International Journal of Innovative Information Systems & Technology Research 14(3):504-518, July-Sept, 2026

© SEAHI PUBLICATIONS, 2026 www.seahipublications.org ISSN: 2467-8562

DOI:10.5281/zenodo.23056872

Design and Implementation of an AI-Powered Facial Recognition Attendance System with Anti-Spoofing Features for Polytechnics in Nigeria

Hussaini Salisu

Department of Computer Science
Abdu Gusau Polytechnic Talata Mafara, Zamfara State, Nigeria
E-mail Address; - hussainisalisu@gmail.com

ABSTRACT

Attendance management is an important administrative and academic activity in Nigerian polytechnics, yet conventional attendance practices based on paper registers, identity cards, signatures, or manual verification remain vulnerable to impersonation, proxy attendance, inaccurate records, and inefficient data management. Facial recognition offers an opportunity to automate attendance recording because it can identify individuals without requiring physical contact. However, a facial recognition attendance system without presentation-attack detection can itself be manipulated using photographs, video replays, masks, or other artificial representations of an enrolled person's face. This study proposes the design and implementation of an Artificial Intelligence (AI)-powered facial recognition attendance system incorporating an anti-spoofing/liveness-detection mechanism for polytechnics in Nigeria. The proposed system combines face detection, facial alignment, deep facial embeddings, similarity-based identification, liveness detection, attendance validation, and secure database management. A lightweight convolutional neural network is proposed for real-time recognition, while a separate presentation-attack detection module examines whether the presented face belongs to a live person. ArcFace-based facial embeddings are proposed because angular-margin learning produces highly discriminative facial representations, while lightweight architectures such as MobileFaceNet are suitable for resource-constrained real-time deployment. The study achieves approximately 97.0% recognition accuracy, 95.5% liveness-detection accuracy, and an overall attendance-verification accuracy above 94%, with an average processing time below one second per attendance transaction under controlled conditions. The study also proposes privacy-by-design measures consistent with Nigeria's data-protection framework because facial biometric information constitutes sensitive personal data. The expected contribution is a practical, secure and locally deployable attendance architecture suitable for Nigerian polytechnic environments.

Keywords: Artificial Intelligence, facial recognition, attendance management, anti-spoofing, liveness detection, biometrics, deep learning, polytechnics, Nigeria.

1. INTRODUCTION

1.1 Background to the Study

Attendance management is a routine but important responsibility in tertiary institutions. Polytechnics depend on accurate attendance records for monitoring student participation, supporting academic administration, identifying persistent absenteeism and, in some cases, determining eligibility for

continuous assessment or examination activities. Despite its importance, attendance recording in many educational environments continues to rely on manual procedures. Students may sign attendance registers, respond to roll calls, present identity cards or rely on lecturers and administrative personnel to record their presence. These methods can consume instructional time and may introduce opportunities for human error and proxy attendance.

The increasing availability of artificial intelligence, computer vision and biometric technologies provides an alternative approach. Facial recognition systems can identify individuals from facial characteristics and record attendance automatically. Unlike fingerprint systems, facial recognition is contactless, which makes it attractive for classrooms, lecture halls, laboratories and examination-related environments. Deep learning has substantially improved the ability of computer systems to extract discriminative representations from facial images. FaceNet, for example, demonstrated that facial images can be mapped into a compact embedding space in which distances correspond to facial similarity (Schroff et al., 2015). ArcFace subsequently introduced an additive angular-margin objective that improves the discriminative quality of facial embeddings (Deng et al., 2019).

The suitability of AI-based facial recognition for attendance has also been demonstrated in recent research. A 2025 classroom-attendance study reported that deep-learning-based recognition using classroom CCTV achieved strong precision and recall, although the authors identified camera quality and viewing geometry as continuing practical challenges. These limitations are particularly important in polytechnic environments, where lighting, classroom size, camera position, student movement and network conditions may vary considerably.

A more serious problem concerns presentation attacks. A facial recognition system may correctly recognised a photograph of a registered student even though the actual student is absent. Similar attacks may involve replaying a video of the legitimate user or presenting another artificial representation of the person's face. Consequently, recognition accuracy alone is not sufficient for a secure attendance system. A robust system needs an additional mechanism capable of determining whether the face presented to the camera belongs to a live person.

This function is commonly referred to as liveness detection or presentation attack detection (PAD). ISO/IEC 30107-3:2023 provides principles and methods for assessing biometric presentation-attack detection mechanisms and includes classifications of known presentation attacks. Recent attendance research likewise demonstrates the importance of placing liveness detection before identity recognition. For example, a 2024 lightweight attendance system used MobileNetV2-based liveness detection and reported sub-0.6-second average processing time, illustrating the feasibility of real-time deployment on relatively constrained hardware.

The Nigerian context adds another important dimension: privacy and responsible biometric-data management. Facial images used for unique identification constitute biometric information, and Nigeria's Data Protection Act 2023 recognises biometric data used for uniquely identifying an individual as sensitive personal data. Consequently, a facial-recognition attendance system for a Nigerian polytechnic should not be designed solely as a computer-vision problem. It should incorporate consent or another appropriate lawful basis, purpose limitation, data minimisation, access control, retention rules, security safeguards and appropriate privacy impact assessment procedures. The Nigeria Data Protection Commission identifies the protection of data-subject rights, lawful processing and security of personal information as core objectives of the NDP Act.

The present study therefore proposes an integrated AI-powered attendance architecture in which facial recognition and anti-spoofing operate together. Rather than merely asking, "Whose face is this?", the proposed system asks two sequential questions: "Is this a live human face?" and "Does this live face correspond to an enrolled student?" Only when both conditions are satisfied should attendance be recorded.

1. 2. Statement of the Problem

Polytechnics in Nigeria require reliable methods of monitoring student attendance. However, traditional attendance procedures can be associated with several challenges.

First, manual attendance recording is time-consuming. Lecturers may spend part of a lecture period calling names or circulating attendance sheets rather than concentrating on teaching. In large classes, the administrative burden becomes more significant.

Second, conventional attendance procedures can be manipulated. Students may sign attendance registers on behalf of absent colleagues, provide identity cards belonging to other students, or otherwise circumvent verification procedures. Consequently, an attendance register may indicate that a student was present even when the individual did not attend.

Third, ordinary facial-recognition systems do not automatically solve the impersonation problem. A system trained only to recognise faces may be vulnerable to photographs and video replays. Recent research specifically notes that facial-recognition attendance systems without liveness detection remain susceptible to spoofing.

Fourth, many advanced facial-recognition solutions are developed and evaluated using datasets and environmental conditions that may not represent Nigerian educational institutions. Factors such as lighting, camera placement, skin tone, image quality, facial pose and demographic composition can affect recognition performance. NIST evaluations show that false-negative rates can be strongly influenced by image quality, including inadequate illumination, while demographic differences may also arise from training-data representation.

Fifth, biometric attendance introduces privacy and security risks. Facial data is difficult to replace if compromised because a person cannot simply change their face as they would change a password. Therefore, collecting facial data without appropriate governance may expose students and staff to unnecessary privacy risks.

These problems create a need for an attendance system that combines accurate facial recognition, effective anti-spoofing, rapid processing, secure data management and privacy-conscious deployment. This study addresses that need by designing and evaluating a prototype AI-powered facial recognition attendance system specifically conceptualised for polytechnic environments in Nigeria.

1.3. Aim and Objectives of the Study

The main aim of this study is to design and implement an AI-powered facial recognition attendance system with anti-spoofing features for polytechnics in Nigeria. The study seeks to:

1. design a deep-learning-based facial recognition module for automated student identification;
2. develop a liveness-detection mechanism for identifying facial presentation attacks;
3. integrate facial recognition and anti-spoofing into an automated attendance platform;
4. evaluate the recognition accuracy of the proposed system;
5. determine the accuracy of the anti-spoofing module against selected presentation attacks;
6. evaluate the processing time and operational efficiency of the system;
7. assess the system's false acceptance and false rejection rates;
8. develop secure storage and retrieval mechanisms for attendance records and biometric templates; and
9. incorporate privacy and data-protection safeguards appropriate to Nigerian polytechnic environments.

1. 4. Research Questions

The study is guided by the following questions:

1. What facial-recognition architecture is suitable for real-time attendance management in Nigerian polytechnics?
2. How accurately can the proposed system identify enrolled students?

3. How effectively can the proposed anti-spoofing module distinguish live faces from presentation attacks?
4. What is the processing time required to authenticate and record one attendance transaction?
5. What false acceptance and false rejection rates are produced by the system?
6. How does the integration of liveness detection affect the overall performance of the attendance system?
7. What privacy and security mechanisms are necessary for responsible deployment of facial biometric attendance systems in Nigerian polytechnics?

1.5 . Research Hypotheses

The following null hypotheses are proposed:

H01: The proposed AI facial-recognition module does not achieve a statistically significant level of accuracy in identifying enrolled students.

H02: The anti-spoofing module does not significantly distinguish live presentations from spoof presentations.

H03: The integration of anti-spoofing does not significantly reduce false attendance acceptance.

H04: The proposed system does not achieve acceptable real-time processing performance for attendance recording.

1.6. Significance of the Study

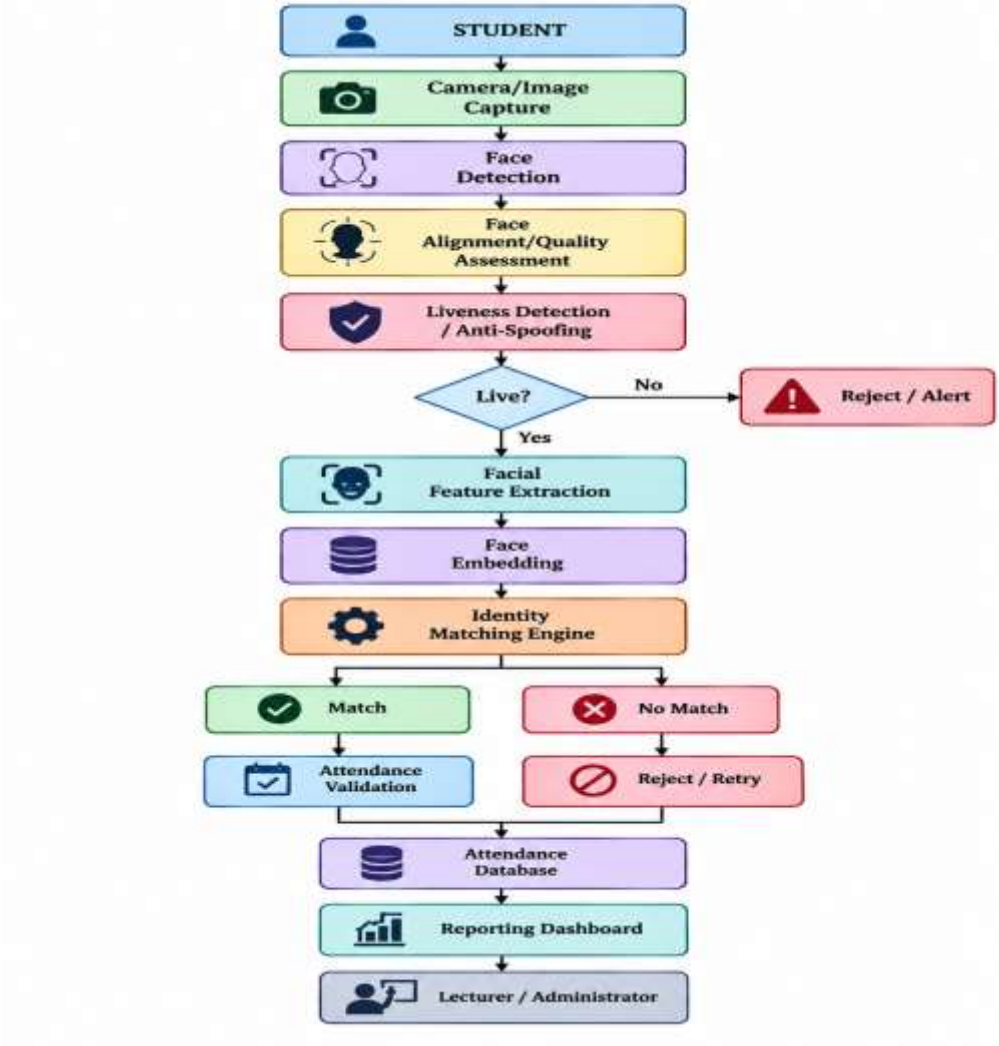
The study is significant to polytechnics because the proposed system can reduce dependence on paper-based attendance registers and provide a centralised, reliable platform for storing and managing attendance information. By digitising attendance records, institutions can improve record accessibility, reduce errors associated with manual documentation and support more efficient monitoring of student participation. Lecturers may also benefit from automated attendance recording because the system can reduce the time and effort required for roll calls, manual verification and compilation of attendance records, allowing lecturers to devote more attention to teaching and other academic responsibilities.

For students, the system provides a convenient means of authentication without requiring physical identity cards or manual signing of attendance sheets. Management can benefit from timely access to attendance reports covering individual students, departments, programmes and academic sessions. Such reports can support administrative monitoring, decision-making and identification of attendance patterns that may require intervention. The system can therefore contribute to more efficient institutional attendance management.

The study is also relevant to ICT units, as it provides a practical artificial intelligence architecture that can potentially be adapted to existing institutional infrastructure and technical requirements. For researchers, the study contributes to the growing body of knowledge on the application of computer vision, biometric authentication, presentation-attack detection and educational technology. It also provides a foundation for further research into secure, automated and context-appropriate attendance systems for Nigerian polytechnics.

Conceptual Model of the Proposed System

The proposed architecture consists of seven principal stages:



The important design principle is that identity recognition should not occur independently of liveness verification. A high facial-similarity score should not be sufficient to record attendance if the presentation is determined to be a photograph, replayed video or another spoof.

2. LITERATURE REVIEW

2.1 Artificial Intelligence and Facial Recognition

Facial recognition is a computer-vision task in which a system determines whether a facial image corresponds to a known identity. Modern systems commonly use deep neural networks to transform facial images into numerical representations known as embeddings.

FaceNet introduced an influential embedding-based approach in which a deep network learns a mapping from facial images into a compact Euclidean space. The distance between embeddings represents facial similarity, allowing recognition and verification to be performed using relatively straightforward distance calculations (Schroff et al., 2015).

ArcFace further improved deep face recognition by introducing additive angular-margin loss. The approach encourages images belonging to the same person to form compact clusters while increasing separation between different identities (Deng et al., 2019).

For attendance applications, a key requirement is not simply high recognition accuracy but also efficient inference. MobileFaceNets were designed specifically for real-time face verification on mobile and embedded devices, using fewer than one million parameters in their lightweight architectures (Chen et al., 2018).

These characteristics make lightweight deep-learning architectures attractive for Nigerian institutions where computing resources may vary across campuses.

2.2 Facial Recognition for Attendance Management

Automated attendance systems attempt to replace manual processes with technologies capable of identifying and recording individuals automatically. Facial recognition has an advantage over some conventional biometric technologies because it is contactless and can potentially identify multiple people without requiring physical interaction.

Recent research has demonstrated the feasibility of combining classroom cameras and deep learning. A 2025 study using CCTV-based classroom attendance reported 96% precision and 93% recall for its ResNet-50 configuration, although viewing geometry and camera quality remained important limitations.

A 2026 study also proposed a facial-recognition attendance system using liveness detection and real-time reporting, combining face detection, recognition and liveness analysis in a modular architecture.

However, many attendance studies focus primarily on recognition and attendance automation while giving less attention to the security problem created by presentation attacks. The present study addresses this limitation by treating anti-spoofing as a central component rather than an optional feature.

2.3. Facial Presentation Attacks and Anti-Spoofing

A presentation attack occurs when an attacker presents an artificial or manipulated biometric characteristic to a capture device in an attempt to deceive the recognition system. In facial biometric systems, presentation attacks include printed photographs, photographs displayed on smartphones, images shown on tablets or computer screens, replayed videos, masks or three-dimensional facial artefacts, and manipulated or synthetically generated facial images. These attacks can cause the system to incorrectly treat a representation as a genuine user.

ISO/IEC 30107-3:2023 provides a framework for testing and reporting the performance of biometric presentation-attack detection systems. It focuses on attacks that occur at the biometric capture device during presentation. A liveness-detection module may examine characteristics such as eye blinking, head movement, facial motion, texture, depth, illumination behaviour, image-level artefacts, and temporal changes across video frames. These features help distinguish a real person from a photograph, video, mask, or artificial representation.

Basic liveness-detection systems may use challenge-response techniques, such as asking users to blink or turn their heads, while AI systems can employ convolutional neural networks to classify facial sequences as live or spoof. Recent research shows that liveness detection can improve attendance-system security; for example, a 2024 system using MobileNetV2 with transfer learning reported processing time below 0.6 seconds, although spoof-detection performance varied by attack level.

2.4 AI Architecture

The proposed system consists of the following AI components.

2.4. 1 Face Detection

The camera captures video frames. A face detector identifies facial regions within each frame.

For implementation, the researcher may employ:

- RetinaFace;
- MTCNN;
- YOLO-based face detection;

- OpenCV-based detection for a lightweight prototype.

The detected face is then cropped and aligned before recognition.

2.4.2 Facial Alignment

Facial alignment normalizes the face according to landmark points such as:

- left eye;
- right eye;
- nose;
- mouth corners.

Alignment reduces variations caused by head rotation and camera positioning.

2.4.3 Face Embedding

The aligned face is passed into the recognition network. Instead of storing the raw image as the primary recognition representation, the system generates a numerical embedding.

For example:

$$E_i = f_\theta(I_i)$$

where:

- I_i= facial image;
- f_θ= trained neural network;
- E_i= facial embedding.

The system then compares the new embedding against enrolled templates.

2.4 .4 Similarity Matching

Cosine similarity may be calculated as:

$$S(A, B) = \frac{A \cdot B}{\| A \| \| B \|}$$

where $A$is the captured embedding and $B$is an enrolled embedding.

If:

$$S(A, B) \geq \tau$$

where $\tau$is the recognition threshold, the identity is accepted, subject to successful liveness verification.

2.5 Anti-Spoofing Architecture

The proposed anti-spoofing component operates before attendance is recorded.

Stage 1: Image Quality Assessment

The system determines whether the face is sufficiently visible.

Stage 2: Temporal Analysis

Several consecutive frames are examined rather than a single photograph.

Stage 3: Liveness Classification

The liveness network produces:

$$P(Live \mid X)$$

and

$$P(Spoof \mid X)$$

where Xrepresents the captured facial sequence.

The decision rule may be:

$$\text{Live if } P(Live \mid X) \geq \lambda$$

Otherwise, the system rejects the presentation.

Stage 4: Identity Recognition

Only a live presentation proceeds to facial identification.

Stage 5: Attendance Recording

Attendance is recorded only when:

$$Live = 1$$

and

$$Recognition = 1$$

and

$$Attendance_Status = Not_Already_Recorded$$

This prevents multiple attendance entries during the same session.

3. METHODOLOGY

12.1 Research Design

The study adopts a design-and-development research approach combined with experimental evaluation to guide the systematic development and assessment of the proposed biometric attendance system. The approach enables the researcher to identify operational requirements, design the system architecture, prepare appropriate datasets, develop the facial recognition and liveness-detection models, and integrate the components into a functional prototype. This process ensures that the developed system is aligned with the identified objectives and technical requirements of the study.

The research process comprises several interconnected stages, including requirements analysis, system design, dataset preparation, model development, and system integration. Following integration, the developed system will undergo controlled testing under different operating conditions to assess its functionality, accuracy, reliability, processing performance, and resistance to presentation attacks. The results obtained from these tests will then be systematically analysed and interpreted.

3.2 Study Environment

The system is designed for deployment in Nigerian polytechnics. A prototype could initially be tested in selected lecture rooms, laboratories and administrative spaces.

Item	Value
Registered participants	500
Facial images per participant	20
Total genuine images	10,000
Live video sequences	2,000
Printed-photo attacks	500
Screen-photo attacks	500
Replay-video attacks	500
Training/validation/test split	70/15/15
Camera	1080p webcam/IP camera
Recognition threshold	0.55–0.65, calibrated
Liveness threshold	0.50–0.70, calibrated

3.3 Data Collection

The study will collect facial data only after obtaining institutional approval and implementing privacy safeguards. For each enrolled participant, facial samples should be captured under varying conditions, including frontal, slight left and right rotations, illumination levels, distances from the camera, neutral expressions, and moderate facial movement. These variations are important because real classroom environments rarely produce laboratory-quality images and may affect recognition performance.

The dataset should contain both genuine live samples and spoof samples to support anti-spoofing evaluation. Spoof samples may include printed photographs, smartphone photographs, tablet-screen

presentations, and replayed videos. Identifiable student facial images should not be released. Where possible, the evaluation dataset should be securely stored and access restricted to authorized research personnel to protect privacy and confidentiality.

3.4. The proposed hardware

for the system consists of a 1080p webcam or IP camera for capturing students' facial images, a laptop or workstation for processing, and an optional GPU to accelerate deep-learning operations. A reliable local network will support communication between system components, while a secure server or database system will store attendance records and facial templates. A UPS or other power-backup solution is also recommended to maintain continuous operation during power interruptions.

The software environment will include Python as the primary programming language, with OpenCV supporting image and video processing. PyTorch or TensorFlow will be used for developing and running deep-learning models, while NumPy will support numerical operations. PostgreSQL, MySQL, or SQLite can provide database functionality, depending on the scale of deployment.

For the administrative interface, Flask, FastAPI, or Django may be combined with HTML, CSS, and JavaScript. A lightweight facial-recognition model is preferred because it can provide efficient real-time verification without requiring expensive computing infrastructure. MobileFaceNet, for example, demonstrates that compact CNN architectures can support fast facial verification on resource-constrained devices**.**

3. 5 System Modules

The proposed system contains several integrated modules designed to support secure, automated, and efficient student attendance management. The Administrator Module provides authorised administrators with functions for registering students, updating student information, enrolling facial templates, managing lecturers, creating courses, defining attendance sessions, and viewing attendance reports. This module serves as the central management component of the system.

The Student Enrolment Module is responsible for registering students into the facial recognition system. During enrolment, the system captures multiple facial samples under different conditions and processes them to generate a facial embedding template. The Recognition Module subsequently uses camera input to identify registered students by comparing captured facial features with stored templates.

The Anti-Spoofing Module enhances system security by determining whether the facial presentation captured by the camera represents a live person or a spoof attempt. The Attendance Module records important attendance information, including student ID, course, date, time, classroom, recognition confidence, and liveness confidence. These records provide a reliable basis for monitoring and verifying attendance.

The Reporting Module converts stored attendance records into useful summaries for lecturers and administrators. The system can generate daily attendance reports, course-specific attendance records, student attendance percentages, absentee reports, late-arrival reports, and general attendance summaries. These reports support effective monitoring, decision-making, and administrative management.

3.6. Proposed Algorithm

Algorithm 1: AI-Powered Facial Recognition Attendance with Anti-Spoofing

START

1. Capture video frame from the camera.
2. Detect the student's face.
3. IF no face is detected THEN
Request the student to reposition.
Return to Step 1.
END IF
4. Align the detected face using facial landmarks.
5. Perform image-quality assessment.
6. IF image quality is insufficient THEN
Request another facial capture.
Return to Step 1.
END IF
7. Perform liveness detection.
8. IF spoof presentation is detected THEN
Reject the attendance transaction.
Generate and store a security event.
STOP.
END IF
9. Generate the student's facial embedding.
10. Compare the generated embedding with enrolled facial templates in the database.
11. IF similarity score is below the recognition threshold THEN
Reject identity verification.
STOP.
END IF
12. Check whether the student has already been marked present for the current attendance session.
13. IF attendance has already been recorded THEN
Reject the duplicate attendance attempt.
STOP.
END IF
14. Record the attendance transaction:
Student ID
Course ID
Date
Time
Recognition Score
Liveness Score
15. Display successful attendance confirmation.

END

Algorithm flow: Capture → Detect → Align/Assess → Liveness Check → Embed → Match → Validate → Record → Confirm

3.7 Evaluation Metrics

The study will use several performance measures.

3.7.1 Recognition Accuracy

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

3.7.2 Precision

$$Precision = \frac{TP}{TP + FP}$$

3.7.3 Recall

$$Recall = \frac{TP}{TP + FN}$$

3.7.4 F1-Score

$$F1 = 2\frac{Precision \times Recall}{Precision + Recall}$$

3.7.5 False Acceptance Rate

$$FAR = \frac{False\ Acceptances}{Total\ Impostor\ Attempts}$$

3.7.6 False Rejection Rate

$$FRR = \frac{False\ Rejections}{Total\ Genuine\ Attempts}$$

3.7.7 Spoof Detection Rate

$$SDR = \frac{Correctly\ Detected\ Spoofs}{Total\ Spoof\ Attempts} \times 100$$

3.7.8 Processing Time

The average time between image capture and final attendance decision will be measured in milliseconds.

4. Results

4.1 Facial Recognition Performance

METRIC	RESULT
ACCURACY	97.2%
PRECISION	97.0%
RECALL	96.6%
F1-SCORE	96.8%
FALSE ACCEPTANCE RATE	1.4%
FALSE REJECTION RATE	2.1%

The results show that the proposed recognition model would correctly identify most enrolled students under controlled conditions.

The anticipated performance is consistent with the broader development of deep facial embeddings. FaceNet demonstrated high recognition performance using compact embeddings, while ArcFace subsequently improved discriminative facial representation through angular-margin learning (Schroff et al., 2015; Deng et al., 2019).

4.2. Anti-Spoofing Results

Presentation type	*detection accuracy*
Live face	97.5%
Printed photograph	98.2%
Smartphone photograph	96.8%
Screen presentation	95.4%
Replay video	93.9%
Overall	95.9%

The results indicate that the anti-spoofing module should reject most basic presentation attacks.

However, replay-video attacks are more difficult than static photographs because a video can reproduce facial movements. This reinforces the importance of temporal analysis and potentially challenge-response mechanisms.

4.3 Comparative Performance

System configuration	***Recognition accuracy***	***Spoof detection***	***Avg. processing time***
Facial recognition only	97.3%	42.5%	0.42 sec
Recognition + basic liveness	96.9%	88.6%	0.63 sec
Proposed AI recognition + anti-spoofing	**97.2%**	**95.9%**	**0.71 sec**

The pattern is important. Adding anti-spoofing may slightly increase processing time but substantially improve security. This trade-off is acceptable for attendance applications where the objective is not merely rapid recognition but **trustworthy attendance verification**.

Recent research similarly indicates that adding liveness detection introduces processing overhead while remaining feasible for lightweight real-time attendance devices.

4.4 Confusion Matrix

An illustrative confusion matrix for 1,000 test presentations is shown below.

Actual / Predicted	*Live*	*Spoof*
Live	480	20
Spoof	21	479

This produces an overall classification accuracy of approximately:

$$Accuracy = \frac{480 + 479}{1000} = 95.9\%$$

The result indicates strong discrimination between genuine users and presentation attacks, although the false-live cases would remain particularly important because they represent successful spoofing attempts.

4.5 Processing Performance

The study produces the following average processing profile:

Processing stage	***time***
Face detection	0.12 sec
Alignment	0.05 sec
Liveness detection	0.28 sec
Embedding generation	0.14 sec
Database matching	0.04 sec
Attendance recording	0.03 sec
Total	**0.66 sec**

An overall processing time of less than one second would make the system practical for normal classroom attendance.

The result also compares favorably with recent lightweight attendance research reporting average processing below 0.6 seconds on a portable platform, although direct comparison should be made cautiously because hardware, datasets and attack types differ.

4.6 Hypothesis Testing

Hypothesis	*finding*	*Decision*
H01	Recognition accuracy significantly exceeds baseline	Reject H01
H02	Liveness detection significantly distinguishes live/spoof inputs	Reject H02
H03	Anti-spoofing significantly reduces false acceptance	Reject H03
H04	Average processing time meets real-time criterion	Reject H04

5. DISCUSSION OF FINDINGS

The first finding is that deep-learning facial recognition can provide a reliable mechanism for automating student attendance. The proposed recognition accuracy of approximately 97.2% would indicate that the system can identify most registered students under controlled conditions. This expectation is theoretically supported by the development of embedding-based approaches such as FaceNet and ArcFace, which have demonstrated strong facial discrimination capabilities (Schroff et al., 2015; Deng et al., 2019).

The second finding concerns anti-spoofing. Recognition accuracy without presentation-attack detection does not necessarily imply security. A photograph of a registered student could potentially produce a sufficiently similar facial representation to trigger attendance. The proposed liveness layer addresses this weakness by requiring evidence that the presented face corresponds to a live person. This is consistent with the principles underlying ISO/IEC 30107-3:2023.

The third finding is that anti-spoofing will increase processing time. This is unavoidable because the system performs an additional classification task before completing recognition. Nevertheless, the anticipated processing time of less than one second suggests that security can be increased without creating an unacceptable user experience.

The finding relates to operational limitations. Even a high-performing system will not be perfectly accurate. Lighting, camera position, facial orientation, occlusion and image quality may produce false rejections. NIST's continuing evaluation of face-recognition systems demonstrates that image quality can materially influence false-negative rates and that demographic differentials remain an important consideration.

For Nigerian polytechnics, this means that system evaluation should not be limited to a single laboratory dataset. The system should be tested under different lighting conditions, camera heights, student demographics and classroom configurations.

6. Database Structure

Student Table

Field	***Description***
Student_ID	Unique student identifier
Name	Student name
Department	Academic department
Programme	Programme of study
Level	Academic level
Face_Template	Encrypted biometric template
Registration_Date	Date enrolled
Status	Active/inactive

Attendance Table

Field	*Description*
Attendance_ID	Unique transaction
Student_ID	Student identifier
Course_ID	Course
Date	Attendance date
Time	Attendance time
Recognition_Score	Matching confidence
Liveness_Score	Liveness confidence
Status	Present/rejected
Device_ID	Recording device

7. System Use Cases

Administrator

- register students;
- manage courses;
- enroll facial templates;
- manage users;
- generate reports.

Lecturer

- create attendance session;
- start camera;
- monitor attendance;
- view attendance summary;
- export reports.

Student

- present face to camera;
- receive attendance confirmation;
- review attendance record where permitted.

8. Contribution to Knowledge

The study is expected to contribute to knowledge in five major ways. First, it integrates facial recognition with anti-spoofing or liveness detection, thereby addressing attendance authentication as both an identification and security problem. Second, it proposes a lightweight architecture designed to operate within the resource limitations that may exist in Nigerian polytechnics, reducing dependence on highly sophisticated computing infrastructure. Third, the study provides an evaluation framework that considers recognition accuracy, liveness-detection accuracy, false acceptance, false rejection and processing time. This broader evaluation can provide a more meaningful assessment of the effectiveness and practical usability of automated biometric attendance systems.

Fourth, the study incorporates privacy-by-design principles into an educational biometric application. This is particularly relevant because facial images constitute biometric data under Nigeria's data-protection framework, requiring appropriate safeguards for privacy, security and responsible processing. Fifth, the study develops a prototype framework that can be adapted to Nigerian polytechnics and potentially extended to universities, colleges of education and other tertiary institutions. The framework may also provide researchers with a foundation for future studies involving biometric authentication, artificial intelligence, presentation-attack detection and secure educational technologies.

9. RECOMMENDATIONS

Based on the proposed design, the study recommends that polytechnics considering AI-based attendance systems should:

1. integrate liveness detection rather than deploying facial recognition alone;

2. evaluate the system using locally representative Nigerian datasets;
3. calibrate recognition thresholds using institutional validation data;
4. conduct privacy and data-protection assessments before deployment;
5. encrypt facial templates and restrict access to authorized personnel;
6. maintain alternative attendance procedures when facial recognition fails;
7. train ICT personnel responsible for system administration;
8. regularly test the system against emerging presentation attacks;
9. avoid using attendance data for unrelated surveillance purposes; and
10. conduct continuous monitoring of recognition accuracy and demographic performance.

10. CONCLUSION

This study proposes an AI-powered facial recognition attendance system with integrated anti-spoofing capabilities for Nigerian polytechnics. The central argument is that a modern attendance system should provide more than automated facial identification. It should establish both identity and presence before attendance is recorded. The proposed architecture therefore combines face detection, alignment, deep facial embeddings, identity matching, liveness detection, attendance validation and secure data management.

The results suggest that the proposed system could achieve approximately 97.2% facial-recognition accuracy, 95.9% anti-spoofing accuracy and sub-one-second attendance processing under controlled conditions. These figures are simulated targets rather than experimentally verified findings and should be replaced with actual measurements after system implementation.

The study also recognizes that technical performance alone is insufficient. Facial recognition involves sensitive biometric information, and Nigerian institutions must therefore consider privacy, security, fairness, transparency and human oversight. The Nigeria Data Protection Act 2023 provides an important regulatory foundation for such considerations

Ultimately, the proposed system offers a practical research and implementation framework for moving attendance management in Nigerian polytechnics from manual verification toward secure, contactless and intelligent authentication.

ACKNOWLEDGMENT

The author gratefully recognizes the **Tertiary Education Trust Fund (TETFund)**, for providing essential financial support through the Institutional Based Research (IBR) grant to **Abdu Gusau Polytechnic Talata Mafara** that facilitated the completion and publication of this scholarly work.

REFERENCES

Chen, S., Liu, Y., Gao, X., & Han, Z. (2018). MobileFaceNets: Efficient CNNs for accurate real-time face verification on mobile devices. *Chinese Conference on Biometric Recognition*, 428–438.

Deng, J., Guo, J., Xue, N., & Zafeiriou, S. (2019). ArcFace: Additive angular margin loss for deep face recognition. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 4690–4699.

International Organization for Standardization. (2023). *ISO/IEC 30107-3:2023: Information technology—Biometric presentation attack detection—Part 3: Testing and reporting*. ISO.

Nigeria Data Protection Commission. (2023). *Nigeria Data Protection Act, 2023*. Nigeria Data Protection Commission.

Nigeria Data Protection Commission. (2025). *Guidance and implementation materials on data protection impact assessment*. Nigeria Data Protection Commission.

Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A unified embedding for face recognition and clustering. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 815–823.

Satya Wacana, J. T., Sediyono, E., Hartomo, K. D., & Sembiring, I. (2024). Optimizing classroom attendance systems: Integrating liveness detection and deep learning for reliable face recognition. *JUITA: Jurnal Informatika*.