iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.50203

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

Secure QR-Code Based Message Sharing System Using Cryptography and Steganography

Prof. Chorade Priti[1], Baravkar Vaishnavi[2], Mhaske Trupti[3], Wankhede Deepak[4], Bhapkar Rohit[5]
Vidya Prasarni Sabha's College of Engineering and Technology, Lonavala, Savitribai Phule Pune University, Pune, Maharashtra, India

Abstract: ***Numerous cryptographic methods are accessible for filling the need of data security over the web, servers, and neighbourhood frameworks.***
Be that as it may, there is consistently request of greater security which may not be meet by such cryptographic calculations alone due to realized security assaults and numerical intricacy. Consequently, envisioning the essential mix of cryptography and steganography strategies can give a more significant level of safety. Speedy Reaction (QR) codes are utilized broadly because of their advantageous attributes.
It incorporates strength, intelligibility, mistake amendment ability, huge information limit than customary standardized tags and so forth. Consequently, in this work, we propose a 3-layered engineering for getting message sharing system by utilizing QR code picture in one layer.
This engineering uses the exact and vital utilization of cryptography and steganography procedures. The proposed framework gives the more significant level of safety based on quantitative and subjective outcomes. Additionally, we consider our framework in contrast to the presentation assessment standards examined in the paper.
Keywords: Cryptography, Image Steganography, 3DES, RSA, AES, QR Codes.

I. INTRODUCTION

In this mechanical time, advanced correspondence is considered as helpful method for sharing data. Data sharing has turned into the foundation of our day to day action. It tends to be in various modes like dividing of data among two unique organizations, divisions inside an association or among a gathering of people. Data sharing and information security has its own significance on account of expanding assaults rehearses now days.

To give a satisfactory security, numerous calculations have been proposed by the time. Many cryptographic algorithms always ensure the integrity and security while sharing information. There is always a trade-off between the computational complexity and strength of these algorithm.

In the advent of electronic age, computational power of machines has increased considerably and thus now computational complexity may be tolerated to some extent.

However, incremented computational power enhances the power of attackers on the cryptographic algorithms and thus, there is a need to improve security strength of the information. Thus in order to enhance security, may researchers are thinking appropriate solution to combine cryptographic and steganographic techniques.

The QR codes are additionally widely utilized in data sharing. These was created by the Japanese Denso-Wave organization in 1994. These codes' principles gives 40 QR variants (1-40) to convey different information payloads. The capacity limit is relies on the variant level. Higher the form, bigger the information payload. Additionally, this code gives the Reed-Solomon blunder amendment capacity.

In this way, they have another huge property, which is dependability. This property permits the QR code perusers to recuperate the information from code accurately regardless of whether piece of QR code is grimy or harmed.

To accomplish dependability, QR code principles offers four revision levels, i.e., L, M, Q and H for each QR rendition. Table I shows the levels of the QR codes.

Cryptographic calculations may not give the better security alone. In this manner, picturing the essential blend of the cryptography and steganographic strategies can give the more significant level of safety. In picture steganography, to full fill the need of advanced picture, QR-Code picture can be utilized.

©IJRASET: All Rights are Reserved

Table I. Reliability of QR Code [3]

TABLE	RELABILITY OF QR CODE
Error correction Level	Error correlation capability % of code words
L(Low)	7
M(Medium)	15
Q(Quantile)	25
H(high)	30

The rest of the paper is organized as follows. The following section II will contain the relevant work and discussed by comparing the approaches. After that in section III, we presented our proposed scheme. Section IV, is about the results and comparison of the proposed scheme. Here we compare the performance with existing one. And finally in section V we presented the conclusion and future work followed by the reference list.

II. RELATED WORK

As information security and secure data sharing is continuously being viewed as a center region, numerous scientists are working in the field and contributed a ton. Likewise, as security prerequisite are expanding a direct result of expansion in data trade, presently the escalated research is going on connected with the QR code-based data sharing frameworks. Hence, we have zeroed in our work on this and recorded some work in this segment.

Shweta Sharmaeta analyze the attributes of QR code labels and proposed three-layer security framework which utilizes the blend of cryptography and Steganography. The execution of their framework is finished utilizing MATLAB. The examination work of creators and momentum research pattern in data sharing gives motivation to us to move the protected data framework towards the picture steganography and QR standardized identification tag.

Pei-Yu Lin, introduced the qualities of QR standardized identification is used to plan a mysterious QR sharing way to deal with safeguard the confidential QR information with a solid and dependable disseminated framework. In the proposed framework the mystery can be parted and conveyed with QR labels in the dissemination application, and the framework can recover the lossless mystery when approved members collaborate. The trial results are given to reason that, the new methodology is achievable and gives content comprehensibility, con artist perceptibility, and a movable mystery payload of the QR standardized tag. This original work proposed by the creators, gives the plan to oppose the print and output activity of QR code and make our framework more adaptable.

K. S. Seetha Lakshmi et al., introduced the visual cryptography which is a prestigious method to safeguard information which is picture based. Creators proposed a plan to improve the security in picture steganography. To upgrade security system, creators proposed the strategy where visual cryptography and picture steganography are utilized together. Creators uses the brain networks are worried about recognizing the best areas in have picture to implant the restricted information hence further developing the picture quality[9]. Here the creator demonstrates that there is no information misfortune when QR code labels uses and cover it with the other visual illustrations. Subsequently, a comparative sort of approach we proposed where we utilized picture steganography by concealing QR code behind veil picture.

III. PROPOSED SYSTEM

The proposed conspire is an essential blend of cryptographic as well as the steganographic procedures. This work zeroed in on improving the security necessities by utilizing QR-code. A three layer layered design is proposed to achieve the undertaking.

In the main layer, the strength of public key cryptosystem is used, hence RSA encryption calculation is utilized to encode the data. In the subsequent layer, picture steganography methods are used where the scrambled message is concealed in the QR code picture. In the third layer, the QR Code picture is encoded utilizing veil picture to give greater security to the data. Fig.1 shows the flow of the proposed methodology of the message sharing system.

A. List of Symbols

Proposed system comprises the algorithms and are discussed in following sections. Table II shows the symbols used in the proposed algorithms.

B. Algorithms

Proposed system follows complicated process which contains four stages. At each stage in the process, complexity of the proposed system increases in terms of security. Process begins by providing secret message to the system and system will generate the encoded image as output.

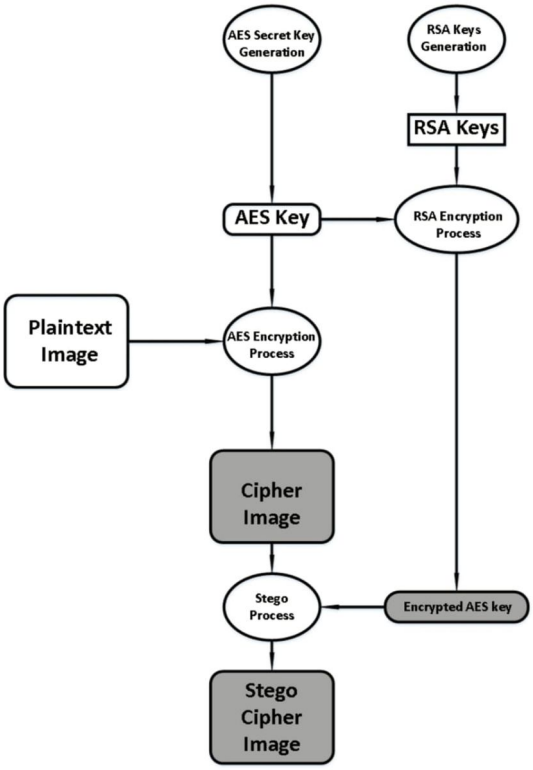


Fig. 1: Proposed Methodology

TABLE II: LIST OF SYMBOLS

M	Message or plain text
CT	Cipher text the outcome of the encryption process which is unreadable text
R	The outcome/results of the system
EQR	Encoded QR code
DQR	Decoded QR Code
RPi	The pixel value of the initialized random image
QPi	The pixel value of QR image

Following algorithm Secure_Message_System_Main() rep-resents the general methodology of proposed work followed by the algorithm description. Fig. 2 shows the data components in the proposed system.

1) Secure_Message_System_Main()

a) Start
b) M Input message from the user
c) CT Call Encryption_RSA(M)
d) QRcode Call_QR_Generator(CT)
e) R Call Image_Encoding(QR code)
f) Show R to user
g) End

- The process starts with providing the plain text (secret message) to the proposed system.
- Next, the RSA encryption technique is applied to encrypt the secret message. This stage will provide the output as cipher text. Here 1024 bit keys is used in RSA encryption technique.
- This unreadable cipher text is then provided to next module, which in turn generate the QR code which represents this cipher text.

QR code image will then be encoded with the help of mask image using proposed image encoding algorithm.
Following algorithm Image_Encoding (QR code) describes the image steganography. This algorithm is proposed to encode the QR code image using mask image, Where the QR image will be encoded into the randomly initialized pixel image.

2) Image_Encoding (QR code)
a) Start
b) Initialize random image with pixel size>=pixel size (QR code)
c) For each pixel of random image RPi:
For each pixel of QR code QPi:
I f QPi is even no:
Do: change RPi to nearest even number
Else if QPi is odd no:
Do: change RPi to nearest odd number
d) return EQR
e) END

- Proposed system initialize the random image having pixel size greater than or equals to the pixel size of QR code image.
- Now, for each pixel value of QR code image, manipulate the pixel value of the random image as per the following rule.
- If the pixel value of QR code image is odd then make the pixel value of random image to nearest odd number.
- If the pixel value of QR code image is even number then make the pixel value of random image to nearest even number.

Following Image Decoding (EQR) algorithm describes the extraction of QR code image at receiver side from encoded image.

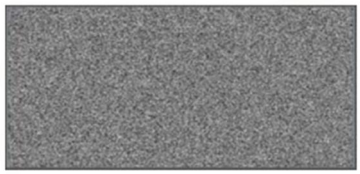
3) Image Decoding (EQR)
a) Start
b) Initialize random image with a pixel size of EQR
c) For each pixel of EQR QPi:
I f QPi is even no:
Do: store 0 in image matrix of EQR
Else if QPi is odd no:
Do: store 1 in image matrix of EQR
d) return DQR
e) END

Fig. (a) shows the original QR code (b) shows the mask image (c) shows the result after applying Image Encoding() algorithm.
- Initialize the random image with pixel size equals the pixel size of encoded QR code image.
- For each pixel value of the encoded QR code image, change the pixel value of the random image to the 0 or 1.
- If the pixel value of encoded QR image is even number then change the pixel value of the random image to the 0 and if the pixel value of encoded QR image is odd number then change the pixel value of the random image to the 1.
- This is how, finally, system will contain the matrix of 0s and 1s. where 0 represents the presence of color (black) and 1 represents the absence of the color (white).
- This matrix constitutes the pixel matrix of an image and this image is our QR code image.

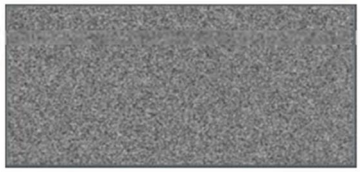
©IJRASET: All Rights are Reserved



(a) Original QR Image



(b) Randomly Initialized Pixel image or Mask Image



(b) Resulted Image

IV. CONCLUSION AND FUTURE WORK

In this proposed work, an itemized examination of lopsided encryption calculations is introduced based on various boundaries. The primary goal was to give security in data sharing by decisively consolidating two security systems for example cryptography and steganography.

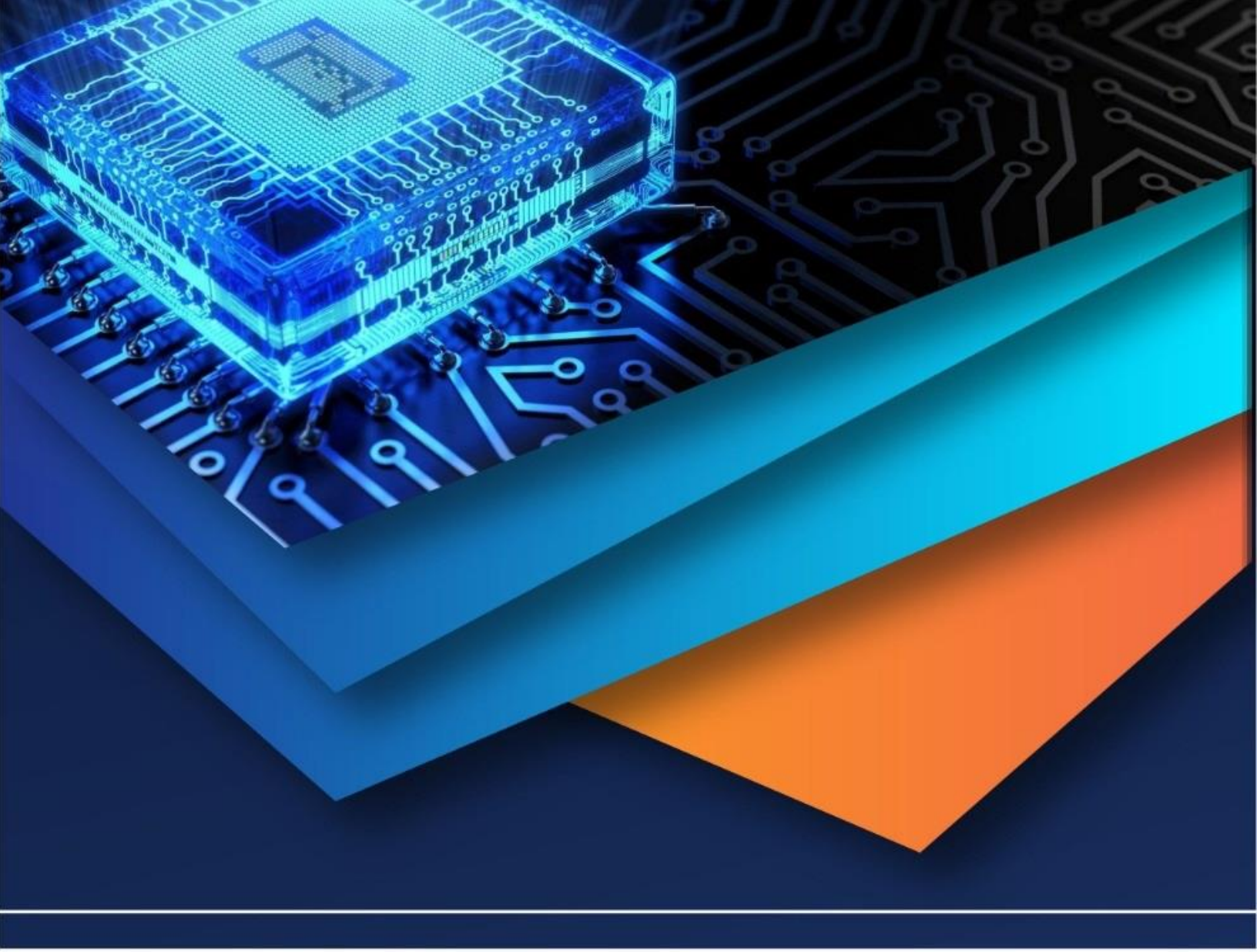
During this examination, it was seen that RSA was awesome among all with regards to Security, Adaptability, and Encryption execution. Albeit the other calculations were likewise skillfull, the greater part of them have a compromise between memory use and encryption execution. Although the proposed methods had already demonstrated a good performance, the following need to be incorporated in future work:

1) Applying different cryptographic asymmetric encryption algorithms to provide more security.
2) Applying different encoding mechanisms to encode QR image for securing data hidden in QR image.
3) Effective use of the 24-bit image in image steganography module to increase security and data storage capacity.

REFERENCES

[1] Information TechnologyAutomatic Identication and Data Capture Techniques Bar Code SymbologyQR Code, ISO/IEC 18004, 2000.
[2] Denso-Wave Inc., QR code standardization, 2003 [Online]. Available: http://www.qrcode.com/en/index.html
[3] Lin, Pei-Yu. "Distributed secret sharing approach with cheater prevention based on QR code." IEEE Transactions on Industrial Informadles 12, no. 1 (2016): 384-392.
[4] Dey, Somdip, Kalyan Mondal, Joyshree Nath, and Asoke Nath. "Advanced steganography algorithm using randomized intermediate QR host embedded with any encrypted secret message: ASA QR algorithm." International Journal of Modern Education and Computer Science 4, no. 6 (2012): 59.
[5] Chung, Chin-Ho, Wen-Yuan Chen, and Ching-Ming Tu. "Image hidden technique using QR-barcode."In Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP'09. Fifth International Conference on, pp. 522-525. IEEE, 2009
[6] Chen, Wen-Yuan, and Jing-Wein Wang. "Nested image steganography scheme using QR-barcode technique."Optical Engineering 48, no. 5 (2009):0570.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)