International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

# Visual Cryptography using QR Code

**Dr. M Sandhya Rani*[1], M. Akhila[2], H. Eshika[3]**
[1]Associate Professor, Department of Information Technology, Bhoj Reddy Engineering College for Women, Hyderabad, India
[2,3]Students, Department of Information Technology, Bhoj Reddy Engineering College for Women, Hyderabad, India

ARTICLEINFO

**Article History:**

Accepted: 10 Feb 2023
Published: 23 Feb 2023

**Publication Issue**
Volume 10, Issue 1
January-February-2023

**Page Number**
392-395

## ABSTRACT

The QR code cryptography with a password and sends it to the required hiding the information QR code. Securing and hiding personal confidential information has become a challenge in these modern days. Due to the lack of security and confidentiality, there are chances that forgery of the confidential information or unauthorized access of a system can cause a big margin loss to a person or a system. At present, confidentiality is maintained in old ways and for that reason, there are possibilities that the confidential information might get forged or hacked. Personal confidential information can be securely shared with the expected person and the person can verify the information by checking its authenticity. Similarly, confidential information can also be kept securely hidden and used to meet a specific purpose like getting access privilege of a secured system and the system can validate the confidential information by checking whether the person is authorized or the information is valid. QR codes are being used increasingly to share data for different purposes. Information communication, QR code is important because of its high data capacity. However, most existing QR code systems use insecure data format and encryption is rarely used. A user can use secure QR code technology to keep information secured and hidden.

**Keywords :** Cryptography, Encrypt, Confidential, Secure, QR Code

## I. INTRODUCTION

Nowadays, it is almost impossible to secure and hide personal confidential information like system credentials, Automated Tray Machine(ATM) Card PINs, Ticket Passenger Name Record(PNR), etc., which can be easily hacked and used for unauthorized purposes. Such hacked information can cause huge loss to a person. At present, personal information confidentiality is done by the person's own manual unsecured way and there are chances that the information is not completely secured and hidden. Advanced Encryption Standard (AES) algorithm for legal document data hiding, message hiding, etc.. However, these methodsdo not consider cases when personal confidential information needs to be shared securely. Quick Response (QR) codes are being used increasingly to share data for different purposes such as authentication, verification, etc. The popularity of QR code is because of its high data capacity, error correction capability using Reed-Solomon error correction algorithm, fast decoding, etc. However, most existing QR code systems use insecure data format and encryption is rarely used. It is possible to use secure QR code technology to keep his important sensitive information perfectly secured at all times, without the information gets leaked to outside world. Cryptographic algorithms like AES, Data Encryption Standard (DES), Rivest, Shamir, Adleman (RSA) etc., can be used to make a QR code system secure.

## II. RELATED WORK

This chapter gives an overview of QR code technology and also provides the background information regarding the concepts of cryptography and the consecutive sections discuss about the concept of RSA algorithm and digital signature.

### QR CODE

Quick Response (QR) code as shown in Figure 2.1 is a barcode standard developed by Japanese company Denso Wave in the 1990s. Compared to traditional 1D (1-dimensional) barcodes, QR codes are 2D (2-dimensional), allowing for a greater amount of information storage. QR code consists of a black square pattern on white background and it contains information in the vertical direction as well as the horizontal direction. QR codes have a wide variety of uses.

**Figure 2.1: A Sample QR Code**

### QR Code Structure

Figure 2.2 shows QR structure regarding code version information, format information, data and error correction areas, required patterns (position detection pattern, alignment pattern and timing pattern) and quiet zone. QR Codes are 2-dimensional, which results in them having a square filled with data. Besides data, there are certain identifiers helping the code being read correctly. The most common QR Code type is model 2, which is broken down in the following information identifiers:

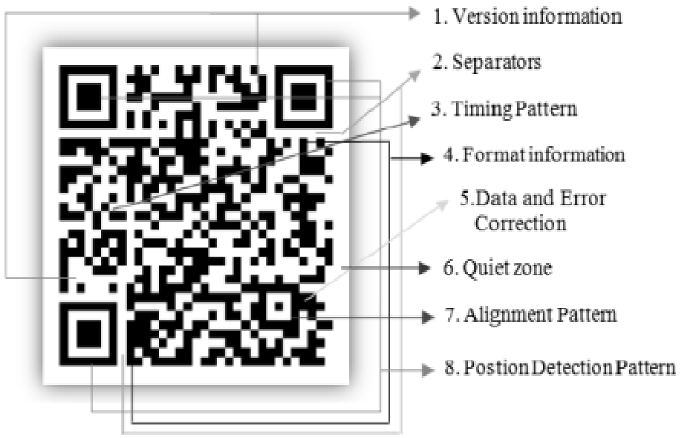

**Figure 2.2 :** QR Code Structure

Version and format information are important for the scanning device to know what kind of data to expect. QR codes have symbol versions from 1 to 40. It determines the data capacity of the code. So the more the data stored, the bigger the size of the QR code. Meanwhile, the data can be slightly damaged or missing and still be readable. This depends on the error correction level being used when writing the code. Rotation of QR Codes is possible whichever direction we may like. This is a courtesy of the position patterns (squares with dots in the middle) that allow the code to be read from any direction in 360 degrees. Meanwhile, the alignment patterns are used to assist in navigation of larger codes and the timing patterns are used to determine the size of modules. The quiet zone requires a margin ofat least 4-module worth.

## III. PROPOSED SYSTEM

An explanation of the suggested QR-based online payment system is given in this section. In the first subsection, the system's functional description will be provided, along with specific operational processes. After that, the second sub-section discusses security issues. The possibility of establishing consumer and merchant accounts has been examined in this research. In order to increase security, consumer accounts have the option to receive and transfer credit, whilst merchant accounts can only accept money. In Fig. 3.1, the suggested QRbased online payment system's architecture and operational flow are depicted. The system is made up of the three components—the cloud server, the consumer, and the merchant—as seen in the image. The three parties' communication during a payment transaction is described by the operational processes below:

Step 1: The first stage entails from the cloud server the merchant requesting a per-bill Quick Respond

Step 2: The second stage is when a QR code with a share embedded in it is sent by the cloud server.

Step 3: involves scanning a QR code by a customer to begin a transaction.

Step 4: involves submitting a payment request to the cloud server's backend system.

Step 5: the cloud server completes the transaction and sends the conformation number to the user.

Step 6: The merchant receives the processing results for approval.

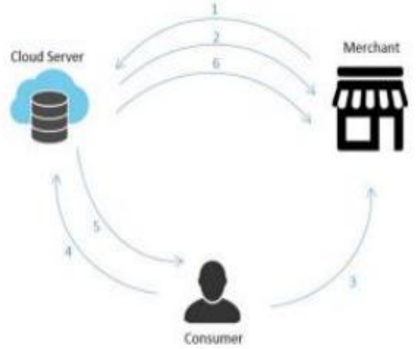

**Fig. 3. 1.** General workflow of the proposed QR payment system

The visual cryptography scheme (VCS) algorithm which is employed in the design to secure user-to-user transactions, is used. It is built on a (2, 2) VCS, where two shares are formed, and the two shares must be stacked to display the original image. The input can be encrypted at one end and then decoded at the other due to the bidirectional nature of the technology. The encryption and decryption of images, as well as QR codes, are carried out on the server's end to increase security and eliminate any chance of manipulation at the client's end. A merchant requests payment to start and provides an estimated amount in advance before the service is rendered. One of the produced shares is transferred by the programme to the merchant in the form of a scannable Quick Response code. Using the merchant data provided by the server, it creates the standard Quick Response code, feeds it into VCS, and outputs the code. The other portion will be kept by the server. When the Quick Response code is scanned, the corresponding twin share will be purchased along with the other share, and a successful transaction will be completed. Fig. 3.2's left side illustrates the process of making two shadows from a Quick Response code, and its right side illustrates the procedure for verifying a Quick Response code after scanning.

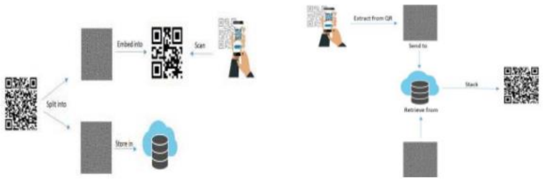

**Fig.3.2.** (left) Construction of (2, 2) VCS, and (right) Stacking of (2, 2) VCS.

## IV. CONCLUSION

In conclude, companies have greatly profited from the developments in online payment technology, which have also markedly increased customer pleasure. Due to the fact that the payment process is concealed from the user, technology replacements are looking into ways to speed up, make it safer, and make it more inventive. Online payment errors cannot be accepted because of how easily a variety of cyberattacks are now conceivable because to the ease of online payment systems. Data leak, denial of service, fraud, and forgeries are a few of the assaults. Numerous strategies of various complexity have been proposed to lessen these hazards. This study suggests a secure QR-based online payment solution. The recommended system's security stands out since it modifies a single algorithm to provide the necessary security services: To provide authentication, confidentiality, and integrity, visual cryptography is utilised. Users will soon be able to create static Quick Response codes that are connected to their accounts exclusively owing to a new feature that will be included. These static Quick Response codes are read, allowing the payee to enter the minimum payment but without saving the balance. Sessions may be used to keep users registered in as an added convenience rather than the current programme, which requires the user to log in each time the software is launched. A last security update includes setting up multiple threads on the server to detect and remove Quick Response codes that have been saved for further than five minutes.

## V. REFERENCES

[1]. Francisco Liébana-Cabanillas “User behaviour in QR mobile payment system: the QR Payment Acceptance Model” University of Granada, Granada, Spain, https://www.tandfonline.com/doi/abs/10.1080/09537325.2015.1047757?cookieSet=1

[2]. SUEBTIMRAT, Panupong “User behaviour in QR mobile payment system” Graduation School of Business, Assumption University https://koreascience.kr/article/JAKO202100569464364.page

[3]. Nishant Goel; Ajay Sharma; Sudhir Goswami” A way to secure a QR code:”, publisher: IEEE: https://ieeexplore.ieee.org/abstract/document/8229850

[4]. I.J. Information Engineering and Electronic Business, 2022, 3, 10-18 “QR: Approaches for Beautified, Fast Decoding, and Secured QR Codes” Published Online June 2022 in MECS

[5]. Li-Ya Yan.Kampar, Malaysia “QR code and mobile payment”, Universiti Tunku Abdul Rahman, Kampar, Malaysia: https://www.sciencedirect.com/science/article/abs/pii/S0969698920313084#!

**Cite this article as :**

Dr. M Sandhya Rani, M. Akhila, H. Eshika, "Visual Cryptography using QR Code", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 10 Issue 1, pp. 392-395, January-February 2023.
Journal URL : https://ijsrset.com/IJSRSET2310172