CRIMDETECT : AN AI-POWERED CRIMINAL FACE DETECTION AND IDENTIFICATION SYSTEM USING MACHINE LEARNING

Divanshu Baghel[1], Mohammad Talib[2], Nitesh Soni[3], Er. Gaurav Singh[4]

1+3 UG Students, Department of Computer Science & Engineering

4 Assistant Professor, Department of Computer Science & Engineering

Raja Balwant Singh Engineering Technical Campus, Agra, India

***Abstract*—**The rapid expansion of digital surveillance systems has increased the need for intelligent platforms that enhance criminal identification and public safety operations. This paper presents **CrimDetect**, an AI-enabled criminal face detection and recognition system developed using a Java-based architecture integrated with machine learning and computer vision techniques. The system features automated face detection from both images and video streams, along with a recognition module for accurate suspect identification. Additionally, it includes a structured criminal record management system to ensure secure and efficient data handling. Optimized machine learning models are utilized to achieve scalability and real-time performance. The proposed system improves identification accuracy, minimizes manual verification efforts, and facilitates faster decision-making in modern law enforcement environments.

Keywords— Artificial Intelligence, Criminal Face Detection, Machine Learning, Face Recognition, Computer Vision, Surveillance Systems, Java Framework.

INTRODUCTION

Modern law enforcement has transitioned from manual record-keeping and human-based identification methods to intelligent digital surveillance systems capable of automated monitoring and rapid suspect recognition. The integration of Artificial Intelligence (AI) enables real-time image processing, automated face detection, and accurate identity verification, thereby significantly enhancing public safety operations and reducing human effort.

CrimDetect is an integrated AI-based criminal face detection and identification platform that combines image processing, facial recognition, and database management within a unified and scalable system architecture. Unlike computationally intensive deep learning frameworks, the proposed system emphasizes efficient and optimized machine learning models, making it suitable for real-world deployment in resource-constrained surveillance environments.

LITERATURE REVIEW

Recent research highlights the increasing application of Artificial Intelligence in law enforcement and surveillance systems. Viola and Jones [1] introduced a real-time face detection framework using Haar-like features, which became foundational for early detection systems. Turk and Pentland [2] proposed the Eigenfaces method for face recognition, demonstrating the effectiveness of appearance-based techniques. Taigman et al. [3] presented deep learning-based face recognition models that significantly improved identification accuracy using convolutional neural networks. Schroff et al. [4] developed FaceNet, which introduced face embedding techniques for high-precision matching.

Although existing studies report high accuracy in controlled environments, many systems function as standalone recognition models and lack integration within scalable, real-time criminal database and surveillance infrastructures.

COMPARISON OF SELECTED AI-BASED CRIMINAL FACE DETECTION SYSTEMS

Ref	Methodology	Key Contribution	Identified Limitation
[1]	Haar Cascade (Viola-Jones)	Real-time face detection framework	Limited accuracy in complex backgrounds
[2]	Eigenfaces (PCA)	Early face recognition approach	Sensitive to lighting and pose variations
[3]	CNN-based Deep Learning	High-accuracy large-scale face recognition	High computational cost
[4]	FaceNet (Deep Learning)	Face embedding for precise matching	Requires large training datasets
[5]	SVM-based Classification	Efficient facial feature classification	Limited performance in large databases
[6]	KNN Recognition Model	Simple and interpretable classification	Slow for large-scale real-time systems
[7]	DL Surveillance Systems	Automated large-scale monitoring	Privacy and ethical concerns
[8]	ML-based Identification Systems	Improved suspect identification accuracy	Lack of unified system integration
[9]	CNN in Security Applications	High detection accuracy in controlled environments	Dataset bias and generalization issues
[10]	Hybrid ML + CV Models	Combined detection and recognition techniques	Limited real-time deployment

Research Gap

Despite significant advancements in AI-based surveillance and face recognition technologies, several limitations still exist in current systems:

1. Lack of integrated face detection and criminal database systems
2. Limited scalability in real-time surveillance environments
3. Low explainability of machine learning models
4. Data privacy and ethical concerns
5. Limited interoperability with existing law enforcement systems

These challenges highlight the need for an integrated, secure, and scalable criminal face detection platform such as CrimDetect.

PROPOSED SYSTEM

The proposed system integrates AI-based face detection and recognition within a scalable platform for criminal identification and surveillance. It supports real-time processing, high accuracy, and secure data management.

The system includes the following components:

A. Face Detection Module – Detects faces from images and video streams.

B. Face Recognition Module – Identifies individuals using machine learning techniques.

C. Criminal Database – Stores and manages criminal records.

D. Secure Storage – Ensures data protection and integrity.

E. Role-Based Access Control – Restricts access based on user roles.

The unified architecture ensures efficient, secure, and scalable system performance.

SYSTEM ARCHITECTURE

The proposed system follows a modular and layered architecture that integrates face detection, feature extraction, recognition, and database management into a unified processing pipeline. The system accepts input from images or real-time video streams, processes facial data, and performs identification by matching it with stored criminal records.

The architecture is composed of the following layers:

A. Input Layer – Acquires images or live video streams from surveillance sources.

B. Face Detection Layer – Detects and localizes human faces using optimized computer vision algorithms.

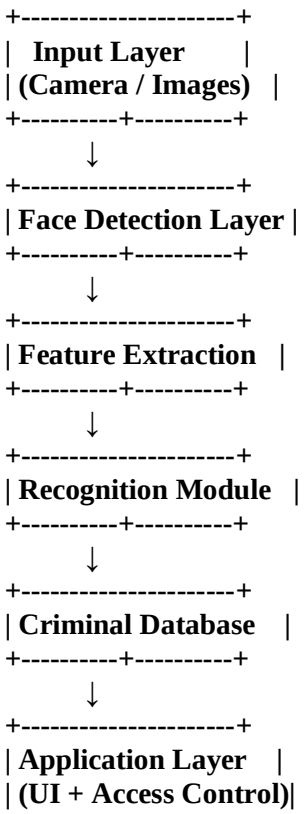
C. Feature Extraction Layer – Extracts distinctive facial features required for accurate recognition.

D. Recognition Layer – Compares extracted features with stored data to identify individuals.

E. Database Layer – Maintains structured criminal records for efficient storage and retrieval.

F. Application Layer – Provides a user interface with role-based access control for authorized users.

This layered architecture ensures real-time performance, high accuracy, scalability, and secure management of sensitive criminal data.



SYSTEM WORKFLOW

The system workflow describes the step-by-step process of criminal face detection and identification. The system operates in a sequential manner to ensure accurate and real-time processing.

The workflow is as follows:

Step 1: Input Acquisition

The system captures input in the form of images or live video streams from surveillance cameras.

Step 2: Face Detection

Detected input is processed using computer vision techniques to locate human faces.

Step 3: Preprocessing

The detected faces are normalized, resized, and enhanced to improve recognition accuracy.

Step 4: Feature Extraction

Distinct facial features are extracted using machine learning algorithms.

Step 5: Face Recognition

Extracted features are compared with stored records in the database to identify the individual.

Step 6: Database Matching

The system retrieves matching criminal data if a match is found.

Step 7: Output Generation

The result is displayed to the user along with relevant details, and alerts may be generated if required.

Input (Image/Video)
↓
Face Detection
↓
Preprocessing
↓
Feature Extraction
↓
Face Recognition
↓
Database Matching
↓
Output (Result/Alert)

CHALLENGES AND FEATURES

A. Challenges

The development of the proposed system involves several technical challenges:

- **Variations in Lighting Conditions** – Changes in illumination can affect face detection and recognition accuracy.
- **Pose and Expression Variability** – Differences in facial angles and expressions reduce matching precision.
- **Real-Time Processing Constraints** – Ensuring fast processing with limited computational resources.
- **Large-Scale Data Handling** – Managing and retrieving records efficiently from large criminal databases.
- **Security and Privacy Concerns** – Protecting sensitive data from unauthorized access and misuse.

B. Features

The proposed system offers the following key features:

- **Automated Face Detection** – Detects faces from images and live video streams.
- **Accurate Face Recognition** – Uses optimized machine learning models for identification.
- **Real-Time Processing** – Enables quick detection and decision-making.
- **Scalable Architecture** – Supports expansion for large datasets and multiple users.
- **Secure Data Management** – Ensures data integrity and confidentiality.
- **Role-Based Access Control** – Restricts system access based on user roles.

CONCLUSION

The proposed system, **CrimDetect**, presents an efficient and scalable solution for criminal face detection and identification using Artificial Intelligence and computer vision techniques. By integrating face detection, recognition, and secure database management into a unified architecture, the system enhances identification accuracy and reduces manual effort in surveillance operations.

The implementation focuses on optimized machine learning models, enabling real-time performance even in resource-constrained environments. Additionally, features such as secure data storage and role-based access control ensure the reliability and safety of sensitive information.

Overall, the system contributes to improved decision-making and supports modern law enforcement agencies in maintaining public safety through intelligent and automated surveillance.

References

[1] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features,"in Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR), 2001.

[2] M. Turk and A. Pentland, "Eigenfaces for recognition," Journal of Cognitive Neuroscience, vol. 3, no. 1, pp. 71–86, 1991.

[3] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "DeepFace: Closing the gap to human-level performance in face verification,"
in Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR), 2014.

[4] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering,"
in Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR), 2015.
[5] R. Lienhart and J. Maydt, "An extended set of Haar-like features for rapid object detection,"
in Proc. IEEE Int. Conf. Image Processing (ICIP), 2002.

[6] G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, "Labeled Faces in the Wild: A database for studying face recognition in unconstrained environments," Univ. of Massachusetts, Amherst, Tech. Rep., 2007.

[7] I. Goodfellow, Y. Bengio, and A. Courville,"Deep Learning," MIT Press, 2016.

[8] O. M. Parkhi, A. Vedaldi, and A. Zisserman,"Deep face recognition," in Proc. British Machine Vision Conf. (BMVC), 2015.

[9] D. King, "Dlib-ml: A machine learning toolkit," Journal of Machine Learning Research, vol. 10, pp. 1755–1758, 2009.

[10] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks,"
in Proc. Advances in Neural Information Processing Systems (NIPS), 2012.