International Journal of Web of Multidisciplinary Studies
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
website: http://ijwos.com
Vol.02 No.11.
OPEN ACCESS
E-ISSN : 3049-2424
DOI:

Fake Product Identification Using QR Code-Based Authentication System

Punya Patil G M[1] , Ms. Anu V B[2]

[1] *Student, Master in Computer Applications, Faculty of Computing and IT, GM University, Davanagere-577006, Karnataka, India*

[2] *Assistant Professor, Faculty of Computing and IT, GM University, Davanagere-577006, Karnataka, India*

Article Info

Article History:

Published:07 Nov 2025

Publication Issue:
Volume 2, Issue 11
November-2025

Page Number:
140-146

Corresponding Author:
Punya Patil G M

Abstract:

Counterfeit consumer goods pose significant economic and safety risks worldwide. This paper proposes a robust framework for fake-product identification using QR codes augmented with cryptographic signatures and contextual tamper- detection to provide fast, reliable authentication at point of sale. Each genuine item is assigned a secure, digitally signed QR payload that contains a product identifier, issuance metadata, and a short public-key signature. A lightweight mobile scanning application verifies the signature against a distributed verification service and cross-checks product metadata against an immutable audit log. To detect physical tampering and copied QR images, the system complements cryptographic checks with visual-analysis models that inspect QR placement, surrounding packaging features, and printing artefacts using convolutional neural networks trained on genuine and counterfeit samples. We implement an end-to-end prototype that integrates QR-generation tools, a verification API, and a user-facing mobile client. Experimental evaluation on a curated dataset of packaged products demonstrates that combining cryptographic verification with visual tamper-detection significantly reduces false acceptances compared to signature-only methods. The proposed approach is designed for low-latency field use, scalable deployment across supply chains, and can be adapted to sectors ranging from pharmaceuticals to luxury goods. Future work will explore privacy-preserving ledger options and large-scale pilot deployments.

Keywords: QR code, counterfeit detection, digital signature, tamper detection, mobile authentication, Supply Chain Management, Machine Learning, Python, Django Framework, Consumer Protection.

1. INTRODUCTION

The global counterfeit market has evolved into a sophisticated criminal enterprise, with estimated annual losses exceeding $500 billion worldwide. Counterfeit products not only cause significant economic damage but also pose serious health and safety risks to consumers. Traditional authentication methods including holograms, security inks, and physical inspection have demonstrated limited effectiveness against advanced counterfeiting techniques.

QR (Quick Response) code technology offers a promising alternative due to its high data capacity, error correction capability, and widespread smartphone compatibility. When integrated with secure backend systems, QR codes can serve as digital fingerprints for genuine products, enabling instant verification throughout the supply chain. The integration of blockchain technology further enhances security by creating immutable transaction records and preventing data tampering.

This research presents a holistic approach to product authentication that combines QR code technology with modern web development frameworks and machine learning algorithms. The system is designed to be scalable, cost-effective, and accessible to both businesses and consumers, addressing the critical need for reliable anti-counterfeiting solutions in today's global marketplace.

2. LITERATURE REVIEW AND BACKGROUND

Previous research in product authentication has explored various technological approaches. Beamon [1] established foundational principles for supply chain design, emphasizing the importance of traceability systems. Bechini et al. [2] demonstrated how collaborative e-business technologies can enhance supply chain transparency, while Aung and Chang [3] highlighted the critical role of traceability in food safety and quality control.

The emergence of blockchain technology has revolutionized supply chain management. Gurtu and Johny [4] comprehensively reviewed blockchain's potential in supply chain applications, noting its ability to create transparent and tamperproof records. Chang and Chen [5] systematically analyzed the convergence of blockchain and supply chain management, identifying authentication and traceability as key application areas.

Recent advancements in QR code technology have expanded its applications beyond simple information storage. Modern QR codes can store up to 4,296 alphanumeric characters and incorporate encryption for enhanced security. When combined with smartphone ubiquity (over 6 billion users globally), QR codes present an ideal platform for consumer-facing authentication systems.

3. SYSTEM OBJECTIVES

The proposed system aims to achieve the following objectives:

A. Primary Objectives

- Develop a scalable QR code-based authentication framework capable of handling high-volume product verification
- Implement robust encryption and security measures to prevent code replication and tampering
- Create an intuitive user interface accessible to consumers with varying technical proficiency
- Establish real-time monitoring and alert systems for suspicious activity detection

B. Secondary Objectives

- Integrate machine learning algorithms for pattern recognition and anomaly detection
- Develop comprehensive analytics dashboard for brand protection teams
- Ensure cross-platform compatibility across iOS and Android devices
- Maintain cost-effectiveness for small and medium enterprises

4. SYSTEM ARCHITECTURE AND DESIGN

The proposed system employs a three-tier architecture comprising presentation, application, and data layers.

A. System Components

1) QR Code Generation Module: This module utilizes Python's qrcode library with the following enhanced features:

- Dynamic QR code generation with unique product identifiers
- AES-256 encryption for sensitive product information
- Error correction levels adjustable based on packaging requirements
- Batch generation capabilities for mass production environments

2) Authentication Engine: The core verification system implements multiple validation checks:

- Database lookup for product existence and status
- Geographic validation against expected distribution regions
- Temporal analysis of scan patterns and frequencies
- Machine learning-based anomaly detection

3) User Interface Layer: A responsive web interface built with Bootstrap 4 provides:

- Mobile-optimized scanning interface
- Multi-language support for global deployment
- Accessibility features for visually impaired users

- Offline functionality for areas with limited connectivity

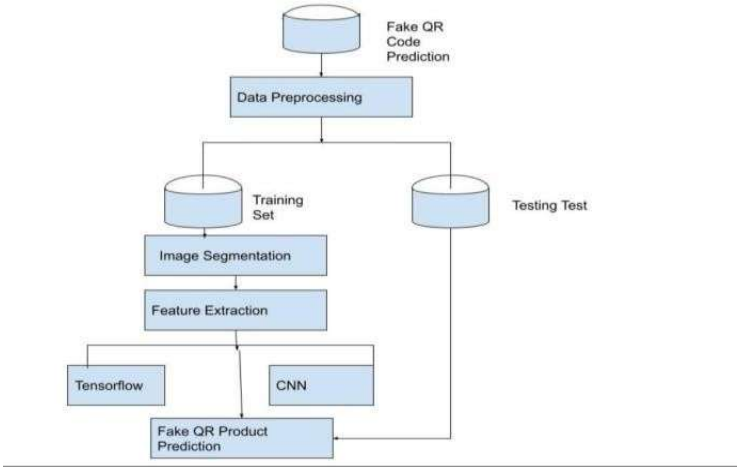

Fig. 1. Comprehensive System Architecture Diagram

5. IMPLEMENTATION METHODOLOGY

A. Technology Stack

1) Backend Development: The system utilizes Django 3.2 with the following key components:

- Django REST Framework for API development
- SQLite database for development and testing
- PostgreSQL for production deployment
- Celery for asynchronous task processing
- Redis for caching and session management

2) Frontend Development: The user interface employs modern web technologies:

- HTML5 with responsive CSS3 design
- JavaScript ES6+ for client-side processing
- Bootstrap 4 framework for consistent styling
- Chart.js for analytics visualization
- Progressive Web App (PWA) capabilities

MACHINE LEARNING INTEGRATION

The system incorporates machine learning for advanced counterfeit detection:

B. Anomaly Detection

A Random Forest classifier analyzes scan patterns to identify suspicious activities:

- Unusual geographic scan locations
- Abnormal scan frequency patterns
- Multiple scans from identical devices
- Time-based anomaly detection

C. Predictive Analytics

The system employs time-series analysis to predict potential counterfeit outbreaks based on historical data and market trends.

6. SYSTEM REQUIREMENTS

A. Hardware Specifications

- Server Requirements: 8GB RAM minimum, 1TB SSD storage, Intel Xeon processor
- Client Requirements: Smartphone with camera, 2GB RAM, iOS 12+ or Android 8+
- Network Requirements: Minimum 10Mbps internet connection

B. Software Requirements

- Backend: Python 3.8+, Django 3.2+, PostgreSQL 12+
- Frontend: Bootstrap 4, JavaScript ES6+, HTML5/CSS3
- Development: PyCharm IDE, Git version control, Docker
- Deployment: Nginx, Gunicorn, Ubuntu Server 20.04 LTS
- Strengthened intellectual property protection frameworks
- Improved regulatory compliance and monitoring capabilities

7. CHALLENGES AND LIMITATIONS

A. Technical Challenges

- QR code durability and readability in various environmental conditions
- System scalability for high-volume manufacturing operations
- Security concerns regarding database protection and encryption key management

- Integration complexity with existing enterprise resource planning systems

B. Adoption Challenges

- Consumer education and awareness campaigns
- Cost considerations for small-scale manufacturers
- Regulatory compliance across different jurisdictions
- Standardization issues across industry sectors

8. CONCLUSION AND FUTURE WORK

The proposed QR code-based authentication system represents a significant advancement in anti-counterfeiting technology. By leveraging widely available smartphone technology and robust backend systems, it provides a practical solution to the global counterfeit problem. The system's scalability, cost- effectiveness, and user-friendly design make it suitable for deployment across various industries and market segments. Future research directions include:

- Integration with IoT devices for enhanced supply chain monitoring
- Blockchain implementation for decentralized verification
- Advanced machine learning models for predictive counterfeit detection
- Expansion to emerging markets with customized deployment strategies
- Development of industry-specific customization frameworks

The continued evolution of QR code technology, combined with advancements in artificial intelligence and blockchain, promises even more sophisticated authentication solutions in the future.

ACKNOWLEDGMENT

The authors gratefully acknowledge the support provided by GM University, Davanagere, and the valuable insights from industry partners in developing this research.

References

[1] B. M. Beamon, "Supply chain design and analysis: Models and methods," *International Journal of Production Economics*, vol. 55, no. 3, pp. 281–294,1998.

[2] A. Bechini, M. G. Cimino, F. Marcelloni, and A. Tomasi, ”Patterns and technologies for enabling supply chain traceability through collaborative e-

business,” *Information and Software Technology*, vol. 50, no. 4, pp. 342–359, 2008.

[3] M. M. Aung and Y. S. Chang, ”Traceability in a food supply chain: Safety and quality perspectives,” *Food Control*, vol. 39, pp. 172–184, 2014.

[4] A. Gurtu and J. Johny, ”Potential of blockchain technology in supply chain management: a literature review,” *International Journal of Physical Distribution & Logistics Management*, vol. 49, no. 9,pp. 881–900, 2019.

[5] S. E. Chang and Y. Chen, ”When blockchain meets supply chain: A systematic literature review on current development and potential applications,” *IEEE Access*, vol. 8, pp. 62478–62494, 2020.

[6] S. Jiang et al., ”BioCHIE: A blockchain-based platform for healthcare information exchange,” in *Proc. IEEE Int. Conf. Smart Computing (SMART- COMP)*, 2018, pp. 49–56.

[7] S. F. Wamba and M. M. Queiroz, ”Blockchain in operations and supply chain management: Benefits, challenges and future research opportunities,” *Int. J. Information Management*, vol. 52, p. 102064, 2020.