QR- Based Encrytion using Cryptography and Stegnography

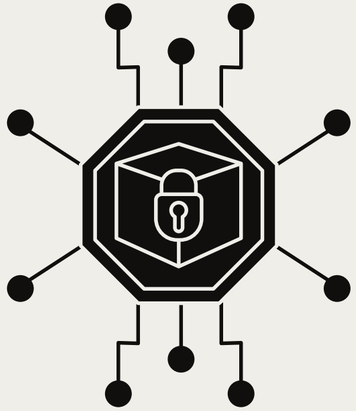
19BCI0078
19BCI0080
19BCI0084
20BCT0349

Objectives

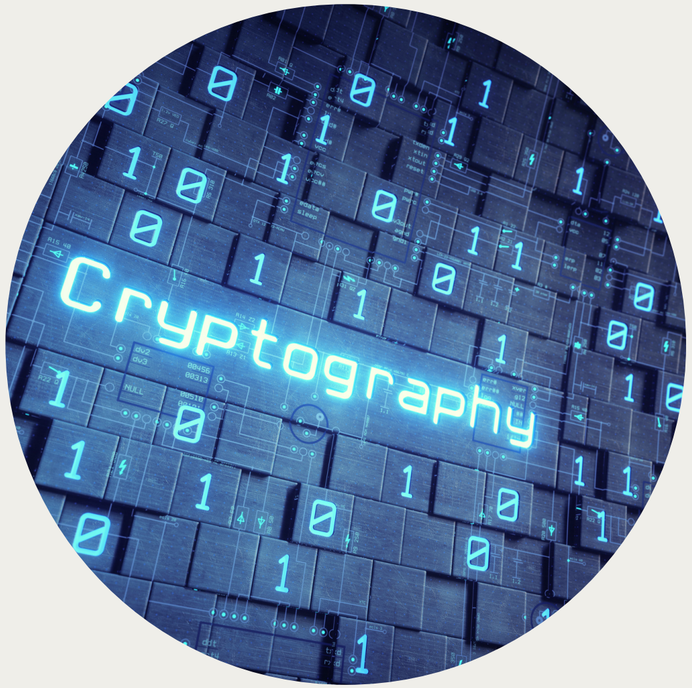
We are implementing a three-layered approach to encrypt data that uses cryptography and steganography in conjunction.

This project aims to take information security a step further by using two algorithms to ensure more security.

Background



+



Many cryptographic techniques are available for serving the purpose of information security over the web, servers and local systems. However, there is always a demand for more security which may not be met 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. This is the motivation and background of this project

Problem Statement

1) Develop a 3 layered approach using both cryptography and steganography to encrypt messages over social media platforms.

2) The first layer will include the encryption of confidential messages using the RSA algorithm(This can be replaced by some other algorithms also like AES.

3)In the second layer the generated encrypted message is embedded into a **QR code.**

4)In the last layer this QR code image is masked behind another image using image encoding algorithms

Related Work and Applications

- Intensive research work is going on related to QR code based message/information sharing and to generate a hybrid encryption algorithm that is robust, efficient, flexible has higher throughput, and has error correction capabilities.
- Pei-Yu-Lin in his paper has focused on QR code tags and proposed three-layer security system characteristics of QR code and those characteristics are utilized to design a secret QR sharing approach, in an attempt to make it more efficient for large chunks of data.

Related Work and Applications

- Another author named K.S. Seethalakshmi presented the renewed cryptographic technique for protecting image-based data and also has proposed methodology where visual cryptography and image steganography are used together, the author also proved that there won't be any loss of data after QR code masks the other visual graphics therefore similar approach is followed in this project and image steganography is done by hiding the qr code behind mask image.

Literature Survey

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

Year:2018

Metrics used to evaluate:

- Robustness
- Time to Encrypt
- Time to Decrypt
- Modularity
- Throughput
- Security Level Strength
- Error Correction Capability
- Architecture and Strength

Drawbacks:

- The proposed algorithm is very secure, but RSA is a slow algorithm to work with, so the throughput is less, which is a subject for improvement.
- Max size of data that is processed conviniently is only limited to text messages. Multimedia of different types and even long messages is not supported, or we can say the processing is not very fast.

Authors :
Abhijeet Mendhe ,Mr. Deepak Kumar Gupta , Dr. Krishna Pal Sharma

Methodology

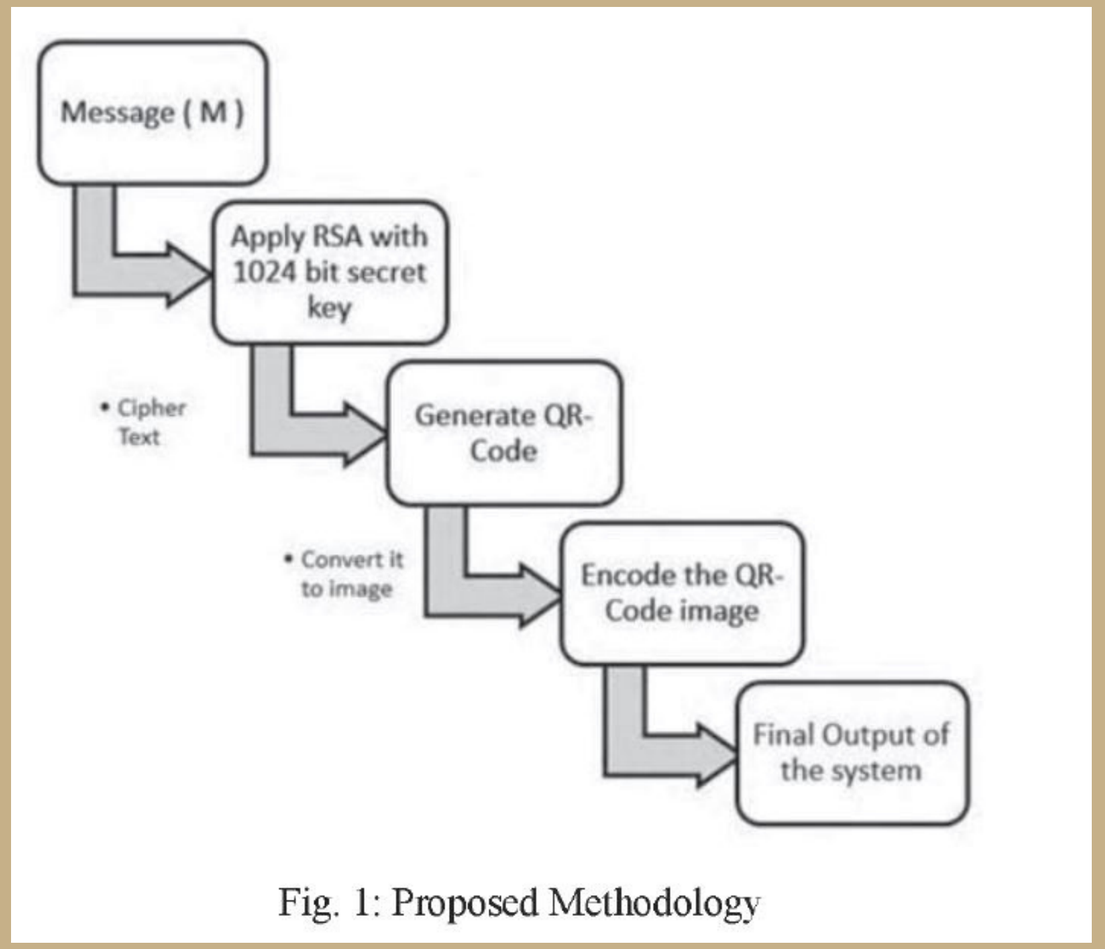


Fig. 1: Proposed Methodology

PROPOSED SYSTEM

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:

change RPi to nearest even number

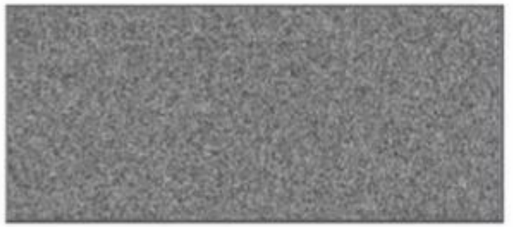
Else if QPi is odd no:

change RPi to nearest odd number

4: return EQR

5: END

(a) Original QR Image



(b) Randomly Initialized Pixel image or Mask Image

(b) Resulted Image

PROPOSED SYSTEM

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

Evaluation Metrics Discussion

- The evaluation metrics are mostly the throughput response. We are going to implement it in python with standard libraries written in cython, which makes the algorithm quite fast. The architecture and error correction ability is contradictory to each other for which a trade-off between the two is a target to be found by varying the parameters. Modularity is also a way to make the algorithm, easy to refactor and increase the throughput. The throughput is expected to be around 100Bytes/sec - 200Bytes/sec.
- The implementation will be timed and a mathematical analysis will be given wrt to the time taken and the parameters passed.

Conclusion and Future Work

During this study of the research paper, 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.

So, RSA is being used.

But RSA replacement is also a necessary task, since it is a slow algorithm

Database used

We are using an open-source API to generate QR information from text.

https://github.com/nayuki/QR-Code-generator

Contributions :

1) Akash Mohan Joshi
Further research and algorithmic analysis to integrate it into an actual application and increase the speed by using multithreading.

2) Arun Kumar Mishra
Scripting and Architecture definition

3)Himanshu Bhardwaz
QR Code API and multiprocessing research in Steganography.

4)Aditya Singh Rawat
Modularization, Documentation and further Literature Surveys

References

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

Thank You!

“He is faithful. Are you faithful as well? To have faith is to put Him first over other worldly things. Is he at your life’s center?”

Offering of Thanksgiving

THE HOLY PARISH CHURCH

SEPTEMBER 2020

Offertory Prayer

We offer you, Lord, ourselves and our work. Please accept it as a token of our gratitude to you, and in the hope that it will contribute to the building of your kingdom on earth; through Jesus Christ our Lord.

Amen.

Recessional Hymn

BREATHE ON ME BREATH OF GOD

BY EDWIN HATCH

BREATHE ON ME, BREATH OF GOD,
FILL ME WITH LIFE ANEW,
THAT I MAY LOVE WHAT THOU DOST LOVE,
AND DO WHAT THOU WOULDST DO.

BREATHE ON ME, BREATH OF GOD,
UNTIL MY HEART IS PURE,
UNTIL MY WILL IS ONE WITH THINE,
TO DO AND TO ENDURE.

BREATHE ON ME, BREATH OF GOD, TILL I AM
WHOLLY THINE, UNTIL THIS EARTHLY PART
OF ME GLOWS WITH THY FIRE DIVINE.

BREATHE ON ME, BREATH OF GOD, SO SHALL
I NEVER DIE, BUT LIVE WITH THEE THE
PERFECT LIFE OF THINE ETERNITY.