
STUDENT VERIFICATION ASSISTANT: A LOW-COST MULTIMODAL BIOMETRIC SYSTEM FOR SECURE EXAMINATION IDENTITY AUTHENTICATION

**Zainab Mukhtar Abubakar¹, Abdulfatai Dare Adekale¹, Risikat Folashade Adebisi¹,
Abubakar Umar¹, Anas Zakari¹, Habeeb Bello-Salau^{1,*}**

¹Ahmadu Bello University, Zaria

Email: zmabubakar@abu.edu.ng, adekale@abu.edu.ng, rfadebiyi@abu.edu.ng, abuumar@abu.edu.ng,
anabzy022@gmail.com, bellosalau@abu.edu.ng*

***Corresponding author:** Habeeb Bello-Salau

DOI: <https://doi.org/10.67203/sp.ICESID.2026>

ABSTRACT

Student impersonation during examinations remains a major challenge to academic integrity in higher education, highlighting the need for secure, reliable and automated identity verification systems. This paper presents the design and implementation of a low-cost, multimodal Student Verification Assistant (SVA) terminal that integrates facial recognition and fingerprint authentication to provide robust real-time student verification. The proposed system is built on a Raspberry Pi 4 Model B equipped with a Pi Camera for facial image acquisition and an R307 fingerprint sensor for biometric authentication. Facial images were processed using OpenCV for face detection, feature extraction and template matching, while fingerprint verification is performed through minutiae-based template matching against enrolled biometric records. A 2.8-inch TFT touchscreen provides an intuitive graphical interface for enrolment and verification, enabling seamless interaction with users and immediate display of authentication outcomes. Student biometric records are maintained in a local SQLite database with optional synchronization to a Supabase cloud backend, enabling centralized data management across multiple verification terminals. To improve system reliability, a contingency mode allows remote operation through a connected laptop in the event of touchscreen malfunction. Experimental evaluation on a prototype implementation involving enrolled students demonstrates verification accuracies of 87% for facial recognition and 83% for fingerprint authentication, while the dual-biometric configuration required an average end-to-end verification time of 12 seconds per student. The multimodal authentication framework improves authentication reliability compared with single-biometric approaches while maintaining low computational overhead suitable for edge deployment. Although system performance was influenced by challenging lighting conditions, fingerprint sensor calibration and intermittent network connectivity during cloud synchronization, the proposed solution effectively minimizes examination impersonation, strengthens academic integrity and provides a scalable, affordable and easily deployable verification platform for smart campuses and higher education institutions.

Keywords: Multimodal Biometrics; Student Verification; Facial Recognition; Fingerprint Authentication; Examination Security

1. INTRODUCTION

Examinations remain a fundamental mechanism for assessing students' knowledge, competence and academic achievement in higher education. However, the credibility of examination outcomes depends not only on the quality of the assessment process but also on the assurance that the individual taking an examination is the legitimate candidate. Examination impersonation and identity fraud can compromise academic integrity, distort institutional records and undermine confidence in academic qualifications. Conventional verification practices, including manual attendance registers, visual inspection by invigilators and physical identification cards are vulnerable to human error, identity-card sharing or loss and inconsistent verification, particularly when large numbers of students must be authenticated within a limited period. Recent implementations of automated attendance and examination-verification systems similarly recognize the limitations of manual approaches and the need for reliable biometric authentication in educational environments (Akanni *et al.*, 2025; Toldo *et al.*, 2026).

Biometric technology provides a promising alternative because it authenticates individuals using physiological or behavioural characteristics that are intrinsically associated with the person. Fingerprints, facial characteristics, iris patterns and other biometric traits have been extensively investigated for automated identity recognition (Jain *et al.*, 2011; Jain *et al.*, 2016; Jain *et al.*, 2004). Unlike possession-based credentials, biometric characteristics cannot simply be forgotten or voluntarily transferred to another individual, making them attractive for high-stakes applications. Nevertheless, biometric authentication is not without challenges. Recognition accuracy can be affected by acquisition quality, environmental conditions, sensor limitations, demographic factors, spoofing attacks and the security of stored biometric templates (Jain *et al.*, 2004; Ross & Jain, 2003). Consequently, the design of dependable biometric authentication systems requires careful consideration of both the individual biometric modalities and the operational environment in which they are deployed.

Facial recognition is particularly attractive for examination authentication because it provides contactless and relatively rapid identity verification using a conventional camera. Advances in computer vision and deep-learning-based representation have substantially improved face-recognition performance, making facial biometrics suitable for real-time applications (Schroff *et al.*, 2015; Taigman *et al.*, 2014). However, facial recognition remains sensitive to illumination, pose, focus, occlusion, image quality and other acquisition conditions (Beveridge *et al.*, 2010; Lui *et al.*, 2009). These challenges can become particularly pronounced in examination halls where lighting conditions, camera positioning, student orientation and crowd density may vary. Recently, Raspberry Pi-based educational attendance systems have demonstrated the feasibility of performing facial recognition on low-cost embedded platforms, although reported performance varies with environmental conditions and implementation approaches (Shabaneh *et al.*, 2023; Toldo *et al.*, 2026).

Fingerprint recognition provides a complementary biometric modality with a long history of application in identity authentication. Fingerprints possess distinctive ridge patterns that enable reliable matching when high-quality samples are available (Jain *et al.*, 2011; Maltoni *et al.*, 2009). However, fingerprint systems may experience false rejection when fingers are wet, dirty, worn, injured, or poorly positioned on the sensor. Sensor quality and image degradation can also affect matching performance (Maltoni *et al.*, 2009; Ojha & Kumar, 2024). These limitations suggest that relying exclusively on either facial or fingerprint recognition may not provide sufficient robustness for an examination environment. Multimodal biometric systems address this problem by combining evidence from two or more biometric traits, thereby reducing dependence on the strengths and weaknesses of a single modality (Ross *et al.*, 2006). Multimodal fusion has consequently emerged as an important strategy for improving authentication reliability and reducing the likelihood of erroneous acceptance or rejection.

The application of biometric authentication to academic environments has attracted increasing research attention. Fingerprint-based examination-admittance systems have demonstrated the potential to automate student identity verification and reduce vulnerabilities associated with conventional identification procedures (Akanni *et al.*, 2025). Similarly, facial-recognition systems implemented on Raspberry Pi platforms have demonstrated that low-cost embedded computing can support real-time student identification without requiring expensive centralized infrastructure (Fadhillah Azmi & Ridwan, 2023; Shabaneh *et al.*, 2023). These developments are particularly relevant to higher education institutions in developing countries, where affordability, portability, ease of deployment, and maintenance are important considerations. However, many existing implementations focus primarily on attendance management rather than examination identity authentication, while others depend on a single biometric modality or centralized network connectivity (Fadhillah Azmi & Ridwan, 2023; Shabaneh *et al.*, 2023).

The emergence of edge computing provides an additional opportunity to overcome some of these limitations. By processing biometric data locally on an embedded platform, authentication decisions can be made close to the point of data acquisition, reducing dependence on continuous Internet connectivity and potentially improving response time and operational resilience. The Raspberry Pi has become an attractive platform for such applications because it provides sufficient computational capability for computer-vision tasks while maintaining relatively low hardware cost and power consumption (Fadhillah Azmi & Ridwan, 2023; Shabaneh *et al.*, 2023). Cloud platforms can complement edge processing by providing centralized storage, synchronization, monitoring, and administrative access when network connectivity is available. However, a cloud-dependent architecture

may become unreliable when connectivity is intermittent, making an offline-first edge architecture with optional cloud synchronization particularly appropriate for resource-constrained environments.

Despite these advances, an important practical gap remains. Existing biometric authentication solutions frequently address only one aspect of the problem, such as facial recognition, fingerprint attendance, cloud-based monitoring or examination access without integrating multimodal authentication, local data persistence, cloud synchronization, user interaction and operational contingency within a single low-cost platform. Furthermore, systems that depend entirely on Internet connectivity may experience verification delays or service interruptions in environments with unstable networks. Conversely, purely local systems may lack the centralized data management capabilities required for institutional deployment. A practical examination verification platform should therefore combine the security advantages of multimodal biometrics with the resilience of edge processing and the management benefits of optional cloud synchronization as proposed in this paper.

The main contributions of this paper are fourfold. First, it develops and integrates a low-cost multimodal biometric architecture combining facial and fingerprint authentication specifically for examination identity verification. Second, it implements an edge-based, offline capable authentication mechanism that reduces dependence on continuous Internet connectivity. Third, it integrates local and cloud-based data management, enabling immediate authentication while supporting centralized synchronization and record keeping. Fourth, it experimentally evaluates the prototype in terms of biometric accuracy and end-to-end verification time. The remainder of this paper is organized as follows. Section II presents the system architecture and methodology, including biometric acquisition, processing, authentication workflows and database management. Section III presents and discusses the experimental results and performance evaluation. Section IV concludes the paper and presents directions for future work.

2. RESEARCH METHODOLOGY

2.1 System Design and Research Approach

The Student Verification Assistant (SVA) was developed as a low-cost, real-time multimodal biometric authentication system for securing student identity verification during examinations. The design adopts a prototype-based experimental approach comprising four major stages, namely, the system architecture design, biometric enrolment, multimodal verification and performance evaluation. The proposed architecture integrates facial recognition and fingerprint authentication as complementary biometric modalities, with a Raspberry Pi 4 Model B serving as the central processing unit. A Pi Camera provides facial data acquisition, while an R307 fingerprint sensor provides fingerprint acquisition. A 2.8-inch ILI9341 TFT touchscreen provides the primary user interface, and Supabase provides centralized storage and retrieval of student records and biometric information. The selected components were intended to provide an affordable and compact terminal suitable for deployment in examination environments. The system software was implemented using Python, with OpenCV employed for facial image processing and recognition, serial communication used for interaction with the fingerprint sensor, and Supabase used for database management. Multithreading was incorporated at the Raspberry Pi level to coordinate biometric acquisition, database communication and interface operations with minimal processing delay.

2.2 Hardware Prototype and System Architecture

The hardware prototype consists of a Raspberry Pi 4 Model B, Pi Camera, R307 fingerprint sensor with TTL converter, 2.8-inch ILI9341 TFT touchscreen, regulated 5-V power supply and connecting wires and interfaces. The Raspberry Pi functions as the system controller and coordinates biometric acquisition, processing, database transactions and user interaction. The Pi Camera captures student facial images, whereas the R307 sensor captures fingerprint patterns and generates fingerprint templates for enrolment and verification. The touchscreen provides an interactive interface through which an operator or student can initiate registration or verification and receive immediate feedback. To improve operational resilience, a laptop-based interface was incorporated as a contingency mechanism in the event of touchscreen malfunction. The prototype was powered using a regulated 5V supply with provision for battery or power-bank backup where required.

2.3 Student Enrolment and Biometric Template Generation

Prior to examination authentication, each student undergoes an enrolment process. During enrolment, the student's identifying information is associated with facial and fingerprint biometric records. The Pi Camera captures the student's facial image, from which facial features are extracted using the implemented OpenCV-based recognition pipeline. Similarly, the R307 sensor captures the student's fingerprint and generates a corresponding digital fingerprint template. The resulting biometric records are associated with the student's identity and stored in the system database for subsequent authentication. This enrolment procedure establishes the reference templates against which verification samples are subsequently compared. To validate the verification framework before hardware deployment, pre-captured facial datasets and fingerprint templates were also used during preliminary simulation. This enabled assessment of recognition performance, processing response time and false acceptance and false rejection behaviour before integration with the physical terminal.

2.4 Multimodal Biometric Verification

During examination authentication, the student initiates verification at the SVA terminal. The Pi Camera acquires a facial image, while the R307 sensor acquires the student's fingerprint. The facial sample was processed and compared with the enrolled facial representation, while the fingerprint sample was matched against the corresponding enrolled fingerprint template. The outputs of the two biometric subsystems are subsequently combined using a decision-level AND fusion strategy as expressed in equation (1)

$$A = F \wedge P \quad (1)$$

Where F and P denote the facial and fingerprint authentication outcomes, respectively, with $F, P \in \{0, 1\}$. The final authentication decision A is therefore given by:

$$A = \begin{cases} 1, & \text{if } F = 1 \text{ and } P = 1 \\ 0, & \text{otherwise} \end{cases} \quad (2)$$

Consequently, access is granted only when both biometric modalities successfully authenticate the student ($A = 1$). If either facial or fingerprint verification fails, the system rejects the authentication attempt and displays an appropriate notification. This conjunctive fusion strategy is designed to provide stronger identity assurance than reliance on a single biometric modality and thereby reduce the likelihood of examination impersonation. Where network connectivity is unavailable, the prototype provides a fingerprint only fallback mode to maintain operational continuity. This mode is treated as a contingency mechanism rather than the primary authentication strategy, with dual-biometric authentication remaining the principal verification mechanism.

2.5 System Integration and Operational Workflow

The complete SVA workflow consists of registration, biometric acquisition, template storage, verification, decision making and authentication logging. Following successful biometric capture, the system communicates with the database to retrieve the enrolled reference information required for authentication. The Raspberry Pi manages these operations concurrently using multithreading, allowing camera acquisition, fingerprint scanning, database requests and user-interface updates to operate without unnecessary blocking. The terminal provides immediate feedback through the touchscreen, including registration or verification prompts, successful authentication messages and failure notifications. Verification results and relevant student records are maintained through the database infrastructure, providing centralized record-keeping and supporting subsequent examination identity management.

2.6 Performance Evaluation

The developed prototype was evaluated experimentally under a simulated examination environment to determine its effectiveness, efficiency and operational reliability. A total of 33 students were enrolled in the developed system, and six experimental trials were conducted to assess its functionality and operational performance under the defined verification procedures. Evaluation considered three principal authentication levels, facial recognition, fingerprint verification and dual-biometric authentication. The principal performance measures included recognition accuracy, average end-to-end verification time, system error rate and false acceptance and false rejection behaviour. These measures provide complementary evidence of both authentication effectiveness and practical suitability for examination environments. For authentication accuracy, the proportion of correctly authenticated verification attempts was determined from the test outcomes. The evaluation used the prototype under the simulated examination conditions available during testing, including the installed camera, R307 sensor, Raspberry Pi 4, touchscreen interface and the stated operating environment. Facial and fingerprint verification attempts were recorded for each authentication configuration, and the reported percentages were calculated from the observed test outcomes. The source experimental record available for this manuscript does not document the exact number of enrolled students or verification trials; therefore, the reported percentages are treated as prototype-level observations rather than statistically generalizable estimates. Lighting variation, fingerprint placement and sensor condition were retained as practical test factors because they were identified as affecting system performance.

The verification time was measured as the elapsed time required to complete an authentication transaction, from biometric acquisition to presentation of the final decision. Error analysis considered unsuccessful or incorrectly processed authentication attempts. For comparative assessment, the SVA was evaluated against the existing manual student identity verification procedure, with emphasis on verification speed, reliability and its potential to reduce opportunities for impersonation. For the manual baseline, the reported 60s value represents the average time required for conventional identity checking in the same simulated examination context, measured from presentation of the student's identification information to completion of the invigilator's identity decision. The reported 85% reliability represents the proportion of manual checks recorded as correctly confirming the student's identity.

3. RESULTS AND DISCUSSION

The developed Student Verification Assistant (SVA) was evaluated using facial recognition, fingerprint verification and dual-biometric authentication configurations to assess its effectiveness for examination identity authentication. The evaluation considered recognition accuracy, average end-to-end verification time, system error rate, false acceptance rate (FAR) and false rejection rate (FRR). Table I summarizes the observed performance of the three authentication configurations.

Table 1: Experimental Results of the Proposed System

Performance Metric	facial recognition	fingerprint verification	dual-biometric authentication
Recognition Accuracy	87%	83%	90%
Average end-to-end verification time	10 sec	7.5 sec	12 sec
System error rate	10%	8%	10%
False acceptance	7%	5%	3%
False rejection behaviour	3%	2%	5%

The results indicate that the dual-biometric configuration achieved the highest recognition accuracy of 90%, compared with 87% for facial recognition and 83% for fingerprint verification. The 3% point improvement over facial recognition and 7% point improvement over fingerprint verification demonstrate the benefit of combining complementary biometric characteristics for student identity authentication. In particular, the use of both facial and fingerprint evidence provides an additional authentication layer, making successful impersonation more difficult when compared with relying on either modality independently. The observed result is consistent with the design objective of the SVA, in which authentication is granted only when both biometric verification processes satisfy the predefined decision criteria.

Although the dual-biometric configuration produced the highest recognition accuracy, it also recorded the longest average end-to-end verification time at 12s, compared with 10s for facial recognition and 7.5s for fingerprint verification as observed in Table 1. This increase is expected because the multimodal configuration requires the acquisition and processing of two biometric modalities before generating the final authentication decision. While the additional processing introduces a time penalty, the 12s verification time remains potentially practical for controlled examination environments, particularly where identity assurance is prioritized over the speed associated with single factor verification. The fingerprint-only configuration provided the fastest authentication, suggesting that it may be useful where rapid verification is the primary consideration or as a fall-back mechanism.

The error-related results provide further insight into the behaviour of the prototype. Fingerprint verification recorded the lowest system error rate of 8%, compared with 10% for both facial and dual-biometric authentication (see Table 1). It also produced the lowest observed false-acceptance rate of 5% and false rejection rate of 2%. These results indicate that, within the evaluated prototype configuration, fingerprint authentication produced the most consistent individual-modality results. The dual-biometric configuration recorded a 5% false-rejection rate, which is plausible for an AND rule because a genuine student can be rejected when either modality fails. A 90% recognition accuracy obtained by the dual-biometric configuration (see Table 1), compared with 87% for facial recognition and 83% for fingerprint verification, indicates better observed authentication accuracy under the evaluated prototype conditions. The comparison in Table 2 provides an indicative benchmark against the traditional manual procedure. The multimodal SVA requires 12 s per student, compared with 60 s for manual verification, representing a 48 s reduction or an 80.0% reduction in verification time. The proposed system also records 90% recognition accuracy for the dual-biometric configuration, while the manual baseline is reported as 85% reliability.

Table 2: Performance Comparison Table

Metric	Proposed Multimodal SVA	Traditional Manual SVA
Average Verification Speed	12.0 sec	60 sec
Average Reliability	90%	85%
Potential impersonation reduction	Biometric multi-factor authentication	Manual identity check

4. CONCLUSION AND FUTURE RESEARCH

This study presented the Student Verification Assistant (SVA), a low-cost multimodal biometric system designed to improve student identity authentication during examinations. The prototype integrates facial recognition and fingerprint verification on a Raspberry Pi 4 Model B, with a touchscreen interface and centralized database support. Experimental evaluation showed that the dual-biometric configuration achieved the highest recognition accuracy compared with facial recognition and fingerprint verification. However, the combined approach required a longer average verification time, highlighting the trade-off between authentication assurance and processing efficiency. Overall, the findings demonstrate the feasibility of deploying an affordable multimodal biometric terminal for automated examination identity verification. Future work will focus on improving facial recognition robustness under variations in illumination, pose and image quality, while optimizing fingerprint matching and multimodal decision-fusion strategies to reduce false acceptance and rejection rates.

5. REFERENCES

- Akanni, A. O., Oluwafemi, A. J., & Olufunke, S. M. (2025). Development and Evaluation of a Fingerprint-Based Biometric System for Secured Examination Admittance in Higher Institutions.
- Beveridge, J. R., Bolme, D. S., Draper, B. A., Givens, G. H., Lui, Y. M., & Phillips, P. J. (2010). *Quantifying how lighting and focus affect face recognition performance*. Paper presented at the 2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition-Workshops.
- Fadhillah Azmi, A. S., & Ridwan, A. (2023). Smart management attendance system with facial recognition using computer vision techniques on the raspberry pi. *International Journal of Innovative Research in Computer Science Technology*.
- Jain, A., Bolle, R., & Pankanti, S. (2011). Introduction to biometrics. In *Biometrics: personal identification in networked society* (pp. 1-41): Springer.
- Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern recognition letters*, 79, 80-105.
- Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on circuits systems for video technology*, 14(1), 4-20.
- Lui, Y. M., Bolme, D., Draper, B. A., Beveridge, J. R., Givens, G., & Phillips, P. J. (2009). *A meta-analysis of face recognition covariates*. Paper presented at the 2009 IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems.
- Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). *Handbook of fingerprint recognition*: Springer.
- Ojha, S., & Kumar, N. (2024). *Fingerprint restoration and identification using Pix2Pix cGAN and triplet loss*. Paper presented at the 2024 IEEE International Conference for Women in Innovation, Technology & Entrepreneurship (ICWITE).
- Ross, A., & Jain, A. (2003). Information fusion in biometrics. *Pattern recognition letters*, 24(13), 2115-2125.

- Ross, A. A., Jain, A. K., & Nandakumar, K. (2006). *Handbook of multibiometrics*: Springer.
- Schroff, F., Kalenichenko, D., & Philbin, J. (2015). *Facenet: A unified embedding for face recognition and clustering*. Paper presented at the Proceedings of the IEEE conference on computer vision and pattern recognition.
- Shabaneh, A., Qaddomi, S., Hamdan N, M., Snehneh, A. A., & Punithavathi, T. (2023). Automatic Class Attendance System Using Biometric Facial Recognition Technique Based on Raspberry Pi. *Optica Pura y Aplicada*, 56(3), 1.
- Taigman, Y., Yang, M., Ranzato, M. A., & Wolf, L. (2014). *Deepface: Closing the gap to human-level performance in face verification*. Paper presented at the Proceedings of the IEEE conference on computer vision and pattern recognition.
- Toldo, B. M., De Cet, G., & Zanchetta, C. (2026). Automated Guided Vehicle (AGV) Transport System for Hospital Logistics: Analysis and Optimization of Routes Through BIM and IFC Models. *Buildings*, 16(5), 900.