MULATU GEBEYAW ASTARKIE IMPROVING ETHIOPIAN POLICE CLEARANCE CERTIFICATION USING FACE BIOMETRICS NEU 2018

IMPROVING ETHIOPIAN POLICE CLEARANCE CERTIFICATION USING FACE BIOMETRICS

A THESIS SUBMITTED TO THE GRADUATE SCHOOL OF APPLIED SCIENCES OF

NEAR EAST UNIVERSITY

By

MULATU GEBEYAW ASTARKIE

In Partial Fulfilment of the Requirements for the Degree of Master of Science in Software Engineering

NICOSIA, 2019

IMPROVING ETHIOPIAN POLICE CLEARANCE CERTIFICATION USING FACE BIOMETRICS

A THESIS SUBMITTED TO THE GRADUATE SCHOOL OF APPLIED SCIENCES OF

NEAR EAST UNIVERSITY

By

MULATU GEBEYEAW ASTARKIE

In Partial Fulfilment of the Requirements for the Degree of Master of Science in Software Engineering

NICOSIA, 2019

MULATU GEBEYAW ASTARKIE: IMPROVING ETHIOPIAN POLICE CLEARANCE CERTIFICATION USING FACE BIOMETRICS

Approval of Director of Graduate School of Applied Sciences

Prof. Nadire CAVUS

We Certify that this thesis is satisfactory for the award of the degree of Master of Science in Software Engineering

Examining Committee in Charge:

Asst. Prof. Dr. Boran Sekroglu	Head of the Department of Information Systems Engineering, NEU
Asst. Prof. Dr. Yöney Kırsal EVER	Head of the Department of Software Engineering, NEU
Assoc. Prof. Dr. Kamil Dimililer	Supervisor, Department of Automotive Engineering, NEU

I hereby declare that all information in this document has been obtained and presented in accordance with the academic rules and ethical conduct. I also declare that, as required by these rules and conducts, I have fully cited and referenced all materials and results that are not original to this work.

Name, Surname: Mulatu Gebeyaw, Astarkie

Signature:

Date:

ACKNOWLEDGEMENTS

First and foremost, I would like to thank the Almighty God for giving me the strength, knowledge, ability and opportunity to undertake this research study and to persevere and complete it satisfactorily. Without his blessings, this achievement would not have been possible.

Next, I would like to express my sincere gratitude to my supervisor, Assoc. Prof. Dr. Kamil Dimililer for the continuous support of my MSc. research, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis.

Besides my supervisor, I would like to thank the rest of my thesis committee members: Asst. Prof. Dr. Boran Sekroglu, and Asst. Prof. Dr. Yöney Kırsal EVER, for their encouragement, insightful comments, and hard questions.

In particular, this note of thanks also goes to Asst. Prof. Dr. Boran Şekeroğlu, for his invaluable information and advice during my educational stay.

I also would like to thank Ethiopian Ministry of Science and Higher Education for giving me the opportunity to study here in Near East University by covering all my educational fees.

Above all, I would like to forward my hearty acknowledgement to all my families and my fiancée being patient, spiritual, and their motivational moral support to complete the thesis. Last, but not the least, a lot of thanks goes to my friends.

To my parents and my fiancée…

ABSTRACT

Police clearance certificate is required to make sure that a person has never partaken in any criminal activity for employment and/or to meet the requirements of the immigration rules for the visa application. However, tasks' labor intensiveness, too much processing time, and identifying criminals accurately are the headache and prominent problems in the bureau. To improve the police clearance certification and to overcome these challenges in the bureau, a prototype, face biometrics criminal identification technique is developed. The prototype is developed using python and Django framework. We use Eigenface recognition, principal component analysis, and support vector machine for the prototype where the principal component analysis is used for diminishing dimension of the face images, and support vector machine is used for feature classification and modeling the recognition algorithm along with Eigenface recognizer. The experimental result shows Eigenface recognition has limitations in light conditions, and this needs a special room where the light becomes consistent enough. However, again the experimental result shows 90% accuracy in identifying of criminals and noncriminal samples. Furthermore, the developed prototype is one step ahead in designing the recognition to be web based, and the prototype can be accessed in the internet in such a way that users can use it in GUI mode. Supporting the work to be done in the bureau by using face biometrics technique is advisable to overcome the prominent problems faced so far in the bureau so that tasks will be accomplished within a minute and as a result customers become satisfy for the service.

Keywords: police clearance certificate; support vector machine; principal component analysis; pattern recognition; Haar-like features; face biometrics; criminal identification

ÖZET

Polis izni belgesi, bir kimsenin istihdama herhangi bir suç faaliyetinde bulunmadığından ve / veya vize başvurusu için göçmenlik kurallarının gerekliliklerini yerine getirmediğinden emin olmak için gereklidir. Bununla birlikte, görevlerin emek yoğunluğu, çok fazla işlem süresi ve suçluları doğru bir şekilde tanımlaması, bürodaki baş ağrısına ve öne çıkan sorunlardır. Polis izni sertifikasyonunu geliştirmek ve bürodaki bu zorlukları aşmak için bir prototip, yüz biyometrisi suç tanımlama tekniği geliştirilmiştir. Prototip, python ve Django çerçevesi kullanılarak geliştirilmiştir. Eigenface tanıma, temel bileşen analizi ve yüz bileşenlerinin boyutunu azaltmak için temel bileşen çözümlemesinin kullanıldığı prototip için vektör makinesi desteği ve Eigenface tanıyıcı ile birlikte özellik sınıflandırması ve tanıma algoritmasını modellemek için vektör makinesi kullanılır. Deneysel sonuç Eigenface tanımanın ışık koşullarında sınırlamalara sahip olduğunu gösterir ve bunun ışığın yeterince tutarlı hale geldiği özel bir odaya ihtiyacı vardır. Bununla birlikte, yine deneysel sonuç, suçluların ve suç teşkil eden olmayan örneklerin belirlenmesinde% 90 doğruluk göstermektedir. Dahası, geliştirilen prototip, web tabanlı olma bilincinin tasarlanmasında bir adım önde ve prototipe, kullanıcıların GUI modunda kullanabilecekleri şekilde internette erişilebilir. Büroda yüz biyometri tekniğini kullanarak yapılacak çalışmanın desteklenmesi, büroda bugüne kadar karşılaşılan önemli sorunların üstesinden gelinmesi ve böylece görevlerin bir dakika içinde yerine getirilmesi ve sonuç olarak müşterilerin hizmet için tatmin olmasının sağlanması tavsiye edilir.

Anahtar Kelimeler: Polis izni belgesi; destek vektör makinesi; temel bileşenler analizi; haar benzeri özellikler; yüz biyometrisi; cezai kimlik

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

API: Application programming interface

ATM: Automated teller machine

EFCFID: Ethiopian Federal Commission Forensic Investigation Department

EFPC: Ethiopian Federal Police Commission

FPCIB: Federal Police Crime Investigation Bureau

GUI: Graphical User Interface

PCA: Principal Component Analysis

PC: Police Clearance

PCC: Police Clearance Certificate

PCB: Police Commission Bureau

SVM: Support Vector Machine

PKL: Pickle

CHAPTER 1

INTRODUCTION

Nowadays most countries apply biometric technologies in different modalities in different service delivery bureaus either to support the service they deliver or for security purpose. Among these bureaus, EFPCB is one which gives different services in Ethiopia, especially in personal security and identifications of criminals in the country.

The EFPC is one of the governmental bureaus in Ethiopia which has different duties and responsibilities (Service-Crime-Federal Police Commission, 2018). Besides these duties and responsibilities, conducting a forensic investigation, disposing fingerprints, and issuing clearance certificates are the major duties and responsibilities of EFCFID.

PCC is issued by the FPCIB which prepares a report that the applicant has never partaken in any criminal activity under EFCFID. This report is required to offer to citizens in Ethiopia for employment and other issues or to meet the requirements of the immigration rules to provide an overseas criminal record certificate for the visa application. For this PC certification, countries other than Ethiopia implement different biometric modality (Gaurav Kataria(Ph.D.), 2015) like a fingerprint, face, iris, speech, giant, and signature etc. for identification and verification of people.

Face recognition is the process of identification faces from a photo or video of a person and it works by taking the photo from camera or other else methods and compare this photo frame by frame from a set of faces in the database. It has a high rank in terms of universality, performance, collectability, acceptability, and circumvention (Anum K. and Monika S., 2016). Furthermore, face recognition comes to provide the criminal investigation technology recently (Fingerprint Recogntion vs Facial Recognition, 2018) by taking personal facial structure as an individual characteristic in identifying and authenticating a person factually.

Most importantly, from physiological modes of biometric techniques, face recognition is the ideal means of recognizing an identity of an individual by people (Akarun, 2005). In addition to

its robustness and non-intrusiveness, it is natural as human brains have a natural ability to remember and distinguish different faces. The author indicated that, indeed, applications of face recognition are continuously growing all over the world; and airports in the most developed countries already adopt this technology to faster the immigration process and tighten the security and authorizing persons to access secured systems.

Face recognition is highly convenient and cost effective biometric modality, and it can be implemented with literal cameras and tools (Face Recognition Vs Fingerprint: 10 Key Differences To Know | Biometric today, 2018). The most, but not the least, deployed facial recognition applications are the following:

- Facebook's face recognition technology
- China's bet on facial recognition
- Biometric technology in Canadian airports.
- iPhone X uses the face as a biometrics password

In issuing PCC countries are using fingerprint biometric modality like India (Fingerprint Expert Delhi, FBI FD 258, RCMP Canada, 2018). In China, Chinese polices are using sunglasses with facial recognition (Chinese police now using sunglasses with facial recognition, 2018), and other twenty-one countries including US Airports, England, and Canada (21 Airport Facial Recognition Adoption Examples – BiometricToday, 2018) are using face recognition to identify and authenticate individuals.

1.1. Statement of the Problem

Currently, in Ethiopia, either Ethiopian or foreign citizens are required to have PCC either for their employment or immigration process. They are asked by the undertaking organization, and the organization gives a kind letter for individuals to bring PCC to the EFCFID. The problem is that EFCFID takes individuals fingerprint manually and this makes FPCIB inefficient and slow in giving services to customers.

Furthermore, individuals have to wait a minimum of two hours by making a queue either to get their turn to give a fingerprint or to take their result. Then the police take the fingerprint by blurring the blue ink color on their hands and fingers manually. After giving their fingerprint, also they have to wait more than a day to receive the PCC result.

The purpose of this PCC is to make sure that the requested individual is free from any criminal activity or otherwise. Most surprisingly, the process is a manual process, wearisome, time-consuming and less accurate. With the help of pattern recognition, biometric technologies are applied in forensic and surveillance to identify and recognize a person by using his biological character, and according to Bhatia (2013) face recognition is one of the leading physiological biometric to recognize people which is used in terrorist identification, criminal identification, and law enforcement purposes.

A report presented by (fanabc, 2018) noted the current challenges the customers faced in getting PCC in Ethiopia. Amongst the challenges, the limited number of bureaus available and the tasks' labor intensiveness are the prominent ones. As the report presented, this labor-intensive results from not using technologies to support the process. Furthermore, currently, Ethiopia has only one FPCIB which is named "Ethiopian Federal Forensic Department Bureau" which is located near "Black Lion Hospital" in Addis Ababa, Ethiopia. Furthermore, the accuracy of checking each and every one of the applicants from the criminals' record is depending on the ability and experience of the crime investigation officers and they have the responsibility in checking and identifying individuals as a criminal or otherwise. And, most of the time every one applied for PCC got free of any criminal records. This resulted from not using technological tools. The current working PCC offering system looks like in Figure 1.2 below.

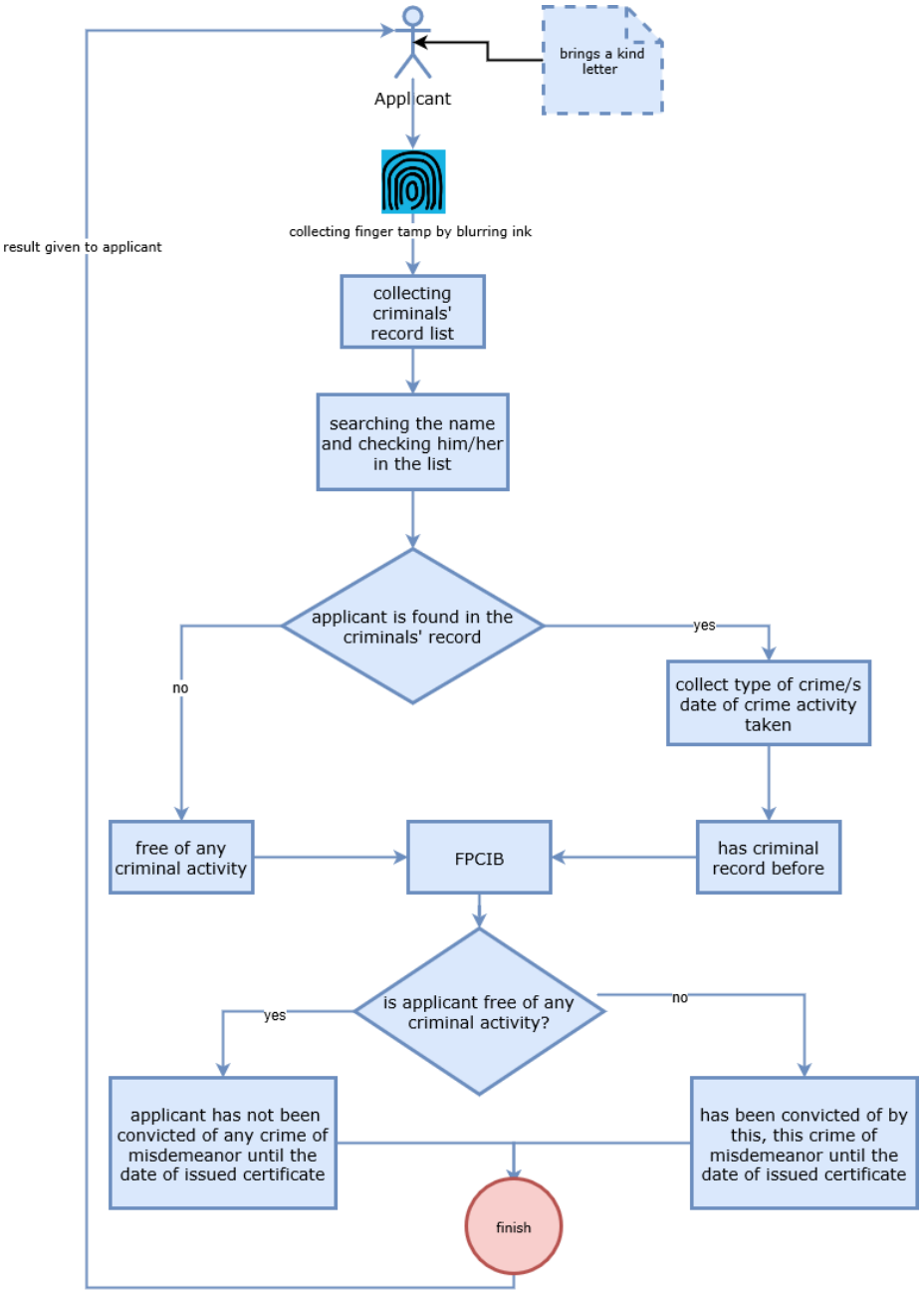


Figure 1.1: The current working PCC offering system model

1.2. Thesis Objectives

1.2.1. General objective

The general objective of the study is to show how the current PC certification platform can be improved in using face biometrics technique of identifying criminals, and then developing a prototype of this technique to prove that how it is going replace the current working framework.

1.2.2. Specific objectives

The specific objectives of this study to achieve the general objective are:

- ✓ Analyzing all necessary requirements required to get PCC
- ✓ Synthesizing the current working framework to offer PCC including forms, documents, and business regulations in which requirements will be generated from
- ✓ Examining and analyzing the efficiency of algorithms to develop face biometrics prototype (the detection, training, classification, and recognition algorithms)
- ✓ Training the recognition algorithm
- ✓ Testing the efficiency of the applied algorithm for detection, classification, and recognition of faces
- ✓ Proving how face biometrics criminal identification technique minimizes the processing time of offering PCC

1.3. Scope of the Thesis

The study aimed to implement face biometrics criminal identification prototype by identifying and analyzing the factors that constrain the prevailing manual police clearance certification in Ethiopia. However, the thesis limited its study on Haar-like feature and Eigenfaces algorithms which helps to develop face recognition based police clearance.

Furthermore, algorithms related to Haar-like features, Eigenfaces, detection, and recognition were studied. Altogether, the prototype implemented based on the Eigenfaces recognition approach, and trained faces which were taken using the live camera. In doing so, the recognition

application prototype has tested and evaluated by comparing with the current PCC offering framework to show how it improved.

1.4. Significance and Audience of the Thesis

Because the study is designed to implement face biometrics technique in offering PCC, in one way or another, it can play a great role in the country specifically for customers who are required to bring PCC for employment and immigration process, for the employees in the FPCIB, for students and other researchers in the area of biometrics technologies, machine learning, face detection and recognition.

Most importantly, the contributions of the study are the following:

- It reduces the queue time and increases the efficiency of PC Certtification
- It avoids the old-fashioned technique of blurring of blue ink color on customers' finger
- It reduces the workload of the polices in taking fingerprint of individuals and checking his/her criminal activity
- It can be used as a beginning for other researchers and programmers to develop biometrics based applications in the country
- It promotes other bureaus in the country to use biometrics technologies for their customers if needed

1.5. Organization of the Thesis

The thesis is grouped into six chapters including the introduction section. The first chapter is introduction of the thesis which discusses about the background, the problem statement, the objectives, scope and significance of the study as explained before in above sections.

Second chapter is the literature review of the study which revises literatures that are found to be relevant to the study including currently used biometrics techniques, comparison of those techniques using some comparison metrics, related works done previously in the area of face biometrics.

The third chapter is methodology and tools of the study which discusses the methodology and tools used, the approaches followed, and the methodology used by the researcher. It also includes analyzing of algorithms which are applied to develop the prototype.

The forth chapter is requirement analysis and modeling which deals on collecting and analyzing requirements including functional, user, and system requirements, modeling those requirements using the selected modeling technique including interactional, behavioral, and structural designs.

The fifth chapter is prototype development and experiment the developed prototype. In this chapter, some parts of the prototype and visualization the test result of the prototype are presented. Moreover, result analysis and conclusion of the study also explained and presented in this chapter.

The last chapter, but not the least, is conclusion and recommendations of the thesis. In this chapter, a conclusion is made according to the results obtained from the developed prototype and the experiment's results made. Recommendation also derived indicating the limitations obtained through the study, and suggestion is made to overcome those limitations.

CHAPTER 2

LITERATURE REVIEW AND RELATED WORKS

2.1. Biometrics System

Biometrics system in the field of machine learning and pattern recognition is an automatic recognition of a person using his behavioral and/or physiological characteristics (Anil K. Jain and et al, 2004). It is a quickly evolving technology and usually used in forensics and safety (Bhatia, 2013).

Anil K. Jain and et al (2004) and Bhatia (2013) stated two types of modes of biometrics systems: identification and verification.

1. ***Identification:*** is 1: N, i.e., used to answer the question "who are you?" in the system. It searches a match to recognize an individual from the database by using his/her own biological or physiological characters. Most importantly, it can only be proven through biometrics techniques (Anil K. Jain and et al, 2004).
2. ***Verification:*** is 1:1, i.e. used to answer the question "Are you …You?" that checks the correctness of an individual. In this mode an individual is required to provide additional verification tools to acquire some information about himself like a personal identity card or passport. This method works by comparing new provided biometric data with stored ones in the database. However, this method can be used by passwords, PINs, etc. as an alternative.

According to Bhatia (2013) and Anil K. Jain and et al (2004) the most widely used biometrics techniques are fingerprint scan, iris scan, hand geometry, face recognition, retinal scanning, signature verification, voice recognition, and keystroke recognition.

2.2. Comparison of Biometrics Techniques

The applicability of all biometrics techniques in today's world is not questionable at all and has a significant role in the current security and forensics systems. However, they do have strengths and weaknesses when we compare them using the same comparison metrics (Kapoor and Anup,

2016; Anil K. Jain and etal, 2004). Most important techniques and their comparison is presented as shown in Table 2.1.

As can be seen in Table 2.1, face recognition has better comparison metrics result than others, and it plays an important role in law enforcement (Kapoor and Anup, 2016). In this regard, face is the most commonly used and natural way of biometric characteristic used by humans to make a personal recognition (Anil K. Jain and et al, 2004; Akarun, 2005).

Table 2.1: comparisons of some biometrics techniques using the same comparison metrics

Technique	**Universality**	**Permanence**	**Collectability**	**Acceptability**	**Circumvention**
Face	High	Medium	High	High	High
Fingerprint	Medium	High	Medium	Medium	Medium
Iris	High	High	Medium	Low	Low
DNA	High	High	Low	Low	Low
Voice	Medium	Low	Medium	High	High
Signature	Low	Low	High	High	High
Keystroke	Low	Low	Medium	Medium	Medium

2.3.Application Areas of Biometrics Techniques in Identifying Criminals

Today biometrics techniques are used in our daily activity, and the most, but not the least, applicable areas of biometrics techniques are in:

- Commercial sectors (digital data security, e-commerce, ATM, medical record management) (Anil K. Jain and et al, 2004)
- Government organizations (driver's license, social security, border control, and passport control) (Anil K. Jain and et al, 2004)
- Forensics and security systems (criminal identification and investigation, terrorist identification, and finding missing children) (Anil K. Jain and et al, 2004; Kapoor and Anup, 2016)

Now face recognition is used in the surveillance system, law enforcement, criminal identification, and forensic investigation (Anil K. Jain and et al, 2004; Bhatia, 2013; Akarun, 2005).

2.4. Applicability of Face Recognition in Identifying Criminals

Even though, face recognition is a new research area in the field of machine learning and pattern recognition, it is applicable in different areas in different platforms which works based on object recognition principle (Riddhi P. and Shruti B., 2013; Vishnu G. and et al, 2017). It also used to check criminal records, recognizing patterns, enhancing security using cameras (Kaur and Himansh, 2015; Faruqe and Hasan, 2009).

2.5. Face Detection Via Haar-like Features

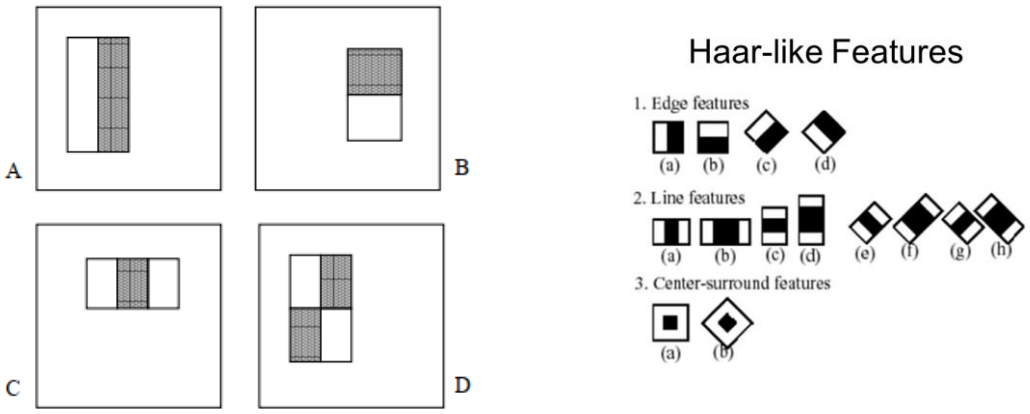
Face detection is used in digital cameras, smart phones, and etc. to autofocus faces from the background in the image. Before face recognition can be applied, the locations and sizes of any face must be first found. Besides, the most and first procedure in recognizing people is detecting faces from the given image in which face region will be localized and extracted from the background. Though, face detection is the task of identifying faces in an image by selecting region of interest.

2.5.1. Haar Cascade Classifier

Object detection using Haar feature-based cascade classifiers is a current object detection method that achieves enlarged detection achievement and reduce computational time (Viola and

Jones, 2001; Dr. Shoken and et al, 2013). The authors indicated that it is a machine learning approach where a cascade function is trained from face images and images without faces either using supervised learning or unsupervised learning. In doing so, the authors compare this technique with a pixel-based approach to show how it is faster in computing time. To prove this, they proposed Haar-like features extraction by using two color channels called grayscale image where each pixel of an image in a grayscale image is represented by black and white colors in OpenCV.

The Haar-like feature used by (Viola and Jones, 2001) reveals a rectangular structure and consists of two or four sub rectangles as can be seen in Figure 2.1. This technique computes an integral image from a pixel intensity of each sub-section by considering neighboring rectangular sections at a specific location in a detection frame.



(a) Common Haar-like Features b) Grouped Haar-like features

Figure 2.1: Viola and Jones Haar-like features

After the integral image and Haar-features calculated, selecting features and classifying them by using OpenCV Haar-cascade classifier follows (Viola and Jones, 2001; Delbiaggio, 2017). More generally, this Haar-cascade classifier algorithm works like this: first, selecting Haar-feature, and computing integral image follows then training the classifier from face and non-face images. Finally, cascading the classifier or grouping the features into different stages of classifiers and apply one-by-one.

2.6. Face Recognition Using EigenFaces

First and for most, it is better to look at a recap scenario to understand what face recognition is. When you look at your friend in your graduate magazine after some years of your graduation. You can identify each of your friends by looking at their photo in the magazine, because you have gathered their physiological features like their hair style, face color, eye, nose, lips, etc., and even their behavioral features like their signature and handwriting. This means that your mind trained all those features per each of your friends during your stay in the campus with them. While looking one of them in the magazine you can say that he is “Mulatu”, he is Mr. x, and so on. However, you may have forgotten some of your campus friends in the magazine. This is due to that you have not gathered enough features to recognize those guys during your stay in the campus. Nobody asks you why and how you did this, because it is a natural way of recognizing persons in our daily life. In doing so, you have doing three things: feature collecting per each of your friends, saving those identified features per each of your friends in your memory, and identifying and saying he is Mulatu, he is Mr. X.

Now the question is how to recognize people like this scenario using a machine learning. The answer is face recognition, which works like this: First, face from an image/video is detected and features are extracted from it. After features are extracted, normalization follows. Finally, feature classification leads to face recognition. The procedures involved during face recognition in machine learning are the same as we discussed it in the above scenario and leads the following three activities:

1. **Data gathering:** gather face data of the person's you want to recognize using OpenCv cascade classifier (Viola and Jones, 2001)
2. **Training the machine:** provide the face data and respective names of each face to the machine. Names used to say he is Mr. x during recognition process as you do in the scenario (Turk & Pentland, 1991; Siswanto and et al, 2014;).
3. **Recognition:** provide new persons' face to the machine and see the result obtained from the recognizer (Turk & Pentland, 1991; Siswanto and et al, 2014;).

Now the question is how to achieve all these activities in the machine learning framework. Here we go to answer these question in the following sections.

2.6.1. Feature extraction

In the above scenario, we have seen how your mind gathers Mulatu's eyes, nose, mouth, and face called features as can be seen in Figure 2.2 in which Viola and Jones features are mapped into grouped features in terms of eyes, nose and mouth.

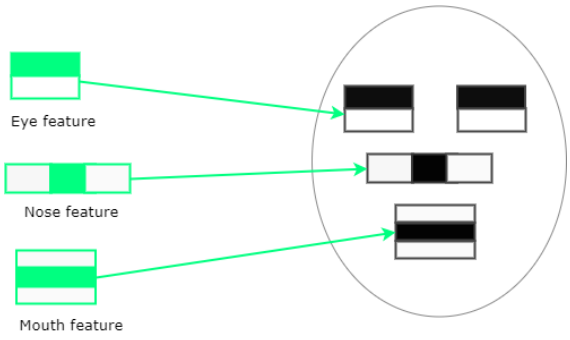


Figure 2.2: Mapped Haar-like features into grouped features

These features (eye, nose, and mouth features) used to train the machine. In machine learning using OpenCV, we can extract these features by using cascading technique with the help of PCA. PCA is the most powerful and the first choice if speed, accuracy, and performance are the dominant factors for the algorithm (Kaur and Himansh, 2015; Kim, 2002).

In the same case, according to Faruqe and Hasan (2009), no technique is available which meets all user requirements in all situations and in different applications in which face recognition

encounters. However, the authors indicate that whatever the case is the performance of the face recognition system cannot be a question and this performance is the dominant factor that is determined by the computational time to extract features and classifying them into groups. Besides this, the authors proposed PCA for feature extraction technique and SVM for classification and recognition.

Furthermore, to overcome face recognition challenges, PCA is absolutely the simplest and standard technique to implement, and has extremely fast computation time to extract the absolute most important and relevant information within a given face, and similarly, it tries to design a model that best describes it (Kaur and Himansh, 2015). The authors also said that PCA is not only used for performance rather it diminishes dimensions of a given face by preserving only the absolute most important information of the face, and reduces noise. This helps to save the storage of the face dataset.

Similarly, Bhardwaj and Gupta (2015) agreed in diminishing dimensionality of data components using PCA in which Eigenfaces obtained from covariance matrix of the trained dataset. Moreover, face contains a set of features and can be extracted using PCA if the performance of the face recognition is in questionable (Kaur and Himansh, 2015; Kim, 2002; Riddhi P. and Shruti B., 2013; Kim, 2002; Faruqe and Hasan, 2009).

In addition to PCA, in another way, Adnan K. and Kamil D. (2008) proposed image compression using Haar image compression and neural networks where the images are compressed manually using Adobe Photoshop from 256X256 to 64X64 and 32X32 to present images over the network by using greyscale imaging technique. To this end, their proposed system shows more than 93% of optimal compression ratio using their methods. However, the quality of the image in their implementation is in questionable due to the nature of lossy compression of the wavelet.

2.6.2. Face Recognizer

When you recognize your friend in the magazine in the above scenario (section 2.6), you are using his distinct features by comparing how they vary with respect to the other friends.

Therefore, you are making actual differences, which is called variance in mathematical term, of the face. Of course, it is not doubt how we are differentiating each other by color, eye, nose, lips, and etc. When you look at multiple faces in the graduation magazine you comparing them by looking at these parts of the faces because these parts are the most useful and important components of a face. Most importantly, because, they catch the maximum change among faces. This is definitely how Eigenfaces works (Turk & Pentland, 1991).

Eigenfaces which is a face recognizer approach, looks at all the trained faces (in the face dataset) of all the persons in the dataset as a whole. According to the authors (Viola and Jones, 2001; Bhardwaj and Gupta, 2015; Faruqe and Hasan, 2009), it tries to extract the principal components which are absolutely important and useful (the components that catch the maximum variance) and rejects the rest of the principal components.

Bhardwaj and Gupta (2015) argued that extracting of the principal components is not only extracts the important components from the training data also saves memory by removing the less important components (diminishing dimensionality). Moreover, Eigenfaces considers the fact that not all parts of a face are equally important (Kaur and Himansh, 2015; Faruqe and Hasan, 2009; Bhardwaj and Gupta, 2015).

The covariance (used in PCA) measures the spread of the data. This variance has results either high variance (direction of maximum information) if the data are spread out or low variance if the data are spread closer as described in chapter three in detail. This maximum variance is called the principal component.

2.7. Related Works with the Implementation of Face Recognition Algorithms

There are a number of applications developed for the purpose of simulating face recognition algorithms in real time applications in different target areas. Face recognition is applied in criminal identification, object tracking, door closing and access control, and time attendance. However, all these shortlisted areas of face recognition applications are developed using different approaches and algorithms. Some of them have limitations in preferring image quality,

computational time, platform selection, and user interactions. However, whatever limitations they do have, they play a great contribution for the advancement of face recognition to be here today. In one way or another, the researcher reviewed some of the works done before related to the proposed system.

A research conducted by Abdullah and et al (2017) developed face recognition algorithm for time attendance based system as a biometrics approach in Malaysia to detect faces of criminals to make detection to be automatic. The authors proposed to change the current criminal identification system of Malaysia from thumbprint into face recognition using a template matching approach using PCA. However, the algorithm is limited only to store faces of criminals without the required information of the suspected individual like his/her name. The algorithm needs more storage space in comparing matches of faces among the faces stored in the dataset. This is the limitation of the algorithm they proposed in addition to the computational cost. Furthermore, the recognition algorithm has limitation in classification and prediction of criminals, but the algorithm resulted 80% accuracy of prediction as they said.

Similarly, but in somewhat, Siswanto and et al (2014) developed face recognition algorithm for biometrics based time attendance system. The authors implemented face recognition algorithm as biometrics technique in the attendance system using Eigenface and Fisherface. Eigenface algorithm resulted 70% to 90% and it is better than Fisherface algorithm as presented in their paper. However, during the implementation of the attendance system taking sample faces needs take care in removing lighting and they used black background behind the students. This is limited only on genuine images and preparing this type of places is another problem in implementing real time face recognition.

Nautiyal and et al (2013) proposed an automatic face recognition method to identify criminals using image partition algorithm where sample faces are extracted from the scanned image using scanner. Furthermore, the algorithm implements pixel based data representation which leads requiring quality images and more storage space.

Piyush and Vibhor (2018) proposed a face detection and recognition based criminal identification technique. The authors used Haar feature-based cascade classifiers for face detection and Local Binary Patterns Histograms(LBPH) for face recognition. They used LBPH recognition algorithm to extract feature efficiently and to recognize faces in different lighting condition. However, this face recognition approach has storage limitation and computational cost during training and recognition phases even if single training image for each person is possible. Most importantly, the authors have developed a system to store criminal information to view the history of the criminal's later.

The researcher noted, whatever the case is, some of these proposed face recognition implementations are command based and desktop based. So that they cannot be applied for surveillance system and criminal identification from far away to the system they configured. Most importantly, what is needed to be improved is how to make face recognition biometrics technique possible to be implemented over the internet and how to make it easy to use using server based scripts and to extends its accessibility to be 24/7.

Furthermore, all these authors indicate that the computational cost and diminishing dimension are the limitations and needs to be improved. However, some of them applied PCA for diminishing this dimension but making it vector based is important for genuine images.

CHAPTER 3

METHODOLOGY AND DESIGN OF THE STUDY

3.1. Methodology and Tools

This thesis is an experimental research, and the experiment and testing of the thesis results have been evaluated based on the facts of the data collected and procedures adopted through the implementation of the thesis.

3.1.1. Data source

Data source, in the technical definition of this study, is the source of information for the study in which the researcher used to collect data, validate data, and use the information during the design (modeling), experiment and testing of the study. In addition to reviewing literature, the study mainly used currently used forms as document analysis and personal observation.

A. Clearance certificate letter

Currently used working framework in FPCIB uses different forms to offer PCC to individuals, private, and governmental bureaus. Among these forms, PCC result announcing form is used, which is given to customers to take for the undertaken bureau. This PCC is valid and authorized by FPCIB. Everyone who gets this certificate is free from any of criminal records in the country and oversea criminal records according to the country context or other ways. The researcher used this currently used certificate form to extract and analyze required data and for requirements elicitation purpose.

B. A kind letter

A kind (supportive) letter is written to FPCIB to investigate criminal records to whom who brings this kind letter. The letter is taken by hand of the requested individual. This letter is valid and authorized because it has the official seal of the bureau which request the clearance

certificate. The researcher used this kind letter to extract information which are required in the prototype of the thesis like personal information attribute and to validity of the letter.

3.1.2. Data Collection

For the development of the prototype of this study, the researcher used the following data collection techniques either for the primary or secondary data sources.

A. Observation

Observation is a systematic data collection approach in which the researcher gets a chance to check the current workflow of the PCC offering system that helped to get valid data in person. During observation, the researcher looked at how fingerprint is taken, how much time it took to take this fingerprint, how many days it took to give the result, what requirements are required to get PCC, and to examine in what way the process will be fast enough with the help of technological tools specifically using face biometric identification technique in offering PCC

B. Document Analysis

Document analysis is a method of interpreting documents to extract valuable information that is used in the implementation of the thesis. The researcher analyzed the current working documents: clearance certificate letter and a kind letter to extract requirements of the proposed system. From these documents, personal information of the person who is going to be certified is extracted. Most importantly, the clearance certificate document is used to get more information.

As can be shown in Figure 3.1, the form requires personal information (full name, date of birth, place of birth, nationality, sex), reason for request, clearance requested by (the undertaking organization, reference number to check which organization gives the letter and to whom it is given, date (which date the undertaking organization gives the kind letter), the message that indicates the individual is free from any of criminal activity in the past, signature of the

directorate director of the FPCIB, and photo of the individual are mentioned as required to get PCC.

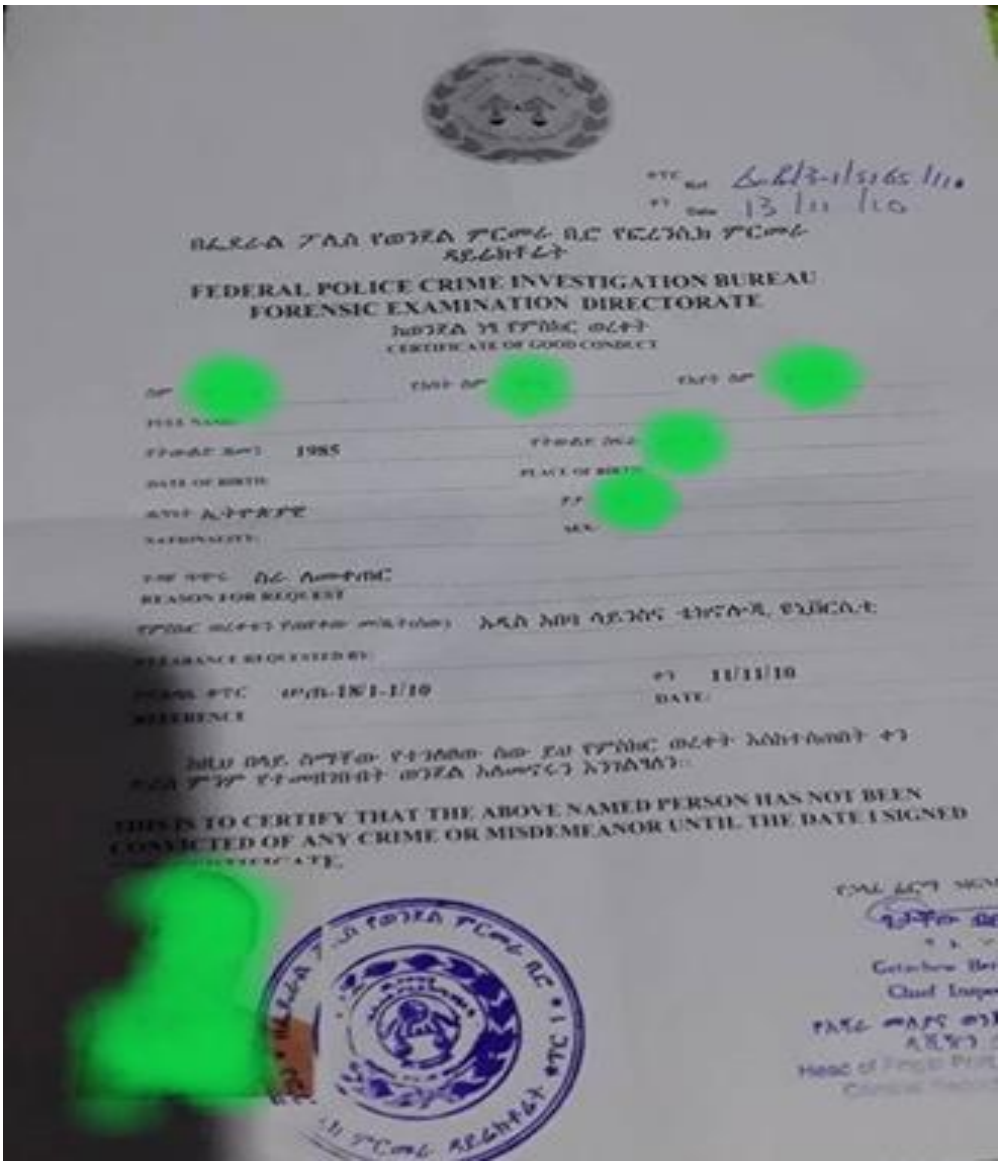


Figure 3.1: Currently Used clearance certificate form

C. Literature survey

Moreover, in the literature survey the researcher analyzed the different biometrics techniques and has selected face biometric technique for criminal identification and investigation in the form of forensic application. This face biometric has better comparison result comparing to other modes of biometrics techniques as stated in the literature part of this study.

Furthermore, the researcher examined literatures how to extract Haar-like features by using cascade classifier where the classifier is consisting of face and non-face images which is already trained algorithm. This helps to detect faces from a given image/video frame through the camera and the way of mapping eyes, noses, mouth, ears, and etc. to Haar-like feature. Besides this, the researcher used cascade classifier in the implementation of the prototype as a face detection approach. Similarly, in the recognition process PCA is selected in EigenFaces face recognition algorithm for diminishing the dimension. Moreover, the researcher used SVM for classification of the results from PCA functions. In doing so, PKL file system is used to save the state and the location of the classification of features (the model in general).

However, in either in face detection during the new person registration or recognition steps of the application greyscale imaging style is applied. This greyscale imaging is a combination of black and white color where black represents 0 and white represents 1. These results from black and white colors are stored in the form of binary representation as a combination of 0's and 1's. Once more, the researcher extracted important procedures how cascade classifier works in classifying features from cascade classifier documentation. This greyscale imaging technique helps to convert the captured image into two-dimensional matrixes by excluding the color channel argument of the cascade classifier algorithm in the OpenCV library.

3.1.3. Tools and techniques

In implementing the prototype of face recognition in PCC offering system as a biometrics technique, the researcher used Python programming language with Django framework to make the application flexible, attractive, and easy to use the prototype with GUI.

For modelling face biometric PCC offering application the researcher used Unified Modeling Language (UML). Besides, the researcher modeled the behavioral and structural modeling of face biometrics PCC offering application. For modeling the behavioral model of the system use case, activity and sequence diagrams are used. Similarly, class diagram is also used for modeling the structural model of the system.

Detection of face is handled by using webcam which is the default integrated camera with the development machine. After face detected, the face is stored in the dataset prepared for this purpose. The information of the individuals is stored in the database. In doing so, SQLite 3 database management system is used to store information other than features. Because, this database management software is the default software in the Django framework to work with Python programming language. To make the prototype easy to use and to use it in all device sizes, the researcher designed the GUI by using responsive design framework called bootstrap.

Testing is mandatory to testify whether the study achieves its objective and answers its question or otherwise. The researcher tested the study after changing the model into prototype. In doing so, the testing process involved: first by inserting sample data, twenty sample personal information along with forty sample faces for each record are collected and registered in the system; then the machine has trained the sample faces, this done through clicking a button. This leads the machine ready for recognition and the recognition followed. During recognition, two category samples are taken. The first category samples are supposed as a trained data, and the second category samples were unknown sample in which the machine does not know. During this step, the number of faces accurately recognized and failed data are recorded to conclude that the model is accurate and is going to improve the current working framework or otherwise.

While making the recognition and if the test data passed the testing as true, a report containing PCC certificate is mandatory task of the model, and for this purpose the certificate conclusion statement is taken from the PCC offering bureau as use in the real business.

3.2. The Process and Approaches of Face Biometric in Criminal Identification System

3.2.1. The process of criminal identification and offering PCC

The researcher observed how fingerprints and criminals' information are collected during observation and document analysis. Most importantly, fingerprints and criminals' information are collected during:

- If they are suspected as criminal and before they have been sent to prison.
- If they are applied to get PCC.
- If they have been get decision from the court to go to prison.

In doing so, during collecting criminals' information their passport or residence id is used as a source of information.

To make it clear, the process of identifying criminals in offering PCC involves collecting a kind letter from individuals, taking sample fingerprints from individuals, collecting criminal records, and searching and checking each and everyone in the list of criminals' record from the collected data prepared in the form of paper list whether the PCC applying individual has been partaken in any criminal activity or not. Upon this procedure, if the individual is partaken in any kind of criminal activity, this individual "has been convicted of by this…, and this crime of misdemeanor until the date of issued certificate" otherwise he "has not been convicted of any crime of misdemeanor until the date of issued certificate". After the requesting individual is checked from criminals' record list, the FPCIB forensic examination Directorate put his official stump on the PCC and given to individuals. Figure 3.11 shows the model of face biometric criminal identification and PCC offering procedure.

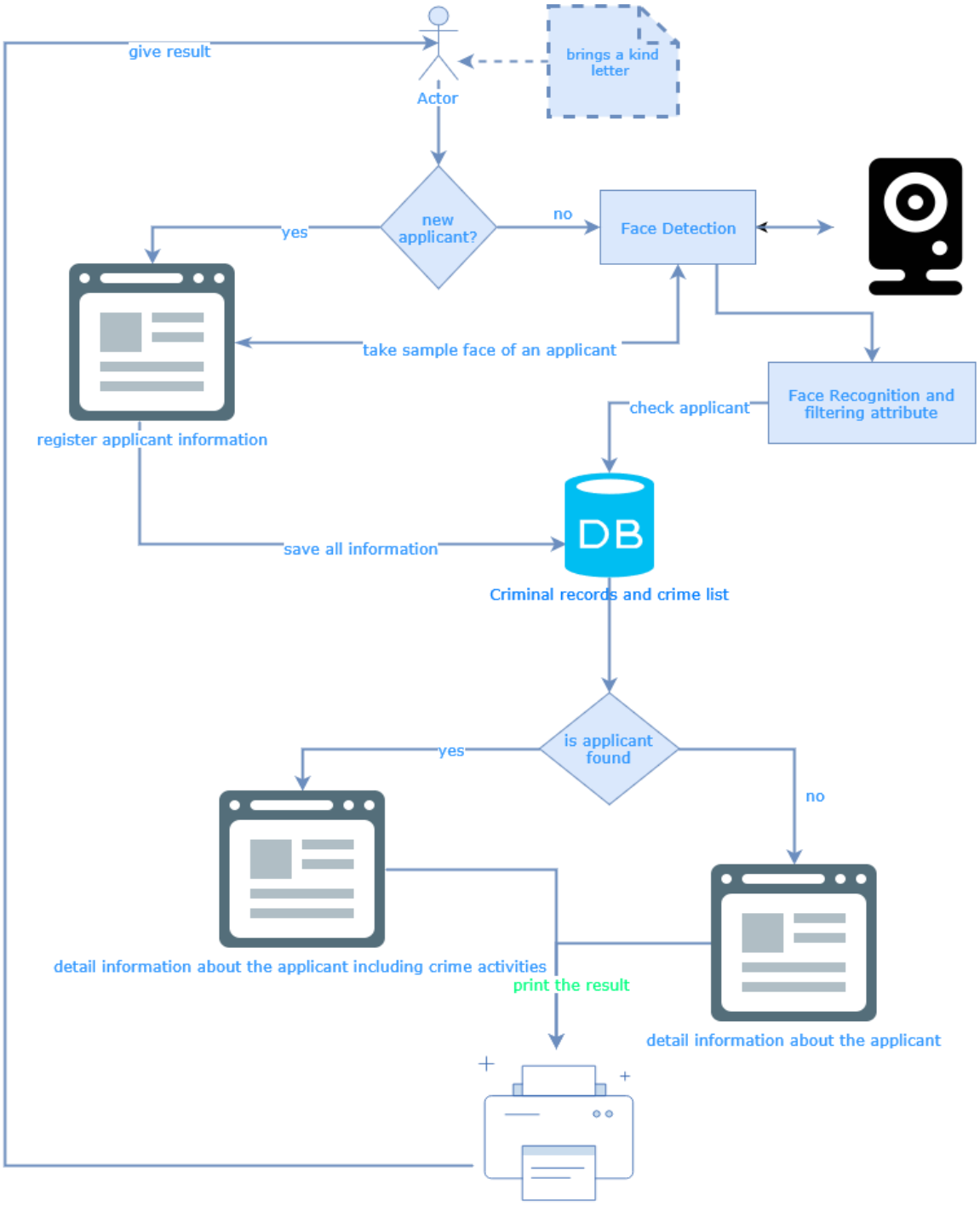


Figure 3.2: Process of PC certification model using Face biometrics technique

3.3. Algorithms Analysis and the Process of Face Recognition

The process of recognizing face among the collection of faces involves face detection, feature classification, training the model, and then recognition by comparing features from a detected face with features stored in the dataset before.

3.3.1. Haar cascade classifiers

Face detection in simple term is the process of verifying a face from an image. However, the process is not simple as we do in natural recognition, and divided into several small tasks: pre-processing, classification and training.

During pre-processing of a face image, the cascade classifier is applied (an algorithm designed for this purpose). Then, before face detection performed, selecting the source of the face is computed. This study used webcam for live face detection. After the source is selected, preparation and normalization follows. During preparation and normalizations of faces different unimportant part of the image has to be diminished from the image: image filtering, noise removal, and scaling. Thanks to OpenCv, all these tasks are evaluated and computed using cascade classifier.

3.3.2. OpenCV for image processing

OpenCv is defined in the official website of the OpenCv library as:

> OpenCV is an open source computer vision library that provide a common platform for computer vision applications and to accelerate the use of machine learning.

The researcher used OpenCV that allows us to do on image processing. In image processing OpenCV provides image computational functions. In the case of face detection and face recognition, OpenCV provides a function to provide the source of the given image, the properties of the image, the representation of the image, and functions of arithmetic calculations of the image. This function is called cascade classifier which is designed to work on Haar-like features.

In this thesis, OpenCV works like this: first, by detecting the image source from a camera (webcam) and returns the image in terms of rows, columns and color channels where rows represent the width of the captured image, columns represent the height of the image, and channels represent the color scheme in the form of RGB (red, green and blue). After loading the image, OpenCV provides us the function to convert this RGB color to grey scale color as discussed before.

Second, the OpenCV allows us to select region of interest. This allows us to collect face and non-face images or to locate a face from the given image. OpenCV has the capability to calculate region of interest by taking the row and column of the given image. This combination of rows and columns results a matrix. This matrix is the representation of an image in the OpenCV platform in the form of 2D dimensional matrix. If the color scheme is included in the representation of the image and if it is required, 3D matrix is used. However, EigenFaces face recognition algorithm requires greyscale image so that the researcher used 2D data matrix. Finally, numpy allows us to compute further computations on the given image by taking its 2D dimensional array to diminish its dimension by using PCA.

3.3.3. Principal Component Analysis and Eigenfaces

In face recognition scheme faces are stored in face database. However, storing faces requires more storage size and needs more computing time either during detection of face/s from image and recognizing the face by comparing it with each and every one of a face in the face dataset. To overcome these challenges, PCA is the first most important in dimensional reduction of faces by extracting the most important information from the given faces as discussed in chapter two: the literature part of this study.

PCA is a method of extracting most important features (information) in the form of components or principal components from the large dataset. This PCA works using principal components by computing the spread of the data of the face as image matrix and it is computed using the following steps.

Step one: converting the given data (image in this thesis) into 2D data matrix.

$$d = \begin{bmatrix} x1 & x2 & \dots & xn \\ y1 & y2 & \dots & yn \end{bmatrix} \quad (3.1)$$

Step two: computing the mean m of the given matrix d

$$\text{mx} = \sum_{\text{i}=0}^{\text{n}} \text{di}$$

$$\text{my} = \sum_{\text{i}=0}^{\text{n}} \text{di} \quad (3.2)$$

step three: computing the difference D by subtracting the mean m from each and every data point in the matrix d by creating another data matrix D

$$D = \begin{bmatrix} x1 - mx & x2 - mx & \dots & xn - mx \\ y1 - my & y2 - my & \dots & yn - my \end{bmatrix} \quad (3.3)$$

Note that: if the given matrix is n then the difference also be n matrix. This newly computed matrix D is smaller than the given matrix d meaning we are applying diminishing dimension by using PCA. Therefore, we need to capture the information containing in the data using smaller dimensions than the given dimension of the image.

Step four: computing the covariance of the matrix C which indicates the direction of the spread of the data in the matrix d on the X, Y, and Z axis

$$\text{C} = \text{MM}^{\text{T}} \quad (3.4)$$

where, T represents the transpose operation, M represents the dimension of the matrix MxM

step five: computing the Eigen vectors (principal components) of a matrix C where each Eigen vector is equivalent to the biggest Eigen value in each iteration of the principal component. These principal components in the PCA algorithm are passed in the form of PCA function argument called number of components (**n_components**).

During the implementation of PCA faces should be in greyscale color. However, faces acquired from camera are colored images. With the help of OpenCV the detected face is converted into

grayscale image on the fly. Once the image is converted to greyscale, diminishing of the dimension follows.

Diminishing the dimension is the process of adjusting the smallest principal components to zero point by reserving maximum data variance during projection of the data. As can be seen in Figure 3.3, here, the researcher has taken a row image taken from phone camera that has 4128 by 3096 original dimension in the form of 2D.

Figure 3.3: Sample image for computing PCA

After computing data distribution using PCA of Figure 3.3, Figure 3.4 clearly shows that there is a closely linear relationship between the x and y variables. As the data distribution increases in the x axis, it also increases in the y.

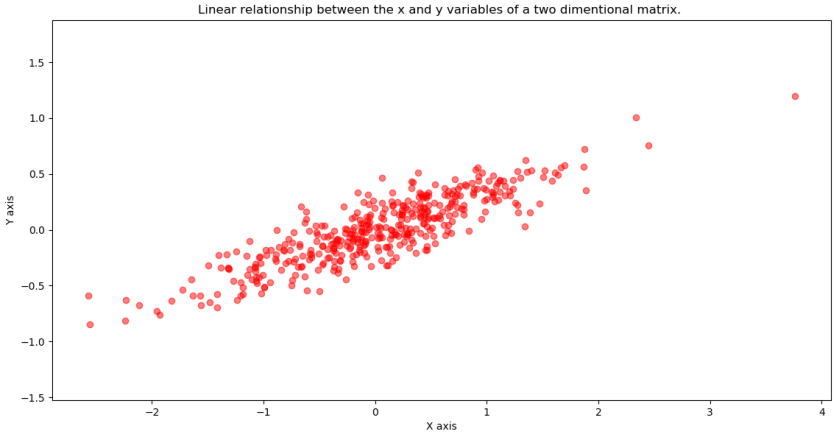


Figure 3.4: Computing linear data distribution in x and y axis of a row image taken from Figure 3.3

By finding the list of principal axes in the data, we can quantify this linear relation and describe the dataset by using those axes. The researcher has used sklearn python library to compute dataset by using two line of codes as follows:

```
pca = PCA(n_components=2)

pca.fit(X)
```

where, X is the dimension of the data: X=4128x3096

Here, the fit function learns some quantities from the data, most importantly the "**components**" and "explained variance". As can be seen in Figure 3.5, principal components are just number, however, they do have significant role in determining the linear relationship between the princi pal axis.

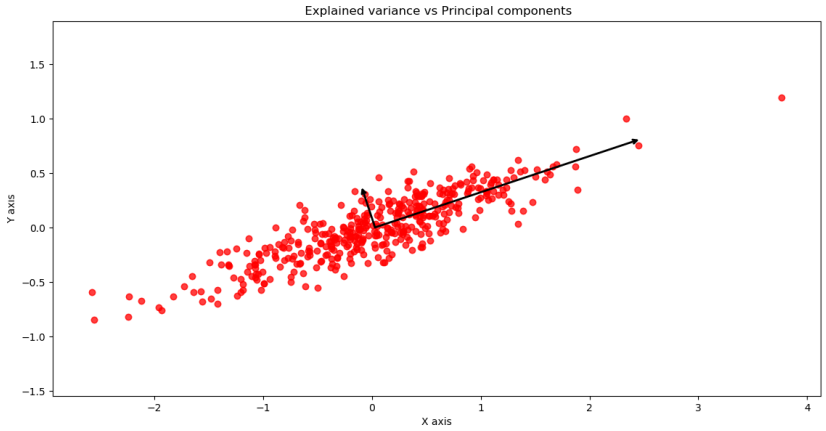


Figure 3.5: Explained variance vs Principal components

The prediction of each data point onto the principal axes are the principal components of the data, these vectors denote the principal axes of the data, and the distance of the vector is a suggestion of how important that axis is in telling the dissemination of the data.

The afterward is diminishing the dimension using PCA. As can be seen in Figure 3.6, the original data are represented using red points while the projected data are represented using the

green points. This helps us to conclude that diminishing the dimension is important by taking (a) the information along the less important principal axis or axes is diminished and (b) preserving only the data component(s) with the biggest variance. The portion of variance that is diminished (proportional to the spread of points about the line formed in the figure) is approximately a measure of how much information is rejected in this diminishing the dimension.

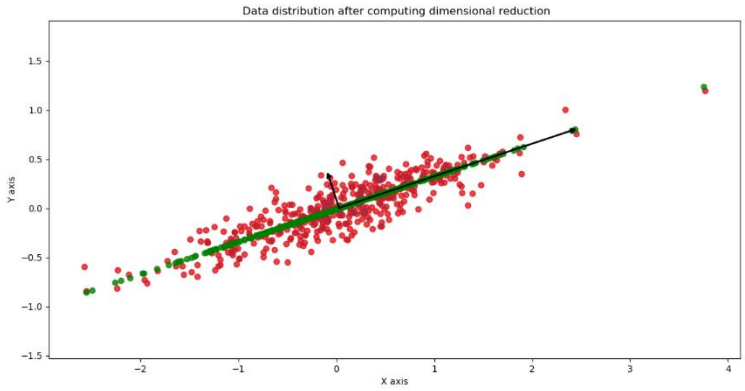


Figure 3.6: Diminishing of the dimension using PCA and comparing the green vs red color marks

Most importantly, this diminished dataset is good enough to encode the relationships between the points: despite diminishing the dimension of the data almost by 50% and approximately 150 components are good enough to denote the whole information, besides, the overall relationship between the data points are mostly preserved as can be seen in the graph depicted in Figure 3.7.

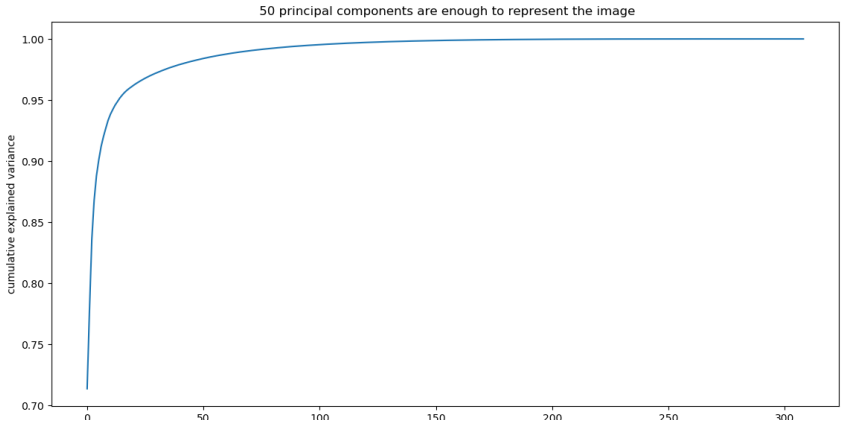


Figure 3.7: 150 principal components to represent 4128X3096

3.3.4. EigenFaces to recognize face

EigenFaces are images that can be added to a mean (average) face to create new facial images with the help of PCA but they are nothing if PCA is not applied in the reconstruction of the newly faces whose dimension is diminished.

In the previous section we have seen how to apply PCA to diminish dimension of an image in the form of 2D dimensional matrix. Now we have turned into how to apply this PCA onto each sample image per person to figure out the most important EigenFaces from the face dataset.

Therefore, the researcher first stored a number of faces in one folder and applied PCA algorithm on the faces. PCA results eigenvectors and eigenvalues. Finally, PCA computed the mean, covariance, and the scalar vector on each image and computes an average face. Figure 3.8 shows that the first twelves sample average faces are generated from a dataset after the machine is trained in decreasing order regarding to their level of importance and the most important EigenFace comes first.

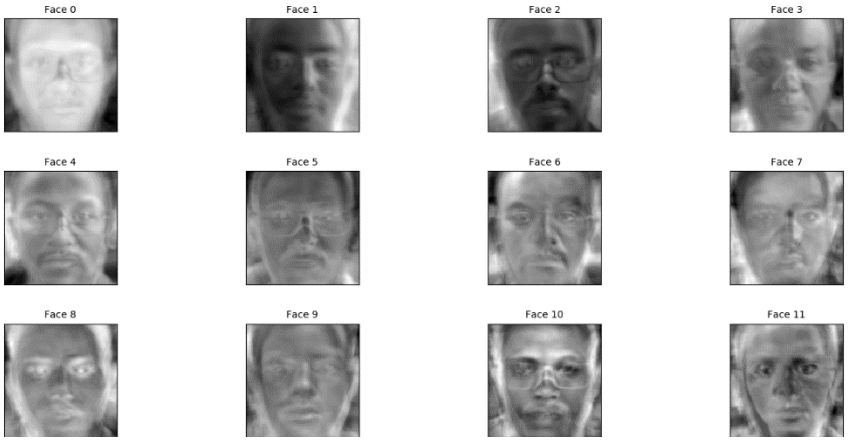


Figure 3.8: The first twelves sample average Eigenfaces generated from a data set

3.3.5. Support Vector Machine

Support vector machine is a supervised machine learning technique used to classify the data distribution. The researcher used this SMV to classify face features and to design recognition model. The SMV uses the top N EigenFaces obtained by PCA. SMV is used because tries to find a boundary that divides the data in such a way that the misclassification error can be minimized and it chooses the decision boundary that take full advantage of increasing the distance from the nearest data points of all the classes. SVM does not just find a decision boundary, it also finds the most optimal decision boundary. So that, it has the power of increasing accumulative prediction accuracy. This SVM takes dataset from PCA for classification and trained of the top EigenFaces.

3.4. Dataset preparation, Training and Classification

3.4.1. Dataset preparation

Dataset, in technical term of this study, is just a folder that used to store face data of each person in the form of image. However, saving images needs more storage space. The researcher created a folder called “Dataset” and used this folder to store all faces coming from a webcam. Before the face is stored the researcher have used dataset preparation whereby the coming face is resized, cropped, and labeled using person’s passport number and/or residence number. The researcher used 40 sample faces per person and labeled as a number from 1 to 40, and concatenating these number with the passport number and/or residence number. This naming of faces helps to identify to whom this face is belongs to in the real database system and helps to fetch more information about the recognized individual from the database since the researcher used this passport number and/or residence number as unique during database design.

3.4.2. Training and Classification of the Model

Once the dataset is prepared, training the model for recognition follows. In doing so, the researcher used PCA to compute Eigenvalues (principal components) and Eigen vectors (explained variance: maximum variance) to generate new faces called EigenFaces among faces

stored under the dataset. This PCA is just unsupervised machine learning used to extract best features of a given face. These features are extracted with the help of linear correlational matrix technique.

After features are extracted and the top EigenFaces are generated (like as can be seen in Figure 3.8 above) a model is created to save the features using PKL[1] file system. This PKL file used to save the status/state and the location of the model during recognition and by default it knows which face is belonging to which ID. In each time the model is trained from the dataset, PCA opens the PKL file and rewrite the data on it, and this is done just by clicking a button.

In conclusion, the model training works like this: first, by fetching training and testing dataset along with their image resolution (height, width) from the dataset, and splitting training and testing dataset. Second, computing the eigenvalues and eigenvectors by transforming each face into a new dimension, and projecting input data on the EigenFaces in orthogonal and normalized (orthonormal in mathematical term) basis. Finally, train a SVM classification model by fitting the classifier to the training set. This model is saved in the form of PKL. Figure 3.9 shows the overall process of generating the model after applying all these techniques.

Figure 3.9: Face recognition model design and training

[1] PKL is file extension: A Python module that allows objects to be serialized to files on disk and deserialized back into the program at runtime;

CHAPTER 4

REQUIREMENT ANALYSIS AND MODELLING

4.1. Requirements Analysis

Requirement analysis is the process of researching, interpreting and analyzing requirements of a system collected from the key stakeholders and documents. Besides, the researcher discovered requirements that are required in the PCC offering system from current working forms and documents. In doing so, the researcher collected and analyzed different functional requirements required to develop the prototype of the study.

4.1.1. Functional Requirements

Functional requirements are the reasons for a project to be developed and deploy on which what the prototype of face biometric PCC can do, what data it shall store and how quickly or how easily it shall perform. Besides, a project must have SMART requirements. This system programmed to receive personal information along with sample face images. More or less these system requirements are grouped into user requirements, system requirements, and business requirements as can be seen in Table 4.2.

Table 4.1: Requirements priority level

Value	Rating	Description
1	Critical	This requirement is critical to the success of the project. The project will not be possible without this requirement.
2	High	This requirement is high priority, but the project can be implemented at a bare minimum without this requirement.
3	Medium	This requirement is somewhat important, as it provides some value but the project can proceed without it.
4	Low	This is a low priority requirement, or a “nice to have” feature, if time and cost allow it.

5	Future	This requirement is out of scope for this project, and has been included here for a possible future release.

Table 4.2: Functional, system and business requirements

Req#	Priority	Description	Rationale	Impacted Stakeholders
User requirements				
FR-U-001	1	A user should first login	Users need to insert their credentials based on the provided GUI	Users
FR-U-002	1	List of buttons must displayed in the home page after the user logged in.	Users select a button action from the list of actions on the displaying screen.	Users
FR-U-003	1	The user should click the button named train the machine	Users read and click the provided button	
FR-U-004	1	The requested action should be executed	The user waits till the process is completed and the page refreshed	
FR-U-005	1	The user should click the button face recognition	A customer must stand on take his/her face to the camera.	Customers

FR-U-006	1	The user have to press g key on the key board if the customer's face is detected	A user can follow the page redirection	Users and Customers
FR-U-007	1	If the customer is new customer, a user should click the button customer registration	A user can ask the customer is s/he is new or not	Users and Customers
FR-U-008	1	The user should fill all the required fields	The customer should bring all required documents	Customers
FR-U-009	1	After filling all the fields, a user should take sample face images	The customer should stand in front of the camera	Customer
System requirements				
FR-S-001	2	If the user is not logged in, the system should redirect the user into login page	The system shall display the login form.	Users
FR-S-002	1	The home page must displayed after the user logged in and	E.g. Welcome	Users

		provide logged in information		
FR-S-003	2	The system must enabled the camera	If the user is click buttons	Users and Customers
FR-S-004	3	The system shall be design based on acceptable GUI standards so that users can easily communicate to the system and navigate from one state of the application to another state with no or fewer (if any) difficulties.		
Business requirements (in applying PCC everyone should fulfill the following business requirements by hand)				
FR-B-001	1	A PCC applying individual has to bring a kind letter from the undertaking bureau if s/he wants the certificate for employment otherwise visa related documents		
FR-B-002	1	The PCC applying individual has to apply in person with identification card (passport or residence id)		
FR-B-003	1	The PCC applying individual has to be willing to give his/her face		
FR-B-004	2	The PCC applying individual has to wait at list for twenty-four (24) hours for result		
FR-B-005	3	The PCC applying individual has to take the result in person		

4.2. Modeling of Face Biometric PCC Offering Application Prototype

System modeling is the process of developing abstract models of a system or representing a system using some kind of graphical notation, and this graphical notation is designed using

Unified Model Language (UML). This helps the researchers, analysts, and other stakeholders to understand the functionality of this system.

The researcher modelled this prototype in such a way that the process and the communication of its customers and its external environments present in an abstract representation. This model is used to show the contextual view of the system, interactions between the system and its customers, and the structural design of the system and dynamic behavior of a system as it is executing whereby the application and the database are communicated each other in each request-response pattern.

The researcher included three major groups of models to view the system with no detail information about the system. The first models are grouped under interaction model which show the dynamic behavior of the objects in a system where a series of changes to the system are described. The second models are under behavioral diagrams which track how the system will act in a real-world environment, and observing the effects of an operation or event, including its results like if the button is clicked and its corresponding action. The last model is structural model of the system to show the static behaviors whereby data tables are derived from class diagrams to store customers' information in the physical database.

Most of the time there is no clear cut difference between behavioral diagrams and interaction diagrams whereby interactions diagrams are derived from the more general behavior diagram most importantly from use cases. However, modeling both behavioral and interaction models is vital in designing any system in software engineering perhaps in engineering fields as a whole.

4.2.1. Use Case (Use Diagram) Model

Use case diagram is used to show the communication between an actor and the system itself, a communication where each actor interacts in the system and what actions can the actor does during in each interaction loop to the system. Each use case represents an isolated task that involves external interaction with a system, and has an actor (people or another which has direct interaction to the system) who is going to perform this isolated task. Besides, in face biometrics

PCC offering application (here after named as system to save space and make clear and understandable for the readers of this thesis) majorly there are three types of actors:

1. Police officer/front officer who uses the system daily to offer PCC to customers and communicates with them directly.
2. Crime investigation officer who uses the system to manage crime and criminal records
3. DBA (database administrator) who manages the overall transactions of the system including managing user activities.

As can be seen in Figure 4.2, the use case diagram represented diagrammatically to provide an overview of the use case, a more detailed textual form is presented in the consecutive tables under section 4.2.2.

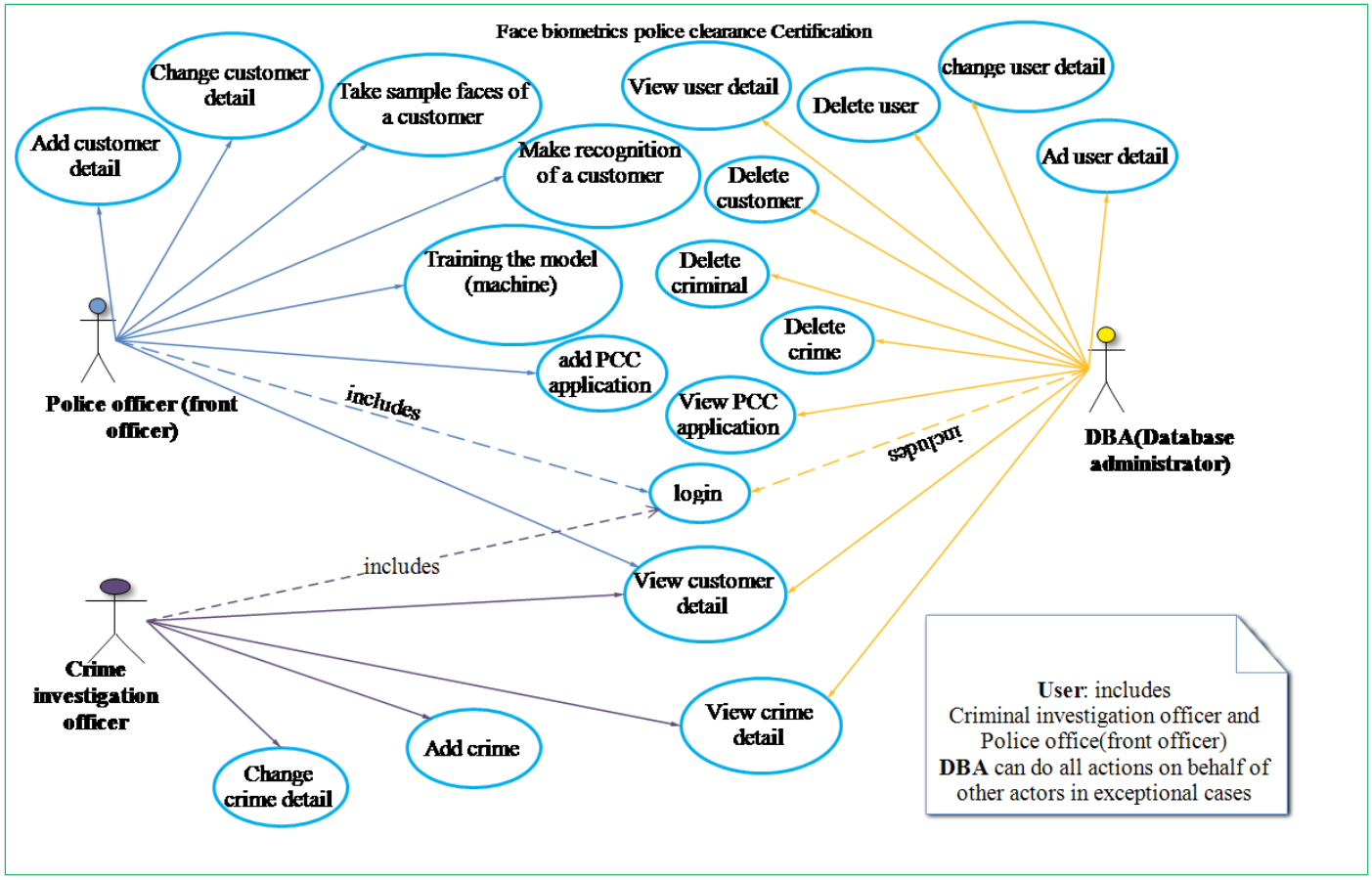


Figure 4.1: Use case diagram of face biometrics PCC offering application

4.2.2. Tabular description (Scenarios) of the use cases

Before preceding to each of the table listed under this section, there are some concepts we first have to understand. All of the tables may not have the same element, however, they shared the same elements too. Besides, we have to make sure that they are requirements. These concepts are the following:

- Use case ID, name where each is used to uniquely identified in this document from other use cases, and name is used to call the use case.

- Actor (s): shows who is going to granted the corresponding action in each of the specified use case.
- Goal: shows for what purpose the use case is required and designed, or what is the final output of the use case specified in each of the table.
- Precondition(s): shows what requirements are required before the basic flow of action the specified use case performed. However, some of the use cases may not have preconditions. These helps to facilitate the flow of the communication between the actor and the system.
- Basic flow: is the reason why the specified use case is required in the system. A use case may have more than one flow. Basic flows show the steps that the specified actor should follow in communicating with the system. If the actor miss one of the steps, the system does not allow the action to be performed.
- Post condition(s): these are the expected results in which the system displays as a success message in each of interaction loop. These may be http response or prepared populated message that shows the system accomplishes the action in the correct way.
- Alternative flow: is exceptional case in which the basic flow is failed or if the system has alternatives other than the basic flow of action. Of course most of the use cases do not have alternative flow of actions.
- Data dictionary: is just requirements or inputs for the specified use case. Data dictionary is just attributes of the table and the form inputs. These requirements are presented along with their data type, input type, and conditions whether they are mandatory or not.

Table 4.3: Use case description for add customer detail

Actor ID, name	**UC001, Add customer detail**				
Actor(s)	Police officer (front officer)				
Goal	The goal of this use case is to register customer details into the system				
Precondition(s)	The actor must have logged into the system				
Basic flow	1. The police officer must click on customer registration button 2. The system must display registration form				
Post condition(s)	1. The system should display confirmation message to the police officer				
Alternative flow	For this use case no alternative flow of action				
Exception(s)	No exception for this use case				
Data dictionary	Name	Field size	Format	Condition	field type
	Name	100	String	Required	Text input
	Surname	100	String	Optional	Text input
	Father name	100	String	Required	Text input
	Date of birth	12	String	Required	Date input
	Place of birth	1000	String	Required	Text input
	Nationality	100	String	Required	Text input

	Sex	6	String	Required	Combo box
	Passport number or residence id	100	String	Required	Text input

According to the table, the specified actor has to provide values accordingly as specified in the data dictionary of Table4.3. Fields in the form should be filled accordingly as specified in the data dictionary part of the table. In doing so, a user has to login to the system first to accomplish this task. Besides, the system is designed in such a way that the user is checked before opening the form using session, and the user has to follow steps according to the use case. Form fields are designed well as specified in the data dictionary in terms of text input or combo box. This use case will be used if there will be a modification in the design, maintenance, data structure, or requirements change.

Table 4.4: Use case description for change customer detail

Actor ID, name	**UC002, Change customer detail**				
Actor(s)	Police officer (front officer)				
Goal	The goal of this use case is to change a customer details				
Precondition(s)	1. The actor must have logged into the system				
	2. The customer detail must be displayed				
Basic flow	1. The police officer must click on customer's name button				
	2. The system must display editing form				
Post condition(s)	The system should display confirmation message to the police officer				
Alternative flow	The police officer can cancel the change operation				
Exception(s)	No exception for this use case				
Data dictionary	Name	Field size	Format	Condition	field type
	Name	100	String	Required	Text input
	Surname	100	String	Optional	Text input
	Father name	100	String	Required	Text input
	Date of birth	12	String	Required	Date input
	Place of birth	1000	String	Required	Text input
	Nationality	100	String	Required	Text input
	Sex	6	String	Required	Combo box
	Passport number or residence id	100	String	Required	Text input

This use case (**UC002**) is depend on the use case **UC001**. An actor who is going to made change to this use case must first choose an applicant and navigate through this use case. The form will be displayed by populating prefilled data from the database, then an actor can make changes as much he wants to change. In doing so, an actor must follow the steps (alternative flows and.or basic flows as well as must login to the system using his user name and password.

Table 4.5: Use case description for take sample faces of a customer

Actor ID, name	**UC003, Take sample faces of a customer**
Actor(s)	Police officer (front officer)
Goal	The goal of this use case is to sample faces from each customer camera for the model
Precondition(s)	1. The actor must have logged into the system 2. The customer detail must be registered before
Basic flow	1. The police officer must click on take sample faces button 2. The system must enable the face detection module 3. The camera must be enabled by the face detection module 4. The customer must arrange him/herself to the camera 5. The system should display a confirmation message to the police officer
Post condition(s)	The system should display confirmation message to the police officer as the number of samples are taken
Alternative flow	No alternative flow for this flow
Exception(s)	No exception for this use case
Data dictionary	No data dictionary for this use case

This use case helps to collect sample faces of an applicant. In doing so, an applicant's information should be first registered in to the system. This use case has no its own data dictionary to store information into the database. However, it takes faces of an applicant in the form of image and store in the predesigned dataset by indexing each and every sample face using applicant's passport number or residence id. Like other use cases, this use case needs an applicants' login.

Table 4.6: Use case for training the model(machine)

Actor ID, name	**UC004, Training the model(machine)**
Actor(s)	Police officer (front officer)
Goal	The goal of this use case is to train the model for the later face recognition process
Precondition(s)	The actor must have logged into the system
Basic flow	1. The police officer must click on machine learning button 2. The system should process training of the machine 3. The system should write the trained model to a file system
Post condition(s)	The system should refresh the page
Alternative flow	No alternative flow for this use case
Exception(s)	No exception for this use case
Data dictionary	No specified data attribute for this use case but it is a file system called PKL

As can be seen in Table 4.6, this use case is designed to train the model after collecting sample faces of applicants'. In doing so, the user must login to the system and navigate to this use case so that the machine can train the collected faces and generate a model in the form of PKL file format which is going to be used during recognition phase of the prototype. This use case doesn't have data dictionary because there is no a need of information to store in to the database.

Table 4.7: Use case description for add PCC application

Actor ID, name	**UC005, Add PCC application**				
Actor(s)	Police officer (front officer)				
Goal	The goal of this use case is to add PCC application into the system				
Precondition(s)	The actor must have logged into the system				
Basic flow	3. The police officer must click on New Application button 4. The system must display application form				
Post condition(s)	2. The system should display confirmation message to the police officer				
Alternative flow	For this use case no alternative flow of action				
Exception(s)	No exception for this use case				
Data dictionary	Name	Field size	Format	Condition	field type
	Name	100	String	Required	Text input
	Reason for request	-	String	Required	Text input
	Clearance requested by	-	String	Required	Text input
	Reference number	100	String	Required	Text input
	Date of reference	12	String	Optional	Date input
	Passport number or residence id	100	String	Required	Combo box

Whenever an applicant applies for PCC, this form is opened. During the execution of this use case, applicant's information is required as specified in the form of data dictionary. A user who is going to perform this use case has to follow steps specified in the use case. This use case requires applicant's passport number or residence id from use case **UC001**. In doing so, a user has to select an applicant from the combo box and fill other data requirements. However, it needs user login and the user must provide his user name and password to perform this use case.

Table 4.8: Use case for make recognition of a customer

Actor ID, name	**UC006, Make recognition of a customer**
Actor(s)	Police officer (front officer)
Goal	The goal of this use case is to identify customers and offer the PCC
Precondition(s)	1. The actor must have logged into the system 2. The customer detail must be registered before
Basic flow	1. The police officer must click on face recognition button 2. The system must enable the face detection module 3. The camera must be enabled by the face detection module 4. The customer must arrange him/herself to the camera 5. The system should identify by comparing the detected face with the trained model and enable the recognition module designed for recognition purpose
Post condition(s)	1. The system should navigate the police officer to the detail page of the customer 2. The police officer should press CTRL + p to print the PCC
Alternative flow	No alternative flow for this flow
Exception(s)	No exception for this use case
Data dictionary	No specified data dictionary for this use case but the data used during the execution of this use case is face in the form of image

This use case is the final use case to provide PCC to applicants. An applicant must provide his face to the camera and keep on until the recognition completes. Once the face is taken the algorithm navigates the user to report page whereby applicant's information is displayed and crime identification is made. Finally, the user prints the report and gives it to an applicant by making it sealed.

Table 4.9: Use case description for view customer detail

Actor ID, name	**UC007, View customer detail**
Actor(s)	Police officer (front officer), Crime investigation officer and DBA
Goal	The goal of this use case is to view a customer details
Precondition(s)	The actor must have logged into the system
Basic flow	1. Actors must click on customer link 2. The system should display customers list in the form of table 3. Actors should click on the name of the customer they want to look
Post condition(s)	No post condition for this use case
Alternative flow	1. Actors can type the customer's passport number or residence id, name, sure name or father name 2. Actors should click on go button
Exception(s)	No exception for this use case
Data dictionary	No specified input

This use case helps to view applicants' information either individually or whole applicants in terms of table. If the user wants to look at a single applicant's information, he has to click on applicant's name or passport number where the link is provided to the detail page. This use case uses data requirements provided in **UC001** and retrieves those data from this us case as well. However, it needs user's login. So a user must login to do this.

Table 4.10: Use case description add crime detail

Actor ID, name	**UC08, Add crime detail**				
Actor(s)	Crime investigation officer				
Goal	The goal of this use case is to register crime details to the system				
Precondition(s)	The actor must have logged into the system				
Basic flow	1. The actor must click on add button 2. The system should display the form 3. The actor should click on save button after filling the form				
Post condition(s)	The system should display confirmation message to the actor				
Alternative flow	No alternative flow for this use case				
Exception(s)	No exception for this use case				
Data dictionary	Field name	Field size	Format	Condition	field type
	Criminal name	100	String	Required	Text input
	Crime title	1000	String	Optional	Text input
	Crime description	-	String	Required	Text input
	Date of crime happened	12	String	Required	Date time input

Crimes registered in the system along with a criminal detail who did it. In doing so, this use case is designed to do this. This use case has its own data dictionary which are required to record the crime details. Crime details are associated with applicants in many to many relationships. This use case is permitted only for crime investigation officers, and they have to login to the system to perform this use case by using their user name and password. This user group is identified using access levels by the database administrator. All input fields should be filled according to the data dictionary specified in the Table 4.10 above.

Table 4.11: Use case for change crime detail

Actor ID, name	**UC009, Change crime detail**				
Actor(s)	Crime investigation officer				
Goal	The goal of this use case is to view crime details to the system				
Precondition(s)	The actor must have logged into the system				
Basic flow	1. The actor must click on change button 2. The system should display the list of crimes 3. The actor should click on the crime title s/he wants to change 4. The system should display editing form 5. The actor should click on the save button after making changes				
Post condition(s)	The system should display confirmation message to the actor				
Alternative flow	1. actor can type the crime title 2. The actor should click on go button 3. The actor should click on the save button after making changes				
Exception(s)	No exception for this use case				
Data dictionary	Field name	Field size	Format	Condition	field type
	Criminal name	100	String	Required	Text input
	Crime title	1000	String	Optional	Text input
	Crime description	-	String	Required	Text input
	Date of crime happened	12	String	Required	Date time input

This use case is used to make changes to crime detail, and the form is populated from use case UC008. In doing so, a user must login to the system and follow the specified flow of actions and fill data inputs accordingly. A user can make changes as much as he wants based on the rules and regulations guided him to do this.

Table 4.12: Use case description for view crime detail

Actor ID, name	**UC010, View crime detail**
Actor(s)	Crime investigation officer and DBA
Goal	The goal of this use case is to view a crime details
Precondition(s)	Actors must have logged into the system
Basic flow	1. Actors must click on crime link 2. The system should display crimes list in the form of table 3. Actors should click on the title of the crime they want to look
Post condition(s)	No post condition for this use case
Alternative flow	1. Actors can type the crime title 2. Actors should click on go button
Exception(s)	No exception for this use case
Data dictionary	No specified input

Crime investigation officer can view crimes as he can add them into the system. This use case retrieves all crimes' information from crime table and an actor can have a look at individual crime as well. This use case doesn't have its own data dictionary since it used to retrieve information and no need of inputting or modifying data attributes of the table. Like other use cases, this use case needs an actor to login to the system and an actor should provide his user name and password to access this use case unless he is prohibited from accessing it. To view individual crime detail, an actor should click on the crime title that navigates him to the detail page of the crime.

Table 4.13: Use case ad user detail

Actor ID, name	**UC011, Ad user detail**				
Actor(s)	DBA (Database administrator)				
Goal	The goal of this use case is to add users' details to the system				
Precondition(s)	The actor must have logged into the system				
Basic flow	1. The actor must click on add button 2. The system should display the registration form 3. The actor should click on the save button after making changes				
Post condition(s)	4. The system should display confirmation message to the actor				
Alternative flow	No alternative flow for this use case				
Exception(s)	No exception for this use case				
Data dictionary	Field name	Field size	Format	Condition	field type
	user name	100	String	Required	Text input
	password	20	String	required	Text input
	First name	100	String	Required	Text input
	Last name	100	String	Required	Date time input
	Email address	100	String	Optional	Text input
	Permission	-	Boolean	required	Check box

This use case used to register actors' information so that they can access the system based on their access level given by the database administrator. During their registration user name and password are generated to them so that they can login to the system and do activities. Their activeness is checked by using sessions and if the session is empty it navigates them to the login page.

Table 4.14: Use case description for change user detail

Actor ID, name	**UC012, Change user detail**				
Actor(s)	DBA (Database administrator)				
Goal	The goal of this use case is to add users' details to the system				
Precondition(s)	The actor must have logged into the system				
Basic flow	1. The system should display the list of users 2. The actor should click on the user's user name s/he wants to change 3. The system should display editing form 4. The actor should click on the save button after making changes				
Post condition(s)	The system should display confirmation message to the actor				
Alternative flow	1. Actor can type the user name of a user s/he wants to change 2. The actor should click on go button 3. The actor should click on the save button after making changes				
Exception(s)	No exception for this use case				
Data dictionary	Field name	Field size	Format	Condition	field type
	user name	100	String	Required	Text input
	First name	100	String	Required	Text input
	Last name	100	String	Required	Date time input
	Email address	100	String	Optional	Text input
	Permission	-	List	required	Check box

Database administrator has full access to view all actors detail since hi adds them into the system. Every time he logs into the system, he can view users and their activities regarding to their level of access.

Table 4.15: Use case description for delete user

Actor ID, name	**UC013, Delete user**
Actor(s)	DBA (Database administrator)
Goal	The goal of this use case is to delete a user from the system
Precondition(s)	The actor must have logged into the system
Basic flow	1. The system should display the list of users 2. The actor should click on the check box displayed from user's user name s/he wants to delete 3. The actor should select delete from action list 4. The actor should click on go button 5. The system should provide warning information including summary of a user with cancel and sure buttons 6. The actor should make sure as s/he wants to delete
Post condition(s)	The system should display confirmation message to the actor
Alternative flow	1. Actor can type the user name of a user s/he wants to delete 2. The actor should click on go button 3. The actor should click on go button 4. The system should provide warning information including summary of a user with cancel and sure buttons 5. The actor should make sure as s/he wants to delete
Exception(s)	No exception for this use case
Data dictionary	No new specified data for this use case

Database administrator can delete a user whenever needed and appropriate. Actors may be prohibited from accessing the system, for instance, they may leave their work, they break the contract, or they may be denied due some business requirements, and during that time their account may be deleted.

4.2.3. Modeling the Class Diagram

Structural models show the organization and architecture of a system in terms of the components that make up that system and their relationships to define the static architecture of the system.

UML Class diagrams are used when developing an object-oriented system model to show the classes in a system and the associations between these classes. In this system majorly there are three UML classes to show the architecture of the system and its components as depicted in Figure 4.3 below.

As a result, the researcher mapped these class diagrams into relation database whereby class names mapped into table and class members mapped into table attribute to develop the prototype of the study.

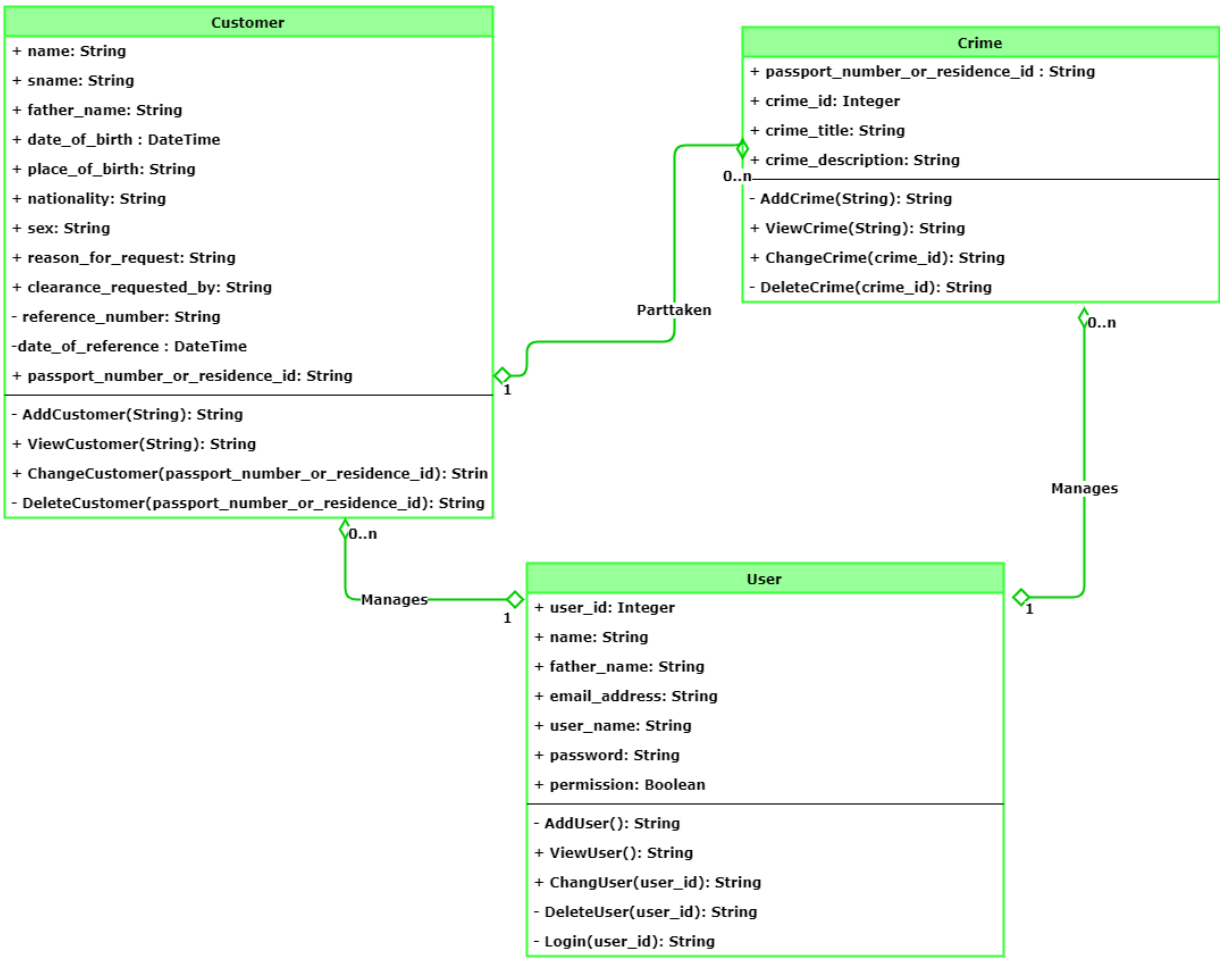


Figure 4.2: Structural view of the system using class diagram

4.2.4. Modeling Activity diagram

Activity diagram is another important behavioral diagram in UML diagram to describe dynamic aspects of the system. Basically, activity diagram is an advanced version of flow chart that modeling the flow from one activity to another activity. The researcher used activity diagrams to illustrate the flow of control in this system and refer to the steps involved in the execution of a list of use case in Figure 4.2. In that way, the researcher modeled sequential and concurrent activities using activity diagrams. Therefore, the researcher basically depicted workflows visually using an activity diagram because an activity diagram focuses on condition of flow and

the sequence in which it happens and the researcher depicted what causes a particular event using an activity diagram as shown in the following consecutive figures.

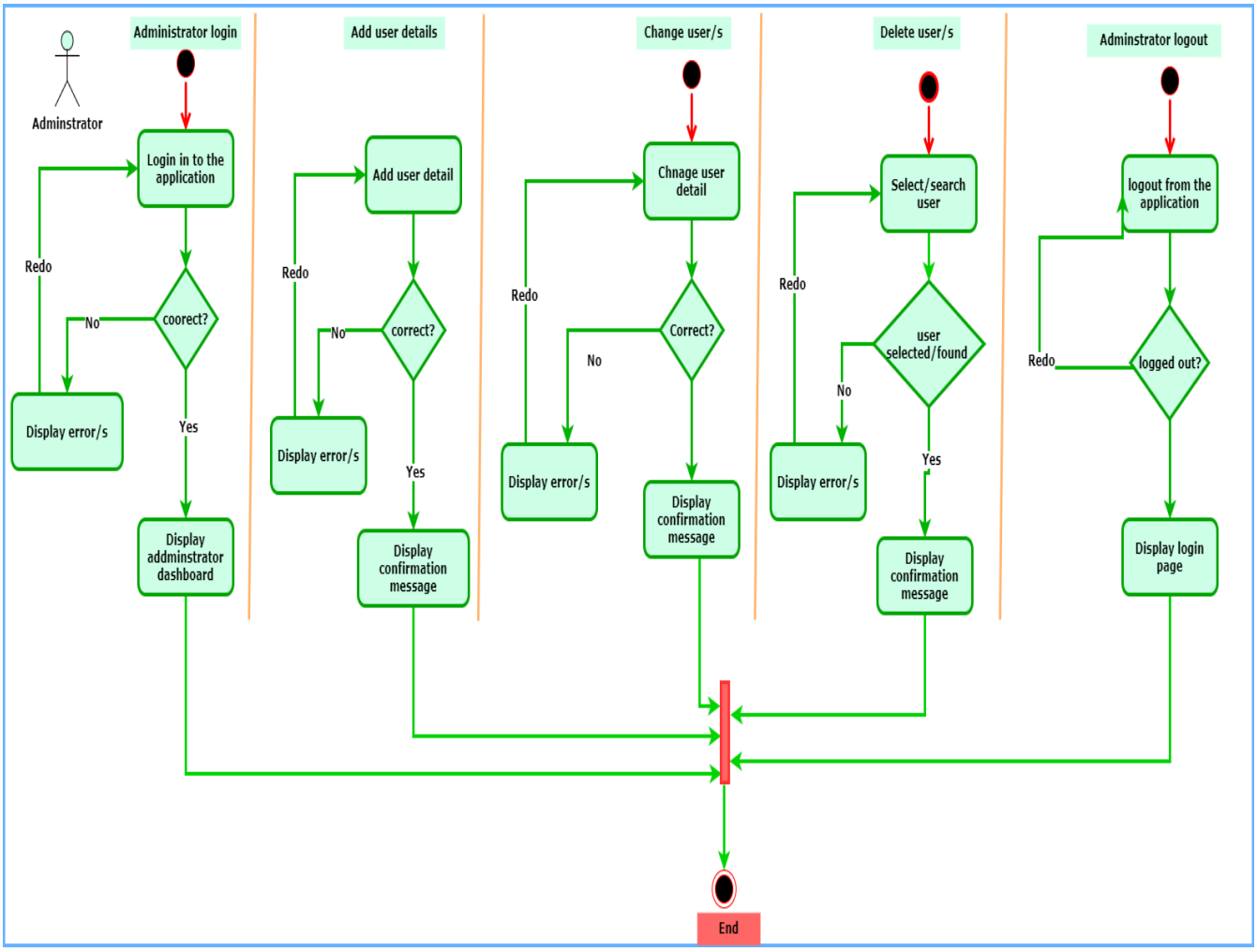


Figure 4.3: Activity diagram for use cases in which the administrator handles users of the system

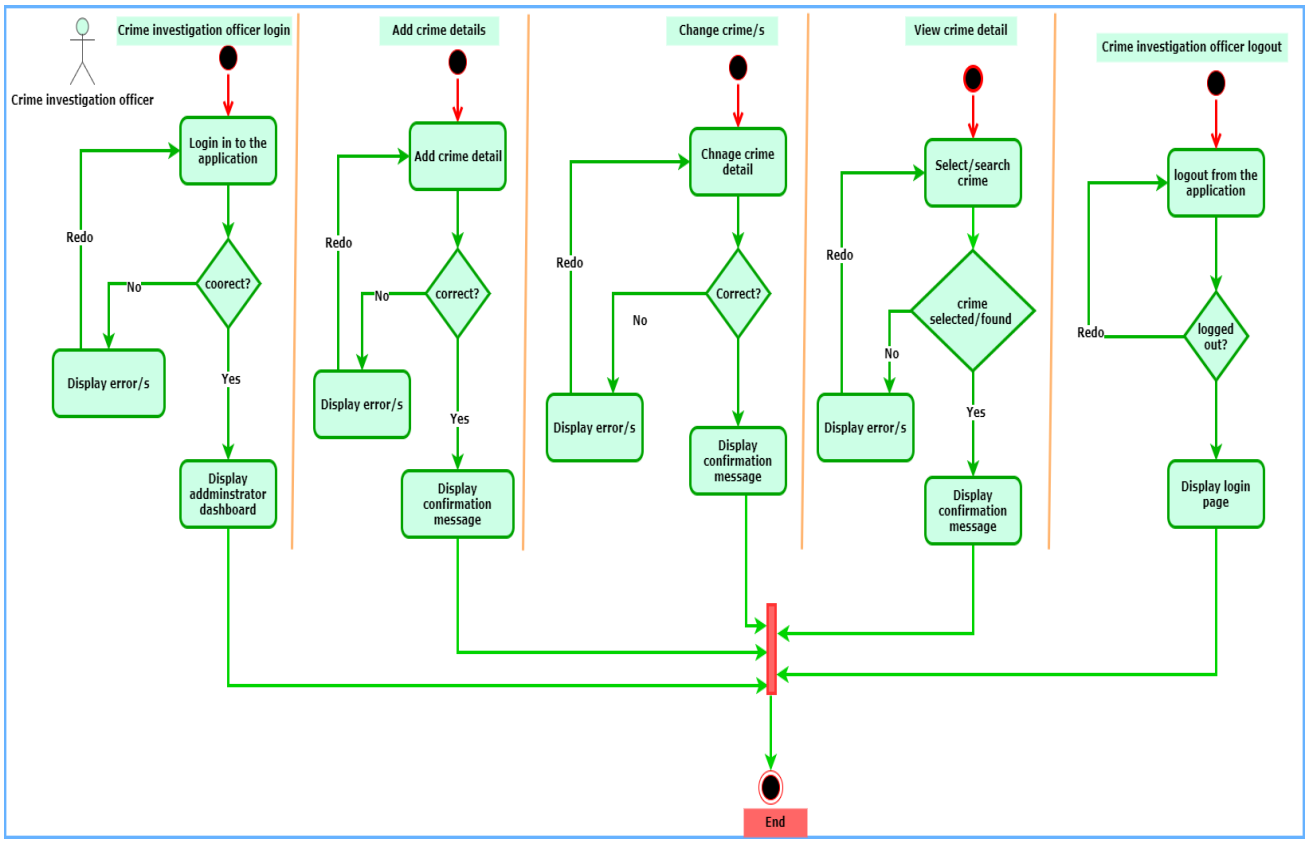


Figure 4.4: Activity diagram for use cases in which the crime investigation officer handles crimes committed by criminals

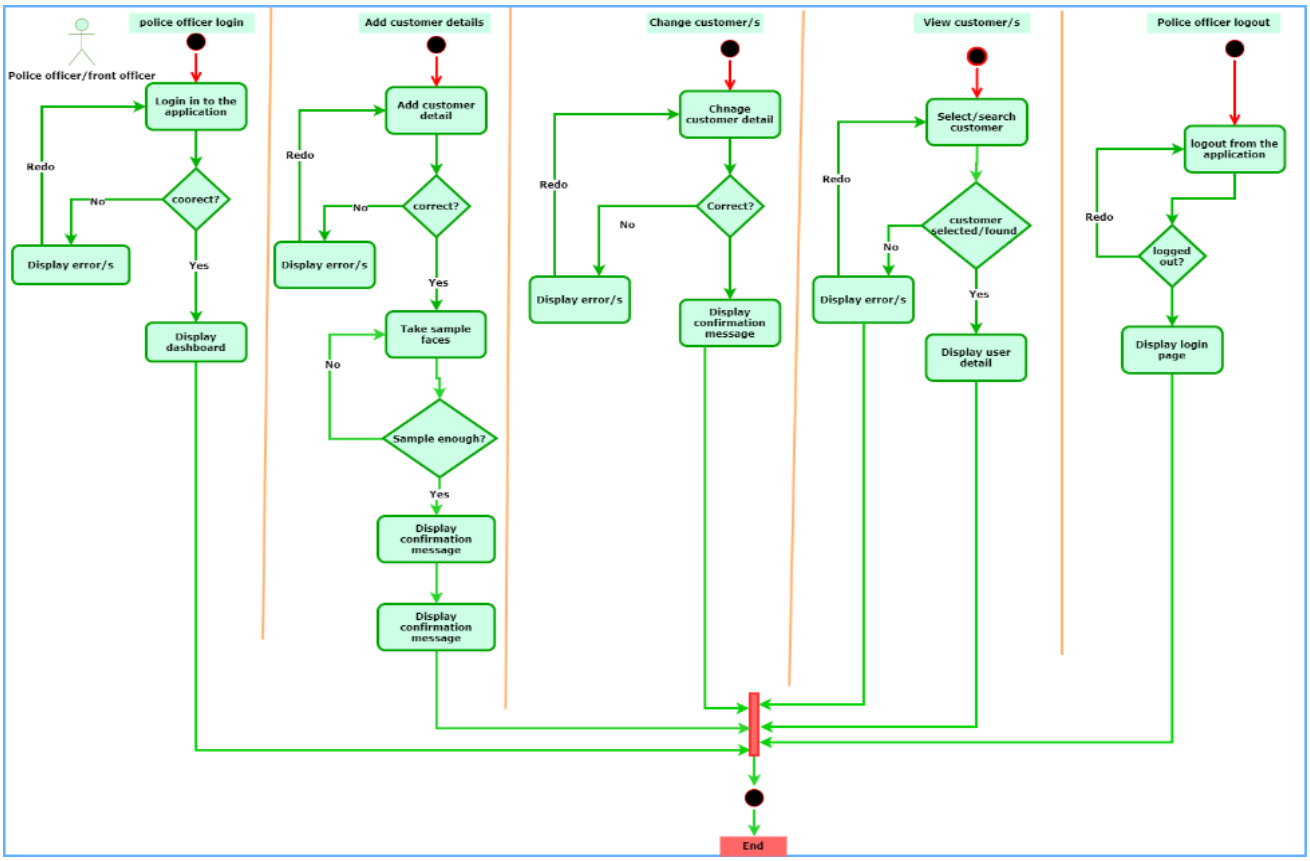


Figure 4.5: Activity diagram for use cases in which the crime investigation officer handles criminal

4.2.5. Modeling sequence diagram

A sequence diagram shows the sequence of interactions that take place during a particular use case or use case instance. As sequence diagrams can be used to capture the interaction between objects in the context of a relationship, one of the primary uses of sequence diagrams is in the transition from requirements expressed as use cases in the above Figure 4.2 to the next and more formal level of refinement. Use cases are often refined into one or more sequence diagrams. To refined the interactions between the actors and objects, we depicted some general sequence diagrams as shown below.

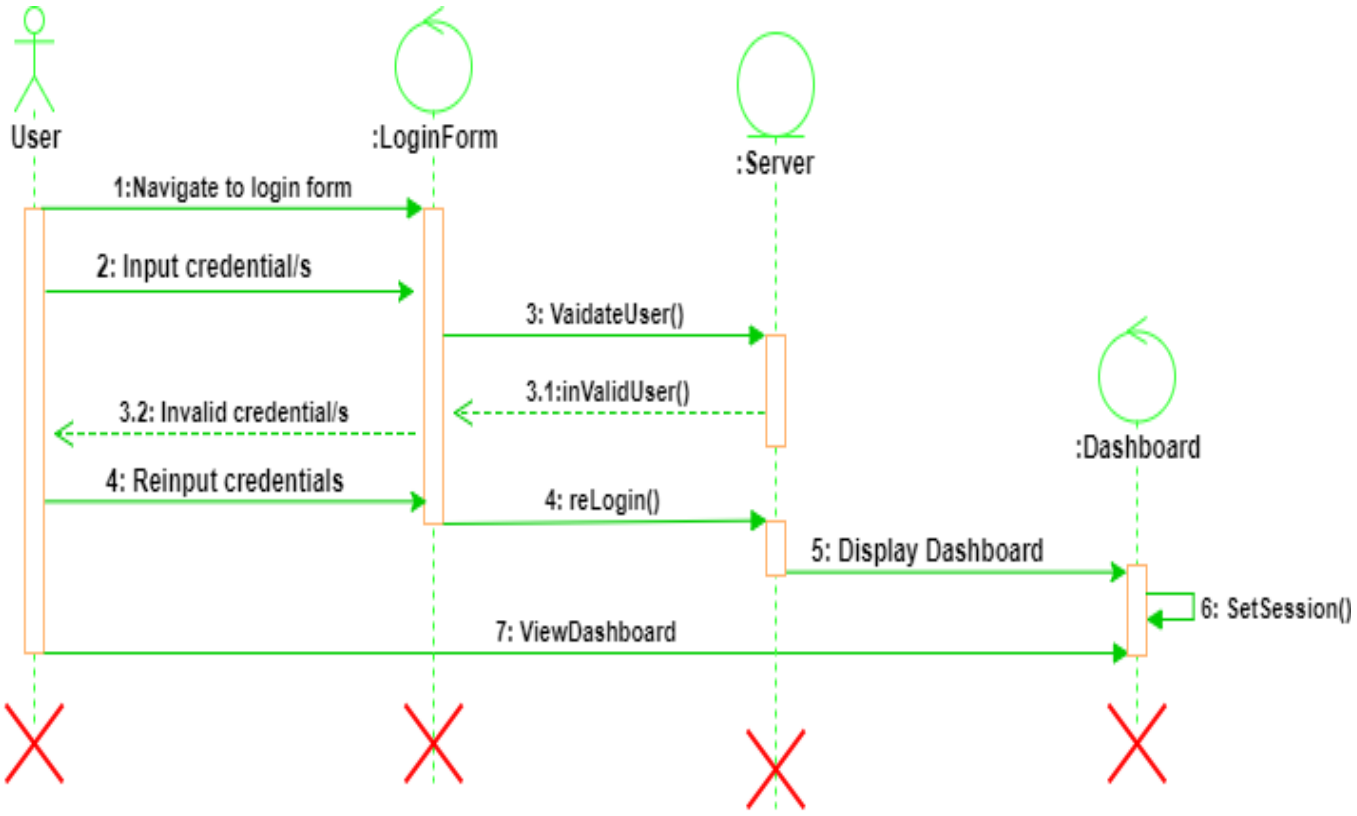


Figure 4.6: User login sequence diagram

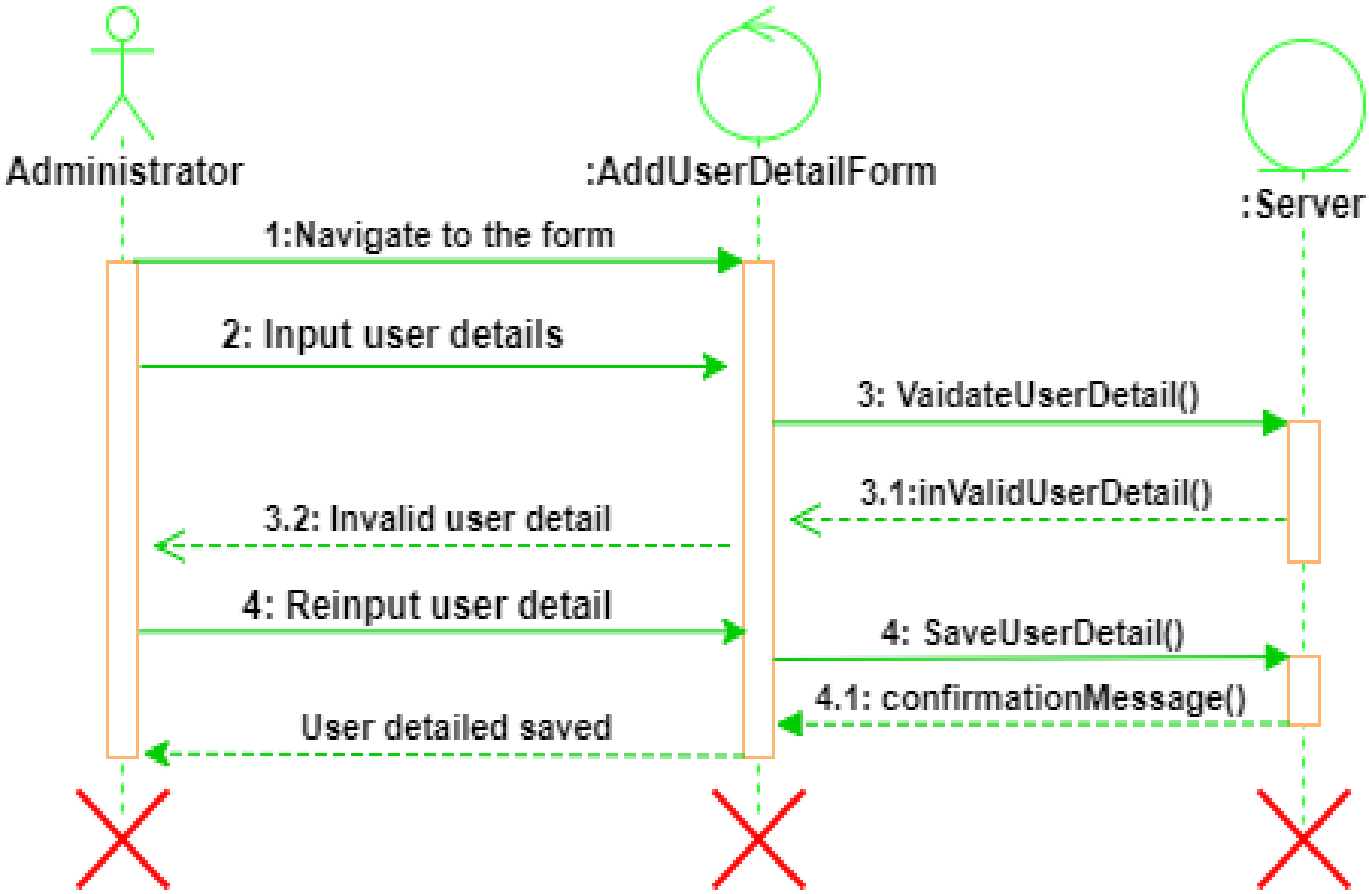


Figure 4.7: Add user detail sequence diagram

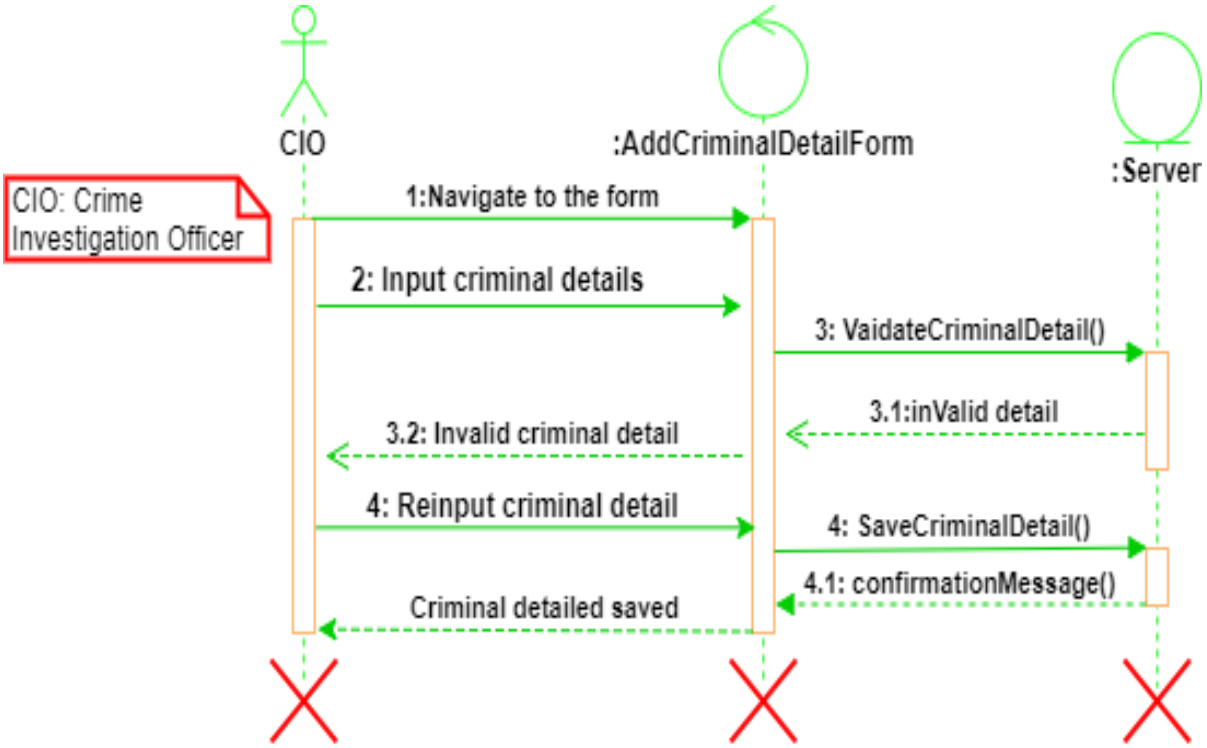


Figure 4.8: Add criminal detail sequence diagram

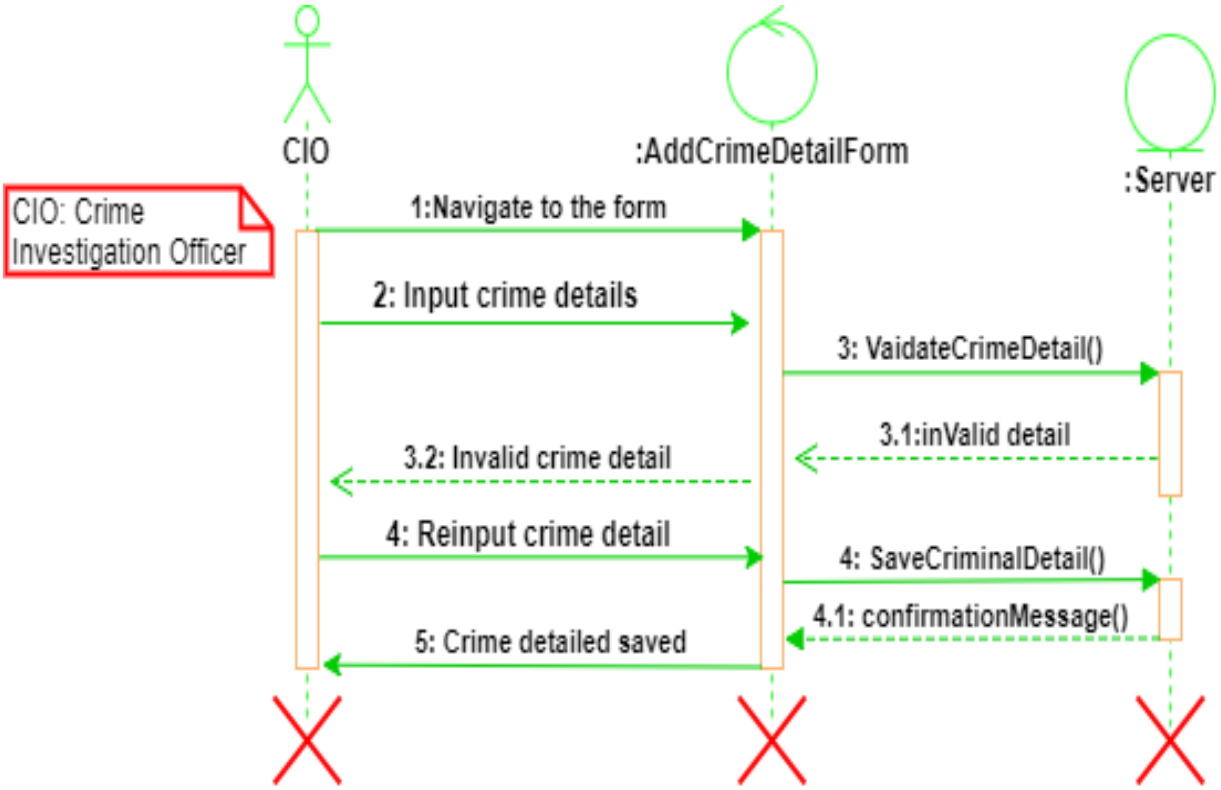


Figure 4.9: Add crime sequence diagram

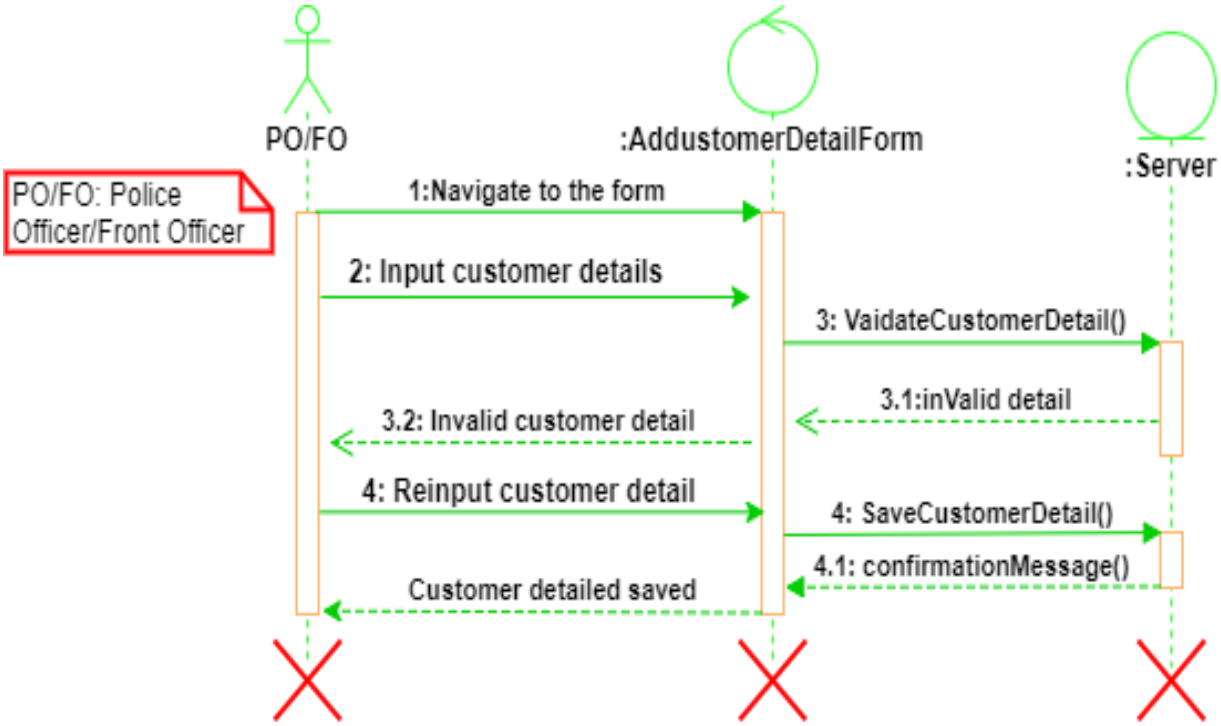


Figure 4.10: Add customer detail sequence diagram

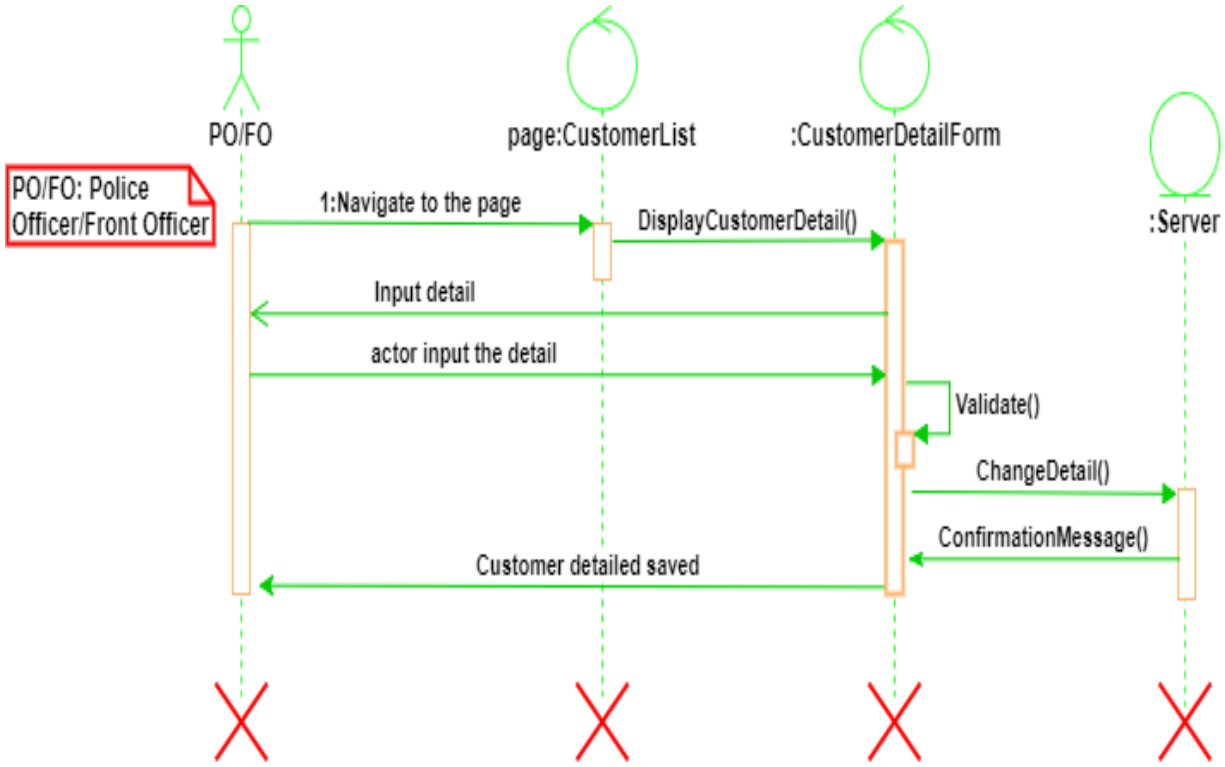


Figure 4.11: Change customer sequence diagram

CHAPTER 5

PROTOTYPE DEVELOPMENT AND EXPERIMENTATION

5.1. Prototype

Prototype is the direct result of the implementation of the model of the system where different model diagrams are converted into computer code. In doing so, use cases are mapped into user actions as buttons and links, data dictionaries are mapped into input fields in the system GUI, class diagrams are mapped into physical database to store dynamic data in the form of data table. However, this prototype is not mean the actual working system of the proposed system rather it is a working version used as testing and simulating the study. Furthermore, the prototype is specifically designed to prove how face biometrics can improve the current working PCC offering system in Ethiopia, and the prototype is implemented in six modules as described in the following sections.

Most importantly, the GUI is designed in such a way that it is simple to use as typing and clicking a button, with standard color scheme by considering color effect, and accessible in all device sizes with the help of bootstrap framework, which have camera interface and internet access.

The system requires different level of user roles, and we have stated three different access level based on the requirements of the system as stated in the requirement section of the study. In doing so, the first access level is offering PCC as per applicant, registering customers' information, identifying criminals using face recognition API, and training the machine for the later recognition. All these are granted for front officer who uses the system daily as per customer request. The second one is registering crime information who is granted for crime investigation officer who records daily if the crime is happened. The last, but not the least, is registering front officers and crime investigation officers, granting access levels for these users, modifying all details if needed, and denying users when terminated. Again, all these access levels are granted for the database administrator (DBA).

5.1.1. Customer registration prototype

Customers' information should be first stored in the system database, and this is the primary duty of front officer. Front officer should collect all necessary customers' information stated as in the requirements section of the study. In doing so, we have designed customer registration prototype. The requirements which are in need for this prototype are converted into form fields. As can be seen in Figure 6.1, all input fields are designed in such a way that they used to accept inputs of different data. Therefore, what can the front officer do is just fill the form inputs accordingly and click the button named "Save and take sample faces".

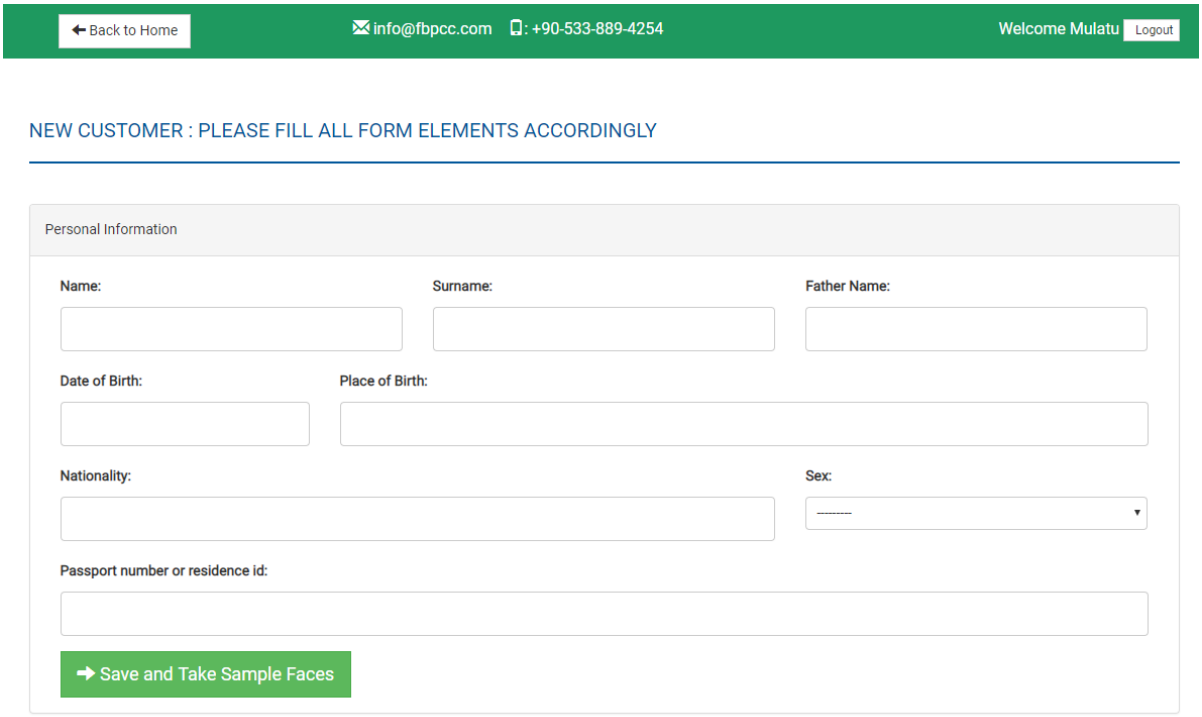


Figure 5.1: Customer registration prototype form

In doing so, these requirements are collected from the applicant passport or residence card, and applicants are required to bring either passport id or residence card in person. Most importantly, this is used for first type applicants in the system per individual.

5.1.2. PCC Application Prototype

Through our observation in the bureau in person, we found that more than five hundred applicants visited the PCC offering bureau per day for applying PCC, so this prototype is the most frequently used prototype and accessed at every applicant request. Every time the police officer uses this form to collect important and mandatory requirements from each applicant. In doing so, the police officer collects those requirements from a kind letter, so that every applicant should bring the kind letter in person. Those requirements include reason for request, requested by (which bureau needs this certificate), reference number in which the kind letter is supposed to explain in case, and the date of the referencing the letter. Referring to Figure 6-2, we can see that all these requirements are organized in such a way that the GUI is designed as simple as locating the cursor and typing. In using this form what a front officer does is just fill all fields accordingly and click the button named “Continue”.

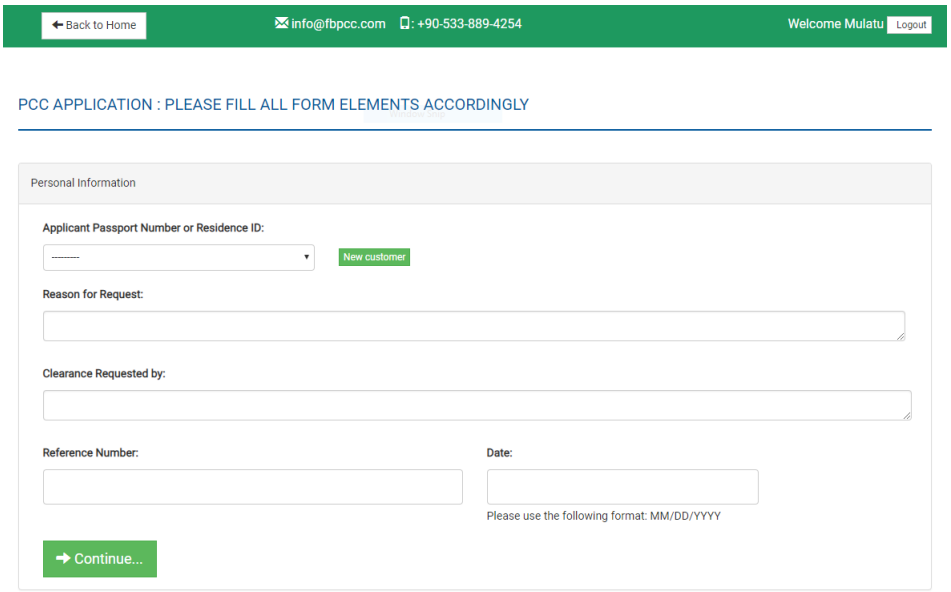


Figure 5.2: PCC application prototype form

5.1.3. Collecting sample faces prototype

While registering customers' information, sample faces should be collected. The application should enable the camera API automatically when the customer registration is completed with success response. In doing so, these faces used while the machine is trained in generating Eigenfaces for the later face recognition. This collecting of sample faces is designed in such a way that first the system detects faces then eyes detection follows, this leads to improve the detection process which helps noise removal. PCC offering bureau will prepare a window equipped with a camera and a chair to allow a single customer to detect. However, customers are required to go into the prepared window, of course, this is mandatory, as can be seen in Figure 6-3, this prototype detects faces and eyes where boxes bordered in green color are eye detection result and the rest is true for face detection.

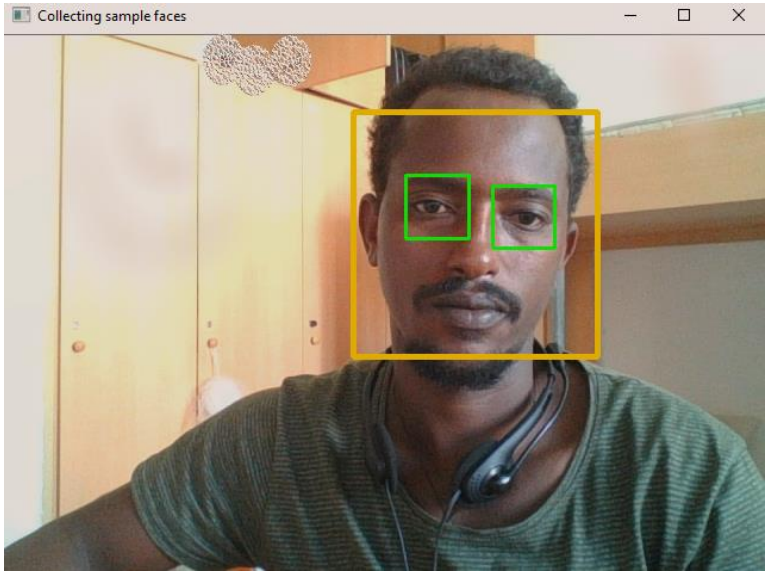


Figure 5.3: Face detection result while taking sample faces after customers' information saved in the database

5.1.4. Crime Registration Prototype

Crime details are registered if a person is partaken in the criminal activity. However, the study did not study how a person is considered as a criminal rather it is designed by taking all other issues at the back and of course the objective is not this. The prototype took as criminals are recorded in this system after a person is taken as a criminal. For more about this prototype, we can see in Figure 5.5.

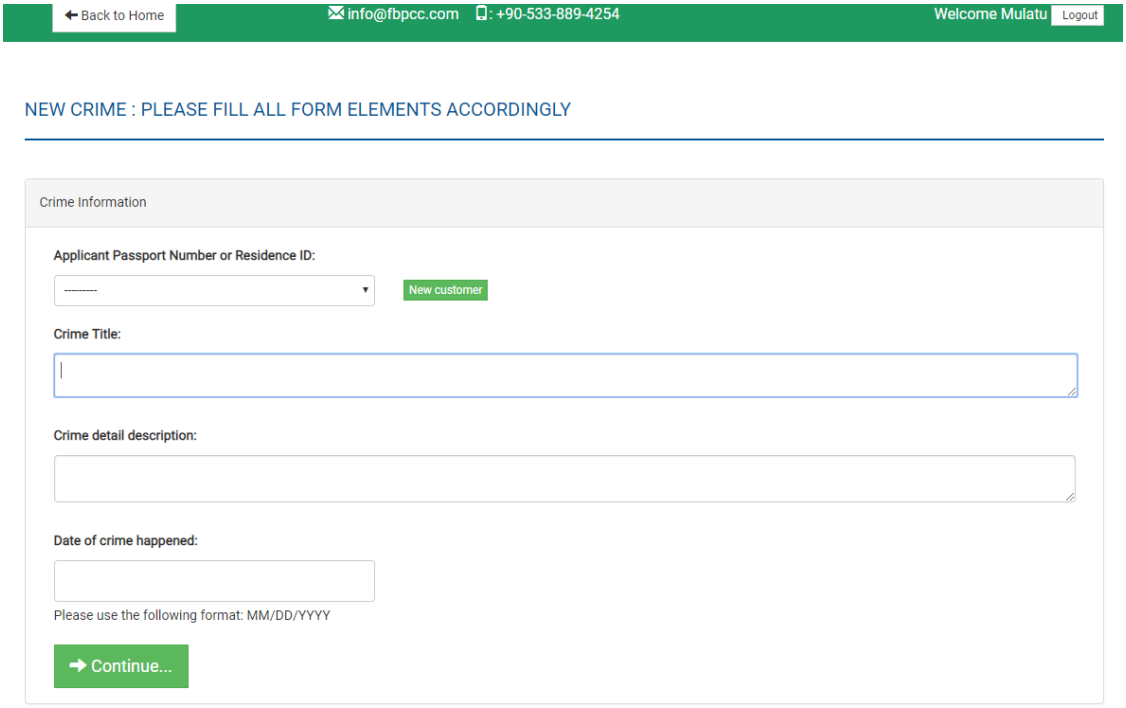


Figure 5.4: Crime registration prototype form

5.1.5. Model Training and Face Recognition Prototype

Model training is just feeding sample faces to the algorithm then a recognition model generated. This model training has no specific GUI and API. However, training the machine works when only if the button named “Model Training” is clicked. After the model has been trained, we can run recognition algorithm. This recognition prototype has no specific GUI like the model training prototype, and works if the button named “Face Recognition” is clicked. As can be seen

in Figure 5.6, both model training and face recognition prototypes are displayed in the same page in the dashboard page of the system.

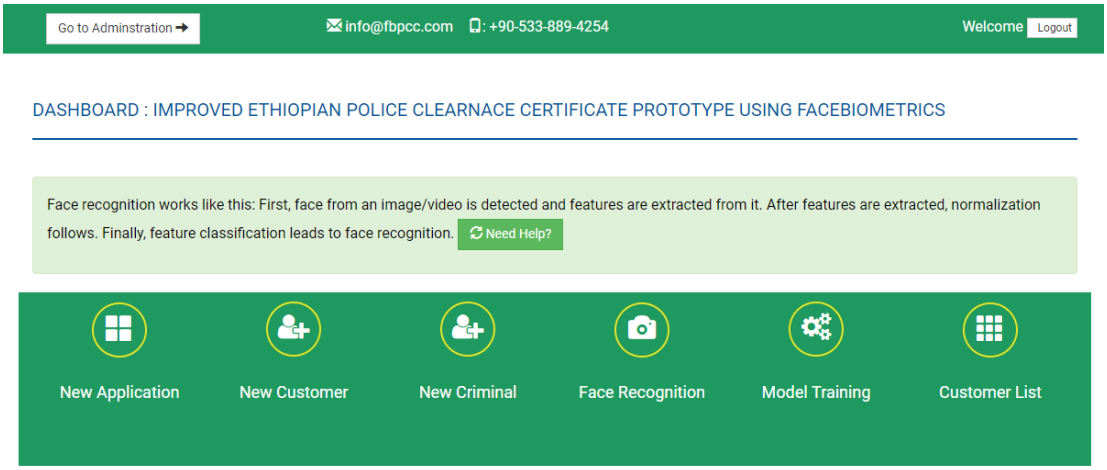


Figure 5.5: Model training prototype in the dashboard of the system

5.2. Prototype Testing

Testing is important and primary to check whether the study achieves its objective/s as proposed or not using its prototype. In previous sections, we have seen some major prototypes especially how customers' information is stored, how sample faces are collected, how each customer is associated with a given crime, and how the customer is recognized using his face in PCC offering application. Now the time is testing these prototypes how it can improve the current working framework of PCC. In doing so, we took twenty people for testing the evaluation, and during testing we recorded all results along with time frame. During testing the prototype, the study runs as expected, however it does not consider twins. Most importantly, the prototype is not designed to do all the process with no human intervention rather it needs majorly front officers and crime investigation officers. The model can generate certificate automatically when the customer is recognized, and crimes recorded by this customer also associated in addition to his personal information.

5.3. Results Analysis and Discussion

Result analysis is the process of interpreting of an experiment, a prototype, an engineering work, study, ... result. Research results may be as expected/proposed or opposite. After the prototype is tested, the results are obtained by running the prototype on the local host, and all results from the prototype are presented.

5.3.1. Result of the Study

The experimental results of the study is generated by running developed prototype and the study has generated four major results. The first result shows how customer information retrieved from the database and how it can display. Figure 6.1 shows that the first four sample applicants' information is retrieved from the database.

Action: --------- Go 0 of 14 selected

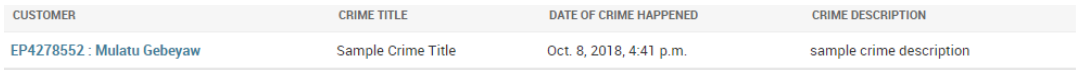
NAME	SURNAME	FATHER NAME	DATE OF BIRTH	PLACE OF BIRTH	NATIONALITY	SEX	PASSPORT NUMBER OR RESIDENCE ID
Amogne	Yibeltal	Workie	March 27, 1989, midnight	Mertulemariam	Ethiopian	Male	EP3245785
Yikeber	Hunachew	Simachew	Jan. 24, 1982, midnight	Bihr Dar	Ethiopian	Male	EP4225299
Seblewongel	Alemayehu	Tezera	Aug. 8, 1992, midnight	Gondar	Ethiopian	Male	EP4225254
Tirunesh	Tessema	Molla	July 16, 1994, midnight	Welega	Ethiopian	Female	EP4225249
Temesgen	Manderso	Mokriaw	Dec. 21, 1990, midnight	Yelemelem	Ethiopian	Male	EP4458576
Yitbarek	Mekonnen	Adnualem	Aug. 13, 1990, midnight	Azena	Ethiopian	Male	EP4774868
Getinet	Mekonnen	Amare	Oct. 17, 1993, midnight	Tilili	Ethiopian	Male	EP4724474
Samuel	Abebe	Tadesse	Oct. 26, 1994, midnight	Arsi	Ethiopian	Male	EP3542512
Abrham	Gelan	Ayele	Sept. 7, 1992, midnight	Jimma	Ethiopian	Male	EP4783027
Wubshet	Metekia	Asnake	April 27, 1985, midnight	Degollo	Ethiopian	Male	EP4432969
Wendmagegn	Sema	Addis	June 19, 1990, midnight	Adis Ababa	Ethiopian	Male	EP4291350
Yared	Aklilu	Yenealem	Aug. 13, 1992, midnight	Quarit	Ethiopian	Male	EP4225245
Mulatu	Astarkie	Gebeyaw	Aug. 13, 1990, midnight	Adet	Ethiopian	Male	EP4225243
Tesfaye	Tarekegn	Adisu	Oct. 23, 1987, midnight	Nekemt	Ethiopian	Male	EP350954

Figure 5.6: Customer information retrieved from the database

The second experimental result of the study is how sample faces are collected and how fast it is like finger tamps are collected in the manual work of this system. The results obtained from this experiment is just capturing faces of the customer after the face and eyes are detected. In doing

so, the prototype took maximum one minute to take 40 faces per customer. Sample faces are normalized and saved in one folder in the form of grey scale imaging technique. Here, the researcher has used two combinations of eye and face detection techniques to achieve and improve the accuracy of the detection so that the machine can train only face images because we have seen the face detection tries to detect non face images. To overcome this challenge, eye detection is used.

The third experimental result of the study is list of crimes. Figure 6.3 shows how crime information retrieved from the database and how it can display, one sample applicant's information is retrieved from the database.



CUSTOMER	CRIME TITLE	DATE OF CRIME HAPPENED	CRIME DESCRIPTION
EP4278552 : Mulatu Gebeyaw	Sample Crime Title	Oct. 8, 2018, 4:41 p.m.	sample crime description

Figure 5.7: How crime information retrieved from the database

Fourthly, the study resulted how the recognition model is trained. Model training can be done in each day where the user starts work or if the user wants to update the model. The result shows that model training can took more than a minute depending on the number of customers stored in the database. If the number of customers stored in the system is increase, the time to train the model also increases. However, it is one-time task for the user of the system and it is just clicking a button before rushing to start recognition.

Fifthly, applicants are recognized and clearance form generated according to the information stored in the crime table in the database. The study showed that if an applicant is registered in the crime table, the generated clearance form will have all crime lists committed by the applicant as can be shown in figure 6.4. The result also shows that all applicant information is retrieved from the database by recognizing the face of an applicant and taking the passport number or residence ID from the face. As can be show in the figure, a place for the applicant's photo is reserved as well as for signature of the authority and the stamp of the office.


ETHIOPIAN FEDERAL POLICE CRIME INVESTIGATION BUREAU

Forensic Examination Diroctorate

Certification of Police Clearance

Full name: Temesgen Manderso Mokriaw SEX: M, Date of birth: Dec. 21, 1990, midnight

Place of Birth: Yelemelem, Nationality: Ethiopian, Passport/Residence ID: EP4458576

Reason for request: tt

Clearance requested by: tt

Reference number: tt , and Date: Nov. 6, 2018, midnight

This to certify that the above named person has not been convicted of any crime of misdemeanor until the date of issued certificate.

Signed by .....

Issuing date: 07/11/2018

Figure 5.8: Generated PCC from the prototype

5.3.2. Improvement of the model

As can be shown in Tables 5.1, the researcher listed out activities in EPCC along with their time takes in duration and average time in the existing system.

Table 5.1: Time takes to process PCC in Ethiopia in the existing system

No	Activity per individual	Duration it takes in minute/s	Average time in minute
1	Recording personal information	5 - 10	7.5
2	Collecting sample finger tamps	120 - 180	150
3	Processing PCC	1740 – 1800	1770
4	Getting PCC after processing	60 - 120	90
	Total time for all activates		2017.5

Figure 5.10 shows that the graphical representation of the time takes to process PCC in the existing system. The researcher used the data from observed experience while getting PCC in person.

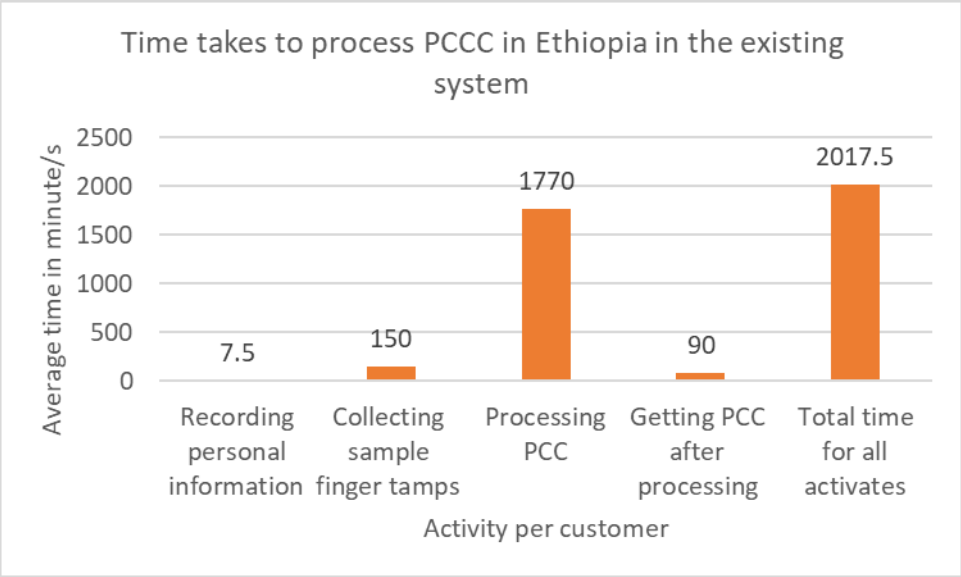


Figure 5.9: Graphical representation of the time takes to process PCC in Ethiopia in the existing system

Table 5.2: Time taken in EPCC processing in the existing system and the prototype

No	Activity per individual	Duration it takes in minute/s	Average time in minute
1	Recording personal information	5-10	7.5
2	Collecting sample faces	0.66-1	0.83
3	Processing PCC(model training, recognition, ..)	0.1-1	0.55
4	Getting PCC after processing	4-10	7
	Total time for all activates		15.88

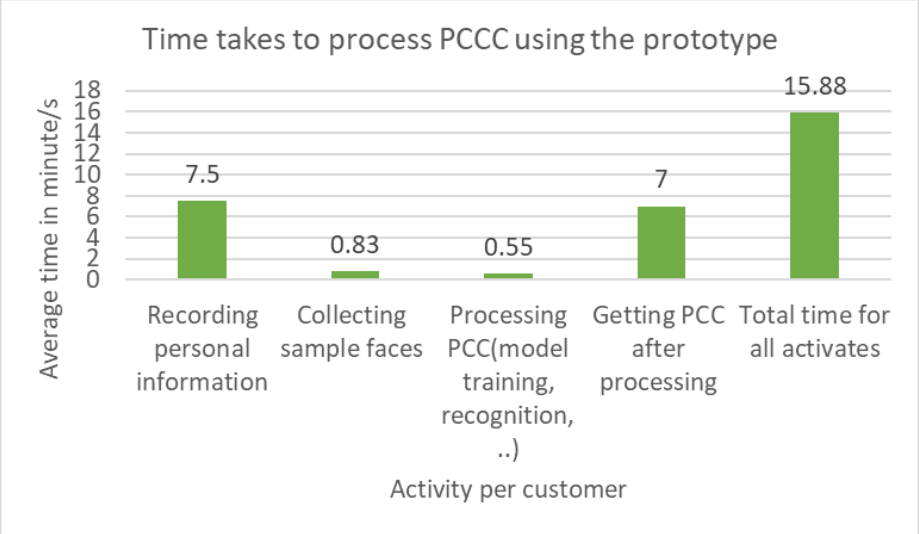


Figure 5.10: Graphical representation of the time takes to process PCCC using the developed prototype

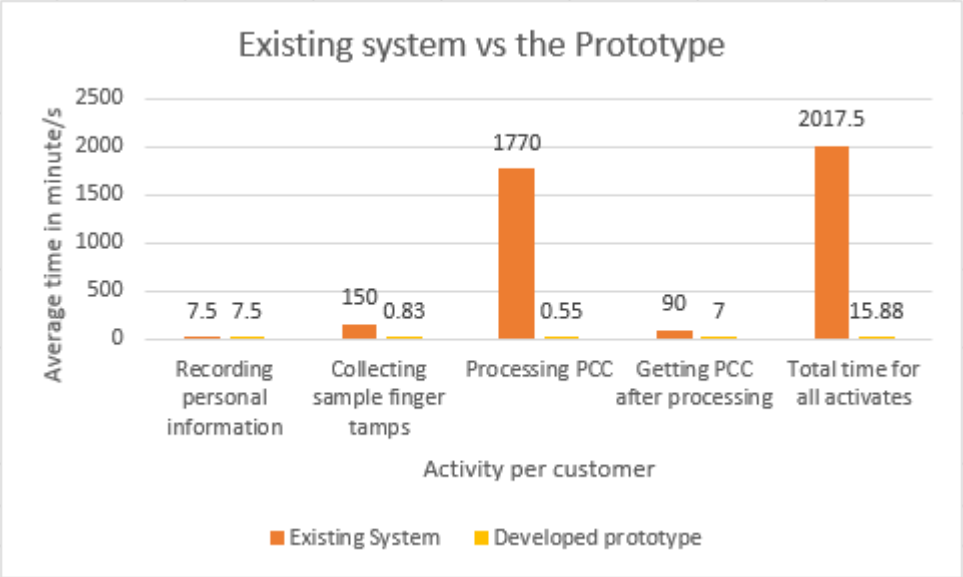


Figure 5.11: Graphical comparison of existing system and developed prototype in time they take

5.3.3. Discussion

The study shows the improvement of the prototype and the challenges that inhibit the accuracy of the recognition. The prototype improved the EPCC by making it web based application and can process the identification process with in a minute or minutes. As can be seen in Figure 5.8, the expected result of the study, PCC, is generated according to the study proposed either as "Convicted" or not "Convicted" by checking the applicant customer from the crime database.

However, the study shows that the recognition section is somehow dependent to the lighting conditions, a customer's sample face should take in a room where lighting condition is normal. This shows that if the sample faces are taken in light condition and dark condition, the result of the greyscale imaging technique also differs where the face taken in lighting condition has more white color compared to faces taken in dark light condition. Therefore, the study shows that there is a need of special window where the recognition and collection of sample faces are taken place unless the customer who is going to recognized in different lighting conditions may have a probability of failure in recognition. Furthermore, as can be shown in Figure 6.4, one customer can have two categories of faces: light faces and dark faces, this results that the recognition model may recognized as two different customers during recognition. However, the recognition works fine even though it returns different results.

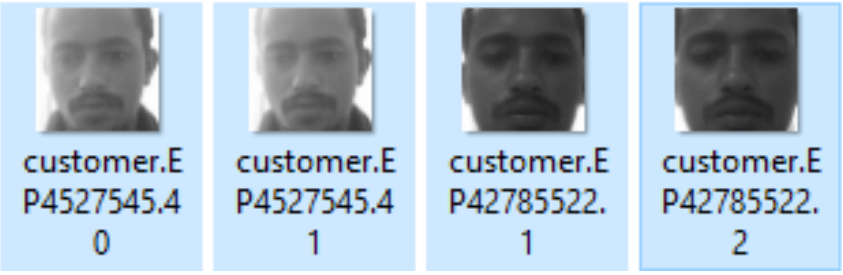


Figure 5.12: Lighting effect while taking sample faces and during recognition phase which makes the recognition accuracy to be low

Furthermore, this face biometric identification model can improve the proposed system having the challenges even though it needs some improvements in lighting condition and a camera

which results consistent pictures in the given lighting condition like HD cameras. However, this study has tested by using webcam which is poor quality in imaging.

Once more, as can be seen in Figure, testing of samples results 90% recognition accuracy, this shows that it is better improvement in applying criminal identification the study area. However, the result shows that 10% of the sample are failed in recognizing them accurately, instead, the recognition resulted others from the sample and this is due to lightening.

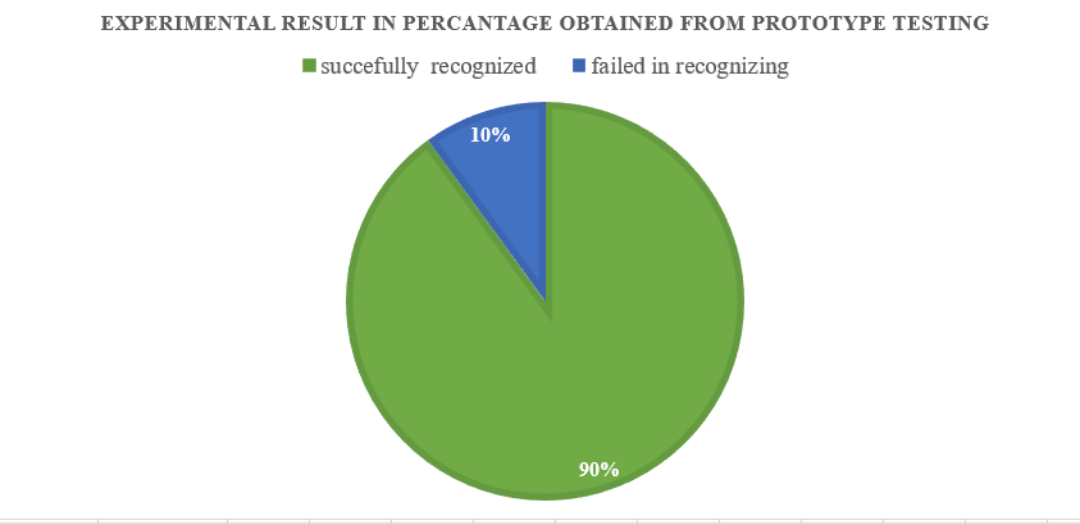


Figure 5.13: Accuracy of recognition during samples testing

Finally, in processing PCC, the study has no question in terms of its speed and accuracy of identifying criminals in the proposed system in the bureau. It can diminish the queue time and can do the PCC application in first come first serve pattern. The result shows that it can decrease the PCC processing time from 2017.5 minutes to 15.88 minutes. This can be taken as a great improvement in the bureau through the use of technologies, face biometrics identification technologies.

CHAPTER 6

CONCLUSIONS AND RECOMMENDATIONS

6.1. Conclusion

The aim of the thesis is to show how PC Certification can be improved using face biometrics technique which is much faster and flexible compared with the current manual working framework. The study area has problems in processing PCC in the bureau. Tasks' labor intensiveness, too much processing time, and identifying criminals accurately are the headache and prominent problems. According to the study result, to overcome these challenges in the bureau, face biometrics identification technique can be taken as a solution.

In implementing face biometrics identification platform, Eigenface recognition model has somehow advantageous in computing time during feature extraction, accuracy in recognizing individuals, and saving storage space during collecting and storing sample faces. Indeed, it uses PCA and SVM to take advantageous over other techniques. PCA is used to diminishing dimension, and as unsupervised machine learning in modeling the recognition algorithm. SVM is used for classification and recognition algorithm, and as supervised machine learning paradigm to apply classification of features and recognition of faces. To this end, the recognition results 90% accuracy in identifying of criminals and noncriminal based on samples during the experiment of the thesis, and 10% of failure in recognizing faces exactly. Once more, however, the result shows that the prototype recognizes individuals exactly whether they are registered in the system or not. To this end, a person whose sample face is not available in the dataset is rejected accurately and confidently. This shows that the prototype is a great achievement to replace the currently used working framework with some improvements.

The results show that face biometrics technique is convenience tool in processing PCC whereby the queue and processing time is minimized into minutes from over 24 hours, criminals can be identified accurately in processing PCC in the bureau, this, because identification of a person can only be achieved through biometrics techniques by using his own physiological characters.

Indeed, face biometrics identification technique has better comparison result compared with other biometrics techniques by using the same comparison metrics as indicated in the literature part of the study.

The result also shows that Eigenface face recognition algorithm is also depending on lighting condition, this shows that there should be a need of an improvement on the algorithm till it becomes independent from this lightening unless there is a need of designing such room where the lighting is going to be consistent through the life of the model.

Moreover, making the recognition to be accessible in the web is also great achievement of this study compared with related works done previously. This prototype of the thesis is one step ahead in designing the recognition to be web based where customers' information is stored using relational data base systems and making the prototype to be accessed in the internet through GUI. This helps the bureaus if they do have branches other than the main bureau.

In conclusion, supporting the work to be done in the bureau by using face biometrics technique is advisable to overcome the prominent problems faced so far in the bureau so that tasks will be accomplished within a minute and as a result customers become satisfy for the service they get.

6.2. Recommendations and Future Works

The study is limited only to show how face biometrics identification can improve PC Certification in Ethiopia, due to time and budget. Even though the prototype is designed well, it is advisable to make the prototype to be a state of the art face recognition platform. Furthermore, it is better to develop this thesis's result in raspberry pi to take sample faces, make the recognition efficient and accurate, and to use camera interfaces.

The camera API is only accessible on the hosted machine so it is better to use remote camera to make it accessible in the remote like IP Webcam. In this regard, there is a need of using libraries which are used to access the host camera other than the machine which does not have the source code. In addition to this, the distance between the camera and the face should be maximized

perhaps it can be improved through the use of high definition camera. However, in this study, the distance is limited only one meter to detect faces efficiently.

The result needs some improvements in lighting conditions where the trained faces and the recognition face could be the same color, unless there may be color difference even though the researcher applied greyscale imaging techniques. Therefore, it is better to improve this study to make it not depend on lightening.

Video analysis and liveness detection, car plate reader design and counter in Amharic language, product cost estimation and recommendations systems, and satellite image segmentation to support the agriculture are going to be the research area of the researcher in his future research career.

REFERENCES

21 Airport Facial Recognition Adoption Examples – BiometricToday. (2018, 08 18). Retrieved from Bimetric Today: https://biometrictoday.com/countries-airport-facial-recognition/

Abdullah N., Saidi, M. J., and Rahman, N. (2017). Face recognition for criminal identification: An implementation of principal component analysis for face recognition. In AIP Conference Proceedings (pp. 149-154). AIP Publishing.

Adnan K. and Kamil D., K. &. (2008). Image Compression using Neural Networks and Haar Wavelet. WSEAS Transactions on Signal Processing, 330-339.

Akarun, L. G. (2005). 3D face recognition for biometric applications. 2005 13th European Signal Processing Conference. IEEE.

Akarun, L. G. (2005). 3D face recognition for biometric applications. 2005 13th European Signal Processing Conference. IEEE.

Anil K. Jain, Arun R., and Salil P.(2004). An introduction to biometric recognition. Transactions on circuits and systems for video technology, 4-20.

Anum K. and Monika S. (2016). Biometrics in Forensic Identification: Applications and Challenges. Journal of Forensic Medicine.

Bhardwaj, R. and Gupta, B. (2015). Face Recognition using Principal Component Analysis. Advances in Computer Science and Information Technology (ACSIT), 69-71.

Bhatia, R. (2013). Biometrics and Face Recognition Techniques. International Journal of Advanced Research in Computer Science and Software Engineering.

Chinese police now using sunglasses with facial recognition. (2018, 08 17). Retrieved from Asian Corespondent : https://asiancorrespondent.com/2018/

Delbiaggio, N. (2017). A comparison of facial recognition's algorithms.

Dimililer, K. (2017). IBFDS: Intelligent Bone Fracture Detection System. Procedia Computer Science, 260-267.

Face Recognition Vs Fingerprint: 10 Key Differences To Know | Biometric today. (2018, 08 16). Retrieved from Biometric Today: https://biometrictoday.com/

Fanabc. (2018, 08 14). FBC. Addis Ababa, Addis Ababa, Ethiopia. Retrieved from Fana Broadcasting Corporate: http://fanabc.com/component/k2/item/24960.html

Faruqe M. and Hasan O. (2009). Face recognition using PCA and SVM. In Anti-counterfeiting, Security, and Identification in Communication, 97-101.

Fingerprint Recogntion vs Facial Recognition. (2018, 08 17). Retrieved from Bayometric: https://www.bayometric.com/fingerprint-vs-facial-recognition/

Kapoor and Anup (2016). Biometrics in Forensic Identification: Applications and Challenges. Journal of Forensic Medicine.

Kataria G., A. K. (2015). Mapping of the emerging digital forensic technologies for crime investigations in Ethiopia: A call for nation security, Safety and sustainability. Journal of Research in Humanities and Social Science, 42-46.

Kaur and Himansh (2015). Face Recognition Using Principal Component Analysis. In Advance Computing Conference, 585-589.

Khashman A. & Dimililer K. (2008). Image Compression Using Neural Networks and Haar Wavelet. WSEAS Transactions on Signal Processing.

Khashman A., Sekeroglu B. & Dimililer K. (2006). ICIS: A Novel Coin Identification System.

Kim, K. I. (2002). Face Recognition Using Kernel Principal Component Analysis. IEEE signal processing letters, 40-42.

Nautiyal, P., Gahlot S., & Mishra (2013). An Automated Technique for Criminal Face Identification Using Biometric Approach. Conference on Advances in Communication and Control Systems 2013.

Paulo Menezes (2004). Face tracking based on haar-like features and eigenfaces. IFAC, (pp. 304-309).

Piyush and Vibhor (2018). Criminal Identification System Using Face Detection and Recognition. International Journal of Advanced Research in Computer and Communication Engineering.

Riddhi P. and Shruti B., R. P. (2013). A Literature Survey on Face Recognition Techniques. International Journal of Computer Trends and Technology (IJCTT).

Service-Crime-Federal Police Commission. (2018, 08 18). Retrieved from Ethiopian Federal Police Commission: http://www.federalpolice.gov.et

Shoken V., Vandna S., and Bhupendra S. (2013). Face detection by haar cascade classifier with simple and complex backgrounds images using opencv implementation. International Journal of Advanced Technology in Engineering and Science.

Siswanto and et al, A. R. (2014). Implementation of Face Recognition Algorithm for Biometrics Based Time Attendance System. In ICT For Smart Society (ICISS) (pp. 149-154). IEEE.

Turk & Pentland, 1. (1991). Face recognition using eigenfaces. In Computer Vision and Pattern Recognition. Proceedings. 1991 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (pp. 586-591). IEEE.

Viola and Jones, P. V. (2001). Rapid Object Detection using a Boosted Cascade of Simple Features. Accepted conference on computer vision and pattern recognition.

Vishnu G., Bagadi R. and Tusar K. (2017). Face Recognition Techniques: A Survey. International Journal of Innovative Research in Computer and Communication Engineering.

Yogesh B. and Dr.Anilkumar N., Y. B. (2015). Human Face Recognition Using Image Processing PCA and Neural Network. International Journal of Innovative Research in Science, Engineering and Technology.

APPENDICES

APPENDIX 1

CUSTOMER DETAIL REGISTRATION SAMPLE CODE

```
#customer detail registration logic goes here
def add_customer(request):
    form= CustomerForm2(request.POST or None)
    success=False
    if form.is_valid():
       passport_number_or_residence_id=
form.cleaned_data['passport_number_or_residence_id']
       form.save()
       success=True
       BASE_DIR = settings.BASE_DIR
       face_cascade =
cv2.CascadeClassifier(BASE_DIR+'/FaceBiometricsApp/haarcascade_frontalface_def
ault.xml')
       eye_cascade =
cv2.CascadeClassifier('FaceBiometricsApp/haarcascade_eye.xml')
       cap = cv2.VideoCapture(0)
       counter=0
       while 1:
           rec,img = cap.read()
           gray = cv2.cvtColor(img, cv2.COLOR_BGR2GRAY)
           faces = face_cascade.detectMultiScale(gray, 1.3, 5)

           for (x,y,w,h) in faces:
               cv2.rectangle(img,(x,y),(x+w,y+h),(0,200,250),3)
               #compute region of interest
               roi_gray = gray[y:y+h, x:x+w]
               roi_color = img[y:y+h, x:x+w]

               eyes = eye_cascade.detectMultiScale(roi_gray)
               for (ex,ey,ew,eh) in eyes:

cv2.rectangle(roi_color,(ex,ey),(ex+ew,ey+eh),(10,255,20),2)
                   counter=counter + 1 #count taken sample faces

cv2.imwrite('FaceBiometricsApp/MachineLearning/Dataset/customer.'+str(passport
_number_or_residence_id)+'.'+str(counter)+'.jpg', gray[y:y+h,x:x+w])
```

```
                cv2.waitKey(250)

        cv2.imshow('Collecting sample faces',img)
        cv2.waitKey(1)
        if(counter>39):
         break
    cap.release()
    cv2.destroyAllWindows()
form=CustomerForm2()
context= {'form': form,'message':success }
return render(request, 'FaceBiometricsApp/new_customer.html', context)
```

APPENDIX 2

MODEL DESIGN SAMPLE CODE

```
from django.db import models

# Create your models here.
class Customer(models.Model):
    name = models.CharField(max_length=200)
    surname =models.CharField(max_length=200)
    father_name=models.CharField(max_length=200)
    date_of_birth = models.DateTimeField('Date of Birth')
    place_of_birth=models.CharField(max_length=1000)
    nationality=models.CharField(max_length=100)
    SEX = (
        ('M', 'Male'),
        ('F', 'Female'),
    )
    sex=models.CharField(max_length=5,choices=SEX)

passport_number_or_residence_id=models.CharField(max_length=100,unique=True)
    verbose_name = 'Customer Summary'
    verbose_name_plural = 'Customers Summary'
    def __str__(self):
        return '%s %s %s' % (self.passport_number_or_residence_id+' :',
self.name, self.father_name)

class PCCApplication(models.Model):
    customer = models.ForeignKey(Customer, on_delete=models.CASCADE)

    reason_for_request=models.TextField(max_length=2000)
    clearance_requested_by=models.TextField(max_length=1000)
    reference_number=models.CharField(max_length=1000)
    date = models.DateTimeField()
    date.help_text="Please use the following format: <em>MM/DD/YYYY</em>."
    verbose_name = 'PCC Application'
    verbose_name_plural = 'PCC Application summary'
    def __str__(self):
        return '%s %s' % (self.customer, '( '+self.clearance_requested_by+'
)')

class Crime(models.Model):
```

```
    customer = models.ForeignKey(Customer, on_delete=models.CASCADE)

    crime_title=models.TextField(max_length=1000)
    crime_description=models.TextField()
    date_of_crime_happened = models.DateTimeField()
    verbose_name='List of Crime'
    verbose_name_plural='List of Crimes'
    def __str__(self):
        return  self.crime_title
```

APPENDIX 3

RECOGNITION SAMPLE CODE

```
#face recognition logic goes here below
def FaceRecognitionLogic(request):
    url=''
    svm_pkl_filename =
BASE_DIR+'/FaceBiometricsApp/MachineLearning/Serializer/svm_classifier.pkl'

    svm_model_pkl = open(svm_pkl_filename, 'rb')
    svm_model = pickle.load(svm_model_pkl)
    print ("Loaded SVM model :: ", svm_model)

    pca_pkl_filename =
BASE_DIR+'/FaceBiometricsApp/MachineLearning/Serializer/pca_state.pkl'

    pca_model_pkl = open(pca_pkl_filename, 'rb')
    pca = pickle.load(pca_model_pkl)
    print ('Loaded pca Model :: ', pca)
    facedata =
cv2.CascadeClassifier(BASE_DIR+'/FaceBiometricsApp/haarcascade_frontalface_def
ault.xml')
    eye_cascade =
cv2.CascadeClassifier('FaceBiometricsApp/haarcascade_eye.xml')
    cascade = facedata
    cap = cv2.VideoCapture(0)

    while 1:
        ret, img = cap.read()
        gray = cv2.cvtColor(img, cv2.COLOR_BGR2GRAY)
        faces = cascade.detectMultiScale(gray, 1.3, 5)

        for (x,y,w,h) in faces:
            cv2.rectangle(img,(x,y),(x+w,y+h),(0,200,250),2)
            roi_gray = gray[y:y+h, x:x+w]
            roi_color = img[y:y+h, x:x+w]
            eyes = eye_cascade.detectMultiScale(roi_gray)
            import socket
            hostname = socket.gethostname()
            fileName=hostname+'_customer.jpg'
            for (ex,ey,ew,eh) in eyes:
```

```
                cv2.rectangle(roi_color,(ex,ey),(ex+ew,ey+eh),(0,255,0),2)

cv2.imwrite('FaceBiometricsApp/MachineLearning/uploads/'+fileName,
gray[y:y+h,x:x+w])

imgPath=BASE_DIR+'/FaceBiometricsApp/MachineLearning/uploads/'+fileName
        cv2.imshow('img',img)
        k = cv2.waitKey(30) & 0xff
        if k == 27:
            break

    cap.release()
    cv2.destroyAllWindows()
    img = Image.fromarray(gray)
    img = img.resize((150,150), Image.ANTIALIAS)
    try:
        print('Function calling...')
        #function to normalize the detected image for recognition
        def nomalizingFace(image):
            cascade =
cv2.CascadeClassifier(BASE_DIR+'/FaceBiometricsApp/haarcascade_frontalface_def
ault.xml')
            img = cv2.imread(image)
            minisize = (img.shape[1],img.shape[0])
            miniframe = cv2.resize(img, minisize)

            faces = cascade.detectMultiScale(miniframe)

            for f in faces:
                x, y, w, h = [ v for v in f ]
                cv2.rectangle(img, (x,y), (x+w,y+h), (255,255,255))

                sub_face = img[y:y+h, x:x+w]
                 gray_image = cv2.cvtColor(sub_face, cv2.COLOR_BGR2GRAY)
                img = Image.fromarray(gray_image)
                img = img.resize((150,150), Image.ANTIALIAS)
            return img
        inputImg =nomalizingFace(imgPath)
    except :
        print("Customer not Recognized")
        return redirect('/FaceBiometricsApp/error')
```

```
    imgNp = np.array(inputImg, 'uint8')
    imgFlatten = imgNp.flatten()
    imgArrTwoD = []
    imgArrTwoD.append(imgFlatten)
    img_pca = pca.transform(imgArrTwoD)
    pred = svm_model.predict(img_pca)
    print(svm_model.best_estimator_)
    if (str(pred[0])!=''):
        print (pred[0])
        url='/FaceBiometricsApp/detail/'+str(pred[0])
    else:
        print('Face Not Recognized')
        url='/FaceBiometricsApp/error'
    return redirect(url)
```

APPENDIX 4

LOADING CUSTOMER DETAILS

```
def detail(request, passport_number_or_residence_id):
    customer = get_object_or_404(Customer,
passport_number_or_residence_id=passport_number_or_residence_id)
    print('recognized customer id: ')
    print(customer.id)
    id=PCCApplication.objects.order_by('-id')[:1]
    print(id)
    application=PCCApplication.objects.get(customer=customer.id)
    context={

           'customer' : customer,
           'application' : application,
   }
    return render(request, 'FaceBiometricsApp/detail.html', context)
```