

Criminal Face Detection Using Machine Learning

Prof. Anup Ganji, Rashmi Kamat, Swapnali Chougule Pooja Biradar, Srushti Gadivaddar

Dept. of Computer Science & Engg.

Vsmsrkit Engg College

KA, India

Nipani anupganji1991@gmail.com, rashmikamat01@gmail.com, swapnalichougule853@gmail.com, poojabiradar110@gmail.com, srushtigadivaddar@gmail.com

Abstract- In practice, identification of criminal in Malaysia is done through thumbprint identification. However, this type of identification is constrained as most of criminal nowadays getting cleverer not to leave their thumbprint on the scene with the advent of security technology, cameras especially CCTV have been installed in many public and private areas to provide surveillance activities. The footage of the CCTV can be used to identify suspects on scene. However, because of limited software developed to automatically detect the similarity between photo in the footage and recorded photo of criminals, the law enforces thumbprint identification. In this paper, an automated facial recognition system for criminal database was proposed using known Principal Component Analysis approach. This system will be able to detect face and recognize face automatically. This will help the law enforcements to detect or recognize suspect of the case if no thumbprint present on the scene. The results show that about 80% of input photo can be matched with the template data.

Keywords- Machine learning, face recognition, criminal identification, CCTV.

I. INTRODUCTION

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. 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.

In other hand, in Malaysia, most cases are investigated by using thumbprint identification to identify any suspect for the case. However, because of unlimited knowledge through internet usage, most criminals are aware of thumbprint identification. Therefore, they become more cautious of leaving thumbprint by wearing gloves except for nonpremeditated crimes. This paper to propose a facial recognition system for a criminal database where the

identification of the suspect is done by facematched rather than thumbprint matched.

II. LITERATURE REVIEW

In this paper, the authors are taking help of the CCTV footage and comparing the images from the footage with criminal database if they didn't find any fingerprint from the crime scene.

This system consists of five stages where the first stage is planning in which the why and how the system is made are discussed. The second stage of Requirement analysis discussed the requirement to design the system. Design, the third stage where they defined system design and its workflow. The fourth ultimate important stage is Implementation and testing, system is implemented using Principal Component Analysis (PCA) Technique and tested. The last stage is maintenance; this phase hadn't undertaken due to this system was developed in a controlled environment. For criminal identification, authors had used PCA Technique for finding similar features of images available in the database with captured images of footage.

The machine will use a database that contains the person's personal information so that if FRCI identifies a face, it can display the person's information. The system interface is implemented using Visual Studio Code and database and coding using MATLAB R2013b. They achieved 80% accuracy using the proposed model.

This paper consists of four steps, the first one is real-time image training and the second one is Harr-classifier using

for face detection. The third step is the comparison of Surveillance camera captured images with real-time images and last, is the result part based on the comparison. The authors are using the Haar-classifier on Open-CV for face detection; Haar-cascading is one of the algorithms for face detection. On the openCV platform, face tracking is taken with help of Harr-like classifiers. More than one person is identified in this system and it can be used to find the suspects whom we are finding. The accuracy of the proposed system is very high as compared to the previous model. They also told us that we use or Adhar database we can easily identify the Indians and foreigners and further can investigate whether a person is a criminal or not. We can use this system by taking the citizenship database which is already available.

III. FACE RECOGNITION OVERVIEW

Face recognition in simple words means identifying and recognizing an individual on the basis of pictures of their faces.

1. Face Detection:

The first step is to check that human faces should be close enough to detect the faces this faces which will be captured and stored the face alignment which take place to capture faces from different angles automatically and it starts pre-processing the faces which can be used for image and video classification.

2. Feature Extraction:

After the detection, the faces are extracted and they are stored the extraction will be carried out for every different expression and feature extraction is done to remove dimensionality reduction and noise.

3. Face Recognition:

This is the last step which the automatic face recognition is done through the database where each face are stored in it when the face is detected in front of the webcam we use face detection and feature extraction and match that face with the database identification tells us that given face system needs to identify and verify it.

IV. PLANING

Planning phase is where the system is being planned, why and how the system will be made are also discussed in this phase. It is divided into two steps as follows:

1. Project Initiation:

A preliminary analysis is undertaken about how to collect face images to be used as the template to the system.

2. Project Planning:

Determining the correct technique/ software to do the detection and recognition

3. Requirement Analysis:

Requirement analysis describes the analysis that is required in order to develop the proposed system through functional requirements and non-functional requirements. Functional requirements outline what the system should do and support the user activities in performing and completing tasks by using the proposed FRCI. The list below shows the functional requirements for FRCI. x The system allows the user to log in by using username and password given default as "admin". x The system allow user to input image to be matched. x The system allows image to be compared.

x The system provide matching event if the input has more than 70% similarity with the image in the face database. The non-functional requirements describe the FRCI's security implementation that includes authentication by login, PCA and Eigenface algorithm.

V. DESIGN

System design defines the architecture, components, modules, interfaces and data for a system requirement. Figure 1 presents the overall system design of Facial Recognition.

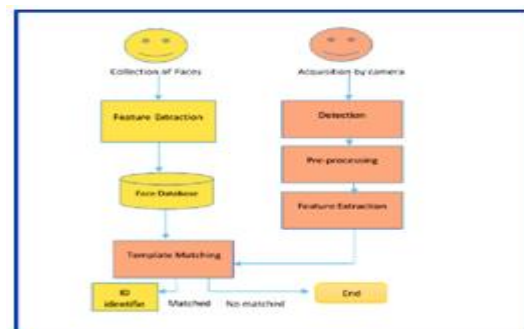


Fig 1. Architecture of Facial Recognition.

According to Figure 1, the first step is to create face databases as the match template for the system. A face database is created by acquiring collection of people photos. The photo should be half body photo where the face is facing front. In the process of verification of id for an image, the image which is captured using digital camera will be processed. The image will be detected and extracted and ready for the next stage. The next stage is pre-processing, where unnecessary features are eliminated.

This is to reduce unnecessary processing effort. In the feature extraction, the images are collected 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. All these photos then are processed using PCA procedures to get the Eigenface as the basis or standard features of human face. These features will be used in recognition phase where it try to match with the correct image in the database. If

matched, the identification of the image will be verified, else it will stop.

VI. IMPLEMENTATION AND TESTING

Implementation phase of FRCI involves implementation on the interface and on the backend coding. The system interface was implemented using Microsoft Visual Studio while the backend components, which are database and coding, were implemented fully using MATLAB R2013b.



Fig 2. Login - is used to login to application.



Fig 3. Registration- is used to register criminal.



Fig 4. Training Data - is used to train the images

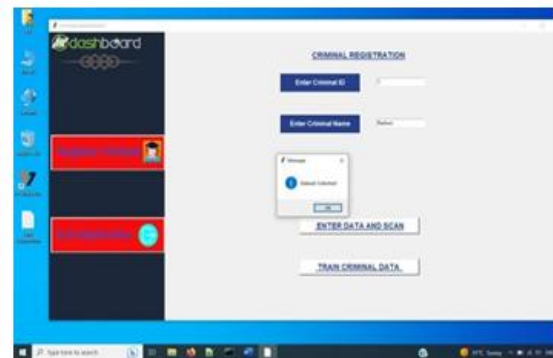
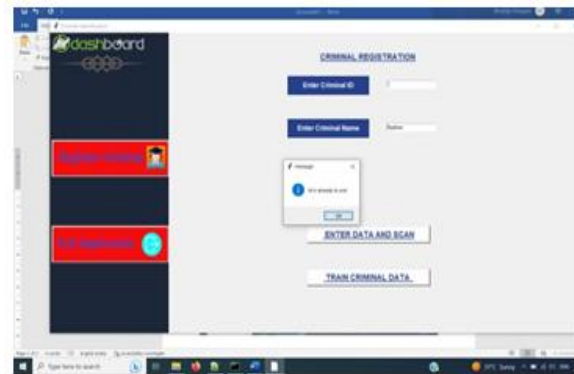


Fig 5. Criminal Dataset Collection & Testing

VII. RESULT AND DISCUSSION

This section highlights the main outcome of Facial Recognition and its advantages. This study aims to design, develop and test the Face Recognition for Criminal Identification, all system functionalities are running well and therefore, this study successfully achieved the objectives.

The main function of Facial Recognition— image identification, was programmed with detection and extraction of image, projecting image and recognition of the image. The user needs to input the image for identification for recognition process as shown in Figure 1. Once the

image is recognized, detected and extracted, all the necessary features are extracted for identification.

The main function of Facial Recognition — image identification, was programmed with detection and extraction of image, projecting image and recognition of the image. The user need to input the image for identification for recognition process as shown in once the image is recognized, detected and extracted; all the necessary features are extracted for identification.

Furthermore, since Criminal Facial Recognition is developed as an open source system, other experienced developer or amateur programmer can add new function to the system with ease. Also, they will be able to give it new design and even improve its recognition algorithm. Its simple design also makes it easier to use.

Overall, there are several advantages that have been identified as follows:

- As a better alternative for criminal identification instead of using thumb print identification.
- Automate most of the identification activities. For instance, criminal photo captured through CCTV just need to feed into the system for identification. The system will then run automatically from recognizing, detecting and extracting the image, features extraction and identification activities.

VIII. CONCLUSION AND FUTURE WORK

As for the future work, a lot more testing and debugging is needed as this system was developed in a very limited time and resources. However, since it is open source software, developer can easily add new function and improve the default function.

Additionally, the system can feature an image processing where the input image can be made less blurry so the system can detect face on lower quality images. Other than that, the system can use a database which contains the personal info of the person in the database, so whenever FRCI recognize a face, it will display the details about the person.

REFERENCES

- [1] S. H. Lin, "An Introduction to Face Recognition Technology", *Informing Science Special Issues on Multimedia. Informing Technologies*, 3:1, (2000).
- [2] R. Rathi, M. Choudhary & B. Chandra, "An Application of Face Recognition System using Image Processing and Neural Networks", *International Journal Computer Technology Application*, 3:1, (2012), pp. 45-49.
- [3] R. A. Hamid & J. A. Thom "Criteria that have an effect on users while making image relevance judgements", in *Proceedings of the fifteenth Australasian Document Computing Symposium*, (2010), pp. 76-83.
- [4] M. H. Yang, D. J. Kriegman & N. Ahuja, "Detecting Faces in Images: A Survey", *IEEE Transaction on Pattern Analysis & Machine Intelligence*, 24:1, (2002), pp. 34-58.
- [5] P. M. Corcoran & C. Iancu, "Automatic Face Recognition System for Hidden Markov Model Techniques", *New Approaches to Characterization and Recognition of Faces*, (2011).
- [6] M. Rouse, "Biometrics Definition", (2013). Retrieved November 23, 2016 from <http://searchsecurity.techtarget.com/definitions/biometrics>
- [7] L. Sirovich and M. Kirby, "Low-dimensional procedure for the characterization of human faces", *Journal of the Optical Society of America A*, 4, (1987), pp. 519-524.
- [8] M. A. Turk & A. P. Pentland. "Face Recognition Using Eigenfaces." MIT Vision and Modeling Lab.
- [9] M. F. Smith, *Software Prototyping Adoption, Practice and Management* (Mc-Graw-Hill, London, 1991).