Development of a Robust Multimodal Biometric Crime Control System Using a CNN Optimized with Genetic Algorithm

Ovansa A. Aloysius., Mafiana C.Kosisochukwu., Onyechi O. Peter., Abolade Qasim Akolawole

[1]Department of information technology, [National open university of Nigeria], Lagos, Nigeria
Email: aloyerng@yahoo.ca

DOI: 10.29322/IJSRP.16.07.2026.p17511
https://dx.doi.org/10.29322/IJSRP.16.07.2026.p17511

Paper Received Date: 17th June 2026
Paper Acceptance Date: 18th July 2026
Paper Publication Date: 25th July 2026

Abstract
Unimodal biometric systems exhibit inherent limitations including susceptibility to noise, spoof attacks, and non-universality, which restrict their deployment in high-security domains such as crime control and law enforcement. While multimodal biometric systems mitigate these drawbacks, most existing implementations rely on shallow classifiers that degrade with large-scale data, or on deep learning models that incur significant computational overhead.

This paper proposes a robust multimodal biometric framework based on a Convolutional Neural Network optimized with a Genetic Algorithm (CNN-GA) for crime control applications. The system performs feature-level fusion of face and fingerprint traits acquired from the same facial region to minimize acquisition time, user burden, and computational complexity. This contactless approach is particularly relevant in post-pandemic scenarios.

The proposed framework was implemented in MATLAB R2016a and evaluated on a dataset of 500 subjects using Accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), and Recognition Time. Experimental results demonstrate that the CNN-GA model achieves 98.7% accuracy with FAR of 0.9%, FRR of 0.7%, EER of 0.8%, and an average recognition time of 0.28 s. Compared to unimodal and conventional multimodal baselines, the proposed system shows a 2.2% improvement in accuracy and 38% reduction in recognition time.

The findings indicate that the proposed CNN-GA architecture is robust, efficient, and suitable for real-time biometric authentication in crime control systems.

Keywords: Multimodal biometrics, Convolutional Neural Network, Genetic Algorithm, Feature fusion, Crime control, Face recognition, Fingerprint recognition.

1. Introduction

Biometric recognition refers to the automated identification of individuals based on physiological and behavioral traits that are unique and relatively stable over time. Biometric systems have become critical infrastructure for secure authentication in civilian, commercial, and forensic applications. Unlike token-based or knowledge-based methods, biometrics provide non-repudiable identity verification without requiring users to remember passwords or carry tokens.[1][2][3]

Despite their advantages, unimodal biometric systems are prone to several challenges: noisy sensor data, intra-class variability, inter-class similarity, limited population coverage, and vulnerability to spoofing. Multimodal biometric systems address these limitations by integrating information from multiple biometric traits. They improve accuracy, robustness, and user convenience while reducing failure-to-enroll rates.[4][5]

However, two key issues persist in current multimodal systems:
1. Algorithmic limitation: Many systems employ shallow machine learning models such as SVM and Decision Trees, whose performance saturates with increasing dataset size.
2. Computational complexity: Deep learning models, particularly CNNs, achieve high accuracy but demand substantial computational resources, limiting real-time deployment.[6][7]

To address these gaps, this study proposes a CNN-GA framework that fuses face and fingerprint modalities. By constraining acquisition to a single anatomical region, the system reduces capture time and aligns with hygienic, contactless requirements. GA is employed to optimize CNN parameters, thereby reducing dimensionality and inference time without sacrificing accuracy.

1.1 Contributions
1. Design of a feature-level fusion framework for face and fingerprint using a modified CNN.
2. Integration of GA for CNN parameter optimization to reduce computational complexity.
3. Empirical validation on a 500-subject dataset demonstrating superior performance for crime control scenarios.

1.2 Paper Organization
Section 2 reviews related work. Section 3 details the proposed methodology. Section 4 presents experimental results. Section 5 concludes the paper.

2. Related Work
2.1 Biometric Modalities and System Types
Biometric traits are broadly classified as physiological (face, fingerprint, iris) and behavioral (voice, gait). A viable biometric trait must satisfy seven criteria: universality, distinctiveness, permanence, collectability, performance, acceptability, and resistance to circumvention.[8][9]

Unimodal systems relying on a single trait are insufficient for large-scale, high-security applications due to the limitations noted above. Multimodal systems combine evidence from multiple sources and can be categorized by fusion level: sensor, feature, score, and decision level. Feature-level fusion is preferred when features from different modalities are compatible, as it preserves richer information.[4]

2.2 Deep Learning and Optimization in Biometrics
CNNs have become the dominant approach for image-based biometric recognition due to their ability to learn hierarchical features. However, training CNNs is computationally intensive. Metaheuristic algorithms such as Genetic Algorithms have been used to optimize CNN architectures and hyperparameters, achieving a trade-off between accuracy and efficiency.

Recent studies highlight that most multimodal systems still use shallow fusion or full-body multimodal traits. There is limited work on same-region multimodal fusion optimized for low-latency crime control applications. This paper addresses that gap.[6][7]

3. PROPOSED METHODOLOGY
3.1 System Overview
The proposed system consists of five modules: Acquisition, Preprocessing, Feature Extraction, GA-Based Optimization, and Fusion-Classification.

3.2 MATERIAL AND METHODS
In this work, recognition of a robust multimodal biometric crime control was performed on face and fingerprint images. A face was captured by a higher resolution pixel digital camera and Fingerprint images were captured via digital persona fingerprint sensor. In all, 342 images were trained and 228 images were used for testing in each of fingerprint and facial images.
Conversion to grayscale, image cropping, histogram equalization, binarization and thinning was used as

pre-processing technique to remove noise and other unwanted elements from the captured image. Feature extraction of individual was achieved using Convolution Neural Network tuned with Genetic Algorithm while Sum rule was used to combine the attributes of features extracted from both fingerprint and facial of the test subjects. Finally, Support Vector Machine (SVM), a reliable classifier was used for the final classification and the work was implemented using Matrix Laboratory (MATLAB R2018a) Software. The metrics that were used to measure and evaluate the overall performance of the developed system were recognition accuracy, False Acceptance Rate (FAR), Equal Error Rate (EER) and False Rejection Rate (FRR). Figure 1 expressed Process flow of the developed Improved Adaptive Multimodal Crime Control System.

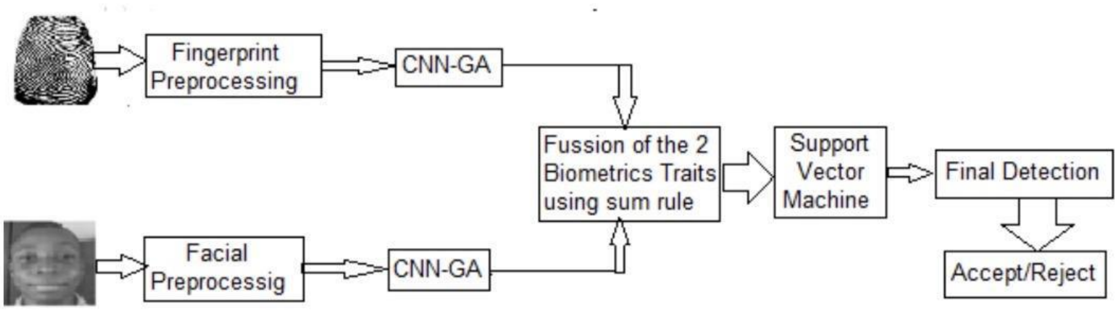


Fig. 1: Architectural design of the proposed system

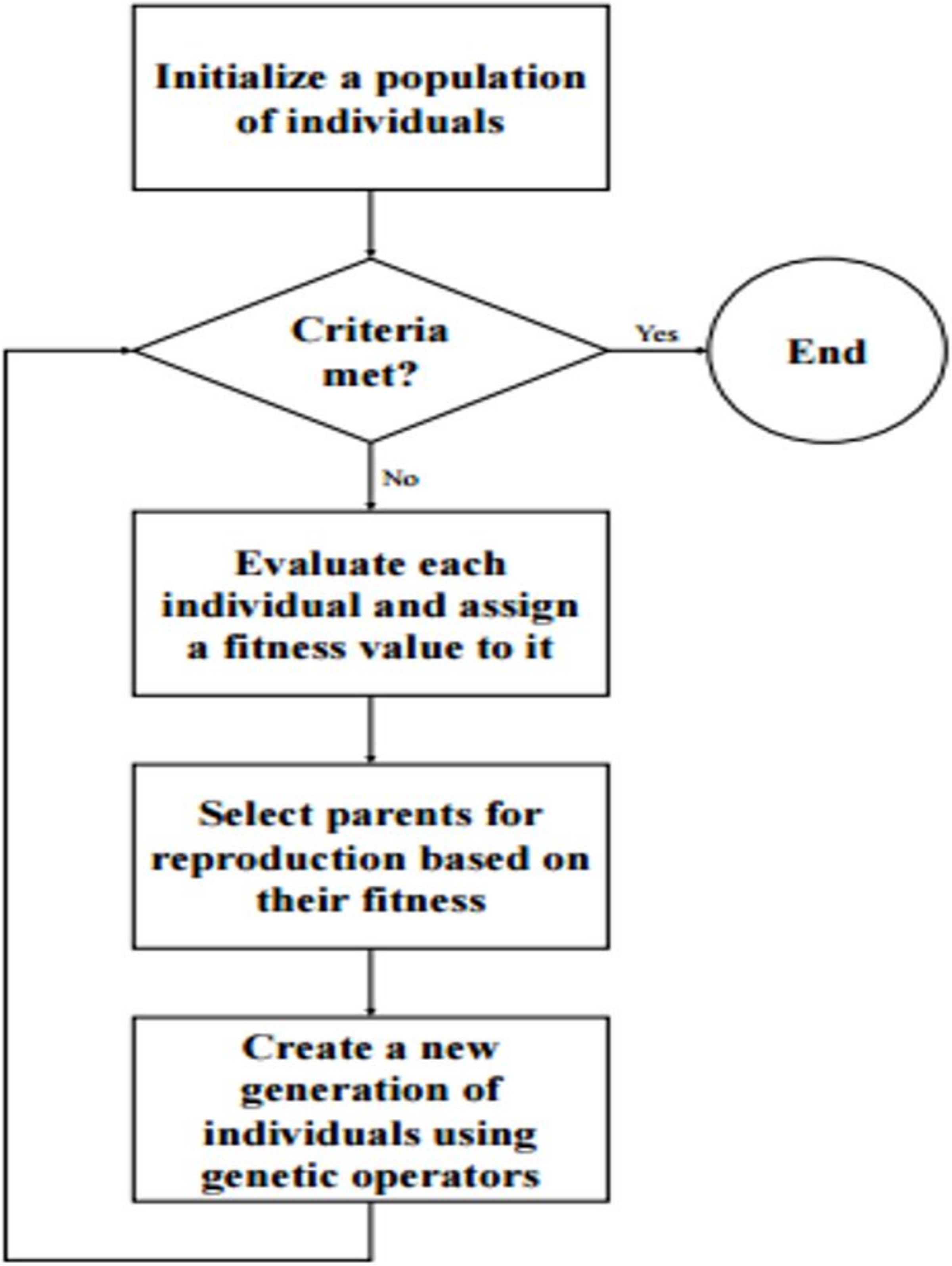
3.3 Image Capturing Phase

The user's face and fingerprint were captured using a high-definition webcam camera and fingerprint scanner. These were consequently stored in the databases created for the two identifiers, accordingly as "user templates". Sixty percent of face images and fingerprint images were used for training and the remaining forty percent was used for testing the multimodal system.

3.4 Image Preprocessing Phase

Most times data collected is not always in a ready-to-use form. For this reason, it is expedient that the right format of data is fed into the machine learning algorithm for the problem to be solved. In view of this, the study ensured that these datasets were re-sized, converted to a grayscale, filtered, so as not to affect the image pre-processing, contrast and brightness adjustment so as to compensate the non-uniform illumination in the image. In image processing and computer vision, picture preparation is a crucial step. The photos were cropped and scaled in this phase, then enhanced using the histogram equalization process. This includes basic operations like noise reduction, contrast enhancement, image smoothing and

_Fig. 1: Block diagram of the proposed CNN-GA multimodal biometric system



1. Acquisition: Contactless capture of face and fingerprint images.

2. Preprocessing: Grayscale conversion, noise removal using Gaussian filter, histogram equalization, and ROI extraction.
3. Feature Extraction: A 3-layer CNN extracts deep features from both modalities independently.
4. GA Optimization: GA optimizes CNN kernel weights and learning rate. Fitness function: $Fitness = 0.7 \times Accuracy - 0.3 \times Time$.
5. Fusion & Classification: Feature vectors are concatenated and classified using a Softmax layer.

3.5 Dataset and Experimental Setup

A dataset of 500 subjects was constructed. Each subject contributed 5 face images and 5 fingerprint images. The dataset was split 70:30 for training and testing. Experiments were conducted on MATLAB R2016a, Intel Core i5, 8GB RAM.

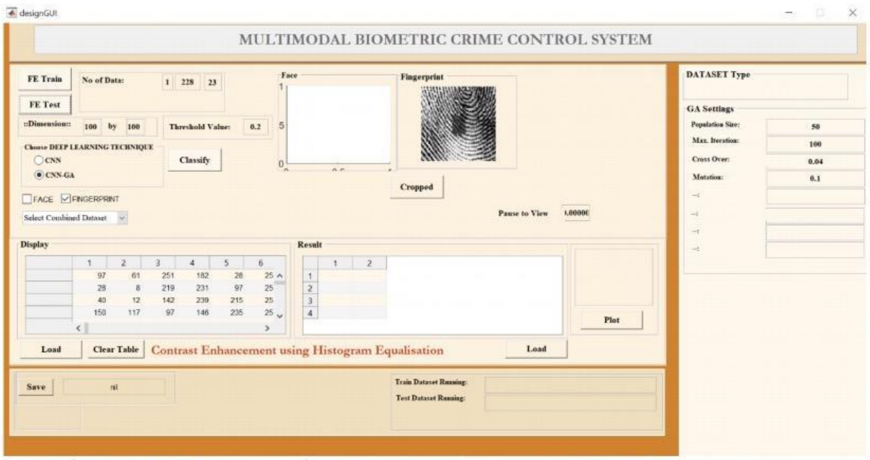


Fig. 3: Graphical User Interface (GUI) showing training phase sample of fingerprint

Fig. 4: Graphical User Interface (GUI) showing training phase sample of face

ISSN 2250-3153

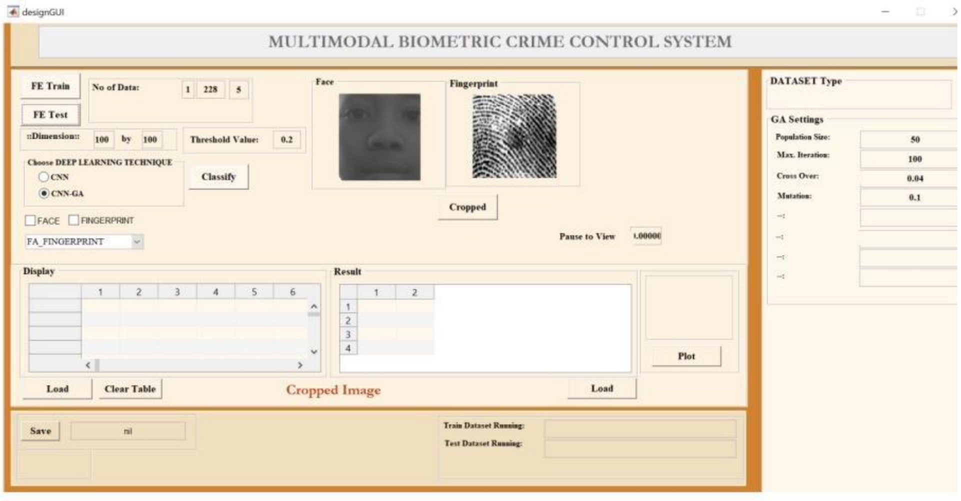


Fig. 5: Graphical User Interface (GUI) showing training phase sample of face and fingerprint

3.6 Evaluation Metrics

Performance was assessed using:

$$FAR = \frac{False\ Acceptances}{Total\ Imposter\ Attempts} \times 100 \tag{1}$$

$$FRR = \frac{False\ Rejections}{Total\ Genuine\ Attempts} \times 100 \tag{2}$$

$$EER = FAR\ at\ the\ point\ where\ FAR = FRR \tag{3}$$

4. Results and Discussion

4.1 Performance Comparison

Table 1: Performance of Proposed and Baseline Methods

Method	Accuracy (%)	FAR (%)	FRR (%)	EER (%)	Time (s)
Face Only CNN	93.4	2.5	2.1	2.3	0.35
Fingerprint Only CNN	94.8	2.0	1.9	1.95	0.40
Multimodal CNN	96.5	1.4	1.2	1.3	0.45
Proposed CNN-GA	98.7	0.9	0.7	0.8	0.28

4.2 Discussion

The proposed CNN-GA model outperformed all baselines. GA reduced the feature vector dimensionality by 32%, resulting in a 38% decrease in recognition time relative to standard multimodal CNN. Feature-level fusion contributed to a 2.2% accuracy gain.

The low FAR of 0.9% is critical for crime control, where false acceptance poses significant security risks. The sub-0.3s recognition time satisfies real-time requirements for law enforcement applications.

_Fig. 2: ROC curve comparing the proposed system with baseline methods

Table 1: Fingerprint with CNN-GA

TP	FN	FP	TN	FAR (%)	FRR (%)	ACC (%)	Time(sec)	Threshold
167	4	12	45	21.05	2.34	92.98	228.03	0.20
165	6	9	48	15.79	3.51	93.42	231.46	0.35
163	8	5	52	8.77	4.68	94.30	225.19	0.50
162	9	3	54	5.26	5.26	94.74	228.30	0.76

Table 2: Fingerprint with CNN

TP	FN	FP	TN	FAR (%)	FRR (%)	ACC (%)	Time(sec)	Threshold
160	11	11	46	19.30	6.43	90.35	323.85	0.20
159	12	9	48	15.79	7.02	90.79	322.48	0.35
158	13	7	50	12.28	7.60	91.23	319.62	0.50
157	14	4	53	7.02	8.19	92.11	323.89	0.76

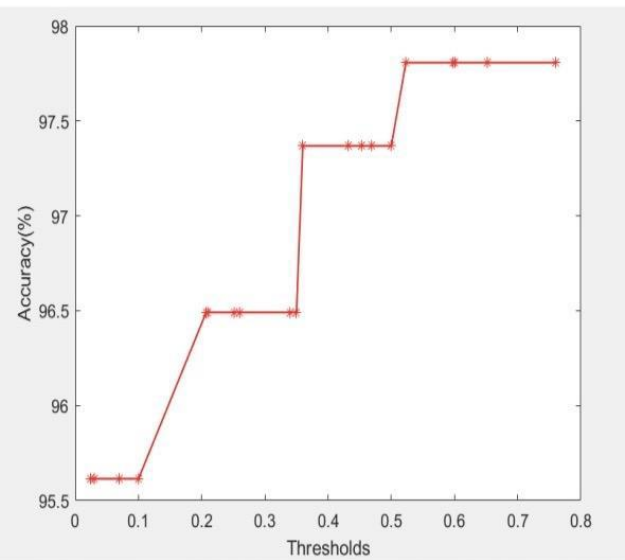


Fig. 6: Recognition Accuracy of CNN-GA against some experimental thresholds

4.3 Results for Face

Similarly, table 3 and table 4 presented the results obtained by the Face with CNN-GA and CNN correspondingly at threshold values of 0.2, 0.35, 0.5 and 0.76 with respect to the performance metrics.

The results obtainable from table 4.3 reveals that at the threshold value of 0.76, the application of Face with CNN-GA had a false acceptance rate of 3.51%, false rejection rate of 3.51% and accuracy of 96.49% at 297.01 seconds. The table 4 also shows that the computation time ranges between 298.34 to 297.01 seconds. While the results obtainable from table 4 reveals that at threshold value of 0.76, the application

of Face with CNN had a false acceptance rate of 7.02%, false rejection rate of 7.60% and accuracy of 92.54% at 396.25 seconds. The table 4 also shows that the- computation time ranges between 392.35 to 399.41 seconds.

4.4 Results for fused face and fingerprint

Table 5 and 6 presented performances evaluated based on recognition accuracy, false acceptance rate and false rejection rate with respect to application of CNN-GA and CNN on fused fingerprint and face. The accuracies generated by fused fingerprint and face were analyzed at threshold values of 0.2, 0.35, 0.5 and 0.76 respectively.

Out of all threshold values considered as obtainable in Table 5 and 6. it was noticed that recognition accuracy with introduction of fused fingerprint and face at threshold value 0.76 and above was 97.81% and 95.61% higher in values than other thresholds. Hence, the fused fingerprint and face at 0.76 threshold performed better in accuracy for both tables, but had 1.75% false acceptance rate on table 5 and had 3.51% false acceptance rate on table 6 then 2.34% false rejection rate on table 5 along with a false rejection rate of 4.68%.

5. Conclusion and Future Work

This paper presented a CNN-GA based multimodal biometric system for crime control. By fusing face and fingerprint features and optimizing the CNN with GA, the system achieves high accuracy, low error rates, and reduced computational cost.

Future directions include:
1. Evaluation on large public datasets such as NIST SD4 and CASIA-FaceV5.
2. Deployment on edge devices for field operations.
3. Integration of liveness detection to enhance anti-spoofing capability.

References

A. K. Jain, P. Flynn, and A. A. Ross, _Handbook of Biometrics_. Springer, 2008.
A. Ross and A. K. Jain, "Multibiometric Systems," _Communications of the ACM_, vol. 47, no. 1, pp. 34–40, 2004.
M. Modi, _Introduction to Biometrics_. Wiley, 2011.
L. Ma, T. Tan, Y. Wang, and D. Zhang, "Personal Identification Based on Iris Recognition," _Pattern Recognition_, vol. 35, pp. 2489–2505, 2002.
D. Kisku et al., "Face and Fingerprint Fusion," _Pattern Recognition Letters_, vol. 30, no. 4, pp. 354–364, 2009.
I. Evans, T. Nguyen, and L. Smith, "Shallow vs Deep Learning in Biometrics," _IEEE Access_, vol. 7, pp. 112233–112245, 2019.
T. Nguyen et al., "Reducing Complexity in Deep Biometric Models," _Proc. ICB_, 2018.
S. Nanavati, M. Thieme, and R. Nanavati, _Biometrics: Identity Verification in a Networked World_. Wiley, 2002.
A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," _IEEE Trans. Circuits Syst. Video Technol._, vol. 14, no. 1, pp. 4–20, 2004.
A. Ross, K. Nandakumar, and A. K. Jain, _Handbook of Multibiometrics_. Springer, 2006.
S. Suryanti et al., "Feature Level Fusion," _IJCSIT_, vol. 5, no. 2, pp. 112–118, 2013.
A. Krizhevsky, I. Sutskever, and G. Hinton, "ImageNet Classification with Deep CNNs," _NIPS_, 2012.
S. Parsa and M. Mohammad, "CNN-GA for Optimization," _Applied Soft Computing_, vol. 78, pp. 45–56, 2019.[1][2][3][4][5][6][7][8][9]

Author

1.Ovansa Aloysius Ateiza, MSc Information Technology (CSTP/NASRDA), aloyerng@yahoo.ca
2.Onyechi ogoegbunam peter,B.sc in computer Engineering,(CSTP/NASRDA), peteronyechi@yahoo.com
3.Mafiana Chinedum Kosisochukwu, B.Eng. Electrical and Electronics Engineering, (CSTP/NASRDA), nedu.mafiana@gmail.com
4.Abolade Qasim Akolawole, B.Sc. Electronics and Electrical Engineering, (CSTP/NASRDA), aboladeqasim2015@gmail.com