

## Identification Of Criminals Using Face Recognition System

Aditya Maurya<sup>1</sup>, Ravi Prakash<sup>2</sup>, Ajay Kumar Maurya<sup>3</sup>

<sup>1</sup>M. Tech. Student, Department of Electronics Engineering, Uma Nath Singh Institute of Engineering and Technology Veer Bahadur Singh Purvanchal University Jaunpur, Uttar Pradesh

<sup>2,3</sup>Faculty, Department of Electronics Engineering, Uma Nath Singh Institute of Engineering and Technology Veer Bahadur Singh Purvanchal University Jaunpur, Uttar Pradesh

*Cite this paper as:* Aditya Maurya, Ravi Prakash, Ajay Kumar Maurya, (2025) Identification Of Criminals Using Face Recognition System. *Journal of Neonatal Surgery*, 14 (6), 595-602.

### ABSTRACT

The "Identification of criminals using face recognition system" is a cutting-edge facial recognition system created specifically to improve law enforcement operations by using facial recognition technology with the Indian government's Aadhar database. By automatically comparing the photos of those caught committing crimes with their Aadhar information, the project seeks to transform the identification and tracking of criminals.

By instantly comparing Aadhar records with surveillance photos, the method seeks to expedite criminal detection. It improves the accuracy of suspect identification by analysing and comparing facial traits with the vast Aadhar database using sophisticated algorithms. By providing law enforcement agencies with a dependable tool for quick responses to criminal situations while upholding privacy and ethical norms, this proactive strategy improves public safety.

**Keywords:** Aadhar, Crime Buster, Facial Recognition, Law Enforcement, Criminal Identification, Biometric Data, Surveillance, Public Safety, Real-Time Matching, Privacy and Ethics.

### 1. INTRODUCTION

For law enforcement authorities worldwide, identifying and tracking criminals is a difficulty. Although they are helpful in many situations, traditional identification techniques like DNA analysis and fingerprinting are not always enough to resolve difficult cases.

Facial recognition technology has emerged as a potent tool for person identification in a variety of domains, including criminal justice, in recent years [1].

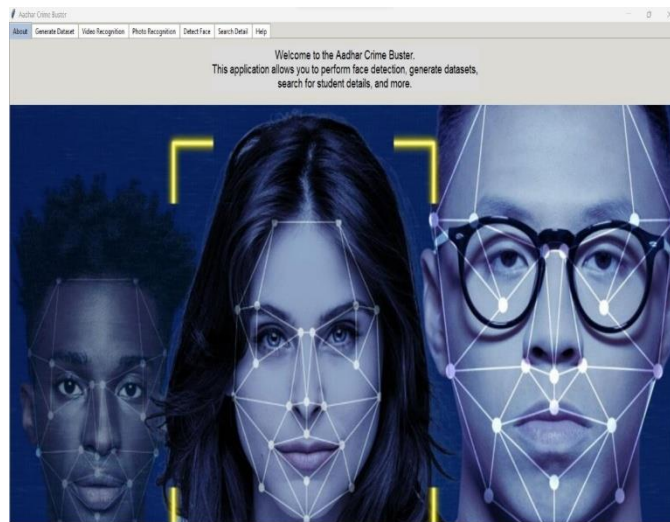
Detect criminals instantaneously or identify possible

offenders from a database of known offenders. When the live camera finds a match, alert the authorities. The system will recognize faces and compare them to a database of known criminals using sophisticated computer vision and machine learning algorithms.

In online mode, the system will analyze live cameras to find possible matches and promptly alert the authorities, while in offline mode, it will analyze photographs of known criminals and produce facial recognition information.

The system will be a crucial tool for law enforcement since it can process vast volumes of data fast and precisely.

Creating a powerful face recognition algorithm that can reliably identify faces in photos taken in a range of environmental settings and connecting it to the Aadhar database to allow for the real-time [4].



**Fig 1: - Proposed Model**

The implementation of the facial recognition system in operational settings and the provision of training to assist staff in using it while addressing ethical issues pertaining to data security, privacy, and matching of suspected faces with their UIDAI records.

Create and design an intuitive user interface so that law enforcement officers can access and use the face recognition system effectively. Thorough testing and validation should be done to guarantee the system's correctness, dependability, and performance in a variety of situations and potential biases in the technology will guarantee that the system is used responsibly and ethically.

## 2. PROPOSED SYSTEM

The Local Binary Pattern and Histogram algorithm (LBPH) for face identification and Haar cascade for face detection form the foundation of the suggested facial recognition system [2].

The quickest and most straightforward method for creating a GUI application [1] is to use the Python module Tkinter to generate the Graphical User Interface (GUI) for this system. traits like collecting pictures of people and entering their information into a database, like the Aadhar database, training the photos in the database and on the camera, and tracking suspects based on their facial traits are all functions that this system will offer.

### 2.1 Components

**Dataset:** Since it contains all of the biometric data required to identify an individual, the database is a crucial component of the facial recognition system. Our system's database is made to effectively and safely handle a lot of [3] photos and their associated metadata, which includes the timestamp, location, and other technical details of the photos.

To make it easier and faster to get and view a large number of suspiciously taken photographs, this dataset will include the images in a structured style.

#### Hardware components:

- Camera Video Input i.e. CCTV device or recorded videos for testing.
- Processing unit i.e. Server system or Laptop for testing.
- Storage device i.e. Cloud systems or local storages like Hard Drives.

#### Software components:

- Haar cascade, Machine Learning Model for image recognition.
- Local Binary Pattern and Histogram algorithm for Image Processing and extracting facial features.

## 3. METHODOLOGY

### a) Image Collection or Capture procedure:

Twenty pictures of each individual will be shot with high-speed cameras for testing purposes during the Aadhar generation or upgrading procedure. To offer thorough information for precise identification, photos will be taken under various lighting conditions and from various perspectives.

#### b) Normalization or preprocessing of images:

To guarantee consistency, images are pre-processed before being stored. This could entail brightness and contrast equalization, grayscale conversion, and scaling.

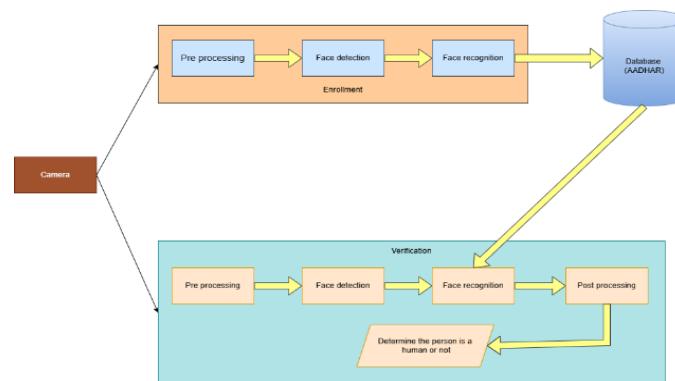
**Algorithm:** In the form of Pseudo Code.

**Input:** Live or recorded video feed of the persons.

**Output:** In Suspect file in excel sheet format.

#### Steps or Procedure

1. Transform each frame from Red Green Blue (RGB) to grayscale format.
2. Apply the Haar Cascade classifier for face detection and get the Region of Interest (ROI) which identifies the areas in the image containing facial features.
3. Now apply the LBPH algorithm on the ROI to get extract the facial features information.
4. Post Processing: if – feature matches with the criminal profiles from Adhar record then information goes to suspect excel file and authorities get alert, else process continues for next ROI (picture) and so on.



(Data Flow Diagram)

#### a) Face detection and pre-processing:

The frame is first converted from RGB colour to grayscale. We employed a Haar cascade classifier, which is suggested in, to identify the faces. This classifier trains a cascade function to identify input features [9]. Haar characteristics including edge, line, and four-rectangle are used for this. Many calculations and characteristics are required for huge or variable-sized images, and the majority of them are pointless [10]. Following that, the Region of Interest (ROI), or the area with faces, is extracted and moved on to the following phase.

#### d) Recognition of Faces:

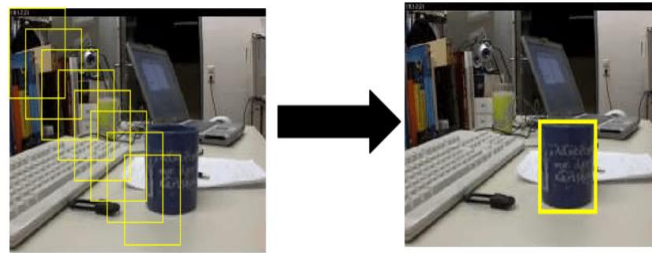
Because the LBPH method is robust, can identify both front and side faces, and outperforms other tools like Eigenfaces and Fisher faces, we choose to utilize it for face recognition [4].

It makes use of the sliding window concept with the neighbours, radius, and settings. It is showed in Fig. 3.

The LBPH algorithm is used to identify the features that best represent a face/object in an image [7]. It is a simpler method in that it efficiently classifies the image and performs better in various lighting and environmental circumstances [11].

Local Binary Pattern (LBP) operation creates an image which highlights the characteristics of ROI

(Region Of Interest) in a better way. It uses the concept of the sliding window with the parameters, radius and neighbours [8].



**Fig 3: - (Sliding window for object detection)**

First, we convert the frame into matrices of  $3 \times 3$  pixels. If a neighbour pixel in a matrix is greater than the median pixel of that matrix then set value 1 else 0 in that pixel position. Now note down the values of neighbour pixels in a line we get a binary number convert that binary number to decimal number and replace it with the median pixel value of the matrix. An image that better illustrate the features of ROI is produced by the local binary pattern (LBP) [11].

We take the histograms from each grid and concatenate them to create a new, larger histogram since the image has now been converted to LBP form. The original image's properties are shown by the concatenated histogram. The facial image from the database is represented by each histogram. The aforementioned procedures are followed for the new image, and a new histogram is obtained [13].

#### e) Post-processing

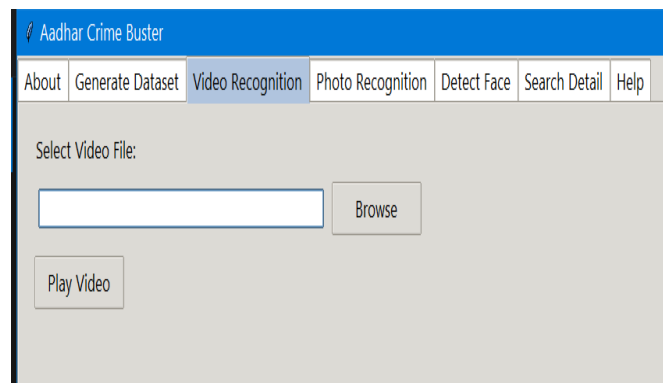
In order to identify the person in the picture, it now compares the new histogram with the histograms from the training dataset (using Euclidean distance). It selects the histogram with the least distance, because they are preferable [12]. It also extracts the ID associated with that histogram.

- **If-** confidence is more than 74% then details belong to the extracted ID is shown on the frame as in the suspected names are updated into a Suspect excel sheet only if such name is not already in the excel sheet to avoid duplication of names.
- **Else-** word "Unknown" is shown on the frame and if confidence is greater than the threshold which is given value 74%, then the person's image is saved in a separate folder. This helps in identifying any intruders in the class and reduce the wrong classification of students to an unknown person.

## 4. TESTING AND RESULTS

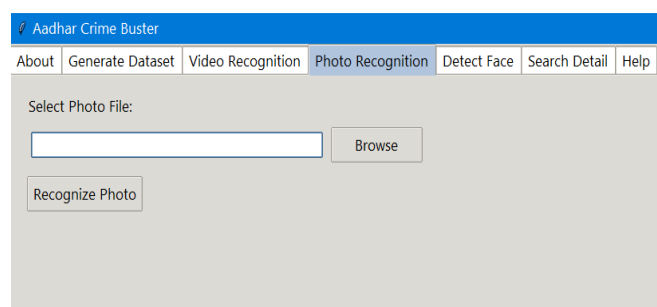
**Fig 4.1: - Generate Dataset**

The dataset generation feature replicates the process of creating Aadhaar cards. It demonstrates that during the Aadhaar enrolment process, 200 photos of the applicant are captured from various angles within a span of just 20 seconds.



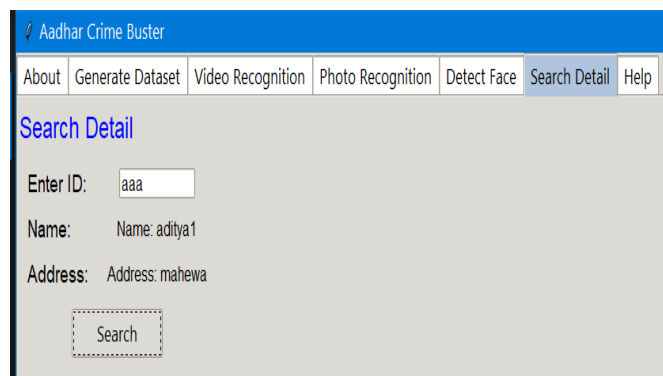
**Fig 4.2: - Video Recognition**

This feature enables law enforcement agencies to upload videos capturing crimes in progress and match them against the existing Aadhaar database.



**Fig 4.3: - Photo Recognition**

This feature allows law enforcement agencies to upload a photo of a suspect or criminal and retrieve their details, such as name, Aadhaar ID, address, and more, from the existing Aadhaar database [6].



**Fig 4.4: - Search Detail**

The face recognition system identifies a face as either unknown or as a match from the database, along with the corresponding Aadhaar ID. The search detail feature then allows you to use the Aadhaar ID to retrieve additional information, such as the individual's name, address, phone number, and more.

The Face recognition rate of suspects is 77% and its false-positive rate is 28%. This system is recognizing persons even when they are wearing glasses or cap or grown a beard.



**Fig 4.5: - (Testing with spectacles)**

Face Recognition of unknown persons for both existing and proposed models is 60%. This happened mostly due to detecting random objects in the background (like cars, curtains, etc.)



**Fig 4.6: - (Testing with two people in a frame)**

Its false-positive rate is 14% and 30% for the proposed and existing model respectively.

In the existing system, it is observed that when a person in the video turned his head sideways more or move away from the frame then the confidence value may decreased than threshold value (74%) then the person in the frame is marked as an unknown [12].

Performance Evaluation	Accuracy %
Person recognition rate (Live Video)	77
False-Positive rate (Person)	28
Unknown person recognition rate (Existing model)	60
Unknown-person false positive rate (Existing model)	30



Unknown person recognition rate (Proposed model)	60
Unknown false positive rate (Proposed model)	14

(Performance analysis table)

## 5. FUTURE SCOPE

Depending on several factors, port scanning initiatives may have varying scopes in the future.

### *Real-time surveillance:*

Create technologies that enable tracking and surveillance of individuals in public areas in real-time, enabling law enforcement to promptly keep an eye out for and react to crimes or threats.

### *Integration with IoT Devices:*

Facial recognition technology is integrated with Internet of Things (IoT) devices, including sensors and smart cameras, to build a network of interconnected devices that enhance security enforcement and surveillance testing.

### *Cooperation with Governmental Organizations:*

Enhance public safety by collaborating with law enforcement and government organizations to implement facial recognition technology for border control, internal security and violence prevention.

### *Multi-modal biometrics:*

combining different biometrics, including voice or iris recognition, to provide a range of biometric applications that improve identification security and precision.

### *Enhanced Accuracy:*

The facial recognition system's accuracy is continuously increased to identify and lower false alarms through integration with deep learning and algorithms.

## 6. CONCLUSION

One of the well-known methods for facial recognition is LBPH. Our technology is able to identify a student who has made inadvertent modifications, such as growing a beard or donning spectacles.

The dataset is small, which is the issue here. A better dataset could be created in the future, which could theoretically produce a more accurate result. By synthesizing fresh and comprehensive training examples, we can enhance these haar cascade classifiers and raise their recognition rate of unknown individuals. If an intruder is identified in the frame, a visual and audio system alarm can be added.

## REFERENCES

- [1] Viola, P.; Jones, M. Rapid Object Detection using a Boosted Cascade of Simple Features. Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR), 2001, pp. 511–518.
- [2] Turk, M.; Pentland, A. Eigenfaces for Recognition. Journal of Cognitive Neuroscience, 1991, 3(1), pp. 71–86.
- [3] Belhumeur, P.N.; Hespanha, J.P.; Kriegman, D.J. Eigenfaces vs. Fisherfaces: Recognition using Class Specific Linear Projection. IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI), 1997, 19(7), pp. 711–720.
- [4] Ahonen, T.; Hadid, A.; Pietikäinen, M. Face Recognition with Local Binary Patterns. Proceedings of the Advances in Visual Computing, Springer Science and Business Media LLC, Berlin, Germany, 2004; Volume 3021, pp. 469–481.
- [5] Li, S.Z.; Jain, A.K. Handbook of Face Recognition. Springer Science & Business Media, 2011.
- [6] Zhao, W.; Chellappa, R.; Phillips, P.J.; Rosenfeld, A. Face Recognition: A Literature Survey. ACM Computing Surveys, 2003, 35(4), pp. 399–458.
- [7] A. "Ozdil and M. M. "Ozbilen," A survey on comparison of face recognition algorithms," 2014 IEEE

- International Conference on Application of Information and Communication Technologies (AICT), Astana, 2014, pp. 1-3.
- [8] Ahonen, Timo, Abdenmour Hadid, and Matti Pietikainen. "Face description with local binary patterns: Application to face recognition." *IEEE transactions on pattern analysis and machine intelligence* 28.12 (2006): 2037–2041.
- [9] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," *Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. CVPR 2001*, Kauai, HI, USA, 2001, pp. I-I. Will Berger, *Deep Learning Haar Cascade Explained*, WILLBERGER,
- [10] <<http://www.willberger.org/cascade-haar-explained>>.
- [11] Kelvin Salton do Prado, *Face Recognition: Understanding LBPH Algorithm*, towards data science.
- [12] A. Ahmed, J. Guo, F. Ali, F. Deebea, and A. Ahmed, "LBPH based improved face recognition at low resolution," in *2018 International Conference on Artificial Intelligence and Big Data (ICAIBD)*, 2018: IEEE, pp. 144-147
- [13] Bishop, C.M. *Pattern Recognition and Machine Learning*. Springer, 2006.
- ..
-