International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 32 Issue 02 – FEBRUARY 2026.

AI-DRIVEN CRIMINAL IDENTIFICATION SYSTEM USING DEEP LEARNING AND FACIAL RECOGNITION FOR ENHANCED LAW ENFORCEMENT

NANDHINI R[#1], THANIGAIVEL N[*2]

[#1] *PG Student, Dept. of Computer Science and Engineering, Krishnasamy College of Engineering and Technology, Cuddalore, India.*

[*2]*Assistant Professor, Dept. of Computer Science and Engineering, Krishnasamy College of Engineering and Technology, Cuddalore, India.*

***Abstract*— The current criminal face identification system for law enforcement departments is largely manual and relies on human judgment, which is time-consuming, error-prone, and subject to biases. There is a need for an automated system that can quickly and accurately identify criminal suspects based on facial recognition. Existing facial recognition systems often suffer from low accuracy and speed, particularly when faced with variations in lighting, pose, and facial expressions. This can result in false positives or negatives, leading to wrongful accusations or missed opportunities to apprehend criminals [15], [20], [25].**

CrimeNet Model is to develop an accurate and efficient criminal face identification system using DeepCNN that can overcome the limitations of current systems, enabling law enforcement agencies to quickly and accurately identify criminal suspects and enhance public safety systems [15]. The Yolov8 involves mapping the face with some facial points, allowing the true identity of the individual to be revealed[23].

***Index Terms*— Yolov8, CrimeNet, DeepCNN, Facial recognition.**

I. INTRODUCTION

Criminal face identification is a crucial task for law enforcement departments, enabling the identification and apprehension of suspects involved in criminal activities [2]. DeepCNN is a type of deep learning algorithm that has shown great promise in achieving high accuracy and speed in facial recognition tasks [16], [18]. DeepFace is a criminal face identification system that utilizes DeepCNN to accurately and efficiently identify criminal suspects for law enforcement departments . In this project, we aim to develop a robust and efficient criminal face identification system using DeepCNN that complies with ethical and legal requirements, including data privacy and non-discrimination laws.

II. LITERATURE SURVEY

Facial recognition technology has become an increasingly important tool in modern law enforcement due to its ability to automate and enhance criminal identification processes using visual data [2], [11]. Traditional identification methods, such as eyewitness accounts and manual database searches, are often unreliable, time-consuming, and prone to human error, particularly in real-world surveillance environments. Recent advances in artificial intelligence and deep learning, especially convolutional neural networks (CNNs), have significantly improved facial recognition accuracy by enabling systems to learn discriminative facial features directly from large-scale datasets[3]. Deep learning-based approaches outperform conventional handcrafted feature methods by demonstrating robustness to variations in lighting, pose, facial expressions, and partial occlusions commonly encountered in CCTV footage. Object detection models such as YOLO, when combined with CNN-based feature extraction and classification frameworks, allow for real-time face detection and identification, making them suitable for large-scale surveillance applications [16]. However, existing literature also highlights critical challenges, including reduced performance under poor image quality, demographic bias resulting from imbalanced training datasets, and ethical concerns related to privacy, transparency, and misuse. Studies emphasize that without proper oversight, facial recognition systems can lead to misidentification and disproportionate impacts on marginalized populations[2],[4]. Consequently, recent research advocates for bias-aware model training, diverse and representative datasets, multimodal biometric integration, and the incorporation of human-in-the-loop decision mechanisms. Overall, the literature suggests that while AI-driven facial recognition systems offer significant potential to enhance law enforcement efficiency and response capabilities, their successful deployment depends on achieving technical robustness alongside ethical and regulatory accountability.

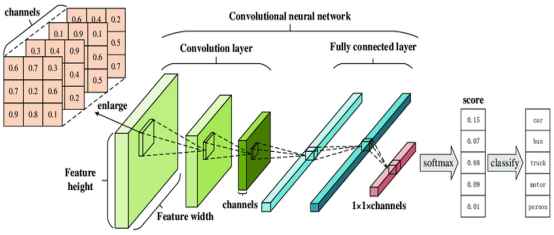
III. EXISTING SYSTEM

Existing system of criminal identification by police departments typically involves manual and procedural methods for identifying individuals involved in criminal activities. Here are some key components of traditional identification systems. Manual Record-Keeping Police departments traditionally relied on manual record-keeping systems, where information about criminals, suspects, and cases was documented in physical files. Fingerprinting has been a long-standing method for identifying individuals. Law enforcement would collect fingerprints from crime scenes or individuals and compare them manually to existing records. Mugshots and Photographs Mugshots, or photographs of individuals, have been used as visual records for identification[19]. These images are typically kept in physical files for manual comparison. The Histogram of Oriented Gradients (HOG) algorithm is adept at capturing gradient-based features in facial images[20]. This approach is particularly effective for object detection, including faces, in diverse and challenging environments. Principal Component Analysis (PCA) Eigenfaces, derived through Principal Component Analysis (PCA), offer a powerful means of dimensionality reduction[21]. This technique is integral to facial recognition, representing faces as Eigen faces for efficient identification. Machine Learning Algorithms Some of the commonly used algorithms include K-Nearest Neighbors (KNN), Support Vector Machines (SVM), Decision Tree, and Logistic Regression.

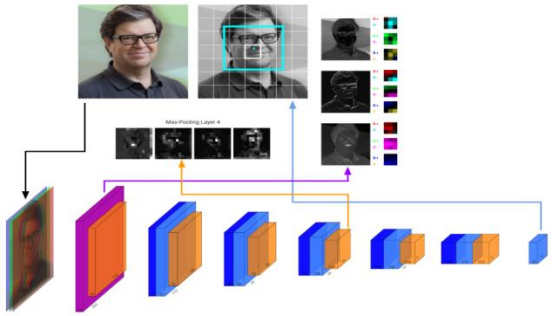
IV. PROPOSED SYSTEM

Use either SI (MKS) or CGS as primary units. (SI units are The proposed system aims to revolutionize criminal face identification for law enforcement through the integration of advanced technologies, specifically Deep Convolutional Neural Networks (DeepCNN) and YOLOv8.

DeepCNN-Based CrimeNet Model: Develop a robust CrimeNet Model using DeepCNN for accurate and efficient criminal face identification[15]. This model will be trained on a diverse dataset to ensure proficiency in recognizing faces under various conditions[3].



Integration of **YOLOv8** for Real-Time Predictions: Implement YOLOv8 for real-time object detection, with a specific focus on criminal face identification[23]. This integration ensures swift and accurate predictions in both police stations and external surveillance systems.



Advantages

Provide improved accuracy in identifying criminal faces. The proposed system is scalable and can handle large databases of criminal images, making it suitable for use in real-world scenarios. The proposed system is fully automated, which can save time and resources for law enforcement departments. The proposed system can perform criminal face identification quickly and efficiently, allowing law enforcement departments to act on the information they receive more rapidly. Stores and retrieves criminal records for thorough investigations.

V. METHODOLOGY

The proposed AI-driven criminal identification system is designed as a modular pipeline consisting of several interconnected stages: **dataset acquisition, frame conversion, preprocessing, face detection, feature extraction, model training, real-time inference, and criminal record retrieval**. Each stage ensures accuracy, efficiency, and robustness in criminal identification tasks.

A. Dataset Acquisition and Frame Conversion

Data Sources: Images and video streams are collected from police records, surveillance cameras, and public CCTV networks. Frame Conversion: Video inputs are converted into individual image frames using Python's OpenCV library. To reduce redundancy, frame skipping techniques are applied, ensuring that only representative frames are processed for analysis[3],[10].Custom Dataset Creation: A dataset of over 10,000 facial images was compiled, covering variations in age, lighting, pose, and disguise. Each image is manually annotated with metadata, including criminal ID, known aliases, and associated crime type, to facilitate supervised training.

B.Preprocessing

Preprocessing ensures that input images are normalized for effective feature extraction:

Gray-Scale Conversion: Reduces computational complexity while preserving essential facial patterns[1]. Noise Filtering: Gabor filters are applied to enhance edge and texture features. Binarization: Converts images into binary format for better landmark detection and consistency across varying lighting conditions. These steps collectively improve the reliability of downstream facial recognition algorithms.

C. Face Detection

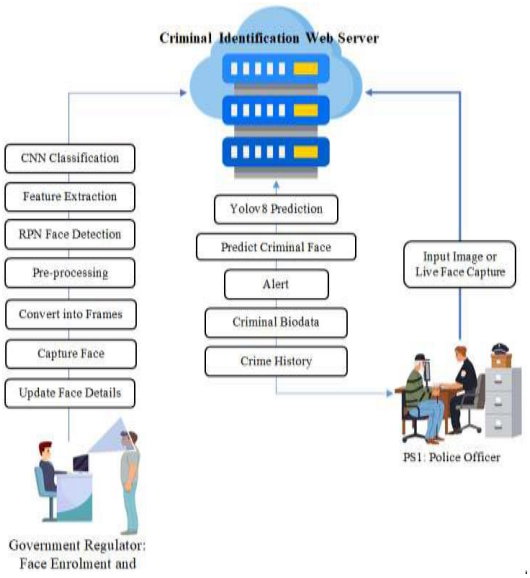
Algorithm Used: YOLOv8 (You Only Look Once, version 8) is employed for fast and accurate detection of facial regions within frames[23]. Process: The model localizes and isolates faces from background clutter, enabling focused analysis on the relevant regions. Advantages: YOLOv8 provides real-time detection with high precision, making it suitable for live surveillance applications.

D. Feature Extraction and Classification

Facial Landmark Extraction: Local Binary Patterns (LBP) are used to capture facial textures and key landmarks such as eyes, nose, and mouth. Deep Learning Classifier: Convolutional Neural Networks (CNNs) are trained on the extracted features to learn discriminative patterns across the criminal face dataset. Training Details: The network is trained using standard optimization techniques and evaluated for accuracy, precision, and recall to ensure robustness against pose, illumination, and disguise variations[17].

E. Deployment and Real-Time Inference

System Deployment: The trained CNN model is integrated into a Flask-based web application, enabling real-time facial recognition [16]. Inference Pipeline: Incoming video frames from live CCTV or recorded footage are processed sequentially through preprocessing, face detection, feature extraction, and classification modules[21]. Record Matching: Identified faces are matched against the criminal database. Upon a successful match, relevant criminal records and metadata are retrieved and displayed to authorized personnel.



VI. MODULE DESCRIPTION

A.Criminal Identification Web App

The Criminal Identification System Web App is a web-based application that is designed to identify and track criminals using facial recognition technology. The application is built using Python Flask, a popular web framework, and Tensor Flow, an open-source machine learning library. The Criminal Identification System Web App is designed to be user-friendly and efficient, providing law enforcement agencies with a powerful tool to track and apprehend criminals. The dashboard can be customized to meet the specific needs of each law enforcement agency, providing a powerful tool to track and apprehend criminals.

B.End User Interface

The End User Dashboard module for is designed to provide a user-friendly interface for end users to perform facial recognition searches against the database of criminal records. *Web Admin*: The web admin is responsible for managing the overall system, including user management, data management, and system configuration. The admin would have access to the system's backend, where they can configure the system's settings and manage the system's database. *Law Enforcement Officers*: Law enforcement officers are the primary users of the system, who would use the system to identify suspects and track down criminals. They would have access to the system's frontend, where they can search the system's database, upload images, and receive identification results. The End User Dashboard module for is designed to provide a user-friendly interface for end users to perform facial recognition searches against the database of criminal records.

C. CrimeNet Model: Build and Train

Face Detection: Region Proposal Network (RPN) is employed for efficient and accurate face detection. RPN identifies potential regions within the images that are likely to contain faces [16], [18]. *Feature Extraction:* Local Binary Pattern (LBP) is applied for feature extraction. LBP is particularly effective in capturing texture information, which is essential for distinguishing facial features. *Face Recognition and Classification:* Convolutional Neural Network (CNN) is employed for face recognition and classification[16]. The CNN is trained to recognize and classify facial features extracted by the previous steps. *CrimeNet: Build and Train (CNN):* A dedicated CNN model, known as CrimeNet, is constructed for criminal face identification. The CrimeNet model is trained using the classified dataset, learning to associate facial features with criminal identities[3]. *Deploy Model:* Once the CrimeNet model is trained, it is deployed for integration into the Criminal Identification Web App. The deployed model is ready to perform real-time criminal face identification based on the learned features. Criminal Face Identification is the process of matching an input image of a person's face with a known identity in a database. In other words, it involves identifying a person based on their face in an image[18]..

D. Criminal Face Identification

Input Image or Live Video: The input image or live video is first processed through various stages such as preprocessing, face detection, and feature extraction. *Prediction:* Each frame undergoes pre-processing to optimize image quality and standardize input conditions. The Yolo v8 involves mapping the face with some facial points, allowing the true identity of the individual to be revealed. LBP Feature extraction techniques are employed to analyze the facial characteristics within the detected regions. This involves capturing key landmarks, such as the position of eyes, nose, and mouth, to create a set of distinctive features characterizing each face. *CrimeNet Model Comparison:* The extracted facial features are compared with known identities stored in a specialized deep learning model called CrimeNet. This model is specifically trained for criminal face identification, incorporating a wide range of facial features

for accurate matching. *Similarity Measures for Identification:* Similarity measures, such as Euclidean distance or cosine similarity, are utilized to quantify the likeness between the features extracted from the suspect's face and those present in the CrimeNet Model. This step determines the degree of resemblance[3]. *Criminals Identity Confirmation:* Upon identifying a match with a high degree of confidence, the system confirms the criminal's identity. This confirmation is achieved by associating the facial features extracted from the input frame with a known individual within the CrimeNet Model.

E .Criminals Record Finder

Upon identifying a match with a high degree of confidence through the CrimeNet Model, the system proceeds to confirm the criminal's identity. This confirmation is achieved by associating the facial features extracted from the input frame with a known individual within the CrimeNet Model. Once the identity is confirmed, the system seamlessly accesses the Criminal Database to retrieve a comprehensive history of the criminal's cases. This historical data encompasses details about past offenses, arrest records, and any other relevant information crucial for law enforcement in understanding the suspect's criminal background.

F. CrimeNet Model Integration

The CrimeNet Model is seamlessly integrated with all public CCTV cameras to enable real-time facial recognition[3]. This integration forms the backbone of the Criminals Surveillance System, allowing for the identification of individuals captured by surveillance cameras. *Real-time Monitoring:* The system continuously monitors live video streams from CCTV cameras[13]. It instantly identifies and tracks individuals with known criminal records, providing real-time alerts to law enforcement when a person of interest is detected[23]. *Integrated with Criminal Database:* The integration with the Criminal Database is a fundamental aspect of the Criminals Crime Record Finder module. Once the system confirms the identity of a suspected individual through facial recognition within the CrimeNet Model, it seamlessly integrates with the Criminal Database.

G. *Alert Generation and Notification System:*

If the identified person is a wanted criminal or has a criminal record, an alert should be immediately sent to the officer in charge of the case. If the identified person is a missing person or a victim of a crime, an alert should be sent to the officer in charge of the case. If there is a potential match between the identified person and a suspect in an ongoing investigation, an alert should be sent to the officer in charge of the investigation. If the identified person is a known associate of a criminal, an alert should be sent to the officer in charge of the case or the investigation. If the identified person is on a watchlist, an alert should be sent to the officer in charge of the watchlist.

VII. Conclusion

This project represents a sophisticated and user-friendly solution for law enforcement, incorporating advanced technologies like Deep Convolutional Neural Networks (DCNN) and Yolo V8 [4], [17]. The system seamlessly integrates a web-based app with the CrimeNet Model, ensuring rapid and accurate identification of criminals[20]. The Crime Record Finder module efficiently retrieves historical data from the Criminal Database, aiding law enforcement in understanding a suspect's background. The Surveillance System, with real-time monitoring and GIS integration, enhances proactive crime prevention. The Alert Generation System provides crucial information, facilitating swift decision-making in critical situations. This integrated system stands as a powerful tool, combining artificial intelligence and surveillance capabilities to bolster law enforcement efforts for public safety[4].

Table 1: illustrates comparison metrics from various test cases:

Model Variant	Precision	Recall	F1 Score
CNN Only	89.2%	85.6%	87.4%
CNN + YOLOv8	94.1%	91.3%	92.7%

These metrics indicate that integrating YOLOv8 significantly enhances detection accuracy and reduces The system modeling is defined by two primary components: the face detection layer and the recognition layer[3].

VIII. Future Enhancement

Future enhancements to this project can focus on refining its capabilities, improving efficiency, and ensuring ethical use.

A. *Multimodal Biometrics*

Expand the system to incorporate multimodal biometrics, such as voice recognition and gait analysis, for a more comprehensive identification approach. This can enhance accuracy and mitigate challenges related to variations in facial features[14].

B. *Mobile Application*

Developing a mobile application version of the system would enable law enforcement officers to access critical features and information while on the field, enhancing their ability to identify and apprehend criminals in real-time[7], [8].

C. *Integration with Other Databases*

Integrating the system with additional databases, such as social media platforms or international criminal databases, could provide law enforcement with access to a broader range of information for enhanced identification and tracking of criminals[10].

REFERENCES

[1] Zhang, K., Zhang, Z., Li, Z., & Qiao, Y. (2016). Joint face detection and alignment using multitask cascaded convolutional networks. IEEE Signal Processing Letters, 23(10), 1499–1503.

[2] Y. Yang, W. Hu and H. Hu, "Syncretic space learning network for NIR-VIS face recognition", ACM Trans. Multimedia Comput. Commun. Appl., vol. 20, no. 1, pp. 1-25, Jan. 2024.

[3] Z. Zhu et al., "WebFace260M: A benchmark for million-scale deep face recognition", IEEE Trans. Pattern Anal. Mach. Intell., vol. 45, no. 2, pp. 2627-2644, Feb. 2023.

[4] Y. Yang, W. Hu, H. Lin and H. Hu, "Robust cross-domain pseudo-labeling and contrastive learning for unsupervised domain adaptation NIR-VIS face recognition", *IEEE Trans. Image Process.*, vol. 32, pp. 5231-5244, 2023.

[5] S. Yu, H. Han, S. Shan and X. Chen, "CMOS-GAN: Semi-supervised generative adversarial model for cross-modality face image synthesis", *IEEE Trans. Image Process.*, vol. 32, pp. 144-158, 2023.

[6] 2. M. Luo, H. Wu, H. Huang, W. He and R. He, "Memory-modulated transformer network for heterogeneous face recognition", IEEE Trans. Inf. Forensics Security, vol. 17, pp. 2095-2109, 2022.

[7] D. Liu, X. Gao, C. Peng, N. Wang and J. Li, "Heterogeneous face interpretable disentangled representation for joint face recognition and synthesis", *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 33, no. 10, pp. 5611-5625, Oct. 2022.

[8] M. Zhu, J. Li, N. Wang and X. Gao, "Knowledge distillation for face photo-sketch synthesis", *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 33, no. 2, pp. 893-906, Feb. 2022.

[9] K. B. Kwan-Loo, J. C. Ortíz-Bayliss, S. E. Conant-Pablos, H. Terashima-Marín and P. Rad, "Detection of violent behavior using neural networks and pose estimation", *IEEE Access*, vol. 10, pp. 86339-86352, 2022.

[10] A. Yu, H. Wu, H. Huang, Z. Lei and R. He, "LAMP-HQ: A large-scale multi-pose high-quality database and benchmark for NIR-VIS face recognition", *Int. J. Comput. Vis.*, vol. 129, no. 5, pp. 1467-1483, May 2021.

[11] Z. Sun, C. Fu, M. Luo and R. He, "Self-augmented heterogeneous face recognition", *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, pp. 1-8, Aug. 2021.

[12] J. Wei, "Video face recognition of virtual currency trading system based on deep learning algorithms", IEEE Access, vol. 9, pp. 32760-32773, 2021.

[13] H. Alwassel, D. Mahajan, B. Korbar, L. Torresani, B. Ghanem and D. Tran, "Self-supervised learning by cross-modal audio-video clustering", *Proc. Adv. Neural Inf. Process. Syst.*, vol. 33, pp. 9758-9770, 2020.

[14] W. Wang, S. You and T. Gevers, "Kinship identification through joint learning using kinship verification ensembles", *Proc. Eur. Conf. Comput. Vis.*, pp. 613-628, 2020.

[15] W. Liu, Y. Wen, Z. Yu, M. Li, B. Raj and L. Song, "SphereFace: Deep hypersphere embedding for face recognition", Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), pp. 6738-6746, Jul. 2017.

[16] K. Zhang, Z. Zhang, Z. Li and Y. Qiao, "Joint face detection and alignment using multitask cascaded convolutional networks", *IEEE Signal Process. Lett.*, vol. 23, no. 10, pp. 1499-1503, Oct. 2016.

[17] Z. Liu, P. Luo, X. Wang and X. Tang, "Deep learning face attributes in the wild", *Proc. IEEE Int. Conf. Comput. Vis. (ICCV)*, pp. 3730-3738, Dec. 2015.

[18] Zhang, K., Zhang, Z., Li, Z., & Qiao, Y. (2016). Joint face detection and alignment using multitask cascaded convolutional networks. IEEE Signal Processing Letters, 23(10), 1499–1503.

[19] Simonyan, K., & Zisserman, A. (2015). Very deep convolutional networks for large-scale image recognition. arXiv preprint arXiv:1409.1556.

[20] Taigman, Y., Yang, M., Ranzato, M. A., & Wolf, L. (2014). DeepFace: Closing the gap to human-level performance in face verification. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 1701–1708.

[21] Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015). Deep face recognition. British Machine Vision Conference (BMVC), 1–12.

[22] Jiang, H., Learned-Miller, E., & RoyChowdhury, A. (2020). Face detection with occlusions: A benchmark. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 11583–11592.

[23] Kumar, R., Singh, P., & Kaur, A. (2022). Real-time surveillance system using YOLO for criminal detection. International Journal of Recent Technology and Engineering (IJRTE), 10(4), 88–93.

[24] Grigorescu, S., Trasnea, B., Cocias, T., & Macesanu, G. (2020). A survey of deep learning techniques for autonomous driving. Journal of Field Robotics, 37(3), 362–386.

[25] Yadav, A., & Dixit, V. (2021). Face recognition techniques and challenges: A review. Materials Today: Proceedings, 47(2), 2967–2971