ISSN 2395-1621

Secret Messaging Based on QR Code by Implementation of Visual Secret Sharing Scheme

Pranav Hadawale, Sumoli Vaje, Dipali Wale, Prof. Pinjarkar N. R.

123Student, Dept. of Computer Engg., Sahyadri Valley COE & Technology, Pune, India

4Head, Dept. of Computer Engg. , Sahyadri Valley COE & Technology, Pune, India

1hadawalepranav@gmail.com, 2Sumolivaje@gmail.com, 3dipawale6@gmail.com

ABSTRACT

The QR code stands for Quick Response code which are mainly used for storage of credentials of particular identity, so that access becomes easy without any manual inputs. The QR codes are so much popular outside the automation industry as it has rapid and accurate detection and reading of data. Also it has more data storage capacity. The secret information are often transferred from one source to another. In case of social media we don't want that any of third person should read our secret data. That's why we require to maintain the security of message during the transfer. Meanwhile the technology has grown up so that some methods can break the traditional cipher text cryptography too. Encryption pattern analysis in case of symmetric key encryption and brute force approach are two major culprits. The proposed approach recover the drawback of the above by using QR code as medium of secret transfer. In this the secret message is converted to cipher text which is then converted to QR code shares and then transferred to another point. The method uses the concept of visual cryptography which enables added security and chances of leakage of data. For the proposed scheme we are using Blowfish algorithm which popular for both its encryption effectiveness and tremendous speed which is said that it has never been defeated. Meanwhile, it has advantage of its free availability in the public domain.

Keywords— Cryptography, Quick Response code, Visual secret sharing scheme, High security, Blowfish Algorithm, visual cryptography.

ARTICLE INFO

Article History

Received: 8th March 2020

Received in revised form :

8th March 2020

Accepted: 10th March 2020

Published online :

11th March 2020

I. INTRODUCTION

The proposed method of securing the secret data transfer using QR codes uses the concept of visual cryptography. The visual cryptography is also called visual secret sharing (VSS) in which the OR code is separated into no. of a secret image shares. This divided images are called as share images or shadow secret images. Due to this sharing mechanism each share will not reveal the secret information when secret image shares are decoded separately. The secret will be revealed when only a particular amount of qualified secret shares are merged to reconstruct the key image. Nowadays, the QR codes are used in the mobile phones and apps. A popular example of this can be the QR code of our UPI in Phonepe or Google pay applications. In that UPI id of our account is embedded in a QR code so that we don't need to enter the details of account manually in order to do a transaction. This increases the speed of transaction by just scanning of our QR code from another application. Similarly in case of secret messaging, it's unsafe to transmit secret information within the general public channel without protection, and mobile devices are widely used nowadays. So encoded secret data in QR code, which is shared into different QR code secret cover images called as shares. Then the shares are transferred through different channels from one mobile to anther mobile.

Figure 1: QR code shares

It works similar to packet transfer in internet. If any suspicious attacks occur during the transmission of secret, the shares cannot reveal the data, so the secret information would not be recovered.

The Visual Cryptography Scheme (VCS) is a scheme that works on sharing secret images. The base idea of this type of visual cryptography is to separate a secret QR image into no. of secret shares which will not reveals any secret information from share of secret image when decoded separately. To reveal the secret information, the secret QR code structure is reconstructed by stacking operation of the QR code shares.

Objectives of our scheme is to propose a visual secret sharing scheme for QR code applications, that mainly focus on higher security and more flexible access structures. Also to Propose the scheme by which reconstructed secret can be read directly by a machine. It is necessary to develop a method to encode a secret image into n noise-like shadow images called share images for added security. The scheme enables QR code as an information carrier to transfer shadow information and secret message.

II. LITERATURE SURVEY

C. N. Yang and D. S. Wang [1] proposed that the effectiveness of XVCS is greater than OR based VCS. The XOR-based VCS uses XOR based decoding. To decode the secret message image stacking operation is done. XVCS gives more accurate reconstructed image than OVCS. But the proposed scheme algorithm operation is difficult to implement.

P. P. Thulasidharan, M. S. Nair [2] presented a key based technique for watermarking that works by embedding a binary format of the watermark information in the cover image. This scheme can represent more information for per bit change. Also it has more error correction capability. As the given technique is limited to a LSB bit of the image intensity values it is more susceptible to attacks.

Tkachenko, W. Puech, C. Destruel [3] has given the two-level QR code (2LQR) method in which public and private storage are used. The public level is the standard QR code storage level so can be read through any QR code read application. The private level is built by replacement of black modules by specific textured patterns. This strategy improved the storage of QR code. But it is requirement to improve the pattern recognition criteria.

III. EXISTING SYSTEM

This system uses concept of steganography. Steganography is the technique of hiding secret data within a standard, non-secret, file or message so as to avoid detection. The secret data is then revealed at its destination. The employment of steganography is combined with encryption as an additional step for hiding or protecting data. Steganography is used to hide text, image. The content to be concealed is commonly encrypted before being incorporated into the document or data stream. If not encrypted, the hidden text is often processed in a way so as to extend the issue of detecting the secret content.

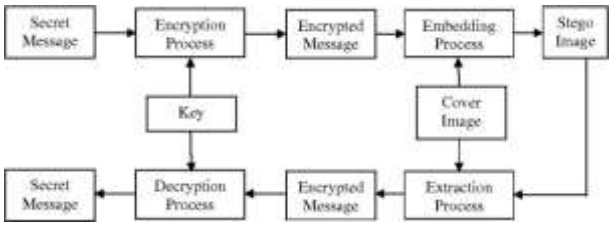

Figure 2: Existing System

IV. PROPOSED SYSTEM

To The secret message is encoded or encrypted to cipher text by using. Then the encrypted message converted to QR code structure. And further it is splited into many secret shares. After that it will send to another user. In receiver end, we have to combine all the QR code shares by stacking and original message can be retrieved. The proposed system involves two users one is sender and another is receiver. The sender have login to through his registered user name and password. Sender can search for a particular friend from the list of friends and select his

receiver from the list of the registered user and send him the message. The receiver who is receiving the message in this phase must connected to the internet so that he can get the message. The message from the sender is received as a shares of QR code. The receiver should merge the QR codes to get the secret data. So the malicious user are unable to detect the original secret data. The basic idea can be described as follows: sender sends the secret data message and that secret message will be encrypted with cryptographic algorithm followed by QR code formation of encrypted text and then splitting and storing it in shares of QR code for of security and to avoid the common access of message.

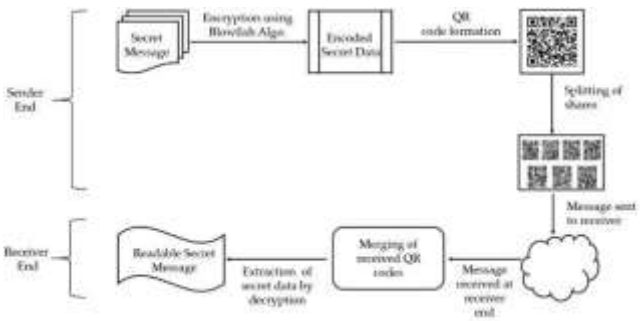

Figure 3: Proposed System Flow

V. IMPLEMENTATIONS

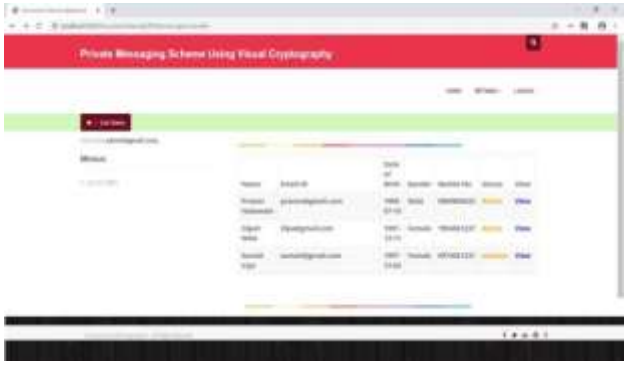

Figure 4: List of active users

The Fig.4 shows the list of users on admin login. The status of the user can be changed to active or inactive. Also the profile of user can be viewed.

Figure 5: Searching a friend

The Fig.5 shows the searching operation at the user login. User can search the name of another user to send the message.

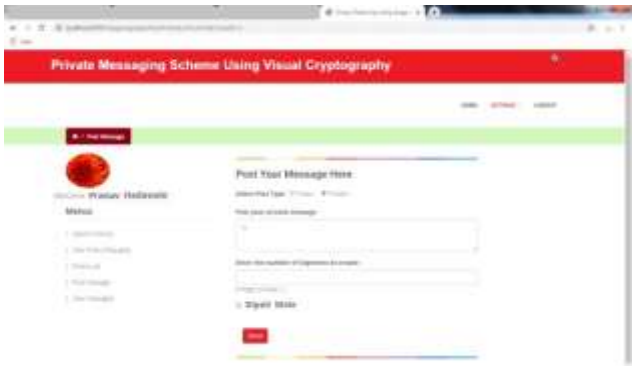

Figure 6: Sending secret message Hi

The Fig.6 shows window to send the secret message to another user. The user has to specify how many shares to be form.

Figure 7: QR code generation and share formation

The Fig.7 shows QR code formation of secret message. After that shares are formed and message send to user.

Figure 8: Shares received at receiver end

The Fig.4 shows shares received at receiver end. After they are merged to get secret data.

Figure 9: Secret message revealed by merging shares

The Fig.4 shows revealed message at receiver end

VI. CONCLUSION

This project uses QR code as an information carrier to transfer secret message. At the same time it ensures security and privacy of data. Compared with traditional cryptography, it has the advantages of concealment, security, simplicity of secret recovery. It is easy to generate value in business applications. The project gives the higher security and more flexible access structures.

REFRENCES

[1] C. N. Yang, D. S. Wang, "Property Analysis of XOR- Based Visual Cryptography," IEEE Transactions on Circuits & Systems for Video Technology, vol. 24, no. 12 pp. 189-197, 2014.

[2] P. P. Thulasidharan, M. S. Nair, "QR code based blind digital image watermarking with attack detection code," AEU - International Journal of Electronics and Communications, vol. 69, no. 7, pp. 1074-1084, 2015.

[3] I. Tkachenko, W. Puech, C. Destruel, et al., "Two-Level QR Code for Private Message Sharing and Document Authentication," IEEE Transactions on Information Forensics & Security, vol. 11, no. 13, pp. 571-583, 2016.

