**Pakistan Journal of Scientific Research, PJOSR**
ISSN (p): 0552-9050
Volume: 4, Number: 1, Pages: 83- 92, Year: 2024

# Next-Gen Facial Recognition for Criminal Detection: Leveraging Advanced Machine Learning Techniques

Anjum Ali[1], Hijab Zehra Zaidi[2], Ijaz Ali Shoukat[3], Amina Nawaz[4], Tahmina Asghar[5], Muhammad Amjad[6]

[1]Riphah College of Computing, Riphah International University, Faisalabad
[2]Department of Computer Science University of Engineering and Technology Lahore
[3]Riphah College of Computing, Riphah International University, Faisalabad
[4]Riphah College of Computing, Riphah International University, Faisalabad
[5] Riphah College of Computing, Riphah International University, Faisalabad
[6]Riphah College of Computing, Riphah International University, Faisalabad

Corresponding author: Sixth Author (amjad.sadiq@riphahfsd.edu.pk).
**Received: 15/05/2024, Revised: 20/06/2024, Accepted: 30/07/2024**

*Abstract-* **The process of identifying and spotting a criminal is slow and difficult creating a criminal detection framework that could help policemen to recognize the face of a criminal or a suspect is proposed. The framework is a client-server video-based face recognition surveillance in real-time. The framework applies face detection and tracking the video footage from the camera can be used to identify suspects, criminals, runaways, missing persons, etc. This project focuses on the development of the client side of the proposed framework, face detection, and tracking using Android mobile devices. For the face detection stage, we are using Python for artificial intelligence. The face-tracking stage is based on an intelligence algorithm. The proposed face detection. Thus proposed paper explains a way to help a criminal identification system using ML and deep neural networks.**

***Index Terms*—Criminal detection, detection framework.**

## I. INTRODUCTION

In this article, we can detect and recognize the faces of the criminals in a video stream obtained from a camera in real-time. The system consists of one database. Local watch list database, which will have the images and details (Unique-id, Name, Gender, Religion, Crimes done, etc.) of each criminal who belongs to that country. All the images are first preprocessed. Then it goes through feature extraction where Artificial Intelligence implemented using Python is used. The video is captured from the surveillance camera which is converted into frames. When a face is detected in a frame, it is preprocessed. The features of the processed real-time image are compared with the features of processed images which are stored in the database. If a match is found, it is a criminal. If he is a criminal a notification is sent to the police personnel with all the details and the time for which he was under the surveillance of the camera. If a match is not found in the watch lists, he is innocent.

### A. BACKGROUND

As the world has seen exponential advancement over the last decade, there is an abnormal increase in the crime rate and also the number of criminals is increasing at an alarming rate, this leads toward a great concern about the security issues. Due to a lack of police resources, many theft-related crimes, stealing crimes, burglaries, kidnappings, human trafficking, and other incidents go unsolved. In many cases, the perpetrator is never identified. In many times, numerous systems were suggested and put into place to prevent this circumstance. Biometrics is a technique that identifies or authenticates people based on their distinct patterns of physical characteristics or behaviors. With the development of biometric technology, biometric scanners are becoming more and more common on smartphones and other low-cost gadgets. Additionally, a growing number of services and apps demand excellent customer service and great security. Old-fashioned authentication techniques are being replaced by biometric technologies. Face recognition is one of the more sophisticated biometric techniques The face is the most important feature of the human body for identification. Faces set people apart. Facial recognition is a difficult problem with applications in security systems, finance, identity verification, and search, among other areas. A computer has to go through a whole different process in order to recognize a face that a human can recognize with ease. People simply and

frequently complete the task of acknowledging faces in their daily lives. It is anticipated that a facial recognition system will automatically recognize faces in photos and videos. Face verification (also known as authentication) and face identification (also known as recognition) are the two modes in which it can function. Face check involves coordinating the comparison of a black-and-white grayscale image with a formatted face (datasets) image whose feature is being retrieved. Face recognition evidence comprises one-to-many matchings, which compare an input face image or video to every format image in the database to see if they match. A watch-list check is another kind of face acknowledgment in which an inquiry face is synchronized with a suspect rundown.

## B. MOTIVATIONS AND CHALLENGES

The motivation behind such a system is rooted in the growing need for advanced technologies to enhance public safety and security measures. By leveraging artificial intelligence (AI) and facial recognition, this project aims to streamline the identification process, enabling quick and efficient identification of individuals with criminal records. One of the primary motivations for implementing this system is the potential to significantly improve the efficiency of law enforcement agencies. Traditional methods of identifying and tracking criminals often rely on manual processes, which can be time-consuming and prone to errors. The real-time nature of your project ensures that suspicious individuals can be promptly identified, allowing law enforcement to take immediate action. Additionally, the integration of facial recognition technology contributes to the overall enhancement of public safety, deterring criminal activities, and providing a robust layer of security for communities.

However, such an ambitious project comes with its set of challenges. Privacy concerns surrounding facial recognition technology have been a prominent issue, as it raises questions about the balance between security and individual rights. Striking the right balance in terms of privacy regulations, ethical considerations, and ensuring that the system is used responsibly is a significant challenge. The potential for false positives and negatives in facial recognition systems can also create challenges. Ensuring high accuracy in identifying criminals while minimizing the chances of misidentifying innocent individuals is a critical aspect that requires thorough testing and optimization. The project's reliance on a local watch list database introduces challenges related to data management and security. Safeguarding sensitive information, such as criminal records and personal details, is paramount to prevent unauthorized access and potential misuse. Additionally, maintaining the accuracy and relevance of the watch list database over time poses an ongoing challenge, considering the dynamic nature of criminal activities and the need for regular updates. Despite these challenges, the potential societal impact of your project is immense. The system holds the promise of revolutionizing law enforcement practices, enhancing public safety, and providing a valuable tool for ensuring the security of communities. By addressing the motivations and challenges head-on, your project stands at the forefront of technological innovation in the field of security and surveillance.

## D. GOALS AND OBJECTIVES

The primary goals and objectives of this innovative facial recognition system for real-time criminal detection are rooted in the pursuit of enhancing public safety, streamlining law enforcement processes, and contributing to the overall security of a nation. The overarching aim is to leverage cutting-edge technology, specifically artificial intelligence implemented through Python, to develop a robust and efficient system capable of swiftly and accurately identifying individuals with criminal records. By utilizing a meticulously maintained local watch list database, encompassing crucial details such as Unique-id, Name, Gender, Religion, and a comprehensive record of Crimes committed, the system aims to provide law enforcement agencies with a powerful tool for proactive crime prevention. Through the meticulous preprocessing and feature extraction of images obtained from surveillance cameras, the system strives to overcome challenges related to varying lighting conditions, facial expressions, and environmental factors, ensuring the accuracy and reliability of the face recognition process. The ultimate goal is to enable the system to promptly recognize and match the features of individuals in real-time, thereby distinguishing between known criminals and innocent individuals. Upon a positive match, the system will trigger an automatic notification to police personnel, furnishing them with all pertinent details, including the individual's identity, committed crimes, and the duration of surveillance. This seamless integration of technology and law enforcement is designed to optimize response times, facilitate prompt apprehension of criminals, and contribute to an enhanced level of security within the country. Through the accomplishment of these goals, the project aspires to exemplify the potential of advanced technologies in revolutionizing traditional crime-fighting methodologies and fostering a safer and more secure society.

## E. SOLUTION OVERVIEW

The development of a real-time facial recognition system for criminal detection, integrating advanced technologies and methodologies to enhance public safety and law enforcement efforts. The system comprises a comprehensive Local Watch List Database, where images and detailed profiles of known criminals within a specific country are stored. The process begins with the capture of a video stream from surveillance cameras, which is then converted into frames. Each frame undergoes a meticulous preprocessing phase to optimize image quality and address potential environmental challenges.

The heart of the system lies in the Feature Extraction stage, where Artificial Intelligence implemented using Python extracts relevant facial features from the preprocessed images. These features serve as unique identifiers for each individual and are crucial for subsequent matching against the stored features in the Local Watch List Database. The comparison is designed to be efficient and accurate, taking into account factors such as lighting conditions, facial expressions, and environmental variations.

When a face is successfully detected and processed in a frame, the system performs a feature comparison with the images in the database. If a match is found, indicating that the individual is a known criminal, an automatic notification is

triggered. This notification is promptly sent to police personnel, providing them with comprehensive details such as the Unique-id, Name, Gender, Religion, a record of Crimes committed, and the duration for which the individual was under surveillance. This immediate alert system aims to empower law enforcement agencies with timely information, facilitating quick and targeted responses to potential threats.

Conversely, if no match is found in the watch lists, the system categorizes the individual as innocent, ensuring that privacy and ethical considerations are upheld. The development of such a solution aligns with the broader goals of leveraging technology to improve crime prevention, streamline law enforcement processes, and contribute to the overall security and well-being of the community.

## II. LITERATURE REVIEW

Biometrics is coming from Greek words, Bio which means "life" and Metrics, which means "to measure". According to **[1]**, an editor from techtarget.com, biometrics is the measurement and statistical analysis of people's physical and behavioral characteristics. A security company uses this technology extensively for access control, identification, and authentication. A crime investigation team uses it in addition to that to identify people based on their physical characteristics or even their thumbprints, voiceprints, and faces. There are two main categories of biometric methods. Physical biometrics is the first type and is used for verification. This technique makes use of fingerprints, faces, hands, and eyes, but it is not restricted to just five senses because biometrics encompass a wide range of data. The second one is Behavioral Biometrics. It is used for identification and also verification process. This method looks at our behavior. Example of this method is a keystroke recognition and speaker identification.

Businesses including Facebook, Apple, ASUS, and the Federal Bureau of Investigation (FBI) as well as other large corporations have adopted facial recognition technology. Users can use it for a variety of purposes, including but not limited to locating, confirming, and examining an individual's face throughout a vast database of faces. In order to do facial recognition, an input image must first be read and pre-processed, removing any undesired elements from the face. The system then displays the image that matches the comparison between the image and the database.

The initial stage in creating a facial recognition system is face detection. Here, the face is detected by the system, which then decides if it is a human face or not. Additionally, it establishes if the system can tell the difference between the subject and the background, making face detection and recognition simple.

Eigenface, which employs an information theory technique to find the best matching or potential face information encoded in a set of faces that will best separate the faces, is likely one of the earliest and most successful algorithms created by [2]. It works by first collecting several images from the database and represent it as a vector, then the algorithm will find the average face vector or the mean and it will subtract the mean face from each sample faces. This is useful in order to find the distinguishable features from each image and it will then find the covariance matrix and it will select the best matching images.

It transforms the face images into a set of basis faces which essentially are the principal component of the face itself **[3]**. In order to minimize the computational effort, the primary components identify the directions in which representing the data is more effective.

Massive real-time applications that can simplify and streamline the conventional identification system are the driving force behind facial recognition research. The basic difficulties in face recognition serve as a source of motivation for the researcher. With its straightforward identifying process, facial recognition has become the main biometric technique. The technology became important since digital cameras were more widely available and security was needed more often. Facial recognition has several advantages over other biometric systems, including being user-friendly, natural, and nonintrusive [4].

The direct appearance model, active wavelet network, and component-based with 3D morphable models are the shape-based techniques for extracting facial features. Certain hybrid algorithms, including AdaBoost with shape constraints and elastic bunch graph matching, combine the best aspects of texture- and form-based techniques. This hybrid approach, in particular the AdaBoost method, is used for OpenCV-based face detection [5,6].

Numerous studies in the field of computer vision deal with the real-time detection and tracking of faces. A paradigm consisting of two tracking modes—short-range tracking mode and long-range tracking mode—was described in the research effort in [7]. Face scaling, rapid movements, and changes in stance are examples of unstable real-time face tracking scenarios that are handled by this model.

An algorithm for real-time head pose estimation was created by the authors in [8]. On mobile platforms, their suggested system has been put into practice. Three techniques are employed: an effective head posture estimation algorithm, color tracking, and Viola-Jones for face detection.

In real-time systems, the Viola-Jones and optical flow algorithms are frequently utilized. A real-time face tracker utilizing viola-Jones and Optical Flow algorithms was presented in the research study in [9]. The Viola-Jones algorithm's intermediate findings are used by the system to create a likelihood map.

Next, Optical Flow is used to extrapolate the likelihood map. A real-time camera-based face tracking technique was proposed in the research paper published in [10]. They extracted feature points using the Shi and Tomasi technique, tracked the stage using Optical Flow, then detected the facial object using Haar-like characteristics.

## III. REQUIREMENT ANALYSIS

The project involves real-time facial recognition for identifying criminals using a surveillance camera's video stream. It has a local watch list database with pictures and information on criminals from a certain nation, such as their Unique-id, name, gender, and crimes committed. The system preprocesses images and extracts features using Artificial Intelligence implemented in Python. Video frames are captured from the surveillance camera, and when a face is detected, it undergoes preprocessing, and its features are compared with those stored in

the watch list database. If a match is found, a notification with details is sent to the police personnel, indicating the time under surveillance. If no match is found, the individual is considered innocent.

Your project idea involves building a real-time facial recognition system for detecting and recognizing faces of criminals in a video stream obtained from a surveillance camera. Below are the functional requirements for the project:

A. FUNCTIONAL REQUIREMENTS:

***a)*** USER AUTHENTICATION AND ACCESS CONTROL:
- Implement a user authentication system to control access to the application.
- Define different user roles (e.g., admin, police personnel) with appropriate permissions.

b) WATCH LIST MANAGEMENT:
- Provide functionality to manage the local watch list database.
- Allow addition, modification, and deletion of criminal records.
- Include fields for Unique-id, Name, Gender, Religion, Crimes done, etc.

c) DATABASE INTEGRATION:
- Integrate a database system to store and retrieve criminal records.
- Implement efficient queries for fast retrieval of information during real-time recognition.

d) REAL-TIME VIDEO CAPTURE:
- Integrate functionality to capture a real-time video stream from surveillance cameras.
- Convert video frames into images for processing.

e) FACE DETECTION:
- Implement a face detection algorithm to identify and locate faces within each video frame.
- Use techniques like Haar cascades or deep learning-based methods.

f) REAL-TIME IMAGE PROCESSING:
- Preprocess the detected faces from the video stream before feature extraction.
- Ensure that the processing is optimized for real-time performance.

g) FACE RECOGNITION:
- Compare the extracted features of real-time faces with features stored in the watch list database.
- Implement a matching algorithm to identify potential criminal matches.

h) NOTIFICATION SYSTEM:
- If a match is found, send notifications to authorized police personnel.
- Include details such as Unique-id, Name, Gender, Religion, Crimes done, and the timestamp of the recognition.

i) LOGGING AND AUDITING:
- Log all recognition events, including successful matches and innocent individuals.
- Provide audit trails for system administrators to review system activities.

j) USER INTERFACE:
- Develop an intuitive user interface for system administrators and police personnel.
- Include features for managing watch lists, reviewing recognition events, and configuring system settings.

B. NON-FUNCTIONAL REQUIREMENTS:

Never forget to iterate and develop the system regularly in response to user feedback and changing requirements. Think about the moral and legal ramifications of using facial recognition in surveillance systems as well.

Requirements that are not functional specify the characteristics or features that the system needs. For your real-time facial recognition system, the following non-functional conditions must be met:

a) PERFORMANCE

There should be little latency in the system's real-time processing of video frames.

The facial recognition system needs to yield precise outcomes in a fair amount of time.

b) SCALABILITY:

A growing number of watch list entries and concurrent recognition requests should be supported by the system.

It ought to accommodate expanding database volumes without seeing a notable decline in efficiency.

c) RELIABILITY:

The system must be always on and functioning to provide constant monitoring.

d) ACCURACY:

A high degree of accuracy in detecting offenders should be possessed by the face recognition algorithm. Reduce false positives and negatives to improve the system's dependability.

e) SECURITY:

Ensure the watch list database's integrity and secrecy. Establish access restrictions to prevent unauthorized individuals from accessing confidential data. When sending notifications, make use of secure communication methods.

f) PRIVACY:

Respect the rules and laws pertaining to the use of face recognition technology. Put in place privacy protections to shield the identities of people who are innocent but were caught in the video stream.

g) USABILITY:

System administrators and law enforcement staff should find the user interface to be simple to understand and easy to utilize. Offer succinct and lucid notifications along with pertinent information to facilitate prompt decision-making.

h) MAINTAINABILITY:

There should be little downtime for updates or maintenance tasks, and the system should be simple to maintain. Use well-documented, modular code to make future updates easier.

i) COMPATIBILITY:

Ensure that the product is compatible with various types and configurations of security cameras. Assist various browsers and OS systems when necessary.

*j)* RESPONSE TIME*:*

Specify acceptable times for the extraction of features, recognition, and face detection.

Provide a support system to resolve problems and respond to inquiries from users.

m) COST:

- Define and manage the total cost of ownership, including initial development, maintenance, and hardware costs.
- Optimize costs while meeting all functional and non-functional requirements

n) USER SATISFACTION:

- Collect feedback from system administrators and users to assess user satisfaction.
- Iterate on the system based on feedback to improve user experience.

Aim for a prompt reaction to matches that are found in order to enable law enforcement to act promptly.

k) AUDITABILITY:

Keep thorough records of all system operations for the purpose of auditing. Keep track of pertinent data, such as system modifications, user activities, and recognition events.

l) TRAINING AND SUPPORT:

Give system administrators and users training materials and documentation.

By addressing both functional and non-functional requirements, you can ensure the development of a robust, reliable, and ethical real-time facial recognition system.

## IV. SYSTEM DESIGN

In our Criminal Detection System project, our meticulous planning revolves around enabling law enforcement agencies to efficiently identify and track criminals, ultimately bolstering public safety. Through the design of user, admin, and employee modules, we ensure seamless collaboration and information sharing among personnel. Our primary aim is to create a reliable, secure, and user-friendly system, emphasizing secure data storage, scalability, and effective use of technologies like Python, Node.js, and React Native. This design phase serves as the bedrock for a sophisticated and community-centered solution to combat crime effectively.

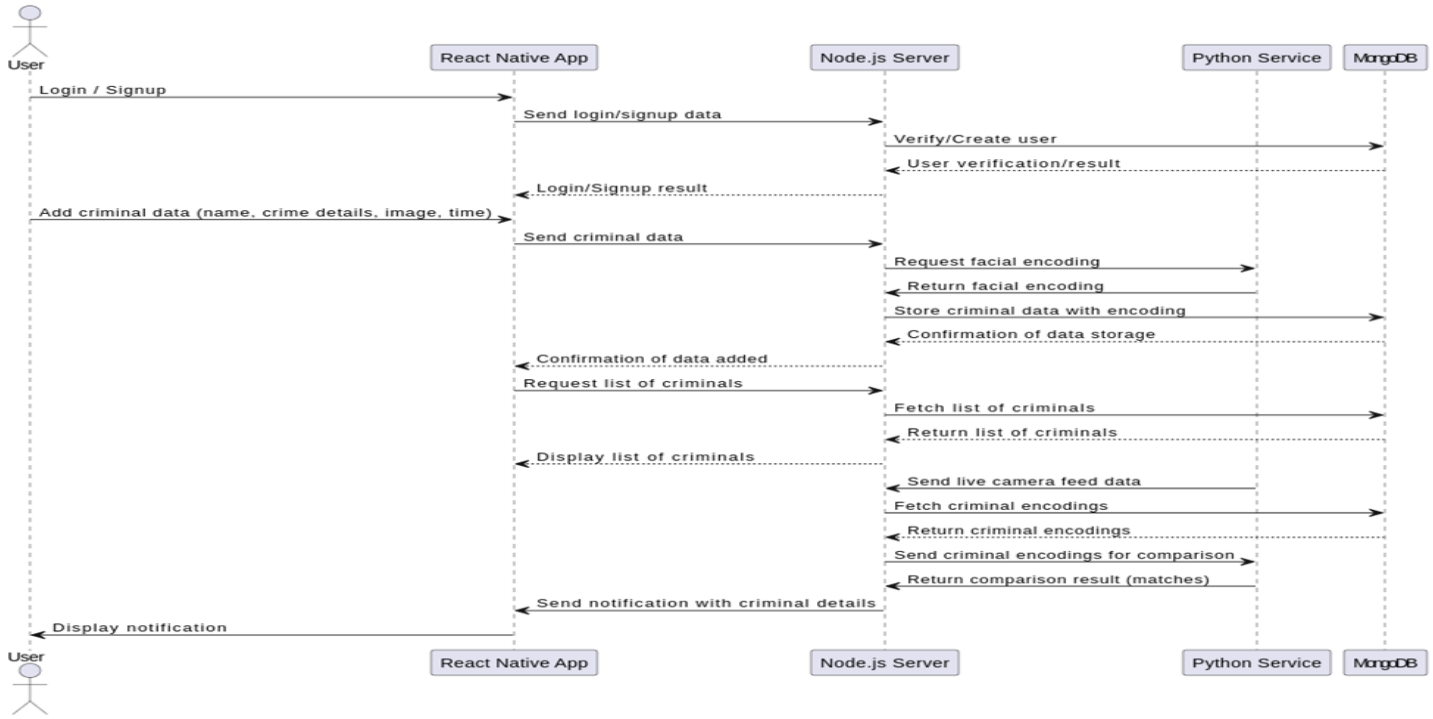


**FIGURE 1.** SEQUENCE DIAGRAM

The Figure 1 shows a sequence diagram for the criminal detection system outlines the interaction flow between the user, React Native app, Node.js server, Python service, and MongoDB. When a user logs in or signs up, the React Native app sends the credentials to the Node.js server, which verifies or creates the user and returns the result When criminal data is added, the app sends this data to the server, which requests and stores facial encodings via the Python service and MongoDB. The server confirms the data storage and returns the list of criminals upon request. For live camera feeds, the app sends data to the server, which processes it through the Python service to fetch and compare facial encodings, ultimately sending notifications back to the user if matches are found.

The Figure 2 show a architecture diagram of the criminal detection system consists of several interconnected components. At the core is the Node.js server, which serves as the central hub for communication and data processing. The React Native app allows users to login, sign up, add and display criminal data, and receive notifications. The camera feed component captures live video and sends video streams to the Python Facial Recognition module. This module encodes facial images and processes live camera feeds, sending detected facial data to the Node.js server. The server interacts with MongoDB to store and fetch criminal data and facial encodings. Finally, the system can compare facial encodings and notify matches, completing the detection loop.

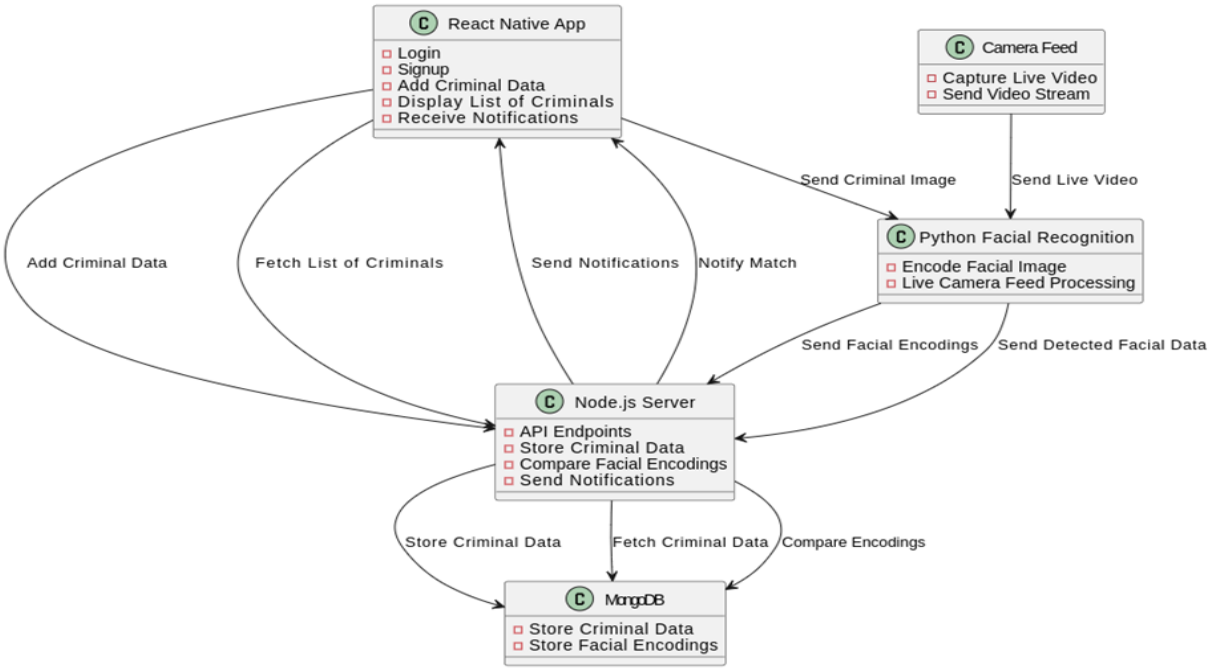


**FIGURE 2.** ACITIVITY DIAGRAM

## V. PSEUDO CODES/FLOW CONTROL

Flow charts are diagrams used in software design to show how to handle tricky parts of a program. Pseudo code is a casual way to explain how a program works using plain language and math. Unlike real programming languages, you don't need special software to write pseudo code. It's just like writing in English, but it helps to explain how an algorithm works. Basically, flow charts show how to solve a problem, while pseudo code explains how an algorithm works without using strict programming language rules.

### A. AUTHENTICATION PSEUDO CODE

Start
Open App
Sign Up Screen Appears
Create an account
If
Information is Verified
Than
Successfully registered
Else
Set error
After successful registered
Login Screen Appears
Insert your login credentials
If
Credentials match
Then
Main Screen appears
Else
Set error
Show Error message
Stay on Login Screen
End

### B. App Activity

Start
Authentication Successful
Main Activity Appears
User will get notified when the image is seen in any camera
End

### *C. Components*

In programming and engineering domains, a component refers to a discernible part of a larger program or structure. Typically, a component is responsible for performing either a single function or a group of interconnected functions. In software design, a system is divided into components, each comprising various modules. In table 1 some components of criminal detection system with their descriptions are mentioned. Component testing involves verifying the functionality of all interconnected modules within a component to ensure its cohesive operation.

**TABLE 1** COMPONENTS OF CRIMINAL DETECTION SYSTEM

| Components | Description |
|---|---|
| **Authentication** | First of all, all users of can register themselves in application |
| **Login** | User can login in the app |
| **Alerts** | User will receive alerts when the image is seen in the cameras on which the python programming is enabled |
| **Student Meeting** | Student can join meeting. |
| **Student Portal** | Student can use multiple options as per required. |
| **Exam** | Teacher can submit exams and student can take that exam. |
| **Notes** | Teacher can upload notes and student can download notes. |

### D. WEB SERVICES

A web services is a software segment that is considered to complete a set of particular task.in mist calculating, web services can be originating and appealed over the internet. In table 2 the description of nodeJS web server is given which is used in the criminal detection sysytem The client that appealed the web service would be able to obtain functionality from the web service.

**TABLE 2** WEB SERVICES OF CRIMINAL DETECTION SYSTEM

| Web Service | Description |
|---|---|
| **NodeJS server** | We have developed the server when the python script found the desired data in cameras a message is send to the server which directs a notification for the app. |

### E. LIBRARIES

A library is a gathering of non-volatile assets used by processer program, most regularly for software development, in computer science. Conformation data, certification, help data, note templates, pre-written code and subroutines, classes, values, and type conditions are some instances. Table 3 shows the libraries used in criminal detection system.

**TABLE 3** LIBRARIES USED IN CRIMINAL DETECTION SYSTEM

| Libraries | Description |
|---|---|
| **NodeJS Authentication** | We are using NodeJS server for authenticating the user and creating accounts on the mobile application |
| **Activity Component** | The Activity component represents a single screen with a user interface that users can interact with. Activities are responsible for handling user input, managing the app's state, and displaying content to the user. |
| **Python Script** | We are using python script for implementing machine learning as a component to detect humans using cameras it will direct the camera for a specific person and when it shows on camera it will display the message to the server |

| | |
|---|---|
| **NodeJS Server** | We are using NodeJS server as the admin panel for our system that will authenticate users and also directs the notifications to the mobile application related the discovery of human on camera. |
| **React Native** | React Native framework is used to create the mobile application for cross platforms (android, iOS) |
| **Android Studio** | Android studio is used to build and run android applications |

## VI. ACHIEVEMENTS AND IMPROVEMENTS

Our real-time criminal face recognition project has made great progress toward improving law enforcement and public safety. Our solution is able to identify and recognize known offenders' faces in real-time video streams by fusing state-of-the-art artificial intelligence technologies with surveillance camera systems. Our face recognition algorithms are now more accurate and efficient thanks to careful preprocessing and feature extraction methods.

Furthermore, our research has made good use of a centralized local watch list database that holds detailed information about criminals across the nation, such as their criminal histories, demographics, and unique identifiers. We have expedited the detection of those with a criminal history by using this database as a reference for comparison during facial recognition, allowing for prompt intervention by law enforcement authorities.

One of the key achievements of our project lies in its ability to seamlessly integrate with existing surveillance infrastructure, thereby augmenting the capabilities of security systems across various public and private sectors. By providing real-time notifications to police personnel upon detection of a match with a known criminal, our system enables proactive intervention, potentially preventing crimes and enhancing overall public safety.

While our project has achieved commendable success in real-time criminal face recognition, there are several areas where further improvements can be made to enhance its functionality and efficacy. Firstly, there is a need to continually update and expand the local watch list database to include newly identified criminals and update information on existing ones. This can be achieved through collaboration with law enforcement agencies and integration with national databases for comprehensive coverage.

Secondly, to improve the accuracy and reliability of face recognition, ongoing refinement of preprocessing techniques and feature extraction algorithms is essential. This involves optimizing parameters such as image resolution, noise reduction, and feature selection to ensure robust performance across diverse environmental conditions and facial variations.

Furthermore, incorporating advanced machine learning models and deep learning architectures could potentially enhance the system's ability to handle complex scenarios, such as occlusions, varying poses, and changes in lighting conditions. By training the model on large-scale datasets and implementing techniques such as transfer learning, we can further improve the system's generalization and adaptability.

## IX. CRITICAL REVIEW

One of the primary criticisms revolves around privacy implications and the potential for misuse of facial recognition technology. Critics argue that mass surveillance using facial recognition algorithms infringes upon individuals' rights to privacy and freedom of movement, raising concerns about the creation of a surveillance state and the erosion of civil liberties. Additionally, there are apprehensions regarding the disproportionate impact of facial recognition on marginalized communities, with studies indicating higher error rates for individuals with darker skin tones and facial features that deviate from the algorithm's training data.

Moreover, the accuracy and reliability of facial recognition systems have come under scrutiny, with reports of false positives and misidentifications leading to wrongful arrests and unjust outcomes. The inherent biases present in facial recognition algorithms, stemming from biased training data and algorithmic design choices, exacerbate these concerns and undermine the system's fairness and impartiality.

Another critical aspect is the lack of transparency and accountability surrounding the deployment of facial recognition technology. There is often limited oversight and regulation governing its use, raising questions about accountability mechanisms, data security practices, and potential misuse by law enforcement agencies or other entities. Concerns have been raised about the lack of informed consent and the opaque nature of data collection and retention policies, leading to fears of surveillance creep and mission creep.

Furthermore, there are technical challenges and limitations inherent in facial recognition technology, including its susceptibility to variations in lighting conditions, facial expressions, and occlusions. These factors can impact the system's accuracy and reliability, particularly in real-world scenarios with dynamic environmental conditions and diverse facial characteristics.

## VIII. FUTURE RECOMMENDATIONS/OUTLOOK

- Implement comprehensive regulatory frameworks to govern the ethical and responsible deployment of facial recognition technology, including guidelines for data privacy, transparency, and accountability.
- Conduct thorough and ongoing audits of facial recognition algorithms to identify and mitigate biases, ensuring fairness and equity in algorithmic decision-making.
- Invest in research and development to enhance the accuracy and reliability of facial recognition systems, particularly in addressing challenges related to variations in lighting conditions, facial expressions, and occlusions.
- Foster collaboration between stakeholders, including policymakers, technologists, civil society organizations, and affected communities, to develop inclusive and participatory approaches to facial recognition governance.
- Prioritize transparency and public engagement in the deployment of facial recognition technology, including

robust mechanisms for informed consent, stakeholder consultation, and independent oversight.

- Explore alternative approaches to public safety and law enforcement that prioritize community-based interventions, social services, and preventative measures, complementing the use of facial recognition technology.
- Promote education and awareness initiatives to enhance public understanding of facial recognition technology, its potential benefits, and associated risks, empowering individuals to advocate for their rights and interests.

Encourage interdisciplinary research and collaboration to address the broader societal implications of facial recognition technology, including its impact on privacy, civil liberties, and social justice.

## IX. CONCLUSION

Criminal Detection System is a milestone of success for using technology to revolutionize our security and police systems using the digital tool of Artificial Intelligence using Machine Learning. As their was a demand for a system that will boost the work security handling organizations. Image detection is becoming so much popular now a days. Therefore, using it to find the criminals is a good initiative. We can save our cost, time and workforce using Criminal Detection System. Using the technology we can modernize this system and the work load becomes shorter than the current traditional system we are using. By seamless integration of our criminal detection system in current traditional system we can make our system safer and easier to use for our security organizations. It will help them to solve cases and catch the criminals in a more efficient and advanced way. Discover the power of the Criminal Detection System, which uses machine learning to search through the cameras and locate the precise criminal faces that the user needs to locate. It will enable them to accomplish their aim much more successfully.

## REFERENCES


[1] Abdullah, N. A., Saidi, M. J., Rahman, N. H. A., Wen, C. C., & Hamid, I. R. A. (2017, October). Face recognition for criminal identification: An implementation of principal component analysis for face recognition. In AIP conference proceedings (Vol. 1891, No. 1). AIP Publishing.

[2] Aherwadi, N. B., Chokshi, D., Pande, D. S., & Khamparia, A. (2021, July). Criminal identification system using facial recognition. In Proceedings of the International Conference on Innovative Computing & Communication (ICICC).

[3] Elrefaei, L. A., Alharthi, A., Alamoudi, H., Almutairi, S., & Al-rammah, F. (2017, March). Real-time face detection and tracking on mobile phones for criminal detection. In 2017 2nd International Conference on Anti-Cyber Crimes (ICACC) (pp. 75-80). IEEE.

[4] Chevelwalla, A., Gurav, A., Desai, S., & Sadhukhan, S. (2015). Criminal face recognition system. International Journal of Engineering Research & Technology (IJERT), 4(03), 2278-0181.

[5] Ratnaparkhi, S. T., Tandasi, A., & Saraswat, S. (2021, January). Face detection and recognition for criminal identification system. In 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 773-777). IEEE.

[6] Ratnaparkhi, S. T., Singh, P., Tandasi, A., & Sindhwani, N. (2021, September). Comparative analysis of classifiers for criminal identification system using face recognition. In 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 1-6). IEEE.

[7] Kumar, M. R. P., Majeed, A., Pasha, F., & Sujith, A. (2020). REAL-TIME CRIMINAL IDENTIFICATION SYSTEM BASED ON FACE RECOGNITION. V26, (05).

[8] Kumar, K. K., Kasiviswanadham, Y., Indira, D. V. S. N. V., & Bhargavi, C. V. (2023). Criminal face identification system using deep learning algorithm multi-task cascade neural network (MTCNN). Materials Today: Proceedings, 80, 2406-2410.

[9] Babu, A., Thomas, A. K., & Dhanya Chacko, S. (2021). Criminal Face Detection System. NAIVIGYAN, 6.

[10] Mittal, N., & Singh, R. (2022). Criminal identification system using face detection with artificial intelligence. In Blockchain Applications for Healthcare Informatics (pp. 421-430). Academic Press.

[11] Naik, A., Basukala, R., Tiwari, S., & Asha, H. V. (2019). Criminal identification using facial recognition.

[12] Kumar, A., & Gupta, R. (2023). Futuristic study of a criminal facial recognition system using open-source images.

[13] Randhir, K. P., Ramesh, O. S., Sanjay, L. S., Gangadhar, K. G., & AP, S. AUTOMATED CRIMINAL IDENTIFICATION SYSTEM USING FACE DETECTION AND RECOGNITION.

[14] Gupta, A., Punj, D., & Pillai, A. (2022). Face Recognition System Based on Convolutional Neural Network (CNN) for Criminal Identification. In Mobile Radio Communications and 5G Networks: Proceedings of Second MRCN 2021 (pp. 21-33). Singapore: Springer Nature Singapore.

[15] Kim, H., Choi, N., Kwon, H. J., & Kim, H. (2023). Surveillance System for Real-Time High-Precision Recognition of Criminal Faces from Wild Videos. IEEE Access.

[16] Railkar, Y., Pawar, S., Pise, R., Nasikkar, A., & Patil, P. (2024, March). Criminal Recognition System. In 2024 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 1-6). IEEE.

[17] Sandhya, S., Balasundaram, A., & Shaik, A. (2023). Deep Learning Based Face Detection and Identification of Criminal Suspects. Computers, Materials & Continua, 74(2).

[18] Chaitanya, A. K., Kartheek, C. H., & Nandan, D. (2020). Study on real-time face recognition and tracking for criminal revealing. In Soft Computing: Theories and Applications: Proceedings of SoCTA 2019 (pp. 849-857). Springer Singapore.

[19] Ullah, U., & Ullah, A. (2022). An evolutionary algorithm for the solution of multi-objective optimization problem. International Journal of Advances in Applied Sciences, 11(4), 287-295.

[20] Udgaonkar, S. (2021). Criminal Identification Using Face Recognition. Available at SSRN 3901729.

[21] Nawara, J. (2010). Machine learning: face recognition technology evidence in criminal trials. U. Louisville L. Rev., 49, 601.

[22] Singh, P., Gupta, S., Gupta, V., Kuchhal, P., & Jain, A. (2022). Face Recognition–Based Surveillance System: A New Paradigm for Criminal Profiling. Digital Forensics and Internet of Things: Impact and Challenges, 1-18.