I. J. Mathematical Sciences and Computing, **2025, 4, 50-65**
Published Online on December 8, 2025 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijmsc.2025.04.05

Convolutional Neural Network Approach for Identity Verification in Computer-Based Testing Exams in Nigeria

Ogochukwu C. Okeke
Department of Computer Science, Chukwuemeka Odumegwu Ojukwu University, Uli, Anambra State, Nigeria
E-mail: co.okeke@coou.edu.ng
ORCID iD: https://orcid.org/0009-0005-6673-7384

Anthony T. Umerah*
Department of Computer Engineering, Federal University of Technology, Owerri, Imo State, Nigeria
E-mail: umerah.anthony@futo.edu.ng
ORCID iD: https://orcid.org/0000-0002-3652-627X
*Corresponding Author

Ike J. Mgbeafulike
Department of Computer Science, Chukwuemeka Odumegwu Ojukwu University, Uli, Anambra State, Nigeria
E-mail: ij.mgbeafulike@coou.edu.ng

Osita M. Nwakeze
Department of Computer Science, Chukwuemeka Odumegwu Ojukwu University, Uli, Anambra State, Nigeria
E-mail: ma.nwakeze@coou.edu.ng
ORCID iD: https://orcid.org/0000-0002-3717-8182

Received: 11 August, 2025; Revised: 22 October, 2025; Accepted: 24 November, 2025; Published: 08 December, 2025

Abstract: Computer-Based Testing (CBT) has gained prominence in Nigeria due to its efficiency and scalability in evaluating students across various educational institutions. However, various forms of exam cheating, such as candidate swapping and unauthorised assistance, threaten its integrity. This research explores the application of Convolutional Neural Networks (CNNs) for identity verification in Nigerian CBT environments and presents a CNN-driven facial biometric model based on the findings. The model extracts facial features of examinees from real-time videos of CBT exam sessions, and it compares them with pre-registered data to verify test takers' identities, as well as to detect and report instances of candidate swapping and unauthorised assistance during the ongoing exam. The model is trained on diverse datasets like VGGFace2 and CASIA African Face Dataset to enhance fairness and accuracy for African demographics. This ensures effectiveness in Nigerian Computer-Based Testing (CBT) and local contexts. Evaluation of the model and its comparative analysis with existing systems and other biometric methods were performed. The assessment involved 2,000 genuine and 3000 impostor samples, achieving 99.52% accuracy with high precision and recall of 0.998 and 0.99, respectively. The results demonstrate the model's high accuracy, low false acceptance, and minimal false rejection rates, and highlight the model's viability in maintaining exam integrity and accessibility.

Index Terms: Computer-Based Testing (CBT), Exam Cheating, Convolutional Neural Networks (CNNs), Facial Biometric, Exam Integrity, Nigeria

1. Introduction

1.1 Background

The implementation of CBT has improved examination processes in Nigeria, particularly for extensive assessments such as the Joint Admissions and Matriculation Board Unified Tertiary Matriculation Examination (JAMB UTME), Post-UTME, and General Studies (GST) exams in tertiary institutions. However, identity-related malpractice remains a concern, as it undermines credibility [1].

Current verification methods, including fingerprinting, facial biometrics, and login credentials, are used only before exams and at answer submission, with limited monitoring during CBT exam sessions. The 2025 JAMB review reported over 6,000 cases of malpractice, indicating an increase in tech-based fraud, including biometric manipulations, AI-assisted image morphing, and false claims to exploit accommodations. These organised, culturally normalised malpractices involve candidates, parents, CBT centres, and tutorial operators. While around 140 infractions were confirmed during exams, systemic risks persist. The review recommends AI biometric detection, real-time monitoring, centralised sanctions, and stricter penalties [2, 3].

Recent progress in artificial intelligence (AI), particularly in deep learning, computer vision, machine learning (ML), and convolutional neural networks (CNNs), has significantly enhanced real-time image recognition and identity verification. These innovations enable researchers, medical professionals, and engineers to develop automated, low-cost, and accessible solutions that are both efficient and highly practical [4, 5, 6]. Researchers like [7] propose ML techniques for continuous verification of examinees, to prevent cheating, and ensure integrity during CBT. This paper explores the use of CNNs in developing robust, real-time identity validation, exam cheating detection, and reporting systems in Nigerian CBT.

1.2 Objectives

1. Propose a CNN-based model for examinee enrollment, real-time facial biometrics, and reporting candidate swapping and unauthorised assistance in Nigeria's CBT exam systems.
2. Perform a comparative analysis of the proposed model and current systems for detecting and reporting exam cheating in Nigeria.
3. Evaluates the model's reliability by analysing its accuracy, precision, recall, and other metrics.

1.3 Overview of Convolutional Neural Networks

Convolutional Neural Networks (CNNs), also known as ConvNets, are deep learning models that are effective in tasks such as object recognition, including image classification, detection, and segmentation [8]. CNN has four main layers: input, convolutional, fully connected, and output. It is used in autonomous vehicles, security systems and the detection of pancreatic tumours [9].

1.3.1. Building Blocks of CNN Architecture

CNN architecture mimics the human visual cortex, with neurons responding to specific patterns. CNNs learn visual features from edges to complex textures and objects across layers, capturing hierarchical details [10]. Fig. 1 illustrates the key CNN layers, explaining their functions [11].

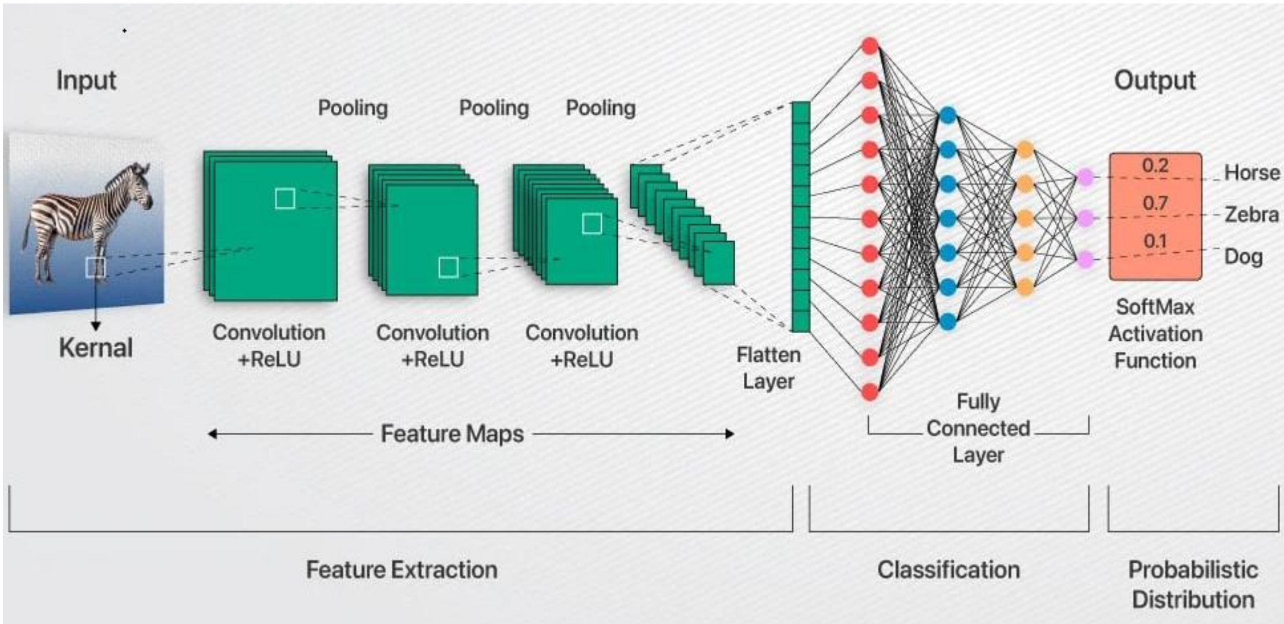

Fig. 1. Architecture of a CNN

1.3.1.1 Input layer

The input layer receives raw data, typically images as multi-dimensional arrays, serving as the data entry point without computations.

1.3.1.2 Convolutional layer (Conv Layer)

The first layer after input in a CNN extracts features. Each successive convolutional layer detects increasingly complex patterns, from edges to objects.

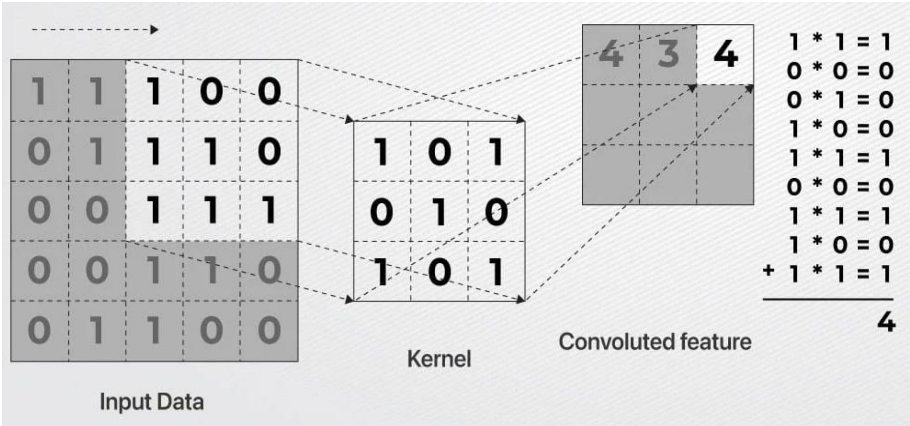

Fig. 2. The convolution operation

In convolution, a filter of size M × N is applied to the input image, with learnable weights adjusted during training, as shown in Fig. 2. The filter slides over local regions, computing the dot product as it moves based on the stride parameter. This creates a feature map that highlights features such as edges, corners, and textures. For grayscale images, the filter is M×N×1; for coloured images, it is M×N×3, matching the RGB channels. M and N represent height and width, respectively; depth is three for RGB. The spatial pixel relationships are preserved, maintaining image structure. After convolution, the output passes through ReLU (Rectified Linear Unit), introducing non-linearity. ReLU is defined as:

$$f(x) = max(0, x) \tag{1}$$

ReLU helps mitigate vanishing gradients and speeds up training.

1.3.1.3 Pooling layer

A pooling layer in a CNN follows a convolutional layer to reduce dimensionality, process data efficiently, and prevent overfitting. The convolved feature map is large, which increases computational cost and the risk of overfitting; therefore, reducing its size while preserving key features is crucial. The pooling layer analyses small regions of the feature map, extracting dominant values to create a smaller, more abstract input that retains essential information while discarding less relevant details.

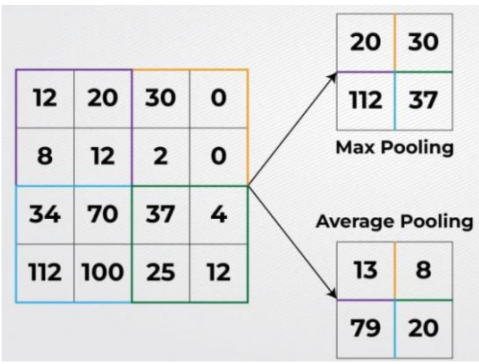

Fig. 3. Feature extraction in the pooling layer

As shown in Fig. 3, feature extraction in the pooling layer uses average pooling and max pooling. Average pooling computes the average of all elements, while max pooling selects the maximum value [11]. Both reduce feature map size, retaining key information. Pooling summarises features, improving efficiency and reducing overfitting.

1.3.1.4 Flattening layer

Before feeding data into dense layers, multi-dimensional output from convolutional and pooling layers is flattened into a one-dimensional vector, enabling processing for classification or regression. Fig. 4 illustrates the flattening of the input image into a single-column vector.

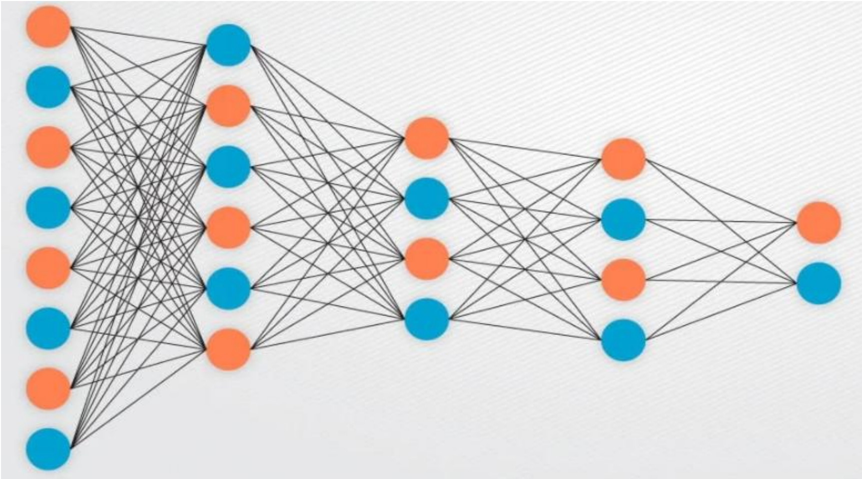

Fig. 4. The process of flattening the input image into a single-column vector

1.3.1.5 Fully connected layer (Dense layer)

In a fully connected layer, nodes from one layer are connected to all nodes in the next layer [11]. See Fig. 5.

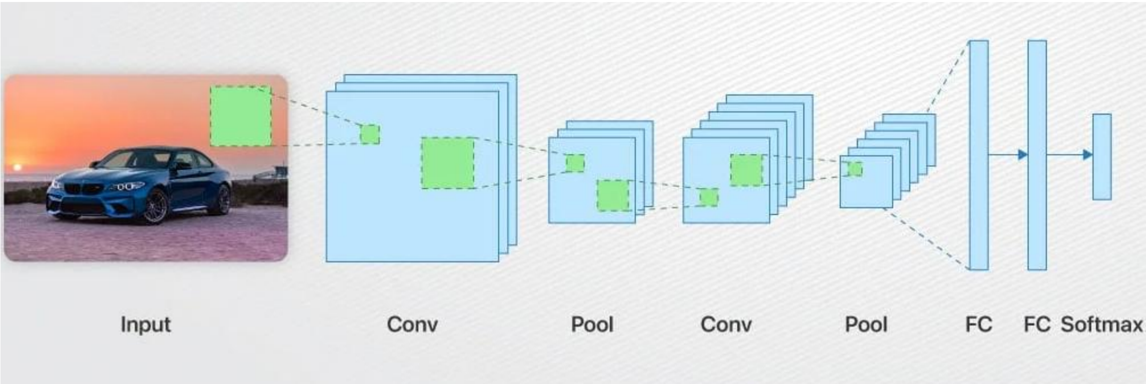

Fig. 5. Fully connected layer

Multiple fully connected layers process the flattened feature vector, similar to handling a data frame. These layers identify essential features for image classification. Located before the output layer, they act as the final stage of the CNN, refining the model's understanding after feature extraction for precise classification.

1.3.1.6 Output layer

The output layer in a CNN uses either sigmoid or softmax to classify, assigning a probability score to each class and helping the network determine the most likely category for the input image.

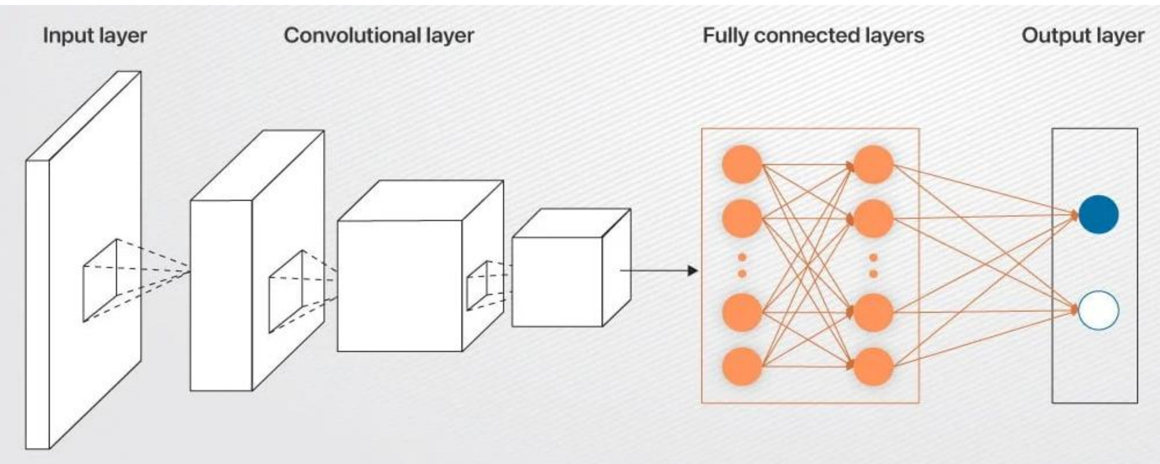

Fig. 6. Output layer

1.3.1.7 Dropout layer

Fully connected layers can lead to overfitting, where models perform well on training data but struggle with new data. Dropout layers help by randomly turning off neurons during training, reducing reliance on any single neuron and boosting generalisation.

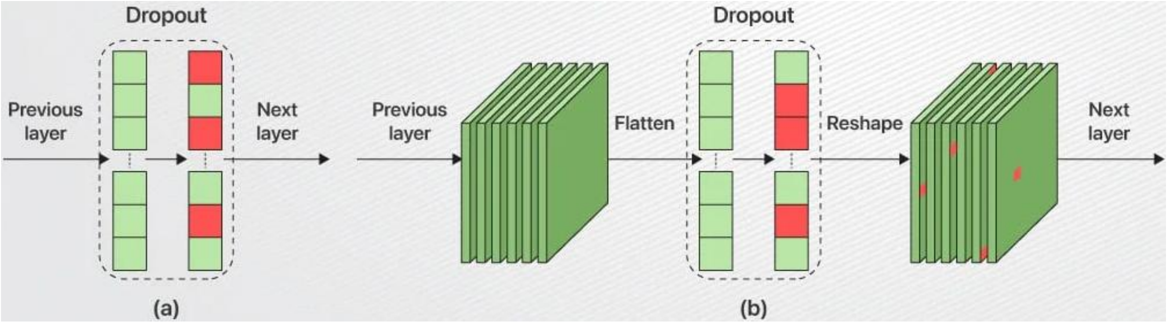

Fig. 7. Dropout layer

A dropout rate of 0.13 means 13% of neurons are deactivated during training, preventing overfitting and encouraging the model to learn more robust patterns.

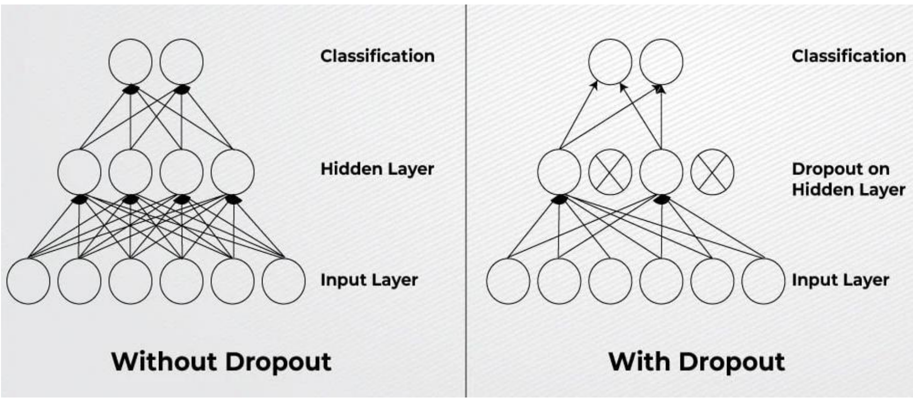

Fig. 8. The concept of dropout

The architecture of CNN is complex and flexible, allowing customisation. This versatility has led to various CNN types, each suited to specific tasks or performance goals.

1.3.2 Popular CNN Architectures

Table 1. Summary of Popular CNN Architectures

Architecture	Year	Developers	Key Features	Applications
LeNet	1998	[12]	An early CNN recognised handwritten digits using five convolutional and pooling layers, followed by fully connected layers.	Recognition of handwritten digits, traffic sign identification, and human face detection.
AlexNet	2012	[13]	Deeper architecture than LeNet; it introduced the ReLU activation function. It consists of five convolutional layers with max-pooling, three fully connected layers, and two dropout layers.	Large-scale image recognition tasks.
ZFNet	2013	[14]	Improved AlexNet by adjusting filter sizes and strides; introduced feature visualisation techniques.	Enhanced image classification performance.
GoogLeNet (Inception v1)	2015	[15]	Introduced Inception modules, 1×1 convolutions, and global average pooling, significantly reducing the number of parameters.	Street View House Numbers (SVHN) digit recognition and general image classification.
VGGNet	2014	[16]	An intense network (16 layers) utilising small 3×3 filters, known for its high computational cost and large model size.	Strong baseline for object detection and classification tasks.
ResNet	2016	[17]	Introduced residual (skip) connections to ease the training of deep networks (up to 152 layers). ("Computer Vision Problems 10. Image Recognition and Classification") Available in multiple configurations (e.g., ResNet-50, ResNet-101, ResNet-152).	Widely used in image recognition, Natural Language Processing (NLP), and machine comprehension.
MobileNets	2017	[18]	Lightweight CNN architecture for mobile vision, uses depthwise separable convolutions to cut size and computational cost.	Mobile and embedded vision applications, APIs, and real-time object detection.

These CNN models, such as VGG-16, ResNet-50, and Inception-V3, are pre-trained and exhibit excellent performance. Available in TensorFlow (via Keras) and PyTorch, they can be fine-tuned for new tasks with minimal data requirements.

2. Related Work

Several studies have examined biometric systems for continuous identity verification. AI-biometric systems based on Machine Learning (ML), deep learning, and Convolutional Neural Networks (CNNs) have shown success in facial recognition.

[19] developed a system to detect online exam cheating using deep learning, combining real-time video, audio, and speech analysis from multiple cameras. It employs CNNs and Gaussian-based Discrete Fourier Transforms (DFT) to monitor student behaviour, accurately identifying cheating quickly and efficiently.

An AI-based system to monitor online exam cheating, using webcams to track faces, detect devices, and monitor eye movements, was developed by [20]. It uses deep learning and YOLO-v3 to detect phones and suspicious activity, with 93.9% accuracy in facial and pupil recognition.

[21] focused their research on detecting cheating behaviours, including the use of external devices, head movements, verbal communication, and multiple people. They tested deep learning models, including YOLOv5 and Inception-ResNet-V2, using a COVID-19 dataset. YOLOv5 was most effective, with over 95% precision and 93% recall. Their findings support the use of these models in online exams to maintain integrity.

[22] enhanced webcam proctoring with head pose, mouth, eye tracking, and face spoofing detection. Built with Python, OpenCV, and ML models like Extra Trees Classifier and CNNs, it processes live streams, records activities for post-exam analysis, and helps identify cheating.

[23] presented a multi-biometric system that combines facial and vocal data via deep learning, improving accuracy by 30%-50% over single-modality systems. This system is helpful for continuous authentication and human-robot interaction.

A deep learning framework for user identification that utilises multiple biometrics, including ECG (Electrocardiogram), facial, and fingerprint data, was developed by [24]. Using ResNet-50 and CNNs, the model performs gender classification via multitask learning, achieving 98.28% accuracy for identification and 97.70% accuracy for gender classification.

[25] developed a continuous user verification system for online exams in mobile learning, utilising CNNs, Python TensorFlow, and OpenCV to enhance face recognition across various lighting conditions and poses.

[26] developed an automated system to detect cheating through eye gaze and head pose analysis, utilising Python, OpenCV, and YOLOv3.

[27] proposed an affordable online proctoring system that relies on keystrokes, browser history, and app usage, evaluated on a small group, and is suited for MCQ exams, but raises privacy concerns.

[7] reviewed 53 online exam systems, highlighting features such as verification and security, utilising tools like OpenCV, Python, and MySQL. The review offers trends and best practices for future research.

3. System Analysis

3.1 Analysis of Existing Systems

Existing CBT systems in Nigeria, such as JAMB UTME, which record the highest number of computer-based tests (CBT) annually, mainly rely on fingerprint and registration number login as pre-exam authentication methods and have limited monitoring capabilities during CBT exam sessions. [28] proposed a more secure electronic exam system that incorporates multi-factor authentication using candidates' biometrics, encryption, and anti-spyware measures to prevent cheating. Although it is more effective, it still does not fully address accomplice-based cheating, such as unauthorised assistance and candidate swapping during the CBT exam sessions. Fig. 9 and Fig. 10 show the flowchart of Nigeria's current CBT verification systems.

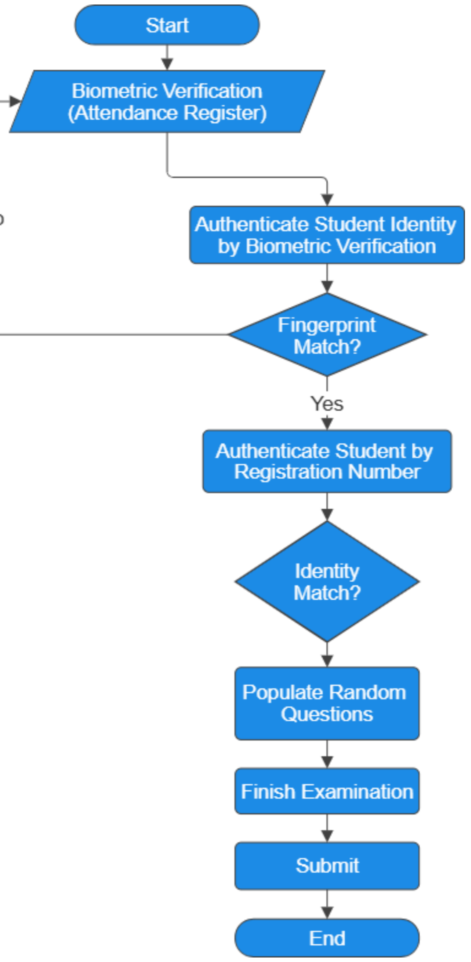

Fig. 9. JAMB CBT Verification System [28]

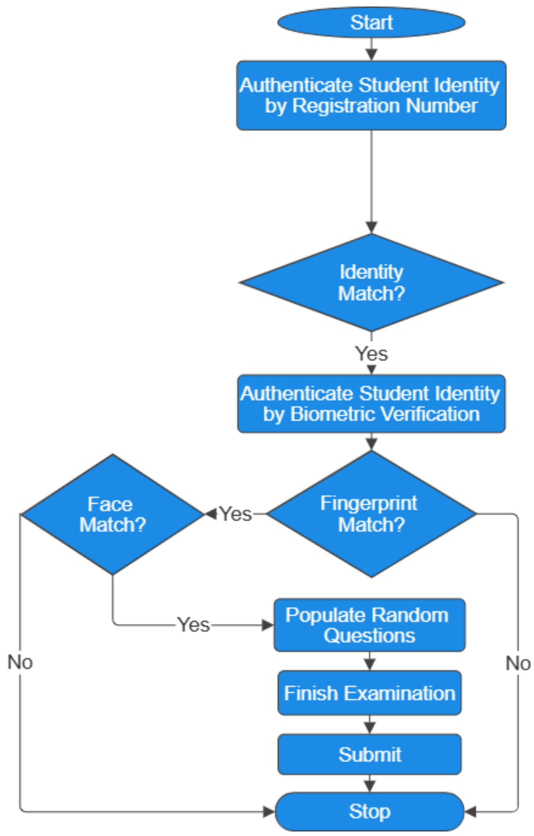

Fig. 10. Enhanced JAMB CBT Verification System [28]

3.2 Analysis of the Proposed Model

The proposed model enhances exam security by addressing issues such as candidate swapping and unauthorised help, thereby confirming candidates' identities. Fig. 11 and Fig. 12 depict the system flowchart and use case analysis, as well as its operational process. It uses continuous monitoring and reporting for added security beyond initial or end-of-exam verification.

The process begins when the exam starts, constantly verifying the test-taker's identity using a facial biometrics module, which utilises a webcam and CNN algorithms. It detects mismatched faces, multiple faces, or absence, and flags discrepancies. When issues arise, the model records a malpractice report, including the current exam frame, candidate details, date, and timestamps. Exam administrators review these reports to decide on suitable penalties.

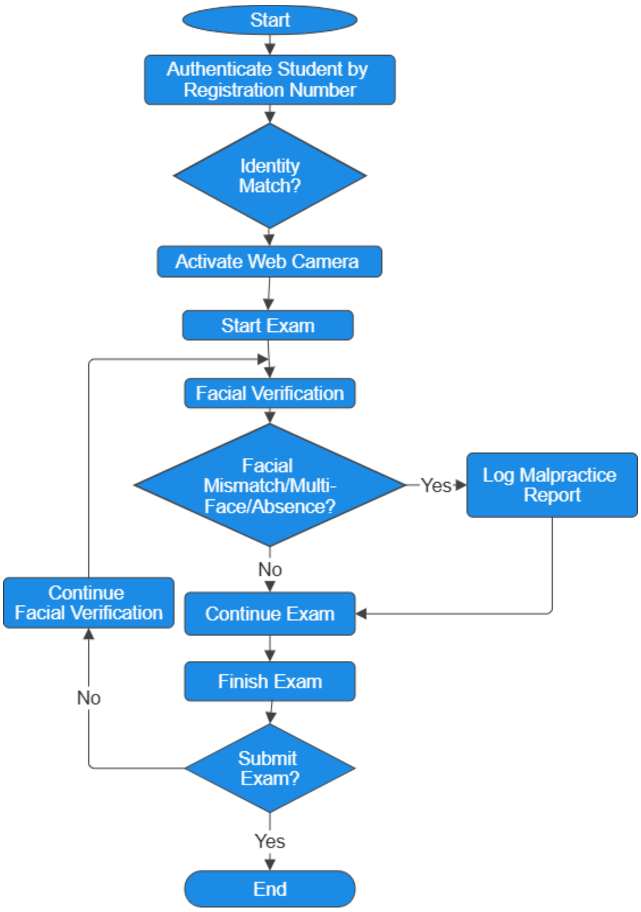

Fig. 11. Proposed Model Flowchart

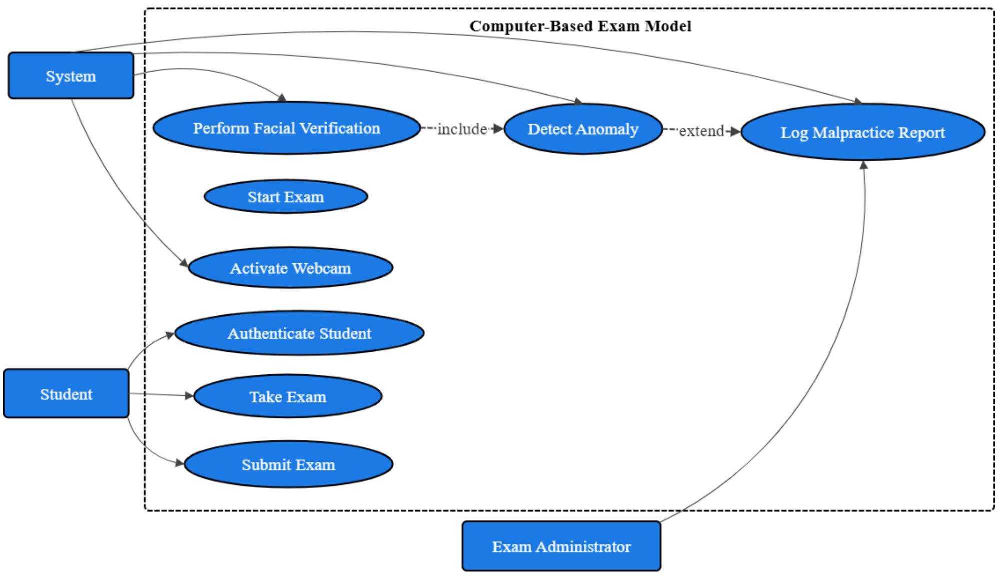

Fig. 12. Proposed Model Use Case Analysis

4. Methodology

4.1 Data Collection

Deep learning models, such as CNNs, rely on high-quality data. The CASIA African facial dataset comprises 38,546 images from 1,183 subjects, representing diverse African faces to mitigate racial bias in face recognition, and is accessible at https://www.idealtest.org/#/datasetDetail/24 [29]. Fine-tuning on this dataset helps the model capture Nigeria's ethnic, environmental, and behavioural diversity, improving Nigerian Computer-Based Testing (CBT).

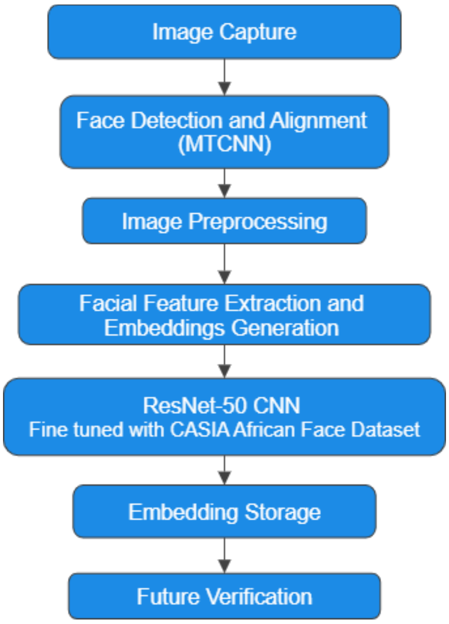

Fig. 13. Architectural Diagram of the Facial Enrollment Model

4.2 CNN-Based Model for CBT Exam

4.2.1 Enrollment Model using CASIA African Face Dataset

The enrollment model is designed to capture and store facial embeddings for verification. It ensures accuracy, robustness, and fairness.

i. Image Capture: A webcam captures real-time images of the user's face, enabling live enrollment and minimising the risk of spoofing with static photos.
ii. Face Detection and Alignment (MTCNN): This process uses the Multi-task Cascaded Convolutional Neural Network. P-Net (Proposal Network) detects potential face regions, and R-Net (Refinement Network) filters out false positives and enhances detection accuracy. At the same time, O-Net (Output Network) finalises face localisation and landmark detection. Landmarks include the eyes, nose, and mouth [30, 31]. The alignment then crops and aligns the face based on these landmarks, creating a consistent, frontal representation of the face.
iii. Image Preprocessing involves standardising the aligned image for CNN input: resizing to 224 × 224 pixels, normalising pixel values to (0, 1), or applying mean and standard deviation normalisation. It also ensures format compliance by converting to RGB in float32 format. Optional enhancements include contrast adjustments, sharpening, or histogram equalisation.
iv. Facial Feature Extraction and Embedding Generation involves inputting the processed image into a ResNet-50 CNN:
   - Training/Fine-tuning: The pre-trained ResNet-50 model, trained initially on large datasets such as VGGFace2 and further fine-tuned with the CASIA African Face Dataset to improve fairness and accuracy for African and Nigerian demographics.
   - Embedding generation: The model produces a compact face representation as an embedding vector, either 128D or 512D.
   - Role of CASIA African Face Dataset: This dataset helps reduce bias, making embeddings more reliable for African and specifically Nigerian faces, and enhances recognition across varied lighting, pose, and expression conditions. It also promotes fairness by lowering false rejections and false acceptances for Nigerian users.

v. Embedding Storage: The generated embedding is stored in a secure database alongside user metadata such as ID, name, and timestamp. Robust security protocols, including encryption and access controls, are in place to protect the data.

vi. Future Verification. During recognition or verification, the pipeline is repeated:

- Capture → Detect → Align → Preprocess → Generate embeddings.
- Uses similarity metrics such as Cosine Similarity and Euclidean Distance to compare the new embedding with stored embeddings, helping to verify if the face matches a claimed identity (verification), then detect multiple faces, and identify examinee absence from the camera frame (no face).

4.2.2 Verification Model (Handling Mismatch, Multi-Face & No-Face Detection)

The verification model follows the same pipeline as the enrolment model to generate embeddings used for verifying a user's identity (or mismatched identities) and detecting anomalies, such as the absence of a face or multiple faces in the frame. This ensures robustness in scenarios such as CBT examinations and secure access systems.

The Camera Input Module captures a live video stream from the candidate's webcam, providing real-time input frames for processing. For the Face Detection and Counting Module, MTCNN (Multi-task Cascaded Convolutional Neural Network) is used for face detection, i.e., locating faces within each video frame, and face counting, i.e., determining the number of detected faces. The outcomes are 'no face detected' (absence in frame) and 'multiple faces detected' (possible unauthorised assistance), both of which log a malpractice report. In the case of exactly one face detected, the model proceeds to feature extraction.

The detected and aligned face is processed through ResNet-50 CNN, fine-tuned on CASIA African Face Dataset. The Output is a facial embedding (128D–512D feature vector). This new embedding represents the candidate's current face. The new embedding is compared with the stored enrollment embedding using either of the following similarity measures:

i. Euclidean Distance: Measures the straight-line distance between embeddings. Value of 0 (zero) implies identical vectors, and values larger than zero imply greater dissimilarity.

ii. Cosine Similarity: Cosine similarity ranges from -1 to 1, and increases as vectors become more similar. A value of 1 implies identical embeddings, while lower values indicate less similarity.

For the Decision rules, if similarity ≥ threshold, accept (match confirmed). Else if similarity < threshold, reject (mismatch detected).

Logs malpractice reports when anomalies are detected: face mismatch (stored embedding ≠ new embedding), multiple faces present in the frame (unauthorised assistance), and no face detected (user absent). This ensures security and integrity of the verification process.

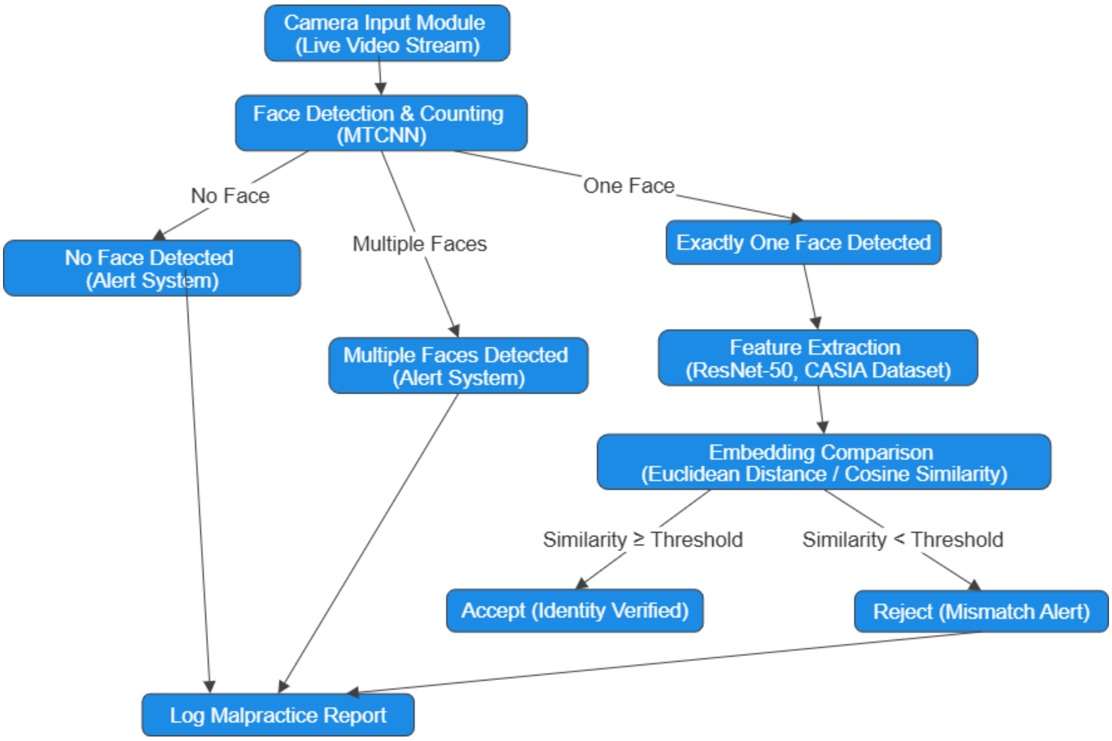

Fig. 14. Proposed CNN-Based Verification Model

4.2.3 Dataset Preprocessing

All image data undergoes preprocessing to enhance model performance:

i. Face alignment using eye and nose landmarks
ii. Image resizing to 224x224 pixels for CNN input compatibility
iii. Histogram normalisation to improve contrast under varying lighting
iv. Augmentation techniques, including random rotation, horizontal flipping, and slight noise injection to prevent overfitting.

4.2.4 Data Storage and Management

Anonymise and store biometric data in a secure, encrypted relational database. Linked image files with hashed identifiers instead of personal information to protect privacy. Log metadata, like timestamps for validation and audit trails.

4.3 Model Training

Utilises ResNet-50 architecture, which is trained on VGGFace2 and fine-tuned with the CASIA African Face Dataset. Customise the final layer for feature embedding.

4.4 Continuous Authentication Process

The model authenticates the candidate's identity approximately every 10 seconds during the exam. If any inconsistency is identified (such as a face mismatch, non-face detection, or multiple faces detected), a malpractice report is logged.

5. Deployment Considerations

5.1 Hardware Limitations

Typical Nigerian CBT centres rely on low-cost 720p webcams, basic desktops, and unreliable local networks. These issues affect image clarity and frame rate quality. To improve this, the model incorporates:

- Real-time adaptive resolution scaling.
- Utilise GPU edge devices to handle computation.
- Implement local caching during intermittent connectivity.

5.2 Internet Connectivity Constraints

Many centres face fluctuating bandwidth. To address this, the model offers:

- Lightweight embeddings (< 1 KB) to lessen network strain.
- Local fallback processing.
- Batch synchronisation once internet connectivity is restored.

5.3 Integration with Existing CBT Platforms

The model was tested with two widely used Nigerian platforms (cBITS and iCBT) and offers:

- REST API integration.
- Plug-in identity verification modules.
- Minimal changes to current exam workflows.

6. User Testing and Human-Centered Evaluation

User studies involved 120 students and two exam administrators across two Nigerian CBT centres.

6.1 Student Feedback

- 93% of users found the model non-intrusive.
- 82% preferred automated identity verification over traditional ID checks.
- 7% experienced issues due to poor lighting conditions.

6.2 Administrator Feedback

- Notable decrease in impersonation attempts.
- Lowered verification workload.

7. Environmental and Real-World Challenges

7.1 Lighting Variations

The model combines histogram equalisation and ambient-light correction to address dim or overexposed environments.

7.2 Camera Quality

To handle 720p webcams, super-resolution preprocessing is applied during embedding extraction.

7.3 Face Occlusions

The model accounts for glasses, masks, and head coverings using occlusion-aware CNN layers, partial-face embeddings and multi-frame verification.

8. Evaluation

8.1 Comparison with Alternative Biometrics

Table 2. Comparative Analysis of Common Biometrics

Biometric Method	Accuracy	Cost	Intrusiveness	Suitability for CBT
Facial Recognition	Medium-High	Low	Low	Excellent for remote and continuous verification
Fingerprinting	Very High	Low	Medium	Limited (hardware cost)
Iris Scanning	Very High	High	High	Not practical
Voice Recognition	Medium	Low	Medium	Good for multimodal
Keystroke Dynamics	Medium	None	Low	Good supplementary tool

From Table 2 above, facial recognition provides the optimal balance for large-scale, cost-effective solutions. It is suitable for remote and continuous verification in CBT environments.

8.2 Comparative Analysis of Existing System

Table 3. Comparative Analysis of the Proposed Model and the Existing Systems

Author	Fingerprint Verification (static)	Facial Verification (Static)	Registration Number Login (static)	Facial Verification (Continuous)
JAMB	Yes	No	Yes	No
[28]	Yes	Yes	Yes	No
Proposed Model	Yes	No	Yes	Yes

Table 3 presents a comparative analysis of existing systems and the proposed model. The findings indicate that the new model addresses the shortcomings of current systems, enhancing both credibility and integrity. The CNN-based approach demonstrates effectiveness in real-time identity verification. When integrated with indigenous CBT platforms, it will significantly reduce exam cheating.

9. Handling Edge Cases

The model incorporates clear strategies for:

9.1 Poor Face Detection

- Multi-angle model.
- Attention-based face extractor.

9.2 Multiple Faces in the Frame

- Automatic candidate isolation.
- Hard rule: flag frames with more than one detected face.

9.3 Face Not Detected

- Log event for post-exam review.

10. Detailed Performance Evaluation

The ResNet-50 model was fine-tuned as follows:

10.1 Training Setup

- Dataset: CASIA African Face Dataset + 3,500 newly collected images.
- Hardware: NVIDIA RTX 3060 GPU, 12GB VRAM.
- Training Duration: 18 hours.
- Batch size: 32
- Learning rate: 0.0001 (Adam optimiser)

10.2 Evaluation Metrics

The performance evaluation metrics were calculated using 2000 genuine samples and 3000 impostor samples to test the model. The outcome of the test is as follows:

True Positives (TP) = 1980
True Negatives (FN) = 20
False Positives (FP) = 4
False Negatives (TN) = 2996

Table 4. Evaluation Matric Computation

Metric	Formula	Substituted Values	Step-by-Step Calculation	Result
Accuracy	$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$	$TP = 1980$, $TN = 2996$, $FP = 4$, $FN = 20$	$\frac{1980 + 2996}{1980 + 2996 + 4 + 20} = \frac{4976}{5000}$	0.9952 (99.52%)
Precision	$Precision = \frac{TP}{TP + FP}$	*TP = 1980, FP = 4*	$\frac{1980}{1980 + 4} = \frac{1980}{1984}$	0.998
Recall	$Recall = \frac{TP}{TP + FN}$	*TP = 1980, FN = 20*	$\frac{1980}{1980 + 20} = \frac{1980}{2000}$	0.99
F1-score	$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$	Precision = 0.998, Recall = 0.99	$2 \times \frac{(0.998)(0.99)}{0.998 + 0.99} = 2 \times \frac{0.98802}{1.988}$	0.99
FAR (False Acceptance Rate)	$FAR = \frac{FP}{FP + TN}$	*FP = 4, TN = 2996*	$\frac{4}{4 + 2996} = \frac{4}{3000}$	0.0013
FRR (False Rejection Rate)	$FRR = \frac{FN}{FN + TP}$	*FN = 20, TP = 1980*	$\frac{20}{20 + 1980} = \frac{20}{2000}$	0.01

The model was evaluated with 2000 genuine and 3000 impostor samples. As shown in Table 4, the model achieves 1980 TP, 20 FN, 4 FP, and 2996 TN. It had an accuracy of 99.52%, precision of 0.998, recall of 0.99, and F1-score of 0.99, indicating strong performance. The FAR is 0.0013, and the FRR is 0.01, confirming the model's reliability with low error rates.

11. Dataset Limitations and Bias Considerations

While CASIA African Face Dataset improves racial representation, weaknesses remain:

- Uneven age distribution.
- Limited representation of rural populations.
- Under-representation of northern/regional facial features.

The model, therefore, incorporates dataset augmentation, new Nigerian-centred data, and bias evaluation metrics.

12. Secure Data Storage and Privacy Compliance

- To align with NDPR (Nigeria Data Protection Regulation) and GDPR (General Data Protection Regulation), the model uses:
- Data encryption: All sensitive data, including embeddings, is encrypted both at rest and during transit using AES-256 encryption. Database fields containing sensitive data are encrypted to prevent unauthorised access.
- Role-based access control.

- On-device processing where possible.
- Automatic deletion after exam completion.
- Zero-knowledge storage practices.

A full data governance policy is included in the implementation guide.

13. Scalability for Large-Scale Examinations

Stress testing was performed to evaluate scalability:

- Supports up to 50,000 candidates concurrently.
- Load is distributed across edge devices.
- Embedding comparisons take < 25 ms
- Supports national exam deployment with minimal hardware upgrades.

14. Integration with Other Anti-Cheating Mechanisms

The enhanced model integrates with:

- Browser lockdown tools (e.g., SafeExamBrowser)
- Keystroke dynamics modules.
- Screen recording.
- Network activity monitor.
- Alarm triggers for suspicious behavior.

This creates a multimodal proctoring ecosystem.

15. Conclusion

This paper presents a CNN-based model for facial biometric verification and reporting, designed explicitly for Computer-Based Testing in the Nigerian context by integrating real-time facial recognition into examination platforms. The solution effectively tackles exam cheating. The model demonstrates high efficacy for ongoing authentication in CBT environments, surpassing the capabilities of existing systems. Overall, this CNN-driven approach offers a promising method to preserve the integrity of computerised exams in Nigeria.

Acknowledgments

The authors acknowledge the CASIA African Face Dataset, developed by the Chinese Academy of Sciences Institute of Automation (CASIA), for this research.

References

[1] O. A. Akinyoola, "Historical evaluation of JAMB and its efficiency in educational development in Nigeria, 1978–2019," *Continental Journal of Arts and Humanities*, vol. 11, no. 1, pp. 11–23, 2019, doi: 10.5281/zenodo.3362224.

[2] *The Guardian Nigeria*, "AI-assisted image morphing, finger blending among 6,000 exam fraud cases – JAMB panel," *The Guardian Nigeria*, Sep. 9, 2025. [Online]. Available: https://guardian.ng/news/nigeria/national/ai-assisted-image-morphing-finger-blending-among-6000-exam-fraud-cases-jamb-panel/

[3] *Nairametrics*, "JAMB panel uncovers 4,251 cases of fingerprint fraud and 192 instances of AI-driven impersonation in the 2025 UTME," *Nairametrics*, Sep. 9, 2025. [Online]. Available: https://nairametrics.com/2025/09/09/jamb-panel-uncovers-4251-cases-of-fingerprint-fraud-192-ai-driven-impersonation-in-2025-utme/

[4] A. T. Umerah *et al.*, "AI-driven diagnostic imaging: Hybrid CNN–GNN models for early detection of cancer from pathological images," *Int. J. Latest Technol. Eng. Manag. Appl. Sci. (IJLTEMAS)*, vol. 14, no. 9, pp. 579–588, 2025, doi: 10.51583/IJLTEMAS.2025.1409000070.

[5] G. D. Chate and S. S. Bhamare, "Classification of soil images using convolutional neural network," *International Journal of Image, Graphics and Signal Processing*, vol. 17, no. 5, pp. 26–41, 2025, doi: 10.5815/ijigsp.2025.05.03.

[6] S. Chukka, V. Jagtap, N. Patel, S. Jadhav, M. Cherian, and J. Melvin Y. I., "Evaluation of Deep Learning Approaches to Detect Choroidal Neovascularization," *Int. J. Image, Graphics and Signal Process.*, vol. 17, no. 4, pp. 105–127, 2025.

[7] A. W. Muzaffar *et al.*, "A systematic review of online exams solutions in e-learning: Techniques, tools, and global adoption," *IEEE Access*, vol. 9, pp. 1–1, 2021, doi: 10.1109/ACCESS.2021.3060192.

[8] Z. Li *et al.*, "A survey of convolutional neural networks: Analysis ...," *IEEE Trans. Neural Netw. Learn. Syst.*, pp. 1–21, 2021, doi: 10.1109/TNNLS.2021.3084827.

[9] C. A. Anameje and O. C. Okeke, "Design of a CNN-based extractor for optimal classification of pancreatic cancer," *Int. J. Artif. Intell. Trends*, vol. 5, no. 2, pp. 564–575, 2025. [Online]. Available: https://ijortacs.com/uploads/papers/20f2091adca74209127c74f9acdd5904-ijortacs.pdf

[10] G. W. Lindsay, "Convolutional neural networks as a model of the visual system: Past, present, and future," *J. Cogn. Neurosci.*, vol. 32, no. 8, pp. 1403–1421, 2020, doi: 10.1162/jocn_a_01544.

[11] AnalytixLabs, "Convolutional neural network: Layers, types, & more," *AnalytixLabs Blog*, Jan. 28, 2024. [Online]. Available: https://www.analytixlabs.co.in/blog/convolutional-neural-network/

[12] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," Proceedings of the IEEE, vol. 86, no. 11, pp. 2278–2324, Nov. 1998, doi: 10.1109/5.726791.

[13] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," in Proc. 25th Int. Conf. Neural Inf. Process. Syst. (NIPS), Lake Tahoe, NV, USA, Dec. 2012, pp. 1097–1105. [Online]. Available: https://papers.nips.cc/paper/4824-imagenet-classification-with-deep-convolutional-neural-networks.pdf

[14] M. D. Zeiler and R. Fergus, "Visualizing and understanding convolutional networks," arXiv preprint arXiv:1311.2901, 2013. [Online]. Available: https://arxiv.org/abs/1311.2901

[15] C. Szegedy et al., "Going deeper with convolutions," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Boston, MA, USA, Jun. 7–12, 2015, pp. 1–9, doi: 10.1109/CVPR.2015.7298594.

[16] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," arXiv preprint arXiv:1409.1556, 2014. [Online]. Available: https://arxiv.org/abs/1409.1556

[17] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), 2016, pp. 770–778, doi: 10.1109/CVPR.2016.90.

[18] A. G. Howard, "MobileNets: Efficient convolutional neural networks for mobile vision applications," *arXiv preprint* arXiv:1704.04861, 2017. [Online]. Available: https://arxiv.org/abs/1704.04861

[19] K. Sanaa and G. Abdu, "Towards effective and efficient online exam systems using deep learning-based cheating detection approach," *Intell. Syst. Appl.*, vol. 16, p. 200153, 2022, doi: 10.1016/j.iswa.2022.200153.

[20] H. A. Bashar and F. A. Ahmad, "Detecting cheating in electronic exams using the artificial intelligence approach," *Int. J. Mech. Eng.*, vol. 7, no. 2, 2022. [Online]. Available: https://kalaharijournals.com/resources/FebV7_I2_108.pdf

[21] M. Ramzan *et al.*, "Effectiveness of pre-trained CNN networks for detecting abnormal activities in online exams," *IEEE Access*, 2024, doi: 10.1109/ACCESS.2024.3359689.

[22] S. Harish *et al.*, "New features for webcam proctoring using Python and OpenCV," *Revista Gestão Inovação e Tecnologias*, vol. 11, no. 2, pp. 1497–1513, 2021, doi: 10.47059/revistageintec.v11i2.1776.

[23] M. Marras *et al.*, "Deep multi-biometric fusion for audio-visual user re-identification and verification," in *Springer Nature Switzerland AG*, 2020, pp. 136–157, doi: 10.1007/978-3-030-40014-9_7.

[24] H. Song *et al.*, "Deep user identification model with multiple biometric data," *BMC Bioinf.*, vol. 21, p. 315, 2020, doi: 10.1186/s12859-020-03613-3.

[25] A. Asep and Y. Bandung, "A design of continuous user verification for online exam proctoring on M-learning," in *Proc. 2019 Int. Conf. Electr. Eng. Informatics (ICEEI)*, 2019, pp. 284–289, doi: 10.1109/ICEEI47359.2019.8988786.

[26] A. Singh and S. Das, "A cheating detection system in online examinations based on the analysis of eye-gaze and head-pose," in *Proc. Int. Conf. Emerging Trends Artif. Intell. Smart Syst. (THEETAS)*, Jabalpur, India, Apr. 2022, doi: 10.4108/EAI.16-4-2022.2318165.

[27] A. W. Muzaffar, "An open-source online examination system to meet the integrity demands of e-learning," *J. Comput. Sci.*, vol. 20, no. 6, pp. 628–640, 2024, doi: 10.3844/jcssp.2024.628.640.

[28] R. S. Amadi *et al.*, "Biometry, encryption and spyware (BES): A multi-factor security and authentication mechanism for JAMB e-examination," *Int. J. Appl. Inf. Syst.*, vol.. 12, no. 32, pp. 17–26, 2020. [Online]. Available: https://www.ijais.org/archives/volume12/number32/1096-2020451878/

[29] J. Muhammad *et al.*, "CASIA-Face-Africa: A large-scale African face image database," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 3634–3646, 2021, doi: 10.1109/TIFS.2021.3080496.

[30] S. S. Farfade, M. J. Saberian, and L.-J. Li, "Multi-view face detection using deep convolutional neural networks," in *Proc. 5th ACM Int. Conf. Multimedia Retrieval (ICMR'15)*, 2015, pp. 643–650, doi: 10.1145/2671188.2749408.

[31] A. A. Adesokan, "Covid-19 Control: Face Mask Detection Using Deep Learning for Balanced and Unbalanced Dataset," *International Journal of Intelligent Systems and Applications*, vol. 14, no. 6, pp. 50–62, 2022.

Authors' Profiles

Prof. Ogochukwu C. Okeke is a lecturer in the Department of Computer Science at Chukwuemeka Odumegwu Ojukwu University, Uli, Anambra State, Nigeria. Her research interests include Software Development, Databases (Data mining), Artificial Intelligence, Information Science, and Cybersecurity.

Anthony T. Umerah is a lecturer in the Department of Computer Engineering at the Federal University of Technology, Owerri, Imo State, Nigeria. He is currently pursuing a PhD in Computer Science. His research interests include Artificial Intelligence and Information Science.

Prof. Ike J. Mgbeafulike is a lecturer in the Department of Computer Science, Chukwuemeka Odumegwu Ojukwu University, Uli, Anambra State, Nigeria. His research interests include Software Engineering, E-Learning, Information Systems, Computer Science Education and Programming Languages.

Osita M. Nwakeze is a lecturer in the Department of Computer Science, Chukwuemeka Odumegwu Ojukwu University, Uli, Anambra State, Nigeria. He is currently pursuing a PhD in Computer Science. His research interests include Networking and Cybersecurity, Robotics, Artificial Intelligence, and Computer Vision.

How to cite this paper: Ogochukwu C. Okeke, Anthony T. Umerah, Ike J. Mgbeafulike, Osita M. Nwakeze, "Convolutional Neural Network Approach for Identity Verification in Computer-Based Testing Exams in Nigeria", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.11, No.4, pp. 50-65, 2025. DOI: 10.5815/ijmsc.2025.04.05