



(RESEARCH ARTICLE)



AI based criminal identification system using facial recognition

Kenechukwu Patrick Okafor ^{1,*}, Nkemdilim Njideka Mbeledogu ¹ and Ewa Uchenna Mba ²

¹ Department of Computer Science, Faculty of Physical Sciences Nnamdi Azikiwe University, Awka, Nigeria.

² Department of Computer Science, Faculty of Basic Medical and Applied Sciences David Umahi Federal University of Health Sciences, Uburu, Nigeria.

World Journal of Advanced Research and Reviews, 2026, 29(03), 1021-1032

Publication history: Received on 25 January 2026; revised on 08 March 2026; accepted on 11 March 2026

Article DOI: <https://doi.org/10.30574/wjarr.2026.29.3.0569>

Abstract

This paper presents the development of a criminal identification system that leverages on deep learning for face recognition to enhance accuracy, speed and reliability in law enforcement. The system was developed using the Object-Oriented Analysis and Design Methodology (OOADM) to guide the requirements modeling, system structuring, and implementation. At its core, the system employed a Residual Neural Network (ResNet) architecture, chosen for its ability to extract deep hierarchical features and maintain robust recognition under challenging conditions such as poor lighting, pose variations, and partial occlusions. A diverse dataset of facial images was used for training and evaluation, with preprocessing steps including face detection, resizing, normalization, and alignment to ensure consistency. The model size using Feature Descriptor Parameters was optimized, and sensitive data were tokenized using Universally Unique Identifier (UUID). Additionally, the National Identification Number (NIN) dataset was simulated. To validate performance, this deep learning-based pipeline Haar + ResNet model was compared with the classical pipeline, that is, the traditional Haar Cascade face detector combined with Local Binary Patterns Histograms (LBPH). While Haar + LBPH performed adequately under controlled conditions, it showed reduced accuracy with difficult lighting and non-frontal images. In contrast, ResNet achieved consistently higher accuracy and faster matching times, making it better suited for real-world applications. Beyond recognition, the system cross-referenced the identified individuals with the NIN registry official records for identity verification. Experimental results confirmed the model's high precision and reliability in supporting its potential deployment in surveillance and investigative systems.

Keywords: Deep Learning; Facial Recognition; Residual Neural Network (Resnet); Haar Cascade; Local Binary Patterns Histograms (LBPH)

1. Introduction

Despite the rich cultural and mineral resources endowed in Nigeria, it fundamentally struggles with insecurity due to its dereliction on the part of the Government and the citizens to protect it. It is challenged with innumerable security issues such as terrorism and extremism, organized armed robbery, assassination, kidnapping, demand for ransom, militia group activities, farmers pastoralists clashes, transnational organized crimes, border security and technological challenges (Musa, 2021; Atai *et al.*, 2024). It has in turn resulted to consequences that affects the citizens and nation at large. Some of such consequences are scarcity of skilled manpower, discouragement of investment, destruction of existing infrastructure, underdevelopment, environmental challenges and threats, economic challenges (poverty) as well as regional and global challenges.

As a result of these issues, there is a need to enhance the efficacy and performance of facial recognition technologies in criminal identification which remains a critical challenge. Despite recent technological advancements, existing algorithms are often computationally intensive and lack efficiency in semi-regulated and unregulated environments,

*Corresponding author: Okafor Patrick Kenechukwu

where there is a lack of structured oversight and control, making it difficult to promptly and accurately identify criminals. This issue necessitated further research in developing a more streamlined and cost-effective algorithms for face recognition. Privacy concerns also persist, particularly in semi-regulated environments where the balance between security and individual rights is delicate.

With the advancement in crimes, to enhance security efforts already on ground, artificial intelligence (AI) was desired. AI is a domain within computer science focused on developing intelligent computer systems that can perceive, analyse, and react to inputs similar to the human intelligence (Patil *et al.*, 2023), and integrating it with ICT can provide significant benefits.

2. Literature Survey

2.1. Artificial Intelligence (AI)

This refers to computer systems performing complex tasks such as reasoning, decision making or solving problems that historically only humans could do (Coursera, 2025). It is based on interdisciplinary fields that have domains in Computer Science, Mathematics, Linguistics, Psychology, Neuroscience, Engineering, Statistics, Economics, Control theory and Cybernetics, Philosophy and Biology. Due to this, it houses a wide range of branches that are based on different technologies and application that have little or more in common than their apparent intelligence that is open to interpretation. These branches are Machine Learning (ML), Natural language Processing (NLP), Computer Vision, Robotics, Expert Systems (ES), Neural Networks and Deep Learning, Fuzzy Logic (FL), Pattern Recognition (PR), Evolutionary Computation, Swarm Intelligence and Cognitive Computing (Geeksforgeeks, 2024). In recent years, AI has played a major role in transforming the field of computer vision, particularly in facial recognition and biometric identification systems. The subset of AI which are Machine learning and deep learning has made it possible for systems to learn from large datasets and has greatly influenced their performance over time. The systems can achieve this through pattern recognition. With the adoption of AI, accuracy, efficiency, and speed is significantly enhanced through the application of AI. By leveraging intelligent algorithms, law enforcement and security agencies can identify individuals from large facial databases faster, reducing the unnecessary delay, stress and errors which can occur with the traditional methods.

2.2. Pattern Recognition (PR)

PR is one of the branches of AI is the science of enabling machines to recognize pattern in data (Parasher *et al.*, 2021). It is the most important trait of cognitive ability. The signals from the environment are received through the sensory organs which are processed by the brain to generate suitable responses. The entire process involves extraction of information from the sensory signals. All the information analyzed are represented by a pattern. Patterns are common denominator among the multiple instances of an entity. These are either physical objects or abstract notion like style of talking or writing. The popularity of PR is attributed to its application potentials as it overlaps with machine learning naturally. There are several important applications such as image recognition, document recognition, remote sensed data analysis, bioinformatics and semantic computing. With the increase in the complexity and volume of modern datasets, manual feature engineering has become insufficient for achieving high accuracy in real-world applications such as criminal identification. Thus, the emergence of Deep Learning models which are advanced machine learning approaches that are capable of automatically learning features from data.

Deep learning models, especially Convolutional Neural Networks (CNNs), have demonstrated exceptional capability in extracting hierarchical features from images, making them highly suitable for facial recognition tasks.

2.3. Haar Cascade Algorithm

The Haar Cascade algorithm is a machine learning-based object detection method introduced by Paul Viola and Michael Jones in 2001. In real time face detection, HAAR cascade is widely considered due to its computational efficiency and processing requirements which are relatively low compared to some other models. The algorithm functions by using Haar-like features, which are digital image features used in detecting the presence of a specific structure in an image. When the digital images are generated, the features are calculated using rectangular regions and are properly evaluated through an integral image representation. AdaBoost algorithm is used in the training process to select the most relevant features from a large feature pool which are then used to construct a strong classifier. The cascade structure enables the rapid rejection of non-face regions, thereby making the detection process faster.

Haar Cascade is particularly beneficial for real-time applications because of its lightweight and computational structure. However, its performance may decline under conditions such as poor lighting, facial occlusion, or pose variation. Despite

these limitations, Haar Cascade remains a reliable preprocessing technique for detecting facial regions before applying more advanced recognition algorithms.

2.4. Local Binary Patterns Histogram (LBPH)

LBPH algorithm is texture-based. Texture in image processing refers to the surface characteristics and variations in pixel intensity within an image. Example of textures include skin smoothness or roughness, wrinkles, edges around the eyes, nose, and mouth. The LBPH algorithm works by converting an image and representing it into a binary pattern. Neighboring pixel values of each pixel in an image are compared to the central pixel value. If a neighbor's value is greater than or equal to the center pixel, it is assigned a value of 1, else 0. These binary values are combined to form a local binary number. The image is then divided into grids, and histograms of these binary patterns are computed and combined to form a feature vector. During recognition, the extracted histogram of a test image is compared with stored histograms using a distance metric such as Euclidean distance. The image with the minimum distance is considered the closest match. LBPH is computationally efficient and performs reasonably well under controlled conditions. However, it struggles when used with variations in illumination, facial expression, and pose. Compared to deep learning models, LBPH provides lower recognition accuracy in large-scale or unconstrained environments.

2.5. Residual Networks (ResNet) Model

This is a classic neural network created to facilitate the training process of neural networks that are much deeper than previously trained models. This architecture explicitly reformulates its layers with residual function learning that references the input layer, rather than learning unreferenced functions (Wen *et al.*, 2020). When compared to conventional networks, the working principle of ResNet builds a deeper network and optimizes the layers to eliminate the problem of vanishing gradients. It applies Batch Normalization which is a technique for normalizing activations in the deepest layers of neural networks and reduces covariance shift or equalizes the distribution of input values because changes in the training process result in constantly changing values. This technique continuously improves activations to have a mean of zero and a standard deviation of one, allowing for a larger gradient step and faster processing.

2.6. Review Of Related Works

Some researchers have worked on face recognition classification using different approaches. They are as follows:

Kakkar and Sharma (2018) implemented a criminal identification system using Haarcascade classifiers. The algorithm adopted by the researchers looked for specific Haar features in an image. The classifiers allowed a face candidate, which is a rectangular part of the original copy of the image to move to the next step of the recognition algorithm when Haar features are found. However, the system failed to cater for cases of undocumented criminals or first-time offenders.

Nguyen *et al.* (2019) designed and developed a smart security system with facial recognition using OpenFace and Inception-v3 models for face recognition in restricted (regulated) environment. The biometric data of the system was not securely managed which potentially violated individuals' privacy. Also, the system failed to accurately recognize individuals which compromised the reliability of the security system.

Zafar *et al.* (2019) proposed a facial recognition system using Bayesian convolutional neural networks for resilient surveillance systems. The researchers enhanced the efficiency of facial recognition systems by minimizing false positive. The results obtained showed that deep learning (DL)-based approaches were quite suitable for feature extraction and representation were performed without much intervention using back-propagation method on supplied data.

Apoorva *et al.* (2019) proposed a robust face detection methodology suitable for real time environments using Haar-cascade classifier on Open-CV platform. Though the researchers obtained results, Haar-classifier performs poorly on complex objects or cluttered background, prone to high positive rate, sensitive to image conditions, thus making it difficult to adapt to new object types.

Kumar *et al.* (2020) designed a suspect identification system using facial recognition in public environments. The Local Binary Pattern Histogram (LBPH) algorithm and Haar-cascade classifier were employed. The system allowed tracking of criminals, suspect and general individuals by simply providing pictures of the individuals against which comparison is made with feed from strategically positioned cameras. The system was limited in dealing with undocumented criminals.

Septyantoet *et al.* (2020) introduced a facial recognition system for attendance tracking using the Haar Cascade Algorithm. The study involved 13 employees from Starcross Store, each participating in 30 trials, totalling 390 attempts. The system

achieved a success rate of 87%, but 13% of attempts failed. The study concluded that while the system could identify faces to an extent under normal conditions, it struggled with variations in lighting.

Tamrkar and Gupta (2020) proposed a face recognition methodology that incorporated feature based, holistic and hybrid approaches for criminal identification in India using face recognition, as traditional methods. The authors proposed three different approaches for face recognition, including the feature-based, holistic, and hybrid methods. The feature-based approach segments local features such as the nose and eyes to use as input for the face detection system, while the holistic approach takes the entire face as input for detection and recognition.

Kumar *et al.* (2020) offered a real-time facial recognition criminal identification system using Haar feature-based cascade classifiers and OpenCV LBPH algorithms. The developed system faced several challenges, including the sensitivity of Haar cascade classifiers to variations in lighting, pose, and facial expressions, which led to misidentifications. The system also required substantial computational resources for real-time processing, which could be problematic in resource-limited environments, affecting its overall efficiency and reliability.

Bharathi *et al.* (2020), worked on criminal identification using K-Medoids clustering algorithm. The paper suggests a supervised approach to identifying a list of suspects using a similarity measure and the K-Medoids clustering algorithm. This is a partition-based clustering algorithm, and a variant of K means algorithm that groups similar offenses into distinct clusters, each with its own set of unique features.

Pawar *et al.* (2021) in a system for criminal identification used face recognition technology to identify individuals in real-time. This system makes use of automated surveillance cameras to detect and recognize faces within a video feed. The system employs Haar Cascade Classifiers. However, this method struggles in more complex settings with cluttered backgrounds and is highly sensitive to changes in lighting, pose, and scale.

Ahmad *et al.* (2021) implemented a video surveillance system using Haar-cascade to identify faces under the following constraints; when accessories cover parts of the face or a face is positioned at a particular angle to the camera and when the face is far from the camera. It struggles to detect faces that are turned significantly to these sides as they primarily rely on frontal facial features. Thus, it is less efficient.

Achmad *et al.* (2023) proposed the development of a Mobile-Based Student Presence System aimed at improving the monitoring of student attendance within a school environment. The system integrates facial recognition technology using the Haar Cascade and Eigenface algorithms to record student attendance when entering or exiting the classroom. The lighting variations and distance limited these technologies in performance because Haar cascade is highly sensitive to lighting which causes detection failure, Eigenface struggles with illumination changes which results in poor recognition accuracy and increased distance reduces accuracy due to lower resolution and smaller pixel representations of the facial features.

Wayakaret *al.* (2024) proposed a machine learning-based method for real-time criminal identification using face recognition technology. The system employs "one-shot learning," which allows it to identify criminal faces with just a single image, and it operates effectively with minimal data. While the approach has notable advantages in terms of real-time identification, its reliance on simple machine learning techniques, such as LBPH and Haar cascade classifiers, limits its ability to perform under real-world conditions.

Yesugadeet *al.* (2024) proposed a robust face detection and recognition system aimed at enhancing the speed and accuracy of suspect identification in criminal cases. Their method combines the Haar cascade classifier for feature detection with the Local Binary Pattern Histogram (LBPH) algorithm for face recognition, addressing challenges such as image quality and environmental variations, the researchers noted that its performance may be compromised in high-variance, practical environments making it inefficient for criminal identification.

Reddy and Naresh (2025) developed a criminal identification system using Haar feature-based cascade classifiers for face detection and Local Binary Patterns Histograms (LBPH) for face recognition. The Haar classifiers were trained on positive and negative images, while LBPH offered efficient feature selection and was effective in varied lighting conditions, even with limited training data.

3. Materials and Method

The methodology adopted for this work is Object-Oriented Analysis and Design Methodology (OOADM), tailored to the context of face recognition using deep learning. The architecture of the ResNet model adopted was the ResNet-34 model. It is a deeper learning-based detector than the simple Convolutional Neural Network (CNN) because it used residual blocks to address issues with deep artificial neural network training. The system included a module where users could submit complaints together with images of suspects or criminals they captured. These images were collected by security operatives or government agencies and scanned with the criminal identification system (face recognition). The system then identified the suspects or criminals with the provision of a tracking code. The tracking code served as tokenized data representing a unique identifier for each person in the database. Whenever the database was queried with the tracking ID, the person's NIN biodata or information was displayed.

3.1. Existing system

The existing system analyzed is the Haar-cascade algorithm with Local Binary Patterns Histogram. Reddy and Naresh (2025) developed a criminal identification system that employed Haar feature-based cascade classifiers for face detection and Local Binary Patterns Histograms (LBPH) for face recognition. For recognition, the system used the LBPH algorithm, which analyzed the local features of a face by comparing each pixel's intensity with its neighboring pixels. The result was encoded into a binary pattern, forming a histogram that represents the unique facial texture of the individual. By comparing these histograms, LBPH provided a robust and relatively simple approach to recognizing faces. The system is limited to high false positive rate, accuracy and flexibility for complex objects and parameter tuning.

3.2. Proposed system

The new AI-based Criminal Identification System was developed to address the limitations of the existing Haar Cascade model and Local Binary Patterns Histograms (LBPH). The system focused on both regulated (private) and unregulated (public) environments using the Residual Neural Network (ResNet) model. The dataset used to finetune the system was VGGFace2, a large-scale dataset containing millions of labeled images, thereby, allowed the residual network to learn robust features that are well-suited for recognizing faces in diverse contexts.

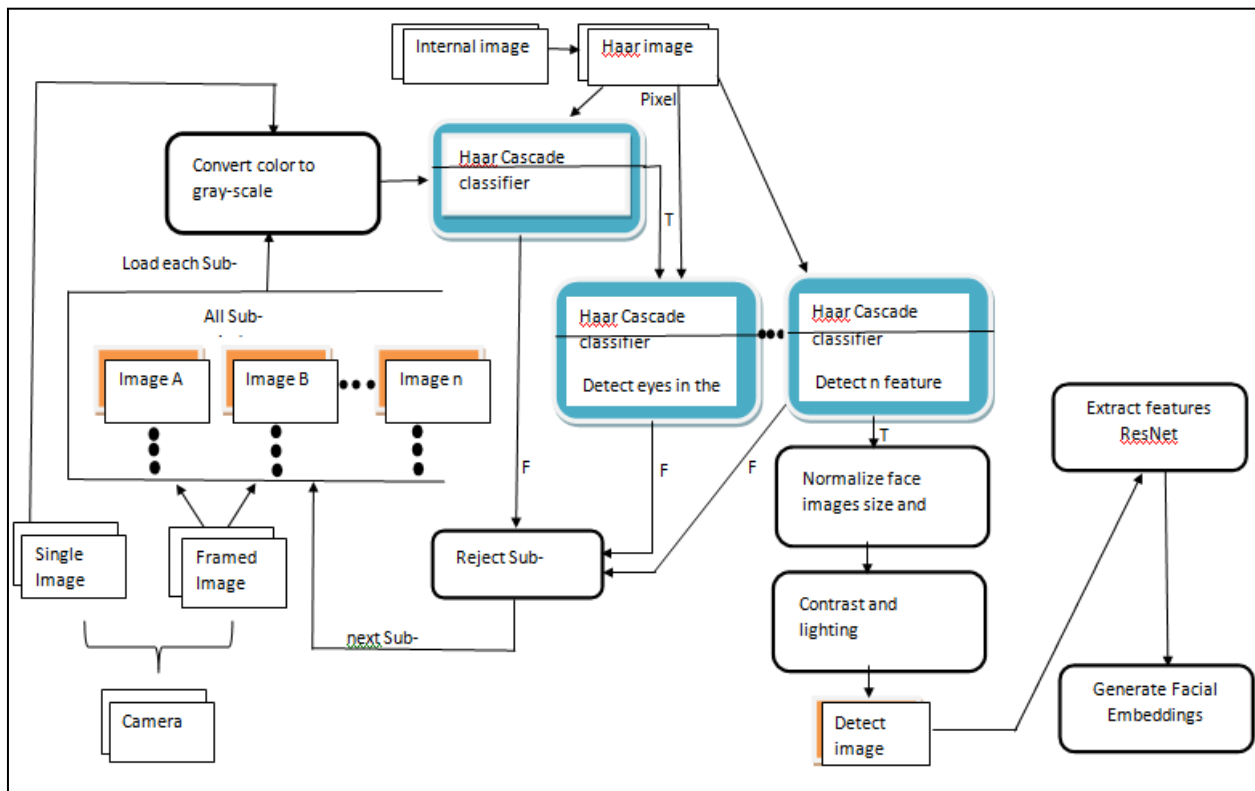


Figure 1 Data Flow Diagram of the face recognition using Residual Neural Network

The model processed images and extracted high-level features from faces, generating a 128-dimensional face encoding (embedding). This embedding captured distinctive characteristics of a person's face, such as the shape of the eyes, nose, and other facial features, in a compact vector form. The embeddings were then compared to determine if two images belonged to the same person or not. The comparison was carried out using Euclidean distance, where a smaller distance indicated a higher likelihood of a match.

The system was developed using VB.NET and Python programming languages. The face-recognition library in Python provided a pre-trained model that had already been trained and fine-tuned on a vast dataset, making it readily usable for face recognition tasks. It has taken few sample test data separately for face images. These images were inputted into the system to verify how well the face recognition model could detect and identify individuals under various conditions. The test also included different lighting scenarios and various angles of the face to ensure the model's versatility. Figure 1 illustrates the dataflow pipeline of the proposed face recognition system.

One of the crucial step in the development of the system is preprocessing, it prepares the facial images for accurate recognition. In this phase, the raw images obtained from the dataset or camera is processed to improve their quality and ensure consistency before they are passed into the recognition model.

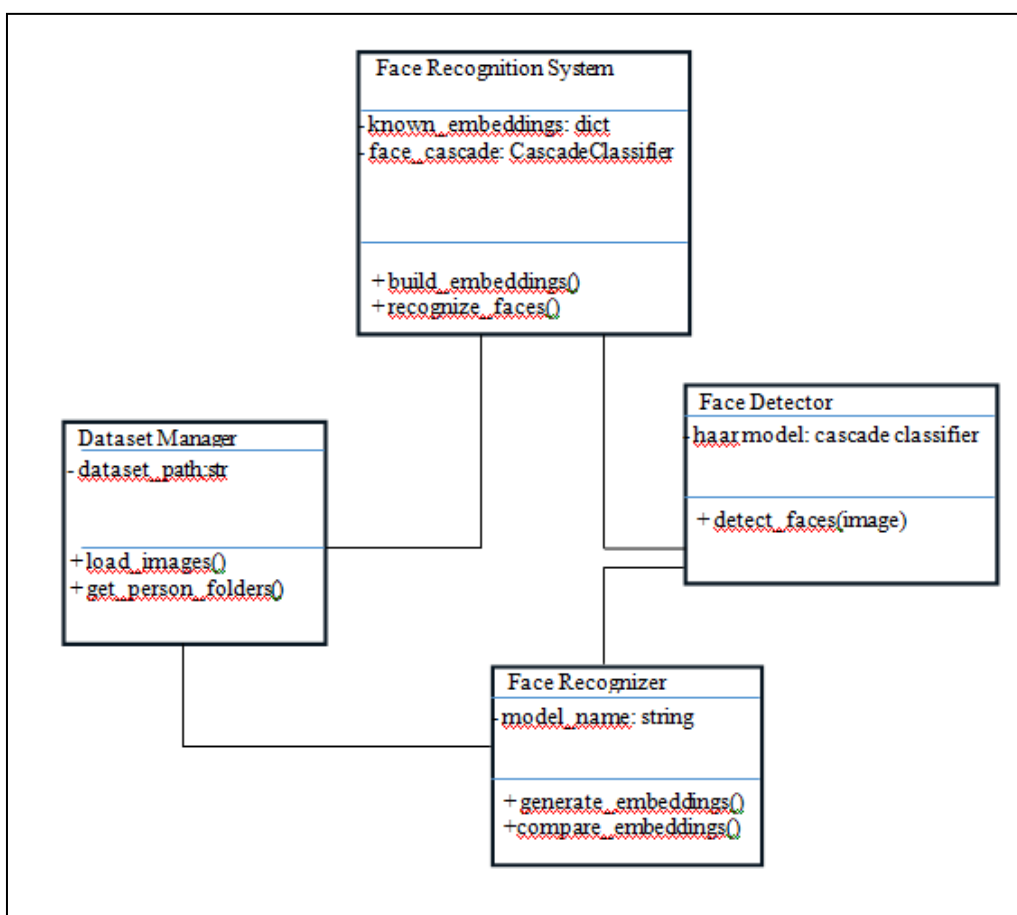


Figure 2 Class diagram of the recognition system

Haar cascade performs the face detection by extracting the facial region when a human face is seen while eliminating unnecessary background information. After the detection of the face, the extracted faces are cropped and resized to a standard dimension in order to maintain a consistent size suitable for the deep learning model. The next step involves the application of image normalization which adjusts the pixels values and reduce variations caused by lighting conditions, noise and camera differences. At the end, the processed images are prepared for feature extraction, where ResNet is used to extract distinctive facial features used for unique person identification.

In the recognition process, the system checks if faces are detected in the video frames. If faces are detected, the system draws a boundary box around the face and displays the name on the image. Conditionally, else the system displays an

“unknown” message appears. Fig. 2 shows the class diagram of face recognition system outlining the face recognition and detection process.

In other to improve the performance of the system and make it usable for real world criminal identification, a **unique identification number** is assigned to each face registered in the database, the number is linked to the individual’s **National Identity Number (NIN)** and can only be accessed by the authorized personnel. The unique identifier serves as a reference key within the system and allows law enforcement agents to efficiently search, retrieve, identify and verify the identity of individuals in the criminal cases. In criminal identification process, a face is uploaded or detected with the aid of camera and the corresponding unique identification number is retrieved, enabling authorities to quickly access the associated criminal records and personal identification details for further investigation. Table 1 shows a portion of the simulated National Identity Number (NIN) information linked with the unique identification numbers assigned to each face in the system. Figure 3(a) and Figure 3(b) illustrates an example of the system output where a detected face is recognized and assigned a unique identification number linked to the NIN database.

Table 1 Sample of National Identity Number (NIN) linked with the face Unique ID

Unique ID	NIN	Full Name	DOB	Gender	State
UID001	30987654321	John Okeke	12/03/1995	Male	Rivers
UID002	45678912345	Mary Musa	21/07/1998	Female	Lagos
UID003	56789123456	David Bello	05/01/1993	Male	Abuja



Figure 3 Face recognition output showing detected faces with assigned Unique Identification Numbers (UIDs) (a) Recognized face displaying UID 3852 linked to NIN record (b) Recognized face of the same persons recognized under a different facial expression

3.3. Analysis

This section shows the performance of described ResNet for face recognition using deep learning. The experiment was conducted on a dataset containing 31 known identities with a total of 2,498 images. For performance evaluation, three test images per identity class were used to assess the system’s ability to accurately recognize faces. A high-level facial features, represented as embeddings were extracted by the Resnet model which were used to capture the unique facial characteristics of each individual. Prior to using the technique, the dataset received some preprocessing to ensure that the input to the model is consistent and optimized for accurate recognition. The performance of the system was evaluated in other to determine its accuracy in facial recognition. Classification metrics employed include, True Positive (TP), False Positive (FP), True Negative (TN), and False Negative (FN).

- False positive (FP): incorrect positive prediction.
- True positive (TP): correct positive prediction.
- False negative (FN): incorrect negative prediction.
- True negative (TN): correct negative prediction

Precision

Measures the accuracy of the face detections by indicating the proportion of correctly identified faces among all faces detected

Formula:

$$Precision = \frac{TP}{TP + FP} \quad \dots 1$$

Recall (Sensitivity or True Positive Rate)

Indicates the system's ability to correctly detect actual faces

Formula:

$$Recall = \frac{TP}{TP + FN} \quad \dots 2$$

F1-Score

A harmonic mean of Precision and Recall, providing a balance between the two. Especially useful when the dataset is imbalanced

Formula:

$$F1 - Score = \frac{2 \times Precision \times Recall}{Precision + Recall} \quad \dots 3$$

The efficiency of the recognition system is evaluated using many statistical evaluation measurements, including F1-score, recall, precision, and confusion matrix.

Table 2 Comparative Performance Analysis

Parameters	LBPH	ResNet
Precision	0.71	0.75
Recall	0.47	0.54
F1-score	0.54	0.60

3.4. Performance Evaluation

For the effectiveness of the proposed criminal identification system, two face recognition pipelines were evaluated and compared. The pipelines are the classical Haar Cascade + LBPH and the deep learning-based Haar Cascade + ResNet approach. In figure 4, the confusion matrix for the LBPH model revealed limited recognition capabilities across many identities. The majority of the identities exhibited poor or zero recall, with over 50% of the classes receiving no correct classifications. This indicates that the LBPH model struggles to generalize in scenarios with high inter-class similarity and variations in lighting, expression, or occlusion. On average, the model demonstrated low recall and high misclassification, often failing to assign faces to the correct identity.

The performance evaluation clearly shows that the ResNet-based ArcFace pipeline is significantly more reliable for real-time and large-scale face recognition tasks within a criminal identification system. It offered better precision and recall, leading to higher confidence in suspect identification, especially under varied imaging conditions. Figure 6 shows the histogram containing the F1 Score by person for LBPH + Haar and ResNet + Haar

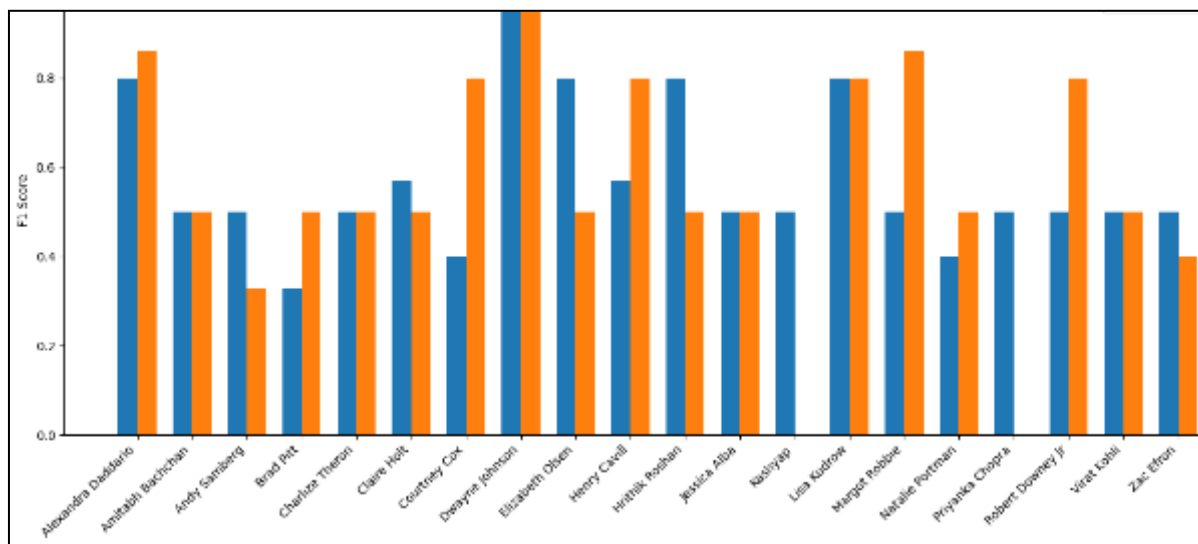


Figure 6 Histogram containing the F1 Score by person for LBPH + Haar vs ResNet + Haar

4. Conclusion and Future Scope

The ability of ResNet to capture deep, high-level facial features enables the system to maintain high recognition accuracy even under conditions that traditionally degrade performance, such as partial occlusion or low image quality. The combination of deep learning and classical detection techniques in this work marks a significant advancement in biometric identification systems for criminal justice applications. The real-time capability and high accuracy of the ResNet-based system underscore its readiness for practical use in environments requiring swift and dependable recognition. Another significant feature of the system is its high level of accuracy, which remains consistent under a variety of occlusion scenarios. This allows the system to meet the rigorous standards required for real-time applications. Additionally, the system's ability to minimize processing delays is crucial for environments where rapid identification is necessary, such as security systems, access control points, and surveillance systems. In these scenarios, where swift and dependable face recognition is critical to safety and operational efficiency, this system proves to be highly effective.

Future studies should explore several advanced directions to further improve the performance, adaptability, and privacy of criminal identification systems based on facial recognition. One promising area is robust occlusion handling, where generative models such as Generative Adversarial Networks (GANs) can be employed to reconstruct missing or obstructed facial features. Addition to improving recognition accuracy, ensuring data privacy is crucial. Federated learning approaches offer a solution by allowing models to be trained locally on edge devices, such as surveillance cameras or local servers, without transferring sensitive facial data to centralized systems. Adaptive lighting compensation should be investigated to enhance the system's performance under extreme or varying illumination conditions.

Compliance with ethical standards

Acknowledgments

The authors would like to acknowledge the developers and contributors of the publicly available facial image datasets used in this research. Their contributions made it possible to conduct the experiments and evaluate the performance of the proposed criminal identification system.

Disclosure of Conflict of Interest

The author declares that there is no conflict of interest regarding the publication of this paper.

Statement of Ethical Approval

All the facial images used in the experiments were obtained from publicly available datasets. The datasets were used strictly for academic and research purposes while ensuring privacy and anonymity. No personally identifiable information was misused, and the research adhered to relevant ethical and legal guidelines governing the use of biometric data.

Statement of Informed Consent

The facial image datasets used in this research were obtained from publicly available sources. The informed consent process was handled by the original dataset providers during the data collection stage.

References

- [1] Musa, Y. E. (2021). Insecurity in Nigeria: Causes, consequences and solutions. 20th Joint Planning Board and National Council on Development Planning, Maiduguri. <https://naturalplanning.gov.ng/uploads/2021/08/Insecurity-In-Nigeria-Causes-Consequences.pptx>
- [2] Atai, A. J., & Esetang, A. (2024). Insecurity in Nigeria: Forms, effects, and remedies. Zenodo, 2(1), 38. <https://doi.org/10.5281/zenodo.11060609>
- [3] Patil, N. H., Patel, S. H., & Lawand, S. D. (2023). Research paper on artificial intelligence and its applications. *Journal of Advanced Zoology*, 44(S8). <https://doi.org/10.53555/jaz.v44iS8.3544>
- [4] Coursera (2025). What is artificial intelligence? Definition, uses, and types. Coursera. <https://www.coursera.org/articles/what-is-artificial-intelligence>
- [5] GeeksforGeeks. (2024). Top 10 branches of artificial intelligence. GeeksforGeeks. <https://www.geeksforgeeks.org/top-10-branches-of-artificial-intelligence/>
- [6] Parasher, M., Sharma, S., Sharma, A., & Gupta, J. (2021). Anatomy on pattern recognition. *Indian Journal of Computer Science and Engineering*, 2(3), 371–378.
- [7] Wen, Y. A., Liu, W., Yang, M., Fu, Y., Xiang, Y., & Hu, R. (2010). Structured occlusion coding for robust face recognition. arXiv. <https://doi.org/10.48550/arXiv.1502.00478>
- [8] Kakkar, P., & Sharma, V. (2018). Criminal identification system using face detection and recognition. *International Journal of Advanced Research in Computer and Communications Engineering*, 9(10), 101–107.
- [9] Nguyen, T., Sheng, W., & Lakshamanan, B. (2019). A smart security system with face recognition. arXiv Preprint, arXiv:1812.09127.
- [10] Zafar, U., Ghafoor, M., Zia, T., Ahmed, G., Latif, A., Malik, K. R., & Sharif, A. M. (2019). Face recognition with Bayesian convolutional networks for robust surveillance systems. *EURASIP Journal on Image and Video Processing*, 1–10. <https://doi.org/10.1186/s13640-019-0406-y>
- [11] Apoorva, P., Impana, H. C., & Siri, S. L. (2019). Automated criminal identification by face recognition using Open Computer Vision classifiers. In *Proceedings of the International Conference on Computing, Communication and Security (ICCMC)* (pp. 1–5). <https://doi.org/10.1109/ICCMC.2019.8819850>
- [12] Kumar, V. D. A., Malathi, S., Vengatesan, K., & Ramakrishnan, M. (2020). Facial recognition system for suspect identification using a surveillance camera. *Pattern Recognition and Image Analysis*, 28(3), 410–420. <https://doi.org/10.1134/S1054661818030136>
- [13] Septyanto, M. W., Sofyan, H., Jayadianti, H., Simanjuntak, O. S., & Dessyanto, B. P. (2020). Aplikasi presensi pengenalan wajah dengan menggunakan algoritma Haar Cascade classifier. *Telematika: Jurnal Informatika dan Teknologi Informasi*, 16(2), 87–96. <https://doi.org/10.31315/telematika.v16i2.3182>
- [14] Tamrkar, S., & Gupta, A. (2020). Criminal Face Detection System Using Python. *IJIRT*, 7(2), 2349–6002. Prashanth Kumar, R., Majeed, A., Pasha, F., & Sujith, A. (2020). Real-time criminal identification system based on face recognition. *Advanced Science Letters*, 26(5), May. E-ISSN: 1936-7317.
- [15] Kumar, S., Gao, X., & Welch, I. (2020). A machine learning-based web spam filtering approach. In *IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*.

- [16] Bharathi, S. T., Indrani, B., & Amutha Prabakar, M. (2020). A supervised learning approach for criminal identification using similarity measures and K-medoids clustering. In International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICT).
- [17] Pawar, R., Rathod, M., Wadvekar, S., Karanjule, P., & Bhadgale, A. M. (2021). Automated criminal identification and notification system. International Research Journal of Engineering and Technology (IRJET), 8(5), 4265.
- [18] Ahmed, A., Guo, J., Ali, F., Deeba, F., & Ahmed, A. (2021). LBPH-based improved face recognition at low resolution. 2018 International Conference on Artificial Intelligence and Big Data (ICAIBD 2021), 144–147. <https://doi.org/10.1109/ICAIBD.2018.839618>
- [19] Achmad, S., AZ, N., & Solichin, A. (2023). Mobile-based student presence system using Haar Cascade and Eigenface facial recognition methods. Jurnal Riset Informatika, 5(2), 219–228. <https://doi.org/10.34288/jri.v5i2.340>
- [20] Wayakar, S., Kolage, P., Rao, B., & Andhare, S. (2024). Crime prediction and criminal identification system. DR. D.Y. Patil Institute of Engineering, Management Research, Akurdi, Pune, India. <https://www.jetir.org/papers/JETIR2304548.pdf>
- [21] Yesugade, K., Pongade, A., Karad, S., Ingale, D., & Mahabare, S. (2024). Face detection and recognition for criminal identification system. Bharati Vidyapeeth's College of Engineering for Women, Pune, India. <https://doi.org/10.47392/IRJAEH.2024.0267>
- [22] Reddy, P. S. K., & Naresh, M. (2025). Criminal identification using machine learning and face recognition techniques. International Journal of Engineering & Science Research, 15(1), 160–166. <https://doi.org/ISSN2277-2685>