

Deep Learning Model Based Criminal Identifications System

Shanmugapriyan M¹, Arunachalam AR², Dharneesh SK³, Tamil Selvan S⁴, Nivetha G⁵
^{1,2,3,4} Department of Electronics and Communication Engineering
¹shanmugapriyan.ec20@bitsathy.ac.in, ²arunachalam.ec20@bitsathy.ac.in,
³dharneesh.ec20@bitsathy.ac.in, ⁴tamilselvans.bitsathy.ac.in, ⁵nivethag@bitsathy.ac.in

ABSTRACT

Criminal record generally contains all the information both personal and criminal with the photograph of the person. In order to recognize Criminal, identification of some sort is required, designated by eyewitnesses. In most cases the resolution or/and quality of the recorded image sections is unsatisfactory and is difficult to recognize the face. Recognition can be achieved in various different ways like DNA, eyes, finger print, etc. One of the ways is face identification. Since facial recognition technology is powered by artificial intelligence, it can provide excellent results in identifying criminals. Even considering that most people, when committing an illicit activity, try to hide their identity: hiding their faces or covering their faces with scarves, masks, etc. In such cases, AI uses deep learning methods to identify the individual. In this project, proposed an Deep Face an automatic criminal identification system for Police Department to enhance and upgrade the criminal distinguishing into a more effective and efficient approach using Convolutional neural network algorithms. In our proposed methodology, a database is created by storing both full and sliced images of the criminals along with all the personal and criminal details. The captured images of the person get compared with the criminal data Law Enforcement Agencies have in their database. The CNN involves mapping the face with some facial points, allowing the true identity of the individual to be revealed. Using technology, this idea will add plus point in the current system while bringing criminals spotting to a whole new level by automating tasks. Law enforcement receive alerts when an individual claimed by the authorities is identified by our technology, speeding up their arrest and preventing new crimes. Customize notifications and alarms based on a variety of detection or recognition events and program automated security response workflows and SMS and email notifications.

Index Terms— Criminal records, Database, Facial recognition, Deep face, User Interface, Neural networks, Detection, Automation.

1. INTRODUCTION

Video surveillance systems have been widely used for various purposes, such as security, traffic monitoring, and crime prevention. These systems have undergone significant technological evolution, from analog to digital, and from wired to wireless. With the increased social awareness and demand for crime prevention and public safety, the market for image security and surveillance equipment systems has grown rapidly, and many high-performance, low-cost imaging devices have been introduced to meet the diverse needs of customers . However, despite the advances in hardware and software, most of these systems still rely on an administrator conducting naked-eye monitoring of videos captured by the surveillance cameras. This poses several challenges and limitations for the effective and efficient use of video surveillance systems. First, the control systems and the personnel for monitoring and managing the collected videos are often limited by the budget, resources, and policies of the organizations or institutions that operate the systems. Second, the amount and quality of the videos captured by the surveillance cameras are often overwhelming and inconsistent, making it difficult for the administrator to detect and respond to abnormal or suspicious events in real time. Third, the storage and retrieval of the videos are also problematic, as the videos are usually stored for 3-15 days depending on the environment of the system and are renewed in a first-in, first-out order. Most videos do not serve a meaningful purpose and are deleted in the process of storing new videos, resulting in a waste of storage space and a loss of potential evidence or information. Therefore, there is a need for more intelligent and automated video surveillance systems that can analyse and utilize the videos captured by the security devices in a more effective and efficient way.

Identifying problems in criminal identifications within a Law Enforcement Department involves recognizing challenges associated with manual or older methods. Traditional criminal identification methods employed by law enforcement departments face several challenges that impede their efficiency and effectiveness. The reliance on physical records introduces inefficiencies in storage, retrieval, and updating processes, leading to slow information retrieval and increased risks of errors. Manual data entry is susceptible to human errors and typos, compromising the integrity of criminal records. Limited accessibility and the lack of standardized data formats across agencies hinder timely information sharing and integration, reducing collaboration and potentially creating gaps in criminal investigations. The time-consuming nature of manual identification processes contributes to delayed suspect identification, impeding swift law enforcement responses.

Criminal identifications using image processing algorithms for law enforcement encounter several challenges. The accuracy and reliability of these algorithms can vary, leading to potential misidentifications and false positives. Biases in training data may result in discriminatory outcomes, raising concerns about fairness and civil rights. Privacy issues arise, especially when deployed in public spaces without adequate safeguards. Inadequate data quality, real-time processing challenges, and a lack of interoperability with other agencies' systems can hinder overall system performance. Security vulnerabilities pose risks of unauthorised access and potential misuse. Ensuring ethical use and transparency, scalability, and adaptability to varied conditions are additional challenges that need careful consideration to balance technological advancements with ethical and legal considerations in criminal identification. Addressing these challenges requires a multifaceted approach that incorporates technological advancements, ethical guidelines, legal frameworks, and ongoing public discourse to strike a delicate balance between the imperative for effective criminal identification and the protection of individual rights and societal values. Machine learning, a subfield of artificial intelligence, includes deep learning. It allows us to retrieve data from the layers that make up its architecture. Image recognition, fraud detection, news analysis, stock analysis, self-driving cars, healthcare applications such as cancer image analysis, etc. are among the industries that employ it. As more data is fed into the network, the layers become extremely well-trained. They fall under the categories of unsupervised, semisupervised, and supervised. Particular information extraction is known to occur at each tier. For instance, in image recognition, the first layer looks for edges, lines, and other features, and the second layer looks for features like the nose, ear, and eye. Rather than supplying our network with full images, CNN breaks down photos into several overlapping tiles as part of its data processing workflow. Next, we apply a method known as a sliding window to the entire original image and save the outcome as a distinct little picture tile. Using a sort of brute force approach, the sliding window finds the object in each potential section by scanning the entire area for the given image. This process is repeated until the desired object is found in each sector.

The facial recognition technology is a branch of computer vision that aims to identify or verify a person from a digital image or a video frame. The technology uses various algorithms and techniques to extract and compare the facial features of a person from a given image or video, and match them with a database of known faces. The facial recognition technology has been widely used for various purposes, such as biometric authentication, access control, social media, and entertainment. However, the technology also has many potential applications for crime prevention and public safety, such as using the video surveillance systems to identify and locate the ex-convicts of crimes. By integrating the facial recognition technology and the video surveillance systems, the intelligent video surveillance systems can automatically detect and recognize the faces of the ex-convicts of crimes from the videos captured by the surveillance cameras, and alert the administrator or the law enforcement officers if they are found in the crime-vulnerable areas. This way, the intelligent video surveillance systems can provide a more proactive and preventive approach to the monitoring and restricting of the exconvicts of crimes, and enhance the public safety and the human rights of the potential victims. The proposed system aims to improve the existing surveillance system, which depends on human observation skills. Our system ensures that security camera videos are carefully examined, allowing for the quick recognition of possible criminals or dangers in areas with high crime rates such as schools, childcare centres, and national security sites. This improves safety by enabling fast alerts to relevant authorities through the surveillance system's notification channel.

2. RELATED WORKS

Criminal face identification system using deep learning algorithm multi-task cascade neural network (MTCNN). The paper possess a new CNN model, known as 48net, is being utilized in the course. It's slower but more powerful, employing a multi-goal approach and featuring a smaller structure akin to the 24-net. The final stage incorporates a 48-alignment net. Detecting faces poses challenges due to factors such as changes in appearance and the extensive search space for face positions and sizes. Previous methods involved extracting faces and conducting searches in a criminal identification database. The system, which registers new criminals, pre-processes images, and achieves an 86% accuracy with a database of 50 records, aims to leverage CCTV footage for proactive crime prevention rather than solely post-incident analysis, enabling real-time action by authorities.

P. Sivakumar, J. V, R. R and K. S, "Real Time Crime Detection Using Deep Learning Algorithm," 2021 International Conference on System, Computation, Automation and Networking (ICSCAN).[2] The rising crime rate necessitates proactive security measures. Utilizing recent technologies like CCTV is common, but human supervision is challenging due to numerous screens and potential errors. To address this, we propose a Real-Time Crime Detection Technique using Deep Learning. Our system employs YOLO as an object detection algorithm, capable of processing images at 45 frames per second. It monitors real-time videos and alerts nearby authorities about crimes, enhancing proactive crime prevention efforts. This approach aims to improve security by swiftly identifying and responding to criminal activities as they occur. .S. T. Ratnaparkhi, A. Tandasi and S. Saraswat, "Face Detection and Recognition for Criminal Identification System," 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2021[3]. The conventional process of identifying criminals is slow and challenging, especially with the lack of biological evidence or



fingerprints. To overcome this, state-of-the-art face identification systems offer a quick and efficient solution. With CCTV cameras increasingly deployed for surveillance, video footage becomes a valuable resource for identifying suspects, criminals, and missing persons. This paper delves into developing a criminal identification system using machine learning and deep neural networks, aiming to streamline law enforcement efforts. By harnessing advanced technology, this approach promises to make the task of identifying and apprehending criminals more efficient and hassle-free.

3. PROPOSED METHOD

3.1 SYSTEM OVERVIEW

This paper proposes a real-time criminal detection system (RTCDS) for high-risk ex-convicts based on face tracking utilizing a deep learning-based face detector and identifier. The proposed system aims to prevent crimes by detecting a face in video data captured by image security devices such as surveillance cameras, and then notifying a chief manager or relevant criminal institutions after identifying the criminal through a comparison with criminal DBs. It uses a facial recognition system powered by artificial intelligence and CNN algorithms for automatic criminal identification. Also it Establish a robust database containing both full and sliced images of criminals, along with their personal and criminal details, to facilitate accurate identification. The paper implements a YOLO v8 for precise face mapping with facial points, allowing for effective identification even when individuals attempt to conceal their faces. It develops a notification system with customizable alerts for law enforcement based on various Detection or recognition events. Program automated security response workflows to expedite Arrests. The figure below depicts the system architecture of the proposed system of this paper.



Figure 1

3.2 PROPOSED WORK

This project is a multifaceted solution, employing state-ofthe-art technology to empower law enforcement agencies in the identification, tracking, and real-time monitoring of criminals. At its core is the user-friendly Criminal Identification Web App, a web-based tool developed with Python Flask and Tensor Flow, providing a robust platform for seamless criminal identification. The End User Dashboard serves as the interface for both Web Admin and Law Enforcement Officers. The Web Admin module, responsible for system management and database configuration, operates at the backend. In contrast, Law Enforcement Officers access the frontend, enabling database searches, image uploads, and receipt of identification results. The Crime Net Model, a Deep Convolutional Neural Network (DCNN), is the engine for criminal face classification. The training process involves uploading datasets or live feeds, frame conversion, pre-processing (including RGB to Grey Scale Conversion, Noise Filter, and Binarization), face detection via the Region Proposal Network (RPN), feature extraction using Local Binary Pattern (LBP), and face recognition and classification using a dedicated CNN model, CrimeNet. Once trained, CrimeNet is seamlessly deployed into the Criminal Identification Web App for real-time operations. The Criminal Face Identification module captures video footage of suspected criminals, predicts potential frames with significant facial features, and undergoes pre-processing for image enhancement. Utilizing advanced face detection algorithms like Yolo v8, feature extraction techniques, and the CrimeNet Model for comparison, the system confirms the identity of criminals with a high degree of confidence. The Criminals Crime Record Finder plays a pivotal role in law enforcement by confirming criminal identities and accessing comprehensive criminal histories from the Criminal Database. This module provides invaluable insights into past offenses, arrests, and relevant details crucial for effective decisionmaking and investigation. The Criminals Surveillance System integrates the CrimeNet Model with public CCTV cameras for real-time facial recognition and monitoring. This includes continuous monitoring of live video streams, integration with the Criminal Database for comprehensive history access, and specific modules for theft and murder detection, missing criminal's identification, and Geographic Information System (GIS) integration for spatial visualization. The Alert Generation and Notification System ensures timely communication with law enforcement officers in critical situations. Alerts are triggered for wanted criminals, missing persons, potential matches in investigations, known associates, or individual's on watch lists. Each alert provides essential details such as names, photos, criminal history, enabling officers to take swift and informed action. The proposed Criminal Identification and Surveillance System amalgamates cutting-edge technologies into a cohesive framework, empowering law enforcement with efficient tools for criminal identification, surveillance, and proactive crime prevention.



3.3 SYSTEM FLOW

The system flow of the Criminal Identification System involves a sequence of interconnected steps, ensuring a streamlined process from capturing video footage to criminal identification and historical record retrieval. This system flow ensures a systematic approach to criminal identification, leveraging advanced technologies for real-time monitoring, facial recognition, and historical record retrieval. The integration of deep learning models and image processing techniques contributes to the efficiency and accuracy of the overall system. Below is a detailed flow outlining the key stages:

3.3.1 CRIMINAL IDENTIFICATION AND SURVEILLANCE SYSTEM INITIALIZATION:

The system initializes with the Criminal Identification and Surveillance System, which integrates advanced technologies for criminal identification and real-time monitoring.

3.3.2 ACCESSING THE CRIMINAL IDENTIFICATION WEB APP:

Law enforcement personnel access the Criminal Identification Web App, a user-friendly web-based application designed for facial recognition and criminal tracking. The web app is built using Python Flask and TensorFlow, ensuring efficiency and user-friendliness.

3.3.3 END USER DASHBOARD ACCESS:

Authorized users, including law enforcement officers, access the End User Dashboard within the web app.

3.3.4 WEB ADMIN MANAGEMENT:

The Web Admin, responsible for backend management, handles tasks such as user management, data management, and system configuration. Admins configure system settings and manage the database through the backend interface.

3.3.5 LAW ENFORCEMENT OFFICER INTERACTION:

Law enforcement officers, the primary users of the system, interact with the frontend interface of the End User Dashboard. They perform facial recognition searches against the criminal records database, upload images for identification, and receive real-time identification results.

3.3.6 CRIMINAL FACE CLASSIFICATION USING CRIMENET MODEL:

The CrimeNet Model, built and trained using Deep Convolutional Neural Networks (DCNN), is utilized for criminal face classification. This model is specifically trained to automatically identify and classify images of criminal faces, aiding in the quick and accurate identification of potential suspects.

3.3.7 DATA COLLECTION AND PRE-PROCESSING:

Datasets containing images of individuals relevant to criminal identification are collected, or live feeds from

surveillance cameras are utilized for real-time model training. Each video frame is converted into individual images, undergoes preprocessing (RGB to grayscale conversion, noise filtering, binarization), and faces are detected using the Region Proposal Network (RPN).

3.3.8 FEATURE EXTRACTION AND FACE RECOGNITION:

Feature extraction techniques like Local Binary Pattern (LBP) capture texture information crucial for distinguishing facial features. A Convolutional Neural Network (CNN) trained for face recognition and classification identifies and classifies facial features extracted through preceding steps.

3.3.9 CRIMINAL IDENTIFICATION:

Upon identifying a match with high confidence, the system confirms the criminal's identity by associating facial features with a known individual within the CrimeNet Model.

3.3.10 RETRIEVE CRIMINAL'S CRIME RECORDS:

With the confirmed identity, the system accesses the Criminal Database to retrieve the criminal's history of cases. Past offenses, arrests, and relevant details aiding law enforcement in understanding the suspect's criminal background are retrieved.

3.3.11 INTEGRATION WITH CRIMINAL DATABASE:

Integration with the Criminal Database ensures seamless access to comprehensive criminal records, empowering law enforcement agencies with valuable information for decision-making and investigation.

3.3.12 ALERT GENERATION AND NOTIFICATION:

Alerts are generated and sent to law enforcement officers in critical situations, including wanted criminals, missing persons, potential matches in investigations, known associates, or individuals on watch lists. Each alert includes essential information such as names, photos, and criminal history, enabling law enforcement officers to take swift and informed action.

3.4 CRIMINAL FACE IDENTIFICATION Capture Video of Criminal:

Law enforcement personnel utilize recording devices to capture video footage featuring the face of a suspected criminal. This serves as critical evidence for identification and criminal investigations.

Prediction and Frame Conversion:

The captured video undergoes predictive processing, enabling the anticipation of potential frames where significant facial features may be present. Subsequently, the continuous video stream is converted into individual frames, creating a temporal sequence of still images.

Pre-processing for Image Enhancement:

Each frame undergoes pre-processing to optimize image quality and standardize input conditions. This involves resizing to a consistent resolution, denoising to reduce visual artefacts, and normalization to ensure uniform brightness and contrast levels.

Face Detection Algorithms:

Advanced face detection algorithms Yolo v8 are applied to the preprocessed frames. These algorithms systematically analyses each frame, identifying and isolating facial regions. Detected faces are then marked as potential points of interest for further analysis.

Feature Extraction Techniques

Feature extraction techniques are employed to analyse 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.

3.5 Criminals Crime Record Finder

The Criminals Crime Record Finder module plays a vital role in law enforcement by leveraging facial recognition technology to identify and retrieve the criminal history of individuals. Upon identifying a match with a high degree of confidence, the system confirms the criminal's identity by associating the facial features extracted from the input frame with a known individual within the CrimeNet Model. With the confirmed identity, the module accesses the Criminal Database to retrieve the criminal's history of cases. This historical data includes comprehensive information about past offenses, arrests, and any other relevant details that aid law enforcement in understanding the suspect's criminal background. Through efficient integration with the Criminal Database and advanced facial recognition capabilities, this module provides law enforcement personnel with critical insights for effective decision-making and investigation.

3.6. Criminals Surveillance System CrimeNet Model Integration

The CrimeNet Model is seamlessly integrated with all public CCTV cameras to enable real-time facial recognition. 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. It instantly identifies and tracks

individuals with known criminal records, providing real-time alerts to law enforcement when a person of interest is detected.

Integrate 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. This integration enables the retrieval of the individual's complete criminal history, including details on past offenses, arrests, and relevant information crucial for law enforcement. The Criminal Database serves as a centralized repository that houses a wealth of information about known criminals. By tapping into this extensive database, law enforcement gains access to a comprehensive set of records that aids in understanding the suspect's criminal background. This integration ensures that the Criminals Crime Record Finder module provides accurate, up-to-date, and thorough insights into the historical activities of identified individuals, empowering law enforcement agencies with valuable information for decision making and investigative purposes.

Theft and Murder Detection:

This module focuses on identifying specific criminal activities such as theft or murder. It utilizes yolov8 with CrimeNet Model to detect anomalies or suspicious behavior in the monitored areas, triggering alerts for immediate investigation. When criminal activities are detected, the system generates alerts, providing relevant details to law enforcement agencies. These alerts may include facial snapshots, location information, and timestamps, facilitating a rapid response.

Missing Criminals Identification:

This module aids in the identification of missing criminals by continuously comparing the faces captured by CCTV cameras with the CrimeNet Model. If a match is found, an alert is generated to notify law enforcement about the location of the missing individual.

Geographic Information System (GIS):

Integration GIS integration allows for mapping the location of criminal activities and the movement of identified individuals. Law enforcement can visualize the spatial distribution of criminal incidents for strategic deployment.

4. CONCLUSION

This project presents a technologically advanced solution for law enforcement agencies in the identification and tracking of criminals. Leveraging cutting-edge technologies such as Deep Convolutional Neural Networks (DCNN), Yolo V8, and advanced facial recognition techniques, the system offers a robust framework for real-time monitoring and crime record retrieval. The web-based Criminal Identification System, built using Python Flask and TensorFlow, serves as a userfriendly interface for law enforcement personnel. The integration of the CrimeNet Model, trained through meticulous processes such as



dataset collection, preprocessing, face detection, feature extraction, and CNN-based classification, enables swift and accurate identification of potential suspects. The Criminals Crime Record Finder module seamlessly integrates with the Criminal Database, providing law enforcement with historical data on identified individuals. This database includes information on past offenses, arrests, and other relevant details crucial for understanding a suspect's criminal background. The Criminals Surveillance System enhances proactive policing by integrating with public CCTV cameras. Real-time monitoring, theft and murder detection, missing criminal's identification, and GIS integration contribute to a holistic approach to crime prevention and response. The Alert Generation and Notification System acts as a crucial component, ensuring that law enforcement officers are promptly informed in critical situations. Whether dealing with wanted criminals, missing persons, ongoing investigations, known associates, or watch list individuals, the system generates alerts containing vital information for informed decision-making. This integrated system empowers law enforcement agencies with efficient tools for crime prevention, investigation, and apprehension. The fusion of artificial intelligence, machine learning, and real-time surveillance capabilities positions the Criminal Identification and Surveillance System as a force multiplier in the relentless pursuit of public safety and security

5. REFERENCES

[1] V. Tsakanikas and T. Dagiuklas, "Video surveillance systems-current status and future trends," Comput. Electr. Eng., vol. 70, pp. 736–753, Aug. 2018.

[2] J. T. Pickett, C. Mancini, and D. P. Mears, "Vulnerable victims, monstrous offenders, and unmanageable risk: Explaining public opinion on the social control of sex crime," Criminology, vol. 51, no. 3, pp. 729–759, Aug. 2013.

[3] D. M. Button, M. DeMichele, and B. K. Payne, "Using electronic monitoring to supervise sex offenders: Legislative patterns and implications for community corrections officers," Criminal Justice Policy Rev., vol. 20, no. 4, pp. 414–436, Dec. 2009.

[4] M. C. Hoffman, "Smart cities: A review of the most recent literature," Informatization Policy, vol. 27, no. 1, pp. 3–35, 2020.

[5] B. C. Welsh and D. P. Farrington, "Public area CCTV and crime prevention: An updated systematic review and metaanalysis," Justice Quart., vol. 26, no. 4, pp. 716–745, Dec. 2009.

[6] E. L. Piza, B. C. Welsh, D. P. Farrington, and A. L. Thomas, "CCTV surveillance for crime prevention: A 40-year systematic review with metaanalysis," Criminol. Public Policy, vol. 18, no. 1, pp. 135–159, Feb. 2019. [7] E. L. Piza, "The crime prevention effect of CCTV in public places: A propensity score analysis," J. Crime Justice, vol. 41, no. 1, pp. 14–30, Jan. 2018.

[8] G. Alexandrie, "Surveillance cameras and crime: A review of randomized and natural experiments," J. Scandin. Stud. Criminology Crime Prevention, vol. 18, no. 2, pp. 210–222, Jul. 2017.

[9] R. V. Clarke, "Situational crime prevention," Crime Justice, vol. 19, pp. 91–150, 1995.

[10] J. Ratcliffe, Video Surveillance of Public Places. Washington, DC, USA: U.S. Department of Justice, Office of Community Oriented Policing Services, 2006.

[11] J.-H. Jeon and S.-R. Jeong, "Designing a crime-prevention system by converging big data and IoT," J. Internet Comput. Services, vol. 17, no. 3, pp. 115–128, Jun. 2016.

[12] P. Chen, H. Yuan, and X. Shu, "Forecasting crime using the ARIMA model," in Proc. 5th Int. Conf. Fuzzy Syst. Knowl. Discovery, Oct. 2008, pp. 627–630, doi: 10.1109/FSKD.2008.222.

[13] Lubna, N. Mufti, and S. A. A. Shah, "Automatic number plate recognition: A detailed survey of relevant algorithms," Sensors, vol. 21, no. 9, p. 3028, Apr. 2021.

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

[15] N. A. Abdullah, M. J. Saidi, N. H. A. Rahman, C. C. Wen, and I. R. A. Hamid, "Face recognition for criminal identification: An implementation of principal component analysis for face recognition," in Proc. AIP Conf., 2017, Art. no. 020002.

I