer that QR code to framework and framework will do invert operation to disentangle the content message. Firstly cipher content from QR will create and after that unscrambling of that cipher content utilizing open key will be done. And the recipient can get plain content.

I. CRYPTOGRAPHY:

Cryptography is the methodology of secure transmission of data by changing over the substance into many nauseated outline so that because it were the arranging client can oust that disgust and can ponder the beginning mystery message. Cryptography has taken after man through various stages of progression. Julius Caesar in his period utilized normal letter set substitution technique for government communication. Nowadays cryptography has come to an unused level and by and by we too have quantum cryptography. Quantum cryptography combines cryptography and fabric science to make an unused cryptosystem that cannot be pulverized without the sender and beneficiary.

Some terminologies used in Cryptography are:-

Plaintext: - It is the original text message.

Encryption: - It is the process of encoding the contents of original message so that attacker or any outsider does not understand the real message.

Decryption: - The process of retrieving backs the original message.
Hash Functions: - They generate the digest of the message.

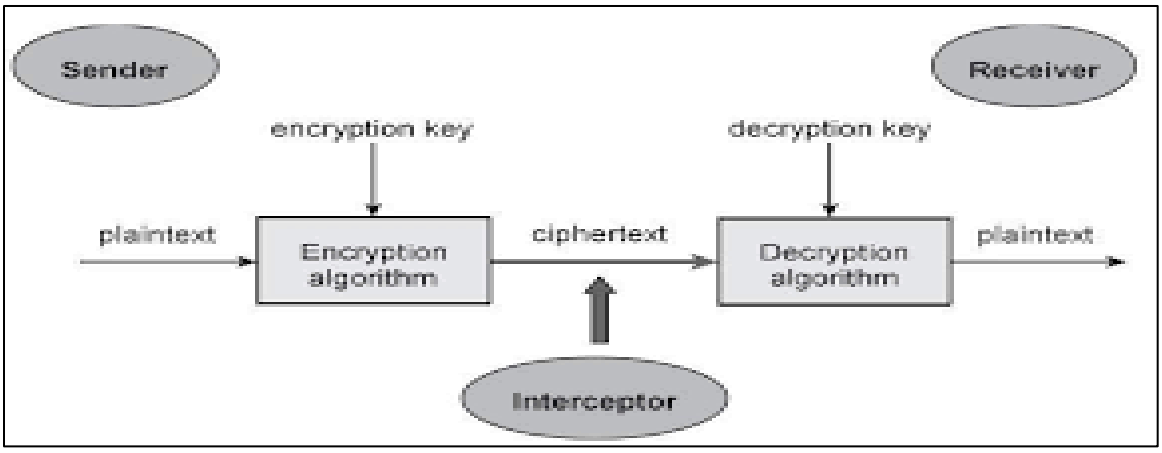


Fig. Basic Encryption and Decryption Process of Cryptography.

Cipher Text: - The encoded text is called the cipher-text.

In Cryptography there are three distinct mechanisms: -

Symmetric key encryption (as well called as riddle key cryptography) in this same key is utilized both for encryption and unscrambling.

Asymmetric key encryption (as well called as open key cryptography) in this there are two diverse keys on is utilized for encryption and other is utilized for unscrambling.

Hash capacities are much utilized for computerized signature .For message affirmation in various applications hash work has gotten to be the standard approach. The result of hash work is hash code.

II. STEGANOGRAPHY:

The word steganography comes from the Greek which pitiless secured or riddle and graphy implies composing or drawing. In this way, steganography may be a “covered writing”. The foremost objective of steganography is for secure communication and the information secured up got to be subtle. The media that's utilized for covering can be computerized pictures, sound, recordings, substance records, and other computer records .These mediums are called Carrier Objects or Cover Objects. After embeddings a secret message into the cover-image, a so called stegano picture is gotten. The essential show of Steganography for implanting and extraction comprises of Carrier Question, Mystery Message, Implanting calculation, Extraction calculation and Stego key.

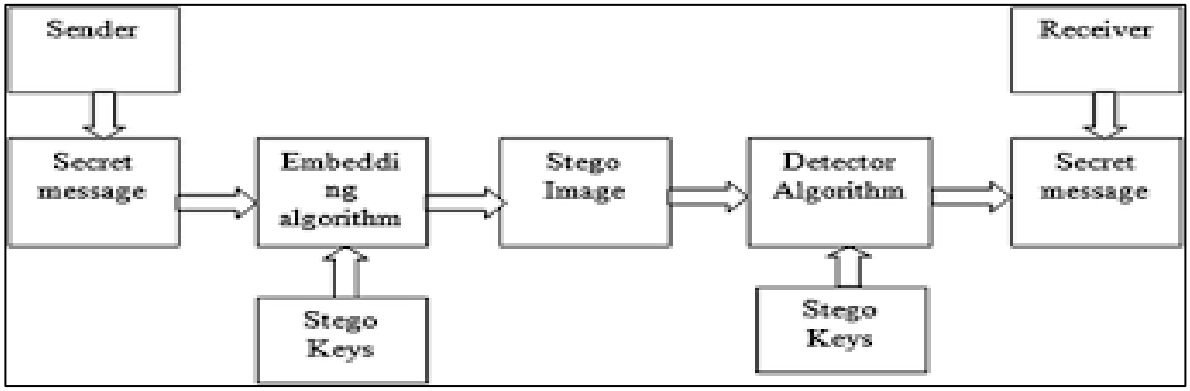


Fig. Basic Steganography Model.

III. COMPARISON OF STEGANOGRAPHY & CRYPTOGRAPHY:

Steganography	**Cryptography**
In this unknown message is passed.	In this known message is passed.
It does not alter the structure of the message.	It alter the structure of the message.
Key is optional.	Key is necessary.
Use to hide message.	Use to encode message.
Output are stego file.	Output are Cipher text.

IV. QR CODE:

Fig. Normal QR code

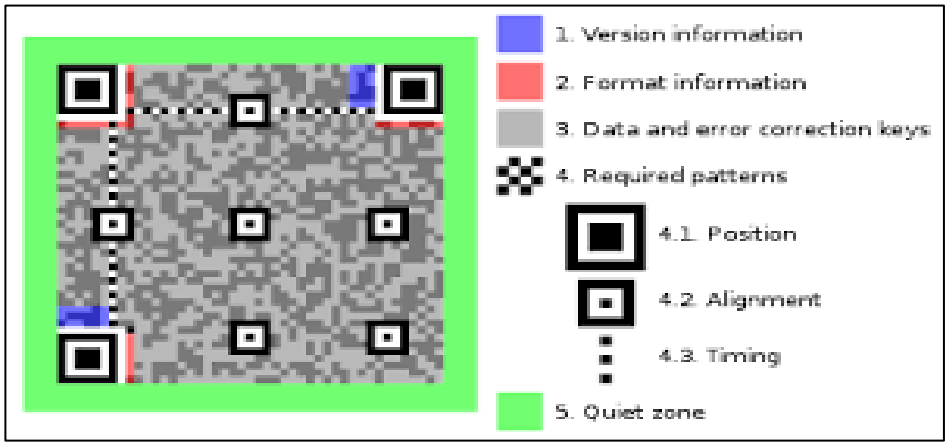


Fig. QR code structure.

A stopped zone that will be a border of cleanse house required for examining the QR code. The very zone is utilized to ease the picture disclosure. Data that chooses the cover designs and so the blunder amendment level utilized inside the QR code. A common course of activity plan that recognizes the central coordination of each cell with substituting dim and white designs. It rectifies the central coordination of the cell once it's misshaped or once there's error inside the cell space.

V. RSA ALGORITHM:

In this proposed method we are using RSA cryptographic algorithm.

The RSA calculation is a deviated cryptography algorithm; this suggests that it livelihoods of public key and private key.

As the names propose, public key is shared publically, though a private key is puzzle and must not be shared with anyone.

The RSA calculation is named after those who planned it in 1978: Ron Rivest, Adi Shamir, and Leonard Adleman.

The Sender Scrambles the data (message) with the receiver's open key at that point cipher substance is produced. After beneficiary got the message/data they interpret it with their have private key.

The RSA calculation ensures that the keys, inside the over traces, are as secure as conceivable.

VI. COMBINING BOTH CRYPTOGRAPHY & STEGANOGRAPHY ON QR IMAGE:

Cryptography scrambles the message which makes a distinction in covering up the substance of the message. So, after encryption the substance of the message are not unmistakable. This gives the security but aggressor can split the code and translated the message. So, to incorporate a present day layer of security cryptography at the side steganography may be a best elective. In case an assailant found that stego picture incorporates a message at that point also he will get an scrambled message not the initial one. The combination of both makes the communication more secure and solid.

Algorithm of the combination techniques:

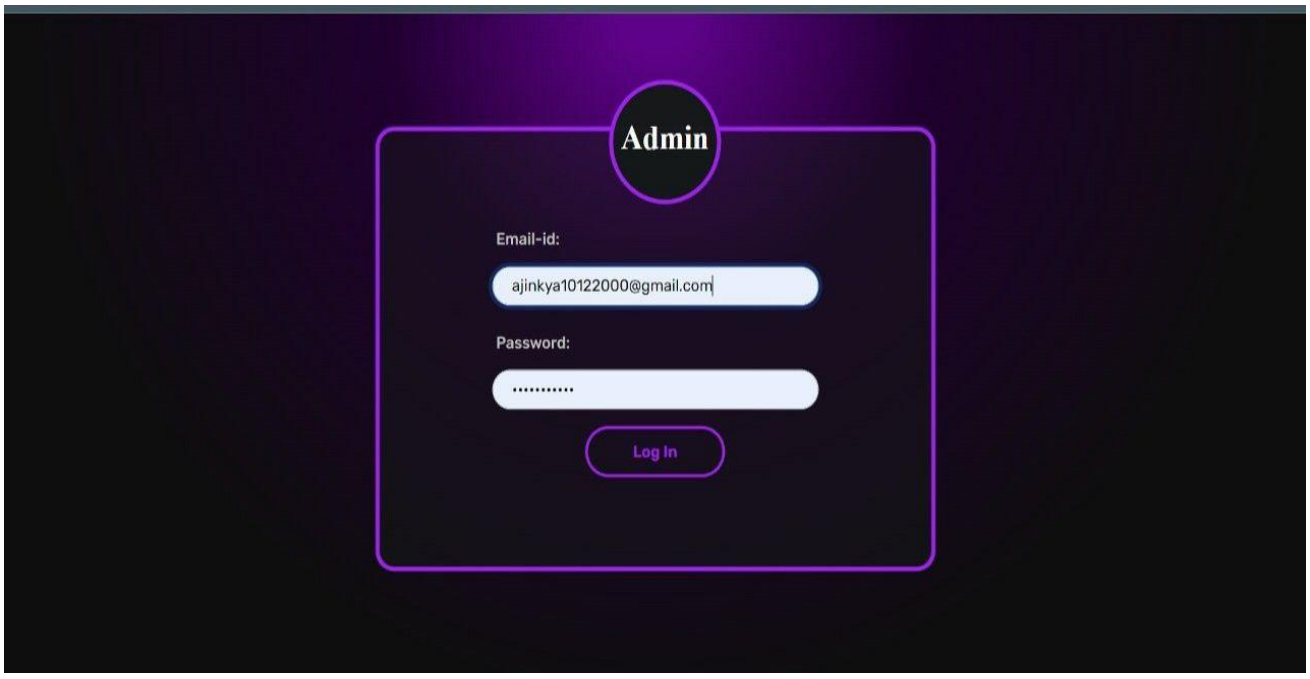
Sender will provide the plain text and a key.
Then an RSA algorithm is used for encryption of the message.
Then this encrypted message or cipher text is embedded in QR image with the help of some algorithm to produce a stego QR image and key is option in this process.
Then the stego QR image is transmitted for communication.
Then the receiver will perform the reverse processes.
Receiver will first extract the cipher message form QR code image using extraction algorithm.
Then receiver will apply decryption algorithm and will provide key to decrypt the cipher text.
The output will be the original plain text message.

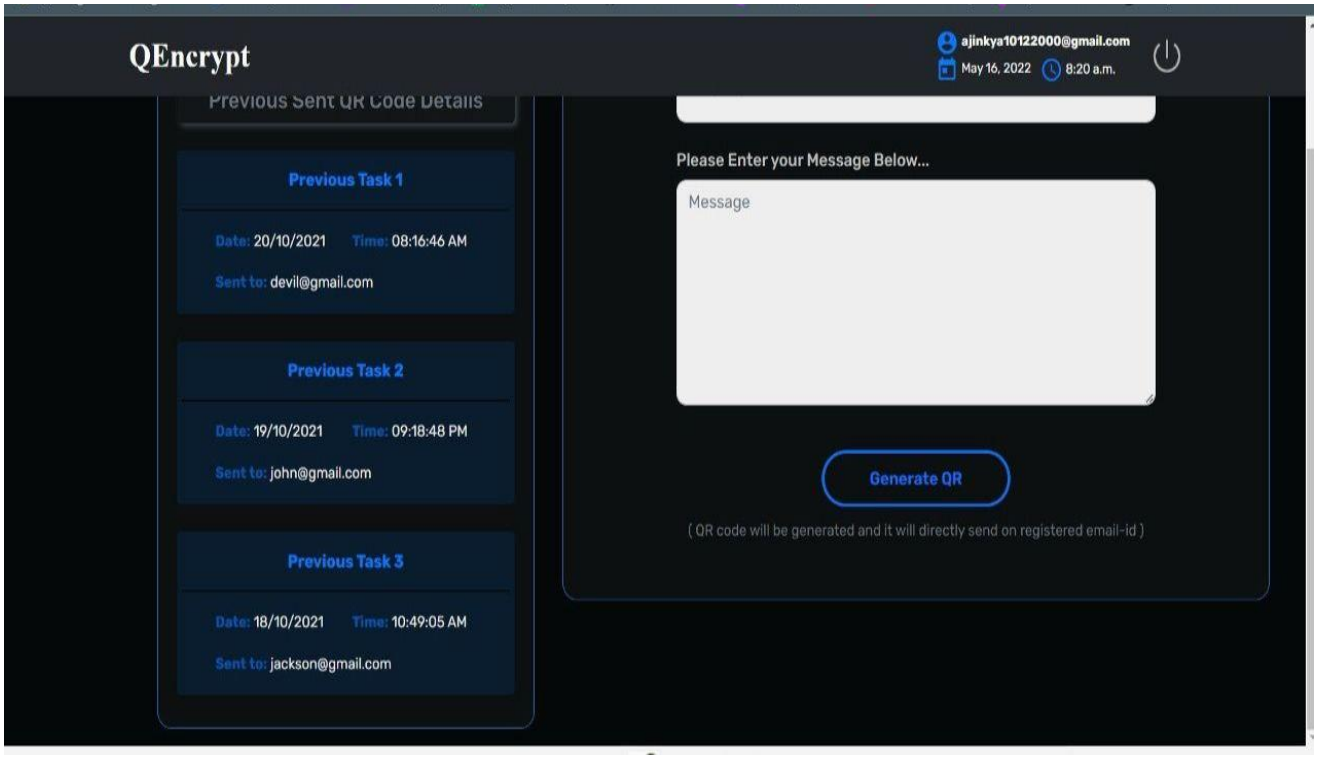
RESULTS:

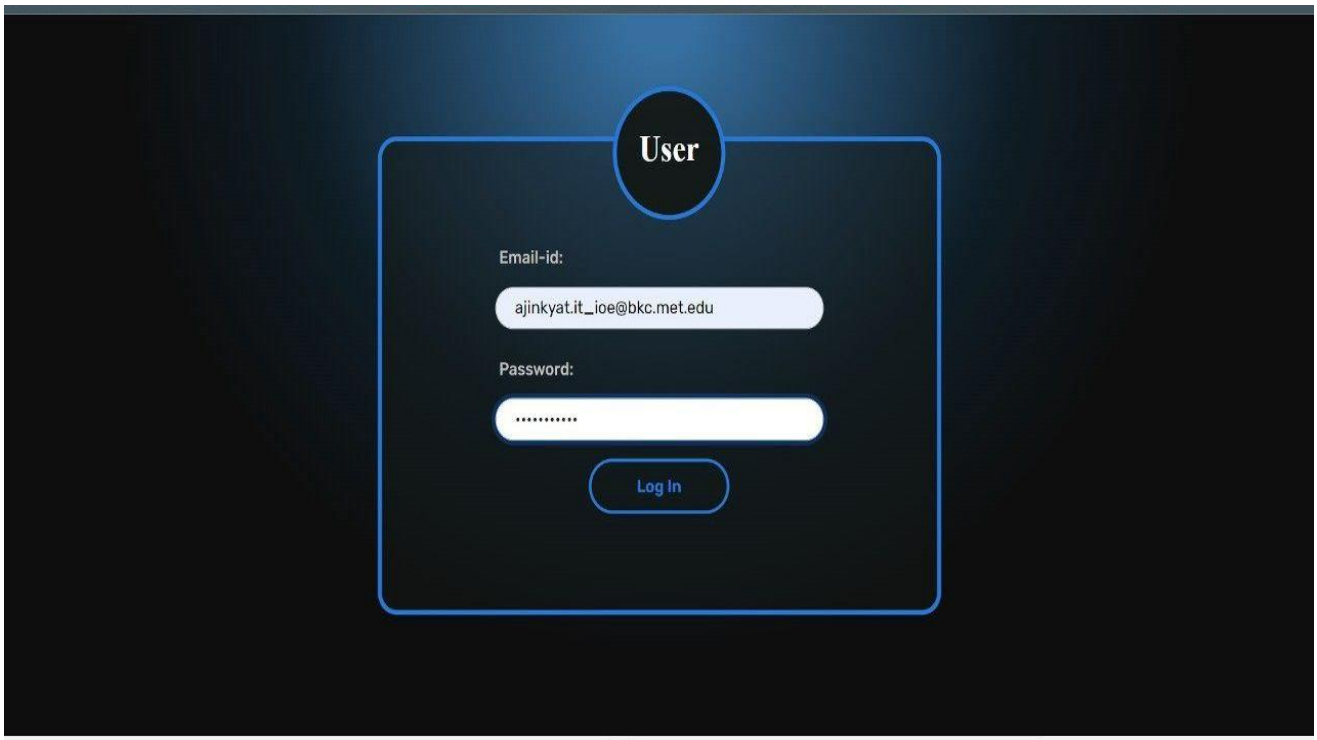
Main agenda of proposed system is secure messaging.

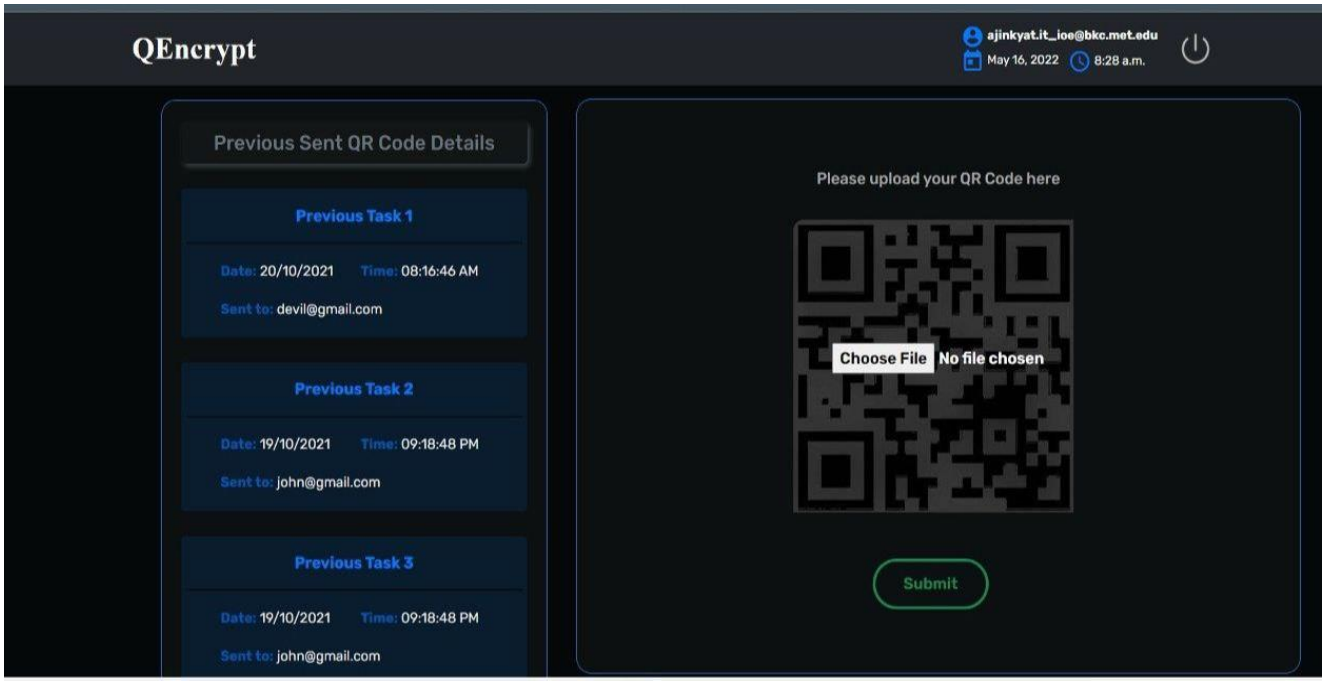
In the application there are two different entites that can simply qadmin and quser. By the qadmin user can be created to share encrypted message in the formate of qr code for secure messaging. Qadmin have option to assign the qr image to receiver. At the time of sharing message, message get encrypted by rsa algorithm and for that encrypted message system generates the qr code for assigned user only. Then quser comes in picture, quser can decrypt original message by portal for their assigned qr code only. No one can decrypt original message without permission. From creating encrypted mesaage to qr and decrypt the qr into original text needs Qencrypt portals only. Without portal message get extracted from qr but it will be in encrypted format. So the system provides the feature for securing the message-converting to QR. At high level the encryption can happen by RSA, at the time of securing message, RSA gives the public and private key. Without public and private key encryption and decryption not possible, No one can access or get your original message even after extracting the text from qr image.

The whole system is to provide seamless and secure message, That can be used in government agencies, embassies, military etc




QEncrypt
ajinkya10122000@gmail.com
May 16, 2022
8:20 a.m.
Previous Sent QR Code Details
Previous Task 1
Date: 20/10/2021 Time: 08:16:46 AM
Sent to: devil@gmail.com
Previous Task 2
Date: 19/10/2021 Time: 09:18:48 PM
Sent to: john@gmail.com
Previous Task 3
Date: 18/10/2021 Time: 10:49:05 AM
Sent to: jackson@gmail.com
Please Enter your Message Below...
Message
Generate QR
(QR code will be generated and it will directly send on registered email-id)


User
Email-id:
ajinkyat.it_ioe@bkc.met.edu
Password:
Log In



CONCLUSION:

A detailed analysis of asymmetric encryption algorithms is presented on the basis of different parameters.

The main objective was to provide security in information sharing by strategically combining two security mechanisms.

This system can be used in the area where security is prime concern.

REFERENCES:

[1] Abhijeet Mendhe; Deepak Kumar Gupta; Krishna Pal Sharma "Secure QR-Code Based Message Sharing System Using Cryptography and Steganography" 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC).
[2] K.S.Seethalakshmi,"Use of Visual Cryptography and Neural Net-works to Enhance Security in Image Steganography", IOSR Journal of Computer Engineering (IOSR-JCE).
[3] Md. Salahuddin Ahamed, Hossen Asiful Mustafa, Ph.D." A Secure QR Code System for Sharing Personal

Confidential Information" IEEE paper 2019.
[4] Xin Zhou "Research and Implementation of RSA algorithm for Encryption and Decryption" 2011 6th International Forum on Strategic Technology.
[5] Fatma Mallouli, Aya Hellal, Nahla Sharief Saeed, Fatimah Abdulraheem Alzahrani "A Survey on Cryptography: comparative study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms" 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom).