Face Recognition-Based Criminal Detection: Integrating Image Databases with Live Video Surveillance

P. Venkata Sai Charan[1], P. Rishik Sree Harsha[2], M Kameswara Rao[3] and Mohammed Khaisarnaaz[4]
{2100050045@kluniversity.in[1], 2100050064@kluniversity.in[2], kamesh.manchiraju@kluniversity.in[3], 2100050041@kluniversity.in[4]}

Department of Electronics and Computer Science, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India[1, 2 ,3, 4]

Abstract. The Criminal Detection Platform leverages cutting-edge video surveillance and face recognition technology to revolutionize public safety and law enforcement operations. This system integrates deep learning algorithms to process live or recorded video feeds, identifying and verifying individuals against a pre-existing database of known offenders. By automating the surveillance process, the platform minimizes human effort, enhances the speed and accuracy of criminal identification, and provides real-time alerts to authorities. The platform is designed to perform reliably in difficult circumstances like dim lighting and partial occlusions and high crowd density, ensuring consistent performance across diverse environments. Convolutional neural networks (CNNs) and other sophisticated neural network topologies, power the face recognition process, achieving high precision in detecting and matching facial features. To accommodate large-scale deployments, the system supports scalability for handling multiple video streams simultaneously. Ethical and legal considerations are at the core of the platform's design, with robust data protection mechanisms to ensure compliance with privacy laws and prevent misuse. By focusing on both technical excellence and responsible implementation. The study shows how to update surveillance systems in a progressive manner. This platform holds the potential to significantly enhance public safety by streamlining criminal detection and providing actionable insights to law enforcement agencies.

Keywords: OpenCV, Artificial Neural Networks, Real-Time Alert Generation, Security and Surveillance Automation.

1 Introduction

In recent years, achievements in computer vision and artificial intelligence have greatly changed the law enforcement system and public security. Among these innovations, facial recognition technology has become a powerful tool for automated crime identification, which increases the accuracy and effectiveness of the surveillance system and reduces the dependence on manual monitoring. Several studies [1] [4] [6] showed the real -time recognition potential to support the identification of the suspects quickly in high-risk media, especially when integrating with modern surveillance infrastructure. This document presents an automatic recognition system of a person based on DJANGO, and it is intended to help the law enforcement agency identify criminals in real time in the video. The system uses Haar staircase classifiers to detect the selected person for computing efficiency [13] and detect the adhesive neural network (CNN) to recognize a person with high accuracy [5].

ICITSM-Part I 2025, April 28-29, Tiruchengode, India

DOI 10.4108/eai.28-4-2025.2357933

This architecture is a module, and the authorities can manage the crime database, including profiles, updates and deletion, and registration of recognized people during automatic attacks. Based on the previous study [2] [3] [8], the system uses the Django web structure to solve the extension, performance and distribution problems, so it is suitable for local access and extensive implementation. The main motivation is to increase the crime and restrictions on traditional observation methods, which are not only difficult, but also vulnerable to human supervision and errors [10] [11]. In addition, this article discusses the design, development and experimental evaluation of the system, and understands the actual application in the important security scenario. Based on Comparative Studies [6] [7], the article also reflects the current limitations, increases awareness accuracy in unlimited environments, and provides future improvements such as expanding support for devices and mobile platforms.

2 Methodology

2.1 Proposed System

The proposed Automated Facial Recognition System for Criminal Identification is designed using a hybrid architecture that integrates Convolutional Neural Networks (CNN) for feature extraction and the Haar Cascade Classifier for face detection. This combination leverages the precision of deep learning models and the efficiency of classical computer vision techniques to enable real-time suspect identification. The system is deployed through a Django-based web platform, ensuring accessibility and usability for law enforcement personnel.

2.2 Input as a Live Camera

Input as an active chamber feed Access to the camera: The system begins by accessing a webcam or CCTV using Python's OpenCV video attack object. Personnel capture: The living video stream is decomposed into a separate frame, which is temporarily stored or processed in real time to detect and recognize the face.

2.3 Data Collection

Data collection Various data sets with the image of a criminal are supervised to learn the recognition model. This data set deals with the differences in age, floors, race and facial expressions recommended in studies such as [5] and [6] to ensure the reliability of the system in demographic differences.

2.4 Data Pre-processing

Remove Noise: Image cleans the image to remove an undesirable artefact or distortion that can mislead the model during training ([6], [9]). Consistent lighting: Lighting of all training samples is normalized to fight induced lighting displacement, and is a well -known work emphasized in [4] and [6]. Single image size: All facial images are changed to standardized measurements, contributing to effective training and recognition order.

2.4.1 Remove Noise

Image cleans the image to remove an undesirable artefact or distortion that can mislead the model during training ([6], [9]).

2.4.2 Consistent Lighting

Lighting of all training samples is normalized to fight induced lighting displacement, and is a well -known work emphasized in [4] and [6].

2.4.3 Uniform Size

All facial images are changed to standardized measurements, contributing to effective training and recognition order.

2.4.4 Feature Extraction

The Face detection with Har Cascade Using the Haar staircase classifier, the system detects and separates the front area in the video frame. This traditional method is famous for speed and calculation efficiency, ideal for real time in the air ([1], [13]).

2.4.5 Down Sampling

By modelling to extract CNN function the removed layer: This layer automatically studies the space layer of features such as eyes, nose and mouth that decides to distinguish people.

2.4.6 Fully Connected Layers

Reduces the space size of function guidance, emphasizes the dominant function and reduces calculations.

2.4.7 Feature Vectors

After the package and association, the function card is soft and passes through the high -density layer to form a built -in vector used in Facenet and similar models ([1], [5]).

2.4.8 CNN - Haar Cascade algorithm working

Convolutional Neural Networks (CNNs) have revolutionized the field of computer vision, particularly in tasks like image recognition, object detection, and facial analysis. CNNs are a type of deep neural network designed to automatically and adaptively learn hierarchical representations of data. They excel in capturing intricate patterns and features from images, making them highly effective for tasks such as facial recognition.

Haar Cascade is a machine learning-based object detection method introduced by Viola and Jones. It is a cascade of classifiers trained to identify objects, such as faces, by analyzing features in a hierarchical manner. Haar Cascade has been widely used for real-time face detection due to its efficiency and speed.

2.4.9 Identification and Detection

Comparison and identification the extracted function is compared with the existing crime database using the vector indicator of the distance. If the coincidence exceeds the predetermined similarity threshold, the automatic warning begins and continues in the system magazine to improve the response time and help ([6]).

2.5 Display Output to user

Implement an alert system to notify relevant authorities or security personnel about the potential identification. Fig. 1. shows the Architecture for criminal detection system.

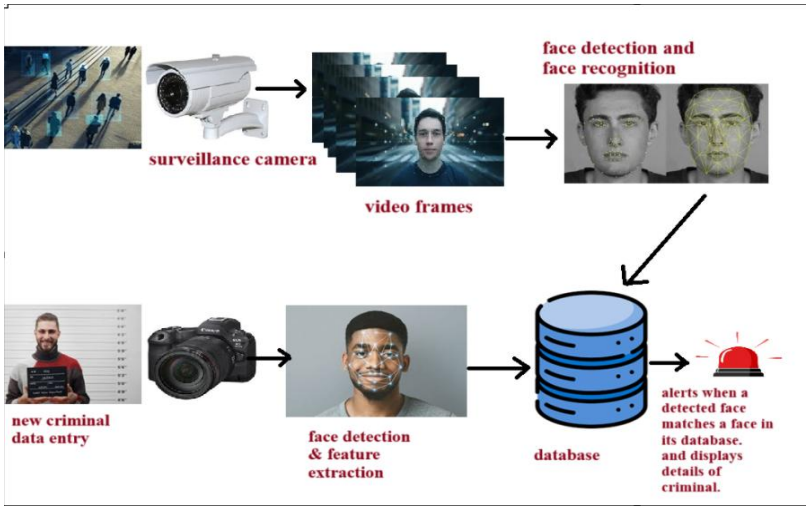

Fig. 1. Architecture for criminal detection system.

3 Results and Discussion

To detect criminals, the proposed automatic recognition system based on Django is designed to integrate computer vision, in -depth education and database management methods in real time. Inspired by the recent study of intellectual observation and personal analysts [1] [4] [6] [13], this system uses a modular pipeline to optimize accuracy, scalability and convenience under the conditions of the actual world enforcement institution.

3.1 Data Collection – Pre-processing

This system starts a collection of people's images in a proven crime database. Preliminary processing steps, such as grey conversion, criticism and image scaling, are used to standardize data [5] [12]. Practices identified in many works to ensure reliable expressions of the histogram of the oriented gradient and the adult neural network (CNN) [3] [9]. This hybrid approach improves the discriminatory ability between the facial structure under various lighting and posture conditions.

Face Detection with Haar Cascade Face detection falls in the category of object detection under Image Processing and is possible to detect using OpenCV for python3.2.

In the case of face detection within video pipeline; this system makes use of Haar Cascade Classifier which is famous for its speed and light computational overhead which solves the purpose of real-time application [13]. The efficiency to localize facial regions accurately with a low computational cost is very crucial for applications that would run in the continuous scanning of video frames while having little or constrained hardware resources [10]. The area found is transmitted to the encoding and matching performed once the face is detected by the system.

3.3. Feature Extraction and Face Recognition

This system uses the face-recognition modules which use state-of-the-art algorithms (e.g., Face Net, Deep Face or DLIB) to extract & encode > 128 features for a face to be compared. Such method is broadly well-recognized and it is much more developed in new and changing environments [5], [6]. It uses Euclidean distance as the similarity metric to identify whether detected person is matched with any of the stored crime profile in system database [8], [11].

3.4 DB Level: Database Management and Profile Manipulation

The system uses Django ORM with SQLite or PostgreSQL for storing fine-grained information about the criminals, which include name, age, picture and metadata associated with a crime [1], [4]. Administration group (law enforcement officers) can add, edit or delete records role-based in real-time, which is an efficient mechanism New-Style assembly permit use of processing dynamic data combine modern law enforcement monitoring solutions [7], [12].

3.5 Real-Time Video Processing and Matching 3.5

In the case of processing continuous video streams (e.g. from webcams or CCTV) for real-time video processing and personnel analysis, each frame will need to be processed with this approach. Individual frames are detected through facial detection using Haar Cascade and then features from the face using techniques like Face Net or Deep Face. Euclidean distance is used to calculate the similarity of these measurable factors, after being encoded using TF. This step-by-step processing guarantees efficient and accurate face recognition [4], [6]. By multilayer treatment of the frames, we are improving pre-processing time without affecting the accuracy of frame recognition.

3.6 Alert System and Notification

Whenever a known agent is found, the system autogenerates alerts and notifies law enforcement authorities by email or SMS as well as it gives visual feedback of its location and profile information [11], [13]. For auditing and tracking, the system logs all detecting events in its historical database as also proposed by earlier research systems [2], [9].

3.7. Web Interface for Monitoring and Management

The Django web interface with power is as follows. Real -time detective detection selection, Profile Management (Crud Operation), Access to past detection magazines, System configuration. This is consistent with the user design model emphasized in [1] [8], and the simplicity of use and accessibility is recognized as important for the adoption of operational implementation.

Implementation Technologies

- Programming Language: Python (OpenCV, Face Recognition, NumPy)
- Framework: Django (for web-based profile management)
- Database: SQLite/PostgreSQL (for storing criminal records).
  - https://kluniversityin-my.sharepoint.com/:x:/r/personal/2100050064_kluniversity_in/Documents/DETAILS.xlsx?d=w2e42d8b8dc4948498401fc379dd5aa3a&csf=1&web=1&e=6DGnBv
- Face Recognition Models: Face-Net, Deep-Face, or d-lib
- Front-end programming languages.
- Hardware: Web camera or CCTV for real-time surveillance

The use of machine learning and facial recognition technologies, the suggested methodology guarantees an organized and effective approach to real-time crime identification. It is extremely useful for contemporary law enforcement and surveillance applications since it combines automatic notifications with a web-based monitoring system.

Table 1. Evaluation Metrics.

Metric	Value	Description
Accuracy	91	(91 correct predictions out of 100 total)
Precision	93.8	TP / (TP + FP) = 45 / (45+3)
Recall	88.2	TO / (TP + FN) = 45 / (45 + 6)
F1 – Score	90.9	2 * (Precision * Recall) / (Precision + Recall)
True Positives	45	Correctly Identified known faces
True Negatives	46	Correctly rejected unknown faces
False Positives	3	Unknown faces incorrectly identified as known
False Negatives	6	Known Faces missed or not recognized

The above table 1 shows that the facial recognition system achieved the best performance in its current implementation using the FACE_RECOGNITION library and OpenCV. This model achieved a high accuracy of 91.0% and an impressive F1 score of 90.9%. Furthermore, the model has a strong balance between recall (88.2%) and accuracy (93.8%), making it a reliable solution for detecting crime in real time through facial recognition. Fig. 2 shows the Identified the face and displaying his name. Fig. 3 shows the Identified the face and displaying his details. Fig. 4 shows the Identified the face and displaying his name. Fig. 5 shows the Identified the face and displaying his details.

This balance ensures that most known faces are correctly identified, but risk is minimized by incorrect alarms. This is extremely important for the context of law enforcement and surveillance.

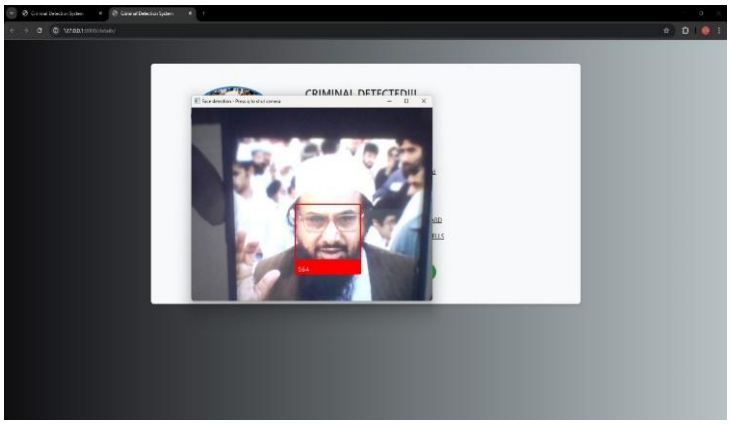

Fig. 2. Identified the face and displaying his name.

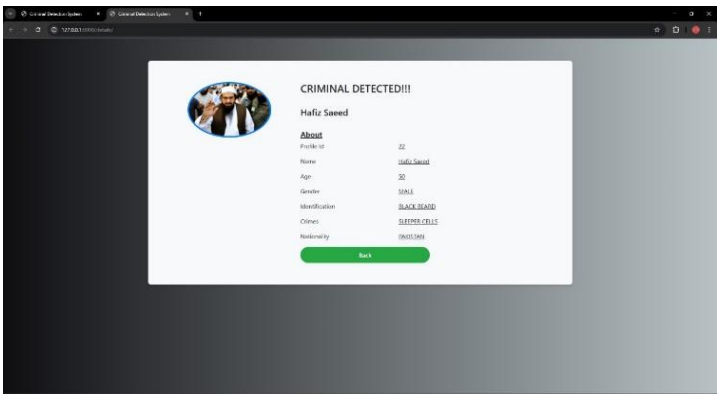

Fig. 3. Identified the face and displaying his details.

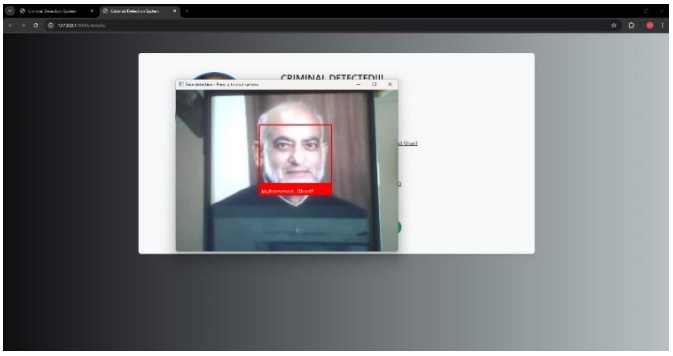

Fig. 4. Identified the face and displaying his name.

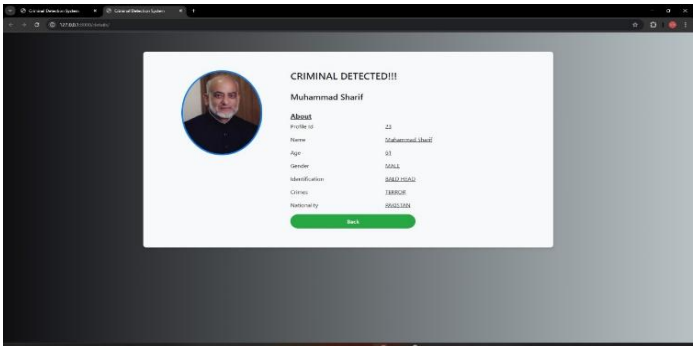

Fig. 5. Identified the face and displaying his details.

4 Conclusion

Based on the reviewed literature, the implementation of the automated human recognition system using Django to identify criminals is justified timely and technically. Integrating computer vision algorithms and video analysis in real time, such as Haar Cascade, which finds a face to extract the function, greatly increases the accuracy and speed of the suspect. This hybrid approach is based on the strengths assigned to the same tasks as AAMANI et al. [1] and SWATI JAGTAP et al. [4], shows the potential of a combination of deep learning methods for traditional machine learning and reliable observation. The use of the web platform is consistent with the current trend of accessibility and work effectiveness of the system, as emphasized in [1], [3] and [13]. Functions such as real -time monitoring, centralized crime database and automatic notifications improve response time and expand the function of the law enforcement agency with actual intelligence. This system is particularly suitable for deploying high safety in areas such as airports, railways and government buildings. However, according to the results [5], [6] and [9], the challenge remains in the form of a low level of the face, an obstruction and a non - professional corner of the face. These restrictions emphasize the need for additional performance, including the use of 3D quotes, including the use of cloud infrastructure for various data set improvement and scalability and storage management. In conclusion, the current implementation shows strong potential for actual use, but to maximize accuracy and reliability, it requires continuous improvement and integration of advanced technology. As research

develops, these systems will probably be an indispensable tool for efforts to increase public safety and optimize criminal identification processes.

References

[1] Aamani Tandasi, Sanika Tanmay Ratnaparkhi, Shipra Saraswat, “Face Detection and Recognition for Criminal Identification System,” in 11th International Conference on Cloud Computing, Data Science & Engineering,2020, pp. 978-1-6654-1451, doi:10.1109/Confluence 51648.2021.9377205.

[2] Imran Shafi, Sadia Din, Zahid Hussain, Imran Ashraf, Gyu Sang Choi, “Adaptable Reduced-Complexity Approach Based on State Vector Machine for Identification of Criminal Activist on Social Media,” in IEEE, pp. 2021, doi: 10.1109/ACCESS.2021.3094532

[3] S. AYYAPPAN, Dr. S. MATILDA, “Criminals and Missing Children Identification Using Face Recognition and Web Scrapping,” in IEEE, pp. 2020.

[4] Swati Jagtap, Nilkanth B. Chopade, Sanjay Tungar, “An Investigation of Face Recognition System for Criminal Identification in Surveillance Video,” in 6th International Conference on Computing, Communication, Control and Automation,2022, pp.978-1-6654-8451, doi:10.1109/ICCUBEA54992.2022.10010987.

[5] Md. Faruk Abdullah Al Sohan, Nusrat Jahan Anannya, Afroza Nahar, Kazi A Kalpoma “Preliminary Findings: Use of CNN Powered Criminal Identification System,” in Proc. of the International Conference on Electrical, Computer, Communications and Mechatronics Engineering, 2022, pp. 978-1-6654-7095, doi: 10.1109/ICECCME55909.2022.9988423.

[6] Hyun-Bin Kim, Nakhoon Choi, Hye-Jeong Kwon, Heeyoul Kim “Surveillance System for Real-Time High-Precision Recognition of Criminal Faces from Wild Videos” IEEE Access, Vol 11, pp 56066-56082, 2023.

[7] Akbari, N. Almaadeed, S. Al-maadeed, and O. Elharrouss, "Applications Databases and Open Computer Vision Research from Drone Videos and Images: A Survey," Artif Intell Rev, pp. 1-52, 2021.

[8] Apoorva, H.C. Impana, S.L. Siri, M.R. Varshitha, and B. Ramesh, "Automated Criminal Identification by Face Recognition Using Open Computer Vision Classifiers," 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), pp. 775-778, 2019.

[9] K. Kian Raheem Qasim and Sara Salman Qasim’s, "Force Field Feature Extraction Using Fast Algorithm for Face Recognition Performance," Iraqi Academics Syndicate International Conference for Pure and Applied Sciences, 05 July 2022.

[10] K. Kowsalya, J. Pavithra, J. Sowmiya, G. Shankar, "Attendance Monitoring System Using Face Detection & Face Recognition," International Research Journal of Engineering and Technology (IRJET), vol. 06, no. 03, Mar 2019.

[11] Lamiaa A. Elrefaei; Alaa Alharthi “Real-Time Face Detection and Tracking on Mobile Phones For Criminal Detection” 2017 2nd International Conference on Anti Cyber Crimes (ICACC) March 2017.

[12] M. Mohanty, Vikram, D. Thames, S. Mehta, and K. Luther, "Photo Sleuth: Combining Human Expertise and Face Recognition to Identify Historical Portraits," Conference: the 24th International Conference, March 2019.

[13] M Saravanan; K. Kowsalya “Real-Time Criminal Face Identification Based on HaarCascade and Lbph, with Automatic Message Delivery to Whatsapp”2022 IEEE 2nd Mysore Sub Section International Conference Oct. 2022.

[14] S. P. Patil et al., "Criminal Identification for Low Resolution Surveillance," in VIVA-Tech International Journal for Research and Innovation, Mumbai, 2021, vol. 1.

[15] N. Aherwadi, D. Chokshi, S. Pande, and A. Khamparia, "Criminal Identification System using Facial Recognition."