

ISSN: 2454-132X Impact factor: 4.295 (Volume 5, Issue 3) Available online at: www.ijariit.com

# Criminal identification using facial recognition

Archana Naik <u>archana.naik@nmit.ac.in</u> Nitte Meenakshi Institute of Technology, Bengaluru, Karnataka

Tanka Prasad Tiwari <u>tiwaritanka75@gmail.com</u> Nitte Meenakshi Institute of Technology, Bengaluru, Karnataka Rohan Basukala <u>roahnbasukala15@gmail.com</u> Nitte Meenakshi Institute of Technology, Bengaluru, Karnataka

Prajwal Deep Bhandari <u>prajwaldeepbhandari@gmail.com</u> Nitte Meenakshi Institute of Technology, Bengaluru, Karnataka Santosh Tiwari <u>santoshmaxtiwari@gmail.com</u> Nitte Meenakshi Institute of Technology, Bengaluru, Karnataka

Asha H. V. <u>asha.hv@nmit.ac.in</u> Nitte Meenakshi Institute of Technology, Bengaluru, Karnataka

# ABSTRACT

The individualistic characters of the human face can be extracted by face recognition. The human face detection and recognition finds a major role in the application as video surveillance, face image database management. Face recognition is a simple and agile biometric technology. This technology uses the most obvious human identifier to the face. The face recognition finds its application in security, health care, criminal identification, places where human recognition is the necessity. With the advancement in technology, the extracting features of the human face are become simpler. This paper discusses on a different algorithm to recognize the human face. The purpose is to identify the criminal face and retrieve the information stored in the database for the identified criminal. The process is categorized into two major steps. First, the face is extracted from the image, distinguishing factors in the face are extracted and stored in the database. The second step is to compare the resultant image with the existing image and return the data related to that image from the database.

*Keywords*— *Cascade face recognition, Face feature extraction, Haar, OpenCV* 

# **1. INTRODUCTION**

Biometrics is a technology that uses the unique patterns of physical or behavioural traits of human for authentication or identification. The advancement in biometric technology is bringing in the biometric scanners onto smartphones and other affordable devices. There is also an increasing number of services and applications that require high security and smooth customer experience. Biometric technology is replacing traditional authentication methods [1]. One of the advanced methods of biometric is facial recognition.

For identifying a person face is the decisive part of the human body. Face distinguishes a person. Facial recognition is a challenging problem that finds application for authentication in

© 2019, <u>www.IJARIIT.com</u> All Rights Reserved

banking services, security systems [2], searching, identifying personal among others. A human can easily recognize the face, for the computer it requires an entirely different process.

Face acknowledgement is an errand that people perform routinely and easily in their day to day lives. The wide accessibility of amazing and minimal effort - work area and inserted registering frameworks has made a tremendous enthusiasm for programmers to prepare computerized pictures and recordings in various applications, including biometric confirmation, observation, human-PC association, and sight and sound administration. Innovative work in programmed face acknowledgement pursues normally. A face recognition system is expected to identify faces present in images and videos automatically. It can operate in either or both of two modes: (1) face verification (or authentication), (2) face identification (or recognition). Face check includes a coordinated match from grayscale image (black and white) against a format face (datasets) picture whose feature is being extracted. Face recognizable proof includes one-to-numerous matches that think about an inquiry face picture or video against all the format pictures in the database to decide if it matches. Another face acknowledgement situation includes a watch-list check, where an inquiry face is coordinated to a rundown of suspects (one-to-few matches).

The research in facial recognition is motivated by enormous real-time applications that can make the traditional identification system smooth and easy. The face recognition motivates the researcher by throwing the fundamental challenges for recognizing the faces. The simple and easy approach to identification has made facial recognition as the primary biometric technology. The importance of the technique owed to easily accessible digital cameras and increased demand for security. The advantage of facial recognition over other biometric technologies is that it is natural, nonintrusive and easy to use [3].

# 2. FACIAL RECOGNITION

#### 2.1 Categories for Facial Recognition

The facial recognition can be carried out in one of the two methods as Geometric that is feature based or Photometric that is view based.

**2.1.1 Geometric:** This method uses the geometrical relationship between the facial landmarks. It finds the spatial configuration of the features on the face. This method recognizes the features of the face like eyes, nose, mouth and eyebrows. It learns the location of these features. The faces are uniquely identified by determining geometrical distance and angles between the features [4].

The process of the geometric approach to facial recognition is as follows. It marks the points at the prominent parts of the face as on eyes, nose and boundary of the lips. Further, only these points are considered, geometrical distance is calculated between these points to uniquely identify the face.

**2.1.2 Photometric stereo:** This method uses several photo/image of a person taken under different lighting conditions and taken from a different angle. Then recover the shape of the face by a gradient map. This image is made up of an array of the surface normal.

In photometric stereo approach, multiple images of the same face are considered to gradient map, to determine the single image.

Out of these two approaches, the implementation of a geometric-based approach to identify and detect face is discussed in this paper. Both of these are efficient in terms of recognizing faces. When dealing with only software, the geometric method is the best option for openCV. [5,6,7]

Haar feature is used to identify the object it deals with only faces to be extracted. Haar cascade algorithm includes four stages:

- (a) Haar Feature Selection
- (b) Creating Integral Images
- (c) Adaboost training
- (d) Cascading classifier

This algorithm requires a lot of positive and negative images so it extracts the face images to a grayscale image. The grayscale image extracts feature from it. A Haar feature extracts adjoining rectangular in all particular area of detection window and ascertains the contrast between these entries. There will be a different feature like an edge feature, line feature, four rectangle feature that is landmarked in the face. The distance between eyebrows will be line feature and the lower eye will be an edge feature, though different possible sizes and location of each kernel are used. Sometimes it becomes irrelevant for applying on cheeks or any other place so this is achieved by AdaBoost[8,9,10,11,12].

# 2.2 Face Detection

A human can detect the face naturally. For a computer, it is a tough task for recognizing and detecting the face. A computer requires data in the form of a finite number of elements each having a particular location and value. The values are in terms of pixels, bit image, picture element. These elements form the prerequisite to detect the face.

Face detection involves separating image windows into two classes, faces and non-faces. For face recognition first, perform the feature extraction. Facial feature extraction is performed as texture based or shape based. Texture-based methods consider the local texture, using the pixel values around the specific feature point. Log Gabor wavelet network, neural-networkbased eye feature detector, hierarchical 2-level wavelet network are some of the texture based facial feature extraction algorithms. The shape-based facial feature extraction algorithms are direct appearance model, active wavelet network, component-based with 3D morphable models. There are some hybrid techniques which use both textures based and shape based techniques developed such as AdaBoost with shape constraints, elastic bunch graph matching. The OpenCV based face detection use this hybrid technique specially AdaBoost method [13,14].

The process of face detection can be divided as:

- (a) Pre-processing: Images are processed before classification to reduce variability in faces. Only the positive frontal face images are used for classification. It compares the difference between dark edges and white edges of faces. Using the standard algorithm the processed images are corrected.
- (b) Classification: For classification, the OpenCV uses neural networks to classify the images as faces or no faces by training on these examples. To optimize the results different network configurations are experimented with.
- (c) Localization: The OpenCV uses a trained neural network to search for faces in an image. If the image is present localize them in the bounding box.

The input received from video, images or webcam is passed through the preprocessing.

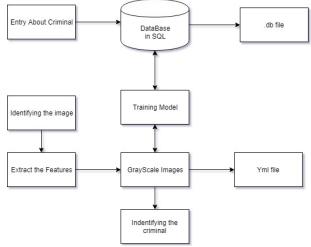


Fig. 1: Overall process

The feature extraction is done using the localization to identify the exact face. Figure 1 shows the overall process for identifying and recognizing the face. Face Recognition finds its application in the field of identification, authentication, security, surveillance system, human-computer interaction, psychology and so on.

#### 2.3 OpenCV

OpenCV (Open Source Computer Vision Library) is a library of programming functions mainly aimed at real-time computer vision. Classifier gives the differences between positive and negative image where the positive image is for face and the negative image is for non-face image. OpenCV trains the classifier on any desired face as set in the program and provides two pre-trained and ready for implementing face detection classifier.

Two files haarcascade\_frontalface\_alt.xml and haarcascade\_eye are used for detecting face and eye

respectively. The other feature provided by OpenCV is LBP (Local Binary Pattern) cascade classifier which is local binary patterns that train the grayscale image of hundreds to thousands. LBP looks at every 9 pixels of  $3 \times 3$  window. Compare the central pixel with the value of surrounding 8 pixels. For each pixel that is greater than the central pixel value, is replaced by 1 and for smaller, it sets the value to 0. Finally, it creates the block histogram to form one image and one feature image converts it into a yml format for further recognizing the face.

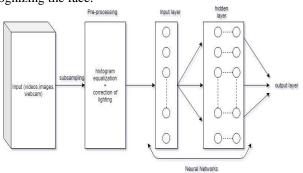
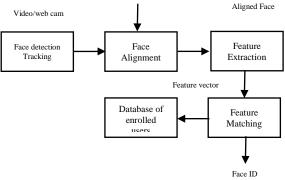


Fig. 2: Face detection process

Figure 2 gives the layers of the learning and detecting the features of the face.

# **3. IMPLEMENTATION**

The criminal face identification is implemented by extracting the face from video or image, identify the face. The face is searched in the database to look for the details about the criminal. If the information about the face is not available user is prompted to add/update description about the face to the database.



**Fig 3: Face matching Process** 

The diagram as given in figure 3 describes the face recognition process and matching the faces in the database.

- (a) **Registering new criminal:** This is the first step of implementing face detection as the criminal face with id, name, age, gender and crime committed is registered to the database. The data are collected in SQL Studio that gets converted into the .db format.
- (b) Each face is given a unique ID, as the faces are recognized using the ID by the program.
- (c) **Face detection**: Once the image is received the model checks the presence or absence of face in the image. Once face is detected its location is localized and only face image is extracted.
- (d) Preprocessing Images: Processing the features that are to be extracted, for improving the rate of recognizing the face. The facial image is cropped and is resized at lesser pixel value. Ascertain images contain disturbances it will be hard to train in LBPH, results in the inaccurate histogram. For this reason, the prepossessed image is normalized to get the

uniform grey level and filtered to extract the preprocessed image.

- (e) **Feature extraction**: The performance of the entire system depends on this step. Different facial features are extracted using different Haar cascade classifier. Grayscale images from this step used for identification of the criminal and train the model.
- (f) **Training**: In this step, the feature extracted images (grayscale images) are used to train the model. The model can even use the webcam images for training. During the training period the unique id, name, age and crime is given by the user for each image.
- (g) Classification and decision: In these two steps, the system must declare the identity of the criminal who appears before them without any a priori knowledge about it. To accomplish this task, this model affects the extracted feature of his face to a class from those learned. Each class is associated with an identity. These two steps are executed only in the recognition module.
- (h) Gray Scale Image: The input from video or camera is converted into grey images. RGB colour value ranges from 0 to 255 (24 bit) but grayscale value comprises of 8bits which is used to classify white and black image faster and accurate. RGB (9,9,9) will become black and RGB(1,1,10) will become white.

#### 3.1 Flow Diagram

The flow diagram given in figure 4 describes the complete process. The image is received from the camera or from the video.

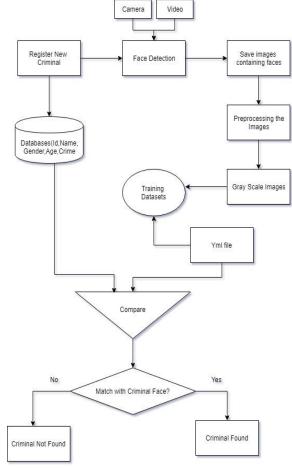


Fig. 4: Flow diagram of the model

Only the face image is extracted, preprocessed, grayscale images are generated. The grayscale images are used for training the model. The trained data are stored as the .yml file. The .yml files are used to compare the faces stored in the

database to extract information about the face. The new face then the details about the face is entered into the database.

# **3.2** The structural algorithm of the model

- **3.2.1 Face detection and recognition**
- Step1: Import cv2 library Step2: Import sys library
- Step2: Import sys notary Step3: Declare the image path
- Step3: Declare the mage path Step4: Declare the cascade path
- Step5: Create the cascade classification from cascade file
- Step6: Read the image
- Step7: Convert image to grayscale
- Step8: Detects the face
- Step9: Print total faces and labels

# **3.2.2 Training function**

- Step1: Get the directories in the data folder
- Step2: List all subject faces
- Step3: the list to hold labels for all subjects
- Step4: Browse each directory and read images within it
- Step5: Build path of the directory containing the image
- Step6: Build path of the directory containing images for the current subject
- Step7: Get the image names that are inside the given subject directory
- Step8: go through each image name, read the image
- Step9: Detect face and add a face to the list of faces
- Step10: Build an image path
- Step 11: Read image
- Step12: Display an image window to show the image
- The above two algorithms are used to detect, recognition and train the model.

# **3.3 Implementation**

The Haar-cascade feature extraction will be imported into the OpenCV python code. The Haar cascade classifier contains different libraries to indent and detect the faces, emotions, eyes, nose, and chin from the faces. For face detection and eye feature extraction library of the Haar cascade classifier is used.

First, train the model using video frames or webcam. Using crime scene CCTV camera footage, train the model and detect the faces from it. If the criminal's face is not in the criminal information database then, the criminal face and details about criminal and crime scene will be stored into the database with the new entry. Every criminal entry will have a unique id. The name, gender, age and crime are also stored in the database. From the input source, the face detection is done using four coordinates. Then the detected faces are converted into the grayscale images and saved into the yml file. This entire yml file will be checked while facial recognition. Using the different coordinates of faces and grayscale images the model will be trained.

After getting new CCTV footage, the model runs the face detection algorithm in it. It extracts the faces from it then it compares the face coordinates and grayscale images from the trained file which contains the grayscale images of the criminals.

# 4. RESULTS

The match in the yml image in the image in the database is found the description about the face is displayed on the screen. In figure 5, the input from the webcam was given after training the datasets that were provided by the user.



Fig. 5: Recognizing the face model in web-camera

For this input, the model identifies the face of criminal and gives the information (name, age, gender, crime) about the criminal the same as above but from web camera.

When a new face is detected, which do not have the match in the database the description about the face to be entered and stored.

Satabases 🗗 🗙	18 8 12 12 12 16 16 17 16 16 16 12 12 12 12 12 12 12 12 12 12 12 12 12
Her by name           Place (SQUe I)           Pace (SQUe I)           People           Vens           et demon (SQUe I)           et demon (SQUe I)	GGGBBBGGXXASS
	Table name: criminal UNITHOUT ROWID
	Name Data type Primary Foreign Unique Check Not Collate Default value 114 STRMS 9 NULL
	2 Name STRING 59 NULL
> Criminal	3 Gender VARCHAR NULL
v I demoface (SQL * 1	4 Age STRING NULL
Tables	5 Crime STRING 😕 NULL
	15 10 10 10 10 10 10 10 10 10 10 10 10 10
	Uppe rearrie

Fig. 6: Entry of criminal description in database

Figure 6 gives the screenshot of entering the description about new face when a new criminal face is detected and added to the database. The authorized user enters this information about criminal along with the source of input. This can further be used to create datasets to train the model (.yml).

# **5. CONCLUSION**

When the witness is available, at the crime incident, it is easy to identify the criminal using sketches and other evidence. But, when a crime happens without witness then, the facial recognition system can be used to identify the criminals. These models are very useful to find out the criminal after the crime. The system recognizes the criminal, useful to prevent the crime. Limitations of the system are that most often criminals do not face the camera/avoid the camera. The exact face can be analyzed by extracting the smaller features of the face such as depth of the eye.

# **6. REFERENCES**

 Wencheng Yang, Song Wang, Jiankun Hu, Guangzhou Zheng and Craig Valli, 23 January 2019, Security and Accuracy of Fingerprint-Based Biometrics: A Review, Page-1-19

- [2] Piyush Kakkar, Mr Vibhor Sharma2, 3 March 2018, Criminal Identification System Using Face Detection and Recognition, page 238-243
- [3] Stan Z. Li, Anil K. Jain, "Handbook of Face Recognition", With 210 Illustrations, Springer
- [4] Gary Bradski and Adrian Kaehler, "Learning OpenCV", September 2008: First Edition, Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472
- [5] Sushil Kumar Paul, Mohammad Sharif Uddin, Saida Bouakaz, "Face Recognition using Eyes, Nostrils, and Mouth Features", Page1-3
- [6] E. Holden, R. Owens, "Automatic Facial Point Detection," Proc. The 5th Asian Conf. on Computer Vision, 23-25 January 2002, Melbourne, Australia.
- [7] M. J. T. Reinders, et al., "Locating Facial Features in Image Sequences using Neural Networks," Proc. IEEE Int'l Conf. Face and Gesture Recognition, pp230-235, 1996.
- [8] C. Hu, et al., "Real-time view-based face alignment using active wavelet networks," Proc. IEEE Int'l Workshop Analysis and Modeling of Faces and Gestures, pp. 215-221, 2003.
- [9] S. Yan, et al., "Face Alignment using View-Based Direct Appearance Models," Int'l J. Imaging Systems and Technology, vol. 13, no. 1, pp. 106-112, 2003.
- [10] B. Weyrauch, et al, "Component-based Face Recognition with 3D

- [11] Morphable Models," 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'04), June 27- July 2, 2004, Washington DC, USA.
- [12] L. Wiskott, et al., "Face Recognition by Elastic Bunch Graph. Matching," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 19, no.7, pp. 775-779, 1979.
- [13] D. Cristinacce, T. Cootes, "Facial Feature Detection Using AdaBoost with Shape Constraints", British Machine Vision Conference, 2003.
- [14] L. Chen, et al., "3D Shape Constraint for Facial Feature Localization using Probabilistic-like Output", Proc. IEEE Int'l Workshop Analysis and Modeling of Faces and Gestures, pp. 302-307, 2004. K. Elissa,
- [15] Abdellatif Hajraoui, "Robust System of Face Recognition," unpublished.
- [16] Di Huang, Caifeng Shan, Mohsen Ardebilian, Yunhong Wang, and Liming Chen, "Local Binary Patterns and Its Application to Facial Image Analysis: A Survey ", https://liris.cnrs.fr/Documents/Liris-5004.pdf
- [17] https://docs.opencv.org/2.4.13.7/modules/contrib/doc/face rec/facerec\_tutorial.html
- [18] https://www.geeksforgeeks.org/opencv-python-programface-detection/
- [19] https://opencv-python tutroals.readthedocs.io/en/latest/py\_tutorials/py\_objdetect /py\_face\_detection/py\_face\_detection.html