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

Abhijeet Mendhe
Computer Science and Engineering
Dr. B. R. Ambedkar NIT Jalandhar Punjab
abhijeetmendhe7@gmail.com

Mr. Deepak Kumar Gupta
Computer Science and Engineering
Dr. B. R. Ambedkar NIT Jalandhar Punjab
guptadk@nitj.ac.in

Dr. Krishna Pal Sharma
Computer Science and Engineering
Dr. B. R. Ambedkar NIT Jalandhar Punjab
sharmakp@nitj.ac.in

***Abstract*— Many cryptographic techniques are available for serving the purpose of information security over the web, servers and local systems. However, there is always demand of more security which may not be meet by such cryptographic algorithms alone because of known security attacks and mathematical complexity. Thus visualizing the strategic combination of cryptography and steganography techniques can provide a higher level of security. Quick Response (QR) codes are used extensively due to their beneficial characteristics. It includes robustness, readability, error correction capability, large data capacity than traditional barcodes etc. Thus, in this work, we propose a 3-layered architecture for securing message sharing mechanism by using QR code image in one layer. This architecture utilizes the empirical and strategic use of cryptography and steganography techniques. The proposed system provides the higher level of security on the basis of quantitative and qualitative results. Also, we evaluate our system against the performance evaluation criteria discussed in the paper.**

**Keywords: Cryptography, Image Steganography, 3DES, RSA, AES, QR Codes**

## I. INTRODUCTION

In this technological era, digital communication is considered as convenient way to share information. Information sharing has become the cornerstone of our daily activity. It can be in different modes like sharing of information between two different companies, departments within an organization or among a group of individuals. Information sharing and data security has its own importance because of increasing attacks practices now days. In order to provide an adequate security, many algorithms have been proposed by the time. Many cryptographic algorithms always ensures 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 tolerate 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 [1].

In image steganography, confidential digital data is hidden behind digital image using specific algorithms. QR-code tag is considered as an best example of image steganography. In recent years, QR codes replaces the conventional 1-D barcodes due to their beneficial properties.

The QR codes are also extensively used in information sharing. These was developed by the Japanese Denso-Wave company in 1994 [1]-[3]. These codes' standards [1] provides 40 QR versions (1-40) to carry various data pay-loads. The storage capacity is depends upon the version level. Higher the version, larger the data payload. Also, these code provides the Reed-Solomon error correction capability. Thus, they has another significant property, which is reliability. This property allows the QR code readers to recover the data from code correctly even if portion of QR code is dirty or damaged. To achieve reliability, QR code standards offers four correction levels, i.e., L, M, Q and H for each QR version [3]. Table I shows the levels of the QR codes.

QR barcode uses the steganographic approach to embed the large data within the small QR tags. Cryptographic algorithms may not provide the better security alone. Thus visualizing the strategic combination of the cryptography and steganographic techniques can provide the higher level of security. In image steganography, to satisfy the need of digital image, QR-Code image can be used.

TABLE I. RELIABILITY OF QR CODE [3]

| Error Correction Level | Error Correction Capability, % of code words |
|---|---|
| L (Low) | 7 |
| M (Medium) | 15 |
| Q (Quartile) | 25 |
| H (High) | 30 |

In this paper, a level security approach is presented, where each level enhances the security of the information. In first layer, the RSA technique is used to encrypt the confidential message. In second layer, encrypted digital message is embedded into the QR barcode and finally in the last layer, QR barcode image is encoded behind mask image with the help of proposed image encoding algorithm. In this way approach provide an enhanced procedure to encrypt data. This work defines the strategic combination of cryptography and steganography to enhance the security to digital information.

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 data security and secure information sharing is always being considered an focus area, many researchers are working in the field and contributed a lot. Also, as security requirement are increasing because of increase in information exchange, now the intensive research is going on related to the QR code based information sharing systems. Thus we have focused our work on this and listed some work in this section.

Shweta Sharma et.al., examine the characteristics of QR code tags and proposed three layer security system which uses the combination of cryptography and Steganography. The implementation of their system is done using MATLAB. [8]. The research work of authors and current research trend in information sharing gives inspiration to us to move the secure information system towards the image steganography and QR barcode tag.

Pei-Yu Lin, presented the characteristics of QR bar-code is utilized to design a secret QR sharing approach to protect the private QR data with a secure and reliable distributed system. In the proposed system 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. The experimental results are provided to conclude that, the new approach is feasible and provides content readability, cheater detectability, and an adjustable secret payload of the QR barcode. [3] This novel work proposed by the authors, gives the idea to resist the print and scan operation of QR code and make our system more flexible.

K. S. Seethalakshmi et al., presented the visual cryptography which is a renowned technique to protect data which is image based. Authors proposed a scheme to enhance the security in image steganography. In order to enhance security mechanism, authors proposed the methodology where visual cryptography and image steganography are used together. Authors utilizes the neural networks are concerned with identifying the best locations in host image in order to embed the secret data thus improving the image quality[9]. Here the author proves that there is no data loss when QR code tags uses and mask it with the other visual graphics. Thus, a similar kind of approach we proposed where we used image steganography by hiding QR code behind mask image.

## III. Proposed System

The proposed scheme is a strategic combination of cryptographic as well as the steganographic techniques. This work focused on enhancing the security requirements by using QR-code. A three layer layered architecture is proposed in order to accomplish the task. In the first layer, the strength of public key cryptosystem is utilized, thus RSA encryption algorithm is used to encrypt the information. In the second layer, image steganography techniques are utilized where the encrypted message is hidden in the QR code image. In the third layer, the QR Code image is encoded using mask image to provide more security to the information.

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.

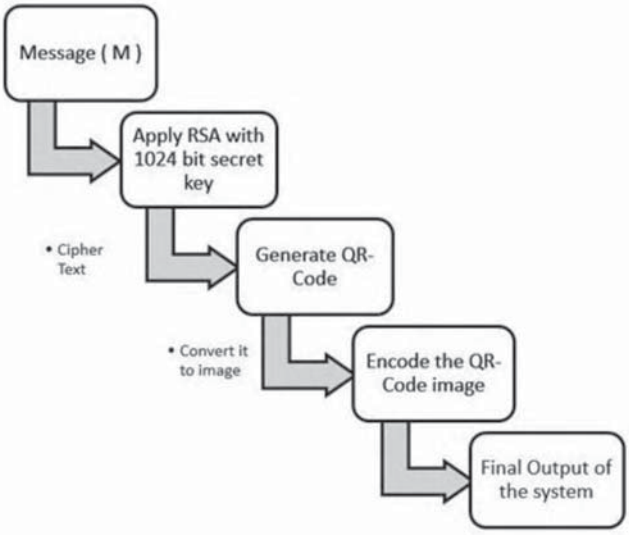



Fig. 1: Proposed Methodology

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 final outcome/result of the system |
| *EQR* | Encoded QR Image |
| *DQR* | Decoded QR Image |
| *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.

**Secure_Message_System_Main():**
*1: Start*
*2: M ← Input message from the user*
*3: CT ← Call Encryption_RSA(M)*
*4: QR_code ← Call QR_Generator(CT)*
*5: R ← Call Image_Encoding(QR code)*
*6: Show R to user*
*7: 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.

**Image_Encoding (QR code):**

*1: Start*
*2: Initialize random image with pixel size>=pixel size (QR code)*
*3: For each pixel of random image RPi:*
*For each pixel of QR code QPi:*
*If QPi is even no:*
*Do: change RPi to nearest even number*
*Else if QPi is odd no:*
*Do: change RPi to nearest odd number*
*4: return EQR*
*5: END*

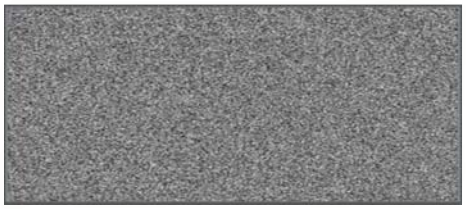
- Proposed system initialize the random image having pixel size greater than or equals to the pixel size of QR code image.
- Now, for each pixel value of QR code image, manipulate the pixel value of the random image as per the following rule.
- If the pixel value of QR code image is odd then make the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

**Image_Decoding (EQR):**

*1: Start*
*2: Initialize random image with a pixel size of EQR*
*3: For each pixel of EQR QPi:*
*If 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*
*4: return DQR*
*5: END*

(a) Original QR Image



(b) Randomly Initialized Pixel image or Mask Image

(b) Resulted Image

Fig. 2: (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.

## IV. Results And Discussion

The proposed work is successfully simulated. For overall simulation process, we have utilized the system/machine on the basis of following parameters.

This simulation setup uses the provided packages from the Python Library to simulate the performance of pro-posed work. This implementation was thoroughly tested and was optimized to give the maximum performance for the algorithms. Proposed System was coded using Python programming language and compiled using Pycharm IDE.

1) System Parameters: The experiments are conducted using desktop machine equipped with a processor Intel Core i7-4790 CPU @ 3.60 Hz with 4 GB of RAM running Ubuntu 16.04 LTS 64-bit operating system. The simulation program is compiled using the default settings in PyCharm IDE for Ubuntu applications of Python. The experiments are performed a couple of times to assure that the results are consistent and are valid to compare the different algorithms.

2) Simulation Results: Simulation results are obtained for both the independent components (Encryption and Decryption). The maximum size of data that can be encrypted by the implementation of this system is 0.80KB (810 bytes). Similarly, maximum characters including alphabets and numerals, special characters etc. are 774 characters. For two parameters, Encryption time and Decryption time, authors calculate the user time and system time.

User time: User time is the amount of CPU time spent in user-mode code (outside the kernel) within the process.

System Time: System time is the amount of CPU time spent in the kernel within the process.

3) Performance Evaluation of Proposed System: In Table III, the simulation results of proposed system are presented against the performance evaluation criteria. The comparative result of proposed system with existing QR barcode related schemes is also shown.

TABLE III: COMPARISION OF RELATED QR BARCODE SCHEMES

| *Functionality* | *[7]* | *[5,6]* | *[4]* | *Proposed* |
|---|---|---|---|---|
| ***Application Field*** | Watermarking | Image Hiding | Image Hiding | Secret Sharing |
| ***Architecture*** | - | - | - | Strong |
| ***Flexibility*** | - | - | - | Yes |
| ***Modular*** | No | No | No | Yes |
| ***Robust*** | Low | Mid | Low | High |
| ***Time to Encrypt*** | - | - | - | 8.0152 Sec |
| ***Time To Decrypt*** | - | - | - | 3.6952 Sec |
| ***Security Level*** | Low | High | Low | High |
| ***Strength*** | Low | High | Low | High |
| ***Secret Capacity*** | Low | QR image | QR image | Adjustable/ QR image |
| ***Throughput (Encryption)*** | - | - | - | 101.05Bytes/Sec |
| ***(Decryption)*** | - | - | - | 219.20 Bytes/Sec |
| ***Error Correction Capability*** | No | No | No | Yes |

## V. Conclusion and Future Work

In this proposed work, 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 i.e. cryptography and steganography.

During this analysis, it was observed that RSA was the best among all in terms of Security, Flexibility, and Encryption performance. Although the other algorithms were also competent, most of them have a trade-off between memory usage and encryption performance.

The proposed system is analyzed on the basis of both qualitative and quantitative measures. As per the result of performance analysis, proposed system provides better security against time measure. This system can be used in the area where security is prime concern rather than the time. The overall analysis of this system is done on the simulation of proposed system.

Although the proposed methods had already demonstrated a good performance, still there is a room for improvement. As a recommendation for improvement, the following need to be incorporated in future work:

- Applying different cryptographic asymmetric encryption algorithms to provide more security.
- Applying different encoding mechanisms to encode QR image for securing data hidden in QR image.
- 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 Informatics* 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): 057004

[7] Gao, Meifeng, and Bing Sun. "Blind watermark algorithm based on QR barcode." In *Foundations of Intelligent Systems*, pp. 457-462. Springer, Berlin, Heidelberg, 2011.

[8] Sharma, Shweta, and Vikas Sejwar. "Impementation of QR Code Based Secure System for Information Sharing Using Matlab." In *Computational Intelligence and Communication Networks (CICN), 2016 8th International Conference on*, pp. 294-297. IEEE, 2016.

[9] K.S.Seethalakshmi, "Use of Visual Cryptography and Neural Networks to Enhance Security in Image Steganography", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727.