

Design And Implementation of Secure Qr Payment Based on Visual Cryptography

Dr. Vineetha K R¹, Habeeba Sinu²

¹Associate Professor, Department of MCA , Nehru College of Engineering and Research centre

²MCA Scholar, Department of MCA , Nehru College of Engineering and Research centre

Abstract:

In this paper, the design and implementation of a secure payment system based on QR codes will be covered. In recent years, QR codes have been widely used due to their capacity to speed up payments and provide customers with the highest comfort. Yet, as convenient as QR-based online payment systems may seem, they are vulnerable to a variety of attacks. Transaction processing needs to be adequately secure in order to protect the privacy and accuracy of each payment operation. The online payment system must also guarantee the legitimacy of each transaction for both the sender and the recipient. This article offers security for the proposed QR-based system using visual cryptography. The recommended solution consists of a mobile application and a payment gateway server that employs visual cryptography. Customers who use the application may conduct financial transactions in a secure environment thanks to its clear and user-friendly layout.

Keywords: online payment system, QR codes, visual cryptography

INTRODUCTION

In several businesses, online payment solutions are expanding quickly. The digitalization of the payment system transaction process has led to the emergence of several apps that make use of this revolutionary technology. Indeed, the development of online payment, from credit cards to NFC-based payment, has a far more promising future. Yet as technology advances, so do the dangers of not safeguarding it. Security is a big concern for both consumers and company owners, according to research on many online payment system deployments. Typically, theft, fraud, and impersonation are threats to payment transactions. These security flaws put the system's availability, confidentiality, and integrity at risk. Therefore, overcoming security is essential to the success of any online payment system. In a QR code, a two-dimensional matrix barcode, large amounts of data may be encoded and saved [1, 2, 3]. Due to their speed and simplicity, QR codes have found significant usage in a number of crucial sectors, including health, education, and finance [4, 5, 6, 7, 8]. There are a number of secure QR-based online payment options available [9–15]. Each of the several payment alternatives offered by [9] offers differing levels of security and quickness. These models include the Operator Centric Model and the Peer-to-Peer Model. To boost security, these methods use public and private keys in each transaction. The online payment mechanism mentioned in [10] uses public and private keys during user registration. The keys are generated using a random seed number, the users' ID, and the Mobile Equipment Identity (IMEI). The approach recommended in [11] modifies the method [10] by switching out the SHA-256 algorithm for the elliptic curve digital signature technique to protect the authenticity of the certificates generated and the transaction messages sent between users. [12]

defines visual cryptography as a technique for hiding a picture using any number of shadow pictures, or shares. Visual cryptography and QR codes are often used together in the procedures given in [13]. This system is made up of the smartphone, the verification server, and the barcode decoder. The approach suggested in [14] starts with a (2, 2) VCS to generate two shares, which are then sent through a transformation function to create a numerical string.

This paper suggests a safe QR code-based online payment system. We compare public key cryptography with visual cryptography to provide the required security for the proposed system. The main disadvantages of using public key cryptography in electronic payment systems include the need for a third party to demand and validate certificates, the need for protection of the private key storage and certificate storage on the device, and the expense of generating the public and private keys. On the other hand, visual cryptography accomplishes secrecy, integrity, and authentication, does not need the sending of any personal information, and offers quick calculation. Based on these performance discrepancies, visual cryptography has been employed as a method of securing the suggested online payment system. The proposed payment method relies on sending data-carrying QR codes, therefore protecting the QR code will offer the required security. With the development of steganography and cryptographic algorithms, visual cryptography is a technique for securing visual data, which in the proposed project will be the QR code itself.

LITERATURE SURVEY

The quick response (QR) code is a useful tool for mobile phone users. The code may be photographed using a smartphone camera and then decoded using a special reader software. The code specifically denotes brief text, contact details, or a web link. Its availability makes keypad typing on phones easier for consumers. This paper suggests a method for paying for on-street parking that is based on an E-QR bill's code. Consumers can think of the code as a bill to pay their parking charge, with the parking details being entered by the fee collectors into a distant server. The major goal of this technique is resource conservation, such as lowering paper usage. The suggested smartphone application offers a new method for Taiwanese on-street parking Ebill payment, according to simulation findings. Also, the aforementioned application acts as a role model for various parking payment methods. A rapid response (QR) code is a helpful tool for those who use mobile phones. The code may be captured using the smartphone camera and then decrypted using a specialised reader application.

Basheer, Amen, & Sawsan Kamal. (2016). A Novel Technique Using QR Codes to Decode a Message: Here. Another information-concealing computation that we've shown totally converts the message to OR code (Quick Response Code) and creates OR for cover (Key). Since OR Codes have greater or much larger capacity restrictions than other ordinary normal standard identifications, they are typically utilised to transmit or store communications. The authors of the current study have described an encryption method that involves first scrambling a message by XORing a section (series of parts) of a QR message with a related piece of OR veil Key, and then inserting the Key into the generated QR.

"An Introduction to QR Code Technology," S. Tiwari:

A two-dimensional network code called "Quick Response" is set up by keeping two feasible focuses. as an example. When distinguished from ID-normalized differentiating pieces of proof, it has to hold enormous amounts of information (data), and any portable device, like a phone, should be able to swiftly

decode it. The whole range of benefits offered by QR codes includes high information store capacity, rapid verification, omnidirectional clarity, error correction (so that a broken code may still be read correctly), and many alternatives. Depending on their requirements, customers can select from a number of QR code image collections, including logo QR codes, scrambled QR codes, and iQR Code.

By X. Yan and Y. Lu, they applied the QR code to secure medical management:

Here, we'll show how a protected payment system with OR codes was planned and implemented. These OR codes are really very popular since they speed up the payment procedure and provide the customers a tonne of ease. Despite how beneficial it may appear, QR-based online payment systems are susceptible to a variety of attacks. This will ensure that exchange handling is sufficiently secure to protect each payment cycle's integrity and privacy. Also, the online payment system should provide authenticity to both the seller and the buyer in every transaction. Here, picture cryptography is used to demonstrate how secure the suggested QRbased architecture is. The app provides customers with a clear and simple interface that is easy to use in a safe environment.

Visible cryptography using the QR code and EVC:

These papers present a new Extended Visual Cryptography (EVC) and OR code-based security provisioning approach for online fraud detection. We can give individuals more security by employing this method. User must first register on the website for the proposed system. The customer transmits their ID and password to the bank server for validation. If it is, create a One Time Password (OTP) and use EVC to generate shares. One share is sent by the bank server to the client and one share is sent by the server [1]. Two shares are merged at the moment of rebuilding to produce the original OTP. The client then transmits this OTP to the bank server for validation.

METHODOLOGY

Visual data (pictures, text, etc.) can be encrypted using a technique called visual cryptography that enables human decryption without the need of computers. M. Naor and A. Shamir first discussed visual cryptography in their essay from 1994[6], which also featured their ideas for visual cryptographic solutions to the general k out of n secret sharing problem. Using a visual encryption technique, a secret picture is encoded into a number of shared images, which must then be decrypted to disclose the secret image [7]. Cryptographic techniques divide the secret image into a number of shareable pictures, which are then sent to other participants. The comprehensive theory of visual encryption states that the secret image is divided up into several shareable images by cryptographic procedures and delivered to other participants. The pixels in each image for sharing appear to be scattered at random [8]. By stacking enough shares, it is possible to decode data. The concealed picture will become visible if there are no complex calculations or replacement techniques, and the human visual system (HVS) may be used to decode it [7]. Therefore, no knowledge of intricate cryptographic techniques is needed for the encryption and decryption processes. Less shares accumulated than t will prevent the concealed image from being viewed. The (t, n) -VCS ((t, n)-threshold visual cryptography system) is the name given to this [9]. Consider the basic two-out-of-two visual threshold method, in which each image pixel is stored into a pair of subpixels in each of the two shares. If the pixel in Fig. 1 is white, one of the two columns tabulated underneath it is chosen. One of the two columns tabulated under the black pixel is chosen if it is black. Each time, the selection is made by

randomly tossing a fair coin, giving each column an equal chance of being picked. Next, share A and share B are allocated to the first two pairs of subpixels in the chosen column, respectively [10]. Consider the two shares superposed, as illustrated in the last row of Fig. 1.













Pixel	White		Black	
	50%	50%	50%	50%
Share A				
Share B				
Stack Share A&B				

FIGURE I. CONSTRUCTION OF A TWO-OUT-OF-TWOVC SCHEME: A SECRET PIXEL CAN BE ENCODED INTO TWO SUBPIXELS IN EACH OF THE TWO SHARES

Consider the fundamental two-out-of-two visual threshold approach, which stores each image pixel as a pair of subpixels in each of the two shares. One of the two columns tabulated beneath the pixel in Fig. I is picked if it is white. If a pixel is dark, one of the two columns displayed underneath it is selected. Every time, the choice is selected by tossing a fair coin at random, providing each column a same chance of being selected. The following step is to assign shares A and B to the first two pairs of subpixels in the selected column, respectively [10]. In the last row of Fig. 1, the two shares are shown superposed.

THE NEW SCHEME OF VISUAL CRYPTOGRAPHY ON THE QR CODE SECURITY

The secure QR code technique we employ will be explained in this section. In order to hide the QR code pattern and the data it contains, we provided an improved visual encryption approach based on the most recent visual encryption technology. In order to more securely achieve the aim of the hidden information, this encryption method makes it more difficult for counterfeiters to obtain the information disguised in QR codes. The QR code is generated from the original secret image using a special encryption method that generates two identical images utilising a pseudo-random matrix and visual cryptography. These are the steps.

- A. Collections of the C0 and C1 Encoding Matrix

The two sets of the Boolean encoding matrices C0 and C1, which, respectively, represent a white pixel and a black pixel of the original secret image
- B. Pseudo-Random Matrix Generation

Make a pseudo-random matrix of size equal to the range of the original secret picture, between 0 and 3, and with values equal to the basic matrices C0 and C1, respectively. The fundamental matrices in C0 and C1 are XORed with the all-1 matrix.
- C. Selecting the Basic Matrix

The pseudo-random matrix is involved while choosing the rule, and C0 or C1 is the basic matrix for the sharing picture.

 - a) The rule for creating the sharing picture A is as follows:

The position of each pixel (including white and black pixels) in the secret image is mapped to the corresponding position in the pseudo-random matrix, and the associated basic matrix is then chosen from C0 in accordance with the value in the pseudo-random matrix.

b) When generating the share image B, the rule is slightly different when white pixels and black pixels mapped to the pseudo-random matrix:

The procedure is as follows in the event of a white pixel: the white pixel's location in the secret picture is mapped to its corresponding location in the pseudo-random matrix, and the associated basic matrix is then chosen from the C0 in accordance with the value in the pseudo-random matrix. The following is the rule when dealing with a black pixel. The pseudo-random matrix is picked from C1 based on the value in the pseudorandom matrix, and the appropriate basic matrix is chosen according to the position of the black pixel in the hidden picture.

D. Hidden Picture Reconstructed

A white or black pixel from the original secret picture is represented by one sub-pixel in the reconstructed secret image.

$$C_0 = \left\{ \begin{matrix} \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} & \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} & \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \end{matrix} \right\}$$

$$C_1 = \left\{ \begin{matrix} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} & \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \end{matrix} \right\}$$

The principle of pixel superposition based on AND in this scheme is shown in Fig:2



























Pixel	White				Black			
								
Probability	25%	25%	25%	25%	25%	25%	25%	25%
Share A								
Share B								
Stack Share A&B								

FIGURE 3. CONSTRUCTION OF A TWO-OUT-OF-TWO SCHEME OF THIS PAPER: A SECRET PIXEL CAN BE ENCODED INTO TWO SUBPIXELS IN EACH OF THE TWO SHARES

The secret sharing images A and B are produced using this method, which uses a visual cryptography system based on the AND operation. Due to the nature of the process and the basics of the visual cypher, the two sharing images A and B may be used to recover the secret image. The sharing photos generated by this method are linked to the pseudo-random matrix. The pixels of Share image A are generated at random from the basic matrix, and the pixels of Share image B are also generated in the same way from the basic matrix. The attacker is unable to decode the data or access the secret information, even if they succeed in obtaining the basic matrix.

The stacked secret image has a lower contrast compared to the original hidden image. The original image's pixel that caused this behaviour was converted to a square matrix. This is normal and what was anticipated

from the experiment. The size of the shared photographs and the stacked hidden image were both four times larger than the original image. Moreover, replacing pixels is involved. Given that a pixel of the original image is replaced by a basic matrix of 4*4, the sharing photographs and the QR image after overlay recovery would be four times as large as the original hidden image.

PROPOSED SYSTEM DESIGN

The planned QR-based online payment system is described in this section. In the first sub-section, a functional description of the system will be provided, along with specific operational processes. In the second subsection, security issues are discussed after this. .

The Feature Description

In this research, the prospect of opening customer and merchant accounts was investigated. Consumer accounts have the capacity to receive and transfer credit, whilst merchant accounts can only accept money to further increase security. The architecture and operational flow of the proposed QR-based online payment system are depicted in Fig. 1. The cloud server, the customer, and the vendor are the three components that make up the system.

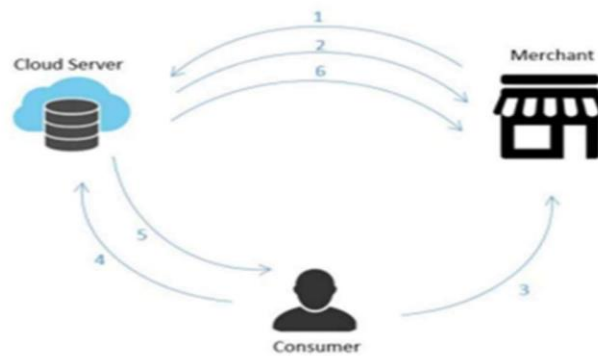


Fig. 4

The operational steps listed below illustrate how the three parties engage during a payment transaction:

- Step 1: is for the merchant to request a per-bill QR code from the cloud server.
- Step 2: The cloud server sends a QR code with built-in sharing.
- Step 3: To begin a transaction, the consumer scans the QR code.
- In step 4: The payment request is sent to the cloud server's backend system.
- Step 5: The cloud server completes the transaction and issues a confirmation number to the customer.
- step 6: The merchant is provided with the processing results for review Security Considerations.

The design incorporates the visual cryptography scheme (VCS) algorithm, which is used to secure user-touser transactions. It is built on a (2,2) VCS, where the original image must be shown by stacking two shares that are formed. Because the method is bidirectional, the input can be encrypted at one end and then decrypted at the other. Both the encryption and decryption of images, or QR codes, are carried out at the server's side for enhanced security and to obviate any possibility of manipulation at the client's end. The service begins when a merchant asks for a payment to start and specifies the expected amount. The application transfers one of the created shares to the merchant in the form of a QR code to be scanned after creating the customary QR code using the merchant data supplied by the server. The server will retain the other share. After the server scans the QR code, it will be prompted to buy the relevant twin share, combine

both shares, and finish the transaction. The procedure of creating two shadows from a QR code is shown on Fig. 2's left side, and it is shown on its right side when a QR code is scanned.



Fig. 5. (left) Construction of VCS and(right) Stacking of vcs.

SYSTEM IMPLEMENTATION

This system is computer-based. The only piece of hardware required to fulfil the activities and criteria was the user's mobile smartphone. An Android application is launched to function as a conduit between users and the server handling authentication and transaction processing. The application was developed in Java using Android Studio, an integrated development environment for Google's Android platform. The host machine linked to the local network and coded in Python serves as a payment gateway server for the mobile payment application. The server manages data in databases housed in a special memory space and responds to and handles requests from the mobile application. Fig. 3 displays the system's overall high-level functional implementation.



Fig. 6. High-level functional implementation of the proposed payment system.

RESULT ANALYSIS

Users of the payment system can swiftly and simply navigate the mobile application. It only acts as a communication channel between users and the payment gateway server. Users are classified as consumers or merchants throughout the registration process, which entails providing personal information that will be hashed and uploaded to the server. A user can make a QR code after logging in or scan and create a QR code depending on whether they are a customer or a merchant. A new user must provide personal information such as name, email, password, phone number, and whether they are a

consumer or a merchant on the registration screen, which is seen in Fig. 7. Depending on the sort of user they are, options like Create QR, Scan QR, and Check Balance are displayed on the home page when the user logs in. A consumer user's home page and a merchant user's home page are both displayed in Fig. 7. Once the user has chosen the Create QR Code option, the programme directs them to Fig. 8, where they must input the desired bill amount to start the payment process. A QR code containing the share is then sent back by the programme after making an attempt to contact the server. There is no userspecific information stored in the returned QR code.



Fig. 7. Registration page, Home page for merchant, and Home page for customer.

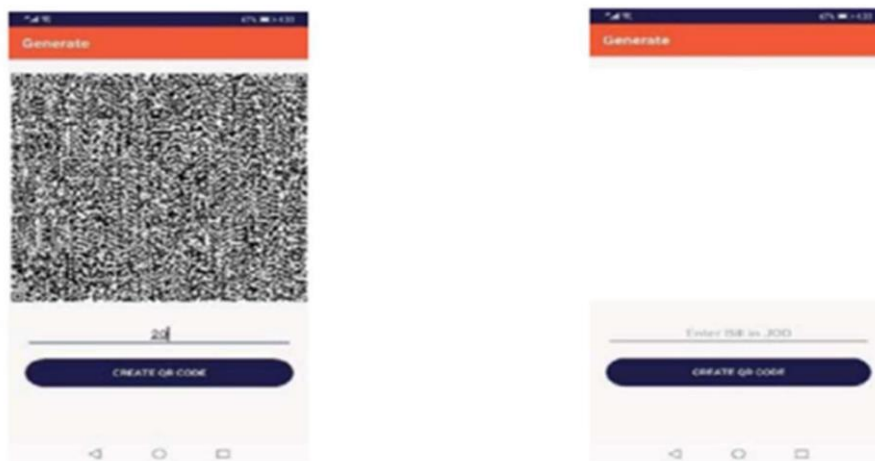


Fig. 8. 'Generate QR code' page with a requested amount of 20 JOD.

When a consumer chooses to pay a QR bill, the application is brought to the Scan page once the customer selects the Scan QR Code option. The scan sheet has a camera, as seen in Fig. 9. In order to have access to the phone's camera, the application must first receive permission from the user. After access is granted, the camera will instantly capture the QR code and transfer the scanned QR information to the server for processing. The bill amount and receiver of the funds are provided to the client as a confirmation box when the server has verified the transaction, giving them the option to accept or reject the payment.

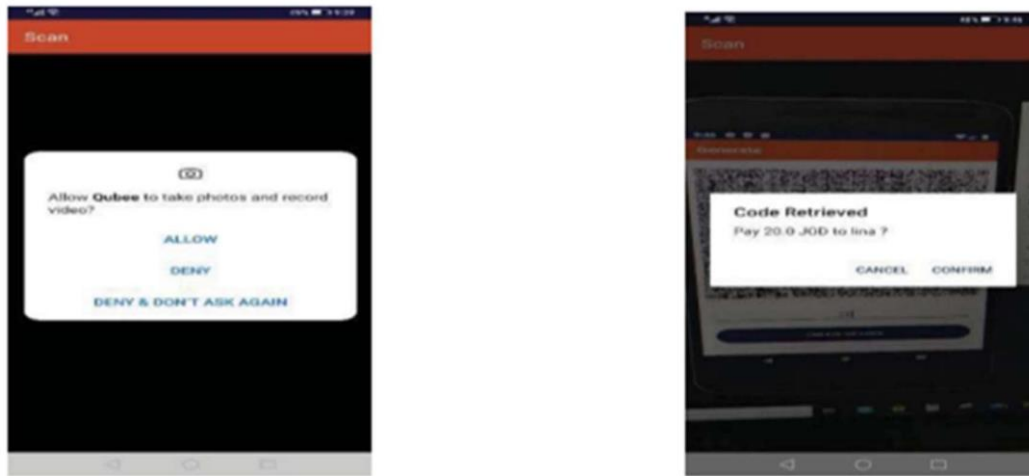


Fig. 9. Scan QR-code

CONCLUSION

In conclusion, the advancement of online payment technologies has greatly helped businesses and significantly raised consumer pleasure. Technical replacements are constantly looking for novel and creative ways to speedup, secure, and optimise the payment process because it is concealed from the user. The simplicity of online payment systems has also rendered them open to a variety of cyberattacks, thus mistakes must be accepted. These offences include data theft, denial of service, and fraud and forgeries. There have been several solutions proposed with differing degrees of sophistication to thwart these attacks. A safe QR-based online payment system has been suggested in this research. The suggested system's security is distinctive in that it uses visual cryptography to modify a single algorithm to deliver the necessary security services—confidentiality, integrity, and authentication. In the future, users will be able to generate static QR codes that are uniquely tied to their accounts thanks to a new function that will be added. The payee can enter the bill amount to be paid after reading such static QR codes, which do not provide balance information. Additionally, since the current program needs logging in each time the application is launched, sessions may be employed to keep users logged in for increased convenience. Last but not least, a security improvement to be made is the introduction of multithreading on the server to check for QR codes that have been saved for more than five minutes and destroy them.

REFERENCES

1. QR codes in library - Does anyone use them? - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Structure-and-components-of-QRcode-1_fig2_26142
2. M. F. Tretinjak, "The implementation of QR codes in the educational process," 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2015, pp. 833- 835.
3. S. Agrawal, "Impact of Error Filters on Shares in Halftone Visual Cryptography," International Conference on Computer Science, Engineering and Applications, 2012, pp.139-148
4. Z. Zhou, G. R. Arce, and G. D. Crescenzo. "Halftone visual cryptography." Image Processing, 2003 International Conference on IEEE, I-521-4.vol.1, 2003
5. P. S. Revenkar, A. Anjum, and W. Z. Gandhare, "Survey of Visual Cryptography Schemes," International Journal of Security & Its Applications 4.vol. 4, 2010

6. S. Tiwari, "An Introduction to QR Code Technology," 2016 International Conference on Information Technology (ICIT), Bhubaneswar, 2016, pp. 39-44.
7. M. Naor and A. Shamir, "Visual cryptography," Lecture Notes in Computer Science vol.950, 1994, pp.1-12
8. Kamal, Sawsan & Ameen, Basheer. (2016). A New Method for CIPHERING a Message Using QR Code. Computer Systems Science and Engineering. 6. 19-24.
9. L. P. Feng, et al. "A halftone visual cryptography schema using ordered dither," vol.9159, 2014, pp.4177-4180
10. Y.C. Hou , Z.Y. Quan , C.F. Tsai , D.S. Wang, "(3, n)-Visual Secret Sharing Scheme with Unexpanded Shares". Chinese Journal of Computers, vol.39, Mar 2016
11. S. Nseir, N. Hirzallah and M. Aqel, "A secure mobile payment system using QR code," 2013 5th International Conference on Computer Science and Information Technology, Amman, 2013, pp. 111-114
12. 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," 2015 International Conference on Network and Information Systems for Computers, Wuhan, 2015, pp. 435-440.
13. L. BURRA P. TUMULURU, S. GONABOINA "Secure QR-Pay System with CIPHERING Techniques in Mobile Devices", International Journal of Electronics and Computer Science Engineering, P.V.P. Siddhardha Institute of Technology, Kanuru, Vijayawada, Krishna, 2012
14. X. Yan and Y. Lu, "Applying QR Code to Secure Medical Management," 2018 9th International Conference on Information Technology in Medicine and Education (ITME), Hangzhou, 2018, pp. 5356.
15. W. C. Wu, "A QR Cod -Based on-Street Parking Fee Payment Mechanism," 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kitakyushu, 2014, pp. 106-109.
16. P. Zhang. Why QR code payment develop well in China? School of Computer Science, University of Birmingham.
17. Klein, Aaron (2019). "Is China's New Payment System the Future?" Brookings Institution Report,
18. Ju
19. 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, 2012.
20. Sangeeta Singh. May 2016. "QR Code Analysis" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 5, ISSN: 2277 128
21. Jianfeng Lu, Zaorang Yang, Lina Li, Wenqiang Yuan, Li Li, and ChinChen Chang, "Multiple Schemes for Mobile Payment Authentication Using QR Code and Visual Cryptography," Mobile Information Systems, vol. 2017, Article ID 4356038, 12 pages, 2017.
22. Yang, Ching-Nung & Liao, Jung-Kuo & Wu, Fu-Heng & Yamaguchi, Yasushi. (2016). "Developing Visual Cryptography for Authentication on Smartphones". 189-200. 10.1007/978-3-319-443508_19.