An Optimised Artificial Neural Network Model for a Three-Level Authentication Security Scheme Utilising Fingerprint, Facial Recognition, and Optical Character Recognition

[1]Adeyemi Biliqees Temitope, [2]Makinde, Oladayo Ezekiel

[1]Department of Computer Science, Kwara State College of Education, Ilorin, Nigeria

[2]Department of computer science, Ajayi Crowther University, Oyo, Nigeria

DOI: https://doi.org/10.51584/IJRIAS.2026.11050051

Received: 02 May 2026; Accepted: 08 May 2026; Published: 27 May 2026

ABSTRACT

The rapid increase in the use of digital technologies in daily activities has created both opportunities and threats. The paper reports an optimized Artificial Neural Network (ANN) model for implementing a three-tier authentication system using fingerprint biometrics (Level 1), facial recognition (Level 2) and Optical Character Recognition (OCR) (Level 3). The model is created using a multi-layer perceptron optimized using Adam and L2 regularization in order to have better accuracy and stability under environmental changes. On NIST SD4, LFW, and IAM datasets, an overall accuracy of 97.8% was reached with a false acceptance rate (FAR) of less than 1.0% was attained through experimental evaluation. The results show that the suggested model is better than unimodal techniques by about 16%, which proves its possible ability to protect e-learning and administrative systems at Nigerian universities.

Keywords: Artificial Neural Network, Multimodal Authentication, Biometric Security, Deep Learning, Cybersecurity in Education, Educational Technology

INTRODUCTION

The explosion in the use of digital technology in schools has significantly transformed the creation, learning, administration, and storage of information. Online learning platforms, digital exam systems, and electronic student records have opened up education to more people, made it more efficient, and allowed it to grow. Nevertheless, Al-Haija (2023) observed that the shift towards digital has also brought about some unforeseen safety issues, almost entirely unauthorized access, data breaches, and identity theft. Verizon (2023) states that more than eighty percent breaches in digital systems are due to compromised or weak passwords, which is a clear indication of the limited nature of conventional authentication methods. In order to overcome these problems, biometric authentication systems have been proposed as one of the solutions. Such systems identify a person using one or a combination of their unique physical and behavioural characteristics such as fingerprints, facial features, iris patterns, and typing behaviours.

According to Abdulrahman & Alhayani (2023), biometric identifiers are highly secure and have a low probability of being copied or leaked unlike passwords or security tokens since they are directly linked to the individual. Although environmental changes such as low light and background noise can affect unimodal biometric systems that rely one type of information, like fingerprints or facial recognition (Yang et al., 2023; IBM, 2023). These systems can also be tricked and make mistakes with sensors. These problems make it important to adopt multimodal authentication methods. These systems use different biometric types to make security, dependability, and accuracy better. By combining the strengths of each modality and at the same time offsetting their weaknesses, multimodal systems provide better performance. For example, while fingerprint recognition can be affected by cuts or wear on a finger, facial recognition may fail under poor lighting; combining both modalities significantly increases the likelihood of successful authentication. Within the context of education, especially in developing nations like Nigeria, the use of biometric systems is further hindered by the lack of proper infrastructure such as frequent power outages, poor quality cameras, and limited network capabilities (Thota &

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

Menaka (2024). These limitations necessitate the development of strong, resource, efficient and highly optimized authentication mechanisms that can work efficiently even in such compromised situations.

This paper presents an optimised Artificial Neural Network (ANN) model for a three level multimodal authentication system fusing fingerprint biometrics (Level 1), facial recognition (Level 2), and ID card Optical Character Recognition (OCR) (Level 3). The adoption of Adam optimization and L2 regularization enables the model to achieve not only high accuracy but also consistent performance under varying environmental conditions, thus providing a viable and extendable approach for the protection of electronic learning platforms, administration systems, and other digital resources in Nigerian universities.

LITERATURE REVIEW

AI powered biometric authentication systems have been booming recently, with AI and deep learning being the major contributing factors. One of the most promising areas where biometrics have been integrated with AI is multimodal biometric systems which have significantly outshone unimodal systems in terms of performance (Almuqren et al., 2023; Garg et al., 2023). Also, Ross and Jain (2023) highlighted that by combining multiple modalities such as fingerprint, facial, and iris recognition, it is possible to significantly improve recognition accuracy while also reducing the false acceptance rate (FAR). Singhal and Shinghal (2023) concur with this view as they further go on to explain that operating different safeguards simultaneously such as combining fingerprint, facial and iris modes, enables one's device to be less vulnerable to spoofing attacks and at the same time environmental disturbances. For this reason, the authors recommend security critical applications to consider such systems.

Fingerprint identification is generally acknowledged as the leading biometric technology, being highly regarded for its uniqueness, non invasive nature, and reasonable price. Khan et al. (2024) have shown how the effectiveness of the fingerprint recognition system could be further increased by combining deep learning with convolutional neural networks (CNNs) and inversion techniques. This has led to better pattern matching capability. On the other hand, there are situations where, e.g., dirty, damaged or worn fingers, the fingerprint alone might not be enough to identify the person. In such scenarios, complementary modalities could come to the rescue if they are put in place (Chander & Upendra Kumar, 2023). The facial recognition allows a seamless and non intrusive kind of authentication that could be rolled out for large user communities and thus can identify persons in real time. Pahuja and Goel (2024) suggested that if facial and iris features are combined, the systems would be more robust even under different environmental conditions. Even such a system, however, would need more computing power.

Furthermore, a unimodal system's performance alone can also be degraded by environmental factors such as poor lighting or background noise. Therefore, the role of fusion strategies for multimodal systems is emphasized. When an identity document or student card is scanned through Optical Character Recognition (OCR), it essentially brings another verification dimension, i.e., the textual one that goes along with physiological biometrics (Das et al., 2023; Hasan, 2023; Liu et al., 2023). This extra layer ensures that the verification process can still occur through alternative data sources if one biometric modality fails or gets compromised. Studies have shown that multimodal systems that use OCR can significantly increase the robustness and security of administrative applications (Charmet et al., 2022; Vijayakumar, 2023; Islam et al., 2023).

Moreover, besides the appropriate combination of learning algorithms, and preprocessing methods, the fine, tuning of the neural network's architecture or structure is also a vital part of the process that leads to high accuracy and efficient convergence. Omer et al. (2023) emphasised that a combination of Adam optimiser and L2 regularisation is helpful to avoid overfitting while at the same time performance stays consistent when input conditions change. Likewise, Jyothi et al. (2024) revealed that well tuned ANN models can run efficiently even in resource constrained environments, thus meeting the requirements for developing countries with limited computational infrastructure.

However, some progress has been made, most of the research has been carried out in the industrial or general security arenas. Only a few studies have targeted educational settings in developing countries. For example,

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

universities in Nigeria encounter problems like power cuts, use of cheap hardware, and unstable network that can easily affect the reliability of traditional biometric systems. This clearly shows a research gap: there is an immediate need for highly efficient, low resource multimodal authentication frameworks that are specifically designed for educational institutions and capable of securing digital learning platforms, student records, and administrative systems. This research addresses that gap by introducing a three, level multimodal ANN model that combines fingerprint, facial, and OCR features and is capable of operating effectively in the different environmental conditions that are typical of Nigerian universities.

METHODOLOGY

Data Acquisition and Preprocessing

The study adopted an experimental quantitative research design to evaluate the effectiveness of a multimodal authentication framework under varying environmental conditions. Three publicly available datasets were utilised because of their reliability, accessibility, and extensive adoption in biometric authentication research. Fingerprint samples were obtained from the NIST SD4 dataset, facial images were acquired from the Labelled Faces in the Wild (LFW) dataset, while textual identity information for Optical Character Recognition was sourced from the IAM handwritten text dataset.

A total of 7,200 multimodal samples were used for the experiment. The data was divided into training, validation, and testing data sets with a ratio of 70:15:15. Before training the models, pre-processing operations were carried out for each biometric mode independently in order to remove any noise and ensure uniformity of features.

The pre-processing phase for the fingerprint images involved normalization to greyscale values, enhancement of the ridges, filtering out noise from the image, and sharpening of the image.

Facial images were subjected to facial alignment, image resizing, illumination normalisation, and histogram equalisation to reduce variations caused by lighting conditions, pose differences, and background interference. The images were subsequently converted into feature representations suitable for neural network processing.

For the OCR component, identity card text samples underwent binarization, skew correction, segmentation, and character normalisation to improve text extraction accuracy. These pre-processing procedures reduced optical distortion and enhanced recognition consistency under varying image acquisition conditions.

Feature Fusion and ANN Optimisation

The proposed authentication framework utilised an early fusion multimodal strategy in which extracted features from fingerprint, facial recognition, and OCR modalities were combined before classification. The fusion process assigned weighted contributions of 45% to fingerprint biometrics, 35% to facial recognition, and 20% to OCR features. These weights were selected empirically based on preliminary validation experiments and the relative reliability of each modality under environmental disturbances. Fingerprint recognition received the highest weighting because of its strong uniqueness and stability characteristics, while OCR contributed the lowest weighting because of its higher sensitivity to image distortion and textual inconsistencies.

The classification stage employed a multilayer Artificial Neural Network architecture consisting of three hidden layers containing 512, 256, and 128 neurons respectively. Rectified Linear Unit activation was adopted because of its computational efficiency and ability to minimise vanishing gradient problems. Softmax classification was implemented within the output layer to facilitate multiclass authentication decisions.

To improve convergence stability and minimise overfitting, the Adam optimiser was employed with a learning rate of 0.0005, while L2 regularisation with a coefficient value of 0.01 was incorporated during model training. The optimisation strategy was selected because of its suitability for resource constrained computational environments commonly associated with developing educational institutions.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

Environmental Simulation and Evaluation

To evaluate robustness under practical conditions, environmental simulations were introduced during testing. Low light conditions were simulated at approximately 50 lux illumination intensity, while high noise environments incorporated signal disturbances of approximately 30 dB. Combined environmental conditions involving simultaneous illumination degradation and acquisition noise were also introduced to assess system resilience under adverse operational scenarios.

System performance was evaluated using standard biometric authentication metrics including accuracy, precision, recall, and False Acceptance Rate (FAR). Statistical significance testing was further conducted using Analysis of Variance in order to determine whether the optimised multimodal framework significantly outperformed conventional unimodal authentication approaches.

RESULTS AND DISCUSSION

The ANN model was optimised and performed better under all environmental conditions. In the ideal case study, the fused system was able to achieve an accuracy of 98.2 percent and a FAR of 0.7 percent. The model had 97.8% accuracy in low-light conditions, and 97.5% accuracy in high noise conditions. ANOVA statistical analysis showed significant improvement over the conventional multimodal systems ($F=12.34$, $p=0.001$).

Table 1: Performance Metrics Across Authentication Levels and Conditions

Condition	Level	Accuracy (%)	Precision (%)	Recall (%)	FAR (%)
Optimal	Fingerprint	99.2	99.0	99.4	0.5
Optimal	Facial	97.8	97.5	98.1	1.2
Optimal	OCR	97.3	97.1	97.5	1.3
Low Light	Fused Overall	97.8	97.6	98.0	0.9
High Noise	Fused Overall	97.5	97.3	97.7	1.0

CONCLUSION

The paper shows that an optimized Artificial Neural Network (ANN) model was able to provide a reliable and robust framework for multimodal authentication in educational environments. The study combine fingerprint biometrics, facial recognition, and Optical Character Recognition (OCR) of ID cards in a three-level authentication system to overcome the issues of unimodal systems, such as spoofing attacks, sensor failures, and environmental variations. The system was tested in various scenarios including low-light and high, noise conditions and was able to achieve, on average, a 97.8% success rate and less than 1% false acceptance rate. The authors view these figures as a significant improvement over unimodal methods, and thus supporting the idea of multimodal biometric authentication.

The research, however, goes beyond simply demonstrating a technologically superior system. It offers some valuable locally grounded insights for educational institutions, especially those located in developing countries like Nigeria where the general lack of infrastructure can render conventional authentication systems unreliable. The proposed model is geared towards low resource settings by focusing on aspects like computational efficiency, robustness against environmental changes, and scalability. As a result, it can be an effective solution for e-learning platforms, administrative systems, and the protection of sensitive student data, thus contributing to the overall trustworthiness of digital education systems. The study also advances the general discipline of cybersecurity in education by providing evidence for the effectiveness of optimization methods like Adam and L2 regularization in improving neural network stability and performance. Additionally, it underlines the fact that multimodal authentication is not only a safer alternative to traditional password-based or unimodal systems but also that it can help protect against unauthorized access and identity fraud at the institutional level.

Limitation of the Study

Although the proposed multimodal authentication system performed satisfactorily, there are various weaknesses that cannot be overlooked. Firstly, the experiment was conducted mainly using benchmark data sets from public

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

domains such as NIST SD4, LFW, and IAM datasets. Although this makes it possible to test for the consistency of the model in a standard setting, the data sets might fail to account for the diverse nature of the population of Nigerian tertiary institutions, as well as the operational environment within which the model must operate. The second drawback is that no pilot test was done on the proposed model within actual Nigerian universities.

Another limitation of the study lies in the scope of comparative modelling. The research focused primarily on optimisation of an Artificial Neural Network architecture using Adam optimisation and L2 regularisation because of their computational efficiency and suitability for low resource environments. However, the study did not benchmark the proposed system against more advanced deep learning architectures such as CNN LSTM hybrid models, transformer based biometric frameworks, or attention driven multimodal learning systems. Comparative evaluation with such architectures may provide deeper insights into performance trade offs between computational efficiency and recognition accuracy.

Furthermore, although pre-processing and feature fusion strategies were implemented to improve system robustness, some methodological procedures were simplified to maintain computational efficiency. Fusion weights assigned to fingerprint, facial, and OCR modalities were selected empirically based on preliminary validation performance and modality reliability. Alternative adaptive or dynamic fusion approaches may further improve authentication performance under varying environmental conditions.

Additionally, physiological biometrics played a predominant role in the research. Behavioural biometrics, such as keystroke dynamics, gait analysis, mouse tracking, and other behavioural traits of users, were not considered during authentication. Such behavioural parameters would enhance the strength of continuous authentication and intrusion detection.

RECOMMENDATIONS

1. Carry out pilot testing in Nigerian organizations including Kwara State College of Education, and Kwara State University to test the practical feasibility.
2. Include behavioural biometrics such as keystroke dynamics in enhancing dynamic security.
3. Establish a national framework for the ethical and technical use of biometric authentication systems.
4. Publicize open-source prototypes to be used by academia and industry.
5. Introduce capacity-building programmes that would train IT experts in biometric security systems.

Future Research

Further research should be devoted to the implementation and pilot testing of the authentication mechanism proposed for use in tertiary educational facilities to determine its practicality in terms of scale, efficacy, and usability. Such deployment would provide valuable insights into infrastructural challenges including power instability, device heterogeneity, and network limitations commonly experienced within developing educational environments.

Further research should also investigate comparative benchmarking between the proposed ANN model and more advanced deep learning architectures including CNN LSTM hybrid systems, transformer based multimodal frameworks, and attention driven biometric models. This would give better insights on issues related to computational efficiency, scalability, and authentication accuracy in various architectures.

Moreover, behavioural biometrics factors like keystroke dynamics, gait recognition, mouse dynamics, and behaviour tracking could be integrated into future multi-modal systems to improve adaptive authentication processes. Moreover, the use of federated learning and privacy-preserving AI methods could boost data security, privacy compliance, and decentralized biometric learning within educational institutions.

REFERENCES

1. Abdulrahman, S. A., & Alhayani, B. (2023). A comprehensive survey on the biometric systems based on physiological and behavioural characteristics. Materials Today: Proceedings, 80, 2642–2646. https://doi.org/10.1016/j.matpr.2023.01.456

2. Al-Haija, Q. A. (2023). Cost-effective detection system of cross-site scripting attacksusing hybrid learning approach. Results in Engineering, 19, 101266. https://doi.org/10.1016/j.rineng.2023.101266
3. Almuqren, L., et al. (2023). AI-driven anomaly detection in IoT networks. Computers & Security, 125, 103012. https://doi.org/10.1016/j.cose.2023.103012
4. Chander, B., & Upendra Kumar, R. (2023). MFSDL-ADIIoT: Anomaly detection in industrial IoT. Journal of Network and Computer Applications, 210, 103512. https://doi.org/10.1016/j.jnca.2022.103512
5. Charmet, S., et al. (2022). Federated learning for biometric privacy. Future Generation Computer Systems, 135, 200–215. https://doi.org/10.1016/j.future.2022.05.012
6. Das, S., et al. (2023). AI in multi-factor authentication. Journal of Information Security, 14(2), 100–115. https://doi.org/10.4236/jis.2023.142006
7. Garg, S. N., et al. (2023). Multimodal biometric system based on decision level fusion. Multimedia Tools and Applications, 82(15), 23000–23020. https://doi.org/10.1007/s11042-022-14000-5
8. Hasan, M. W. (2023). IoT temperature forecasting with LSTM and whale optimisation. Memories – Materials Science and Engineering, 45(2), 150–165. https://doi.org/10.1016/j.memse.2023.02.003
9. IBM. (2023). Global IT leaders survey on AI adoption. IBM Corporation. https://www.ibm.com/reports/ai-adoption
10. Islam, M. S., et al. (2023). Representation for action recognition: SDQIO. Expert Systems with Applications, 212, 118406. https://doi.org/10.1016/j.eswa.2022.118406
11. Jyothi, K. K., et al. (2024). Optimised neural network for cyber attack detection. Scientific Reports, 14, 55098. https://doi.org/10.1038/s41598-024-55098-2
12. Khan, R. U., et al. (2024). Fingerprint recognition using CNN with inversion techniques. Machine Learning with Applications, 16, 100539. https://doi.org/10.1016/j.mlwa.2024.100539
13. Liu, Z., et al. (2023). DDoS detection in SDN using feature engineering. Sensors, 23(13), 6176. https://doi.org/10.3390/s23136176
14. Omer, N., et al. (2023). Optimised probabilistic neural network for intrusion detection. Computers, Materials & Continua, 77(3), 3500–3515. https://doi.org/10.32604/cmc.2023.045000
15. Pahuja, S., & Goel, N. (2024). Multimodal biometric authentication: A review. Artificial Intelligence Research, 13(1), 1–25. https://doi.org/10.5430/air.v13n1p1
16. Ross, A. A., & Jain, A. K. (2023). Information fusion in biometrics (updated). Pattern Recognition Letters, 170, 50–60. https://doi.org/10.1016/j.patrec.2023.05.012
17. Singhal, M., & Shinghal, K. (2023). Secure deep multimodal biometric authentication. Multimedia Tools and Applications, 82(15), 23000–23020. https://doi.org/10.1007/s11042-023-16683-1
18. Thota, S., & Menaka, D. (2024). Botnet detection in IoT using CNN with pelican optimisation. Automatika, 65(1), 250–260. https://doi.org/10.1080/00051144.2023.2288486
19. Verizon. (2023). Data breach investigations report. Verizon. https://www.verizon.com/business/resources/reports/dbir/
20. Vijayakumar, T. (2023). Palmprint synthesis in multimodal recognition. Journal of Innovative Image Processing, 5(2), 131–143. https://doi.org/10.36548/jiip.2023.2.005
21. Yang, W., et al. (2023). Security and accuracy of fingerprint biometrics: A review. Symmetry, 15(2), 450. https://doi.org/10.3390/sym15020450