A QR Code Used for Personal Information Based on Multi-Layer Encryption System

https://doi.org/10.3991/ijim.v17i09.38777

Haroon Rashid Hammood Al Dallal[1](✉), Wijdan Noaman Marzoog Al Mukhtar[2]
[1] Department Infocommunication Technologies and Communication Systems, Saratov State Technical University, Saratov, Russia
[2] Department of Computer Engineering and Information Technology, Razi University, Kermanshah, Iran
haroonra1994@gmail.com

Abstract—Protecting and concealing sensitive data in the modern world is challenging. Due to insufficient protection and privacy, it is feasible for critical information to be fabricated. This led to a significant financial loss for someone. The intended recipient must be trusted with sensitive information and be able to independently authenticate the accuracy of the information by independently checking the specifics. There are several driving the rise in QR codes used for information transmission. Due to their enormous capacity for storing information, QR codes are vital for dissemination. However, most currently deployed QR code solutions employ insecure data formats and never employ encryption. Secure QR Code is data protection and data concealing available technology. The Quick Response (QR) code is widely used and accessible without extensive technical training. Now, the user data stored in a QR code is effectively public knowledge and occasionally even illegally used. To address the abovementioned issues, this study's authors propose a novel QR code encryption system. Using the image's mathematical processing method, we may apply the equivalence class principle to the ordered equations of the two-dimensional code, producing the desired cryptographic result. This method exploits the unique visual properties of the QR code. Only a QR code reader can decode the code's useful information, which is too complex for standard reading methods. It will be utilised to address issues in speedy business client data protection Security, commodity anticounterfeiting, and bicycle sharing QR codes.

Keywords—QR code, privacy protection, multi-directional identity authentication, encryption system, image symmetrical processing, data processing

1 Introduction

With the growth of the Internet, 4G/5G technology, and business, among other aspects, smartphones have become an integral part of life for many customers. Additionally, an increasing number of people are deciding to travel abroad for vacations and are doing so by making hotel reservations online. It serves a purpose by speeding up the check-in procedure at the front desk, but it also carries a risk because some information and personal privacy may be made public[1-3]. There is a greater risk of disclosure because the individual now handles sensitive personal data manually and insecurely. Experts have recommended employing TTJSA and the Advanced Encryption Standard (AES) to obfuscate information and messages in court documents [4-6]. QR barcodes, also known as two-dimensional codes (QR codes), are a type of matrix barcode that uses a black-and-white pattern to encode symbolic data and is dispersed along a lane (the QR direction) using a specific geometry [7]. The system's foundation rests on the binary number system of "0" and "1," and numerous geometric objects with direct correspondence to binary systems are utilised to represent numerical data in the text [8].

Automated processing of data is possible with the help of a picture transmitter or a photographic scanning machine. Its high density, vast capacity, and other features make it suitable for usage as a symbol for the number. Evidence from print (including Chinese character files), visual, and other media suggests that QR codes are among the most useful methods for connecting the physical and digital worlds [9].

2 Literature review

In the early nineties, the Japanese automobile industry was the target market for the invention of the QR code. Comparable to barcodes, which use two-dimensional codes to record data about the object they are connected to or related to QR codes are essentially visual identifiers by the computer. To store information effectively, a QR code uses four specified coding modes, including numeric, alphanumeric, byte/binary, and kanji (a subset of Chinese characters used in the Japanese language)[10].

Numerous studies on the data hiding technology of QR codes are now being conducted. But both nationally and internationally, the majority of techniques involve encrypting and altering the raw data using cryptographic techniques or analyzing and identifying a massive number of secret keys [7, 11]. The former is not very portable.

In the transport industry, individual privacy leakage is a serious issue right now. Large-scale sales are being made of sensitive information from the logistical waybill, including name, address, mobile number, and other details. Fraudsters have access to a lot of private details, which gives them the chance to steal identities and commit fraud. Numerous receivers whose data is compromised incur serious consequences. They can suffer the abuse of useless knowledge or experience fraud [12, 13].

In the study by Dudheria,[14], the available Android secure QR code readers are examined, their security protocols are highlighted, and their effectiveness at spotting malware Or malicious codes is assessed. Numerous QR code readers make the claims to be safe scanners, although investigation shows that this is not the case and that they need to be improved. The paper discusses the potential flaws and restrictions of safe scanning applications and offers suggestions to raise the level of security. Unfortunately, the usability of barcode scanners is not taken into account in this study [15].

The cryptographic algorithms of the top 31 Android QR code scanners are examined in the literature by Yao and Shin [16]. Only 2 out of 31 applications offer security alert features, however, extensive testing reveals that phishing and infection threat detection techniques are relatively unreliable. To address this, the researchers suggest SafeQR, a new QR code reader that relies on two already-existing security APIs: Google safe browsing and Phishtank (Google, site; Phishtank, site). The ability of the scanning to increase the rate at which malicious URLs are discovered is not, unfortunately, supported by any actual data provided by the authors [17].

The authors Wahsheh al., [17] provide a thorough review of the security and privacy concerns relating to QR codes. The data gathered indicate that the majority of reader applications are unable to identify fraudulent URLs. Additionally, by requesting additional rights and obtaining users' private information, these apps breach users' privacy. The study offers design suggestions for practical and safe reader applications and suggests a model that uses URL checking and Base64 digital signatures. Results demonstrate that users can be adequately shielded from malicious QR codes byllowing to the design suggestions[17]. Numerous ways to prevent QR code scamming assaults have been suggested; nonetheless, the threat is growing and phishing is now a prevalent method of committing cybercrime [15].

This study develops a plan to protect consumer privacy utilizing RFID technology and multi-layer cryptographic functions. It uses the protection of user private information in the express logistics industry as its primary research object. The plan can accomplish a dual level of confidentiality for the logistics firm's internal and external customers and it can also guarantee that the person in charge of disclosing personal information will be subject to review [12].

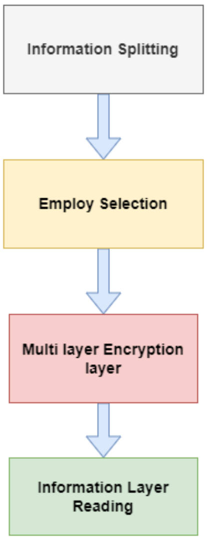


Fig. 1. Express delivery facility procedure of logistics business

A QR code phishing detection was suggested by Yao and Shin [16]. They did this by leveraging Google Safe browsing and Phish Tank, two APIs. The research-based solution is superior in terms of user usability and sincere manipulation table, there is no recognition rate, and TP, TN, FP, and FN are mentioned. There is no developed QR code phishing dataset [16].

Ishihara suggested a temperament detecting system. Work that was not done mainly focuses on QR code production and ignores digital detection system solutions and uses encryption without taking 2014 detect signature and wet usability into account. The content modifications for QR codes [18].

In this study, the researchers suggest a networked hospital management system called CoviReader that securely distributes user data. The IOTA is used to build the application for the users with access to the tangle platform and detailed, immutable, and quick access to their private data. CoviReader manages data, availability of the data, security, and authentication (With important factors to take into account when updating confidential Users engage with IOTA's tangle through a mobile device to exchange data. an application that houses a FIREBASE database. The objective of This brief paper will present a functional prototype for evaluating and examining methods for lessening the effects of the health emergency caused by COVID-19 [19, 20]. Modulation and simulations in OPNET have been used in this research to examine a cloud computing model of a distribution network. By using the experiment, the model is looking into cloud computing to see how well it can be used as a framework for combining satellite communications, data management, and systems for establishing and maintaining human trust. The development of a multiple supply chain architecture will be modelled, with the modeling approach demanding the combination of data and communications as well as the establishment of human trust and integrity through the developing idea of building trust in multiparty sessions. The OPNET Simulation tool has already been used to generate an early model, and the preliminary findings have been carefully examined. The goals and objectives for this paper have been established thanks to this initial project, which has also assisted in building confidence in designing the much bigger structure of supply chains [21]. The research also doesn't account for the offline risks that come with QR codes, such as SQL and command injections, privacy worries, and usability problems. A bit of string is carried by a QR code, which then transports the string to a database where the information is encrypted. This is the current commercial architecture for such services in the domestic market. The user side, or first-level user, is the only one capable of reading the QR code and deciphering the string. The secondary user, or business side, utilises the URL to access the information database. Encrypting the user's information is achieved by utilising the user's personal information. Said this approach does not encrypt any information. For as long as the database is available, this means that all user information is, in fact, completely public. Multiple types of personal information have been hacked, exposing a serious system security flaw. A novel encryption method is presented in this research. The information included in a QR code image is cut up using the bite rule and the Attribute principle to create a camouflage QR code, which a data reader reads. Key matching can be used to decrypt data encrypted by Terminal and restore it to its original state. If the secret key is to be believed, No matter if the key is private or public, the value of the key determines how the QR code is broken into blocks. The segment's effects are then determined and a baseline for future comparison. One technique to secure a secret key is a paper wallet, simply a piece of paper printed with the private key and a QR code so that the transaction may be completed quickly by scanning the paper.

Each group of rectangles assigned the same value consists of four blocks. The size of the segmented m-block isometric quadrilateral is determined by the distance between its location and the circle of the analogous point. The Attribute principle describes this. Whether you're left- or right-handed, the squares will trade positions to form a different picture.

The scanning process for two-dimensional codes is omitted from the two-dimensional code computing method, which uses the image feature instead. Information is safe, and cryptographic processing times are reduced.

3 Method & data

3.1 Basic structure of QR code

2D barcode is another name for a QR code. Quick Response is the full title of the widely used QR code or QR code.

Fig. 2. Simple QR code

In recent years, smartphones have increasingly used this encoding technique. Compared to the conventional barcode, it can save more Additional data categories can be indicated via information.

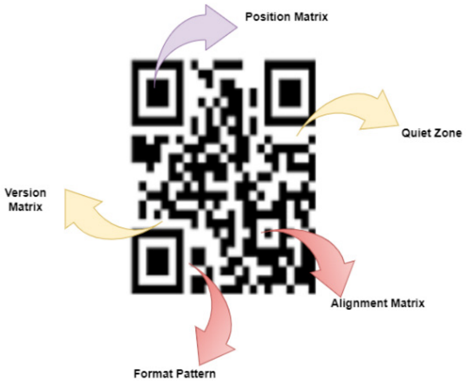


Fig. 3. "Basic Structure of QR code which is Black & White"

A carefully coded black-and-white image known as a QR code stores data symbol information in a plane (two-dimensional direction) using a certain geometric pattern. The textual mathematical information is represented using a variety of geometric forms that relate to the 1s and 0s, using the idea of "0" and "1" bit which is machine language composing the logic of the inside logic of the computer, which are used to read the image automatically, input method or the photoelectric scanning device. information processing automatically: It shares several characteristics with bar code technology, such as the distinct character sets and check functions that are unique to each coding system. The QR code is created using the pre-propagating data, inserted in the classification frame, and then an image frame is acquired. The grayscale and median filters used in image preprocessing are applied, and the positive rectangular image is created by identifying the location point. The coding algorithm generates the rectangular picture that is disguised. accomplish the encryption of the QR code. The encrypted, disguised QR code picture is placed straight into the recognition frame, where it undergoes " grayscale, median filtering " and other image preprocessing procedures. The decoding algorithm is equivalent to the recognition coding algorithm processes used to disguise the image.

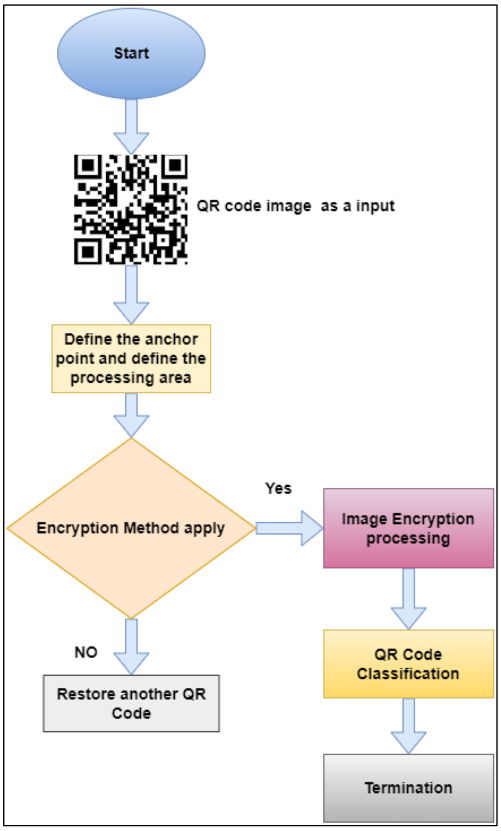


Fig. 4. Flow Chart of Encryption Algorithms

Method. It is used to identify and identify the local secret key. Following the correspondence of the secret key, the decrypting mode is retrieved and transmitted to the image verification unit to decipher the QR code's upper application logic. According to the findings of this study, the primary QR code area can be divided into equal-sized blocks. The QR code's mapping from analogous points is calculated using these blocks. Recalibration by 2n assignment is a method employed by some protocols, and it is based on the circle distance between the position and effects of the (B) block equip rod quadrilateral. For every group of four identical quadrilaterals, there are eight cubes. As a means of ushering in a new era, the equal rectangle is flipped from its traditional orientation.

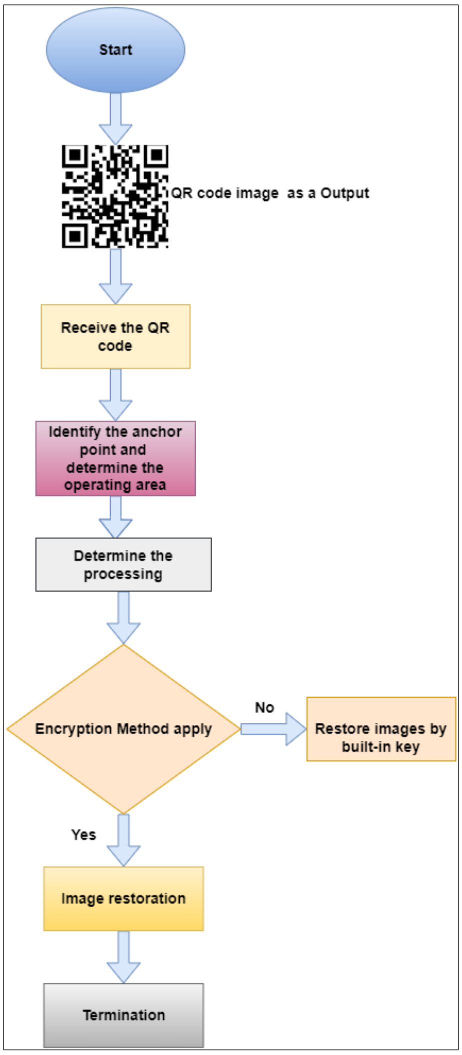
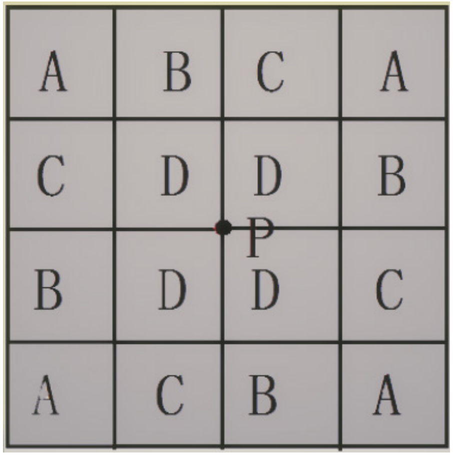

Start
QR code image as a Output
Receive the QR code
Identify the anchor point and determine the operating area
Determine the processing
Encryption Method apply
No
Restore images by built-in key
Yes
Image restoration
Termination

Fig. 5. Flow chart of signal frequency spectrogram

4 Analysis and results

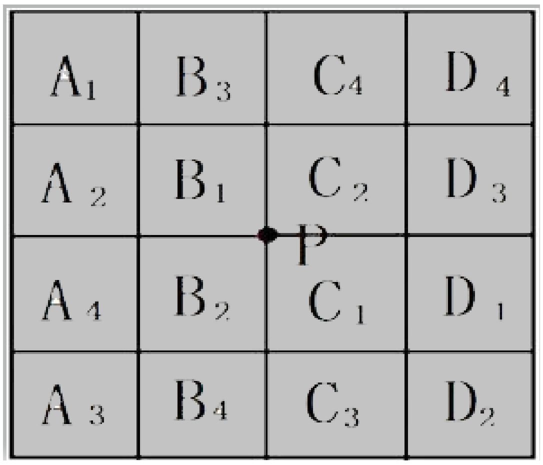
The technique recognition libraries are used to obtain the decoding mode that corresponds to the encrypting mode of the secret image and match the classification key with the encryption key.



A	B	C	A
C	D	D	B
B	D	D	C
A	C	B	A

Fig. 6. The sub sub-bandana rate of the spectrogram

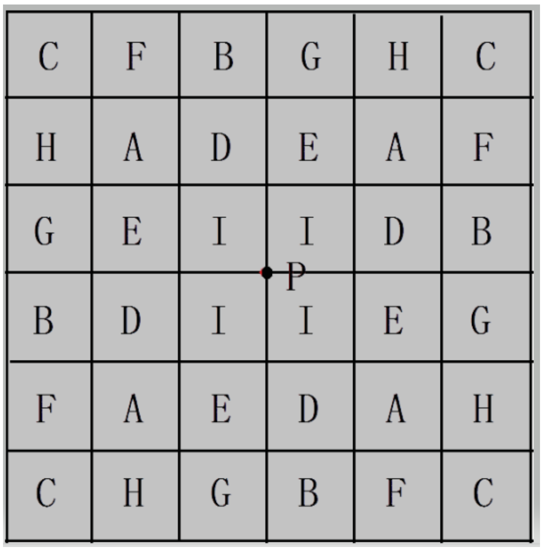
In Figure 5, the mathematical formulation used to explain this concept is displayed, and a method of a standard contains is used. The center of the graph is P, and the letters "A, B, C, and D" each occupy four squares; the position of each letter is similar but unique. A, B, C, and D could be randomly selected for data encryption, but various selection process is required to create disguise images. The image is divided into a 4 h 4 matrix in Figure 5, and there are 256 different encryption algorithms available.



A_1	B_3	C_4	D_4
A_2	B_1	C_2	D_3
A_4	B_2	C_1	D_1
A_3	B_4	C_3	D_2

Fig. 7. The result of Equivalence class principle 4X4

For each extra row in the matrix, the number of possible schemes grows exponentially. For instance, as demonstrated in Figure 7, when the image is split into six h6 matrix, the matrices of encryption techniques rise to 4096. Splitting choice into 2 different codes is as easy as a two-value image and tends to infinite. If the computer tries to be decrypted using statistical breaking, the computations will be extremely big. It will be quite challenging to attempt to decrypt the image using a computer.



C	F	B	G	H	C
H	A	D	E	A	F
G	E	I	I	D	B
B	D	I	I	E	G
F	A	E	D	A	H
C	H	G	B	F	C

Fig. 8. Extension of Correspondence class value

The four clusters of "A1-A4, B1-B4, C1-C4 " and D1-D4 are, accordingly, comparable at the picture level, based on the Class Label Principle. A1, B3, C4, and D4 are identified as the multiple user variations among A1-A4, B1-B4, C1-C4, and D1-D4.

Each zone is reorganized in the sequence of scanning, as indicated in Figure 6 ,The D4 section is used for reading, and a guideline says it should be read aloud four times (often left- or right-handed). The number of unmerged images can be increased if the image units are only completely joined by using the simple square combining.

123456

Fig. 9. The data acquired by scanning a sample QR code

$$m \square (m \square 1) \square (2m \square 1) \tag{1}$$

Equation number one is used to show the rectangular edge unit value that greatly enhances the cost of the violation.

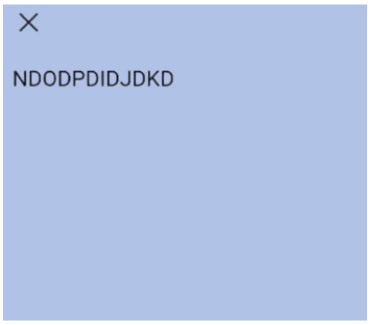
Image synthesis analysis can be used to produce multi-layer decryption, and key matching can be used to retrieve encryption information for QR codes. The QR code image can be encrypted multiple times using the built-in private key; if it is the initial layer of encryption, the area will be split immediately.

The QR code information is recovered using the appropriate decoding technique. The area of multi-layer disorder is identified if there is multi-layer cryptography. The local disorder is initially repaired in the appropriate decoding mode, and only then is the general restoration carried out.

The two-dimensional code encryption system is split into two sections during the actual application process: the producing end and the recognizing end. The two-D- code that needs to be transmitted must be disguised and encrypted by the producing end, and the recognizing end is in charge of decrypting the encrypted 2 D- code2-Dd restoring the 2-D-dimensional code image using the private or public key that was originally established. It is important to create an algorithm database in preparation, find keys that belong to users of various terminals, and finish decoding by system key matching in order tosh the abovementioned activities.

5 Discussion

As seen in Figure 2, a technique is used to create a disguised QR code using the sample information "123456." When you scan the QR code, the incorrect information is displayed, and the interface shown in Figure 8 appears. QR code and read the correct information that are shown the simple issshown3456.



NDODPDIDJDKD

Fig. 10. Restore the Qr information

6 Conclusion

In this research paper, a unique QR code cryptography based on the national standard code system is presented and implemented. The combination of image geometric processing with information encryption using QR codes is a novel and useful approach that has a significant impact and great practical value.

The need of user needs the algorithm's encryption level can be adjusted flexibly. The basic flexibility is that the two-dimension codes could only include real information that can be read by a specialized scan monitoring system, while the conventional reading system can only read the data that has been camouflaged. The technique is intelligent, full of variance, and to the maximum capacity matches the variety and non-repeatability of encryption techniques. With the advancement of the QR code technique, it can be expanded as secondary processing based on the technology. This study introduces a new method for using QR codes and the information they convey. It is possible to obfuscate the encryption process to implement multi-layer encryption, increase the size of the method library, use more advanced methods, and make decoding more difficult. How the decoding of picture attributes impacts the covert transmission of data with QR codes is a topic we intend to explore further. Second, we plan to increase the QR code encryption system's functionality by extending it at the application level, creating the necessary mobile operating system, and employing cell phones as the identifying end. Additionally, we plan to incorporate local physical data into the next round of development. If the recognition end can receive the secret key through physical information matching rather than the built-in key, it can reduce the production cost and technological barrier.

7 References

[1] R. E. Crossler, J. H. Long, T. M. Loraas, and B. S. Trinkle, "Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap," *Journal of Information Systems,* vol. 28, no. 1, pp. 209-226, 2014. https://doi.org/10.2308/isys-50704

[2] H. T. Hazim, "Secure Chaos of 5G Wireless Communication System Based on IOT Applications," *International Journal of Online & Biomedical Engineering,* vol. 18, no. 12, 2022. https://doi.org/10.3991/ijoe.v18i12.33817

[3] S. Dey, S. Agarwal, and A. Nath, "Confidential encrypted data hiding and retrieval using qr authentication system," in *2013 International Conference on Communication Systems and Network Technologies*, 2013: IEEE, pp. 512-517. https://doi.org/10.1109/CSNT.2013.112

[4] H. A. Hassan, "Review Vehicular Ad hoc Networks Security Challenges and Future Technology," *Wasit Journal of Computer and Mathematics Science,* vol. 1, no. 3, 2022.

[5] R. Mohamad, "Data hiding by using AES Algorithm: Data hiding by using AES Algorithm," *Wasit Journal of Computer and Mathematics Sciences,* vol. 1, no. 4, pp. 112-119, 2022.

[6] H. T. Hazim, "Enhanced Data Security of Communication System using Combined Encryption and Steganography," *International Journal of Interactive Mobile Technologies,* vol. 15, no. 16, pp. 144-157, 2021. https://doi.org/10.3991/ijim.v15i16.24557

[7] M. Xu, L. Lv, J. Zhang, M. Xu, C. Zhang, and J. Zhang, "A New QR Code Multi-layer Encryption System based on Image Geometric Processing," in *2019 IEEE International*

Conference on Mechatronics and Automation (ICMA), 2019: IEEE, pp. 1-5. https://doi.org/10.1109/ICMA.2019.8816462

[8] M. A. Khalifa, A. M. Ali, S. A. Alsadai, N. F. Alwan, and G. S. Mahdi, "A Novel Arabic Words Recognition System Using Hyperplane Classifier," *Wasit Journal of Computer and Mathematics Sciences,* vol. 1, no. 2, pp. 12-20, 2022.

[9] Y. Gu and W. Zhang, "QR code recognition based on image processing," in *international conference on information science and technology*, 2011: IEEE, pp. 733-736.

[10] J. Yang, Y. Zhang, and C. J. Lanting, "Exploring the impact of QR codes in authentication protection: A study based on PMT and TPB," *Wireless Personal Communications,* vol. 96, no. 4, pp. 5315-5334, 2017. https://doi.org/10.1007/s11277-016-3743-5

[11] L. Gong, Q. Zhu, Z. Zhou, and N. Zhou, "Comprehensive design experiment for digital image processing based on Matlab," *Experimental Technology and Management,* vol. 35, no. 11, pp. 48-53, 2018. https://doi.org/10.1201/9781351069205-2

[12] H. Feng, "Application of QR Code Technology in the Design of User Information Privacy Protection Logistics System," *International Journal of Frontiers in Engineering Technology,* vol. 3, no. 3, 2021. https://doi.org/10.25236/IJFET.2021.030302

[13] A. S. Hussein, R. S. Khairy, S. M. M. Najeeb, and H. T. ALRikabi, "Credit Card Fraud Detection Using Fuzzy Rough Nearest Neighbor and Sequential Minimal Optimization with Logistic Regression," *International Journal of Interactive Mobile Technologies,* vol. 15, no. 5, 2021. https://doi.org/10.3991/ijim.v15i05.17173

[14] R. Dudheria, "Evaluating features and effectiveness of secure QR code scanners," in *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 2017: IEEE, pp. 40-49. https://doi.org/10.1109/CyberC.2017.23

[15] S. Subairu, J. Alhassan, S. Abdulhamid, and J. Ojeniyi, "A Review of Detection Methodologies for Quick Response code Phishing Attacks," in *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*, 2020: IEEE, pp. 1-5. https://doi.org/10.1109/ICCIS49240.2020.9257687

[16] H. Yao and D. Shin, "Towards preventing qr code based attacks on android phone using security warnings," in *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*, 2013, pp. 341-346. https://doi.org/10.1145/2484313.2484357

[17] H. A. Wahsheh and F. L. Luccio, "Evaluating Security, Privacy and Usability Features of QR Code Readers," in *ICISSP*, 2019, pp. 266-273. https://doi.org/10.5220/0007346202–660273

[18] T. Ishihara and M. Niimi, "Compatible 2D-code Having tamper detection system with QR-code," in *2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2014: IEEE, pp. 493-496. https://doi.org/10.1109/IIH-MSP.2014.129

[19] B. Cisneros, J. Ye, C. H. Park, and Y. Kim, "CoviReader: using IOTA and QR code technology to control epidemic diseases across the us," in *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, 2021: IEEE, pp. 0610-0618. https://doi.org/10.1109/CCWC51732.2021.9376093

[20] A. Al-zubidi, R. K. Hasoun, and S. H. Hashim, , "Mobile Application to Detect Covid-19 pandemic by using Classification Techniques: Proposed System," *International Journal of Interactive Mobile Technologies,* vol. 15, no. 16, pp. 34-51, 2021. https://doi.org/10.3991/ijim.v15i16.24195

[21] G. Tulemissova, I. Bukenova, and A. Korzhaspayev, "Sharing of teaching staff information via QR-code usage," in *Proceedings of The 10th European Conference on Information Systems Management*, 2016, p. 195.

8 Authors

Haroon Rashid Hammood Al Dallal, Bachelor's degree, Department Engineering in Communication Techniques, Al-Furat Al-Awsat Technical University, Najaf, Iraq. Master's degree, Department Infocommunication Technologies and Communication Systems, Saratov State Technical University, Saratov, Russia (email: haroonra1994@gmail.com).

Wijdan Noaman Marzoog Al Mukhtar, Bachelor's degree, Department Computer Science College of Science for Women, University of Babylon, Babylon, Iraq. Master's degree, Department of Computer Engineering and Information Technology, Razi University, Kermanshah, Iran (email: wijdanalmokhtar@gmail.com).

Wijdan Noaman Marzoog is an Assistant Lecturer at the University of Babylon / Faculty of Science for Women. I teach computer subject for the first and second stages in the Department of Life Sciences.

Article submitted 2023-02-01. Resubmitted 2023-03-27. Final acceptance 2023-03-29. Final version published as submitted by the authors.