International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 08 | Aug - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Criminal Eye

Student Divya K G[1] Assistant Professor Supriya [2]

[1]Student, 4th Semester MCA, Department of MCA, BIET, Davangere

2 Assistant Professor, Department of MCA, BIET, Davangere

Abstract

Criminal Eye is an AI-powered criminal detection and management system designed to enhance law enforcement operations through centralized data handling, real-time updates, and advanced face recognition technology. The platform facilitates seamless communication between police stations and a central administration, enabling effective coordination and efficient criminal tracking. The system comprises two main modules: the Admin Module and the Police Station Module. The Admin Module provides comprehensive control over districts, cities, and police stations, allowing administrators to manage station details, oversee criminal records, and respond promptly to reports of missing criminals. The Police Station Module equips police personnel with the tools to maintain accurate and up-to-date criminal records by adding, modifying, or deleting suspect information. It also enables officers to capture and compare suspect photographs against a centralized database to identify previous offenses. This AI-driven approach empowers police agencies to make data-informed decisions, improve crime prevention efforts, and enhance overall public safety. Criminal Eye represents a significant step toward modernizing traditional crime management systems and ensuring more effective law enforcement through technological innovation.

Keyword: Criminal Detection, Face Matching, Centralized Criminal Database, Real-Time Crime Tracking, Police Collaboration

I.INTRODUCTION

In today's world, where technological advancements are rapidly transforming every sector, law enforcement and criminal investigation are no exception. The rise in crime rates and the evolving nature of criminal activities demand smarter, faster, and more efficient solutions to support police departments and law enforcement agencies in their mission to maintain public safety. Traditional methods of crime tracking and criminal record management are often decentralized, time-consuming, and prone to human error. These limitations result in delayed investigations, poor inter-agency communication, and insufficient tracking of repeat offenders. To address these pressing challenges, there is a growing need for an integrated digital solution that can centralize criminal records, facilitate real-time updates, and support police officers with intelligent decision-making tools. One such solution is Criminal Eye, an AI-powered criminal detection and management system designed to revolutionize the way law enforcement agencies handle criminal data and operations.

Criminal Eye is a state-of-the-art platform that leverages artificial intelligence and face recognition technology fig 1. Shows that to provide a unified system for managing and tracking criminal records across various jurisdictions. By connecting police stations through a centralized database, the system ensures seamless communication and cooperation between different law enforcement units. This enhanced coordination enables quicker responses to criminal activities, more accurate identification of suspects, and efficient data-driven decision-making. The system is built with two primary modules: the Admin Module and the Police Station Module, each playing a crucial role in ensuring the smooth functioning of the platform. The Admin Module is responsible for managing the overall system, including the configuration of cities, districts, and police stations. It provides administrators with full control to add, update, or delete police stations and to access or remove criminal records as needed. Additionally, the admin can monitor reports related to missing criminals submitted by police stations and take necessary action based on the data.

On the other hand, the Police Station Module is specifically designed to empower police personnel in their daily tasks related to criminal data management. It allows officers to create, edit, or delete records in the criminal database, thereby maintaining up-to-date and accurate information. A significant feature of the system is its integration with advanced face recognition technology. When a suspect is detained, the police can capture their photograph and use the system to match it against the existing database to check for prior convictions or criminal history. This not only aids in the identification of repeat offenders but also saves valuable time that would otherwise be spent on manual verification processes. Furthermore, the system enables police stations to share information about criminals who are at large, ensuring that all connected stations are informed and can work collaboratively in tracking and apprehending suspects.

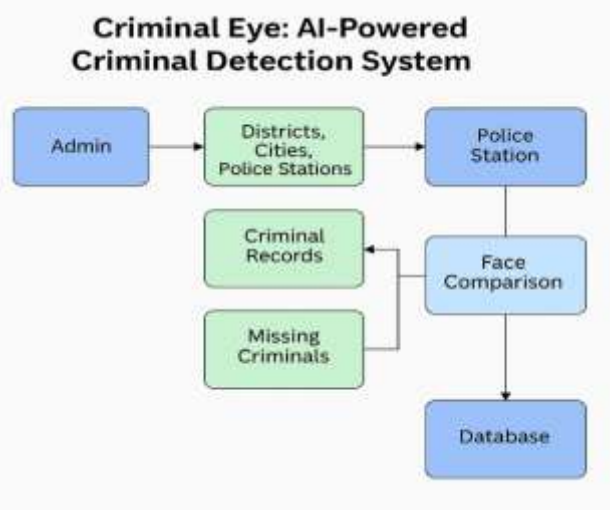

Fig 1. Architecture diagram for criminal Eye System

The benefits of Criminal Eye extend beyond efficient data handling. The system enhances the investigative capabilities of police officers by providing them with quick access to vital information, thereby increasing the overall effectiveness of law enforcement operations. By allowing real-time updates and a centralized approach, the platform minimizes communication gaps and ensures that all departments are operating with the most current and accurate data. This integrated framework also supports the implementation of preventive measures, as agencies can analyze data trends and take action before crimes occur. Moreover, the use of face comparison technology reduces the dependency on traditional and often unreliable methods of suspect identification, leading to more reliable and evidence-based outcomes.

As criminal activities continue to grow in complexity and scale, the role of intelligent systems like Criminal Eye becomes increasingly crucial. The platform not only aids in solving crimes faster but also in preventing them through proactive surveillance and inter-departmental cooperation. It transforms the conventional reactive approach to crime management into a proactive and technology-driven strategy. By bridging the gap between technology and law enforcement, Criminal Eye empowers police agencies to respond more effectively to criminal threats, ultimately contributing to a safer society.

In Criminal Eye is not just a technological tool but a comprehensive solution aimed at modernizing and strengthening the core functions of law enforcement agencies. Its ability to centralize data, facilitate real-time communication, and utilize AI-driven face recognition makes it a powerful asset in the fight against crime. Through its Admin and Police Station modules, the system ensures full coverage and coordination among various law enforcement entities, creating a robust infrastructure for managing crime. As the world moves toward a more digital future, solutions like Criminal Eye are essential to keeping pace with the evolving challenges of public safety and criminal justice.

II.RELATED WORK

This paper is to explore how modern facial recognition technology can be effectively used for criminal identification, especially in cases where traditional evidence like fingerprints or DNA is unavailable. With the growing use of surveillance cameras in public places and buildings, face recognition offers a fast and reliable way to identify criminals, missing persons, and suspects. The paper reviews recent advancements in facial recognition, discusses various application scenarios, and examines the typical architecture of face detection systems. It highlights methods such as Haar cascades, Histogram of Oriented Gradients (HOG), and deep learning techniques like Convolutional Neural Networks (CNNs), along with technologies such as OpenCV, TensorFlow, and Dlib, which are used to build and deploy facial recognition models. These tools and methods help detect and analyze facial features accurately, while the study also addresses challenges and future improvements needed for wider and more ethical implementation [1].

This paper aims to explore the application of facial recognition (FR) technology as a reliable and efficient tool for criminal identification, particularly in scenarios where conventional evidence like fingerprints or DNA is unavailable. Leveraging recent advancements in artificial intelligence (AI), the study focuses on overcoming real-world challenges such as poor lighting conditions and limited criminal image databases. To address these issues, the system utilizes a modified ResNet-34 deep learning model, implemented through the Face_Recognition library—an enhanced interface built on top of the Dlib library and its supporting tools. A dataset comprising 200 criminal images was created, and the system was designed to perform accurate recognition using a single frontal face image, achieving an accuracy rate of 99.38%. Although the model demonstrates high efficiency, it faces challenges such as increased processing time with larger databases and reduced accuracy with side-profile images, which are noted as areas for future improvement[2].

This paper aims to examine the rapid evolution and increasing deployment of facial recognition technology (FRT) in the context of state surveillance, particularly focusing on its application in policing and security. As FRT enables real-time tracking, identification, and categorization of individuals by analyzing facial images, it significantly enhances the ability of authorities to monitor people and vehicles, collect large-scale data, and map social networks and relationships. While these capabilities support efforts to detect, prevent, and respond to serious crimes and threats, they also pose substantial risks to fundamental human rights, including privacy, freedom of expression, and freedom of assembly. The paper highlights that although academic research and advocacy efforts have addressed the ethical and societal implications of FRT, the development of coherent and principled regulatory frameworks remains underexplored. By analyzing three contemporary case studies involving the regulation of FRT in policing and security contexts, the study seeks to uncover the complexities, challenges, and gaps in current regulatory practices and contribute to the discourse on how to balance public safety with the protection of individual rights[3].

This paper aims to design and develop an intelligent system that assists law enforcement in promptly and accurately identifying the type and severity of criminal cases using machine learning technology. The system is capable of analyzing text-based criminal case summaries, specifically in the KICS data format, which contains real-world police data. By leveraging this data, the system predicts one of 21 predefined crime types and calculates a crime risk score based on the severity and damage of the case using a custom-developed risk calculation formula. To achieve these predictions, the paper introduces both Deep Neural Network (DNN) and Convolutional Neural Network (CNN)-based models. These models demonstrated superior accuracy compared to traditional classification algorithms like Naïve Bayes and Support Vector Machine (SVM), with the CNN model outperforming SVM and Naïve Bayes by 7% and 8%, respectively, in crime type prediction tasks. The technology is implemented as a user-friendly software platform with a graphical user interface (GUI), enabling police officers and

field personnel to quickly assess the nature and risk level of new criminal cases through automated text analysis, thus enhancing decision-making efficiency and public safety response[4].

This paper is to create a smart video surveillance system that can help find and track dangerous criminals, such as child sex offenders, in real-time—especially when they go near sensitive places like schools or childcare centers. Traditional systems rely on security guards watching camera footage with the naked eye or reviewing video recordings later, which is slow and not always effective. To solve this, the proposed system uses advanced face recognition technology that can detect and identify criminal faces from live surveillance camera footage. It works by using a smaller version of each video frame to quickly find faces and then tracks them using a unique face ID. To improve accuracy, it uses a scoring method that combines how confident the system is with how closely the face matches a known criminal. This method also reduces mistakes when there are many faces stored in the system. The system tested very well, achieving 90% accuracy and an F1-score of 0.943, and it performed better than older methods. It can help protect public areas by quickly alerting authorities when a known criminal is detected, helping to prevent crimes before they happen[5].

This paper presents an efficient and practical Face Detection and Recognition system designed to support law enforcement by making it faster and easier to identify suspects in criminal cases. Unlike traditional methods, this system uses real-time processing and scalable databases to detect and recognize faces accurately. It uses the Haar-cascade classifier to detect facial features and the LBPH (Local Binary Pattern Histogram) algorithm for reliable face recognition. When a match is found, the system sends an instant Gmail alert using the smtplib library, helping authorities respond quickly. This setup has proven effective in real-time scenarios and contributes to public safety by speeding up investigations and improving criminal detection. Beyond policing, the system is versatile and can also be used in areas like automated attendance systems and access control for enhanced security. Its ability to adapt to different applications shows great potential for widespread use across various industries, making it a valuable tool for both safety and operational efficiency[6].

This paper aims to give a clear and complete understanding of how cybercrimes are handled by the police. It explains what cybercrime is, the different types of cybercrimes, and how criminals plan and carry out these activities. The study highlights each stage of a cybercrime and helps law enforcement better prepare to investigate such cases. One of the main points is the importance of digital evidence—like files, logs, or data—that helps track and catch cybercriminals. The paper also looks at how cybercrimes affect victims and how the public views the police's role in handling these cases. It discusses the challenges police face when dealing with cybercrime and the need for proper investigation steps. The paper also shows how important it is for government and private companies to work together to fight cybercrime effectively. It reviews current methods used in investigations and suggests a new, improved model for handling cybercrime cases. Overall, this paper provides useful knowledge and tools that can help law enforcement better protect people in today's digital world[7].

Digital technology now plays a critical role in policing and security management, with policing apps, drones and body-worn cameras potentially being game-changers. Adoption of such technologies is, however, not straightforward and depends upon the buy-in of senior management teams and users. This study examines what obstacles practitioners face in the procurement, deployment and use of crime prevention and detection technologies. The issue is explored through a number of expert interviews conducted with practitioners in London between August 2019 and March 2020. This work expands previous, more theoretical, literature on the topic by adding a practical perspective and advances the understanding of issues faced in innovation processes and their management. We identified a variety of issues and obstacles to technological innovation for policing. These include the deployment of new systems at the cost of old ones, lack of financial and political support, issues in public–private partnerships, and public acceptability. Although individual practitioners may have the expertise and willingness to unleash the full potential of surveillance and crime-reduction technologies, they are usually restrained by institutional rules or, in some cases, inefficiencies. In terms of the latter, this study especially highlights the negative impact of a lack of technical interoperability of different systems, missing inter- and intra-agency communication, and unclear guidelines and procedures[8].

This paper focuses on tackling the growing problem of criminal activities by developing a real-time face detection and recognition system to help police identify criminals more efficiently. Since the number of police officers is often not enough to keep up with rising crime, this system aims to support law enforcement by automating the identification process. The system uses a Multi-Task Cascade Neural Network (MTCNN) to accurately detect and recognize faces. It works in real-time and uses one-shot learning, which means it can recognize a criminal using just a single image. Once a match is found, the system retrieves the criminal's details from the database and sends a notification to the police with the person's information and the location where the camera detected them. This makes the process faster, more reliable, and helpful for real-time crime monitoring and prevention[9].

This paper introduces a smart Crime Monitoring System (CMS) that uses CCTV cameras and artificial intelligence to detect crimes in real time and alert police officers. The system helps overcome human weaknesses like slow response or missed details. It works in three steps: detecting weapons, identifying violent actions, and recognizing faces. The CMS uses deep learning models—YOLOv5 for weapon detection, MobileNetV2 for spotting violence, and a face recognition algorithm to identify people. The system was trained using both image and video data and showed high accuracy: over 80% for weapons, 95% for violence, and 97% for face recognition. Tests in real situations proved that the system

works well and can help improve public safety by quickly spotting crimes and notifying authorities[10].

III. METHODOLOGY

The Criminal Eye system follows a clear and structured process to build and operate an advanced criminal detection and management platform. It combines software development and a central database to help police departments work more efficiently. The system is divided into two parts: the Admin Module and the Police Station Module, each playing an important role in managing and tracking criminals.

1. Understanding Requirements: The first step is to understand what the system needs to do. Discussions are held with police officers and technical experts to find out the most important features, like keeping a central record of criminals, using facial recognition, and allowing smooth communication between police stations.

2. Creating the Database: A central database is built to store all the important information, such as names, photos and missing person reports. This database is shared among all police stations, so they can access and update the same data in real-time.

3. Building the Admin Module: This part of the system is for admin. They can add or remove cities and police stations, view and delete criminal records, and manage reports of missing criminals. The admin panel is protected with login and security features to prevent misuse.

4. Developing the Police Station Module: This module is for police officers, this module has the ability to add, update, or delete criminal information to keep the records accurate and up to date. Police officers can also use face comparison technology to identify suspects by taking a photo and checking if the person has any criminal background. The system allows police to update their login password for security. Additionally, police stations can share missing criminal information with other stations by posting or removing such details in the system, helping improve cooperation and tracking across regions.

5. Using Face Recognition: One of the most powerful features is face recognition. When police take a photo of a suspect, the system to check the photo against stored images. If it finds a match, the system shows the suspect's past record. This helps police quickly identify repeat offenders.

6. Testing the System: Before launching, the system is tested to make sure everything works properly. The face recognition feature is tested carefully to ensure it gives accurate results. Police officers give feedback during this stage so improvements can be made.

IV. TOOLS AND TECHNOLOGIES USED

A. Android Studio

Android Studio is the official integrated development environment (IDE) for Android application development, developed by Google. It provides a unified platform for building, testing, and deploying Android apps for various devices such as smartphones, tablets, and smart TVs. Android Studio supports programming languages like Java, Kotlin, and C++, and is equipped with advanced tools such as a powerful code editor, visual layout editor, real-time error detection, and a built-in Android emulator. One of its key strengths is the Gradle-based build system, which allows flexible and automated app builds. Developers can also utilize Android Studio's performance profilers to monitor memory usage, CPU load, and network activity, ensuring efficient and optimized applications. In the context of the Criminal Eye paper, Android Studio plays a critical role in developing the mobile application used by police officers. Through this app, officers can log in securely, capture and upload suspect photographs, access criminal databases, and use face matching functionality integrated with the backend system. Its user-friendly interface, powerful debugging tools, and seamless integration with Firebase and other Google services make Android Studio an essential tool for creating secure and responsive mobile applications that enhance real-time law enforcement operations.

B. ASP.NET 2015

ASP.NET 2015 refers to the version of Microsoft's web development framework available around the release year 2015. At that time, ASP.NET was undergoing major enhancements, particularly with the introduction of ASP.NET 5, which was later renamed to ASP.NET Core 1.0. ASP.NET 2015 allowed developers to build modern, high-performance web applications and APIs using the .NET Framework and the new .NET Core runtime.

ASP.NET 2015 supported the development of dynamic web pages, web services, and enterprise-level applications using server-side technologies. It provided built-in support for MVC (Model-View-Controller) architecture, which helped separate the application's logic, user interface, and data handling. Developers could build scalable, maintainable, and secure web applications efficiently using C# or VB.NET within Visual Studio 2015. Features like Razor view engine, Entity Framework integration, and SignalR for real-time communication made ASP.NET a preferred choice for web-based systems. In the context of a system like Criminal Eye, ASP.NET 2015 could be used to develop the Admin module or central dashboard, allowing administrators to manage districts, police stations, and criminal records securely through a responsive web interface. Its strong support for authentication, role-based access, and integration with SQL Server made it suitable for handling sensitive law enforcement data securely.

C. SQL Server 2014

SQL Server 2014 is a robust relational database management system (RDBMS) developed by Microsoft, designed to store, manage, and retrieve data as requested by other software applications. It supports both transactional and analytical processing, making it suitable for enterprise-level applications that require high performance, security, and scalability.

One of the key features of SQL Server 2014 is In-Memory OLTP (Online Transaction Processing), which significantly improves the speed of data operations by allowing selected tables to be stored and processed in memory. It also includes enhanced backup and restore features, improved security mechanisms, support for AlwaysOn availability groups for high availability and disaster recovery, and integration with Microsoft Azure for hybrid cloud scenarios. In the context of the Criminal Eye paper, SQL Server 2014 plays a crucial role in managing centralized criminal data. It is used to store structured data such as police station details, criminal profiles, missing person reports, user credentials, and photograph metadata. The relational structure allows for efficient querying, indexing, and retrieval of records across districts and stations. SQL Server's strong support for stored procedures, triggers, and security features ensures data integrity and controlled access—vital for handling sensitive law enforcement information securely and reliably.

V. CONCLUSION

In conclusion, Criminal Eye: AI-Powered Criminal Detection presents an innovative and centralized approach to modernizing law enforcement processes through advanced face matching technology and efficient criminal data management. By integrating both admin and police station modules, the system ensures streamlined coordination, real-time information sharing, and accurate tracking of criminal activities across regions. It empowers police officers to verify suspect identities quickly and manage criminal records with ease, while providing administrators with full control over districts, stations, and data monitoring. With its secure, user-friendly, and scalable infrastructure, Criminal Eye enhances the capability of law enforcement agencies to respond to threats, prevent crimes, and maintain public safety. This smart solution not only improves the efficiency of criminal detection but also fosters stronger collaboration among police departments, thereby contributing to a more secure and connected policing ecosystem.

References

[1]. Menon, Arjun. "Leveraging Facial Recognition Technology in Criminal Identification." Interdisciplinary Innovations and Developments towards Smart and Sustainable Industries https://doi. org/10.13052/rp-978-87-7022-828-2 (2023).

[2]. Manj, W., Zunaira Faraz, Hamza Farooq, M. Fazal, and M. Baig. "Automatic Face Recognition of Criminals in Investigation Using Artificial Intelligence." Journal of XYZ (2023): 83-94.

[3]. Lynch, N. (2024). Facial Recognition Technology in Policing and Security—Case Studies in Regulation. Laws, 13(3), 35. https://doi.org/10.3390/laws13030035.

[4].Baek, M., Park, W., Park, J., Jang, K., & Lee, Y. (2021). Smart policing technique with crime type and risk score prediction based on machine learning for early awareness of risk situation. IEEE Access, 9, 131906–131915. https://doi.org/10.1109/access.2021.3112682.

[5].Kim, H., Choi, N., Kwon, H., & Kim, H. (2023). Surveillance system for Real-Time High-Precision recognition of criminal faces from wild videos. IEEE Access, 11, 56066–56082. https://doi.org/10.1109/access.2023.3282451.

[6]. Yesugade, N. P. K., Pongade, N. A., Karad, N. S., Ingale, N. D., & Mahabare, N. S. (2024). Face detection and recognition for criminal identification system. Deleted Journal, 2(07), 1950–1957. https://doi.org/10.47392/irjaeh.2024.0267.

[7]. Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. Journal of Economic Criminology, 2, 100034. https://doi.org/10.1016/j.jeconc.2023.100034.

[8]. Laufs, J., & Borrion, H. (2021). Technological innovation in policing and crime prevention: Practitioner perspectives from London. International Journal of Police Science & Management, 24(2), 190–209. https://doi.org/10.1177/14613557211064053.

[9].Kumar, K. K., Kasiviswanadham, Y., Indira, D., Palesetti, P. P., & Bhargavi, C. (2021). Criminal face identification system using deep learning algorithm multi-task cascade neural network (MTCNN). Materials Today Proceedings, 80, 2406–2410. https://doi.org/10.1016/j.matpr.2021.06.373.

[10].Mukto, M. M., Hasan, M., Mahmud, M. M. A., Haque, I., Ahmed, M. A., Jabid, T., Ali, M. S., Rashid, M. R. A., Islam, M. M., & Islam, M. (2023). Design of a real-time crime monitoring system using deep learning techniques. Intelligent Systems With Applications, 21, 200311. https://doi.org/10.1016/j.iswa.2023.200311.