INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

OPEN ACCESS
Received: 31-07-2024
Accepted: 21-10-2024
Published: 26-02-2025

Citation: Wosu JT, Chukwudebe GA, Agubor CK, Ezema LS, Nwanga ME (2025) A Novel Quick Response Code Generator and Scanning System for Counterfeit Product Detection Using Product Inherent Features. Indian Journal of Science and Technology 18(7): 539-549. https://doi.org/10.17485/IJST/v18i7.2455

* **Corresponding author**.

longinus.ezema@futo.edu.ng

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

A Novel Quick Response Code Generator and Scanning System for Counterfeit Product Detection Using Product Inherent Features

Jeremiah T Wosu[1], Gloria A Chukwudebe[2], Cosmas K Agubor[2], Longinus S Ezema[2]*, Mathew E Nwanga[3]

1 PhD. Student, Department of Electrical and Electronic Engineering, Federal University of Technology, Owerri, Nigeria
2 Professor, Department of Electrical and Electronic Engineering, Federal University of Technology, Owerri, Nigeria
3 Lecturer, Department of Information Technology, Federal University of Technology, Owerri, Nigeria

Abstract

Objectives: The study aims to build trust in the relationships between producers, distributors, retailers, and final consumers in society by reducing product counterfeiting to the barest minimum. **Methods**: This study presents the use of a Quick Response (QR) Code Generator (QRCG) to store the fundamental manufacturing features of a product and for quick and accurate verification of originality on validation. The quickness and efficiency of the developed system were verified using the speed of execution and the probability of obtaining the wrong result or the detection accuracy. Object-oriented systems modeling was adopted alongside the Rapid Unified Process (RUP) software development approach in designing the novel QR code generator. **Findings:** The Novel QRCG demonstrated good performance as it comprehensively captures the prime features of singular products and readily validates their originality concerning speed and accuracy when a product is subjected to it to verify originality and detect counterfeits. The execution speed was virtually constant as it lies between 9ms - 10ms with zero probability of obtaining a wrong result on scanning a product. **Novelty:** A Novel QR code generator and scanning system for detecting product counterfeits using the product's inherent features is presented. To enhance the security of the QR code, an intrinsic feature of the product and a Copy Sensitive Graphical Code (CSGC) is inserted into the QR code.

Keywords: Counterfeit Product Detection; QR Code; QR Code Generator; Product Inherent Features; Product Originality Verification; Scanning System

1 Introduction

In today's market, dealing with counterfeit products is a major threat facing consumers, businesses, and regulatory government agencies. Detecting counterfeit/fake products is an intriguing task that requires efficient and innovative technology. One of the promising and innovative technologies is the integration of QR codes and product packaging. This enables the consumers to scan the generated QR code embedded in the product package to verify the product's authenticity. This simple, efficient, and cost-effective approach has been deployed by various researchers with varying degrees of success[1,2].

The authors in[3] proposed a new technique of protected QR codes to ensure that the unique product information code for protecting the product supply chain is well secured from counterfeiters. The proposed approach developed a data-encrypted transmission technique for the generated QR code to establish an anti-counterfeit scheme. This approach ensures that the protected QR product information can not be replicated and tampered with.

The application of blockchain technology in the development of an 'Anti-Counterfeit Detection System' is developed in[4]. With emphasis on blockchain which is a decentralized ledger platform that facilitates security by ensuring that transactions are immutable. However, the proposed solution in this work did not account for certain intricate features of the products such as texture, size, and weight. Rather, the focus was centered on the components of the blockchain technology used which included the Ethereum blockchain, the smart contracts that were driven by the solidity code, and the code execution.

The research by[5] proposed Counterfeit Product detection in e-commerce. In this work, the focus was to generate a QR code using blockchain technology which is attached to the products at the manufacturer's point. Although the work referred to the use of web-based applications (which run on blockchain technology), the specification of how the QR code is to be generated was not captured. Furthermore, the project suggested the attachment of RFID tags on products which will aid the verification of the authenticity of a product by using specific information on a product.

Counterfeit product detection using frequent pattern mining is the approach adopted in[6]. The authors gave attention to product traceability - which is the ability to track and trace individual items throughout their life cycle from manufacturing to recycling. The project then proposed a standardized traceability system architecture in implementing a product detection algorithm. Although the system was not implemented, the proposed algorithm was subjected to simulation, and data generated were used to identify genuine trajectories across the life cycle. The genuine product trajectories were then subjected to analysis using a frequent pattern mining algorithm. The identified trajectories were used as a reference point to identify counterfeit products.

A novel QR code named the nested QR code is presented in[7]. It consists of two different QR codes which are separated by a shared square image. By modifying the length and angle at which pictures are captured, it is possible to read both QR codes separately. Implementation techniques for producing the proposed nested QR code with high decoding robustness were presented, and experimental results verified the feasibility of the proposed method.

In[8], an efficient technique for bar code and QR code recognition together was presented. The technique detects the Bar code QR code automatically and shows the comprehensive details of the product. The real-time capture of the QR code image was further processed using the developed technique. The captured and decoded code was compared with the stored product data frame and the displayed result will either be a match or a mismatch. The developed technique executes this process within 0.25 seconds.

A unique color QR code that integrates different types of identification information is proposed in[9]. This code adopts multiplexing and colour-coding technique to display the publicly encoded information as plain code, and traceability, blockchain, anti-counterfeiting authentication and other information concealed in the form of hidden code. The experimental results show that the color quick response code realizes the multi-code integration and can be read directly without special scanning equipment, which has unique advantages in the field of printing anti-counterfeiting labels.

The study by[10] proposed a three-level QR code scheme based on super-pixel segmentation in response. Employing a good QR code scanner, public information can be scanned directly from shares. Furthermore, confidential data can only be obtained by the difference in the shares. The key picture in this work is the reorganized confidential picture and the mechanism is repellent to destructive changes, weight, and stress because it maintains the benefits of visual ciphers and QR codes. Results obtained from various tests reveal that this approach has several improvements over others.

The work by[11] demonstrated optimized modulation and coding for dual modulated QR (DMQR) codes that increased state-of-the-art QR codes to accommodate more information in the arrangement of thumbnail blotches that substituted black clusters in the barcode image. Moreover, the work designed an approach for the programming axis for more information that allows easy decoding through 5G NR (new radio) codes. Comprehensive tests were carried out on the developed system to ascertain its performance of the system. Interestingly, the developed system's capacity to make good use of DMQR codes is easily accessible QR code beautification that creates space on a little part of the barcode image area for a logo or image to be interposed. The system was tested with a capture distance of 15 inches, and it was observed that the decoding success rates improved to about 10% and 32% for the additional information, which also resulted in an improvement in the root information captured at far distances.

The approach for identifying counterfeit and duplicate products presented in [12] proposed the use of a quick response code (QR code), which is safe and efficient. The QR code is almost impossible to decode or duplicate. The method was executed using blockchain technology to ensure that the generated QR code is tamper-free. This approach against counterfeiting is far more cost-effective than conventional techniques such as Radio-Frequency Identification (RFID) and the Hologram technique.

In the works reviewed thus far, it is evident that the product's inherent feature was not considered which characterizes a product as a means of curbing counterfeiting across the supply chain - right from the manufacturing point, through the distributor's stocks, to the end users. The majority of the reviewed work did not utilize Copy Sensitive QR codes (CSQRC) nor did they consider the integrity and authenticity of the data transmission. Existing blockchain-based systems do not make use of efficient consensus algorithms. None of the existing systems utilized location information i.e., GPS coordinates in combination with blockchain technology. Furthermore, none of the works adopted an object-oriented systems analysis and design approach in modeling or/and implementing the reviewed work.

This work adopted an object-oriented systems modeling approach, alongside the Rapid Unified Process (RUP) software development pattern, in designing a novel QR code generator and scanning system which is based on the capture of the inherent features of a product such as the texture, weight, size, etc., as well as other manufacturing details as the criteria upon which the originality of a product is ascertained. To generate the QR Codes, the following parameters were used; mfd ID, password, name, address, longitude, latitude, login (Mfd ID, Password), prodTexture, name, weight, dimension, batchNum, productionDate, expiryDate, ownershipStatus and the product inherent feature which in this case is product texture. To enhance the security of the QR code, an inherent feature of the product and a copy of Sensitive Graphical Codes (CSGC) is inserted into it and a blockchain system is developed to further enhance the security. While other researchers have adopted various features such as manufacturer's ID, Batch number, production date, and expiry date among others, none have tried to incorporate product texture in generating QR Codes. The texture of the original product can never be the same as the fake product and cannot be copied. The inherent features of a product are imperative as it's impossible to counterfeit or fake it and the QR code can not be duplicated unless one has access to the company's copy of its embedded content which in this case is the product's inherent features and the manufacturing details.

2 Methodology

In this work, object-oriented system analysis and design utilizing Unified Model Language (UML) tools and Rapid Unified Process (RUP) software engineering procedure are adopted as the methodological approach in implementing the QR Generator and Scanner System. This system combines a novel product's inherent features, copy-sensitive QR Code, location information, and track and trace technologies. It utilizes a method of detecting counterfeit by capturing inherent features indissolubly linked with the product induced by the production process itself. The specific conditions of production, manufacturing technologies, and materials generate specific features that identify the product uniquely. Since counterfeiters gain margin by the use of inferior production processes and materials, the difference between genuine products and counterfeit can be captured from these inherent features in an automated fashion.

Copy-sensitive QR code is employed by the system to detect counterfeit products. To enhance the security of the QR code, an inherent feature of the product and a copy of Sensitive Graphical Codes (CSGC) is inserted into it. The detection of counterfeits using CSGC relies on an "information loss principle", which states that every time a digital image is printed or scanned, some information is lost about the original digital image. A CSGC is a maximum entropy image that attempts to take advantage of this information loss. Since producing a counterfeit CSGC requires additional scanning and printing processes, it will have less information than an original CSGC. By measuring the information in the scanned CSGC, the detector can determine whether the CSGC is an original or a copy. Additionally, each printer or scanner has its own signature. Using these two technologies, the authentication test can distinguish the original CSGC (printed once) from copied/counterfeited (printed several times). The system representation includes use cases, a tabular presentation of major entities, data, and operations as well as a conceptual class diagram, use case diagram, and activity diagram.

2.1 Use Cases

Considering the nature of the system, the functional requirement of this system will be to:

1. Accurately capture the manufacturing/product detail of a product at the production point,
2. Process the captured information and store it in a QR Code format (QR Code generation), and

3. Authenticate product authenticity by scanning the QR code and comparing it with the list of genuine products QR code (QR Code scanning).

Based on the outlined functional requirements of the system, the captured use cases are shown in Table 1 and Table 2.

Table 1. QR code generation for the system

#1 **Name:** Generate QR Code	
Brief description: This use case presents the operational execution of events that lead to the generation of a QR Code of a genuine product by a manufacturer on registering the product to the system.	
Primary Actor: Manufacturer.	
Precondition:	The manufacturer has successfully logged on to use the system using some data as required by the system. The scanner is ready to capture product data.
Trigger	The manufacturer presents the genuine product to the scanner.
Main Flow	
1) The system captures the texture, size, weight, dimension, color, and other data of the product. 2) The system converts captured data into data. 3) The system downsizes the image. 4) The system converts images to grayscale. 5) The system applies matrix filters to the grayscale image. 6) The system performs Max-Polling. 7) The system flattens the matrix result. 8) The system extracts product details. 9) The system combines data from 5 and 8 using Rejex JSON. 10) The system utilizes data from 9 to generate a QR code.	
Alternative Flow	
If the system fails to accomplish any step: 1. Notify the manufacturer. 2. Return flow to step 1.	
Result: The QR Code of a genuine product has been successfully generated by the manufacturer using the available data provided.	

Table 2. The product authentication process for counterfeit identification

#2 **Name:** Authenticate Product	
Brief description: This use case highlights the actions required to be executed for the system to authenticate a product by scanning the QR Code generated at the point of production.	
Primary Actor: Distributor / Consumer / Regulating Body	
Precondition:	The manufacturer has successfully generated a QR code for a genuine product.
Trigger	Distributor / Consumer attempts to validate the authenticity of a product.
Main Flow	
1) The system prompts the QR Code of the product in focus. 2) The user presents the system with the Code. 3) The system scans the code, decodes data embedded in it, and compares it with the list of data about the genuine products. 4) The system outputs authentication results to the user.	
Alternative Flow	
If comparing product data, 1. Product data is not found, - notify the user, - return control to step 1.	
Result: The originality of a product has been authenticated using the QR code scanner.	

2.2 Entities Involved

From the use cases, the entities that make up the system; which have state and behaviors, as well as attributes and operations[13–15], are considered to be:

1) Manufacturer,

2) Consumers (including regulatory bodies, distributors, and end users who attempt to confirm the authenticity of a product), and

3) Product. Thus, it is important to note that 'Product' is the most important of all the entities as it is the object for which the QR code is generated and scanned to ascertain positive or negative results.

The attributes and operations of the identified entities would be as follows:

1. Manufacturer
- mfd ID
- password
- name
- address
- longitude
- latitude
+ login (Mfd ID, Password)
+ generate QR Code (Product): QR Code
+ register Product (QR Code)

2. Product
- prodTexture
- name
- weight
- dimension
- batchNum
- mfd ID
- productionDate
- expiryDate
- ownershipStatus

3. Consumer
+ authenticateProduct (QR Code): Product

The identification of the entities and their respective attributes and operations brings about the conceptual class diagram of the system which shows the static view and interrelationship between entities [4] as shown in Figure 1.

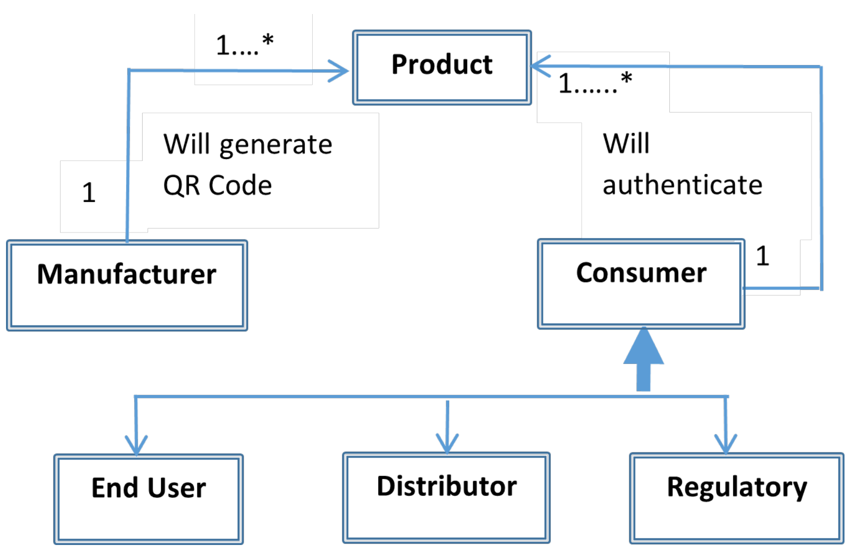

Fig 1. Conceptual Class Diagram of the System

Steps for Generating QR Code

To generate this special QR code, the following steps are taken:

1) Capture product texture as an image

2) Downsize the image
3) Convert image to Grayscale
4) Apply matrix filters
5) Do max-polling
6) Flatten matrix result
7) Extract product details
8) Combine data from (6) with data from (7) using Regex json
9) Feed data obtained from (8) into a QR generator

These steps are explained below.

- **Product Details and Image Capture:** The application starts by prompting the user to provide product details. These details could include information such as product name, manufacturing date, expiry date, batch number, price, and any other relevant data. Once the user submits these details, the application activates the device's camera to capture an image of the product.
- **Image Processing:** After capturing the image, the application performs image processing operations, similar to those used in convolutional neural networks (CNNs). These operations help enhance the image quality and extract relevant features. The specific techniques employed include resizing the image to a standardized size and applying convolutional filters to emphasize important patterns. Image processing plays a crucial role in enhancing the captured product image and extracting relevant features. The techniques employed in this step are inspired by convolutional neural networks (CNNs), which are commonly used for image analysis and recognition tasks. Although a full-fledged CNN is not implemented in this process, some of the fundamental concepts are applied.
- **Resizing:** Resizing the image is an essential preprocessing step to ensure consistency in the subsequent operations. By resizing the image to a standardized size, such as 24x24 pixels, we simplify the subsequent calculations while maintaining the vital visual characteristics of the product.
- **Convolutional Filters:** Convolutional filters, also known as kernels, are applied to the image to extract specific features. These filters act as sliding windows that traverse the image and perform mathematical operations on small patches of pixels. The filters emphasize patterns, edges, textures, or other relevant features within the image. By applying convolutional filters, the processed image highlights important visual cues that aid in subsequent analysis.
- **Max pooling:** Max pooling is a down-sampling technique used in CNNs to reduce the spatial dimensions of feature maps obtained from convolutional operations. It helps to extract the most prominent features while reducing the computational complexity. Max pooling divides the feature map into non-overlapping rectangular regions (often referred to as pooling windows or pooling kernels) and retains only the maximum value within each region. This down-samples the feature map by a factor determined by the size and stride of the pooling windows. Max pooling serves two primary purposes in image processing:

1. **Translation Invariance:** By selecting the maximum value within each pooling window, max pooling helps to capture the most significant features while being invariant to small translations or shifts in the input image. This property allows the CNN to recognize features irrespective of their precise location within the image.
2. **Dimension Reduction:** The downsampling effect of max pooling reduces the spatial dimensions of the feature map, reducing the number of parameters and computations required in subsequent layers. This dimension reduction aids in extracting more abstract and higher-level features from the image.

In the context of our QR scanner application, max pooling is applied after the convolutional filters. The feature map obtained from the convolutional operations is divided into pooling windows, and the maximum value within each window is retained, forming a downsampled feature map.

- **Matrix Representation:** The resulting downsampled feature map is converted into a matrix representation with reduced dimensions, similar to the matrix conversion step discussed earlier. This matrix captures the essential features extracted through convolution and max pooling, further aiding in subsequent processing steps.

By incorporating max pooling into the image processing step, our QR scanner application is effectively downsampled and captures the most salient features of the product image. This downsampling reduces computational complexity and improves the efficiency of subsequent operations, ultimately contributing to the generation of accurate and informative QR codes.

- **Matrix Conversion:** Following the image processing step, the image is converted into a matrix representation. This matrix represents the image with dimensions typically reduced to 24x24 pixels. The downsizing helps to reduce the complexity of subsequent operations while retaining the essential information needed for QR code generation.
- **Product Information Encryption:** Simultaneously, the extracted product details are converted into a JSON string, creating a structured representation of the information. This JSON string is combined with the image matrix as input for an encryption algorithm. The encryption process protects the data and ensures its confidentiality during transmission and storage.
- **QR Code Generation:** The encrypted output from the encryption algorithm is passed to a QR code generator. The QR code generator takes the encrypted data as input and generates a QR code image that encodes the information. When scanned, the QR Result is the encrypted information that is used to uniquely identify the product.
- **Saving the QR Code:** Once the QR code is generated, the application saves it for future use or sharing. The saved QR code can be displayed on the screen, printed, or transmitted to be stored in a network.in

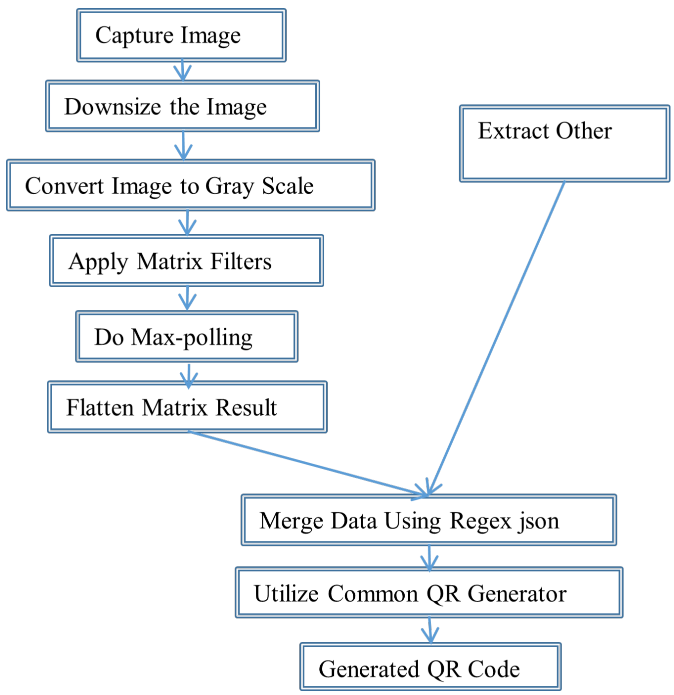

Fig 2. System Flow Diagram

2.3 The Blockchain Network Implementation

The blockchain-based system follows these four stages of implementation with the conceptual diagram presented in Figure 3.

The manufacturers and distributors enrolled on the network: In this stage, all the manufacturers and distributors are enrolled in the blockchain network. Their authentication is done through registration. In so doing, they will be required to furnish the system with their registered business name, contact information (phone number(s), email address, location cordinates, etc). The system issues a unique identification (ID) and passwords to each manufacturer and distributor.

The second phase is the enrolment of the product on the network: Here a request is made by the registered manufacturer to add a product to the network. The unique product texture is captured as an image and converted to text, and other parameters/features such as manufacturing date, expiration date, serial number, batch number, etc. are inputted to generate a unique QR code. Then smart contract is created to eliminate the risk of third-party manipulation and the the QR code for the product will be encrypted for improved security.

Product shipment: In this stage, the product is shipped to a distributor, and this changes the product status as shipped; the ownership of the product will not change until the system approves the parties involved mutually to buy and sell the product. Soon after, its ownership in the blockchain network system is transferred in the form of a smart contract automatically after the payment is confirmed.

The end user gets details about the product: In this last stage, end users can then scan the QR code embedded in the product a scanner app installed on a smartphone which automatically transmits retrieved information from the QR code along with the transaction location information (GPS coordinates) to the blockchain platform. The blockchain system compares the stored data during product enrolment with retrieved data received from the app. The outcome of the comparison will be sent as a message to the end user confirming the genuineness of the product.

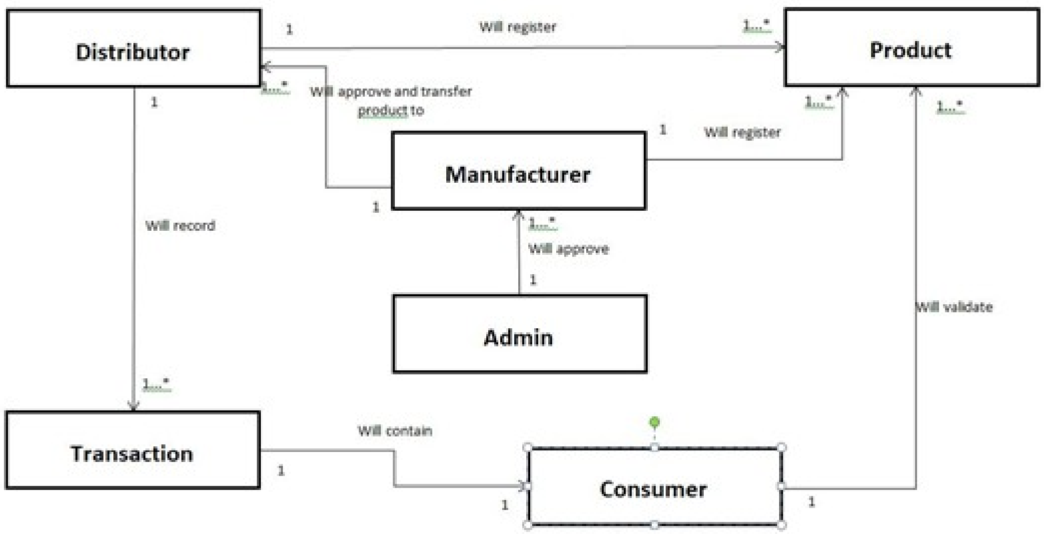

Fig 3. Conceptual class diagram of the system

The developed system should allow manufacturers to register and log on to the network to register their products. The blockchain network will allow manufacturers to authenticate and approve distributors on the network. The network should enable approved distributors to record transactions on the blockchain network. The blockchain network should allow end users to register and have access to the network using the developed application. In all, manufacturers, distributors, and the general public (end users) should be able to validate the authenticity of a product using the blockchain network.

To set up a private Ethereum blockchain network for the product anti-counterfeiting system, the following tools were installed; Ganache, VS Code, Truffle Suite, Node. Js and MetaMask. The Ganache is the principal component of the Truffle Suite that will be utilized in setting up our personal Ethereum blockchain network. The VS Code is the main programming environment where we will write, edit, and debug our codes while MetaMask is an extension for Chrome that enables interaction between the Ethereum dApp, blockchain network, and user interface.

2.4 Performance Evaluation of the System

The performance of the system was tested against two factors which served as the key performance indicators (KPIs) of the system. These factors include - the speed of product authentication, and the accuracy of result obtained. In this case, twenty (20) different products from ten (10) manufacturers were registered into the system and a QR code was generated for each of them. Another set of ten (10) products which were similar to the initial ones but considered counterfeit were also acquired, and a QR code was generated for each. The generated QR codes for the sets of original and considered counterfeit products captured the weights, color, texture, and surface area of the respective products. Information regarding a specific product (as captured in the QR codes) was then scanned into the Novel Product Counterfeit Detection System. The records of the genuine products were considered the benchmark upon which the originality of a product is ascertained. The two sets of products were then mixed up together to form a single set containing both genuine and (considered to be) counterfeit products. In so doing, a total number of thirty (30) products were then obtained in the single set. Each product was then scanned at a light intensity of 1000 lux to ascertain originality. A total number of thirty (30) scans were made. The time of processing, which is the duration in which result scan result is obtained after scanning, was noted.

3 Results and Discussion

The result in Table 3 is the performance analysis of the developed system against two key factors that served as the key performance indicators (KPIs). These include the speed of execution and the accuracy of the result obtained. Results must be validated with previous results in the relevant literature and be discussed with favoring and contradicting the current findings. Comparison with existing reports should be provided to prove the validity of the present model or program developed. Finally, the originality of the product was also recorded as presented in Table 3 and the comparative analysis is shown in Table 4.

Table 3. Performance result of product authentication via QR code scanning

S/N	Product	Time of processing (s)	Light Intensity (lux)	Originality (Yes/No)
1.	Product 1	0.010	1000	Yes
2.	Product 2	0.009	1000	Yes
3.	Product 3	0.009	1000	No
4.	Product 4	0.008	1000	Yes
5.	Product 5	0.010	1000	Yes
6.	Product 6	0.009	1000	Yes
7.	Product 7	0.009	1000	Yes
8.	Product 8	0.010	1000	No
9.	Product 9	0.009	1000	Yes
10.	Product 10	0.009	1000	No
11.	Product 11	0.010	1000	Yes
12.	Product 12	0.010	1000	No
13.	Product 13	0.009	1000	Yes
. . .				
49	Product 49	0.010	1000	No
50	Product 50	0.010	1000	Yes

Table 4. Comparative analysis of the proposed system against the existing works

	Detection Accuracy (%)	Processing Time
[16]	92 & 98	35ms
[17]	78.63	23ms
[18]	93.50	22ms
[19]	99.13	12ms
[20]	98.90	10.3ms
This work	100	9.5ms

The test results from the QR code generator and scanning system practically show that in a well-regulated environment where the luminous intensity is kept constant at a good level, the accuracy of the system is optimal. This is evident in the thirty (30) genuine and twenty (20) counterfeit results obtained, which were the actual number of products that were scanned into the system. Furthermore, the speed of execution was virtually constant as it lies between the figures of 0.009 - 0.010 seconds. This is most likely because the fifty (50) products were all tested using the same computer, an Intel Core i5 laptop running on 1TB HDD and 8GB RAM at a processor speed of 3.5GHz. From Table 3, the probability of obtaining a wrong result on scanning a product is practically reduced to zero. Therefore, the developed QR code generator and scanning system accurately detects counterfeit products at a very high speed, which is quite different from already existing systems reviewed in [9] [10] [6] [8]. However, an increase in sample size will provide more control of the risk of false-positive findings. This will reduce the error margin and the standard deviation measure thereby increasing the precision of the system.

shows the detection accuracy and processing time of 5 QR code scanner applications from recent quality research and how they compared with the results from this work. The excellent performance of this work is established from the information in Table 4. The execution time and the accuracy of this work are impressive and can be recommended for large-scale deployment to curb the menace of counterfeiters.

4 Conclusion

Object-oriented system modelling approach has been adopted alongside Rapid Unified Process in the design of a novel QR code scanner system which is used to ascertain the authenticity of a product. Results have shown that in a controlled environment where the surrounding light intensity is kept constant at a reasonable level, the possibility of mistaking counterfeit products for genuine products is drastically reduced. The developed system is unique as it combines product inherent features, copy-sensitive QR code, location information (i.e., longitude and latitude coordinates) as well as Track and Trace technologies. It utilizes the method for detecting counterfeit by the capture of texture which is indissolubly linked with the product. The inherent features of a product such as colour, texture, weight, dimension, and so on, are highly fundamental in determining the authenticity of the product when subjected to validation. While validating a product, the accuracy of the result obtained is highly fundamental in ascertaining whether or not a product is genuine. The speed of execution was virtually constant as it lies between the figures of 9ms - 10ms with zero probability of obtaining a wrong result on scanning a product. It is therefore recommended that this novel approach be integrated into the manufacturer-consumer supply chain for easy identification of genuine and counterfeit products. A blockchain-based counterfeiting system with an enhanced consensus algorithm will likely improve the proposed system. This could provide a balance between the efficiency and security of the system.

Acknowledgements

The authors extend their gratitude to the editor for their valuable contributions and express appreciation to the anonymous reviewers for their insightful comments. The APC is deferred partially by the Indian Society for Education and Environment.

References

1) Mahendrian N, S KRV. Fake Product Detection Using QR Code. *International Journal of Research Publication and Reviews*. 2024;5(4):1093–1096. Available from: https://ijrpr.com/uploads/V5ISSUE4/IJRPR24668.pdf.
2) Toshihiro O, Shuya K, Kai K, Hayato K, Tatsuya S, Daichi O, et al. Detecting Fake QR Codes Using Information from Error-Correction. *Journal of Information Processing*. 2021;29:548–558. Available from: https://www.jstage.jst.go.jp/article/ipsjjip/29/0/29_548/_pdf#:~:text=In%20a%20QR%20code%20with,if%20such%20a%20codeword%20exists.
3) Aulia MM, Saha N, Rahman MM. Protected QR Code-based Anti-counterfeit System for Pharmaceutical Manufacturing . 2024;p. 1–6. Available from: https://arxiv.org/pdf/2404.07831.
4) Aggarwal M, Ranjan H, Gupta G, Walia S, Tyagi D. Anti-Counterfeiting Detection System Using Blockchain. *International Journal for Research in Applied Science and Engineering Technology*. 2022;10(5). Available from: https://www.ijraset.com/research-paper/anti-counterfeit-detection-system-using-blockchain.
5) Gumma LN, Reddy CV, Sattish I, Teja AS, Teja AR. A Review on Counterfeit Product Detection in E-Commerce. *International Journal Of Multidisciplinary Research In Science, Engineering and Technology (IJMRSET)*. 2023;6(2). Available from: https://www.ijmrset.com/upload/5_A%20Review.pdf.
6) Benatia MA, Baudry D, Louis A. Detecting counterfeit products by means offrequent pattern mining. *Journal of Ambient Intelligence and Humanized Computing*. 2022;13:3683–3692. Available from: https://link.springer.com/article/10.1007/s12652-020-02237-y.
7) Chou GJ, Wang RZ. The Nested QR Code. *IEEE Signal Processing Letters*. 2020;27:1230–1234. Available from: https://ieeexplore.ieee.org/document/9130829.
8) Aman A, Singh A, Raj A, Raj S. An Efficient Bar/QR Code Recognition System for Consumer Service Applications. In: 2020 Zooming Innovation in Consumer Technologies Conference (ZINC). 2020;p. 127–131. Available from: https://ieeexplore.ieee.org/document/9161778.
9) Huang Y, Cao P, Lyu G. A Directly Readable Halftone Multifunctional Color QR Code. *Chinese Journal of Electronics*. 2023;32(3):1–11. Available from: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10124659.
10) Wu W, Zhang L, Zhang J, Cui C, Zhang X, Liu M. A three-level QR code sharing scheme based on SLIC and Hamming code. In: 2022 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC). IEEE. 2022;p. 1–6. Available from: https://ieeexplore.ieee.org/document/9984448.
11) Barron IR, Sharma G. Optimized Modulation and Coding for Dual Modulated QR Codes. *IEEE Transactions on Image Processing*. 2023;32:2800–2810. Available from: https://ieeexplore.ieee.org/document/10120729.
12) Mhatre M, Kashid H, Jain T, Chavan P. BCPIS: Blockchain-based Counterfeit Product Identification System. *Journal of Applied Security Research*. 2022;18(4):740–765. Available from: https://www.tandfonline.com/doi/full/10.1080/19361610.2022.2086784.
13) Dennis A, Wixom BH, Roth RM. Systems Analysis and Design. 5th ed. and others, editor;John Wiley & Sons. 2021. Available from: https://www.uoitc.edu.iq/images/documents/informatics-institute/Competitive_exam/Systemanalysisanddesign.pdf.
14) Agu SC, Elugwu F. Object Oriented Programming Approach: A Panacea for effective Software Development. *African Journal of Advances in Science and Technology Research*. 2022;6(1):1–14. Available from: https://www.researchgate.net/publication/364343740_Object_Oriented_Programming_Approach_A_Panacea_for_Effective_Software_Development.
15) Habtamu K, Department of Information System. Object Oriented System Analysis and Design (OOSAD). Ethiopia. 2020. Available from: https://www.studocu.com/row/document/ambo-university/database-systems/revised-oosad-module-2020/32367136.
16) Prabhu BS, Jayavadivel R, Viswanath TK. A Novel Approach For Detect Counterfeit Product Using Color QR Code. *International Journal of Scientific & Technology Research*. 2020;9(1):1–6. Available from: https://www.ijstr.org/final-print/jan2020/A-Novel-Approach-For-Detect-Counterfeit-Product-Using-Color-Qr-Code.pdf.
17) Wahsheh H. Barsec Droid. 2018. Available from: https://m.apkpure.com/barsec-droid/barcode_security.heider.apk.
18) Rafsanjani AS, Kamaruddin NB, Rusli HM, Dabbagh M. QsecR: Secure QR Code Scanner According to a Novel Malicious URL Detection Framework. *IEEE Access*. 2023;11:92523–92539. Available from: https://ieeexplore.ieee.org/document/10172018.

19) Kamnounsing P, Sumongkayothin K, Siritanawan P, Kotani K. Adversarial Halftone QR Code. *IEEE Acces*. 2024;13:126729–126737. Available from: https://ieeexplore.ieee.org/document/10538266.
20) Chindaudom A, Siritanawan P, Sumongkayothin K, Kotani K. AdversarialQR: An adversarial patch in QR code format. In: Joint 9th International Conference on Informatics, Electronics & Vision (ICIEV) and 2020 4th International Conference on Imaging, Vision & Pattern Recognition (icIVPR). IEEE. 2020;p. 1–6. Available from: https://ieeexplore.ieee.org/document/9306675.