ENCRYPTED QR CODE FOR BRAND AUTHENTICATION: ENQRURE MOBILE APPLICATION DEVELOPMENT AND EVALUATION

[1]Qi Jun Chong, [2]Mohammed Alsamman & [3]Noraziah Che Pa
[1,2&3] School of Computing, Universiti Utara Malaysia, Malaysia

[1]Corresponding author: alsamman@uum.edu.my

ABSTRACT

Counterfeit products pose a growing concern for brand owners and consumers due to their adverse effects on user experience and brand value, leading to unsatisfied customers, negative publicity, and even potential health risks. This paper addresses the growing issues surrounding fake goods, which negatively affect customers and brand owners, including harmed user experiences, tarnished reputations, and potential health risks. The work proposed an encrypted QR code emphasising encryption techniques embedded in a mobile application with a friendly user interface and seamless interaction with existing authentication mechanisms to resolve this problem. The application aims to detect counterfeit goods, protect brand reputation, and increase consumer confidence by guaranteeing product authenticity. The study conducted a usability evaluation with 30 volunteers. The results indicated that enQRure proved to be a valuable and user-friendly application. Respondents expressed satisfaction with the application's feature that facilitates product authentication. Feedback analysis on features offered by enQRure, such as product registration, product authentication, and encrypted QR code generation processes, revealed that most respondents found them straightforward and useful. They perceived enQRure as an effective means to authenticate products, aligning with their preferences and needs.

Keywords: Brand Authentication, Encrypted QR code, Fraud Perception.

BACKGROUND

Various approaches and techniques have been developed to combat the proliferation of counterfeit products globally (Jonatan, 2021). One commonly used method involves the implementation of holographic watermarks and steganographic markings. For instance, laser direct writing is utilised to create tamper-

resistant holographic patterns on metal surfaces, particularly for high-value items like luxury watches, medical tools, collector coins, and similar goods (Wlodarczyk, 2019). These holographic structures consist of optically smooth craters organised to form diffractive images, ranging from company logos to alpha-numeric strings. This unique feature enables the authentication of genuine products, providing a reliable means to distinguish them from counterfeits (Wlodarczyk, 2019). Also, holographic structures can be combined with standard marking patterns like QR codes and data matrices, resulting in visually appealing holographic marks that conceal concealed product information. In some cases, multiple holographic patterns can be merged to create "holographic watermarks," further enhancing product authentication (Wlodarczyk, 2019).

Another effective anti-counterfeiting technique involves using low-cost Radio-frequency Identification (RFID) tags attached to products. RFID systems utilise protocols for tag authentication and database correction, providing a means to identify counterfeit items (Tran, 2015). The protocols allow tag authentication without compromising sensitive data, allowing clients to inquire about the tag at their convenience (Tran, 2015). By incorporating these advanced technologies, brand owners can strengthen their anti-counterfeiting efforts and protect consumers from counterfeit products. Implementing a combination of holographic watermarks, RFID tags, and other state-of-the-art methods can significantly reduce the prevalence of counterfeit goods worldwide (Wlodarczyk, 2019).

Encrypted QR codes operate by encrypting the data to be embedded within the code using robust encryption algorithms like Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA) and Secure Hash Algorithm 2 (SHA-2) (Bala Krishna, 2016). The security of encrypted QR codes for brand verification operates by fusing them with the distinctive identification skills of QR codes. Only the brand owner can access the decryption key, which generates each encrypted QR code. As a result, even if an attacker successfully copies or changes an encrypted QR code, they won't be able to unlock it and access the data inside. The brand owner would create a unique QR code for each product before using an encrypted QR code for brand authentication. The proprietary encryption key of the brand owner would then be used to encrypt the QR code. The product packaging or another method of product attachment would subsequently be printed with the encrypted QR code. A buyer would use their smartphone to scan the encrypted QR code to verify goods. After that, the smartphone would decipher the QR code and check the product's legitimacy. A message confirming authentication will be given to the client if the goods are genuine. A negative authentication message will be sent to the customer if the product is not genuine (Picard, 2021). Encrypted QR codes offer a reliable means for brands to ensure product authenticity and protect consumers from counterfeit goods. They serve as a secure conduit for sharing information while deterring fraudulent activities.

METHODOLOGY

A set of programming languages, frameworks, and tools were chosen carefully to create the encrypted QR code application for the brand authentication name enQRure. The primary programming language was Dart, used with the versatile Flutter framework. This combination allowed us to create a user-friendly experience that is both seamless and responsive. Additionally, it provided cross-platform compatibility to reach a more significant number of users. To establish a robust backend infrastructure, the capabilities of PHP were leveraged, a server-side scripting language renowned for its dependability and adaptability. PHP seamlessly facilitated the communication between the mobile application and the MySQL database, which functioned as the central repository for all essential data of brand authentication. MySQL was used as the database management system based on its established reputation for data integrity and scalability, guaranteeing the secure storage and retrieval of critical brand information.

Visual Studio Code was chosen to select development environments, a highly regarded integrated development environment (IDE). Its user-friendly interface, vast plugin ecosystem, and solid debugging capabilities have enabled greater efficiency in the development process, such as writing, testing, and optimising code with excellent efficiency. Additionally, working within a Windows 11 environment has further enhanced our development process, providing a reliable and secure foundation for software development. To enable instantaneous data exchange between the mobile application and MySQL database, the services of a web hosting provider were utilised. This intermediary facilitated seamless communication and data synchronisation, enhancing our brand authentication solution's scalability, reliability, and responsiveness.

A product's unique identity is established by amalgamating critical information elements, including the product identifier, product name, manufacturing date, manufacturer's name, and a randomly generated unique identifier. These diverse data components are meticulously processed and fortified by applying SHA-256 encryption, a robust cryptographic method. Subsequently, this fortified product identity is encapsulated within a QR code, a two-dimensional barcode capable of securely storing and facilitating the retrieval of this vital product information. This comprehensive approach enhances security, fosters brand authentication, streamlines inventory management, and supports traceability by ensuring the product's identity is unique and shielded from unauthorised access or tampering.

By following this methodology, organisations can maintain a robust product authentication system that leverages encryption and QR code technology to safeguard the integrity and uniqueness of the products, ultimately bolstering consumer confidence and enhancing the overall efficiency of their brand authentication. In brief, the development of enQRure was a carefully planned and executed endeavour, utilising Dart and Flutter for the mobile application, PHP for the backend, MySQL for data storage, Visual Studio Code for development, and a web hosting service for seamless data transmission. This comprehensive technology stack facilitated the delivery of a secure, efficient, and user-friendly solution for brand authentication, in accordance.

DEVELOPMENT OF ENQRURE

This section describes the design and development of enQRure. A requirement-gathering process was conducted by analysing relevant documents and existing systems related to brand authentication. During the development phase, the prototype interface was shown to the experts to gather their feedback and comments, ensuring that the app met their expectations and needs. Various documents and resources related to QR code scanning, encryption techniques, and brand authentication were analysed for the requirements-gathering process. Online searches were conducted using relevant keywords, such as "encrypted QR code scanning," "brand authentication with QR codes," "secure QR code generation," and "QR code encryption methods." The documents were reviewed to extract the requirements for developing an encrypted QR code scanner for brand authentication. Table 1 lists seven significant requirements and their priority identified from this analysis.

Table 1

List of Requirements of enQRure

No.	Requirement ID	Requirements Description	Priority
1	**EQS1**	**Register Account**	
	EQS1_1	The buyer can register a new account by providing their information.	Optional
	EQS1_2	The buyer can upload his profile image.	Optional
	EQS1_3	The system will display a reminder message when the user enters a user email address that already exists in the system.	Desirable
	EQS1_4	The buyer will be prompted with an error message if the registration form is incomplete.	Desirable
	EQS1_5	The system will send a verification email to the registered user.	Mandatory
2	**EQS2**	**Login**	
	EQS2_1	The system admin, manufacturer, retailer, and buyer must insert a user email address and password to log in to the application.	Mandatory
	EQS2_2	The application will prompt error messages such as "Invalid login" if the user inputs the wrong email address or password.	Desirable
	EQS2_3	The system must verify the user's role as an admin, manufacturer, retailer and buyer.	Mandatory
	EQS2_4	The admin, manufacturer, retailer and buyer could select forgot password links to reset the password if they forgot the password.	Desirable
	EQS2_5	The system will send a password reset email to the user if the admin, manufacturer, retailer and buyer select the forgotten password section.	Mandatory
3	**EQS3**	**Manage Account**	
	EQS3_1	Admin can add accounts for manufacturer and retailer by entering some information.	Mandatory
	EQS3_2	The manufacturer, retailer or buyer can view their account details.	Optional
	EQS3_3	The manufacturer, retailer or buyer can change their account password.	Desirable
	EQS3_4	The buyer can edit his account details.	Desirable
	EQS3_5	Admin can edit the details of manufacturer and retailer accounts.	Desirable
	EQS3_6	Admin can delete the user account.	Desirable
4	**EQS4**	**Generate QR Code**	
	EQS4_1	The manufacturer can generate an encrypted QR code by	Mandatory

		inserting information about the product.	
	EQS4_2	The system will prompt error messages such as "Incomplete information" if the information is incomplete.	Optional
	EQS4_3	The manufacturer can generate bulk encrypted QR codes by uploading a CSV file filled with the information of the products.	Optional
	EQS4_4	The manufacturer can view the list of the generated QR code	Mandatory
	EQS4_5	The manufacturer can print the QR code.	Mandatory
5	**EQS5**	**Register Product**	
	EQS5_1	The manufacturer and retailer can register the product by scanning the encrypted QR code.	Mandatory
	EQS5_2	The system will prompt error messages such as "Invalid QR Code" if the QR code is invalid or registered before.	Desirable
6	**EQS6**	**Authenticate Product**	
	EQS6_1	The buyer can authenticate the product by scanning the encrypted QR code.	Mandatory
	EQS6_2	The buyer can view the information of their own authenticated product, such as the warranty period and the retailer and manufacturer information.	Mandatory
	EQS6_3	The system will prompt an error message if there is an invalid QR code.	Desirable
	EQS6_4	The system will prompt a warning message if the QR code is used for verification.	Desirable
	EQS6_5	The buyer can submit a counterfeit product report by uploading some information such as purchase date, purchase store and others.	Desirable
	EQS6_6	The buyer can upload a picture of the counterfeit product.	Optional
7	**EQS7**	**Generate Report**	
	EQS7_1	The manufacturer and retailer can view the list of their registered products.	Mandatory
	EQS7_2	The buyer can view the list of their own authenticated product.	Mandatory
	EQS7_3	The system admin can view the list of users.	Mandatory
	EQS7_4	The manufacturer can view the list of counterfeit product reports.	Mandatory

The requirements outlined in Table 1 were transformed into the functionalities of the computer system. The Unified Modelling Language (UML) was employed in this project to visualise and model these requirements. Specifically, the use case diagram collectively represents the app's structural and behavioural aspects. Star UML was utilised as the tool for creating these diagrams. Figure 1 presents the use case diagram, which showcases the interactions between the app's use cases and the actors involved. In this context, the actors are the users who interact with the mobile application. The diagram includes seven

major use cases: register an account, log in, manage an account, register a product, authenticate a product, and generate a report.

enQRure PROTOTYPE DEVELOPMENT

A functional prototype of the encrypted QR code scanner for brand authentication, named enQRure was successfully developed, incorporating all the requirements detailed in the previous section. Software prototyping is a valuable approach to showcase the software's functionalities, allowing users to interact with the prototype and provide valuable feedback based on their firsthand experience. Visual Studio Code was chosen as the primary integrated development environment (IDE) tool for the prototype's development. Additionally, MySQL was utilised as the database for securely storing the app's data. The enQRure prototype offers a tangible representation of the envisioned application, enabling users to test its features and functionalities in a controlled environment. The feedback from users during this prototyping phase will be crucial in refining the app's design and optimising its performance before the final deployment. Figures 3 and 4 show the selected interfaces of enQRure.
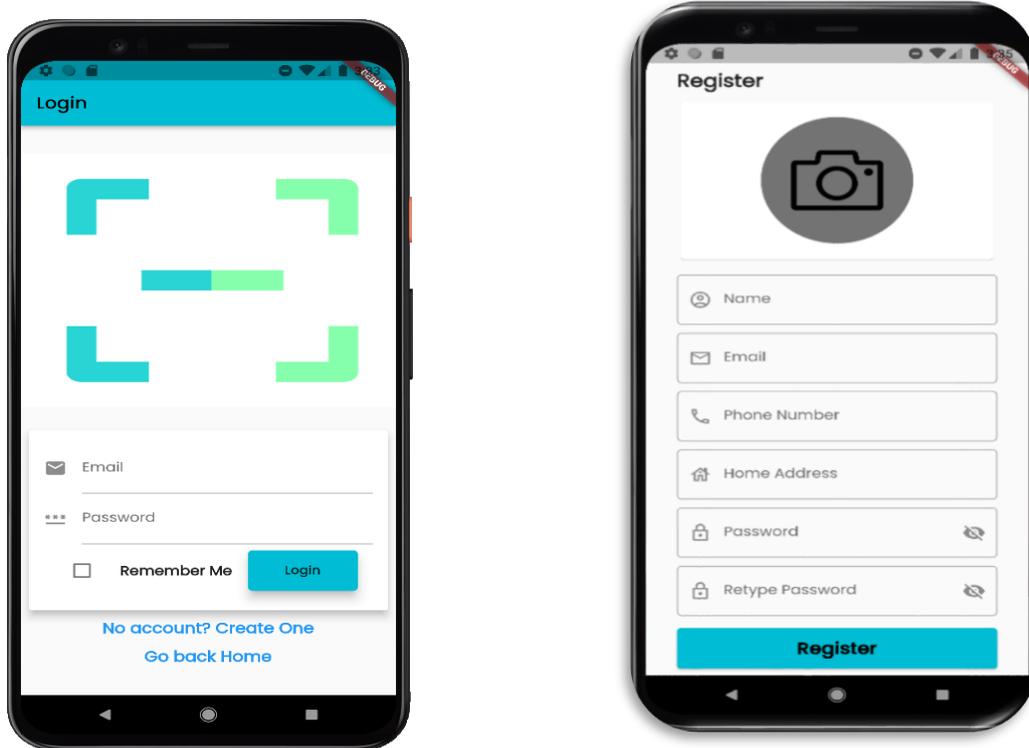
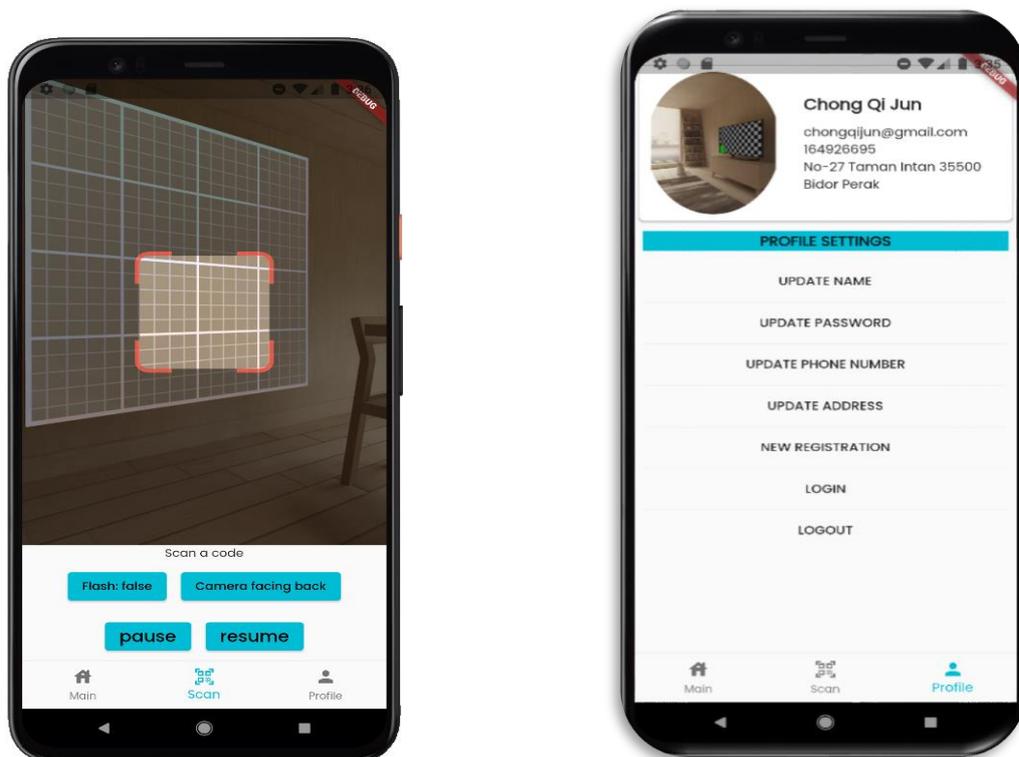**Figure 1**

The use Case Diagram of enQRure
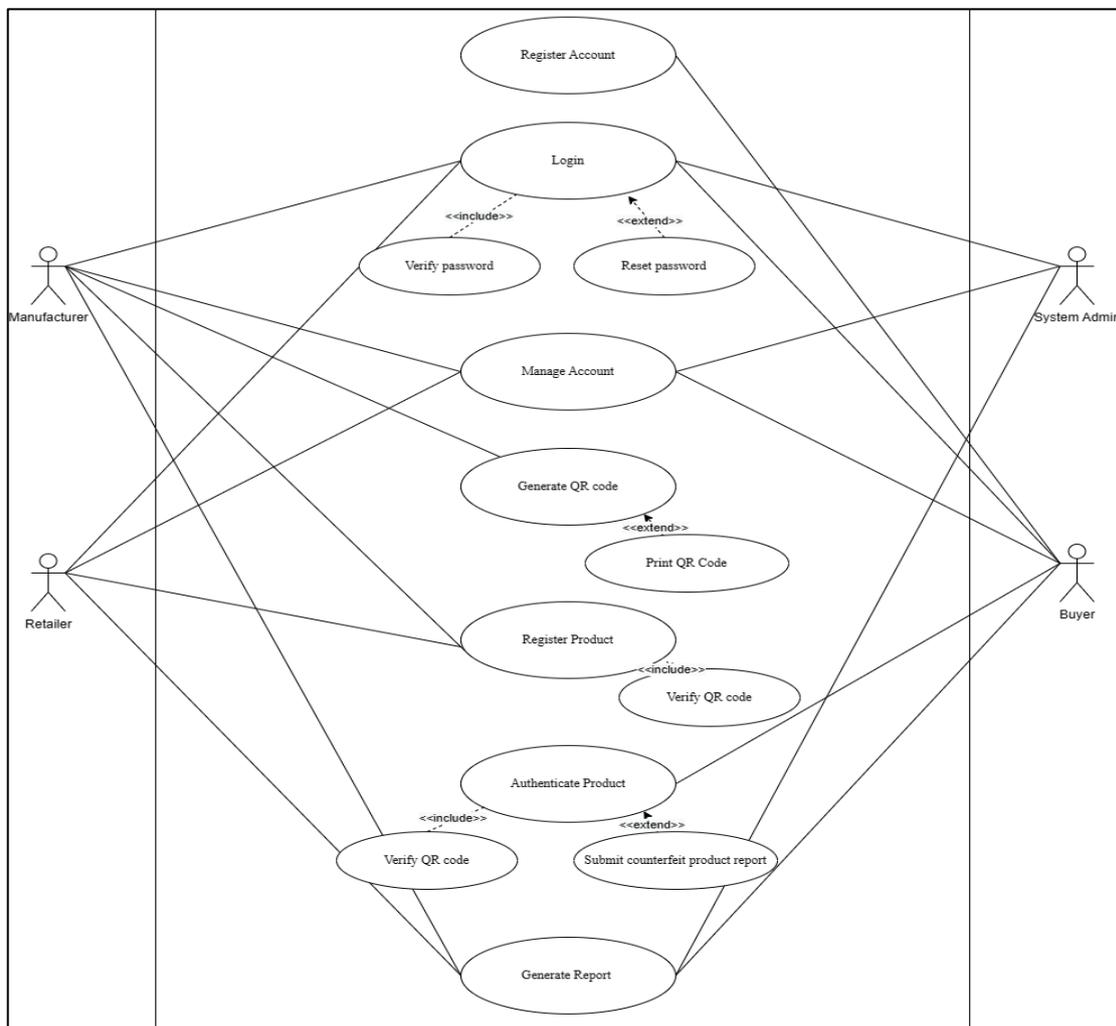
Figure 3

The Interface for Login (left) and Registration (right)

Figure 4

The Interface for Authenticating a Product (left) and the user Profile (right)

EVALUATION

A usability evaluation was conducted on 30 randomly selected respondents representing consumers. Participation in the study was voluntary, and the respondents were approached without bias. The evaluation involved two main instruments: the enQRure mobile application and a post-task questionnaire. The questionnaire, adapted from a reputable source, comprised 26 items divided into two sections. Section A collected demographic information from the respondents. Section B gauged their opinions on the enQRure mobile application using a five-point Likert scale, where one indicated "strongly disagree" and five represented "strongly agree."

During the evaluation, the respondents followed a step-by-step procedure, interacting with the enQRure mobile application as outlined in the experiment procedure. Afterwards, they completed the post-task questionnaire, providing valuable feedback on their experience with the application. The usability evaluation aimed to gather insights into the navigation and interface, application design, usefulness, and satisfaction of the enQRure mobile application, helping refine its design and functionality based on the respondents' feedback and opinions. (Meng, 2023) (Keerthy, 2023)

The Respondents' Demographic Information

An examination of the respondents' demographic data indicates that a substantial majority, comprising 86.67%, belonged to the age group of 15 to 24 years, and all participants possessed a bachelor's degree. Regarding gender distribution, 66.67% of the respondents identified as male, while all are Malaysian. Notably, all the respondents had encountered instances of unintentionally purchasing counterfeit products. Furthermore, a significant portion, amounting to 86.67%, confirmed that they have not personally used any brand authentication application. These demographic insights provide valuable context and considerations for the usability evaluation of the enQRure mobile application.

The Usability of enQRure

An analysis was conducted on the respondents' responses in Section B of the post-task questionnaire. The section measures the navigation and interface, application design, usefulness, and satisfaction of enQRure. Tables 2, 3, 4, and 5 reported the frequency and average of the responses with the following abbreviation - SD = Strongly Disagree, D = Disagree, N = Neutral, **A =** Agree, SA = Strongly Agree, A= Average.

Table 2

The Respondents' responses on the Navigation and Interface of enQRure

The post-task questionnaire items	SD	D	N	A	SA	A
I can navigate between different screens with ease and without any difficulties.	0 (0)	0 (0)	0 (0)	26 (86.67%)	4 (13.33%)	4.13
It was easy to learn to use this application.	0 (0)	0 (0)	0 (0)	4 (20%)	24 (80%)	4.8

	SD	D	N	A	SA	AV
I can easily navigate back to previous screens.	0 (0)	0 (0)	0 (0)	20 (66.67%)	10 (33.33%)	4.33
This application is designed to be user-friendly.	0 (0)	0 (0)	0 (0)	17 (56.67%)	13 (43.33%)	4.43
All the buttons in the application are working properly and performing their intended functions without any issues.	0 (0)	0 (0)	0 (0)	19 (63.33%)	10 (33.33%)	4.2

Table 3

The Respondents' Responses on the Application Design of enQRure

The post-task questionnaire items	SD	D	N	A	SA	AV
The application's content arrangement is thoughtfully organised and structured in a well-organised manner.	0 (0)	0 (0)	0 (0)	22 (73.33%)	8 (26.67%)	4.27
The colour scheme used in the application is visually appealing.	0 (0)	0 (0)	0 (0)	6 (20%)	24 (80%)	4.8
The application's use of whitespace and layout spacing enhances readability and reduces clutter.	0 (0)	0 (0)	0 (0)	16 (53.33%)	14 (46.67%)	4.47
The application's visual design is consistent across different screens.	0 (0)	0 (0)	0 (0)	5 (53.33%)	14 (46.67%)	4.47
The visual hierarchy in the application helps users easily identify important elements.	0 (0)	0 (0)	0 (0)	15 (50%)	15 (50%)	4.5

Table 4

The Respondents' Responses on the Usefulness of enQRure

The post-task questionnaire items	SD	D	N	A	SA	AV
The application improves my productivity or efficiency in completing tasks.	0 (0)	0 (0)	0 (0)	19 (63.33%)	11 (36.67%)	4.37
The information presented in the application is accurate and reliable.	0 (0)	0 (0)	0 (0)	11 (36.67%)	19 (63.33%)	4.63
The application enhances my knowledge or understanding of a particular area.	0 (0)	0 (0)	0 (0)	18 (60%)	12 (40%)	4.4

	SD	D	N	A	SA	AV
The application simplifies complex tasks or processes for me.	0 (0)	0 (0)	0 (0)	13 (43.33%)	17 (56.67%)	4.57
The application provides a seamless and intuitive user experience.	0 (0)	0 (0)	0 (0)	14 (46.47%)	16 (53.33%)	4.53

Table 5

The Respondents' Responses on the Satisfaction of enQRure

The post-task questionnaire items	SD	D	N	A	SA	AV
The application effectively fulfils my needs and requirements.	0 (0)	0 (0)	0 (0)	19 (63.33%)	11 (36.67%)	4.37
I am satisfied with the performance and speed of the application.	0 (0)	0 (0)	0 (0)	11 (36.67%)	19 (63.33%)	4.63
The application offers a wide range of useful features and functionalities.	0 (0)	0 (0)	0 (0)	18 (60%)	12 (40%)	4.4
I feel that the application enhances my productivity or efficiency.	0 (0)	0 (0)	0 (0)	13 (43.33%)	17 (56.67%)	4.57
I am overall satisfied with the experience of using the application.	0 (0)	0 (0)	0 (0)	14 (46.47%)	16 (53.33%)	4.53

The evaluation results indicated that enQRure was a valuable and user-friendly application. Respondents expressed satisfaction with the app's feature that facilitates product authentication. Feedback analysis on features offered by enQRure, such as product registration, product authentication, and encrypted QR code generation processes, revealed that most respondents found them straightforward and valuable. They perceived enQRure as an effective means to authenticate products, aligning with their preferences and needs.

Regarding the user interface, respondents reported that enQRure was intuitive to use, requiring no written instructions, and they could easily recall the steps for interacting with the mobile app. Additionally, they expressed satisfaction with the app's appearance and indicated their willingness to recommend enQRure to others. The overall evaluation demonstrates that enQRure successfully meets user expectations, providing an efficient and user-friendly platform for brand authentication via encrypted QR codes. The positive feedback from respondents affirms the app's potential to effectively combat counterfeit products and enhance consumer confidence in the authenticity of their purchases.

CONCLUSION

The global prevalence of counterfeit goods continues to rise, causing adverse effects on customers and severely impacting nations' economies. To effectively combat counterfeiting, it is essential to leverage modern technology and increase awareness of these illicit practices. The mobile application, enQRure is developed to enhance brand authentication through encrypted QR code technology, aiming to improve

efficiency in the authentication process significantly. This application offers a cost-effective and convenient solution for sellers and buyers by leveraging encrypted QR codes for brand authentication. Its primary goal is to eradicate product counterfeiting, often leading to substantial losses. Through enQRure, genuine manufacturers can safeguard their revenue while customers can confidently exercise their rights. The findings show enQRure is a valuable and approachable application, and respondents expressed pleasure with its function for product authentication and found its characteristics beneficial. The user interface was well-liked by users, who were eager to share enQRure with others. EnQRure is an effective and user-friendly platform for brand verification using encrypted QR codes that satisfy user expectations. It could help fight counterfeit goods and increase consumer confidence in their purchases.

REFERENCES

Bala Krishna, M. A. (2016). Product authentication using QR codes: a mobile application to combat counterfeiting. *Wireless Personal Communications*, 381--398.

Basu, M. M. (2015). Factors influencing consumers' intention to buy counterfeit products. *Global Journal of Management and Business Research, 15*(6), 23-35.

Coalition, I. A. (2021, September 23). What is Counterfeiting? International Anti Anti-Counterfeiting Coalition.

Development, O. F. (2019, March 18). Trade in fake goods is now 3.3% of world trade and rising. Retrieved from https://www.oecd.org/newsroom/trade-in-fake-goods-is-now-33-of-world-trade-and-rising.htm

Hernandez-Fernandez, A. A. (2019). Brand authenticity leads to perceived value and brand trust. *European Journal of Management and Business Economics, 28*(3), 222-238.

Jonatan, S. (2021). Brand authenticity: 25 Years of research. *International Journal of Consumer Studies, 45*(4), 645--663.

Keerthy, G. a. (2023). Enhancing Product Authentication and Counterfeit Detection Using QR Codes and Blockchain Technology. *2nd International Conference on Edge Computing and Applications (ICECAA)* (pp. 262--267). IEEE.

Maldonado, C. a. (2005). Attitudes toward counterfeit products: An ethical perspective. *J. Legal Ethical & Regul. Issues, 8*, 105.

Meng, X. A. (2023). An efficient authentication protocol for brand cosmetics anti-counterfeiting system. *10th International Conference on Cyber Security and Cloud Computing (CSCloud)/2023 IEEE 9th International Conference on Edge Computing and Scalable Cloud (EdgeCom)p*(pp. 120--125). IEEE.

Picard, J. A. (2021). Counterfeit detection with QR codes. *21st ACM Symposium on Document Engineering*, 1-4.

Quoquab, F. A. (2017). Factors affecting consumers' intention to purchase a counterfeit product: empirical study in the Malaysian market. *Asia Pacific Journal of Marketing and Logistics, 29*(4), 837--853.

Tardi, C. (2022, March 23). *Trademark Definition, What It Protects, Symbols, Example*. Retrieved May 07, 2023, from https://www.investopedia.com/terms/t/trademark.asp

Tran, D.-T. A. (2015). RFID anti-counterfeiting for retailing systems. *Journal of Applied Mathematics and Physics, 3*(01), 1.

Wlodarczyk, K. L. (2019). Holographic watermarks and steganographic markings for combating the counterfeiting practices of high-value metal products. *Journal of Materials Processing Technology, 264*, 328--335.