International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 03 | March - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Criminal Identification by Face Recognization System

V.Sandhiya

Guide: Prof. K. Rajeswari

Department of Computer Application, Adhiyamaan College of Engineering, Hosur.
EMAIL ID:sandhiya.mca2023@adhiyamaan.in

ABSTRACT:
The Criminal Identification by Face Recognition system is an advanced surveillance solution designed to enhance security by identifying individuals using facial recognition technology. This system automates the process of analyzing images and video feeds, comparing detected faces against a pre-trained database of known individuals. By integrating computer vision and deep learning, the system ensures accurate and real-time identification, significantly improving response times in critical security environments.
Traditional surveillance methods rely heavily on manual monitoring, making them prone to human error and inefficiencies. This system overcomes such limitations by employing automated face detection and recognition techniques. It features modules for criminal database
management, image and video surveillance, recognition and matching, and real-time alert generation. The system utilizes Haar Cascade for face detection and K-Nearest Neighbors (KNN) for matching, ensuring high accuracy. Additionally, all criminal records and datasets are securely stored in an SQLite database, allowing for efficient management and retrieval.

KEYWORD; Facial Recognition- Criminal Identification-Surveillance System-Deep Learning, Computer Vision-Real-Time Detection-Image Processing-Video Surveillance-Face Detection- Haar Cascade- K-Nearest Neighbors (KNN)-Euclidean Distance-SQLite Database- Security System,AI-Based Recognition- Pattern Matching-Dataset Management, Real-Time Alerts.
DOMAIN: Artificial Intelligence

INTRODUCTION:

- The Criminal Identification by Face Recognition system is an advanced surveillance solution that leverages artificial intelligence and computer vision to enhance security by identifying individuals through facial recognition. Traditional criminal identification methods rely heavily on manual monitoring, which is time-consuming, prone to errors, and inefficient in large-scale surveillance environments. This project aims to overcome these challenges by automating the identification process using real-time image and video analysis, ensuring faster and more accurate suspect detection.
- The system works by capturing facial images from video feeds or uploaded photographs, detecting faces using Haar Cascade algorithms, and extracting
- facial features for comparison against a pre-trained database of known individuals. It employs K-Nearest Neighbors (KNN) for matching and confidence-based scoring to minimize false positives. The system is designed to provide real-time alerts upon detecting
- With applications in law enforcement, public safety, and private security, this system enhances security operations by reducing manual effort and improving response times. By integrating artificial intelligence and real-time processing, the Criminal Identification by Face Recognition system represents a significant advancement in modern surveillance technology, contributing to a safer and more secure

environment.

match, allowing security personnel to respond promptly.

- This project incorporates various modules, including criminal database management, image and video surveillance, recognition and matching, and automated reporting. It utilizes Python, OpenCV, TensorFlow, and SQLite for database management, ensuring efficient storage and retrieval of criminal records. The web-based interface, developed using Flask, HTML, CSS, and Bootstrap, provides an intuitive platform for managing and accessing surveillance data.

OBJECTIVE:

- The primary objective of the Criminal Identification by Face Recognition system is to enhance security by automating the process of identifying individuals using facial recognition technology. The system aims to reduce reliance on manual surveillance, minimize human errors, and improve response times in critical security situations.
- This project is designed to accurately detect and recognize faces from images and video feeds, matching them against a pre-trained database of known individuals. It seeks to provide real-time alerts upon successful identification, enabling law enforcement and security personnel to take immediate action. Additionally, the system focuses on efficient criminal database management, ensuring secure storage, quick retrieval, and easy updating of records.
- Another key objective is to integrate artificial intelligence and machine learning techniques to improve the accuracy and efficiency of face detection and matching. By utilizing Haar Cascade for face detection and K-Nearest Neighbors (KNN) for classification, the system ensures high recognition accuracy with minimal false positives.
- Furthermore, the system is designed to be user-friendly and scalable, allowing for easy integration with existing security infrastructure. It aims to provide an intuitive web-based interface using Flask, HTML, CSS, and Bootstrap, ensuring seamless interaction for users. By meeting these objectives, the system contributes to enhancing public safety, supporting law enforcement efforts, and improving modern surveillance technology.
- With applications in law enforcement, public safety, and private security, this system enhances security operations by reducing manual effort and improving response times. By integrating artificial intelligence and real-time processing, the Criminal Identification by Face Recognition system represents a significant advancement in modern surveillance technology, contributing to a safer and more secure environment.

EXSISTING SYSTEM:

- The current criminal identification and surveillance systems rely heavily on manual monitoring and traditional methods of suspect identification. Security personnel are responsible for observing live CCTV footage, identifying suspicious individuals, and manually comparing captured images with existing criminal records. This process is time-consuming, inefficient, and prone to human errors, making it difficult to monitor multiple locations simultaneously. Additionally, the reliance on human observation increases the chances of missing critical incidents, leading to delays in taking necessary actions.
- Most existing systems lack automated facial recognition capabilities, requiring law enforcement agencies to manually search through databases to find potential matches. In many cases, these databases are fragmented across different departments and organizations, making cross-referencing slow and ineffective. The absence of a centralized data management system further complicates record retrieval, often resulting in duplicate or outdated profiles. Furthermore, the inability to analyze historical data and detect patterns limits the effectiveness of current surveillance operations.
- Another major drawback of traditional systems is the lack of real-time alerts and automated reporting. When a suspect is identified, officers must manually document the incident, generate reports, and communicate findings to relevant authorities, causing delays in response times. Additionally, existing systems often struggle with poor image quality, lighting variations, and occlusions, leading to frequent false positives or missed identifications.

DISADVANTAGES:

- **Manual Surveillance Dependency:** The existing system relies on human observation, making it difficult to monitor multiple locations simultaneously, increasing the risk of missing critical events.
- **Time-Consuming Identification:** Matching suspects with criminal records is a slow process, requiring manual comparison, which delays decision-making and response times.
- **High Error Rate:** Human-based identification is prone to errors, including false positives and missed detections, reducing the overall reliability of the system.
- **Lack of Real-Time Alerts:** Traditional surveillance systems do not provide instant notifications when a suspect is identified, preventing quick action by law enforcement.
- **Fragmented Databases:** Criminal records are often stored in multiple locations, leading to inconsistencies, duplication, and difficulty in retrieving complete suspect profiles.
- **Limited Search and Filtering Capabilities:** Existing systems lack intelligent search options, making it challenging to filter records based on criteria such as name, location, or crime type.

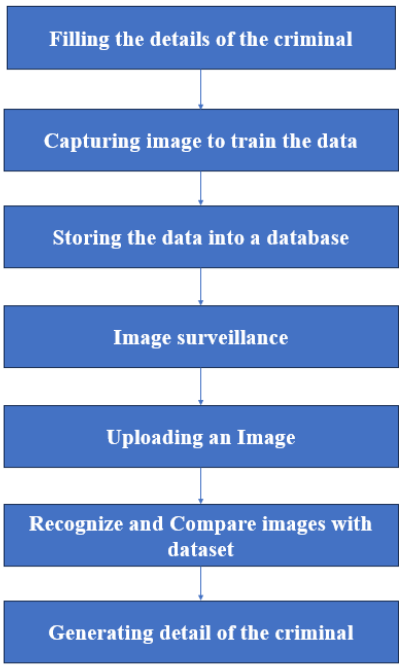
PROPOSED SYSTEM:

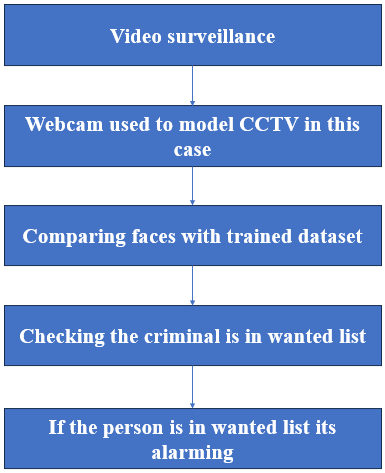
- The Criminal Identification by Face Recognition system is designed to overcome the limitations of existing surveillance and identification methods by integrating artificial intelligence, computer vision, and deep learning. This advanced system automates the process of identifying individuals from images and live video feeds, significantly reducing human dependency and improving accuracy. By leveraging facial recognition technology, the system matches detected faces with a pre-trained database, providing real-time alerts when a suspect is identified.
- The proposed system consists of multiple modules, including criminal database management, image and video surveillance, recognition and matching, and automated reporting. The Haar Cascade algorithm is used for face detection, while the K-Nearest Neighbors (KNN) classifier with Euclidean Distance is employed for accurate matching. This ensures that facial recognition operates with high precision, even under challenging conditions such as variations in lighting, camera angles, and facial expressions. The system stores all criminal records in a secure SQLite database, allowing for efficient retrieval and updating of profiles.

ADVANTAGES:

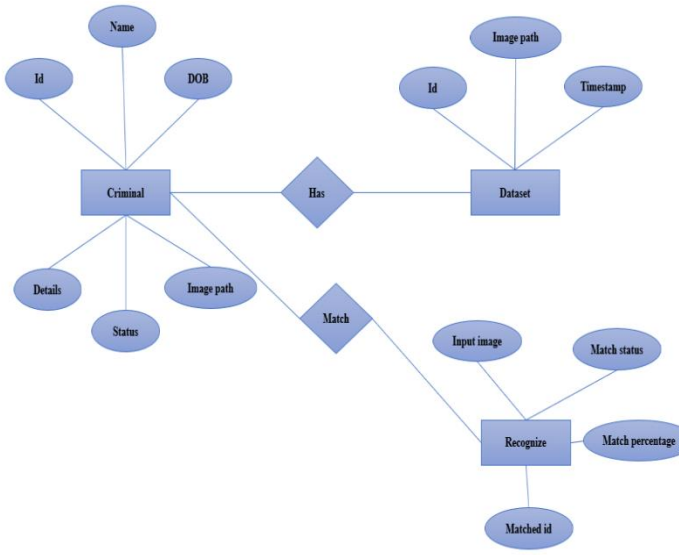
- **Automated Facial Recognition:** The system eliminates manual identification by using AI-based facial recognition, improving efficiency and accuracy.
- **Real-Time Detection and Alerts:** Authorities receive instant notifications when a match is found, enabling quick decision-making and faster response times.
- **High Accuracy in Identification:** The system employs advanced algorithms such as Haar Cascade for face detection and K-Nearest Neighbors (KNN) for matching, ensuring precise identification.
- **Reduces Human Dependency:** By automating surveillance and suspect identification, the system minimizes errors caused by human fatigue or oversight.
- **Centralized Criminal Database:** All criminal records are stored in a secure SQLite database, allowing for easy retrieval, updating, and management of profiles.
- **Efficient Image and Video Processing:** The system can analyze both uploaded images and real-time video feeds, improving surveillance efficiency.

ARCHITECTURE DIAGRAM:





ER DIAGRAM:



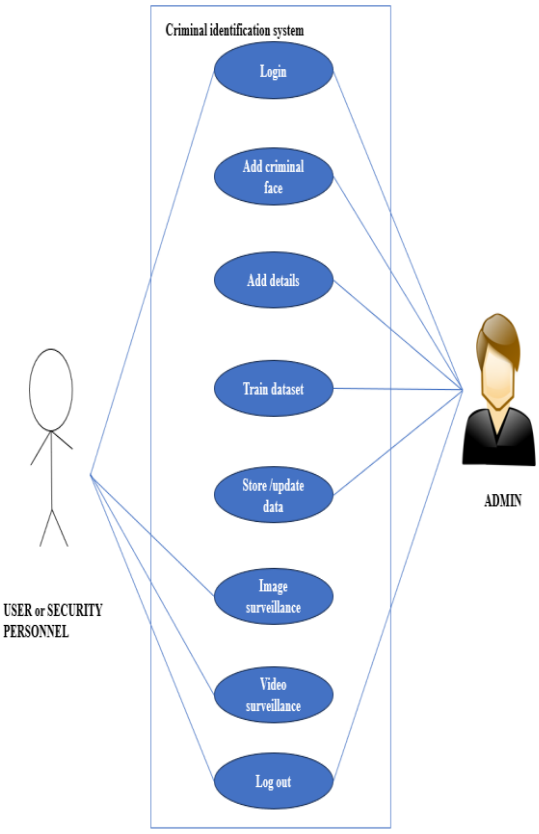
MODULE:

- Login Module
- Criminal Database Management Module
- Image Surveillance Module
- Video Surveillance Module
- Recognition and Matching Module
- Alerts and Reporting Module
- Dataset Management Module
- System Administration Module

MODULE DESCRIPTION:

- Login Module – This module ensures secure access by allowing only authorized users to log in. It verifies user credentials and prevents unauthorized access to sensitive criminal records and surveillance data. It also logs authentication activities, such as successful and failed login attempts.
- Criminal Database Management Module – This module stores and manages detailed criminal profiles, including name, age, gender, offense history, and facial images. It allows users to add, update, search, and delete records efficiently while securely storing all data in an *SQLite* database.
- Image Surveillance Module – This module processes uploaded images for facial recognition. It detects faces using the *Haar Cascade* algorithm and extracts facial features. These features are then compared with the stored dataset using *Euclidean Distance* to determine a match.
- Video Surveillance Module – This module performs real-time facial recognition from live camera feeds. It continuously captures video frames, detects faces, and matches them against a pre-trained database. If a match is found, the system generates an alert for security personnel.
- Recognition and Matching Module – This module is responsible for feature extraction and facial matching. It converts detected faces into numerical embeddings and uses *K-Nearest Neighbors (KNN)* for classification. A confidence-based threshold scoring system ensures accurate identification with minimal false positives.
- Alerts and Reporting Module – This module generates real-time notifications whenever a suspect is identified. It logs detection events, including timestamps, source (image or video), and confidence scores. Users can generate detailed reports in *PDF* or *Excel* format for further analysis.
- Dataset Management Module – This module handles the addition, updating, and removal of training datasets. It ensures high-quality dataset storage by applying preprocessing techniques such as facial alignment, contrast adjustment, and noise reduction to improve recognition accuracy.
- System Administration Module – This module allows administrators to manage user roles, configure system settings, and control access permissions. It includes security features such as encrypted data storage, account lockout for multiple failed login attempts, and backup management to ensure system reliability.

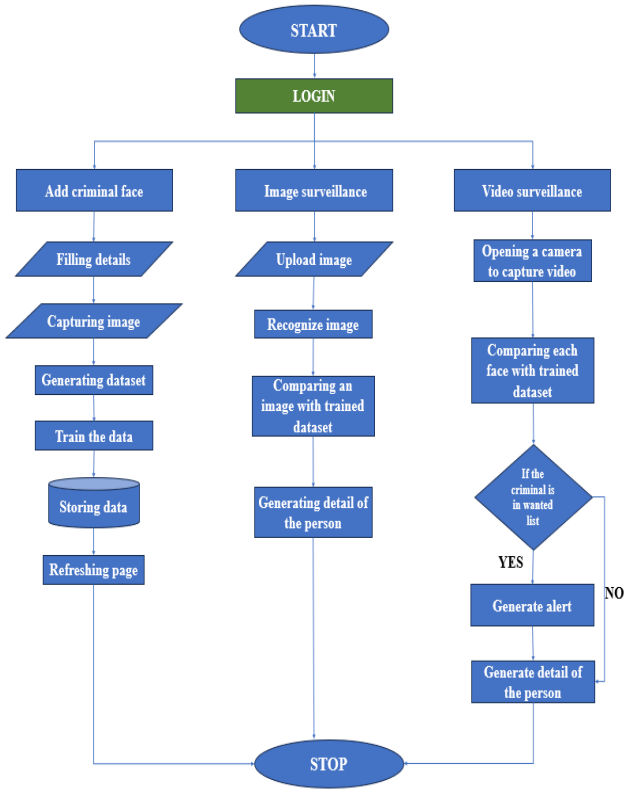
USECASE DIAGRAM:



The Criminal Identification by Face Recognition system operates through various use cases that define its core functionalities. The Login Module ensures secure access by authenticating users before they can interact with the system. Once logged in, users can access the Criminal Database Management Module, where they can add, update, search, and delete criminal records, including personal details, offense history, and facial images. The system also allows law enforcement personnel to use the Image Surveillance Module, where an image can be uploaded, and facial recognition algorithms detect and match it against stored profiles. If a match is found, an alert is generated. Similarly, the Video Surveillance Module processes live video feeds, continuously detecting and identifying faces in real time, making it highly effective for monitoring public spaces.

The Recognition and Matching Module extracts facial features from detected faces and compares them with stored data using K-Nearest Neighbors (KNN) for accurate identification. When a match is confirmed, the Alerts and Reporting Module generates real-time notifications and logs the detection event for further review. These reports can be exported in PDF or Excel formats, aiding investigations. Additionally, the Dataset Management Module ensures that the system maintains high-quality training data by allowing administrators to update and refine facial datasets. The System Administration Module gives administrators control over user roles, access permissions, and system settings, ensuring secure data management. These interconnected use cases make the system highly efficient in automating criminal identification, reducing human effort, and improving real-time security surveillance.

DATAFLOW DIAGRAM:



ALGORITHMS AND TECHNIQUES

1.Face Detection – Haar Cascade Algorithm

Detects faces in images and video using pre-trained filters.

Works efficiently for real-time face detection.

2.Feature Extraction – Face Embeddings

Converts facial features into numerical values (embeddings) for accurate recognition.

Helps in comparing faces even with different lighting and angles.

3.Face Recognition – K-Nearest Neighbors (KNN) Algorithm

Compares the detected face with stored faces in the database.

Uses Euclidean Distance to find the closest match.

4.Matching Logic – Confidence Score

Sets a threshold to decide if a match is accurate.

Reduces false matches and improves recognition accuracy.

5.Real-Time Processing – OpenCV and Deep Learning

Uses OpenCV for handling images and videos.

TensorFlow/PyTorch helps in deep learning-based face recognition.

6.Database Management – SQLite

Stores criminal records and facial features securely.

Enables quick searching and matching of suspects.

7.Web Interface – Flask Framework

Provides an easy-to-use interface for uploading images and checking matches.

Uses HTML, CSS, and Bootstrap for a simple and responsive design.

CONCLUSION:

The Criminal Identification by Face Recognition system is an advanced solution that enhances security and law enforcement by automating the process of identifying individuals through facial recognition technology. By integrating artificial intelligence, computer vision, and deep learning, the system improves the accuracy, efficiency, and speed of criminal identification. Unlike traditional surveillance methods, which rely on manual observation and are prone to errors, this system provides real-time facial recognition, instant alerts, and automated report generation, reducing human effort and increasing response times.

The system effectively detects, recognizes, and matches faces from images and live video feeds using algorithms such as Haar Cascade, K-Nearest Neighbors (KNN), and Euclidean Distance for accurate classification. It ensures secure storage and retrieval of criminal records using an SQLite database, making data management more efficient. Additionally, the user-friendly web interface, built with Flask, HTML, CSS, and Bootstrap, allows for easy access and monitoring of surveillance data.

With applications in law enforcement, public safety, and private security, this system significantly improves the process of criminal identification. Its ability to operate in real-time, handle multiple camera feeds, and minimize false positives makes it a reliable and scalable solution for modern security challenges. By automating suspect detection and reducing manual intervention, the Criminal Identification by Face Recognition system represents a major step forward in modern surveillance, making communities safer and improving investigative capabilities.

RESULT:

- The *Criminal Identification by Face Recognition* system successfully detects, recognizes, and matches faces against a pre-trained database with high accuracy. The system efficiently processes both images and real-time video feeds, identifying individuals using facial recognition algorithms. When a match is found, real-time alerts are generated, allowing law enforcement or security personnel to take immediate action.
- The use of Haar Cascade for face detection and K-Nearest Neighbors (KNN) for matching ensures precise identification while minimizing false positives. The system also stores criminal records securely in an SQLite database, enabling quick data retrieval and seamless record management. The web-based interface, developed using Flask, HTML, CSS, and Bootstrap, provides a user-friendly platform for managing surveillance data, making the system easy to use and accessible.
- The implementation of automated facial recognition has led to faster identification, improved security monitoring, and reduced manual workload for law enforcement agencies. The system's ability to analyze large datasets, process live video feeds, and generate instant reports makes it a highly efficient and

scalable solution for criminal identification. This project demonstrates the effectiveness of AI-driven facial recognition in enhancing surveillance and improving public safety.

LITERATURE SURVEY:

Facial recognition technology has been widely studied and developed for security, law enforcement, and surveillance. Earlier methods, such as Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA), were used to extract facial features, but they struggled with changes in lighting, facial expressions, and angles, making them less effective in real-world situations (Turk & Pentland, 1991).

The introduction of Haar Cascade Classifiers by Viola and Jones (2001) improved face detection by using a fast and efficient method to locate faces in images and videos. However, this method sometimes produced inaccurate results due to background noise and poor image quality. Later, machine learning models like Support Vector Machines (SVM) and K-Nearest Neighbors (KNN) were used to improve recognition accuracy.

REFERENCE:

1. Turk, M., & Pentland, A. (1991). Eigenfaces for recognition. *Journal of Cognitive Neuroscience, 3*(1), 71–86.
2. Viola, P., & Jones, M. (2001). Rapid object detection using a boosted cascade of simple features. *Proceedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 511–518.
3. Taigman, Y., Yang, M., Ranzato, M., & Wolf, L. (2014). DeepFace: Closing the gap to human-level performance in face verification. *Proceedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 1701–1708.
4. Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A unified embedding for face recognition and clustering. *Proceedings of IEEE Conference on Computer Vision and* Pattern Recognition (CVPR), 815–823.
5. Dlib Library. (2017). Dlib: A toolkit for making real-world machine learning and data analysis applications. Retrieved from http://dlib.net
6. OpenCV Library. (2023). Open Source Computer Vision Library. Retrieved from https://opencv.org