Design of secure QR payment system using Visual Cryptography method

Dr. Praveena Narayanan
Assistant Professor Department of Computer Science and Technology
Madanapalle Institute of Technology & Science
Madanapalle, India
praveenan@mits.ac.in

Yadlapalli Lokesh
Department of Computer Science and Technology
Madanapalle Institute of Technology & Science
Madanapalle, India
18691A2820@mits.ac.in

P.Charitha
Department of Computer Science and Information Technology
Madanapalle Institute of Technology & Science
Madanapalle, India
18691A2512@mis.ac.in

G.Chethan Teja Kumar
Department of Computer Science and Information Technology
Madanapalle Institute of Technology & Science
Madanapalle, India
18691A2513@mis.ac.in

B.Bhavya
Department of Computer Science and Information Technology
Madanapalle Institute of Technology & Science
Madanapalle, India
18691A2509@mits.ac.in

S.Hemalatha
Department of Computer Science and Information Technology
Madanapalle Institute of Technology & Science
Madanapalle, India
18691A2526@mits.ac.in

2023 International Conference on Computer Communication and Informatics (ICCCI) | 979-8-3503-4821-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICCCI56745.2023.10128604

Abstract— **In this paper, we will discuss how asecure link-sharing system based on QR codes was created and put into operation. In recent years, QR codes have grown in popularity since they expedite linksharing and provide users with the greatest level of ease. QR-based online systems, as easy as they may appear, are subject to a variety of assaults. As a result,link sharing must be safe enough to ensure each process, integrity and secrecy. The link sharing system must also guarantee each transaction's sender and receiver's legitimacy. The suggested QR-based systemin this paper is secured using visual cryptography. Thevisual cryptography is carried out using a web application that is part of the proposed system. Users can exchange URLs through QR code using a simple and user-friendly interface provided by the app.**

Keywords - Visual cryptography, Quick Response code and E-Payment systems.

I. INTRODUCTION

A two-dimensional matrix barcode called a QR code can encode and store a lot of data. Numerous essential applications, including those in health, education, and finance, have made substantial use of QR codes because of their efficiency and ease [1]. Several safe QR-based online payment methods have been put forth in the literature. Different payment schemes have been presented, with each offering varying degrees of speed and security. These models include, for instance, the Operator Centric Model and the Peer- to-Peer Model.

As digital images grow increasingly significant in multimedia technologies, users' privacy becomes more vital. Image encryption is essential to provide the user with this level of security and privacy. Only a handful of the uses for picture encryption include military communication, telemedicine, medical imaging, and multimedia systems [15]. Colour photos are widely transmitted and stored through the Internet and cellular networks, taking advantage of rapid advancements in multimedia and network technologies. Image encryption differs from data encryption. There are also various security issues involved with digital picture processing and transmissions, thus image integrity andconfidentiality must be maintained.

Digital images are additionally less sensitive than data since a single pixel change does not impact thecomplete image [2]. In other words, a small alteration to a digital image makes it more susceptible to hackers yet is acceptable compared todata.

A. Visual Cryptography

Visual information (pictures, text, etc.) is encrypted using a technique called visual cryptography, which results in a visual image whenthe information is decoded [11]. The emerging encryption technology known as visual cryptography rewrites encrypted images using the traits of human eyesight. Secure digital transmissionis offered by visual cryptography, however it is only ever used once. Numerous instructions, including corporate and military identifiers and maps, are transmitted online. Security concerns must be taken into account while designing patterns for covert

979-8-3503-4821-7/23/$31.00 ©2023 IEEE

ictures since hackers may use a communication network's vulnerability to obtain the data they need. Different image secret sharing systems are developed to address the protection issues with hidden photos. Without any knowledge of science and with any calculations, anyone may use it for coding.

The subsequent sections are structured as follows. The system's overall design is described in Section II. In section, III describes the literature survey. Whereas Section IV discusses how it is put into practise. The paper is concluded in Section V with a discussion of the findings and future work.

II. PROPOSED SYSTEM DESIGN

We propose a novel framework based on the image encryption and QR Code for sharing the links. The URL will be transformed to QR Code first, then encrypted, and finally the URL of the encrypted QR Code will be turned to QR Code again. This manner, even if we publish the QR Code, no one will be ableto access the actual URL; only those who have an image decryption tool will be able to decrypt the QRCode and access the link.

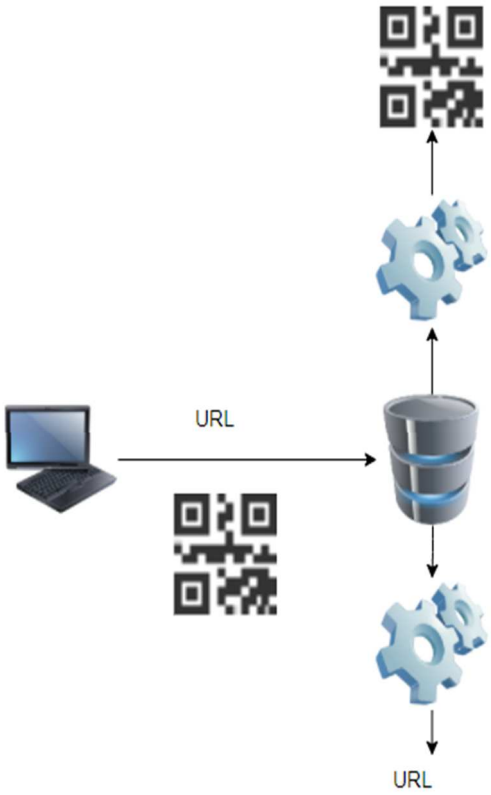

Fig. 1 Functionality of QR payment system

The following diagram depicts how the actual system works. The figure shows mainly five steps.These steps are explained below:

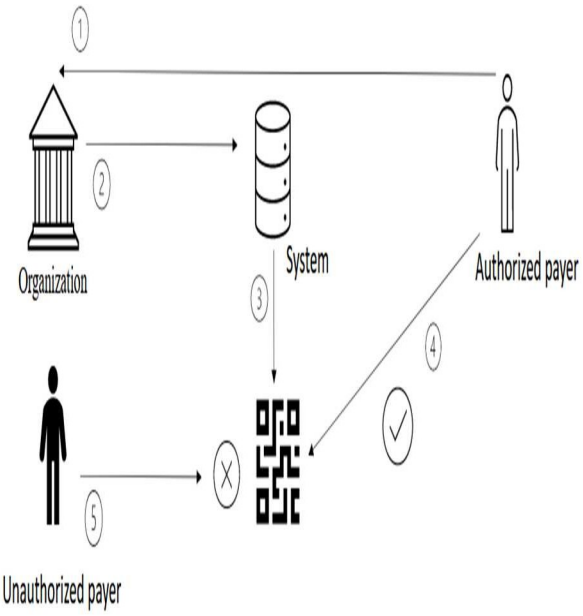

Fig. 2 Design of Proposed System

Step 1: The main theme of the system is security, which is the one who is authorized can only access the system details, so that the organization details are shared only with its consumer/authorized user. Initially the organization should have the details of its users or payers.

Step 2: The details of the organization and its payersare shared with the system.

Step 3: The system generates the QR code for that particular organization and its payers. Using thesecure QR code payment methodology using visual cryptography.

Step 4: The payer who is authorized can access the payment link embedded in the QR code.

Step 5:The unknown payer or other user cannotaccess the actual link embedded in the QR code.

III. LITERATURE SURVEY

S. No	Author	Year	Technique or Algorithm	Performance	Merits	Demerits
1.	Jianfeng et al[3]	2020	RSA Encryption Algorithm	Data integrity checks.	Pure RSA encryption technique is less time consuming and less processor-intensive	It has slow data transfer rate due to large numbers involved.
2.	Yang et al [4]	2019	Near field communication technology	Speed	Can be scanned for various payment options.	It requires more encryption techniques.
3.	Sangeeta et al [5]	2019	Encoding and decoding techniques based on timing and alignment pattern	Error correction level	High capacity data storage, small printout size.	Emerging technology, such as near field communication, may cause obsolescence.
4.	Espejel et al [6]	2018	Data hiding Algorithm, Encryption technique, Error correction algorithm,	Based on existing key pairs.	Sensor for digital images in two dimensions In addition, possible to create artistic QR codes for error correction.	If message is splits into several Reed-Solomon code blocks then it limits the complexity of the decoding algorithm
5.	M. F. Tretinjak et al [7]	2019	QR draw Ad software and QR maker Ad	Accuracy	It contains the teacher's contact information, connections to other important web pages for the course, and information about the course learning outcomes and grading system.	It was difficult to read on a mobile device's display.

IV. SYSTEM IMPLEMENTATION

This system runs on software. The web application is designed without any physical components to give organisations access. Thewebsite is developed using the Django framework.

The application is written in python programming language using PyCharm [8]. The online application's UI is straightforward and user-friendlyfor those who utilise the payment system. Whether users are individuals or businesses is determined

during the registration process, which involves providing personal information that will be hashed and sent to the server. A user can generate a QR code after logging in or Scan and Generate a QR code, depending on whether they are a client or a memberof an organisation.

The organizations can login to the website and provide the details including the actual paymentURL[9]. Then the actual payment URL converted tothe QR code. Then this QR code is encrypted using the visual cryptography. Visual data (such as images, text, etc.) is encrypted using a technique called visual cryptography, which can only be decoded visually. Then the URL of this encrypted code is changed to another Quick Response code once again. This QR code is shared for the paymentprocedure among the payers. So, only the authorized user can access the actual link. From the site organization can download that QR code and share among their payers. On the website, users can choose to decode the QR code so that an actuarial payment [10] link appears when they upload an image or QR code. The below diagram represents the block diagram of the methodology implemented.

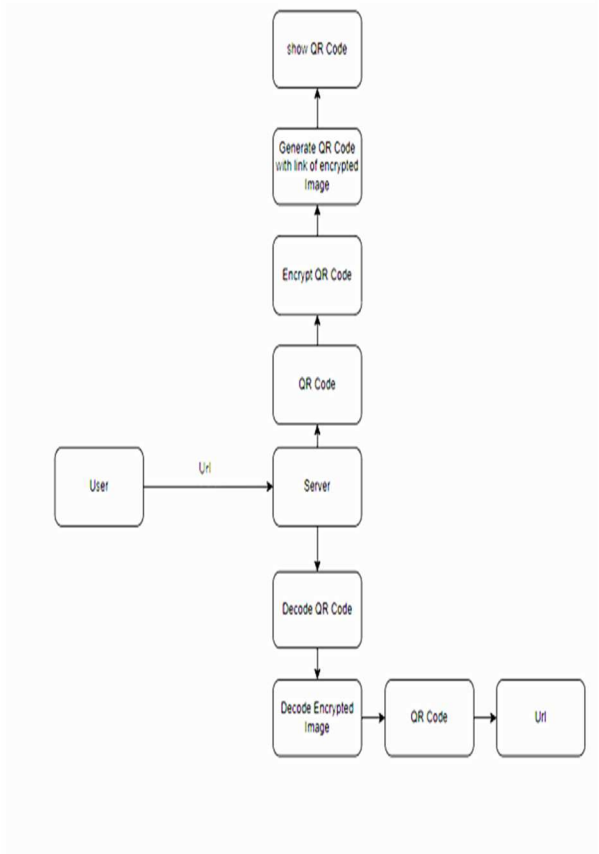

Fig.3 QR Payment system Methodology

The following figures show the website pages.

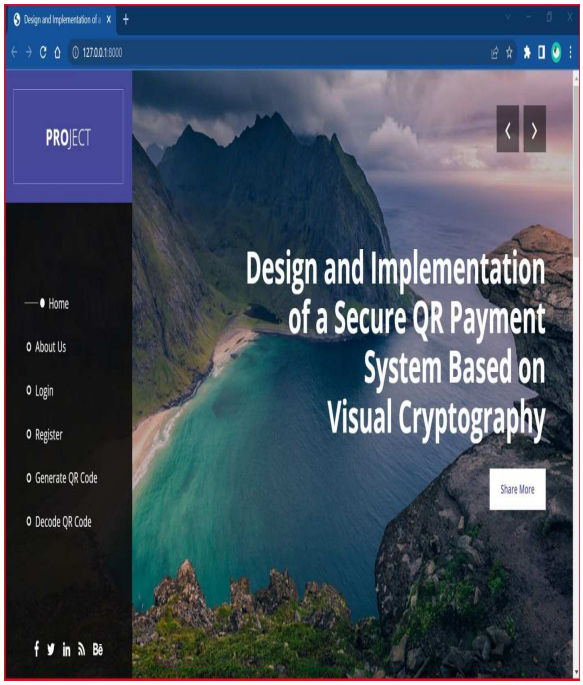

Fig 4: Home Page of QR Payment system Website

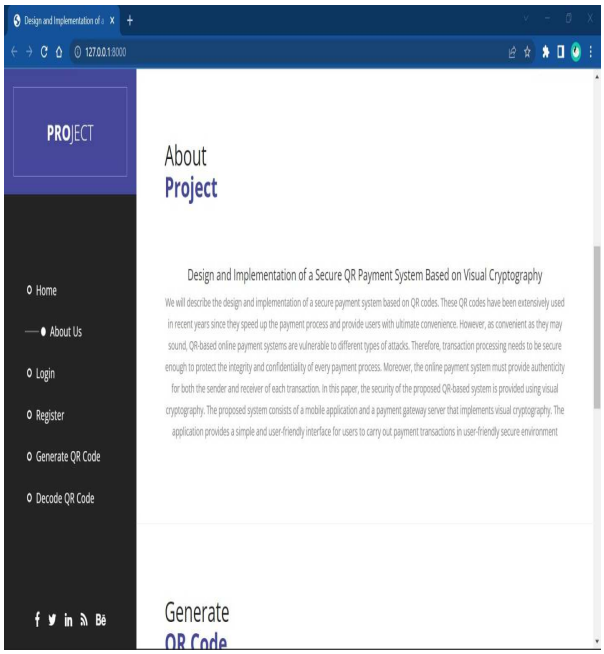

Fig 5: About us page in QR payment system

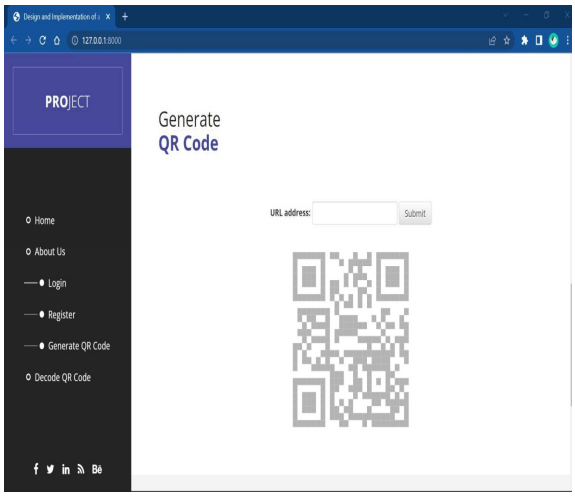

Fig 6: Generate QR code page in QR paymentwebsite

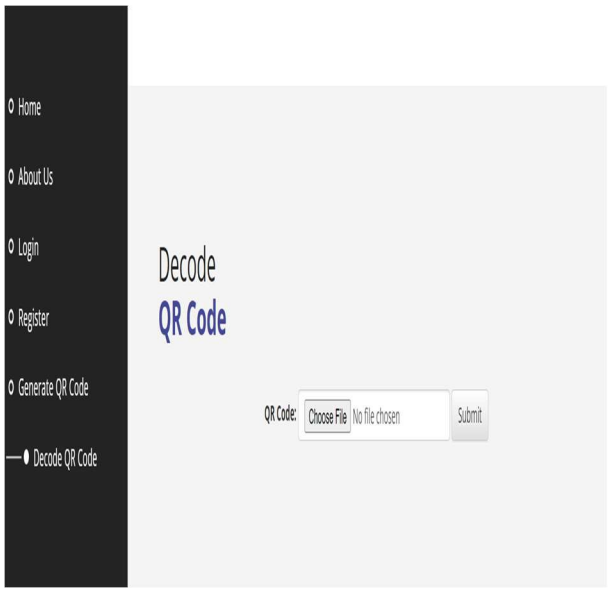

Fig 7: Decode QR code page in QR payment website

V. CONCLUSIONS AND FUTURE WORK

In conclusion, the development of onlinepayment methods thriving commercially and dramatically enhanced customer experience. Because the user is unaware of the payment process,technical solutions are exploring for ways to accomplish this problem. Faster, safer, and more creative payment methods are now available in the online world You can't make mistakes for payment, convenience Online payment systems are another significant target of cyberattacks [14]. Data theft, denial of service attacks, fraud, and counterfeiting are the most serious types of these attacks. Numerous solutions of differing degrees of sophistication have been put forth to thwart these attacks. In this research, we suggested a safe QR code sharing application and used image cryptography to make links more secure. Further research on the application of deep learning techniques is advised for future works in order to maximise the outcome for detecting fake faces. Additionally crucial is the selection of photos from various datasets. In order to increase the accuracy offace spoofing detection, deep learning will be used in future.

VI. REFERENCES

[1]. T. Ma, H. Zhang, J. Qian, X. Hu and Y. Tian,"The Design and Implementation of an Innovative Mobile Payment System Based on QR Bar Code," 2018 International Conference on Network and Information Systems for Computers, Wuhan, 2018, pp. 435-440.

[2]. L. BURRA P. TUMULURU, S. GONABOINA "Secure QR-Pay System with Ciphering Techniquesin Mobile Devices", International Journal of Electronics and Computer Science Engineering, P.V.P.Siddhartha Institute of Technology, Kanuru, Vijayawada, Krishna, 2019.

[3]. Jianfeng Lu, Zaorang Yang, Lina Li, Wenqiang Yuan, Li Li, and ChinChen Chang, "Multiple Schemes for Mobile Payment Authentication UsingQR Code and Visual Cryptography," Mobile Information Systems, vol. 2017, Article ID 4356038, 12 pages, 2020.

[4]. Yang, Ching-Nung & Liao, Jung-Kuo & Wu, Fu-Heng & Yamaguchi, Yasushi. (2019). "Developing Visual Cryptography for Authentication on Smartphones". 189-200. 10.1007/978-3-319-44350-8_19.

[5]. Sangeeta Singh. May 2019. "QR Code Analysis" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 5, ISSN: 2277 128.

[6]. Espejel-Trujillo, I. Castillo-Camacho, M. Nakano-Miyatake, and H. Perez-Meana, "Identity

document authentication based on VSS and QR codes," Procedia Technology, vol. 3, pp. 241–250, 2018.

[7]. M. F. Tretinjak, "The implementation of QR codes in the educational process," 2019 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2019, pp. 833-835.

[8]. X. Yan and Y. Lu, "Applying QR Code toSecure Medical Management," 2018 9th International Conference on Information Technology in Medicine and Education (ITME),Hangzhou, 2018, pp. 53-56.

[9]. W. C. Wu, "A QR Code-Based on-Street Parking Fee Payment Mechanism," 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kitakyushu, 2014, pp. 106-109.

[10]. S. Nseir, N. Hirzallah and M. Aqel, "A secure mobile payment system using QR code," 2020 5th International Conference on Computer Science and Information Technology, Amman, 2013, pp. 111-114.

[11]. Ariana Tulus Purnomo, Yudi Satria Gondokaryono, Chang-Soo Kim, Ilkyeun Ra, "The Combining Method of Fingerprint and QR Code as Mutual Authentication for Mobile Payment", SERSC Korea Information and Communications Society Journal of Information and Communication Convergence Engineering, 2018.

[12]. Somdip Dey, "SD-EQR: A New Technique toUse QR Codes in Cryptography", International Journal of Onformation Technology and Computer Science, IJITCS, May/June 2019.

[13]. C. Chan and C. Lin, "A New Credit Card Payment Scheme Using Mobile Phones Based on Visual Cryptography," in Intelligence and Security Informatics, vol. 5075 of Lecture Notes in Computer Science, pp. 467–476, Springer, Berlin, Germany, 2018.

[14]. C. Yang, J. Liao, F. Wu, and Y. Yamaguchi, "Developing visual cryptography for authenticationon smartphones," in Industrial IoT Technologies and Applications, vol. 173 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 189–200, Springer International Publishing, Cham, 2019.

[15]. W.-P. Fang, "Offline QR code authorization based on visual cryptography," in Proceedings of the 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing *(IIHMSP '11)*, pp. 89–92, October 2020.