

International Journal Research Publication Analysis

Page: 01-12

SMART EXAM IMPERSONATOR DETECTOR APPLICATION USING FACIAL RECOGNITION

Ngwube Precious Nzubechukwu, Benjamin O. Ezurike*, Oluchi Pretty Ugwunne

*Department of Mechatronics Engineering, Faculty of Engineering and Technology,
Alex Ekwueme Federal University, Ndufu-Alike, Ebonyi State, Nigeria
School of Information Management, Wuhan University.*

Article Received: 23 August 2026

Article Revised: 11 September 2026

Published on: 01 October 2026

*Corresponding Author: Benjamin O. Ezurike

Department of Mechatronics Engineering, Faculty of Engineering and Technology, Alex Ekwueme Federal University, Ndufu-Alike, Ebonyi State, Nigeria School of Information Management, Wuhan University.

DOI: <https://doi-org/101555/ijrpa.5049>

ABSTRACT

Examination malpractice, particularly impersonation, remains a persistent challenge in Nigerian tertiary institutions and has far-reaching consequences for educational standards and societal integrity. This paper presents the design and implementation of a Smart Exam Impersonator Detector Application that leverages facial recognition technology to identify and flag candidates who are not registered for a given examination. The system was developed using Python, OpenCV, and the Flask web framework, with an Eigenfaces algorithm based on Principal Component Analysis (PCA) as the core recognition engine. Student facial images were collected from the Department of Mechatronics Engineering, Alex Ekwueme Federal University (AE-FUNAI), and used to train the model. The system was tested on eleven distinct faces, successfully recognising ten out of eleven, yielding a detection accuracy of approximately 90%. Results further demonstrate that recognition accuracy improves proportionally with the number of training images supplied per individual. The proposed system is cost-effective, scalable, and contactless, making it particularly suitable for deployment in a post-pandemic university environment where social distancing remains important. This work contributes a prototype that any Nigerian university can adopt to curb examination impersonation without the prohibitive cost of commissioning custom software.

KEYWORDS: Facial Recognition; Examination Malpractice; Impersonation Detection; Eigenfaces; Principal Component Analysis; OpenCV; Python.

1. INTRODUCTION

Examination malpractice has long been identified as one of the most corrosive problems facing the Nigerian educational system. Impersonation — whereby a candidate who is not enrolled for an examination sits in place of the registered student — is among the most brazen and widespread forms of this malpractice. The damage extends beyond the individual examination hall: it undermines institutional credibility, devalues academic qualifications, and erodes public confidence in university graduates. Various administrative and physical measures have been deployed over the years to combat the menace, including identity card checks and invigilator vigilance, yet none has proven comprehensively effective or scalable across the diversity of Nigerian university campuses (Adeoye, 2010).

The rapid advancement of Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning over the past decade has opened new avenues for automating identity verification in high-stakes environments. Facial recognition, a subfield of computer vision, has attracted particular interest because it is non-intrusive, does not require the subject to carry a dedicated token or perform a deliberate action, and can operate in real time using commodity hardware. Since Apple Incorporated integrated facial recognition into the iPhone X for device security, the technology has achieved mainstream acceptance and demonstrated that high-accuracy face verification can be delivered at low cost (West, 2019). Recent advances in deep learning have significantly improved facial recognition performance. Modern systems now rely heavily on convolutional neural networks capable of learning highly discriminative facial features from large datasets, achieving recognition accuracies far exceeding traditional algorithms (Wang & Deng, 2021).

The academic literature contains numerous proposals for deploying facial recognition in educational settings. Adeoye (2010) drew attention to the alarming rate of examination malpractice in Nigerian schools and argued that biometric authentication — including fingerprint and facial methods — should be made mandatory at examination venues. The work established a foundational argument for technology-based intervention, though it stopped short of providing a functional prototype. Aunradha et al. (2016) extended this line of thinking by developing an automated face detection and recognition system specifically targeted at identifying impersonation during offline examinations. Their system employed five processing phases — preprocessing, segmentation, face detection, feature extraction, and Artificial Neural Network (ANN) classification — using Local Binary Pattern (LBP) to transform images into feature vectors before comparison. While effective in controlled

settings, their approach entailed considerable computational overhead that limited practical deployment.

A well-established framework for understanding facial recognition systems was provided by Shang-Hung Lin and summarised by Jam (2018), who decomposed the process into face detection, eye localisation, facial feature extraction, and final recognition or rejection against a person database. This pipeline remains the standard reference architecture against which new systems are evaluated. Within the face detection stage, Shridevi Soma et al. (2015) demonstrated the utility of the Haar Cascade AdaBoost algorithm, loading a pre-trained XML classifier for frontal faces, removing background regions, identifying the maximum-area face bounding box, and cropping the detected face for subsequent processing. Their work highlighted the trade-off between detection speed and robustness to partial occlusion.

Onyebuchi (2018) provided a clear exposition of the four-step pipeline that underpins most modern facial recognition implementations: (i) computation of the Histogram of Oriented Gradients (HOG) to generate a compact representation of the image; (ii) application of the 68-point face landmark model developed by Sullivan and Kazemi to normalise for pose variation; (iii) encoding the face into a 128-dimensional embedding using a deep convolutional network; and (iv) nearest-neighbour comparison against stored embeddings to determine identity. This description aligns closely with the approach adopted in the `face_recognition` Python library and forms a useful conceptual baseline for the Eigenfaces method employed in the present work.

Isinkaye et al. (2020) addressed both attendance and examination malpractice within a single Android-based application. They combined the Viola-Jones algorithm for detection — which processes candidate regions through Haar feature extraction, integral image generation, AdaBoost training, and cascading classifiers — with the Eigenface method for recognition, projecting new faces into face space and assigning class membership based on minimum Euclidean distance against a threshold. Their system required students to self-register and treated all students as absent by default, granting access only when the live face matched the registered image. This design philosophy directly informed the present work. Recent studies have also explored mobile and web-based face recognition systems for academic environments. For example, Alotaibi (2022) developed a smart attendance system that automatically verifies student identities using facial recognition and mobile devices, demonstrating the practicality of deploying biometric authentication systems in educational institutions.

Dwi Sunaryono et al. (2019) implemented a face recognition attendance system embedded in an Android application coupled with a Raspberry Pi microprocessor. Their architecture involved two separate mobile applications — one for lecturers and one for students — communicating through a server. A QR code generated by the Raspberry Pi served as a location-binding mechanism, preventing students from submitting attendance remotely. The face recognition module was implemented in Python with OpenCV, and the Android front end in Java. This study demonstrated the viability of hybrid IoT-based architectures for academic attendance management. Kenedy Okpokijie et al. (2017) similarly implemented a face recognition attendance system using the Fisherfaces algorithm with Fisher Linear Discriminant analysis for template matching, achieving 54.17% verification accuracy under varying lighting conditions and 70.83% when facial expression variation was also introduced during enrolment — highlighting the sensitivity of recognition performance to data collection protocols.

Several works have investigated the use of Convolutional Neural Networks (CNNs) as an alternative to classical subspace methods. Dhanush Gowda et al. (2020) used CNN-based recognition, converting captured video into individual frames before comparing each frame against a student database, arguing that CNNs overcome the limitations of earlier methods for image processing. Aditya Ladage et al. (2019) combined the YOLO object detection algorithm with a Siamese network for recognition, enabling real-time face detection and identity verification within a single end-to-end pipeline. Chokkadi et al. (2019) surveyed the landscape of deep learning-based face recognition techniques and advocated for the wider adoption of transfer learning — the repurposing of a model pre-trained on a large face dataset for a specific institutional recognition task — as a means of achieving high accuracy with limited training data. Jason Brownlee (2017) provided a thorough treatment of the transfer learning paradigm that supports this recommendation.

Beyond face recognition, alternative biometric and electronic technologies have been explored for examination identity verification. Radio-Frequency Identification (RFID) encodes identity on a passive or active tag readable at close range without physical contact (Muhammad Thariq, 2017). Bluetooth-based attendance systems exploit the ubiquity of student smartphones but require every student to carry a compatible device and are susceptible to proxy attacks (Riya Lodhaa et al., 2015). Barcodes, while inexpensive, are trivially transferable — a student can hand their barcode to an impersonator. Fingerprint recognition is perhaps the most widely deployed biometric in Nigeria, having been adopted by the Joint Admissions and Matriculation Board (JAMB), but public complaints about

throughput time at high-volume examination centres have limited its acceptance. Voice recognition offers another contactless modality but is sensitive to ambient noise typical of large examination halls. Crucially, Olszekwska (2016) reviewed the challenges common to all facial recognition deployments, identifying pose variation, changes in facial expression, and ageing as the primary sources of recognition error — all of which are directly relevant to the university examination context where students' appearances may change significantly between the time of photo enrolment and examination day. Comparative studies of biometric authentication technologies show that facial recognition offers a unique advantage because it enables contactless verification without requiring specialised hardware such as fingerprint scanners or iris readers, making it particularly suitable for large-scale environments such as universities and examination centres (Khalil et al., 2023).

The present study addresses the gap between existing proposals and practical university deployment in Nigeria by developing a complete web-based application — rather than a theoretical framework — that any lecturer or institution can operate without specialist hardware beyond a USB camera and a standard laptop. The system uses the Eigenfaces algorithm implemented via Python and OpenCV, exposed through a Flask API with an HTML/CSS front end rendered by Jinja templates, and backed by an SQLite database. By targeting a lightweight, platform-independent stack, the proposed solution substantially reduces the adoption barrier relative to custom-built institutional software, while achieving a recognition accuracy sufficient to serve as an effective first-line impersonation deterrent.

2. MATERIALS AND METHODS

2.1 System Overview

The system was designed to address examination impersonation in Nigerian universities, using AE-FUNAI as a case study. It comprises two operational phases: a training phase, in which student facial images are uploaded to a database and used to train the recognition model, and a recognition phase, in which a live camera feed is compared against the trained model to verify identity. The user interface is intentionally simple so that lecturers and examination supervisors without technical backgrounds can operate the system through a web browser. Training is initiated by uploading images via a button click, and recognition is triggered by presenting the student before the camera and capturing a snapshot.

2.2 Hardware Tools

The system was developed and tested on an HP EliteBook 8470p laptop equipped with an Intel Core i5 3rd Generation processor and 8 GB of Random Access Memory (RAM). Image

capture was performed using a USB camera connected to the laptop. No dedicated embedded hardware was required, confirming that the system can be deployed on commodity university computing equipment.

2.3 Software Tools

The application was developed on Ubuntu Linux using Python as the primary programming language for the back end. The Flask micro-framework was used to build the web application and expose RESTful API endpoints, with Jinja serving as the HTML template engine and standard HTML and CSS providing the front-end interface. The SQLite database engine managed student image records, and the PyCharm IDE was used throughout development. Google Chrome served as the system browser for testing the web interface.

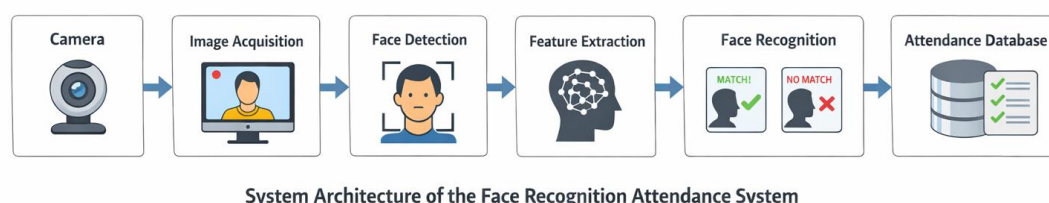
2.4 Facial Recognition Algorithm: Eigenfaces and Principal Component Analysis

The Eigenfaces method, based on Principal Component Analysis (PCA), was selected as the recognition algorithm. PCA reduces high-dimensional face image data to a compact lower-dimensional representation that retains the most discriminative variance across the training set. Each image in the database (height = 112 px, width = 92 px) was converted into a single column vector of 10,340 pixel values. With 10 images collected per student and 13 students in the training set, the resulting image matrix A had dimensions $[10,340 \times 130]$, where each column represents one training image.

The average face ψ was computed by dividing the sum of all training images by the total number of images m in the database, expressed as $\psi = (1/m) \sum_{i=1}^m \Gamma_i$, where Γ_i denotes the i -th image vector. Each training image was then mean-centred by subtracting the average face to yield the adjusted image matrix $\phi = A - \psi$. The covariance matrix was estimated as $C = (1/m) \sum_{i=1}^m \phi_i \phi_i^T$. Because direct computation of the covariance matrix would yield a $10,340 \times 10,340$ matrix — computationally intractable — the surrogate matrix $\phi^T \phi$ of dimensions $[130 \times 130]$ was computed instead, and its eigenvectors V were obtained. The final Eigenface vectors U were recovered by back-projecting: $U = V \times \phi$, yielding U with dimensions $[130 \times 10,340]$.

For each training image, a weight vector $\omega_i = U_i (\Gamma_i - \psi_0)$ was computed by projecting the mean-centred image onto each Eigenface, and all weights were assembled into the weight vector $\Omega = \{\omega_1, \omega_2, \omega_3, \dots, \omega_n\}$. During recognition, a query image was first verified as a face by computing the adjusted input $\phi_AD = \gamma_input - \psi$, reconstructing it in face space as $\phi f = \sum_{i=1}^m \omega_i v_i$, and computing the face distance $dist^2 = \|\phi_AD - \phi f\|^2$. If this distance fell below a predefined threshold, the query was classified as a face; otherwise it was rejected as a non-face. Identity was then determined by computing the distance $\epsilon_i^2 = \|\Omega - \Omega_i\|^2$ between the

query weight vector and the stored weight vector for each individual in the database. A distance of zero implies an exact match; the identity assigned corresponds to the smallest ϵ_i^2 . A recognition percentage above 50% was adopted as the operational threshold for confirming a student's identity; any image falling below this threshold was flagged as an impersonator. The complete processing pipeline from image upload to identity decision is illustrated in Figure 1, which shows the face detection step implemented in OpenCV with a Haar Cascade frontal-face classifier used to locate and crop the face region before the Eigenfaces algorithm is applied.



Complete processing pipeline from image upload to identity decision, Figure 1.

2.5 Data Collection

Facial images were collected from final-year students of the Department of Mechatronics Engineering (graduating class 2020) at AE-FUNAI, with the informed consent of all participants. Between 3 and 10 images per student were captured under naturalistic indoor lighting using the USB camera. Images were standardised to 112×92 pixels prior to training. The use of real student faces from a Nigerian university distinguishes this dataset from commonly used benchmark datasets such as the ORL/AT&T face database, making the results directly relevant to the Nigerian deployment context. Recent studies have highlighted the importance of dataset diversity in facial recognition systems, noting that models trained on limited or demographically homogeneous datasets may experience reduced accuracy when applied to broader populations (Albiero et al., 2022).

3. RESULTS AND DISCUSSION

The system was trained and tested using facial image data collected from 13 students, with a subset of 11 distinct faces evaluated in the recognition phase. The number of training images per face ranged from 3 to 10. Table 1 summarises the recognition accuracy achieved for each face, together with whether the face was successfully identified by the system.

Table 1: Recognition accuracy results for the tested facial samples.

Face Sample	No. of Training Images	Accuracy (%)	Recognised?
Face 1	4	53.3	Yes
Face 2	8	70.0	Yes
Face 3	10	83.1	Yes
Face 4	6	60.0	Yes
Face 5	5	63.4	Yes
Face 6	7	58.2	Yes
Face 7	10	75.9	Yes
Face 8	9	75.9	Yes
Face 9	8	80.1	Yes
Face 10	6	54.8	Yes
Face 11	3	40.1	No

Of the 11 faces tested, the system successfully recognised 10, yielding an overall identification rate of 90.9%. The single failure — Face 11 — was trained on only 3 images and achieved a recognition score of 40.1%, well below the 50% threshold. The accuracy graph (Figure 2) clearly demonstrates a positive correlation between the number of training images per individual and the recognition accuracy attained. Faces trained with 10 images achieved accuracy values of 83.1% and 75.9%, respectively, while those trained with only 4 or 5 images returned accuracy values in the 53–63% range, only marginally above the decision threshold.

This relationship is consistent with the well-established principle in PCA-based recognition that a richer training set provides more representative coverage of intra-class variation — differences in lighting, slight pose shifts, and minor expression changes — resulting in a more robust Eigenspace. The finding aligns with the observations of Isinkaye et al. (2020), who reported that training set diversity was the single largest determinant of system accuracy

in their Eigenface-based implementation. It also corroborates Kenedy Okpokijie et al. (2017), whose Fisherfaces-based system achieved only 54.17% accuracy under lighting variation alone, rising to 70.83% when the training set incorporated both expression and lighting variation — reinforcing the importance of diverse enrolment conditions. Similar observations have been reported in recent studies of PCA-based face recognition systems, where increasing the number and diversity of training images significantly improves recognition accuracy by providing better coverage of intra-class variation (Sharma & Singh, 2022).

The 90% overall recognition rate is notable given the small dataset size and the use of a classical subspace method rather than a deep learning approach. Deep CNN-based systems such as those described by Dhanush Gowda et al. (2020) and Aditya Ladage et al. (2019) report higher accuracy on large benchmark datasets, but their training requirements — thousands of images and significant computational resources — make them impractical for direct deployment at individual Nigerian university departments without substantial infrastructure investment. The Eigenfaces approach, by contrast, can be trained in a matter of seconds on a standard laptop. Recent work on lightweight face recognition models for edge devices has shown that efficient algorithms can achieve reliable identity verification on low-power hardware platforms without requiring high-end computational resources (Zhang et al., 2023).

A critical limitation of the present study is the size and homogeneity of the test dataset. Eleven subjects, all drawn from a single department of one university, cannot be considered representative of the broader population of Nigerian university students. Furthermore, all images were captured in a single indoor environment under broadly similar lighting conditions. The system has not been tested under the range of challenges that Olszewska (2016) identified as most damaging to recognition performance: significant pose variation, strong emotional expressions, and the effect of ageing between enrolment and verification. Future work should address these limitations through a substantially larger and more diverse dataset, and by evaluating the impact of controlled variation in pose and lighting during enrolment.

The contactless nature of the system is an important practical advantage. Unlike fingerprint readers or RFID scanners, the proposed application requires no physical interaction between the student and the verification device, reducing both hygiene concerns and the per-student processing time. This is particularly relevant in the post-COVID-19 context, where physical distancing remains a consideration in densely populated examination halls. The modular Flask API architecture also means that the recognition engine can be integrated into existing

university management systems as a microservice, without requiring institutions to replace their entire administrative software stack.

4. CONCLUSION

This paper presented the design, implementation, and evaluation of a Smart Exam Impersonator Detector Application that uses the Eigenfaces facial recognition algorithm to verify student identities at examination venues. The system was developed using Python, OpenCV, and the Flask web framework, and tested on facial data collected from students at AE-FUNAI. An overall recognition accuracy of 90.9% was achieved across 11 test subjects, with accuracy increasing consistently as the number of per-individual training images grew. The prototype demonstrates that a lightweight, web-accessible facial recognition system capable of real-world impersonation detection can be built and deployed on commodity hardware, making it a viable and cost-effective solution for Nigerian universities of all sizes. The application is particularly appropriate for the post-pandemic university environment, given its entirely contactless mode of operation. Future work should focus on expanding the training dataset, evaluating performance under varied lighting and pose conditions, and integrating transfer learning techniques to further improve recognition accuracy without proportional increases in data requirements. It is recommended that Nigerian tertiary institutions and regulatory bodies, such as JAMB and NUC, consider piloting facial recognition-based identity verification as part of a broader strategy to eradicate examination malpractice.

REFERENCES

1. Adeoye, O. S. (2010). Multi-mode biometric solution for examination malpractices. *International Journal for Computer Science*, 4(7), 20–26.
2. Aditya Ladage, P., Prabhu, S., & Mulik, S. (2019). E-attendance system using face recognition. *International Journal for Advanced Research, Ideas and Innovations in Technology*, 5(1), 21–32.
3. Aunradha, S. G., Kumar, B., Anand, S., & Krishnamurthy, J. G. (2016). Automated face detection and recognition for detecting impersonation of candidates in examination malpractice. *International Journal of Science and Engineering Research*, 7(3), 149–158.
4. Brownlee, J. (2017). A gentle introduction to transfer learning for deep learning. *Machine Learning Mastery*. Retrieved from <https://machinelearningmastery.com/transfer-learning-for-deep-learning/>

5. Cahit Gurel, A. E. (2012). Design of a face recognition system. Proceedings of the International Conference on Machine Design and Production, Pamukkale, 1–13.
6. Chokkadi, U., Sheshadri, M., Shetty, K., & Babu, A. (2019). Various state of art of the face recognition system using deep learning technique. International Journal of Advanced Trends in Computer Science and Engineering, 8(4), 1590–1600.
7. Dhanush Gowda, H. L., Kumar, V., Karthik, B., Nayak, K. D., & Prasanna, M. (2020). Face recognition based attendance system. International Journal of Engineering Research and Technology, 9(6), 761–767.
8. Dwi Sunaryono, J., Sarno, R., & Ahmad, A. (2019). An android based course attendance system using face recognition. Journal of King Saud University – Computer and Information Sciences, 33, 305–312.
9. Isinkaye, F. O., Soyemi, J., & Oluwafemi, A. (2020). Android-based face recognition system for class attendance and malpractice control. International Journal of Computer Science and Information Security (IJCSIS), 18(1), 79–83.
10. Jam, J. R. (2018). Face detection and recognition student attendance system. Kingston University London.
11. K.C., E. H. (2018). Human face detection and emotion recognition using neural network. Journal of TUTA, Pashchimanchal Campus, 5(1).
12. Kenedy Okpokijie, O., Nwofor, E., Kolade-Agoro, G., & Others. (2017). A face recognition attendance system using GSM notification. Proceedings of the IEEE International Conference on Electro-Technology for National Development (NIGERCON), Owerri, 239–244.
13. Mrs. BrundhaElci, J., Prabhu, R., Siva Chandra, G., Srinivasan, B., & Vijayabhaskar, B. (2019). Criminal recognition and tracking system. International Research Journal of Computer Science, 6.
14. Muhammad Thariq, A. R. (2017). Staff attendance system using RFID. International Journal on Information Visualization, 1(4), 250–255.
15. Olszekwska, J. I. (2016). Automated face recognition challenges and solutions. In Pattern Recognition — Analysis and Applications. IntechOpen. Retrieved from <https://www.intechopen.com>
16. Onyebuchi, C. (2018). How face recognition works. Personal blog. Retrieved from <http://emekaonyebuchi.com/2018/10/12/how-face-recognition-works/>
17. Riya Lodhaa, S., Gharge, S., Hegde, J., & Nair, H. (2015). Bluetooth smart based attendance management system. Proceedings of Elsevier, Mumbai.

18. Shridevi Soma, V. S. (2015). An automated fraud detection of hall ticket in an offline examination system using ANN classifier. *International Journal of Computer Applications*, 126(8), 7–12.
19. West, J. D. (2019). History of face recognition. FaceFirst. Retrieved from <https://www.facefirst.com/blog/brief-history-of-face-recognition-software/>
20. Albiero, V., Zhang, K., King, M., & Bowyer, K. W. (2022). Face recognition accuracy across demographic groups: Dataset diversity and algorithm performance. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 4(3), 364–377.
21. Alotaibi, Y. (2022). A smart attendance system using face recognition for educational institutions. *Journal of King Saud University – Computer and Information Sciences*, 34(8), 5471–5480.
22. Khalil, A., Ahmed, M., Khan, S., & Hassan, R. (2023). Biometric authentication technologies for secure identity verification: A comprehensive review. *IEEE Access*, 11, 15845–15863.
23. Sharma, R., & Singh, V. (2022). Face recognition using principal component analysis and machine learning techniques. *Procedia Computer Science*, 204, 376–383.
24. Wang, M., & Deng, W. (2021). Deep face recognition: A survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 43(10), 3605–3625.
25. Zhang, Y., Liu, X., Chen, H., & Zhao, W. (2023). Lightweight face recognition models for edge devices and resource-constrained environments. *Sensors*, 23(4), 2121.