Face recognition for criminal identification: An implementation of principal component analysis for face recognition

Cite as: AIP Conference Proceedings **1891**, 020002 (2017); https://doi.org/10.1063/1.5005335
Published Online: 03 October 2017

Nurul Azma Abdullah, Md. Jamri Saidi, Nurul Hidayah Ab Rahman, et al.

Face Recognition for Criminal Identification: An implementation of principal component analysis for face recognition

Nurul Azma Abdullah[a)], Md. Jamri Saidi, Nurul Hidayah Ab Rahman[b)], Chuah Chai Wen[c)], and Isredza Rahmi A. Hamid[d)]

Information Security Interest Group (ISIG)
Fakulti Sains Komputer dan Teknologi Maklumat, Universiti Tun Hussein Onn Malaysia, 86400 Batu Pahat, Johor, Malaysia

[a)] azma@uthm.edu.my
[b)] hidayahar@uthm.edu.my
[c)] cwchuah@uthm.edu.my
[d)] rahmi@uthm.edu.my

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 enforce 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.

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 [1, 2, 3]. 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 non-premeditated crimes. 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.

The 2nd International Conference on Applied Science and Technology 2017 (ICAST'17)
AIP Conf. Proc. 1891, 020002-1–020002-6; https://doi.org/10.1063/1.5005335
Published by AIP Publishing. 978-0-7354-1573-7/$30.00

The objective of this study is two-fold:

1. Matching a face with available database accurately.
2. Applying principal component analysis for finding distinguishable features from many images to get the similarity for the target image.

The remaining of this paper is structured as follows. Next section discusses on related concepts of this study and relevant previous works, design and development describes the whole processes of system development, result and discussion highlights the outcomes and advantages, and final section outlines conclusion and future work.

OVERVIEW OF FACE RECOGNITION SYSTEMS

Face Recognition for Criminal Identification is a face recognition system in which the security expert will input an image of the person in question inside the system and the system will first preprocess the image which will cause unwanted elements such as noise to be removed from the image. After that, the system will then classify the image based on its landmarks for example, the distance between the eyes, the length of the jaw line, etc. Then, the system will run a search through the database to find its perfect match and display the output. This work is focusing on implementing the system for criminal identification. Current practice of thumbprint identification which is simple and easy to be implemented can be challenge by the use of latent thumbprint and sometimes cannot be acquired from the crime scene. The criminals have become cleverer and normally be very careful in leaving any thumbprint on the scene. This system encompassed face database and an image processing algorithm to match the face feed with faces stored in the database.

There are two parts vital to the success of this system; detection and recognition. A face detection is one of the most important steps in a face recognition system and can be classified into four principle categories; knowledge based, feature invariant, template matching and appearance-based methods [4]. In recognition, two stages are required; training process and evaluation process. In a training process, the algorithm is fed samples of the images to be learned and a distinct model for each image is determined while in an evaluation process, a model of a newly acquired test image is compared against all existing models in the database. Then the near corresponding model is acquired to determine whether the recognition is triggered [5]. In this stage, a statistical procedure, Principal Component Analysis (PCA) is used to on a collection of face images to form a set of basis features, which is called a set of eigenfaces. Any human face can be considered to be a combination of these standard face.

Related works

Biometrics is came from Greek words, Bio which means “life” and Metrics, which means “to measure”. According to [6], an editor from techtarget.com, biometrics is the measurement and statistical analysis of people’s physical and behavioural characteristics. This technology is widely used by a security firm for identifications, authentications and access control purpose. Other than that, it is also used by a crime investigation unit in order to identify individuals based on things like thumbprints, voiceprints and faces or even their physical condition.

In general, there are two types of biometric method, the first one is Physical Biometrics which is used for verification purposes. This method uses fingerprints, face, hand, and eyes, but not limited to this five things only because biometrics cover a lot of area. The second one is Behavioural Biometrics. It is used for identification and also verification process. This method looks at our behaviour. Example of this method is a keystroke recognition and speaker identification.

Facial recognition system has been used by organizations like Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), Facebook and other big companies such as Apple, ASUS and so on. It is being used for various reason but not limited to help users in identifying, verifying and searching the face of a person over a large database of faces. Basically, face recognition works by first reading the input image and pre-process the image, in which unwanted element in the face is removed. After that, the image is compared to the one in the database and the system display the matching image.

Face detection is the first step in developing a facial recognition system. This is where the system detect the face and determines whether it is indeed a human face or otherwise. It also determines whether the system can distinguish between the subject and the background thus allowing it to detect and recognize faces easily.

Eigenface is probably one of the earliest and first successful algorithm developed by [7] 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 [8]. 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.

THE DESIGN AND DEVELOPMENT OF FRCI

The whole FRCI development activities are presented in this section. This study was carried out using evolutionary prototyping methodology adopted from Smith [9] that consists of five phases, namely: (1) planning; (2) requirement analysis; (3) design; (4) implementation and testing; and (5) maintenance – this phase was not formally undertaken due to FRCI was developed in a controlled environment.

Planning

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.

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.

- The system allows the user to log in by using username and password given default as “admin”.
- The system allow user to input image to be matched.
- The system allows image to be compared.
- 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.

Design

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

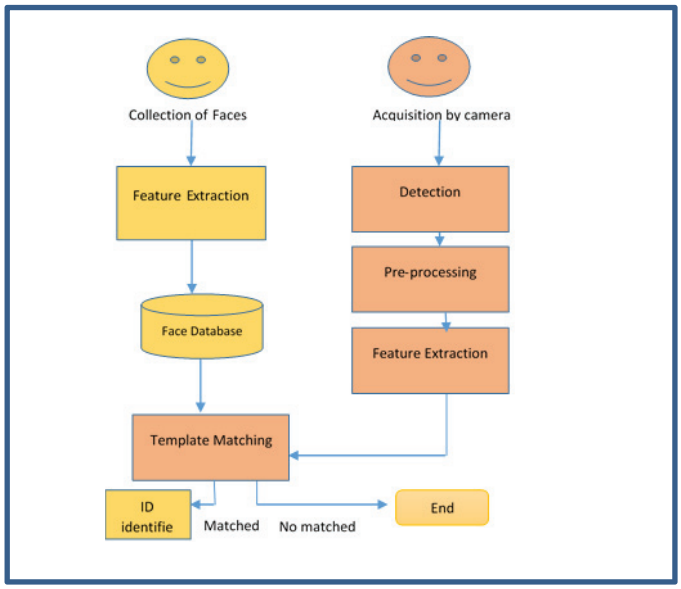

FIGURE 1: Architecture of FRCI

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.

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.

```
function OutputName = Recognition(TestImage, m, A, Eigenfaces)
```

FIGURE 2: Recognition Function Code

Figure 2 shows the function OutputName for the purpose of recognizing the image. This function takes four parameters which are the TestImage, m, A, and Eigenfaces. TestImage is the input image which we want to find the matching image in the databases. *m* is the mean image in the database and *A* is the deviation of the images. Lastly, Eigenfaces is the Eigen vectors of the covariance matrix of the training database. Next is to project the image to be

stored. Then, the most important step in this system which is extracting necessary features for matching procedures is started.

```
InputImage = imread(TestImage);
temp = InputImage(:,:,1);

[irow, icol] = size(temp);
InImage = reshape(temp',irow*icol,1);
Difference = double(InImage) - m; %Centering the image
ProjectedTestImage = Eigenfaces'*Difference;
```

FIGURE 3: Feature extraction

Figure 3 show steps in extracting all features for matching procedures. Line 1 of the function will read the input image. On line 2, a *1*-dimensional temporary file of the input image is created. Line 3 is to set size of the image file, remember that the dimensionality should be the same for all images. Line 4 will reshape the image by *m x n* resolution and then the face feature are extracted from the input image. Next, it will ready for identification procedures. Figure 4 and Figure 5 shows the example of identification process.

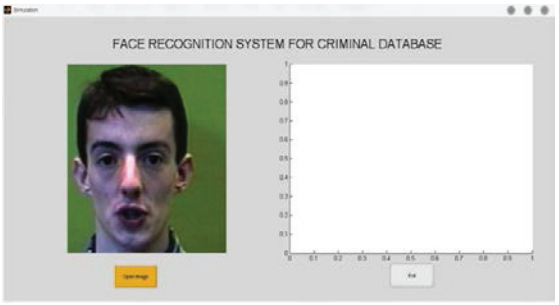

FIGURE 4: Chosen image is displayed in the left hand side

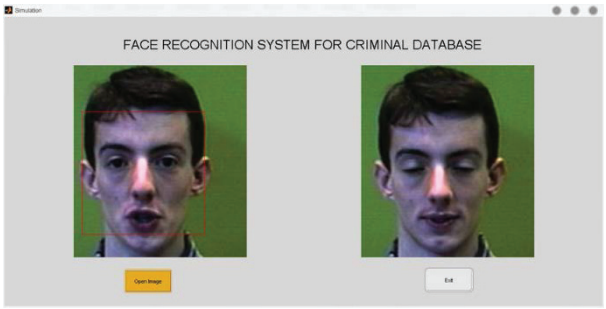

FIGURE 5: FRCI after identification of a person face

RESULT AND DISCUSSION

This section highlights the main outcome of FRCI 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 FRCI—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 Figure 1. Once the image is recognized, detected and extracted, all the necessary features are extracted for identification

There are many other similar software out there that provide the same functionality as FRCI, however, FRCI also has its own benefits that can contribute to society. Developing an automated facial recognition system can be challenging given its complexity and limited exposure, however with FRCI, students without knowledge to the biometrics system can use the source code to study the basic of facial detection and recognition system. Other than that, FRCI also features a user-friendly interface that requires minimum interaction between the users. With FRCI, users only need to input an image in the database and the system will do the rest.

Furthermore, since FRCI 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.

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 an 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 contain the personal info of the person in the database, so whenever FRCI recognize a face, it will display the details about the person.

ACKNOWLEDGMENTS

The authors would like to thank Ministry of Higher Education (MOHE), for granting RAGS Grant (Vote R066) to support this research. The authors would also like to thank Universiti Tun Hussein Onn Malaysia (UTHM) and Gates IT Solution Sdn. Bhd. for supporting this research. Thanks to anonymous reviewer for valuable comments.

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, Practise and Management* (Mc-Graw-Hill, London, 1991).