Khatik Huzaifa Mohammad Aarif, 2026, 14:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Criminal Face Detection

Khatik Huzaifa Mohammad Aarif[1], Dr. Jasbir Kaur[2], Prof. Sandhya Thakkar[3]
Master of Computer Applications (MCA Course), Guru Nanak Institute of Management Studies, Mumbai, India[1]
Director, Head of IT, Guru Nanak Institute of Management Studies, Mumbai, India[2]
Assistant Professor, Guru Nanak Institute of Management Studies, Mumbai, India[3]

Abstract- Criminal face detection is a critical aspect of law enforcement and public safety. This project explores the application of machine learning and computer vision techniques to identify potential criminal faces from images. The methodology involves preprocessing image data, extracting facial features using deep learning models like Convolutional Neural Networks (CNNs), and implementing facial recognition algorithms .The project utilizes popular Python libraries such as Open CV , Tensor Flow, and Keras to train and deploy the models. Additionally, a dataset comprising diverse facial images is employed for model training and evaluation. The trained model's performance is assessed using metrics such as accuracy, precision, recall, and F1 score. Results demonstrate the feasibility of using machine learning algorithms to detect potential criminal faces with a certain degree of accuracy. Ethical considerations regarding biases in data and implications of using such technology in law enforcement are discussed. Further research directions are suggested to enhance the robustness and fairness of criminal face detection systems. This abstract provides a high-level overview of the project's objectives, methodologies, findings, and potential ethical considerations without getting into specific code implementations or technical details.

Keywords— machine learning, face recognition, CCTV, CNN , Open CV , Keras.

I. INTRODUCTION

In today's modern world, national security is a big concern, and security especially at airports is a major issue to be addressed as airports are often the transit points for crimes like drug trafficking, transnational organized crime, and acts of terrorism. Most of the criminals involved in such cases have a past criminal record. Thus, making a

system that can recognize a criminal or a person with past criminal records can help airports provide a safer environment for passengers. However, the detection of faces from complex backgrounds and recognizing those faces is challenging. Traditionally, manual techniques have been used for this purpose. These techniques involve security surveillance, pass-port verification at boarding counters etc[2].
Throughout the years, tracking down a criminal has been a difficult process. Earlier, the entire method consisted of leads based on evidence found on the crime scene. Biological evidence can be easily tracked down. However, criminals have evolved and are smarter than ever in terms of covering tracks and not leaving behind any kind of traceable evidence.Face recognition and detection come into play here. The face is significant for human identity and due to its distinguishable nature, every face is unique. Face recognitionfor criminal identification is one of a kind biometric technique that possesses the merit of high accuracy and low intrusiveness. It is a technique that uses the person's face to automatically detect and verify their identity from videoframes or images.

The face identification system presented in this paper is a unique combination of the best techniques available today for face detection, feature extraction and finally classification. The deep learning methods like MTCNN for detection and FaceNet for embeddings have previously beenproven to be elegant and state of the art.

Automatic face recognition is a method where the system extracts meaningful facial features such as the length of the nose or jawline, the distance

between the eyes, the color of the eye, etc. These features are useful for classification and performing matches with the database. There are two significant processes involved in this system: Detection and Identification. Face recognition triggers two major methods: training and evaluation. Training deals with feeding the algorithm with a sample of images model is trained on the training set. The evaluation phase of the face recognition compares the newly acquired test image with the already existing database [4].

II. RELATED WORK

System Design and Architecture

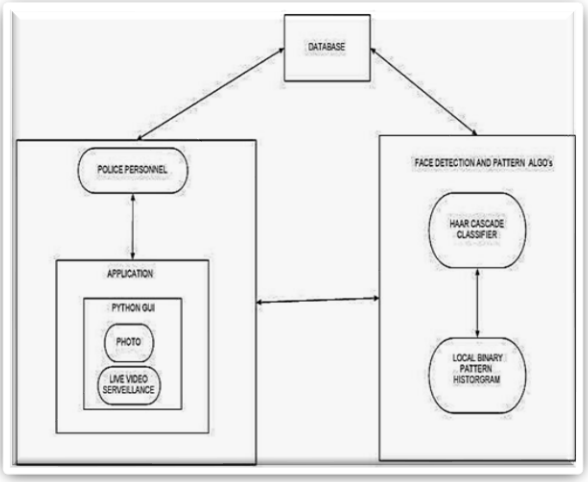

Figure 1 Proposed System Architecture

III. DATASET DESCRIPTION

The system consists of several components that work together to detect and identify criminals in video footage.

- Video Capture: This component captures video input from surveillance cameras or other sources.
- Face Detection: This component detects faces in video frames using deep learning or other techniques.
- Feature Extraction: This component extracts distinctive facial features from detected faces.
- Feature Matching: This component compares extracted facial features to a database of known criminals or suspects.
- Decision Module: This component evaluates matching scores and determines potential matches based on a matching threshold.
- Alert System: This component generates alerts for potential matches and notifies relevant personnel.
- Database: This component stores facial features of known criminals or suspects.

IV. PROPOSED METHODOLOGY

1. Use Case Diagram

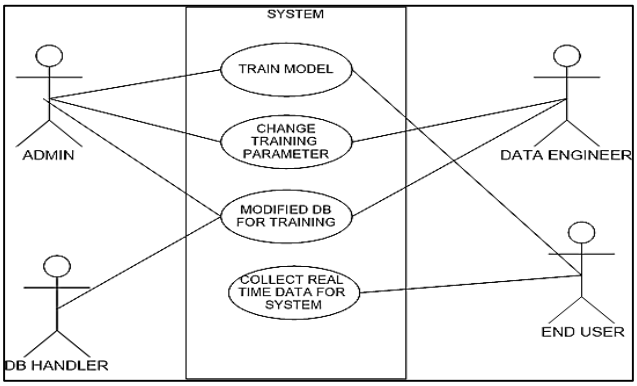

Figure 2 Proposed Use case diagram

The use case diagram for a Criminal Face Detection System represents the various futionalities and interactions of the system with different actors. Here's a detailed description:

Actors

Administrator: Responsible for system management, user access control, and database administration. Law Enforcement Officer: Uses the system to search, identify, and track criminals based on facial recognition.

System: Represents the criminal face detection system itself, comprising the software and hardware components.

Use Cases

Login: Both the Administrator and Law Enforcement Officer can log into the system using their credentials to access its functionalities.

Manage Database: The Administrator can add, delete, and update criminal face data in the system's database. This includes uploading images, entering descriptions, and marking individuals as wanted or identified.

Search Face: The Law Enforcement Officer can initiate a search by uploading a suspect's image or using a live feed. The system then compares this image against the database.

Match Face: The system matches the uploaded face with the stored criminal faces, identifying potential matches based on facial recognition algorithms.

Relationships

Administrator-Login-Manage Database: The Administrator logs in to manage the database, updating criminal face data.

Law Enforcement Officer-Login-Search Face: The Officer logs in to initiate face searches within the system.

System-Search Face-Match Face-Alert/Notify: These interactions depict the core functionalities of the system, where facial recognition algorithms compare uploaded faces with the database and alert officers about potential matches.

This diagram showcases how different actors interact with the Criminal Face Detection System, outlining the key functionalities they perform within the system to effectively utilize facial recognition technology for law enforcement purposes.

2. Data Flow Diagram

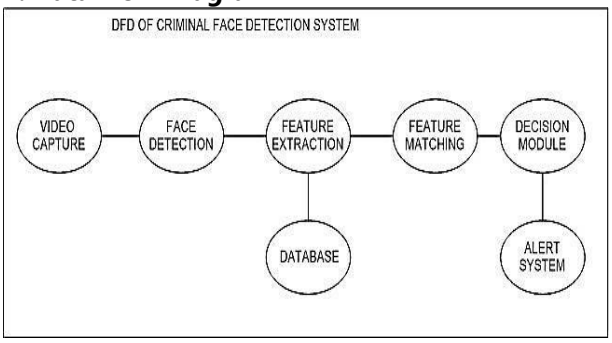

Figure 3 Proposed Data Flow Diagram

The Data Flow Diagram (DFD) for a Criminal Face Detection System illustrates the flow of data within the system components. It showcases the interaction between external entities like Law Enforcement Officers inputting facial data and a Criminal Database storing criminal face information. Processes such as the Face Recognition Algorithm compare uploaded faces with the database, triggering notifications to officers via an Alert System upon potential matches. Additionally, Data Management oversees the database updates, while Reporting generates usage and match reports. This diagram highlights how facial data moves between users, processes, and data stores, emphasizing the system's functionality in identification, notification, and reporting while maintaining administrative control and system oversight.

3. Sequence Diagram

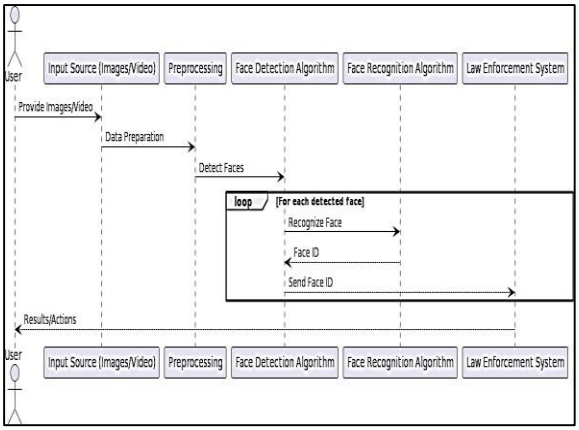

Figure 3 Proposed Sequence Diagram

The Sequence Diagram for a Criminal Face Detection System illustrates the sequential interactions between key components. The Law Enforcement Officer initiates the process by requesting facial recognition, triggering the Face Recognition System to compare the uploaded face with stored criminal data from the Database. Upon completion, potential matches are identified, and if found, the Alert System notifies the Officer. This interaction showcases the lifelines of the Officer, Face Recognition System, Alert System, and Database, depicting the flow of messages and actions over time. The diagram emphasizes the sequential flow of control and communication between these entities, elucidating

the process of facial recognition, match identification, and subsequent alert notification within the system.

V. EXPERIMENTAL RESULTS

1. Output Screen

Figure 4 Home page

Home page

This is the home page of our system , here we add criminal details and register there identity. Depending on the interface, there might be user interaction features, such as buttons or keyboard shortcuts for controlling the detection process, switching between different input sources, or saving

For effective face detection, users should ensure good lighting, a clear camera angle, and an unobstructed face. Keeping software updated, adjusting privacy settings, and being mindful of environmental conditions enhance the overall experience.

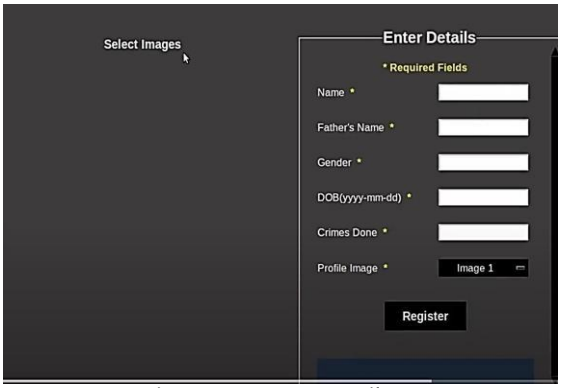

Figure 5 Enter Details

Selecting Images

This is the interface provided by the system for selecting an image for identification.

For optimal image selection from files, users should prioritize well-lit and clear images, ensuring they are unobstructed. It's beneficial to follow specific guidelines provided by the application or software. Additionally, keeping the software up-to-date and considering privacy settings can contribute to an enhanced and reliable image selection process. When selecting images from files, users should prioritize well-lit and clear visuals to ensure optimal quality. Unobstructed images, free from distractions, contribute to better results. Adhering to any specific guidelines or recommendations provided by the application or software enhances the selection process. Regularly updating the software not only ensures access to the latest features but also improves overall performance. Additionally, users should be mindful of privacy settings, striking a balance between convenience and safeguarding personal information during the image selection and storage process.

Figure 6 Detected Criminals

Detected Criminals

In This section we select the images from our file that we want to upload in our system ,As well as we can manage the data-files here. When choosing files for detection purposes, users should prioritize high-quality, well-lit images to ensure accurate and reliable results. Opt for files with unobstructed subjects, minimizing distractions to enhance detection capabilities. Adhering to specific guidelines provided by the detection application or software is crucial for optimal performance. Keeping

the software up-to-date ensures compatibility with the latest detection algorithms and improvements.

Additionally, consider privacy settings to ssensitive information within the selected files.

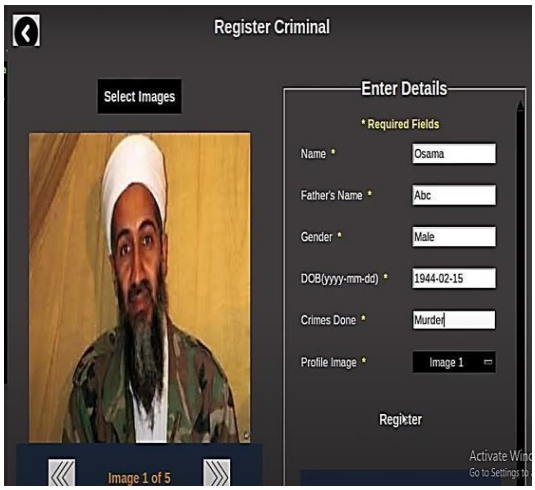

Figure 7 Register Criminal

In this section we are able to match face with our previous stored data, so it would identify the system detects the face from video footage.

When utilizing a system that employs a green rectangle for face detection and associates it with name identification, users should ensure they select well-lit images with clear visibility. Opt for files where faces are unobstructed, as this enhances the accuracy of the green rectangle's detection. Follow any specific guidelines provided by the system to achieve optimal results during the identification process. Regularly updating the system ensures it incorporates the latest advancements in face detection technology. Mindful consideration of privacy settings is essential to strike a balance between effective face detection and responsible handling of personal information linked to identified names within the system.

VI. CONCLUSION

Criminal face detection is a promising technology that has the potential to revolutionize crime prevention and investigation. However, it is important to carefully consider the feasibility of implementing this technology before investing significant time and resources.A thorough feasibility study is essential to assess the technical, operational, and economic feasibility of a criminal face detection project. This study should consider factors such as the accuracy of the technology, the integration with existing law enforcement systems, and the potential cost savings.

the feasibility study shows that the technology is organizations should proceed with a phased implementation plan. This plan should include a pilot phase to test the technology in a small area and gather feedback from users. The system should then be gradually rolled out to other areas as needed.

Criminal face detection is a powerful tool that can be used to improve public safety. However, it is important to use this technology responsibly and ethically. Organizations should carefully consider the benefits and risks of the technology before implementing it.

Acknowledgment
I would like to convey my gratitude to Prof. Sandhya Thakkar for sharing their pearls of wisdom with me during this work.

REFERENCES

1. Lamiaa A. Elrefaei1,2, Alaa Alharthi1,Huda Alamoudi1,Shatha Almutairi1,and Fatima Al-rammah Real-time Face Detection and Tracking on Mobile Phones for Criminal Detection .2nd International Conference on Anti-Cyber Crimes (ICACC) 26-27 March 2017.
2. W. Yimyam, T. Pinthong, N. Chumuang and M. Ketcham, "Face Detection Criminals through Cameras," 2018 14th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), Las Palmas de Gran Canaria, Spain, 2018, pp. 351-357, doi: 10.1109/SITIS.2018.00061.
3. S. Jagtap, N. B. Chopade and S. Tungar, "An Investigation of Face Recognition System for Criminal Identification in Surveillance Video," 2022 6th International Conference On Computing, Communication, Control And

Automation (ICCUBEA, Pune, India, 2022, pp. 1-5, doi: 10.1109/ICCUBEA54992.2022.10010987.

4. S. T. Ratnaparkhi, P. Singh, A. Tandasi and N. Sindhwani, "Comparative Analysis of Classifiers for Criminal Identification System Using Face Recognition," 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2021, pp. 1-6, doi: 10.1109/ICRITO51393.2021.9596066.
5. K. P. Teja, G. D. Kumar and T. P. Jacob, "Face Detection and Recognition for Criminal Identification," 2023 8th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2023, pp. 1431-1435, doi: 10.1109/ICCES57224.2023.10192845
6. J. Dhamija, T. Choudhury, P. Kumar and Y. S. Rathore, "An Advancement towards Efficient Face Recognition Using Live Video Feed: "For the Future"," 2017 3rd International Conference on Computational Intelligence and Networks (CINE), Odisha, India, 2017, pp. 53-56, doi: 10.1109/CINE.2017.21.
7. D. -Y. Huang, C. -H. Chen, T. -Y. Chen, J. -H. Wu and C. -C. Ko, "Real-Time Face Detection Using a Moving Camera," 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), Krakow, Poland, 2018, pp. 609-614, doi: 10.1109/WAINA.2018.00153.
8. 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, pp. 773-777, doi: 10.1109/Confluence51648.2021.9377205.
9. K. Sumathi, D. V. Sakthi, G. Nirmala, P. Sellamuthu, R. Walia and M. Usman, "IoT based Novel Face Detection Scheme using Machine Learning Scheme," 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2022, pp. 1-5, doi: 10.1109/ACCAI53970.2022.9752504