

# Criminal Face Detection

Prof. Sagar Badjate

Dept. Of Information Technology

SVKM'S IOT

Dhule, India

[Sagarbadjate@gmail.com](mailto:Sagarbadjate@gmail.com)

Bhupendra Pawar

Dept. of Information Technology

SVKM'S IOT

Dhule, India

[pawarbhupendra2002@gmail.com](mailto:pawarbhupendra2002@gmail.com)

Chetan Khairnar

Dept. of Information Technology

SVKM'S IOT

Dhule, India

[khairnarchetan62@gmail.com](mailto:khairnarchetan62@gmail.com)

Zaid Ansari

Dept. Of Information Technology

SVKM'S IOT

Dhule, India

[ansarizaid01@gmail.com](mailto:ansarizaid01@gmail.com)

Prathamesh Raghuvanshi

Dept. of Information Technology

SVKM'S IOT

Dhule, India

[raghuvanshipratham773@gmail.com](mailto:raghuvanshipratham773@gmail.com)

**Abstract** — One of the areas where criminal face recognition is important is in ensuring law and order and public safety. To do this, this research used computer vision and machine learning techniques to identify potential criminal faces in an image. The process involved pre-processing the image data, using a face extractor deep learning model, Convolutional neural networks, to extract facial features and applying facial recognition algorithms. The project uses Python libraries, including Tensor Flow, Open CV, and Keras, to train and make inferences from the model. Lastly, the face extractor deep learning model is trained and tested with a dataset of face photographs. Performance metrics such as recall, accuracy, precision, and F1 score are used to evaluate the trained model. The inference indicates that it is possible to have an accurate model identifying potential criminal faces. Finally, the article also raises the issue of the use of data technologies in law enforcement and their ethical consequences of their use and the potential bias in the data. To some extent, this can become the research subject since the robustness, and fairness of the criminal face detection algorithms may be rigorously tested at multiple stages in future streams of research. This abstract does not dive into specific code implementations or any technical jargon, but it lays out the project's goals, methodology, results, and potential ethical or legal issues.

**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. Biologicalevidence 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 important for defining human identity, and each face is distinct because of this. A unique biometric technology with great accuracy and minimal intrusiveness is face recognition for criminal identification. It is a method that automatically recognizes and confirms a person's identity from still photos or video frames by using their face. This work presents a novel face identification system that combines the state-of-the-art methods for face detection, feature extraction, and classification. Previous research has demonstrated the elegance and state of the art of deep learning techniques like FaceNet for embeddings and MTCNN for detection.

The process of automatically recognizing faces entails the system extracting important features from the user's face, like eye color, eye distance, nose length, jawline, etc. These traits have applications in both classification and database matching. The identification and detection processes are two crucial functions of this system. Face recognition starts two key processes: training and evaluation. Giving the algorithm a sample of photographs to work with so it can be trained on the training set is the training procedure. Facial recognition assessment stage compares the newly acquired test image with the pre-existing database.

## II. LITERATURE SURVEY

The fundamental ideas of the criminal face detection system are reviewed in this section. Prior to anything else, we must comprehend the different elements that make up the face detection system used for criminal detection. Alternatively, we may claim that we will simplify the picture so that it can be compared to the criminal history or other data. The intricacy of the image captured by the CCTV or any other camera could not be eliminated in the past. The method employed was to build a multilinear structure based on a high order tensor and simulate the various components that contribute to face variations. conclusion: The research presented a novel idea on the usage of appearance factor, or the identity factor described by a tensor structure, in order to improve recognition systems, particularly for various kinds of the same faces appearing. Project Goal: The goal

of this project is to use previously obtained photographs to identify a person. The identifying process will be carried out using earlier photos of various people[2]. Project Scope: The image storage and database archiving are the only things covered by this project. The photographs kept in the database are checked with the available information when a person has to be identified. Project overview: The goal of this project is to locate offenders within any department that handles investigations. Here, the method is to use certain Criminal Face Identification System photos that we already have stored [4]. The offenders in our database are divided into numerous slices, such as eyes, lips, noses, and hairs, along with their details and corresponding photographs. In order to identify any criminals, eyewitnesses will see the photos or slices that display on the 11 screen. Using this information, we create the face, which may or may not match our images. These images are again recorded in another database record. We anticipate that any image that matches 99% of the others is simply the criminal context for

[5]. Any face may be readily designed to identify criminals with ease. A method called "criminal face detection" uses a person's facial traits to identify them. In order to identify suspects, track down offenders, and discourage crime, this technology is frequently employed in security and law enforcement applications. The three primary categories of criminal face detection techniques are feature-based, template-matching, and neural network techniques. Face features including the separation between the eyes, the contour of the nose, and the general form of the face are extracted using feature-based approaches. Then, faces can be identified or tracked using these traits. Although feature-based techniques can be highly accurate and are comparatively easy to use, they are not resistant to changes in face expression, illumination, occlusion, or posture[7]. Techniques for matching templates compare a face to a collection of recognized face templates. The face that most closely resembles the template is chosen. Although template-matching techniques can be computationally expensive and necessitate a huge library of templates, they are incredibly precise. Artificial neural networks are used in neural network techniques to train them to recognize faces. Even under difficult circumstances, neural networks can learn from vast volumes of data and perform exceptionally well at face detection[9]. Among the difficulties in criminal face detection include stance variation, variation in illumination, occlusion, and facial expression. The term "pose variation" describes the range of possible facial poses, including frontal, profile, and upside-down. The term "illumination variation" describes how lighting conditions can differ significantly, which can make precisely extracting features challenging. The term "occlusion" describes how faces might be obscured by glasses, hair, or other things, making it challenging to recognize them clearly. Facial expression is the idea that a person's expressions can alter their look, making them harder to recognize and detect. Applications for criminal face detection are numerous and include access control, monitoring, and criminal investigations. Face detection is a technique used by surveillance systems to locate and follow offenders in video footage. Technique Face detection is a face detection used by surveillance systems to spot and monitor offenders from the footage. Access control systems, on the other hand, have employed the facial detection Technique Face Detection in Reference to Facial Recognition [8]. Building to help restrict offenders from having access to several locations. A facial detection technique takes facial detection. One other instance is criminal investigation organizations using face detection in instances involving several occurrences. Proof to identifying suspects. Over the past few years, modern attribute tracking

techniques, effective template integration algorithms, and deep learning have been utilized to enhance facial detection. Data to extract knowledge by deep learning, a form of machine learning, using artificial neural networks. Previous face detection in the case of deep learning has been successful, exhibiting excellent results even in more challenging environments. Developments in criminal face detection.

### RELATED WORK

#### System Design and Architecture

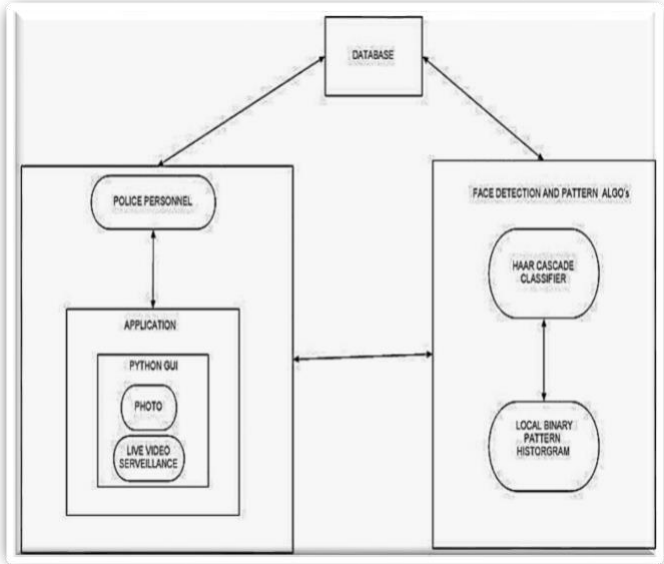


Figure 3.1 Proposed System Architecture

The system is made up of a number of parts that cooperate to find and identify criminals in video footage.

- Video Capture: Video input from security cameras and other sources is captured by this component.

- Face Detection: This part uses deep learning or other methods to identify faces in video frames.

- Feature Extraction: This part takes identified faces and extracts distinguishing traits from them.

- Feature Matching: In this step, extracted facial features are compared to a database of suspected or known criminals.

- Decision Module: Using a matching threshold as a guide, this module assesses matching scores to identify possible matches.

- Alert System: This part creates alerts for possible matches and sends out notifications to the appropriate staff.

- Database: This part keeps track of suspects' or known criminals' face traits.

## 5.1 USE CASE DIAGRAM:

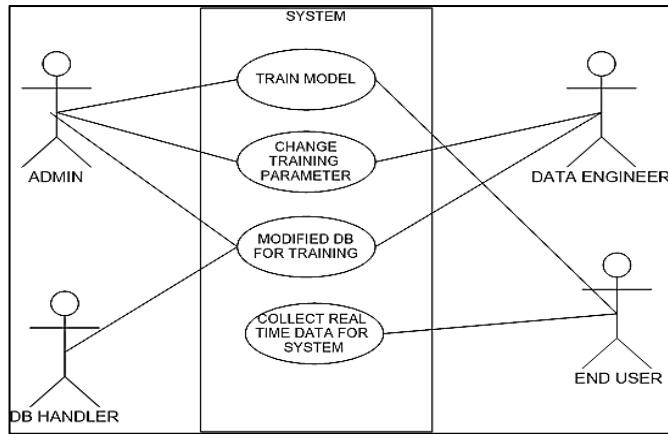


Figure 5.1 Proposed use case diagram

The use case diagram for A Criminal Face Detection System represents the various functionalities 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 could log in the software by using their information 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.

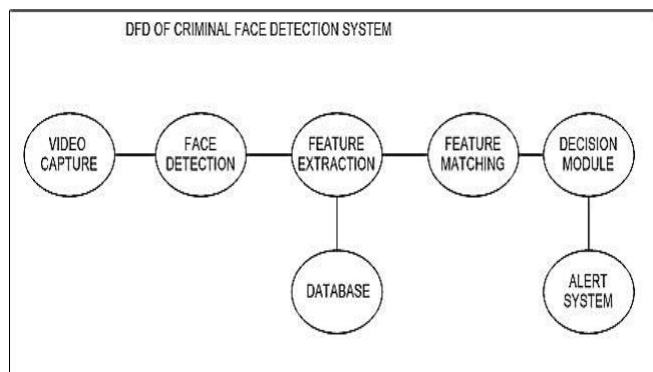
**Match Face:** The system matches the uploaded face with the stored criminal faces, identifying potential matches based on facial recognition algorithms.

**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.

## 5.2 Data Flow Diagram:



Figure 5.2 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.

## 5.3 Sequence Diagram

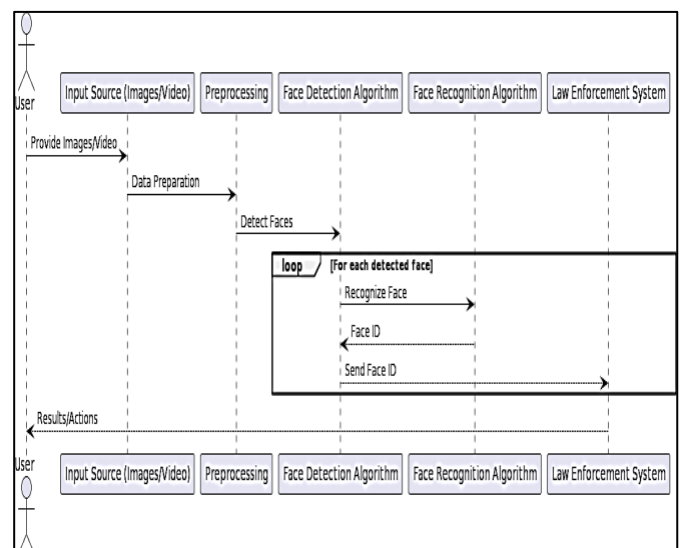


Figure 5.1 Proposed Sequence diagram

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.RESULTS AND DISCUSSION

6.1 Output Screen:

Figure 6.1 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.

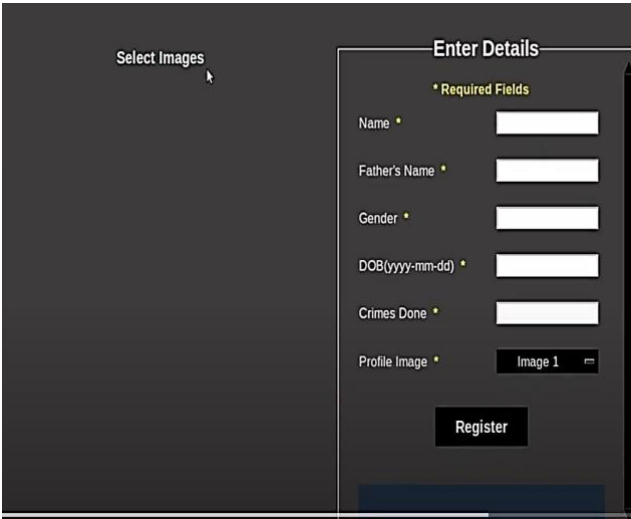


Figure 6.2 Enter Details

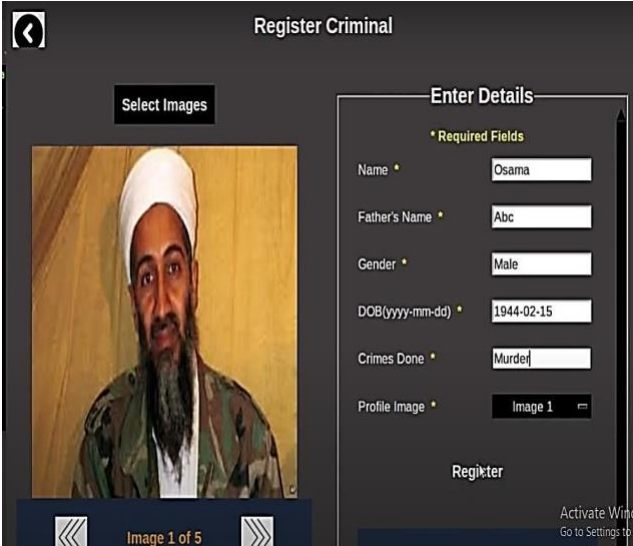


Figure 6.4 Register Criminal

In this section, we are able to do matching for the stored previous data with the face, so it would identify that the system detects the face from the video. Systems using green rectangle for face detection should always be used where a clear vision and clear, good lighting on the chosen image are in place. Use clear-faced files for better recognition by the green rectangle, and take instructions from the system on how to bring out images to have the best results after identification. Update the system regularly and acquire the new technology on identifying faces. Therefore, due consideration needs to be taken regarding privacy settings that establish the fine balance between better face detection and responsible personal information handling linked with identified names in the system.

VI. CONCLUSION

Criminal face detection is such a great technological innovation that it is surely going to change the very scenario of fighting and investigating crime. Therefore, one would surely like to take up the task of exploring technology implementation feasibility prior to investing any time or treasury into it. A comprehensive feasibility study helps one check whether or not a project for criminal face detection is technically sustainable, operationally workable, and financially feasible. The key factors in this study are the accuracy of the technology, how it will integrate with the current police systems, and potential cost savings. Feasibility study states that "technology is feasible and business should proceed to development plans in a gradual adoption," this may include pilot program to test technology in a small area with the availability of suggestion of user about technology. Then it could progressively be expanded to other localities should the need arise for the same, one of the useful technologies in increasing public safety is the criminal face detection software. Even then it is also greatly needed that this technology is used in a responsible and just manner. Under such a scenario, the companies involved have to balance the implications of using a sort of particular kind of technology limited locality to gather user feedback.

VII.ACKNOWLEDGMENT

We would like to convey our gratitude to Mr. Sagar Badjate for sharing their pearls of wisdom with us during this work.

SELECTING IMAGES:



Figure 6.3 Detected Criminals

DETECTED CRIMINALS

This portion allows us to control the data files and choose the photographs from our file to upload to our system. For the best result, quality and well-illuminated photos will be considered to use in detecting files. Eliminate distractors and choose those files with a clear subject to increase your performance while making detections. The best thing when you receive good results is by following each given instruction by the detection program or software. By updating the software, one gets to match the latest techniques of detection and improvements made. Keep in mind the sensitiveness of any private data with the chosen files' privacy settings.

## VIII. REFERENCES

- [1] Lamiaa A. Elrefaei<sup>1,2</sup>, Alaa Alharthi<sup>1</sup>, Huda Alamoudi<sup>1</sup>, Shatha Almutairi<sup>1</sup>, 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.

