Electronic Crime Identification Using Face Matching

Adebayo, A.A.[1], Lawal, O.A.[2], Famuyiwa, K.S.A.[3] & Adekunle, K.O.[4]
Department of Computer Science, Moshood Abiola Polytechnic, Abeokuta Ogun State Nigeria [1,2]
Department of Computer Science, D .S Adegbenro ICT Polytechnic, itori, Ogun state Nigeria [3]
Department of Computer Science, Federal Polytechnic, Ile-Oluji, Ondo State Nigeria [4]
E-mails: debamos04@yahoo.com[1], oyindamola2008@gmail.com[2], foluwa926@gmail.com [3],
kadekunle@fedpolel.edu.ng [4]

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 becoming simpler. This research 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

25th iSTEAMS Trans-Atlantic Multidisciplinary Conference Proceedings ReferenceFormat
Adebayo, A.A., Lawal, O.A, Famuyiwa, K.S.A. & Adekunle, K.O. (2020): Electronic Crime Identification Using Face Matching.. Proceedings of the 25th iSTEAMS Trans-Atlantic Multidisciplinary Virtual Conference, Laboratoire Jean Kuntzmann, Universite Laboratoire Jean Kuntzmann, Universite Grenoble, Alpes, France June, 2020. Pp 229-240. www.isteams.net/France2020.

1. INTRODUCTION

Biometrics is a technology that uses the unique patterns of physical or behavioral 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 (Yang et. al., 2019). One of the advanced methods of biometric is facial recognition. First, we need to know what Face detection and Face recognition they are two totally different things although one builds upon the other. Detection is the process by which the system identifies human faces in digital images and video streaming, regardless of the source while Recognition is the identifying a known face with a known name in digital images, still regardless of the source. The resource can be a scanned copy of an image to a live video stream. Face detection and recognition is a section of Machine learning with a good number of research topics focused on improving the existing algorithms (Niranjani et. al., 2017).

The human face plays an important role in our social intercourse in conveying identity and emotions and human ability to recognize faces is remarkable. In our lifetime we can recognize thousands of faces and identify familiar faces at a glance even after years of separation. The skill is robust, despite large changes in the visual stimulus due to viewing conditions, angle, expressions, aging, and distractions such as glasses or changes in hairstyle or changes in beard. But developing a computational model of face recognition is quite difficult because human faces are multidimensional, complex, and subject to change over time (Viraj et. al., 2015). 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 banking services, security systems (Kakkar and Sharma, 2018), searching, identifying personal among others. A human can easily recognize the face, for the computer it requires an entirely different process.

Face recognition is an interesting and challenging problem and impacts important applications in many areas such as identification for law enforcement, authentication for banking and security system access (Hui-Xing & Yu-Jin, 2009), and personal identification among others. Face recognition is an easy task for humans but it's entirely different task for a computer. A very little is known about human recognition to date on How do we analyze an image and how does the brain encode it and Are inner features (eyes, nose, mouth) or outer features (head shape, hairline) used for a successful face recognition? Neurophysiologist David Hubel and Torsten Wiesel has shown that our brain has specialized nerve cells responding to specific local features of a scene, such as lines, edges, angles or movement. Since we don't see the world as scattered pieces, our visual cortex must somehow combine the different sources of information into useful patterns (Kakkar and Sharma, 2018).

1.1 Problem Statement

As the world has seen exponential advancement over the last decade, there is an abnormal increase in the crime rate and also the numbers of criminals are increasing at an alarming rate, this leads toward a great concern about the security issues. various causes of theft, stealing crimes, burglary, kidnapping, human trafficking etc. are left unsolved because the availability of police personnel is limited, many times there is no identification of the person who was involved in criminal activities.

1.2 Aims and Objectives

The main objective of this work is reducing the consumption of time in the old manual system and developing a much easier and effective automated system, which is an advantage over the manual system to increase the efficiency. It is to construct an automatic face recognition system using a standard PC camera in the real-time. This project work is to provide the better security application.

The objectives of this project work are as follows:

i. To conduct and review the existing system
ii. To develop a face recognition system for the identification of criminals.
iii. To implement the design using a java programming language
iv. To design a systematic and user friendly system.

2. LITERATURE REVIEW

Over the years, a lot of security approaches have been developed that help in keeping confidential data secured and limiting the chances of a security breach. Face recognition which is one of the few biometric methods that possess the merits of both high accuracy and low intrusiveness is a computer program that uses a person's face to automatically identify and verify the person from a digital image or a video frame from a video source. It compares selected facial features from the image and a face database or it can also be a hardware which used to authenticate a person (Abdullah et. al., 2017). In the early years of the 21st century, we found ourselves continually moving further away from the necessity of physical human interaction playing a major part of everyday tasks. Striding ever closer to an automated society, we interact more frequently with mechanical agents, anonymous users and the electronic information sources of the World Wide Web, than with our human counterparts. For these reasons, biometric authentication has already begun a rapid growth in a wide range of market sectors and will undoubtedly continue to do so, until biometric scans are as commonplace as swiping a credit card or scrawling a signature (Chevelwalla et. al., 2015).

This technology is a widely used biometrics system for authentication, authorization, verification and identification. A lot of company has been using face recognition in their security cameras, access controls and many more. Facebook has been using face recognition in their website for the purpose of creating a digital profile for the people using their website. In developed countries, the law enforcement create face database to be used with their face recognition system to compare any suspect with the database.

This paper to propose a facial recognition system for a criminal database where the identification of the suspect is done by face matched rather than thumbprint matched. (Abdullah et. al., 2017). Face Identification is a technique that is mainly used to identify criminals based on the clues given by the eyewitnesses. Based on the clues, an image is developed by using an existing image in the database and then it is compared with the images already had. To identify any criminals there must be a record that generally contains name, age, previous crime, gender, photo, etc.

2.1 Face Recognition System

The advances in computing technology have facilitated the development of real-time vision modules that interact with humans in recent years. Examples abound, particularly in biometrics and human computer interaction as the information contained in faces needs to be analyzed for systems to react accordingly (Caarls et. al., 2002). It is evident that face detection plays an important and critical role for the success of any face processing systems. The face detection problem is challenging as it needs to account for all the possible appearance variation caused by change in illumination, facial features, occlusions, etc. In addition, it has to detect faces that appear at different scale, pose, with in plane rotations. Often the size of the image is very large, the processing time has to be very small and usually real-time constraints have to be met. This is the first step of any fully automatic system that analyzes the information contained in faces (e.g., identity, gender, expression, age, race and pose).This work focuses on how to make parallel computations by partitioning the image into manageable and meaningful parts for efficient calculations and results. (Nautiyal et. al., 2013)

Face acknowledgement is an errand that people perform routinely and easily in their day to day lives. 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).

2.1.2 Face Recognition Technique

The method for acquiring face images depends upon the underlying application. For instance, surveillance applications may best be served by capturing face images by means of a video camera while image database investigations may require static intensity images taken by a standard camera. Some other applications, such as access to top security domains, may even necessitate the forgoing of the nonintrusive quality of face recognition by requiring the user to stand in front of a 3D scanner or an infra-red sensor (Chevelwalla et. al., 2015).

2.1.2.1 Face Recognition from Intensity Images

Face recognition methods from intensity images fall into two main categories: feature-based and holistic. An overview of the well-known methods in these categories is given below.

- **Featured-based**

  Feature-based approaches first process the input image to identify and extract (and measure) distinctive facial features such as the eyes, mouth, nose, etc., as well as other marks, and then compute the geometric relationships among those facial points, thus reducing the input facial image to a vector of geometric features.

- **Holistic**

  Holistic approaches attempt to identify faces using global representations, i.e., descriptions based on the entire image rather than on local features of the face. These schemes can be subdivided into two groups: statistical and AI approaches.

- **Statistical**

  In the simplest version of the holistic approaches, the image is represented as a 2D array of intensity values and recognition is performed by direct correlation comparisons between the input face and all the other faces in the database. Though this approach has been shown to work under limited circumstances (i.e., equal illumination, scale, pose, etc.), it is computationally very expensive and suffers from the usual shortcomings of straightforward correlation-based approaches, such as sensitivity to face orientation, size, variable lighting conditions, background clutter, and noise.

2.2.2.2 Predominant Approaches

There are two predominant approaches to the face recognition problem: geometric (feature based) and photometric (view based). As researcher interest in face recognition continued, many different algorithms were developed, three of which have been well studied in face recognition literature: Principal Components Analysis (PCA), Linear Discriminate Analysis (LDA), and Elastic Bunch Graph Matching (EBGM) (Chevelwalla et. al., 2015).

- **PCA:**

Principal Components Analysis (PCA) is the technique pioneered by Kirby and Sirivich in 1988. With PCA, the probe and gallery images must be the same size and must be normalized to line up the eyes and mouth of the subjects within the images. The PCA approach is then used to reduce the dimension of the data by means of data compression and reveals the most effective low dimensional structure of facial patterns. This reduction in dimensions removes information that is not useful and precisely decomposes the face structure into orthogonal (uncorrelated) components known as eigen faces. Each face image may be represented as a weighted sum (feature vector) of the eigen faces, which are stored in a 1D array. A probe image is compared against a gallery image by measuring the distance between their respective feature vectors. The PCA approach typically requires

the full frontal face to be presented each time, otherwise the image results in poor performance. The primary advantage of this technique is that it can reduce the data needed to identify the individual to 1/1000th of the data presented.

In the training phase, you should extract feature vectors for each image in the training set. Let *A* be a training image of person A which has a pixel resolution of *M £ N* (*M* rows, *N* columns). In order to extract PCA features of *A*, you will first convert the image into a pixel vector *ÁA* by concatenating each of the *M* rows into a single vector.
The length (or, dimensionality) of the vector *ÁA* will be *M £N*. In this project, you will use the PCA algorithm as a dimensionality reduction technique which transforms the vector *ÁA* to a vector *A* which has a dimensionality *d*. For each training image *i*, you should calculate and store these feature vectors *I*.

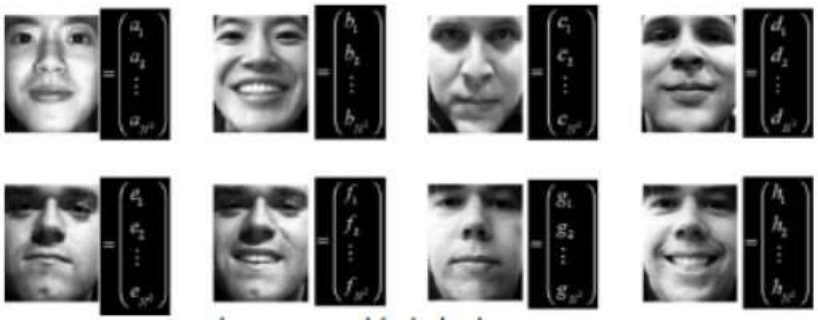

Fig 1: Faces with the Eigen Vector

In the recognition phase (or, testing phase), you will be given a test image *J* of a known person. Let *J* be the identity (name) of this person. As in the training phase, you should compute the feature vector of this person using PCA and obtain *J*. In order to identify *J*, you should compute the similarities between *J* and all of the feature vectors *I*'s in the training set. The similarity between feature vectors can be computed using Euclidean distance. The identity of the most similar *I* will be the output of our face recognizer. If *I* = *J*, it means that we have correctly identified the person *J*, otherwise if *I!* = J, it means that we have misclassified the person *J*.

- **LDA: Linear Discriminant Analysis**

LDA is a statistical approach for classifying samples of unknown classes based on training samples with known classes. This technique aims to maximize between-class (i.e., across users) variance and minimize within-class (i.e., within user) variance. In Figure where each block represents a class, there are large variances between classes, but little variance within classes. When dealing with high dimensional face data, this technique faces the small sample size problem that arises where there are a small number of available training samples compared to the dimensionality of the sample space.

Fig 2: Examples of Six Classes using LDA

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-network-based 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 (Cristinacce and Cootes, 2003).

2.3 Related Works

Eigenface is probably one of the earliest and first successful algorithm developed by L. Sirovich and M. Kirby (1987) where it uses an information theory approach which will search for the best matching or possible face information that is encoded in a collection of faces that will best differentiate the faces. It works by first collecting several images from the database and represent it as a vector, then the algorithm will find the average face vector or the mean and it will subtract the mean face from each sample faces. This is useful in order to find the distinguishable features from each image and it will then find the covariance matrix and it will select the best matching images. It transforms the face images into a set of basis faces which essentially are the principal component of the face itself. The principal components determine which directions in which it is more efficient to represent the data that will be helpful in reducing the computational effort.

Viraj et. al., (2015): The goal of the system is to implement the model for a particular face and distinguish it from a large number of stored faces with some real-time variations as well. Android mobile takes image or video as an input and pass to the web services or web server using HTTP method then on the server side video or image

match with existing criminal record in database and gives response of result to android application and application get these information by using XML parse technique.

The proposed approach essentially is to implement and verify the algorithm Eigenfaces for Recognition, which solves the recognition problem for two dimensional as well as three dimensional representations of faces, using the Principal Component Analysis (PCA). The video snapshots, representing input images for the proposed system, are projected in to a face space (feature space) which best defines the variation for the face images training set. The face space is defined by the 'Eigenfaces' which are the eigenvectors of the set of faces. These eigenfaces contribute in face reconstruction of a new face image projected onto face space with a meaningful named weight. The projection of the new image in this feature space is then compared to the available projections of training set to identify the person using the Euclidian distance.

3. RESEARCH METHODOLOGY

E-crime identification using face matching is an application developed to provide profiling convenience and data retrieval with ease for the Police departments in order to reduce or remove completely, duplication of crime data. The application works by capturing the face of a criminal using OpenCV and matches the captured face with some already available records in the system, if no record is found for the captured face, the criminal has not committed any crime and a new profile can be created for such criminal.

To achieve this functionality, the JavaFX has being used to develop and beautify the interface, Java programming Language is used to validate the inputs and also validate the functions of the system. MySql database is used in storing, share and authenticate users data.

3.1 Data Collection Method

Data was collected through use of questionnaires, interviews and in-depth literature review with the aim of collecting reliable and complete data that can provide concrete conclusions and recommendations for the study.

3.2 Design Methodology

While executing the design process, there exist tools preferences for the software development, with reasons to justify why these tools are selected. An OO language called JAVA with a JavaFX IDE, Wamp testing server for MySql database development of the system and for testing the software with the Netbean IDE.

3.3 Design Goals

The following are the design goals intended to be accomplished by this application:

- To ease process of record finding in investigation department
- To reduce duplication of criminal profiles.
- To automate the record profiling in investigation departments
- To reduce workload related to files searching

3.4 Who Uses the Application

Investigation Department: This is an investigating team in charge of finding and probing criminals.

Police Department: This is the entire police force consisting of the booking officers and others.

3.5 System Architecture and Flowchart

The architecture of the designed system explains the general views of the main interfaces of the application. It also explains the interfacing of the system with the external web services and API and it is shown in Fig 3:

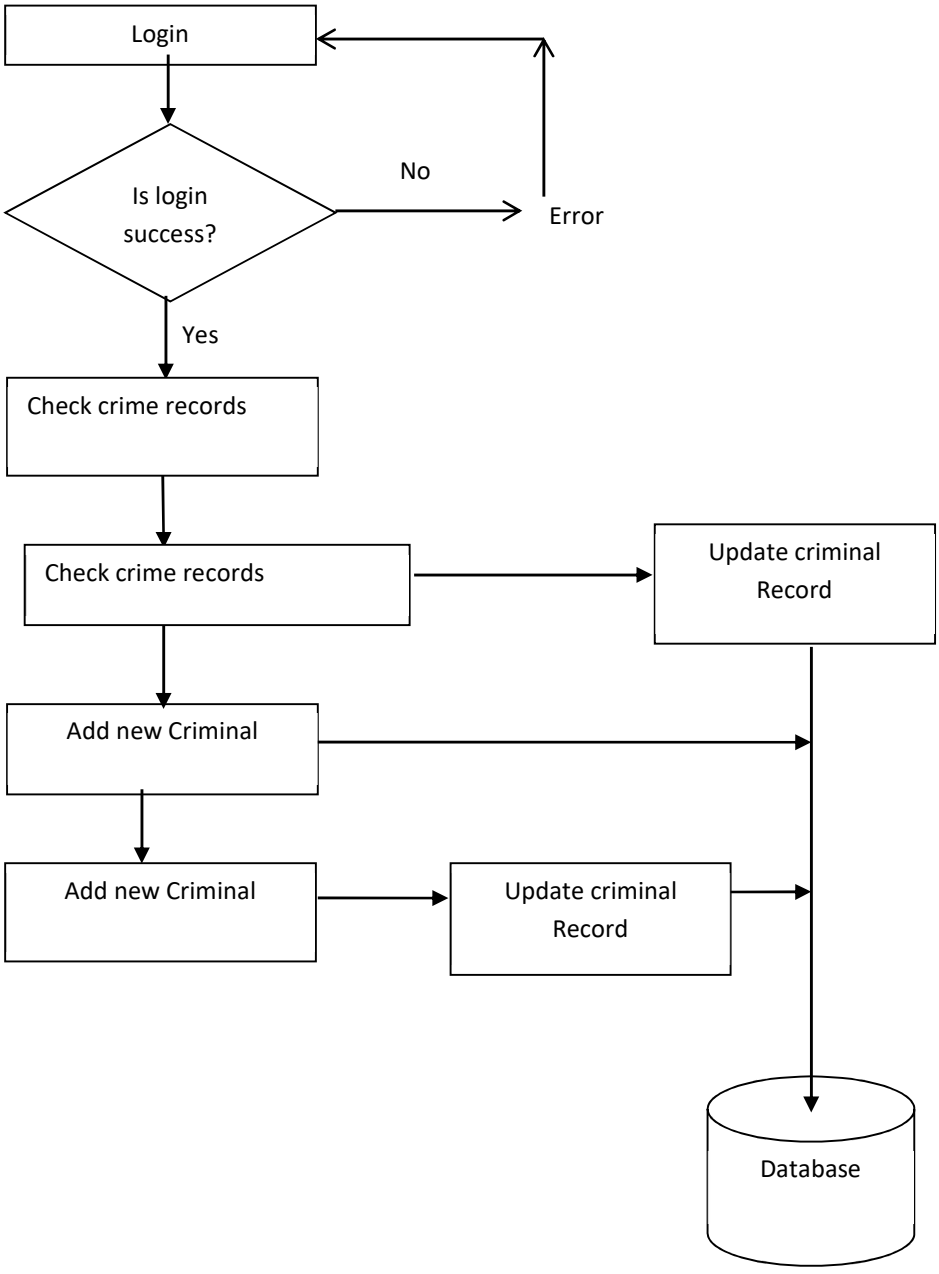

Fig 3: System Architecture and Flowchart

4. IMPLEMENTATION AND RESULT

This section deals with the implementation and result of the proposed system for verification and validation of the various program function/modules embedded in the design. It introduces the software and hardware requirements for the system to work properly.

4.1. Application Screenshot

Fig 4: Face Capture interface

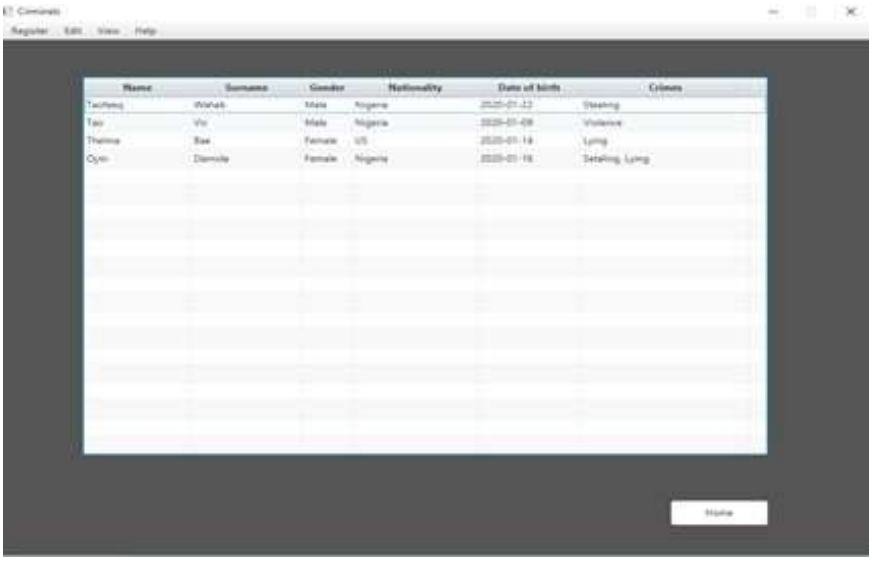

Fig 5: Interface for List of all Recorded Criminal

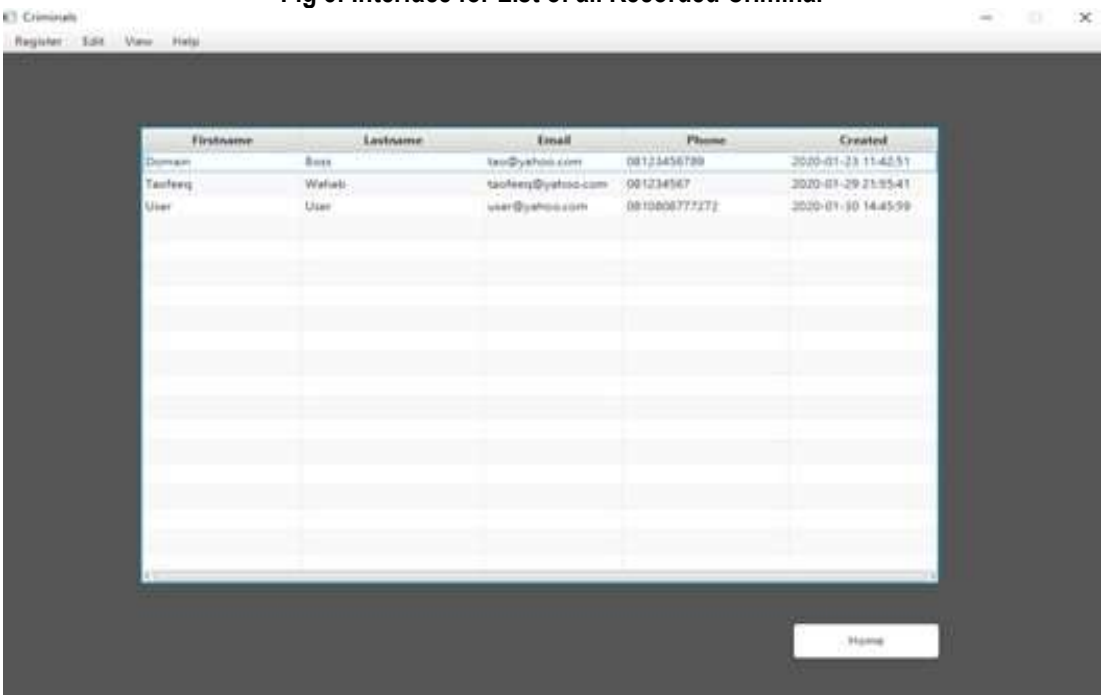

Fig 6: Interface for List of Administration

5. SUMMARY AND CONCLUSION

5.1 Summary

Criminal Identification using Face Matching System is a challenging problem in the field of image analysis and computer vision that has received a great deal of attention over the last few years because of its many applications in various domains. Face detection and recognition technology was used for many purposes. Real-time detection and recognition of people in a camera setup especially for security purposes.

5.2 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.

REFERENCES

1. Alireza Chevelwalla, Ajay Gurav, Sachin Desai, Sumitra Sadhukhan (2015): Criminal Face Recognition System, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181, Vol. 4 Issue 03, March-2015
2. Bureau of Justice Statistics, U.S. Department of Justice, (April 1990), pp. 43-66; SEARCH Group, "Legal and Policy Issues Relating to Biometric Identification Technologies".
3. Deng Cai, Xiaofei He, Jiawei Han and Hong-Jiang Zhang (2006): "Orthogonal Laplacianfaces for Face Recognition", IEEE Transactions On Image Processing, 2006.
4. E. Holden, R. Owens (2002): "Automatic Facial Point Detection," Proc. The 5th Asian Conf. on Computer Vision, 23-25 January 2002, Melbourne, Australia.
5. Hui-Xing, J., Yu-Jin, Z. (2009): Fast Adaboost Training Algorithm by Dynamic Weight Trimming. Chinese Journal of Computers
6. Jyoti Nautiyal, Shivali Gahlot, Pawan Kumar Mishra (2013): An Automated Technique for Criminal Face Identification Using Biometric Approach, Conference on Advances in Communication and Control Systems 2013 (CAC2S 2013).
7. L. Sirovich and M. Kirby (1987): Low-dimensional procedure for the characterization of human faces, Journal of the Optical Society of America A, 4, (1987), pp. 519-524.
8. N.Niranjani, B.Tharmila, C. Sukirtha, K. Kamalraj, S. Thanujan, P. Janarthanan, N. Thiruchchelvan, K. Thiruthanigesan (2017): *The Real Time Face Detection and Recognition System*, International Journal of Advanced Research in Computer Science & Technology (IJARCST 2017), Vol. 5, Issue 4 (Oct. - Dec. 2017)
9. Nurul Azma Abdullah, Md. Jamri Saidi, Nurul Hidayah Ab Rahman, Chuah Chai Wen, and Isredza Rahmi A. Hamid (2017): Face Recognition for Criminal Identification: An implementation of principal component analysis for face recognition, *The 2nd International Conference on Applied Science and Technology 2017 (ICAST'17)*
10. Piyush Kakkar, Mr. Vibhor Sharma (2018): Criminal Identification System Using Face Detection and Recognition, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 7, Issue 3, March 2018
11. Stan Z. Li, Anil K. Jain, "Handbook of Face Recognition", With 210 Illustrations, Springer
12. Viraj, Pradip More, Pankaj Thombre, hweta Malvi (2015): Criminal Detection Using Eigenfaces Approach on Android Device, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1), 2015, 539-541
13. Wencheng Yang, Song Wang, Jiankun Hu, Guangzhou Zheng and Craig Valli (2019). Security and Accuracy of Fingerprint-Based Biometrics: A Review, Page-1-19