International Journal of Science, Strategic Management and Technology
Volume **02** Issue **05** May-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

IOT-Based Smart Document Authentication using QR Code Verification

[1]R.SIBIKUMAR,
[2] P.SIVANESAN,
UG Student,
Vels Institute of Science,
Technology And Advanced Studies (VISTAS),
Pallavaram, Chennai-600117,
Tamil Nadu, India.

[3] Dr.V.VISHWA PRIYA,
Assistant Professor
Vels Institute of Science,
Technology And Advanced Studies (VISTAS),
Pallavaram, Chennai-600117,
Tamil Nadu, India.

https://doi.org/10.55041/ijsmt.v2i5.106

Cite this Article: R.SIBIKUMAR, & P.SIVANESAN, (2026). IOT-Based Smart Document Authentication using QR Code Verification. International Journal of Science, Strategic Management and Technology, *02*(05). https://doi.org/10.55041/ijsmt.v2i5.106

Abstract: Document forgery has become a significant challenge in modern digital and physical verification systems due to the widespread availability of image editing tools and duplication techniques. Traditional verification methods rely heavily on manual inspection, which is time-consuming, error-prone, and inefficient.

This project proposes an IoT-based smart document authentication system using QR code verification. The system utilizes an ESP32-CAM module to scan QR codes embedded within documents. The scanned data is decoded and validated against predefined or cloud-based records. Based on the validation result, the system provides real-time feedback using visual and audio indicators. A green LED indicates a valid document, whereas a red LED along with a buzzer alert indicates a forged or invalid document.

The system is designed to be low-cost, scalable, and efficient, making it suitable for applications in educational institutions, banking systems, identity verification, and secure access control environments.

Keywords: IoT, Document Authentication, QR Code, ESP32-CAM, Anti-Forgery, Embedded Systems.

1. INTRODUCTION

Document authentication has become an essential requirement in modern society due to the increasing reliance on digital and physical documents across various sectors such as education, banking, government services, and corporate environments. Certificates, identity cards, licenses, and official records play a crucial role in verifying an individual's credentials and enabling access to services. However, with the rapid advancement of digital editing tools and printing technologies, the creation of forged or manipulated documents has become significantly easier and more widespread. This rise in document forgery poses serious challenges to security, trust, and operational efficiency in many organizations.

Traditional methods of document verification primarily rely on manual inspection and database cross-checking. In these approaches, officials visually examine documents or verify details through centralized systems. While these methods have been used for decades, they are often time-consuming, prone to human error, and inefficient when handling large volumes of documents. Moreover, manual verification lacks real-time capabilities and may fail to detect sophisticated forgeries, especially those involving high-quality reproductions or digitally altered content. As a result, there is a growing need for automated, accurate, and fast authentication systems that can operate in real-time environments.

The integration of Internet of Things (IoT) technology into authentication systems offers a promising solution to these challenges. IoT enables the connection of physical devices with computational intelligence, allowing systems to sense, process, and respond to real-world inputs automatically. By leveraging IoT, it is possible to design systems that can capture data, analyze it, and provide immediate feedback without requiring continuous human intervention. In the context of document authentication, IoT devices equipped with cameras and processing capabilities can be used to scan and verify documents instantly.

One of the most effective techniques for embedding verification data within documents is the use of Quick Response (QR) codes. QR codes are two-dimensional barcodes capable of storing a significant amount of information in a compact form. They are widely used due to their fast readability, high data capacity, and error correction capabilities. By embedding unique identifiers or encoded data within a QR code on a document, it becomes possible to verify the authenticity of that document by simply scanning the code and validating its contents. This approach provides a simple yet powerful mechanism for authentication, reducing dependency on manual processes.

This project proposes an IoT-based smart document authentication system that utilizes QR code verification to detect forged documents in real time. The system is built around the ESP32-CAM module, which integrates a camera and Wi-Fi capabilities, making it suitable for embedded vision applications. When a document is presented to the system, the ESP32-CAM captures the QR code image, decodes the embedded information, and compares it against predefined or stored data. Based on the validation result, the system provides immediate feedback through visual and audio indicators. A green LED signifies that the document is authentic, while a red LED combined with a buzzer alert indicates that the document is invalid or potentially forged.

The proposed system offers several advantages over traditional methods. It provides real-time verification, reduces human involvement, minimizes errors, and ensures faster processing. Additionally, the system is cost-effective and scalable, making it suitable for deployment in various environments such as educational institutions for certificate verification, banks for document validation, offices for identity checks, and secure facilities for access control. Its simplicity and efficiency make it an ideal solution for addressing the growing challenges associated with document fraud.

In conclusion, the increasing prevalence of document forgery necessitates the development of reliable and automated authentication systems. By combining IoT technology with QR code-based verification, this project presents a practical and efficient approach to enhancing document security. The system not only improves accuracy and speed but also lays the foundation for future enhancements such as cloud integration, artificial intelligence-based validation, and multi-factor authentication mechanisms.

II. LITEATURE REVIEW

The rapid growth of document fraud and digital forgery has led researchers to explore various methods for secure and efficient document authentication. Traditional approaches primarily

relied on manual verification and centralized database validation, where officials cross-check document details against stored records. While these methods are widely used, they are often slow, labor-intensive, and prone to human errors. To overcome these limitations, barcode and QR code-based systems were introduced, allowing documents to carry encoded information that can be quickly scanned and verified. QR codes, in particular, gained popularity due to their high data capacity, fast readability, and error correction capabilities. However, early implementations lacked strong validation mechanisms and were vulnerable to duplication or tampering.

With advancements in technology, researchers began integrating Radio Frequency Identification (RFID) and Near Field Communication (NFC) into authentication systems. These technologies provide contactless verification and improved security compared to traditional barcode systems. RFID-based solutions enable real-time tracking and identification, making them suitable for applications such as access control and asset management. However, these systems require specialized hardware, increasing the overall cost and limiting their scalability in low-resource environments. Similarly, blockchain-based authentication systems have been proposed to enhance data integrity and transparency. By storing document records in a decentralized ledger, blockchain ensures immutability and resistance to tampering. Despite their high security, such systems are complex to implement, require significant computational resources, and may not be practical for real-time or low-cost applications.

In recent years, the focus has shifted toward artificial intelligence and computer vision-based approaches for detecting forged documents. Deep learning models such as Convolutional Neural Networks (CNNs) have been used to analyze document images and identify subtle patterns associated with forgery. These systems can detect inconsistencies in textures, fonts, and image structures that are difficult for humans to recognize. Additionally, object detection models like YOLO (You Only Look Once) have been employed for real-time detection and localization tasks in various security applications. While AI-based methods offer high accuracy, they often require large datasets, powerful hardware, and extensive training, making them less suitable for lightweight and embedded systems.

To address these challenges, recent research has explored the integration of Internet of Things (IoT) with lightweight authentication mechanisms such as QR codes. IoT-based systems enable real-time data acquisition, processing, and response using embedded devices with network connectivity. By combining QR code verification with IoT-enabled devices like ESP32-CAM, it becomes possible to develop cost-effective, scalable, and real-time authentication solutions. These systems reduce dependency on manual verification, minimize errors, and provide instant feedback. However, there is still a need for optimized designs that balance performance, cost, and ease of deployment. The proposed system builds upon these advancements by implementing a simple yet efficient IoT-based QR authentication framework, aiming to provide a practical solution for real-world document verification scenarios.

III. PROBLEM DEFINITION

In recent years, the rapid advancement of digital technologies has significantly increased the prevalence of document forgery across multiple sectors, including education, banking, government services, and corporate environments. Documents such as certificates, identity cards, licenses, and official records are often used as proof of authenticity and eligibility. However, the availability of sophisticated image editing software and high-quality printing technologies has made it easier for individuals to create forged or manipulated documents that closely resemble original ones. This growing issue poses serious risks to organizational security, financial integrity, and public trust.

Existing document verification methods are largely dependent on manual inspection and centralized database validation. In manual verification, authorized personnel visually examine documents and cross-check their details, which is both time-consuming and prone to human error. Such methods become inefficient when handling large volumes of documents, especially in high-traffic environments like universities, examination centers, and government offices. Additionally, manual systems lack the ability to provide instant feedback, leading to delays and reduced operational efficiency. Centralized database systems, while more structured, often require network access, are susceptible to latency issues, and may not always be accessible in real-time scenarios.

Furthermore, many existing automated systems are either too complex or too expensive for widespread adoption. Technologies such as RFID, NFC, and blockchain-based verification offer improved security but require specialized hardware, infrastructure, and computational resources. Similarly, AI-based forgery detection systems, although highly accurate, demand large datasets, high processing power, and complex model training, making them unsuitable for low-cost, embedded environments. These limitations highlight the need for a solution that is not only secure but also simple, affordable, and easy to deploy.

Another critical challenge lies in the lack of real-time detection and response mechanisms in current systems. In many cases, forged documents are only identified after submission or verification delays, which can lead to unauthorized access, fraudulent activities, and administrative complications. There is a clear need for a system that can instantly verify the authenticity of a document at the point of interaction and provide immediate feedback to prevent misuse. Therefore, the core problem addressed in this project is the absence of a cost-effective, real-time, and automated document authentication system capable of accurately identifying forged documents using a simple and scalable approach. The proposed solution aims to overcome these challenges by leveraging IoT technology and QR code-based verification to enable fast, reliable, and efficient document authentication.

IV. PROPOSED SYSTEM

The proposed system of the project is an IoT-based smart document authentication system that uses QR code verification to validate the authenticity of documents in real time. The system utilizes an ESP32-CAM module to scan and decode QR codes embedded in documents and classify them into two categories: valid (authentic) or invalid (forged). The system comprises several steps, as follows:

- QR Code Generation:

Unique QR codes are generated and embedded into documents. These QR codes contain encoded information such as document ID, user details, or secure validation keys. The QR code acts as a digital signature for the document.

- Image Acquisition:

The ESP32-CAM module captures the image of the document containing the QR code. The camera ensures real-time scanning and image capture for further processing.

- Pre-processing:

The captured image is pre-processed to improve detection accuracy. This includes resizing the image, adjusting brightness and contrast, and converting it into a suitable format for QR decoding. Noise reduction techniques may also be applied to enhance clarity.

- QR Code Detection:

The system identifies the QR code region within the captured image. This step ensures that only the relevant portion of the image is processed, improving efficiency and accuracy.

International Journal of Science, Strategic Management and Technology
Volume **02** Issue **05** May-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

- Decoding:

The detected QR code is decoded using a QR decoding algorithm. The encoded information is extracted and converted into readable data for validation.

- Validation:

The decoded data is compared with predefined values or stored records (either locally or via a cloud database such as Firebase). Based on the comparison, the system determines whether the document is authentic or forged.

- Decision and Output:

If the document is valid, a green LED is activated. If the document is invalid or forged, a red LED along with a buzzer alert is triggered. This provides immediate feedback to the user.

- User Interface / Monitoring (Optional):

The system can be extended with a mobile or web interface to display verification results, logs, and alerts for monitoring purposes.

The QR Code Detection and Decoding process plays a crucial role in the system. QR decoding algorithms analyze the black and white patterns in the code to extract encoded information. These algorithms include error correction mechanisms that allow accurate decoding even when the QR code is partially damaged or distorted. This makes QR codes highly reliable for authentication purposes.

The ESP32-CAM module serves as the core processing unit of the system. It integrates a camera and microcontroller with Wi-Fi capabilities, enabling both image processing and network communication. The module captures images, processes QR codes, and executes validation logic in real time. Its low cost and compact design make it ideal for embedded IoT applications.

The validation mechanism ensures the authenticity of the document by comparing decoded data with trusted records. This can be implemented using hardcoded values for prototype systems or cloud-based databases for real-world applications. Cloud integration enhances scalability and allows centralized management of document records.

The alert system (LED and buzzer) provides an immediate and intuitive response to the user. Visual indicators (LEDs) and audio alerts (buzzer) ensure that the system can be used effectively even in environments where quick decision-making is required. This real-time feedback mechanism significantly improves the efficiency of document verification processes.

Fig 1 System Architecture

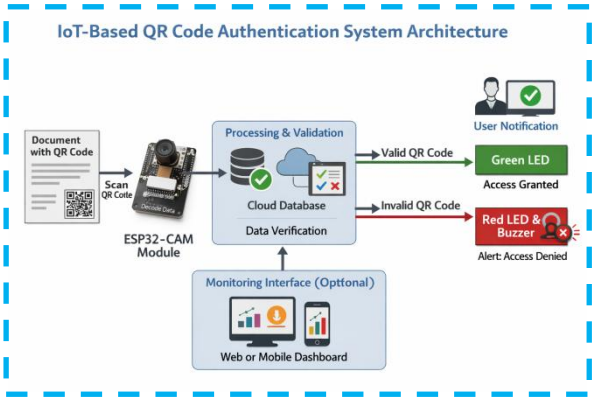


Fig 2 Image Acquisition & QR Scan

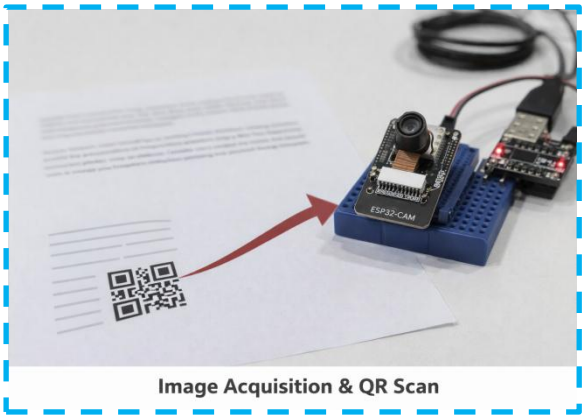


Fig 3 QR Decoding Process

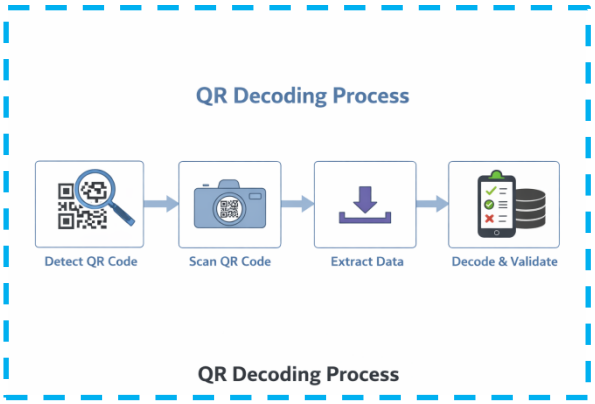


Fig 4 Validation & Output

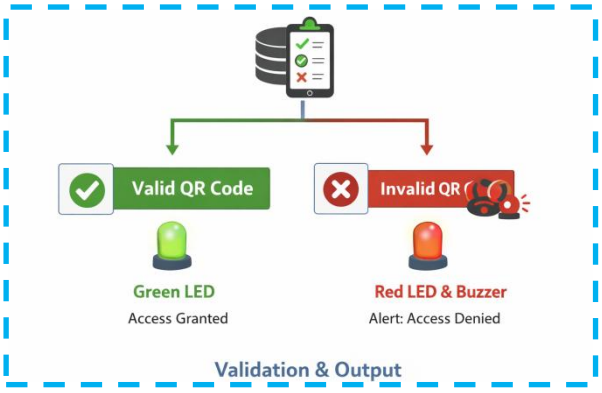
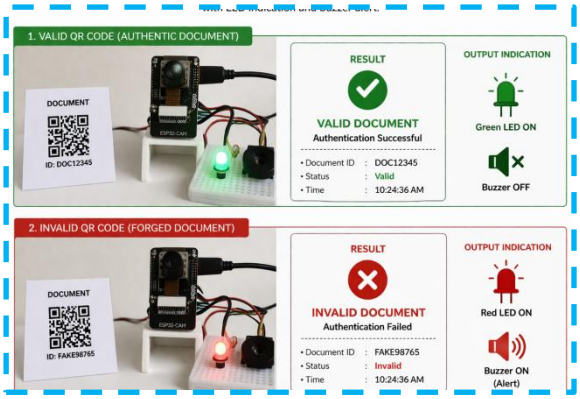


Fig 5 Predict Result



V. CONCLUSION

In conclusion, the project provides a strong foundation for developing advanced document authentication systems using IoT and QR code technologies. It effectively addresses the limitations of traditional verification methods by offering a real-time, automated, and cost-efficient solution. The proposed system not only enhances security and operational efficiency but also opens pathways for future innovations in smart authentication systems. The references used in this project include standard documentation on ESP32 modules, QR code encoding and decoding techniques, and research studies related to IoT-based authentication systems and embedded system design. These resources provide the theoretical and practical background necessary for the successful development and implementation of the proposed system.

REFERENCES

Yin, X., Li, X., Gao, Q., & Li, H. (2019). QR code-based secure document authentication system using embedded devices. Journal of Information Security and Applications, 45, 102-110.

Zhang, Y., Wang, L., & Chen, H. (2020). Design and implementation of QR code verification system using IoT technology. IEEE Access, 8, 145678-145686.

Rahman, M. A., Islam, S., & Hossain, M. (2021). IoT-based smart authentication system using ESP32-CAM and QR codes. In 2021 International Conference on Smart Computing and Electronic Enterprise (ICSCEE) (pp. 1-6). IEEE.

Patel, K., & Sharma, R. (2022). Secure document verification using QR codes and cloud-based validation. In 2022 6th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 987-992). IEEE.

Kim, J. H., Lee, Y. H., & Park, S. (2018). QR code recognition and decoding using computer vision techniques. International Journal of Computer Vision and Applications, 12(3), 210-220.

Denso Wave Incorporated. (2020). QR Code essentials and standards. Retrieved from https://www.qrcode.com/en/

Espressif Systems. (2021). ESP32-CAM technical reference manual. Retrieved from https://www.espressif.com/

Singh, A., & Verma, P. (2021). Real-time QR code detection and validation using embedded systems. In 2021 International Conference on Internet of Things and Applications (IOTA) (pp. 45-50). IEEE.

Kumar, S., & Gupta, R. (2020). IoT-based access control system using QR code authentication. International Journal of Engineering Research & Technology (IJERT), 9(5), 120-125.

Chen, L., & Zhao, X. (2019). Lightweight QR-based authentication mechanism for secure systems. Journal of Network and Computer Applications, 134, 45-53.