



# REAL TIME CRIMINAL FACE IDENTIFICATION SYSTEM USING MACHINE LEARNING.

SRIDHAR C <sup>1</sup> Mrs .V. BAKYALAKSHMI <sup>2</sup>

PG Student <sup>1</sup>, Assistant professor <sup>2</sup>,

PG & Research, Department Of Computer Applications

HINDUSTHAN COLLEGE OF ARTS AND SCIENCE

COIMBATORE, INDIA

Abstract: Crime histories often include a person's photo along with all relevant biographical and criminal details. Eyewitness identification of some kind is necessary in order to identify the criminal. In most circumstances, the captured picture parts' resolution or/and quality is inadequate and makes it difficult to identify the face. There are many other methods to be recognized, including through DNA, the eyes, the finger prints, etc. Face identification is one method. In our suggested process, a database is constructed by saving the offenders' full and sliced photos together with all of their personal and criminal information. Then, a new database is made in an effort to locate the offender; Eyewitnesses will attempt to construct the criminal face using the slices contained in the database with the assistance of a professional. Next, using Amazon Recognition, it makes a prediction about the criminal by comparing the newly formed image with the database; if the result is 70–80%, the criminal status of that face is determined.

Keywords: NLTK, Tensor flow, Face Reorganization, Criminal Detection

INTRODUCTION: The goal of this project is to locate criminals within any investigating department. The method used in this case is to segment the offenders' photos into various slices, such as their eyes, hairs, lips, noses, etc., before storing the photographs and details in our database. Eyewitnesses will see the photos or slices that show on the screen by utilizing it we create the face, which may or may not be matched with our images in order to identify any offenders. These images are once again recorded in another database record. We assume he is the lone criminal if any picture matches another one by 99%. As a result, our initiative offers a highly welcoming atmosphere that allows both operators and eyewitnesses to simply designate any face as being a criminal very quickly. Personal information on a specific person is included in criminal records, along with a photograph. To identify any criminals using the information provided by the eyewitness about that person. Fingerprints, eyes, DNA, and other features can be used for identification. Face identification is one of the uses. Our primary point of emphasis during social interactions is the face, which is crucial for expressing identity and emotion. Although it might be challenging to deduce intellect or character from a person's face, the human brain is remarkably adept at remembering and recognizing faces. Several security strategies have been created throughout the years that aid in protecting sensitive data and reducing the likelihood of a security breach. Face recognition is a computer software that utilises a person's face to automatically identify

and verify the person from a digital image or a video frame from a video source. It is one of the few biometric approaches that has the advantages of both high accuracy and Minimal intrusiveness [1, 2, 3]. It may also be hardware that is used to verify people that compares certain facial traits from a picture with a database of faces. A common biometrics system for identity, authentication, authorisation, and verification is this one. Face recognition technology is used by many businesses in their access controls, security cameras, and other applications. Facial recognition has been included into Facebook's website with the goal of generating digital profiles for visitors. Law enforcement agencies in industrialised nations construct face databases to be utilised with their facial recognition technology to cross-reference any suspect with the database. On the other side, thumbprint identification is used in Malaysia to identify any suspects in the majority of instances. Yet, most thieves are aware of thumbprint recognition because to the vast knowledge provided by internet usage. As a result, they wear gloves unless it is a non-premeditated act and are more cautious about leaving thumbprints. In this research, a facial recognition system for criminal databases is proposed, one that uses face matching rather than fingerprint matching to identify suspects.

#### LITERATURE REVIEW:

[1] If they couldn't uncover any fingerprints at the crime site, the authors of this article used CCTV video to their advantage and compared the photographs with criminal databases. This system has five stages, the first of which is planning, during which the system's purpose and construction process are addressed. The need to design the system was covered in the second step of Requirement analysis. The third step was design, when they specified the process and system design. Implementation and testing, which involves the use of the Principal Component Analysis (PCA) Method, are the final and most crucial stages. The system's development took place in a controlled atmosphere, thus the maintenance phase wasn't carried out until now. The authors had employed the PCA Method to detect comparable aspects of pictures that were included in the database with collected images of film in order to identify criminals. In order to show the person's information if FRCI recognises a face, the computer will use a database that holds the person's personal data. MATLAB R2013b is used for database and coding, while Visual Studio Code is used to develop the system interface. Using the suggested model, they were 80% accurate.

[2] The real-time picture training stage is the first in this work, followed by the face identification step utilising the Harr classifier. The third phase is the comparison of real-time photos with images acquired by surveillance cameras, and the last step is the conclusion based on the comparison. The Haar-classifier on Open-CV is being used by the authors to detect faces; Haar-cascading is one of the face detection techniques. Harr-like classifiers are utilised for face tracking on the open-CV platform. This method may be utilised to find the suspects that we are looking for because it has several people's identities. As compared to the prior model, the suggested system's accuracy is quite high. Moreover, they informed us that by using the Adhar database, we could quickly distinguish Between Indians and foreigners and further explore whether a person was a criminal or not. By using the citizenship database that is currently accessible, we may use this system.

[3] In this essay They are determining if the passenger is an authorized passport holder or not using the Passport database. In this, they combine the LBPH mathematical model with image processing methods. This procedure includes the following six procedures for airport security purposes: a) Webcam image capture b) transmission of the captured picture to the Django server c) extraction of LBPH features from the image d) comparison of the image with the database image by applying classifier e) If a match is made, user information is retrieved from the database; f) the predicted information about the user is emailed to the admin. They analyse webcam photos for LBPH before applying classifiers and compare the results with database images. Also, it will make it easier to apprehend criminals who cross borders illegally. If the traveller has a bank loan, then specific information about them will be transmitted to the police station for verification.

[4] In this study, a web-based technology called Picture Sleuthing is used to identify Soldier Portraits from the American Civil War (1861–1865). They said that using this identifying method is like looking for a needle in a haystack. Where it has three components: a) haystack construction; b) a narrowed haystack; and c) a needle found in a haystack. Combining automatic facial recognition with crowdsourced human

knowledge is how the work is done. The authors highlighted the implications for person identification pipelines at the time this technology was introduced and how it assisted to identify the unknown photos. They demonstrate how Photo Sleuth's pipeline has assisted in identifying thousands of previously unidentified photographs and in fostering sustained volunteerism.

[5] An automated facial recognition system for attendance tracking is presented by the authors of this research. They are employing a camera to take pictures of people's faces, and they then compare those pictures to pictures that are already in their database. For name recognition they are employing an SVM classifier, and for face recognition they are utilising a gradient-oriented histogram. They are utilising open-CV for image detection and identification, Tkinter for creating GUI applications, and Numpy for dealing with arrays because they are all python libraries. utilising the Xampp server, which is a free open source server, to create and test the application. A 99.38% accuracy rate was attained with the suggested model. The system's viability can be improved by using the cloud.

[6] The importance of an attendance tracking system to the teaching and learning process was explored by the writers of this research. As a pupil enters the classroom, his or her image is taken. Using the acquired image as a starting point, pre-processing and face region extraction are performed. In order to mark a student as present if they showed up to class or absent if they did not, they use a facial recognition algorithm. They are employing a camera to take the student's picture, preprocessing it, then matching it to their student database and recording attendance.

[7] The authors of this research have created a quick algorithm-based face identification system. Two datasets are used in this model: 1) Unconstrained Face Pictures, 2) Olivetti Research Laboratory (ORL) (UFI). 400 92X92 pixel pictures total in the ORL, 9 of which are utilised for training and 1 of which is used for individual assessment. UFI has 401 pictures with a resolution of 128x128 pixels, of which 7 are utilised for training and 1 is used to test each individual. Face field characteristics are taken from the captured picture after it has been converted to the HSV format. Three distance-based classification techniques—Manhattan, Euclidean, and Cosine—are used. With the datasets ORL and UFI, they obtained the best resolution and a 99.9% accuracy by comparing various approaches.

#### EASE OF USE:

**Open-CV:** The open-source computer vision library is called Open-CV. The collection has over 2500 optimised algorithms that cover a wide range of both traditional and cutting-edge computer vision and machine learning methods. Moreover, it offers interfaces for C++, PYTHON, JAVA, and MATLAB that support Windows, Linux, Android, and Mac OS. Open-CV is accessible for free for both personal and professional usage. For taking pictures and movies in public spaces, OpenCV is employed.

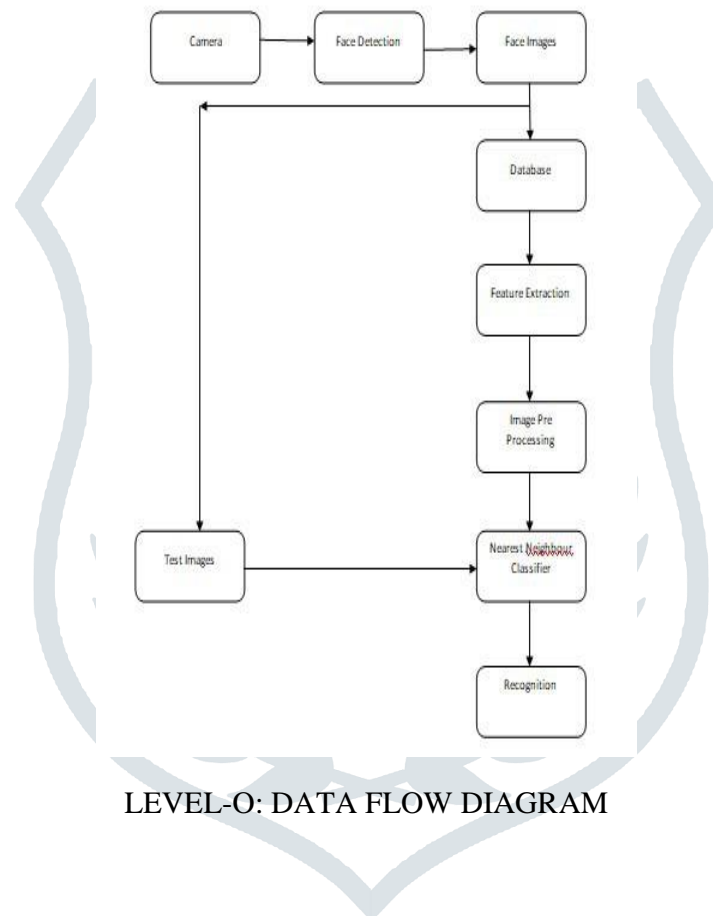
**Facial Recognition:** The main goal of this stage is to take pictures of the faces of the accessible subjects for the camera. This stage produces patches that include every face in the input image. to create an ideal and favoured facial recognition system. To explain the scales and direction of these patches, face alignment is done. Human face patches are extracted as the next step following the face detection process.

**Facial Recognition :** Facial recognition is a technique for utilising a person's face to identify or confirm their identification. The next stage is to identify the faces after they have been represented. In this comparison of the recognised face image with the photos, we use face encodings from our database. Using biometrics, a face recognition system maps facial emotions from an image or video. It compares the information to a database to identify matches for recognised faces. Although facial recognition may help identify a person's identity, it also raises privacy issues. Facial recognition is employed in commercial applications as well, and it may be used for everything from security to marketing.

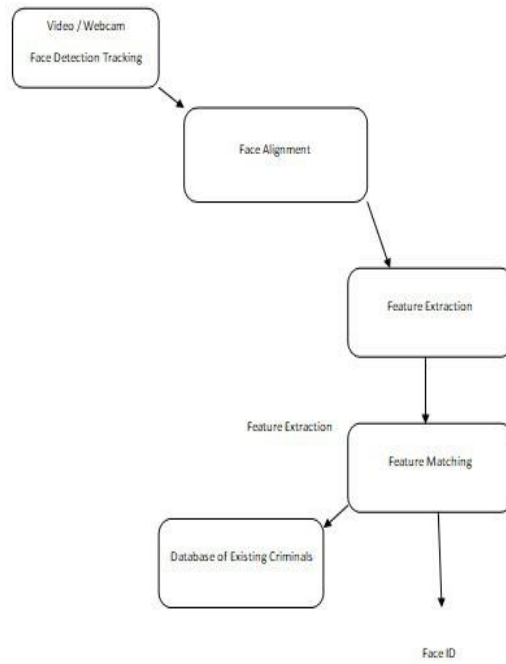
PROPOSED SYSTEM: In this study, we make use of CCTV cameras that are always on and operating in a public setting. As part of the system's implementation, we already saved criminals' picture data with their names on the photos in the database.

We are processing those photos and extracting features from them, and as part of feature extraction, we are using Pickle to save the face encodings from the current images into a single file. As CCTV video is being recorded, its face encodings are collected, compared to our saved face encodings of the criminal database, and if a match is discovered, a message with the name of the criminal is immediately shown on screen along with a picture of that criminal whose face matches. Even if he was once caught on camera, authorities will still go and arrest him from that public area since his taken image will be saved into a specific folder. Police will learn whose photograph was matched with a previously taken one from the moment we saved the person's image in the designated folder.

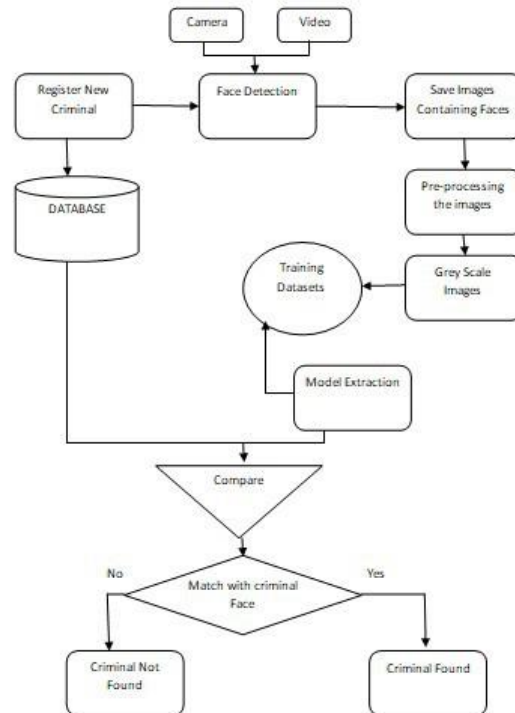
DATAFLOW DIAGRAM:



LEVEL-O: DATA FLOW DIAGRAM



### LEVEL-1: DATA FLOW DIAGRAM



### LEVEL-2: DATA FLOW DIAGRAM

## WORKING DESCRIPTION:

Working: In order to identify the correct individual who is experiencing a problem, we are deploying CCTV cameras to record photographs of the general public.

criminal history database to find.

1. Initially, we will separate the names that are stored with criminal image storing into another list and discover the face encodings of the criminal database photos.
2. In order to readily identify and apprehend criminals who are present in public places, we are now deploying CCTV to record public photos.
3. Taking the face-encodings of the collected photos and extracting the features from them.
4. Contrasting the image encoding values of the captured images with those in our database.
5. If the encoding values match those of the taken image, the criminal's image, name, and message about where they were discovered will be shown on the screen.
6. An image of that individual will be saved into a specific desktop folder so that police may quickly identify the offender who stands out from the other persons in the area.

The following are some benefits of the suggested system: · Quick and precise face positioning for repeatable multiple face detection in the video streams and still photos.

- Identification of many faces simultaneously in a single shot.
- It can manage substantial face databases.

## RESULTS:



Fig : 1

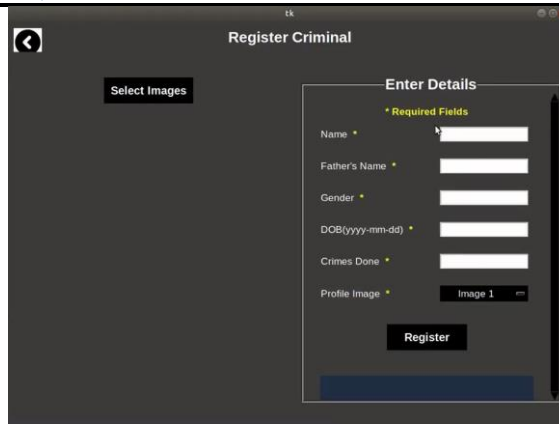


Fig 2



Fig 3



Fig 4



Fig 5

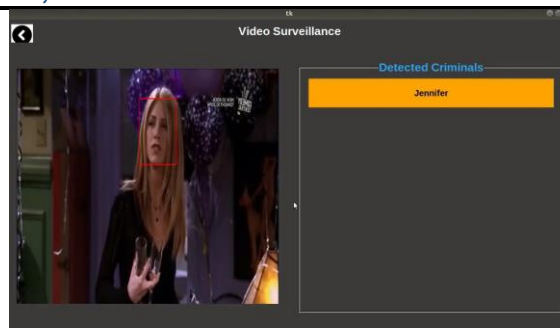


Fig 6

**CONCLUSION:** The method used in this study employs an image partition technique that scans the input picture practically at every pixel position and scale in order to improve accuracy and performance of the detector. Here, we've divided image processing into three levels of complexity: low, medium, and high. Based on the proposed system's facial recognition procedure, this paper has recommended a better method for criminal identification. In this study, we used processing techniques to an already-captured image. We plan to do "real time image processing" on actual images in the future.

**FUTURE SCOPE:** In addition to offering the Police great convenience in identifying criminals, this enhanced version of the criminal detection system also saves them time because operations are automated. This research paper is unique in that it uses face encodings to recognise faces. For next work, we can upgrade the criminal detection system to include Alarms. It will only sound when a match is made, letting everyone who isn't watching the CCTV room know that someone from the database has been located in that public area. This study describes a

surveillance system that will notify us if a conflict, protest, or burglar is spotted on CCTV footage.

#### REFERENCES:

- [1] "FACE RECOGNITION FOR CRIMINAL IDENTIFICATION: AN IMPLEMENTATION OF PRINCIPAL COMPONENT ANALYSIS FOR FACE RECOGNITION," AIP Conference Proceedings 1891, 020002 (2017); doi:10.1063/1.5005335; written by Nurul Azma Abdullah, Md. Jamri Saidi, Nurul Hidayah Ab Rahman, Chuah Chai Wen, and
- [2] "AUTOMATED Criminal Identification by Face Recognition Using Open Computer Vision Classifiers," Third International Conference on Computing Methodologies and Communication (ICCMC 2019), Apoorva P., Impana H.C., Siri S.L., Varshitha M.R., and Prof. Ramesh B.
- [3] "AIRPORT SECURITY USING FACE- RECOGNITION," International Journal of Future Generation Communication and Networking, vol. 13, no. 3, by Prof. Rupali T. Umbare, Ms. Janhavi S. Takalgavankar, Ms. Harshada S. Yadav, and Ms. Pruthvi A. Tilekar (2020).
- [4] "Photo Sleuth: Mixing Human Knowledge and Face Recognition to Identify" by Vikram Mohanty, David Thames, Sneha Mehta, and Kurt Luther 24th International Conference, Historical Portraits, March 2019, doi:10.1145/3301275.3302301
- [5] Automated Face Recognition Attendance System Using Python and OpenCV by Dr. Asif Ali, Radhika Mandhanya, Shraddha Birla, Ujjwal Mandloi, and Vipul Jain, GRD Journals- Global Research and Development Magazine for Engineering, Volume 6 | Issue 4 | March 2021



[6]"ATTENDANCE MONITORING SYSTEM USING FACE DETECTION & FACE RECOGNITION," International Research Journal of Engineering and Technology (IRJET), Volume: 06 Issue: 03 | Mar 2019. P. Kowsalya, J. Pavithra, G. Sowmiya, and C.K. Shankar.

[7] "Force Field Feature Extraction Using Fast Algorithm for Face Recognition Performance," Iraqi Academics Syndicate International Conference for Pure and Applied Sciences, Kian Raheem Qasim and Sara Salman Qasim, <https://doi.org/10.1088/1742-6596/1818/1/012195>

