

# A Study of Secure Authentication Techniques Using QR Code and Biometric Verification

Prof. Dr. Neelam Kumar<sup>1</sup>, Anjali Siraskar<sup>2</sup>, Arti Kulkarni<sup>3</sup>, Snehal Shivale<sup>4</sup>, Srushti Jadhav<sup>5</sup>

<sup>1</sup>(Professor, SRCOE, Department of Computer Engineering Pune)

<sup>2,3,4,5</sup>(Student, SRCOE, Department of Computer Engineering Pune)

---

**Abstract:** Ensuring secure and reliable student authentication during examinations remains a critical challenge in academic institutions, where manual verification processes are prone to impersonation, data errors, and administrative inefficiencies. This paper presents a comprehensive study and design of a dual-layer authentication framework that integrates Quick Response (QR) code technology with biometric fingerprint verification to enhance examination integrity. We analyze the fundamental limitations of traditional examination control systems and focus our framework on two core authentication mechanisms: (1) QR code-based identification, for its ability to encode unique student and examination data, enabling fast and contactless verification; and (2) fingerprint recognition, for its precision in validating physical identity and preventing proxy attendance. The proposed system architecture encompasses three primary modules—QR code generation and encryption (via Advanced Encryption Standard, AES), biometric enrollment and verification, and database management—implemented using Python and MySQL within a hybrid web-mobile environment. The integration of these modules enables a robust, scalable, and real-time verification process. Preliminary design evaluations demonstrate that combining QR and fingerprint technologies significantly improves verification accuracy, reduces entry delays, and strengthens institutional security. Future extensions will explore the incorporation of blockchain for tamper-proof audit trails and AI-based anomaly detection to further enhance reliability. By automating the examination authentication process, the proposed model provides an efficient, cost-effective, and secure solution adaptable to modern educational ecosystems.

**Key Word:** QR code, biometric verification, AES encryption, student identification, secure access, blockchain integration.

---

## I. Introduction

Maintaining the integrity of examinations is a critical challenge in modern evaluation systems. Traditional methods of candidate verification—such as manual ID checks and attendance marking—are prone to human error, impersonation, and administrative inefficiencies. These challenges often result in delays as invigilators manually cross-check identification documents, verify examination entries, and resolve mismatched records. Such time-consuming processes reduce operational efficiency, increase the workload on staff, and leave examination systems vulnerable to fraud and unauthorized access.

With advancements in digital authentication, Quick Response (QR) code technology and biometric verification systems have emerged as reliable tools for identity management. QR codes provide a convenient and cost-effective method of encoding candidate-specific data, enabling instant verification through scanning devices. On the other hand, biometric fingerprint verification ensures accuracy by validating a candidate's unique physiological traits, thereby preventing proxy participation or fraudulent entries. Integrating these two approaches results in a multi-factor authentication mechanism that combines digital data verification with biometric validation for enhanced security and transparency.

Over the years, several digital authentication models have been developed to improve examination security. QR-based systems focus on generating encrypted codes that can be verified through mobile or web platforms, while biometric-based systems emphasize physical verification using fingerprints, facial features, or iris recognition. Although both technologies independently strengthen authentication, systems relying on a single method remain vulnerable to duplication, spoofing, or data manipulation.

To address these limitations, this study proposes a dual-layer examination authentication framework that integrates QR code encryption (secured using the Advanced Encryption Standard, AES) with biometric fingerprint verification. The proposed system design is adaptable for various examination environments offering flexibility, scalability, and enhanced identity assurance, and a cross-platform mobile application for real-time verification at examination checkpoints. This hybrid model establishes a secure, efficient, and transparent foundation for next-generation examination management systems.

---

## II. Literature Review

A Review on Authentication by Embedding Biometrics in QR Codes by Chaudhari A.Y., Kulkarni J., Ghorpade A., Sakore S., Dube U., Gupta A.K. (2024) explored the fusion of QR code technology with biometric authentication. The authors argued that embedding biometric templates into encrypted QR codes addresses weaknesses of password-based systems and reduces reliance on static codes. Their analysis highlighted the need for cryptographic protection of QR data and discussed how combining QR scanning with biometric validation can simplify user verification while enhancing security. [1]

QR code-based two-factor authentication to verify paper-based documents by Naser M.A., Jasim E.T., Al-Mashhadi H.M. (2023) examined using QR codes combined with cryptographic hashes to verify the authenticity of printed documents. The study showed that applying two-factor authentication (QR + hash verification) could reduce document forgery and unauthorized access. The findings reinforce the potential of QR-based systems for identity and access control beyond conventional environments. [2]

Comprehensive Survey: Biometric User Authentication Application, Evaluation, and Discussion by Alrawili R., AlQahtani A.A.S., Khan M.K. (2023) conducted a broad review of biometric traits, performance metrics, and attack vectors across authentication systems. They reviewed physiological (fingerprint, iris) and behavioural modalities, discussed challenges such as spoofing and template protection, and highlighted how biometric systems must be paired with other factors (e.g., tokens) to improve robustness. This survey provides useful background on general biometric system design and evaluation.. [3]

Iris Liveness Detection for Biometric Authentication: A Systematic Literature Review and Future Directions by Khade S., Ahirrao S., Phansalkar S., Kotecha K., Gite S., Thepade S.D. (2021) reviewed methods for detecting fake biometric inputs (e.g., printed iris images or masks) in iris recognition systems. Although focused on iris, the work is relevant for assessing vulnerabilities in biometric verification. The authors emphasized that biometric systems on their own face risks of presentation attacks and need complementary mechanisms (such as secure tokens or codes) to strengthen authentication. [4]

Encryption and encoding of facial images into quick response and high capacity color 2D code for biometric passport security system by Choudhury Z.H. (2022) explored embedding biometric data (facial image, hand geometry) into color QR codes for passport security. The study used AES and SHA-256 encryption to secure biometric and personal data embedded in the code. The approach demonstrated how QR codes can serve as carriers of encrypted biometric identifiers, which can then be scanned and validated at checkpoints. [5]

Dommari, Sandeep, & Mishra, Rupesh Kumar in the paper “*The Role of Biometric Authentication in Securing Personal and Corporate Digital Identities*” (2024) discussed how biometric-based multi-factor authentication enhances security for digital identities. They reviewed modalities like fingerprint and facial recognition, addressing how biometric data provides stronger protection than PINs or passwords, especially when used in combination with other authentication methods.[6]

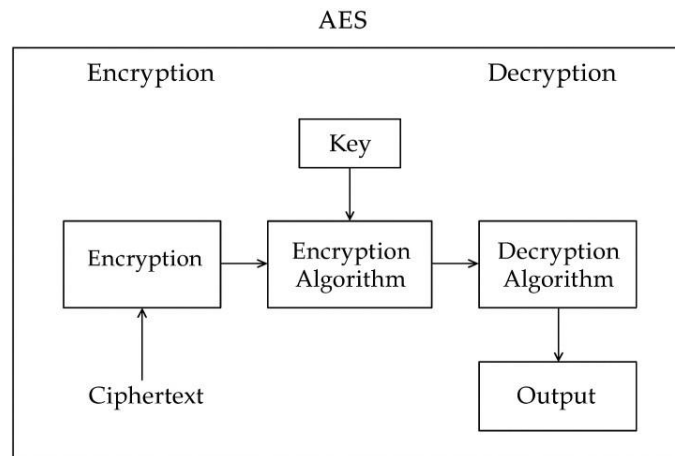
R. Sawant, M. Kirve, C. Dusunge, K. Dhotre, S. Pede in the paper “*Multi-Layered Security by Embedding Biometrics in Quick Response (QR) Codes*” (2022) presented a design in which user fingerprint data and identity metadata are embedded within a QR code. The authentication process then verifies the scanned fingerprint against the QR-contained biometric template, requiring a full match for successful authentication.[7]

## III. Algorithm

### 1. AES (Advanced Encryption Standard) – For Securing QR Data

Even though the QR is printed, it must not reveal student details in plain text (for example, scanning with any random app)

AES ensures the QR data is readable only by your verification app — not by outsiders.



**Fig 1.0 :- Diagram for Algorithm AES**

**Working and Process**

1. System takes student data.
2. Encrypt this using AES with a secret key known only to verification app.
3. Encode the encrypted text as a QR code.
4. During scanning, the app decrypts using the same AES key to get the original data

**Advantages**

- **High Security:** AES uses substitution–permutation network (SPN) operations across multiple rounds (10, 12, or 14), making it resistant to brute-force and differential attacks. With 128-, 192-, or 256-bit key sizes, AES provides strong encryption suitable for sensitive student and examination data.
- **Confidentiality and Data Integrity:**By encrypting student details within the QR code, the information remains unreadable to unauthorized scanners or malicious apps.

**Disadvantages**

- **Key Management Complexity:** AES relies on a shared secret key; if the key is leaked, all encrypted QR codes can be decrypted. Proper key rotation and secure storage mechanisms (like HSM or server vault) are required.
- **Vulnerability to Implementation Errors:** Incorrect padding schemes or improper key handling can make AES vulnerable to padding-oracle or side-channel attacks.

**Limitations**

- Static (printed) QR cannot be changed once printed.
- If hall ticket is photocopied, QR will still scan — hence use extra hash or biometric for authenticity.

**2. SHA-256 (Secure Hash Algorithm 256-bit) – For Data Integrity Verification**

SHA-256 is a cryptographic hash function that converts any input message into a fixed 256-bit (64-character) hash value. It is a one-way function — meaning the original data cannot be derived from the hash — making it ideal for verifying data integrity.

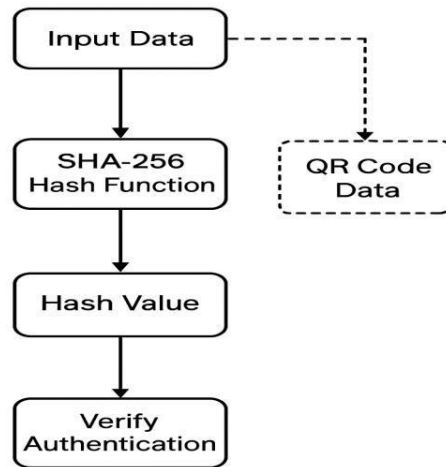


Fig 2.0 :- Diagram for Algorithm SHA

### Working and Process

1. **Input:** The plaintext data (e.g., student details) is fed into the SHA-256 algorithm.
2. **Preprocessing:**
  - The data is padded to ensure its length is a multiple of 512 bits.
  - A 64-bit representation of the original message length is appended.
3. **Initialization:** Eight 32-bit constants (H0–H7) are used as initial hash values.
4. **Message Processing:**
  - The input is divided into 512-bit chunks.
  - Each chunk undergoes 64 rounds of bitwise operations: *Logical AND, OR, XOR, rotations, and modular additions.*
  - Each round updates the intermediate hash values based on a set of pre-defined constants (K0–K63).

### Advantages

- **Strong Data Integrity Verification:** SHA-256 generates a unique 256-bit hash for any input; even a one-bit modification in data produces a completely different hash (avalanche effect).
- **Collision Resistance:** The probability that two different inputs produce the same hash is extremely low ( $\approx 1$  in  $2^{256}$ ), ensuring authenticity of QR code data.
- **Integrity Check for Encrypted Data:** When combined with AES, SHA-256 can verify that encrypted QR data has not been altered or reprinted illegally.

### Disadvantages

- **No Encryption Capability:** SHA-256 only verifies integrity; it cannot hide or encrypt data. It must be used alongside **Fixed Output Size:** AES or other ciphers for full protection.
- Regardless of input length, the 256-bit output may require extra handling for very large or structured datasets.

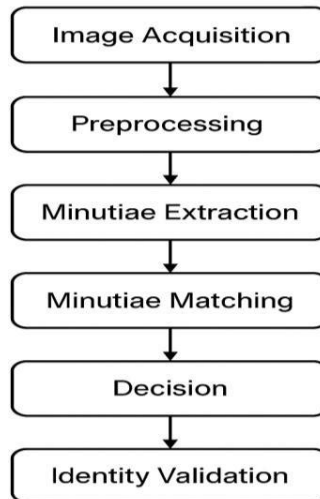
### Limitations

- Matching large fingerprint databases increases computation time.
- Cannot identify the source or user; it only detects data changes.

### 3. Minutiae-Based Fingerprint Matching – For Biometric Authentication

The Minutiae-based fingerprint matching algorithm is one of the most reliable biometric identification methods.

It works by analyzing small distinctive features in fingerprint patterns — known as minutiae points — such as ridge endings and bifurcations.



**Fig 3.0 :- Diagram for Algorithm Minutiae-Based Fingerprint Matching**

#### Working and Process

1. **Image Acquisition:** The user's fingerprint is captured using a digital scanner.
2. **Preprocessing:**
  - Enhancement: Filters remove noise and clarify ridge lines.
  - Binarization: Converts grayscale image to binary form (ridges = 1, valleys = 0).
  - Thinning: Reduces ridges to single-pixel width for precise analysis.
3. **Minutiae:** The algorithm identifies ridge endings and bifurcations and stores their coordinates and angles. Example data: Minutiae = [(x1, y1, θ1), (x2, y2, θ2), ...]
4. **Template Creation:** These minutiae points are stored in a secure, encrypted database as a "template."
5. **Matching:** During verification, a live fingerprint is scanned and its minutiae extracted. The system computes a matching score (S) based on the overlap of spatial positions and orientations. Formula:  $S = (\text{Matched\_Points} / \text{Total\_Points}) \times 100\%$
6. **Decision:** If  $S \geq$  threshold (e.g., 80%), the fingerprint is accepted; otherwise, rejected.

#### Advantages

- **High Accuracy and Uniqueness:** Fingerprints are biologically unique; the chance of two individuals sharing the same minutiae pattern is almost zero. This provides a strong assurance that the person presenting the hall ticket is genuine.
- **Difficult to Forge:** Physical fingerprint replication requires advanced equipment, making impersonation virtually impossible.

#### Disadvantages

- **Hardware Dependency:** Requires fingerprint scanners or sensors, increasing project cost and setup complexity.
- **Image Quality Sensitivity:** Accuracy drops with dry, wet, or worn fingerprints. Dust, lighting, or sensor noise can affect minutiae detection.

#### Limitations

- Ineffective for users with damaged or faded fingerprints.
- Requires strong encryption for stored biometric templates to prevent misuse.
- May need recalibration or retraining of sensors over time.

#### IV. COMPARATIVE STUDY OF ALGORITHMS

Category	Algorithm 1	Algorithm 2	Algorithm 3	Best Algorithm (From Study) & Reason
Encryption	AES – Fast, secure, lightweight.	RSA– Strong but slow.	ECC-Compact but complex.	AES – Offers high speed and strong encryption, best for secure QR code generation.
Hashing / Integrity	MD5 – Weak, collision-prone.	SHA-1– Moderate, deprecated.	SHA-256– Secure, efficient.	SHA-256 – Provides robust data integrity and smooth integration with AES.
Biometric Verification	Fingerprint (Minutiae)– Accurate, low cost.	Pattern Recognition – Moderate accuracy.	Iris Scan– Precise but costly.	Fingerprint Minutiae – Reliable, accessible, and ideal for identity verification.

#### V. Applications

- **Examination Management Systems:** The proposed framework can be integrated into examination platforms of schools, universities, competitive testing agencies, and online certification bodies to ensure secure and tamper-proof student authentication. By replacing manual ID checks with QR-based and biometric validation, it eliminates impersonation and enhances operational efficiency.
- **Institutional Identity Verification:** Educational and training institutions can deploy this system for identity verification at various checkpoints such as exam halls, laboratory access, library entry, and hostel management, reducing administrative burden while maintaining transparency.
- **Event and Conference Security:** The hybrid QR-biometric authentication model can be adapted for verifying participants in conferences, seminars, or job recruitment drives, ensuring that only authorized individuals gain access to restricted venues.
- **Digital Certification and Document Validation:** The QR encryption and hashing mechanism can be extended to secure degree certificates, transcripts, and digital credentials. Encrypted QR codes on official documents allow instant online or offline verification of authenticity.
- **Attendance and Access Control Systems:** Mitigation Beyond examinations, this authentication mechanism can be used for daily attendance tracking in educational or corporate environments, providing accurate time-stamped logs and eliminating proxy attendance.

#### VI. Conclusion

This Phase-1 study analyzed various cryptographic and biometric authentication techniques to identify the most reliable combination for secure identity verification. Through comparative evaluation, AES encryption (for confidentiality), SHA-256 hashing (for integrity), and minutiae-based fingerprint matching (for authenticity) were found to be the most balanced and effective techniques among those studied. The research concludes that multi-factor authentication—integrating both digital and biometric methods—offers a strong foundation for building next-generation identity verification systems. In Phase-2, the focus will shift to practical implementation, system modeling, and performance evaluation of these algorithms in real-time authentication environment.

## VII. References

- [1] J.A. Inyangetoh and E.A. Johnson, "Development of QR Code-Based Authentication System for Admitting Students into Examination Hall for Polytechnics in Nigeria," *European Journal of Computer Science & Information Technology*, vol. 13, no. 3, pp. 20–42, 2025. DOI: 10.37745/ejcsit.2013/vol13n32042.
- [2] D. Mwambeleko, "QR Code and Fingerprint Systems for University Examinations Management," *International Journal of Advances in Scientific Research Engineering (IJASRE)*, vol. 9, no. 12, pp. 37–48, 2024.
- [3] V. Kulkarni, M. Waghmare, S. Gund, and D.B. Shivpuje, "Fingerprint Based Exam Hall Authentication," *International Research Journal of Engineering and Technology (IRJET)*, vol. 7, issue 5, May 2020.
- [4] B. Muthukumar, A. Mayan, G. Nambiar et al., "QR Code and Biometric Based Authentication System for Trains," *IOP Conference Series: Materials Science and Engineering*, vol. 590, 2019, Art. no. 012010.
- [5] T. Bhuvaneswari, "Fingerprint Exam Hall Authentication System," *ADBU Journal of Engineering Technology (AJET)*, 2022.
- [6] R. Alrawili, A.A.S. AlQahtani, and M.K. Khan, "Comprehensive Survey: Biometric User Authentication Application, Evaluation and Review," *arXiv preprint*, arXiv:2311.13416v2, 2023.
- [7] C. Benegui and R.T. Ionescu, "Improving the Authentication with Built-in Camera Protocol Using Built-in Motion Sensors: A Deep Learning Solution," *arXiv preprint*, arXiv:2107.10536, 2021.
- [8] T. Ahmed et al., "Database Optimization and Query Performance in MongoDB for E-Commerce Systems," 2024. [Note: relevant for backend/database efficiency].
- [9] N. Labhade-Kumar, "Combining Hand-Crafted Features and Deep Learning for Educational Data Classification," *Journal of Artificial Intelligence and Technology*, vol. 12, issue 3, pp. 242–250, 2023.
- [10] N. Labhade-Kumar, "An Image Processing Method for Data Segmentation Based on CNN-Regularized Extreme Learning Machine," *Hybrid and Advanced Technologies*, vol. 7, issue 1, pp. 217–222, 2025.
- [11] N. Labhade-Kumar, "Developing Interpretable Models and Techniques for Explainable AI in Decision-Making," *The Scientific Temper*, vol. 14, issue 4, pp. 1324–1331, 2023.
- [12] N.A. Kumar, "Study of Different Sensors Used in IoT," *Indian Journal of Technical Education (UGC Care Group I)*, ISSN 0971-3034, vol. 47, special issue, pp. 136–140, Apr. 2024.
- [13] N. Labhade-Kumar, "Study on Object Detection Algorithm," *Indian Journal of Technical Education (UGC Care Group I)*, ISSN 0971-3034, vol. 47, special issue, pp. 14–17, Apr. 2024.
- [14] N. Kumar, "Study of SHA-256 Hashing Algorithm," *Alochana Journal*, vol. 13, issue 12, ISSN 2231-6329, pp. 1172–1176, Dec. 2024.
- [15] N. Kumar, "Detailed Study of Histogram Computation Algorithm in Image Processing," *Alochana Journal*, vol. 13, issue 12, ISSN 2231-6329, pp. 1071–1078, Dec. 2024.