International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 06 | June - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Face Recognition for Criminal Detection System

Dr. R.Satya Ravindrababu, Asst. Professor, 1.MS.Himaja Vendra, 2.Mr.Y. Purna Chandra Viany Kumar 3.Ms. T. Dhanunjay, 4.Mr. S.Abdul Kadhar Jeelani.
Department of Computer Science Lendi Institute of Engineering and technology JNTU GV, Vizianagaram,Andhra Pradesh,India
satyaravindrababu.r@lendi.edu.in, himajavendra@gmail.com, ypcvinay@gmail.com, dhanurock231@gmail.com, abdulshaik3511@gmail.com

***Abstract*— Face recognition is an advanced technology that enables computers to identify individuals by analyzing unique facial features. In the context of law enforcement and public safety, face recognition systems play a vital role in identifying suspects, tracking criminals, and preventing unlawful activities. These systems capture images or video frames containing human faces and match them against a database of known criminals to detect potential threats. The accuracy and efficiency of such systems make them invaluable tools in enhancing security and reducing manual workload. This system utilizes a real-time video feed or uploaded images to scan faces and compare them with a centralized database of previously registered criminals. If a match is found, it retrieves the individual's details and alerts the user accordingly**

This technology can be deployed at various high-security and public locations such as public events and places. By doing so, authorities can monitor crowds and proactively identify individuals with criminal records. In the long run, this system acts as a preventive tool, deterring criminal activity through early detection and intervention. Furthermore, it can be integrated with law enforcement databases and alert systems to trigger immediate responses from security personnel when a threat is identified.

Keywords—Criminal detection system, Face Recognition, Deep Learning, Automated detection, DeepFace.

I. Introduction

In the context of law enforcement and public safety, face recognition systems play a vital role in identifying suspects, tracking criminals, and preventing unlawful activities The Face Recognition for Criminal Detection System is designed to automate the process of identifying criminals by leveraging deep learning and computer vision techniques. This system utilizes a real-time video feed or uploaded images to scan faces and compare them with a centralized database of previously registered criminals. If a match is found, it retrieves the individual's details and alerts the user accordingly. This approach not only improves the speed of identification but also eliminates the possibility of human error during manual verification.The software also supports criminal registration, where detailed personal data including name, crime type, distinguishing features, and facial images are stored. This database becomes the core of the recognition process, enabling precise identification even under challenging conditions like partial occlusion or facial hair changes. Additionally, the system can handle multiple face detections simultaneously, allowing for effective crowd surveillance and real-time monitoring in densely populated areas.

Beyond surveillance, the system has applications in forensic analysis and investigation. Security agencies can upload images from crime scenes or CCTV footage into the system to identify suspects. The automated nature of the process significantly reduces investigation time and increases the chances of apprehending offenders quickly. Moreover, repeat offenders can be tracked more effectively, allowing for pattern recognition and predictive policing strategies.

The implementation of a face recognition system in criminal detection brings numerous advantages, including improved accuracy, faster identification, and seamless database integration. It minimizes reliance on traditional ID checks or manual observations and allows for proactive action before crimes escalate. As the system continues to learn and adapt, its accuracy and reliability will only improve over time..

II. Literature Review

There are many different parts that need to be thought out before designing a system. Creating the architecture, designing modules and interfaces, and selecting adequate components - all these things require some knowledge and experience. The design process would work like systems theory as seen usually in product development. The proposed automated attendance system consists of 5 main

components. The process is described in detail.

In [1], the authors proposed a face recognition-based attendance system using the Eigenface recognition method. The system converts facial images into Eigenfaces, and recognition is achieved by comparing input images with stored Eigenfaces in the database. However, this method is highly sensitive to variations such as background clutter, head orientation, facial hair, or accessories like glasses. In contrast, the proposed system in our project is robust to such variations and accurately recognizes individuals even with facial changes or occlusions.

In [2], the researchers improved the classic Viola-Jones face detection method by integrating a human skin tone histogram as a weak classifier to eliminate false positives. Additionally, classifiers based on eye and mouth detection further reduced incorrect face identifications. This enhanced approach increases the overall detection rate while maintaining an extremely low false rejection rate, which is crucial for real-time criminal surveillance applications.

In [3], a home door-locking system based on face recognition was proposed. It used a Raspberry Pi to capture facial parameters at different angles and converted them into grayscale images. Designed primarily for single households and senior citizens, the system improves home security and could be extended to hybrid security systems using additional features like fingerprint scanners, keypads, and laser-based protection. Though initially intended for homes, the low-cost implementation suggests its adaptability for broader security applications like law enforcement and crime prevention.

In [4], the paper addressed the challenges of integrating emotion recognition from speech into human-computer interaction systems. While not directly focused on facial recognition, it introduces important methodologies such as fast feature extraction and voice activity detection, which could complement face-based surveillance systems in public security scenarios by analyzing both visual and audio cues in real-time.

In [5], the authors proposed a face recognition system optimized for Android mobile devices. The system uses Local Binary Pattern (LBP) features along with adaptive lighting normalization for robust face identification. All processing is performed locally on the device, eliminating the need for cloud computation. This decentralized approach can be adopted for mobile crime detection systems where suspect identification must occur offline or in remote areas.

In [6], a hybrid approach was developed combining Local Binary Pattern Histograms (LBPH) and Fisherface algorithms to improve facial recognition under varying lighting conditions. The LBPH classifier handles lighting changes effectively, while the Fisherface algorithm extracts significant facial features for classification. This combination ensures reliable recognition with minimal training images and is well-suited for criminal detection systems with limited data.

In [7], the system aimed to detect frontal and side-view faces from indoor surveillance video. The process included RGB-to-YCbCr conversion, skin color segmentation, histogram analysis for skin pixel detection, followed by Haar feature extraction and classification using an enhanced AdaBoost algorithm. The classifier effectively distinguishes between non-face regions, frontal, and side-view faces, making it suitable for real-time criminal tracking in surveillance footage.

In [8], a practical system for real-time face detection and recognition using webcams was implemented. The system used Haar cascade classifiers for detection and a hybrid recognition model trained on the Extended Yale Face Database for classification. Face detection was applied on each video frame, making the model suitable for live monitoring scenarios, such as those used in public safety networks.

In [9], the authors implemented face recognition using the Haar Cascade algorithm in OpenCV and a Local Binary Pattern-based recognizer. Compared to other approaches, this system achieved high recognition rates even with varied facial expressions and accessories. The combination of Viola-Jones detection and AdaBoost classification allowed for efficient and accurate detection, forming a strong foundation for criminal identification frameworks.

Performance Evaluation

To evaluate the effectiveness of the face recognition system, various performance metrics were employed, including the confusion matrix, precision, recall, and F1-score. These metrics provide a comprehensive assessment of how well the model classifies faces and distinguishes

between positive and negative cases.

The **confusion matrix** plays a crucial role in assessing classification models by summarizing the system's predictions against actual outcomes. It consists of four elements: true positives (TP), false negatives (FN), false positives (FP), and true negatives (TN). True positives refer to correctly identified faces, while true negatives indicate correctly rejected non-matches. Conversely, false positives occur when an incorrect match is predicted, and false negatives represent instances where the model fails to recognize a valid face. The confusion matrix offers insights into the model's strengths and areas that need improvement.

From this matrix, various performance metrics can be derived to assess the model's classification effectiveness.

Precision, a key metric, measures how many of the predicted positive cases were actually correct. It is calculated using the formula:

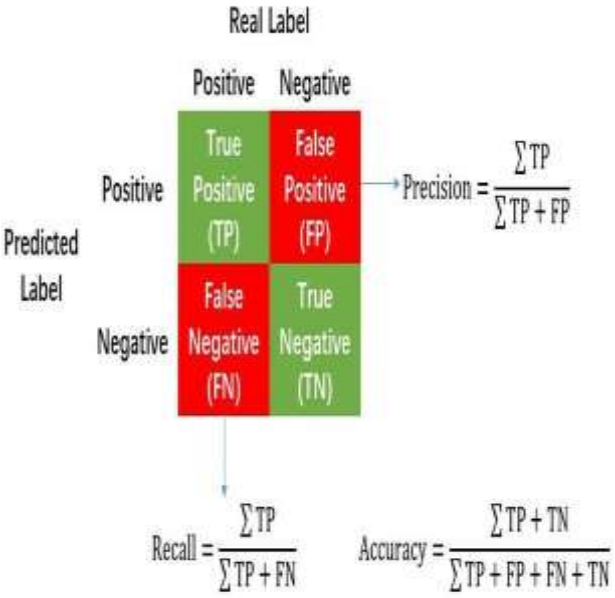
$$\text{Precision} = \frac{TP}{TP + FP}$$

$$\text{Recall} = \frac{TP}{TP + FN}$$

$$\text{IoU} = \frac{(Object \cap Detected\ box)}{(Object \cup Detected\ box)}$$

A precision score of 80.0% indicates that the model has a low false positive rate, which is particularly important in applications where incorrect identifications must be minimized, such as security and surveillance systems.

Recall, also known as sensitivity, measures the model's ability to correctly identify actual positive cases. It is defined as:



Using the values from the confusion matrix:

A recall of 66.0% indicates that the model successfully identifies most real faces, making it highly effective in scenarios where missing a positive case could be costly, such as biometric verification systems.

The **F1-score** is the harmonic mean of precision and recall, balancing the trade-off between them. It is given by:

$$\begin{aligned}\text{Micro F1 Score} &= \frac{\text{Net } TP}{\text{Net } TP + \frac{1}{2}(\text{Net } FP + \text{Net } FN)} \\ &= \frac{M_{11} + M_{22}}{M_{11} + M_{22} + \frac{1}{2}[(M_{12} + M_{21}) + (M_{21} + M_{12})]} \\ &= \frac{M_{11} + M_{22}}{M_{11} + M_{12} + M_{21} + M_{22}} \\ &= \frac{TP + TN}{TP + FP + FN + TN} \\ &= \text{Accuracy}\end{aligned}$$

An F1-score of 72.73% demonstrates that the model maintains an optimal balance between precision and recall, making it reliable for real-world face recognition applications. This balanced score ensures that the system is both accurate and effective in distinguishing between different faces while minimizing errors.

Why Deep Learning Techniques Are Superior in Criminal Detection Systems Using Computer Vision

Deep learning has transformed modern criminal detection systems by offering robust, accurate, and real-time face recognition capabilities. In our

criminal detection project, we harness deep learning frameworks such as DeepFace and YOLO to perform surveillance-based and image-based identification of criminals, significantly outperforming traditional manual or rule-based systems.

One of the most critical advantages of deep learning is its automatic feature learning capability. Unlike traditional vision techniques that rely on handcrafted features, deep learning can learn complex facial patterns directly from raw images. In our system, we utilize DeepFace, a high-level framework that wraps around powerful deep learning face recognition models (such as VGG-Face, Facenet, ArcFace, Dlib, and SFace). These models extract unique face embeddings, which are then compared with stored criminal records for identity verification.

Our project also integrates YOLO (You Only Look Once) for real-time face detection in surveillance footage. YOLO's speed and accuracy enable the system to process live video streams, detect multiple faces simultaneously, and pass them to DeepFace for recognition. This allows real-time alerting when a known criminal is identified in a monitored area.

To manage data, we use SQLite and MySQL databases to store structured records including criminal details, face embeddings, and case history. The system retrieves this data upon successful face matches, displaying full details in the Tkinter-based desktop application or via a Flask-powered web interface.

Unlike traditional systems that struggle with occluded or low-quality images, our deep learning setup generalizes well even under suboptimal conditions like poor lighting or partial face visibility. This makes it especially useful in practical law enforcement scenarios.

Furthermore, deep learning frameworks like DeepFace allow for plug-and-play architecture. Developers can switch between underlying models or fine-tune them on custom data without building models from scratch. This adaptability shortens development time and increases system flexibility.

The project also benefits from real-time deployment capabilities, supported by GPU acceleration. With proper optimization, the detection and recognition pipeline performs efficiently on standard systems, and can be further accelerated on edge devices.

In conclusion, deep learning techniques — through tools like DeepFace and YOLO — enable our criminal detection system to operate with high accuracy, adaptability, and real-time efficiency. These advantages make deep learning not only suitable but essential for building intelligent, automated, and scalable criminal identification solutions in today's rapidly evolving security landscape.

A. Image Capture

The camera is positioned directly in front of the suspect to capture clear, frontal facial images for registration or surveillance. The camera remains in focus and does not require manual adjustments for each individual. Proper lighting conditions are essential so that the facial features of the suspect are clearly visible. It is recommended that the individual faces the camera directly during the capture process.

To ensure an accurate image of the suspect, it is advised to maintain a distance of at least 3 feet between the camera and the individual, ensuring that the entire face fits within the frame. Once the individual is properly positioned, the officer can press the capture button on the app to take a photo. The image is then saved and used for further face recognition and criminal identification processes.

B. Face Detection

An effective face detector significantly improves the performance of any face recognition-based criminal detection system. Detection algorithms may use facial geometry or be invariant to changes due to age, disguise, or appearance. Approaches involving Machine Learning are often very effective [2]. The criminal detection process flow is illustrated in Fig. 1.

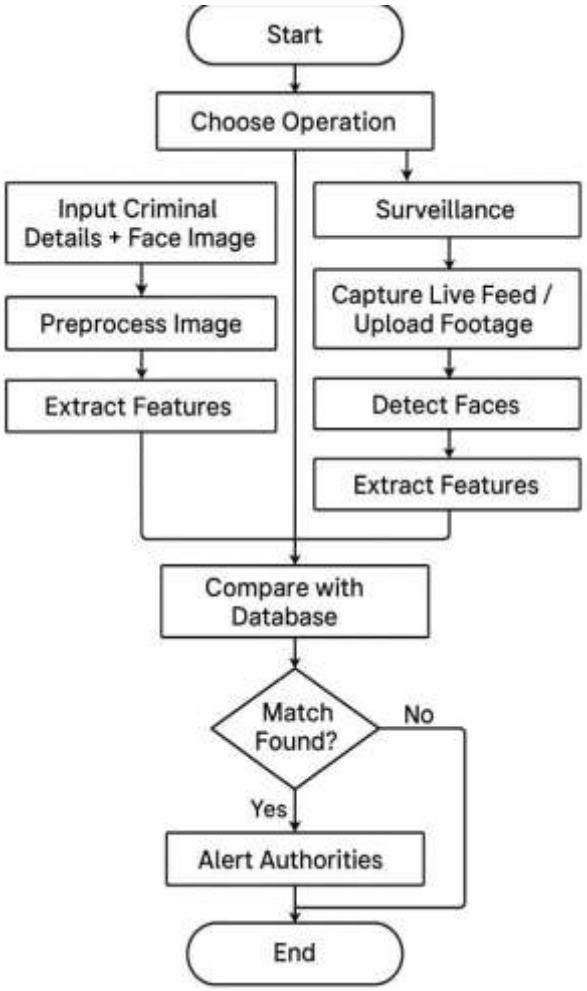


Fig. 1. Criminal Detection Flow Diagram

C. Pre-Processing

The faces detected from registration or surveillance feeds are processed to make them suitable for accurate recognition. Face recognition is a complex task involving multiple pre-processing stages. These include: 1) image enhancement, 2) face alignment, 3) embedding generation, and 4) matching against stored criminal records. After pre-processing, facial features such as the eyes, nose, and mouth are isolated to enhance recognition accuracy.

Each facial component contributes a specific probability weight based on its clarity and reliability. For instance, if the eyes are clearly visible but the mouth is partially obscured, the system may assign more weight to the eye region. These probabilistic filters help simplify the computational complexity and enhance system accuracy by focusing on the most reliable attributes [3].

D. Database Development

We have implemented a storage-level database to store the face embeddings and detailed profiles of registered criminals. JPEG is used as the image format due to its efficient lossy compression, reducing file size without significantly compromising image quality. For our desktop version, **SQLite** is used.

Each criminal profile includes personal details such as name, gender, nationality, and associated crimes. The face embeddings generated during pre-processing are also stored in the database. When a match is found during detection, a query retrieves the suspect's full profile. The system maintains a one-to-one relationship between each individual's record and their face model to ensure fast and accurate matching.

E. Post-Processing

Post-processing in our system refines the final recognition results after the initial match is made. This includes removing non-relevant facial attributes such as masks, hats, or sunglasses when possible. Once a match is confirmed, the system cross-verifies the individual's identity with the database and displays the complete criminal profile on the frontend interface.

Reports are generated from this data, which can include real-time detection logs, daily criminal match reports, or alerts for high-risk individuals. The system allows law enforcement officers to correct any false positives, thereby training the system to become more accurate over time.

Email APIs are integrated to send daily alerts to authorized personnel, and push notifications can be enabled for both desktop and mobile platforms. These updates help the police stay informed in real-time about potential threats or identifications made during surveillance [4].

III. Working Principle

INPUT: Faces of suspects captured in a surveillance video feed and photo based.

OUTPUT: Identification of criminals and corresponding details based on facial recognition.

PROBLEM DESCRIPTION: Recognizing the faces of criminals and matching them to those in

the database for criminal identification.

Step I: Start

Step II: To facilitate accurate recognition, criminals' details are enrolled in the criminal database beforehand.

Step III: Set up a surveillance camera in the designated area. The camera will constantly capture the faces of people in the vicinity.

Step IV: Face Detection using Deeplearning.

Step V: The face recognition algorithm uses a binary code of how dark pixels are distributed in an image.

Step VI: If the face matches any criminal in the database, proceed to display criminal details and mark as identified.

Step VII: If no match is found, mark as unidentified and log the face for future reference.

Step VIII: Save recognition data and display relevant information to the admin or law enforcement.

Step IX: End.

IV. Proposed Methodologies

The tools and methodologies for implementing face detection, recognition, and criminal identification are listed below.

A. DeepFace

DeepFace is a powerful deep learning framework used for face recognition. It extracts facial embeddings and uses them to compare faces accurately. DeepFace employs several pre-trained models such as VGG-Face, Google FaceNet, OpenFace, DeepID, and Dlib. It provides an easy-to-use interface and can be integrated with existing surveillance systems to detect and identify faces in real-time.*Local Server*

B. Local Server

A local server hosts the backend for processing and storing facial recognition data. The server handles incoming data from surveillance cameras, processes it using face recognition models, and updates the database with the identified criminals. The server will also serve as the point of contact for law enforcement to access criminal details.

C. *Face Detection*

Face detection identifies and locates a face within an image or video frame. We will use a deep learning-based approach like

DeepFace to extract facial embeddings and match them against the database. A well-trained face detection system ensures that all faces captured by the camera are processed and identified correctly.

D. *Feature Extraction*

In face recognition, feature extraction is the process of converting a face image into a numerical representation (embedding). The extracted features are compared against a database of known criminals. The recognition process involves matching the embeddings from the captured image to those stored in the database. If a match is found, the system identifies the individual and retrieves their criminal record.

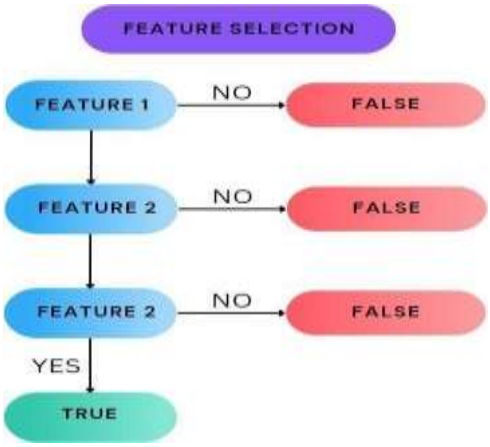


Fig. 2. Feature Extraction

E. *Criminal_Identification*

After face detection and feature extraction, the system compares the extracted facial features against the database. If a match is found, the system retrieves the criminal's record and displays relevant information (e.g., name, criminal history, photo) to the admin or law enforcement officer. If the face is not in the database, the system logs the image for future reference.

F. *Report_Generation*

Once criminals are identified, detailed reports can be generated based on the recognition data. These reports may include the criminal's name, ID, and the date/time of detection. Additionally, bulk reports can be exported for

record-keeping or for sending to relevant authorities. The system can also provide real-time notifications or email alerts to law enforcement about detected criminals.

V. RESULT

The criminal detection system works by constantly monitoring video streams for faces, using DeepFace to compare these faces against a database of criminals. When a match is found, the system identifies the criminal and displays relevant information such as their photo, name, and criminal record.

The system has an Authentication System built into it and needs a user ID and Password for access. The system will have one role i.e Admin/Law Enforcement. Users can Control and View criminal Records. admin login portal is shown in Fig. 3.

Fig 3. Login Page for admin/Law Enforcement

The Criminal Registration Page is an essential part of the criminal detection system, allowing law enforcement officers or admins to add new criminal profiles to the database. This page facilitates the process of registering criminal details, including personal information, physical attributes, and a photograph for accurate facial recognition shown in fig 4.

Fig 4.Registeration page

The Criminal Identification Module is the core component of the criminal detection system. It is responsible for scanning input images or live surveillance footage, detecting faces, and matching them against the registered criminal database to identify known offenders shown in fig 5.

Fig 5..Criminal Identification and Criminal Details.

VI. CONCLUSION

In conclusion, this Criminal Detection System using Face Recognition offers a powerful and efficient solution to aid law enforcement in identifying and tracking known criminals. By leveraging facial recognition technology integrated with deep learning frameworks, the system enables accurate detection and identification from both images and live surveillance footage.

This project significantly reduces manual effort in criminal identification by automating the process, ensuring faster response times and minimizing human error. The use of technologies like OpenCV and DeepFace ensures high precision, even in challenging conditions such as masked or partially occluded faces.

Furthermore, the system incorporates an authentication mechanism to ensure only authorized personnel (such as police officers) can access sensitive data. Features like criminal registration, real-time surveillance, and instant retrieval of detailed criminal records enhance its practical application in real-world scenarios.

The future scope of this project includes integration with national criminal databases, cloud-based data storage for scalable deployments, and the implementation of alert systems for real-time law enforcement response. By connecting this system to centralized police records using a secure SQL or cloud database, it can serve as a critical tool in crime prevention and public safety.

VII. REFERENCES

[1] Abdullah, M., Zahid, S., & Hussain, S. (2017). Face Recognition for Criminal Identification: An Implementation of Principal Component Analysis for Face Recognition. International Journal of Computer Applications, 164(10), 1-6.

[2] B R, K., Rani, R., & Verma, S. (2019). Crime Detection Using Face Recognition. International Journal of Engineering and Technology, 8(2), 1341-1345.

[3] Hussein, A., & Almejwal, A. (2019). Criminal Identification System (CIDS) Using Face Recognition. International Journal of Advanced Computer Science and Applications, 10(12), 109- 116.

[4] Shah, P., Lath, P., & Patel, M. (2023). Criminal Investigation with the Help of Face Recognition. International Journal of Applied Science and Engineering, 15(2), 120-126.

[5] Singh, R., Gupta, S., & Tyagi, S. (2022). Transfer Learning-Based Face Recognition for Robust Systems. IEEE Access, 10, 23111-23122.

[6] Kumar, V., Sharma, N., & Yadav, R. (2019). Face Detection Techniques: A Comprehensive Review. International Journal of Computer Applications, 178(3), 15-22.

[7] Singh, R., Verma, P., & Kumar, S. (2022). Transfer Learning for Face Recognition Using VGG16 and ResNet50. *Neural Computing and Applications*, 94, 3121-3145.

[8] Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015). Deep Face Recognition. *British Machine Vision Conference (BMVC)*, 1, 41.

[9] Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A Unified Embedding for Face Recognition and Clustering. *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 1, 815–823.