BIOMETRIC SYSTEM BASED ON FACE RECOGNITION SYSTEM

Suad Hajı Ahmed Omar

Master Thesis

Department of Software Engineering

Supervisor: Prof. Dr. Asaf VAROL

June-2016

REPUBLIC OF TURKEY
FIRAT UNIVERSITY

THE INSTITUTE OF NATURAL AND APPLIED SCIENCES

BIOMETRIC SYSTEM BASED ON FACE RECOGNITION SYSTEM

MASTER THESIS

Suad Haji Ahmed Omar

(141137102)

Thesis Submitted Date: **05 May 2016**
Thesis Defense Date: **02 June 2016**

Supervisor: **Prof. Dr. Asaf VAROL (F.Ü.)**
Other members of the jury: **Assoc.Prof. Dr. M. Fatih TALU (I.U.)**
Asst. Prof. Dr.Mustafa ULAŞ (F.U.)

June - 2016

DECLARATION

I am presenting this thesis with title “Biometric System Based on Face Recognition System” for the requirement of Master’s degree in Software Engineering. I declare that proposed system in thesis is my own work with all simulations and programming.

Suad Haji

Elazig, 2016

DEDICATION

This thesis is dedicated to my wonderful mother for her love and measureless support and my husband and my older sister for their greatest influence on my life.

ACKNOWLEDGEMENTS

I want to thank all the staff members of Department of Software Engineering at Firat University, without their help it would be impossible for me to complete my study of Master Degree. It was my first time in my life to stay outside of my own country for as long but the love and care of all staff members including staff of my hostel never let me to feel any difference. Prof. Dr. Asaf VAROL was not only chairman of my department, he was also supervisor for my thesis. During the study he helped me more than a chairman and teacher. Words cannot pay back anyone's kindness and help but still I want to say thanks to all.

Secondly, I would like to thanks to the department members of Software Engineering for their significant helps and feedback as well as for accepting my thesis and continued to encourage me, I learned a lot from them.

Lastly, I would like to express my sincerest gratitude to my parents for their supports and encouragement throughout my studies. This studies would not have been possible without support of my wonderful mother, sisters, my husband, and brother's, thanks for their support and companionship.

TABLE OF CONTENTS

Page No

ABSTRACT

Biometrics is a term used to define an individual's DNA, hand geometry, face, etc. or behavioral characteristics, such as hand signature, voice tone, keystrokes and so on. For that reason, these biological characteristics are unique in every individual. In many situations, face recognition related technologies are becoming more popular among biometric-based technologies as it measures an individual's natural data. Genetic biometrics generally used to authenticate and identify individuals by analyzing their physical characteristics, such as fingerprint, eye iris, can act as an additional security measure at Automated Teller Machines. Instead of using a bankcard, a camera installed at the Automated Teller Machines would capture an image of the customer's face, and compare it against the account holder's photos in the bank database to verify the customer's identity. The purpose of this thesis is to present a Windows based real time application system using face recognition algorithms. This new system can be applied in various different fields such as identity verification and other potential commercial applications. Both Eigen and Local Binary Patterns face algorithms were used to reduce the impact of light exposure that will affect the accuracy of the system.

Keywords: Biometrics, Face Detection, Face Recognition, Eigen Faces, LBP algorithms.

LIST OF FIGURES

Page No

LIST OF TABLES

Page No

ABBREVIATIONS

PCA : Principal Component Analysis

FRS : Face Recognition Systems

LBP : Local Binary Patterns

AI : Artificial Intelligence

DNA : Deoxyribo Nucleic Acid

ATM : Automated Teller Machine

US-VISIT : (United States Visitor and Immigrant Status Indicator Technology)

PINs : Personal Identification Number

1. INTRODUCTION

In the last decades the concern to different biometric identification systems among individuals has grown up. Government agencies and private organizations are interested in technology of biometric recognition as it increases the level of protection of secret and the security of confidential information. Companies that deal with the range of information technology use fingerprints, face, voice, iris recognition in order to protect diffusion of external individuals to their systems.

Face recognition is one of the biometric systems that automatically identifies or verifies a person's identity using his/her facial features and expressions. It is widely used to identify passports and driver's licenses carrying individuals even if they are not aware that a face recognition system is autonomously checking their identity [1,2]. Face Recognition System has many applications in the modern world such as logging in to a computer using facial verification as a password, gaming, people tagging, security and so on [3]. The current Face Recognition Systems and applications in the market have deficiencies that ranges from reliability problems, reduced recognition accuracies in certain environment, complicated feature extraction, high setup costs and performance issues. However the demand for a robust Face Recognition System (FRS) applicable across various industrial uses, organizations and the general public is increasing dramatically.

1.1. Statement of the Problem

Biometric recognition of people is a challenging problem, which has received much attention in these years because of its increasing security demands and its potential applications in different fields. Face Recognition is one of them, and up now, it is not providing a robust solution, so that our system is Face Recognition, which makes it a great biometric project that can identify perfect a person's face at the same time.

Security issue is a special case concerned almost each and every school, organization, institutions and general public everywhere. All private and public sectors need to increase their security major in order to prevent any external intrusion or illegal usage of resources or facilities. Human computer interface security system is one of the most important fields of research in recent years; there are many systems and programs developed in order to address security issue in the globe today. But the deficiencies of the developed applications make it necessary for the developers to come up with a reliable solution to address those issues**.**

1.2. Project Overview

Artificial Intelligence (AI) [4] is a branch of computer science and engineering that focuses on many applications. AI is an area of study concerned with making computers copy intelligent human behavior. The aim of this project (Face Recognition System) is to develop an application (windows based application) that will provide intelligent security solution to public and private sectors. Face Recognition System (FRS) is a system that can be used to save the images of registered staff or members of an organization in a database, after that the system will be used to detect and recognize anyone that is not registered and inform the personal in charge of security in order to take necessary actions.

1.3. Scope and Limitation

The system has the following limitations:

- The system can detect, extract and recognize only frontal faces from acquired live images;
- The distance of the person from the camera should be in 1 to 3 feet for better result;
- The system will be applied and tested in a fix environment with ordinary illumination;
- The problems such as sunglasses, eyeglasses and other accessories that can partially or fully cover the face are not subject for face recognition;
- The system cannot identify the difference of an identical twin;

2. BIOMETRICS

2.1. Overview

Biometric is a Greek word that consists of two words (‘bio’ and ‘metric’) which means ‘life’ and ‘to measure’ respectively. Biometric systems are used to measure and analyze an individual’s unique characteristics.

According to research conducted by Bonsor (2008), biometric is a science identifying the person's biological data by using both unique physical characters of person and technology. Biometric measures and analyzes human body characteristics such as voice, facial patterns, fingerprints, eye irises, and hand measurements, by taking advantage of information technology [5].

Biometric systems use two kinds of modes. These are identification and verification (authentication) modes. In the identification mode, the system tries to find a match for captured biometric data of the person from a database (probably large) storing different records of people's biometric data comparing N of samples or templates and then decides if both captured and stored data refers to the same person. Figure 2.1 illustrates the identification concept.

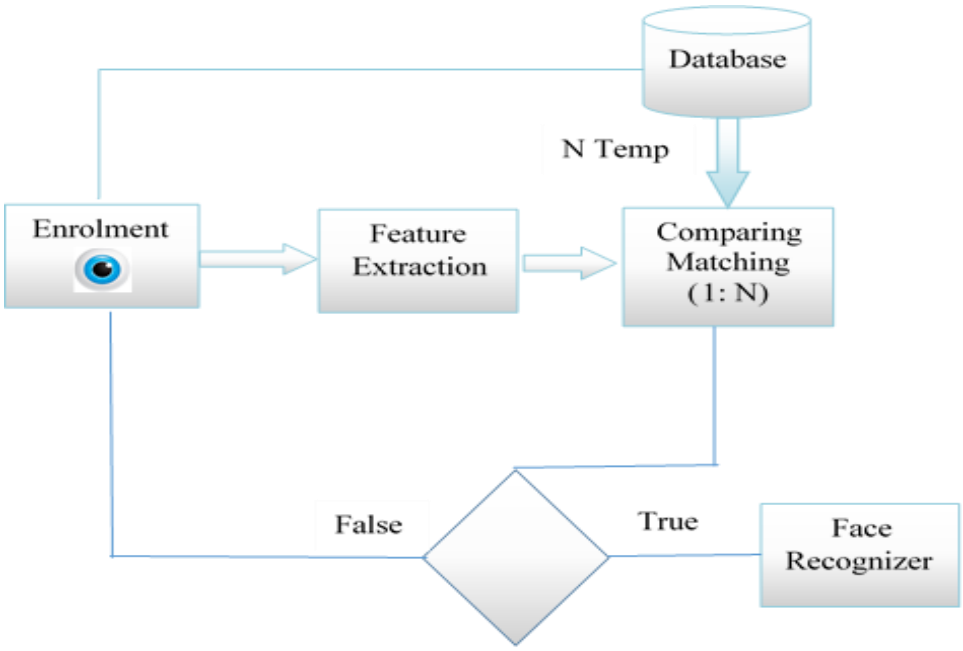


Figure 2.1. Identification Mode

In the verification mode, system compares the captured or scanned person's biological data like images of face, iris, scanned fingerprint patterns or voice, to person's biometric samples or

templates that already stored in a database to ensure that this is the same person. The procedure of verification mode is given in Figure 2.2. This mode requires less time and is used for access control in buildings or systems.

In the both identification and verification modes the first time of entering a biometric data into a system is called enrollment. During the enrollment process, biometric data is captured from the individuals and then stored to a database. In subsequent uses, biometric data is captured and compared with the information kept and stored at the time of enrollment stage.

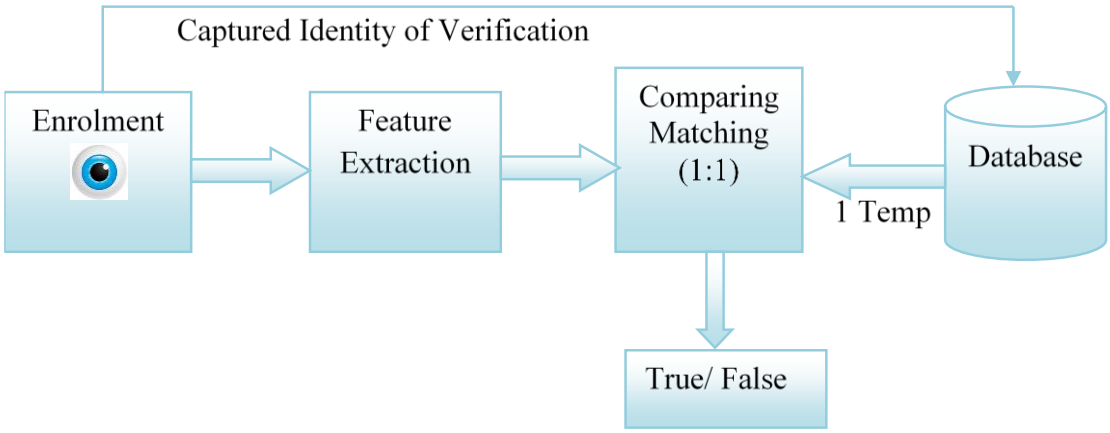


Figure 2.2. Verification Mode

2.2. Types of Biometrics

Biometrics can be classified into two groups according to their functionality modes or methods they are using. These two groups are Behaviometrics and Physical biometrics. Each of them is discussed in the following sections.

2.2.1. Behaviometrics (behavioral biometrics)

The word Behaviometrics combines two terms behavioral and biometrics. Behavioral implies the behavior of an individual and biometric refers to the technologies and methods that measure and analyze spiritual biological characteristics of the individual's body for identification or verification purposes. In other words, Behaviometric or behavioral biometric is a measureable behavior used to recognize and verify the identity of a person and it focuses on behavior interactive patterns rather than physical attributes.

Signatures, keystrokes are examples of behavioral biometrics. For example, by using Behaviometrics, the behavior of a person's signature (like speed, direction, pressure and the total

time it took for the person to complete the creation of a signature), can be verified. Likewise, the behavior of a person's key-strokes on a keyboard (like speed, pressure, total time it took to type particular words and time between hits on specific keys) can be determined. Figure 2.3 shows some examples of behavioral biometric.

Figure 2.3. Examples of behavioral biometric (a) Keystroke, (b) Signature

2.2.2. Physical Biometrics

Physical biometric relates to physical characteristics of the individuals in contrast to behavioral biometric. It is a kind of biometric that is based on a physical characteristic of an individual or a person. Some examples of physical biometrics are Face and Iris recognition systems, fingerprint, hand geometry, and DNA. Here, we are discussing them briefly.

Face recognition identifies or verifies an individual's identity using his/her facial features and expressions. The face recognition process often involves detecting the face by extracting it from the rest of the person's image, or locating face image into a database if it does not already exist, or compare it to images which are already stored to a database for recognition purposes. Face recognition systems use some algorithms to analyze physical features of a person's face. Every human face has different nodal points. Some of these points that can be measured by the face recognition systems are:

- Size and shape of the eyes
- Distance between the eyes
- The shape of the cheekbones
- Width and shape of the nose
- The length of the jaw line

Iris recognition is one of the biometric systems that use physical identification based on the person's unique characteristics of the eye (iris). Iris is the colored circle area of the eye that usually colored with brown or blue. Iris recognition works on individual's eye. It takes eye image as an

input and then extracts iris part from the eye image. Iris recognition systems compare the scanned or captured iris image to the stored photos or templates to make identification and find a match for iris image.

Fingerprint biometric is one of the physical biometrics used to identify individuals and verify their identity using unique fingerprint attributes. Normally, a fingerprint scanner system gets and scans an image of person's finger. After that, the system determines whether the pattern of arch ridges and loop ridges of the scanned or captured finger image matches the pattern of arch ridges and loop ridges in pre-stored images. Figure 2.4 shows some examples of commonly used physical biometrics.

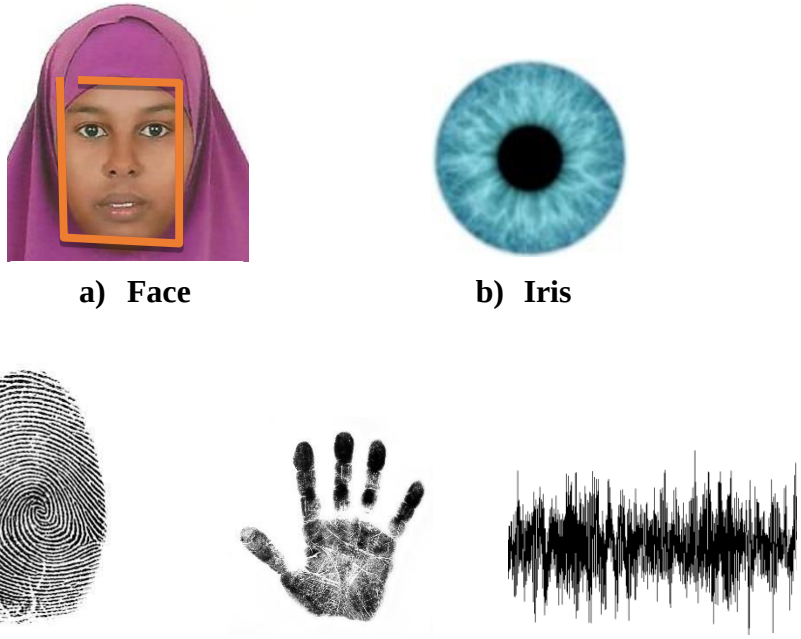


Figure 2.4. Examples of physical biometric that are commonly used

The work of this thesis concerns only Face Recognition Systems. It explores how face recognition works and finally recommending to build a security system using face recognition biometrics.

3. FACE RECOGNITION

This chapter presents a short discussion about uses of face recognition systems, the tasks and processes of face recognition system and existing dimensional methods that are used to extract face features.

3.1. Use of Face Recognition Systems

In recent years, biometric-based techniques have become the most useful and popular option for recognizing and authenticating individuals. In order to allow individuals access physical or virtual systems, biometric-based authentication techniques use an individual's physiological or behavioral characteristics to define his/her identity, instead of using passwords, PINs, smart cards, keys and so on.

Passwords and PINs are hard to recall and can be easily stolen or predicted. Also, cards, keys and others can be misplaced, forgotten, or duplicated. Likewise, magnetic cards can become unreadable or partially corrupted. On the other hand, an individual's biological qualities cannot be stolen, misplaced, forgotten or copied. Biometric-based technologies include identification based on physiological characteristics (such as iris, face, finger geometry, fingerprints, hand geometry, ear and voice) and behavioral traits (such as signature and keystroke).

As one of these (Biometric-based technologies), there are many situations where the Face Recognition System is becoming popular. Face recognition can be used as a security measure at Automated Teller Machine (ATM). Instead of using a bank card, a camera installed in the ATM would capture an image of the customer's face, and compare it to the account holder's photos in the bank database to confirm the customer's identity [6].

Face Recognition System is widely used by government agencies for security and also to eliminate frauds. For example, the U.S. government has begun using a program called US-VISIT (United States Visitor and Immigrant Status Indicator Technology). This program is aimed to identify the foreign travelers entering to the United States using combination of face photograph and fingerprints. When a foreign traveler receives his/her visa in somewhere outside the US, his/her fingerprints and photographs are taken. When the person arrives in the US, those fingerprints and photographs will be used to prove that this person is the same person who received the visa [7].

3.2. Face Recognition Methods

Like other biometric systems, face recognition system functions in either face identification (recognition) or face verification (authentication) method. The use of these two methods depends on the nature of the system, like how quickly the system operates and what size of a biometric database consumes. Let us discuss each in detail.

3.2.1. Identification (recognition)

This is the process of recognizing an individual's identity by executing matches against multiple image templates already stored in a database or in a file. Face identification systems are different from face verification systems because they try to accept or deny the identity claimed by an unknown individual. These systems try to answer the questions "Who is this individual?" or "To whom this face image refers to?" So that, they have to compare the presented face template against the trained face of known people, those already stored in the database. If there is a match, they accept and recognize the individual's identity otherwise they deny it [8].

In simple words, in face identification (recognition) systems the input image will be compared to number of known images, so as to identify to whom the input image belongs to or even whether it does not belong to no one in the database. Figure 3.1.demonstrates the concept.

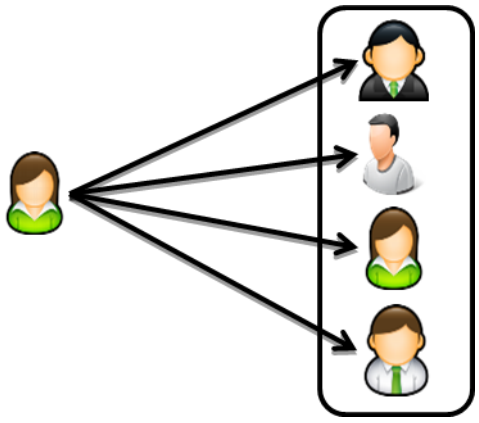


Figure 3.1. Face Identification Method

Face identification (recognition) systems are described as a One-to-Many (1: N) matching systems. Where N is the total number of face image templates in the database or in the file. Forensic databases, where a government tries to identify and recognize a face of a criminal or an offender often use face identification (recognition) system.

3.2.2. Verification (Authentication)

In the face verification system, the individual claims that he/she is in the system's image templates and presents his/her facial biometric sample to the system. The system then checks the presented individual's face image and compares to the template that he/she claimed to be. The system accepts if the claimed identity is true or rejects if it is false [9].

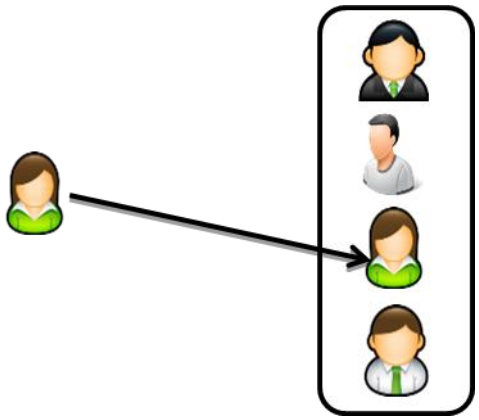


Figure 3.2. Face Verification Method

Verification systems are generally called as one-to-one matching systems because these systems try to match the biometric of facial characteristics presented by the individual against a specific image template already stored in a database or in a file. For example, if an individual stands up in front of a face verification (authentication) system and claim to be a certain individual, the system only checks if the claimed individual's identity is that person or not as shown in Figure 3.1.

Systems that use verification task method are commonly generate results more quickly and are more accurate than systems that use identification task method, because they only need to compare the individual's facial biometric to only one template reference stored in the database. The purpose of the verification systems is to prevent from multiple individuals to use the same identity [10].

3.3. Face Recognition Processes

In this section we discuss the processes that face recognition system passes during its normal operation of work. Face recognition system typically involves four steps as shown in Figure 3.3. These steps include capturing (acquiring) face image, preprocessing face image, extracting face features, and matching face features (recognition). We discuss these steps in the following sections.

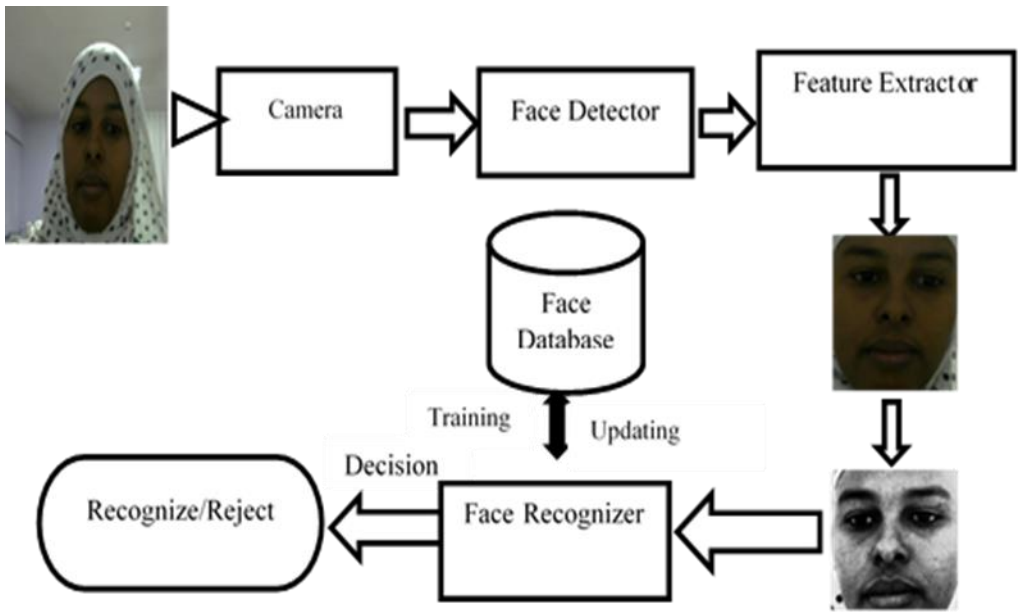


Figure 3.3. A Framework for Face Recognition System

3.3.1. Face Detection (acquisition)

Face Detection is the prior step and the entry point of the face recognition process. This step is where the face image under consideration is presented to the face recognition system. To have an accurate detection of individual's face image, is one of the most important processes involved in face recognition system. When face image exactly and accurately placed in the detection step, the other remaining recognition steps would not be so complicated.

Face Detection or acquisition step can capture a face image from different surrounding equipment. The face image can be an image file format that is located on either an optical or magnetic disk. It can also be captured by a digital camera directly or it can be scanned from photo paper with the help of a scanner machine. The next step is preprocessing and aligning face image.

3.3.2. Preprocessing Face Image

The main midpoint of the face preprocessing step is to normalize and filter face image after detection. Preprocessing helps achieving a strong face feature at the feature extraction process. It determines the location and size of the captured image face. It also resets the color of the image in order to increase the image quality. Some of the pre-processing steps that may be applied in a face recognition system include:

- **Face Image Size Normalization**: It usually changes the acquired face image size to a default image size such as 160 x160, on which the face recognition system can be easily operated on it.
- **Histogram Equalization**: In order to normalize and enhance image quality, equalizing histogram of too dark or too bright images and modifying the contrast range of the images is important. As a result of that equalization and modification, some important facial features become more obvious and overall face recognition performance become improved.
- **Filtering the Median**: It normalizes images which contain noisy effects especially those have been obtained from a camera, and median filtering cleans the image without losing its original information.
- **Background Removal**: In order to detect pure face and ignore anything else found inside the image file, such as background buildings, trees and bodies, face background technique may be used. This is important for face recognition systems which use entire information contained in the face image. Therefore, the preprocessing step must be able to determine and detect only the face skeleton.

3.3.3. Feature Extraction

The aim of this step is to extract a compressed set of personal discriminating geometrical and biometrical features of the face image. After performing some pre-processing steps (if necessary), the normalized face image is passed to the feature extraction section in order to find the key features that will be used for classification and matching process. In other words, this section is responsible for producing a feature vector that is sufficiently well enough to characterize the face image.

The goal of feature extraction process is to improve the effectiveness and efficiency of analysis and matching. This may be done by eliminating redundancy in the image data, and extracting dimensional information (size, shape and so on) which is vital to target identification.

3.3.4. Feature Matching

Feature matching is the real recognition process. The feature vector or geometrical features obtained from the feature extraction is matched to individual's facial images already enrolled and stored in a database or a file.

In this final step maybe we can have different purposes, whether it is identification or verification. As we mentioned in the previous sections, if identification takes place the image will be compared with all images in a database. But if it is verification the image will match to only one image in a database.

3.3.5. Training set

Training set: In our project, which contains about 50 faces images and are categorized both female and male. Also the dataset has different conditions for each person to be tested, including frontal face. Moreover, in the project, the incoming picture is captured in real-time, we are able to add the new faces into the database to be part of the training images.

3.3.6. Face database

Face database: describes face images component and it also retrieve and stored information about the faces images.

A data file database is similar to database that it is a storing place for a database. Like a data file, a database it's not allowed you or does not existing data directly to a user; the user runs an application that accesses data from the database and presents it to the user in an reasonable format.

We implemented a very single backend with Microsoft office access 2013. Currently, the database conducts the basic functions by only storing the new data / staff records. Also, academically, the database should store millions of face image to be compared other database already stored.

3.4. Dimensions used by Face Recognition

To measure the nodal points of a face image, facial recognition System uses an algorithm to create a special numeric code that represents the face template in the database.

3.4.1. 2-D (Two-Dimensional)

This is the oldest and widely used method in face recognition systems. This method it is not more reliable but does not need any expensive equipment. It uses normal digital camera to capture face images which means it strongly depends on the light mechanisms. For that reason problems may occur if the person wears classes or has a big beard or moustache. To reduce these problems the individual should look straight forward to the camera with natural face expressions as shown in Figure 3.4 [11]. The light variation mechanisms should also be clear and professional.

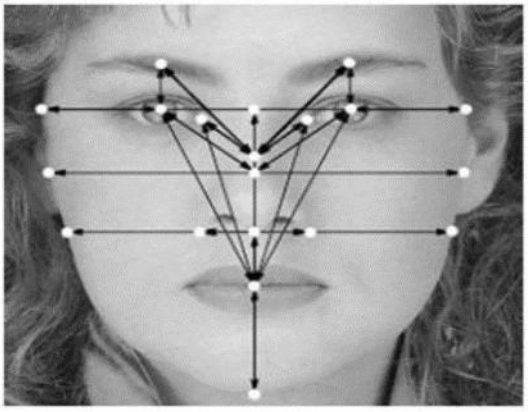


Figure 3.4. Example of 2D facial recognition technology

3.5. Face Recognition Advantages

Face recognition can play an important role in various fields like:

- **Security**: the main reason of this type of systems where developed is security and surveillance issues access control for homes, companies, stores, banks, etc.
- **Law enforcement**: Fingerprint was the strongest evidence that can convict a criminal in crime scene, or in borders check point, now face recognition can offer important role for criminals identification investigations, airports security to recognize forbidden person from traveling and watching terrorist.
- **Authentication**: investigating the identity of a person for certain condition, tasks, permissions access control.
- **Banking**: banking field requires high level of accuracy in systems for authentications and security system, face recognition helps great deal in these purposes.
- **Military**: where no mistakes are allowed most existing technologies now where developed to serve military field in the first place and permitted later for civil and commercial use.
- **Commercial**: human interaction with products that has face recognition system could raise their desire to buy such product, taking smart phones as example that has interaction applications face recognition is one of these applications.

- **Smart technologies**: the whole word is directed toward smart phones, smart electronic boards in class room, smart cars, smart, etc., even smart home access person don’t need a key or pin code to get into his house.

4. LITERATURE REVIEW

There is a rapid advancement in the field of recognition and biometric security systems over the years and the research development growth is not slowing down at all. In 1964-1965, Bledsoe, along with Helen Chan and Charles Bisson, made a significant breakthrough when they use computers to recognize human faces [12]. Currently, there are several works and projects in the field of artificial intelligence or biometrics in particular [13] such as the face detection security system used by the German Federal Police Department in Frankfurt Rhein-Main international airport. However, there are still many lingering issues that need to be resolved.

In the Face Recognition System (FRS) domain, various different methods were presented and applied. Principal Component Analysis (PCA) is one of the first successful and strongest approaches in the FRS domain [14]. This method takes a whole image as a vector and uses it to generate statistical information. It combines all image vectors together and forms an image matrix and then eigenvectors of this matrix will be calculated. The face images can then be expressed as a linear solution.

4.1. Principal Component Analysis

Karl Pearson was invented Principal component analysis (PCA) in 1901 [15]. PCA is useful when we obtain data with some redundancy and it can be considered as variable reduction procedure. As the result of that reduction, smaller number of variables which are called Principal Components will be accounted for the most observed variables.

When we hope to carry out recognition in a high-dimensional space, some problems occur. One of the main goals of PCA is to reduce the dimensionality of the data through retaining as much as variation possible in our original data set. Though on the other hand, dimensionality reduction itself involves information loss. However, using best principal component analysis, the best low-dimensional space can be achieved.

One major advantage of using PCA is applying it in Eigenface approach. This will help reducing the complexity and size of the database for recognition of a test images. This technique allows us to store images and their feature vectors in a database and then find out reflecting data for each and every trained image to set of Eigen faces obtained. In summary, in order to reduce the dimensionality of a large data set, PCA is better applied on Eigen face approach.

4.2. Eigen Face Approach

Accoding to Slavkovic and Jevtic (2012), defined Eigenfaces as one of the simplest and most effective approaches used in face recognition system, Eigenface approach transforms faces into a small set of essential characteristics. Eigenfaces also known as trainig set which describes the main component of initial set of face images. In Eigenfaces, recognition of faces is done by processing a new images (test image) in the Eigenface subspace, then the person is classified by comparing its position in Eigenface space with the position of known individuals. The objective of this Eigenface approach in face recognition systems includes simplicity, speed, insensitivity to small faces and gradual changes [16].

Eigenfaces is classified as image base approaches, where its goal to find eigenvectors of covariance matrix of the distribution, the eigenvectors resulted from processing training set of face images into linear subspace with lower dimensional space, whereby the dimensional reduction can be achieved through implementation of PCA concept of face image. Moreover, Eigenfaces doesn't analyze the face feature variation [17].

Reseach conducted by Belhumeur, Hespanha et al (1997), the authors considered Eigenfaces approach as one of the best solutions that have been developed. The authors use dimension reduction approaches by considering each face as a vector in the face space, where vector comparison is much easier and faster than matrices comparison. The training set of face images where every face is represented by two dimensional matrix is now a matrix with every face image is a vector, this vector is the face image after processing to face space [18].

This training set has constraints on the face image must be the same size to be calculated and view the frontal features such as eyes, mouth and nose. These face features are analyzed and transferred into unrelated components known as orthogonal component [19]. Another constraint is lighting where image background is the wall or any object behind the face that affect the recognition, the background must be aware because PCA face recognition is very sensitive to the changes in these factors [20].

It is adequate and efficient method to be used in face recognition due to its simplicity, speed and learning capability. Eigenfaces are a set of Eigen vectors used in the computer vision problem of human face recognition. They refers to an appearance based approach to face recognition that

seeks to capture the variation in a collection of face images and use this information to encode and compare images of individual faces in a significant manner.

The Eigenfaces are Principal Components of a distribution of faces, or equivalently, the Eigen vectors of the covariance matrix of the set of the face images, where an image with N by N pixels is considered a point in N 2 dimensional space. The probability number of Eigenfaces is equal to the number trained set. The faces images can also be approximated using Eigenface. The primary reason for using fewer Eigen faces is computational efficiency.

4.3. Local Binary Patterns Approach

Another successful approach [21] is Local Binary Patterns for facial feature extraction. The LBP operator merges a region in the image and assigns a value as a central pixel. These central pixels are labeled either 0 or 1. If the value is lower or higher than the value assigned to the central pixel, a histogram of the labels is computed and used as a descriptor. The LBP descriptor will be constructed and collected in every region and the results are combined together to create one vector representing the entire face image. For every given pixel, a binary number is obtained by merging all these binary values in a clockwise manner, starting from the top-left neighbor pixel. Example LBP operator actually used a fixed 3 x 3 neighborhood just like this:

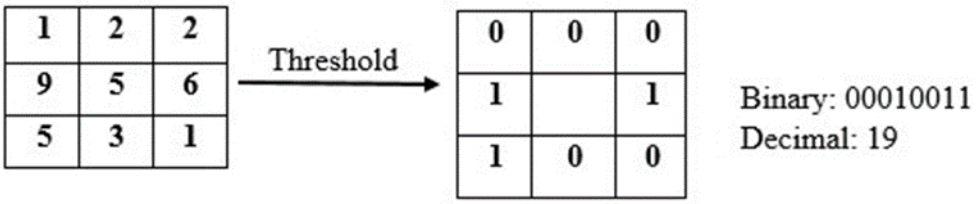


Figure 4.1. LBP operator

Eigenface, and Local Binary Patterns Approach were two most known algorithms used for face recognition and supported also with OpenCV, each algorithm has their own way on how to perform face recognition though it varies on the time execution of performing face recognition but still it gives the right and accurate result.

The following Table 4.1 shows Comparison Eigenface and Local Binary Patterns [22].

Table 4.1. Comparison Eigenface between local binary patterns

Eigenface	**Local Binary Patterns**
• In Eigenface method, we compare all the datasets at the same time • Eigenface use principle component analysis (PCA) technique map image faces. • Feature vectors of Eigenface use linear combinations to represent the face images • Eigenface is easy to code and processing the training set is automatic • Reduce the complexity of face images in terms of statistical representation • Eigenface using to handle large number face databases. • In terms of real time, recognition can easily be achieved	• In LBP, we analyzed each image separately • The LBP images can characterize locally when unknown images provided. • LBP can be uniform if transition is between 0 to 1 at two bitwise high • LBP calculates the pixel of every image • It keeps the occurrence of possible pattern of each images • In LBP, segment the images face into a spatial grid. • In LBP, feature vector a form from histogram of grid square

Table 4.2 matches up to some of the lately used biometric systems, according to the cost, accuracy, required devices and social acceptability. Face recognition is a medium in cost and accuracy but does not require more devices and it is highly accepted by society [23].

Table 4.2. Biometric technology comparison

BİOMETRIC TECHNOLOGY	Accuracy	Cost	Devices Required	Social Acceptability
Face Recognition	Medium-Low	Medium	Camera	High
Voice Recognition	Medium	Medium	Microphone, Telephone	High
Fingerprint	High	Medium	Scanner	Medium
Signature Recognition	Low	Medium	Optic pen , touch panel	High
Hand Geometry	Medium-Low	Low	Scanner	High
Iris Recognition	High	High	Camera	Medium-Low
Retinal scan	High	High	Camera	Low

5. METHOD/APPROACH

5.1. Overall Description

Although Face Recognition Systems are known for decades, there are many well active research works on the topic. These can be divided into two main parts; face detection and recognition of the detected face. So during our research we have found many areas that related to face recognition system; such as processes approaches and algorithms that used in developing of those systems. In developing this feature we will be using the data model diagram to show these processes and stages. This data model diagram will help us in making decision that will give us a good idea to the development stages like locating face in a form of color image, also will help us in retrieval of information as well as storing the record for further usage in time.

5.2. Product Perspective

The real challenge in face detection and recognition technologies is the ability to handle all those difference face that where subjects for trained. In our project first we are going to review the development of face detection and recognition approaches, followed by a review of face modeling and model compression methods. After development of this project, Face Recognition System will able to detected and recognized each difference faces where subject to trained, are show below Figure 5.1.

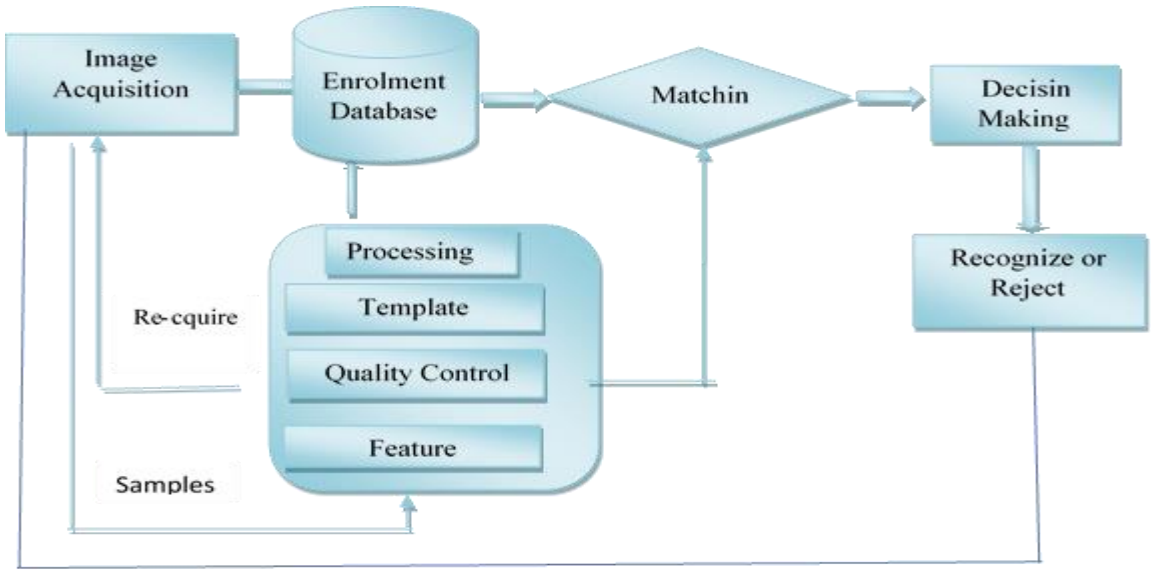


Figure 5.1. Product Perspective of Face Recognition System

5.3. System Interfaces Requirement

During development process, Face Recognition System, face images acquiring depends upon application. For instance, in system applications may function as or served by capturing face images with means of camera also save image into database. After saving image into database, if person detected and recognized by returning known or unknown. So all the process explain how user will interact with the system. In general design and interface requirement specification shall be elaborated based on process are show at below Figure 5.2.

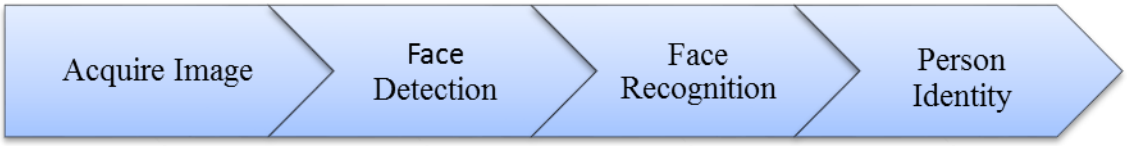


Figure 5.2. Steps of Face Recognition System

5.4. User Interface Requirement Analysis

In Face Recognition System users are able to interact with application after login. User will login using password and username, because the system is planned to provide authentication to the person in charge of system in order to maintain high level security. Then the main interface will display after login, the user will be able to capture image instantly, delete, insert new track image, update an image or update specific record. Also user is able to search all record of a specific person. The below block diagram (Figure 5.3) will show the structure of the system requirement analysis of user interface.

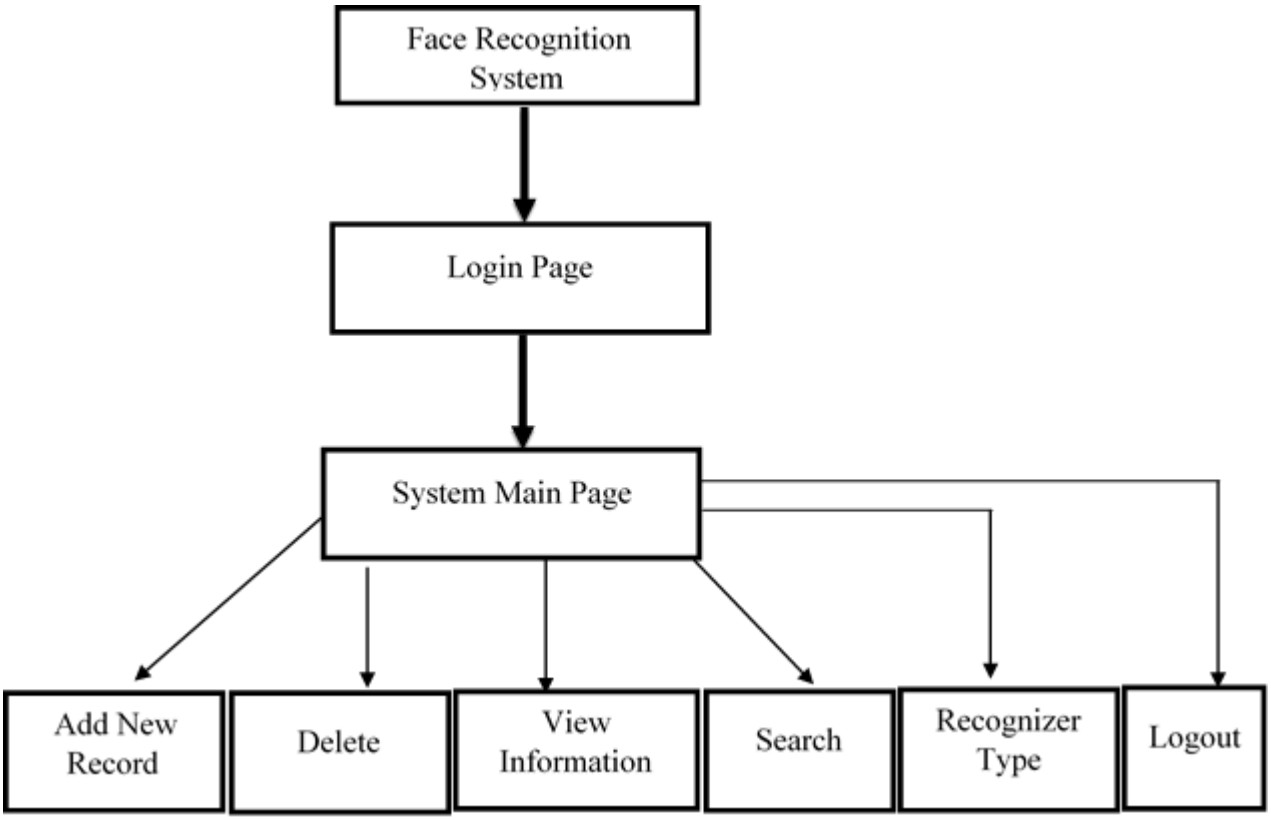


Figure 5.3. System Structure Requirement

Face Recognition System is planned to get the face region particularly, the face region will serve as the input that will be used in matching with other records in the system. The phases in face detection and recognition are as follows: Image captured from the camera, face region detected, searching, matching display and updating the particular image or saving the new record. All this explain the different steps of an image face detection process. The below activity in (Figure 5.4) diagram explain more about it.

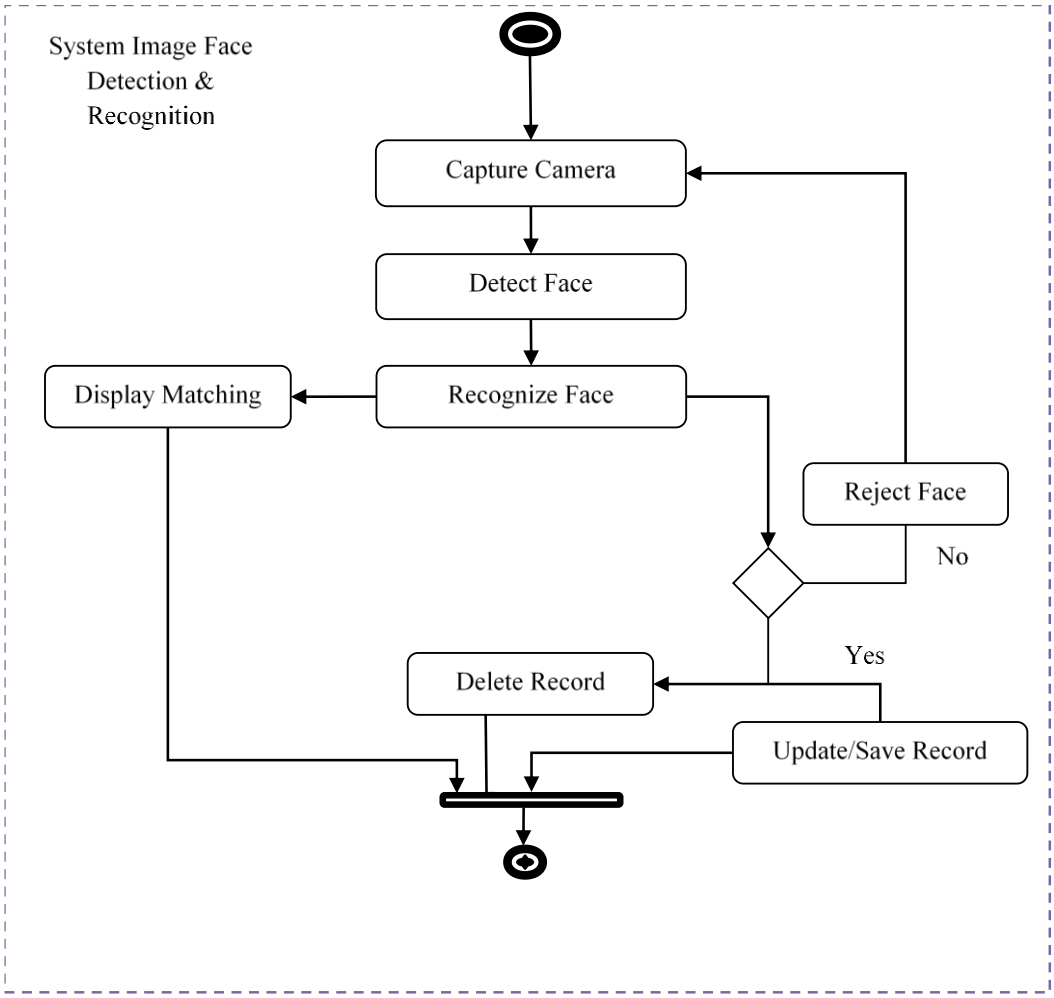


Figure 5.4. Activity Diagram of Face Recognition System

5.5. Hardware Interfaces

The system hardware interfaces is one of the most essential issue in this planned work or project, because capturing image has the priority in all the stages, so external Camera/Webcam is required in the process. Record will be inputted with the help of mouse, keyboard and the output result will be obtain from the screen display image and even speakers might be used to make it more user friendly by producing a sound that shows valid or invalid activity. Some of hardware interfaces.

a) A personal computer with 6GB RAM running on Intel Core i-5.
b) CPU speed of 2.40GHz,
c) 500GB of harddisk space were used to experiment and test the program.
d) Accessories: WebCam, Keyboard & Mouse.

5.6. Software Requirements

- Operating system: Microsoft Windows 10.
- Programming Language : Visual Studio 2012 with C#
- Library Emgu Cv, Open Cv
- Database : Microsoft Access 2013

5.7. Software Interface

This application is Windows based application that runs on laptops, desktop computers, and the developed software will be used or run on all the major operating systems like Windows, Mac system or UNIX. This application will have access to camera that connected to the system for image processing. The database structure of this application is one of the most important parts after the camera, because there will be track of records and all the details and even the images will be kept in the database. The added records might be updated, deleted or searched using DBMS.

6. SYSTEM DESIGN & DEVELOPMENT

This chapter elaborates the development and result of the study “Camera – Image based: Real Time Face Recognition System. It discussed how the proposed method used to perform an efficient technique in detecting and recognizing images and recording automatically the presence of an individual as their attendance upon entering the Database Library.

6.1. Design Constraints

When preparing a prototype of this application a laptop will be used and webcam of the laptop will be the only camera in the development process, in later stages external camera will be installed and fix in the system. Established tests of system for personal computers will be more comprehensive in later stages. Currently the system will save the snapshot, which will be used to match the images in the system database at the beginning. Person standing before entering the system as the security personal while adding or deleting record will have to provide his own unique ID and password in order to avoid of tempering of these system illegally.

6.2. Quality Features

When we evaluate various aspects of the proposed system we are developing its properties are useful in several areas. Aspects of usability, users will be prepared for the various system-related training images, such systems are much more advantageous because institutions that use this software will be give services and maintenance. Also, provided Face Recognition System has the following quality such as reliability, availability, security, maintainability and portability.

6.3. Login Screen Image

The aim of face recognition system is to maintain security. Therefore, users must login to the system. To do that, one of the most important issues is the simplicity of the user interface of the system. Transitions between menus have to be easy in order to increase functionality in specific situations. Figure 6.1 show the login screen that any user must login before he/she accesses the system.

Figure 6.1. User Login Interface Screen

When the user enters the credentials i.e. username and password and clicks on login button then the entered username and password will be checked from the database and if matches then the login attempt will be successful. Otherwise, user will get a message e.g. "Wrong Username/Password" or "Login Failed...Try again!" if you are not registered before into database you have to into register and click signup.

In a situation where a user forgets his or her password the user need to click the “forget password” button.

Sign Up: Initially the security officer or administrator is in charge to register his or her record into the systems. Figure 6.2 shows the button to click and the required information for the new user registration.

The user needs to use his registered email, so that an email that contains his/her password will be sent to him/her.

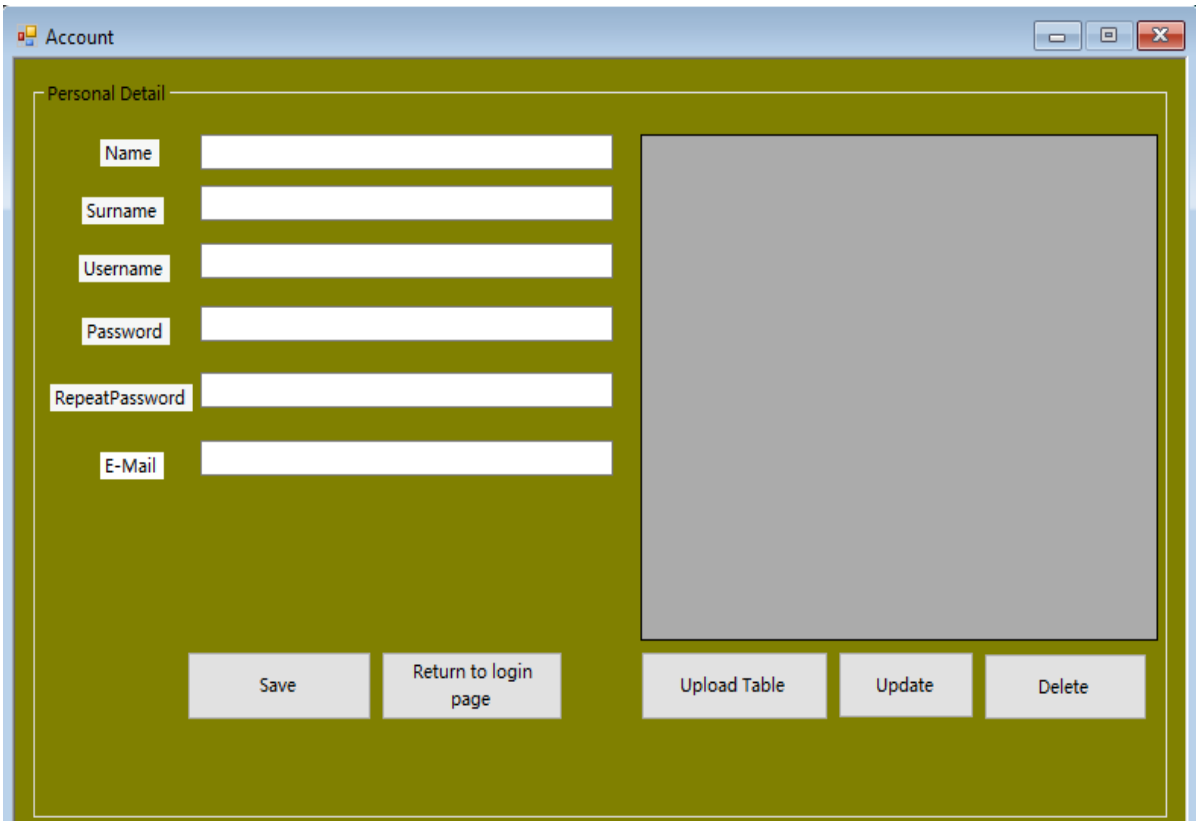


Figure 6.2. User Create new Account Interface Screen

User will fill up the registration form with details such as FirsName, LastName UserName, Password, Repeat Password, email address, etc. and these details will be saved in the database table.

6.4. Main Menu

The System is responsible for detecting and validating of user's face. This component is also responsible for sending appropriate signal to interface module. Furthermore, it must have high success rate and it sends false signal when face of stranger is appeared from camera.

After a successful login, the main menu screen will appear for face detection and face recognition. Here, the user can select the appropriate menu by clicking of the corresponding menu option. In main interface, user can add a new record, delete an existed one, search or view information etc. as the screen of Figure 6.3 shows.

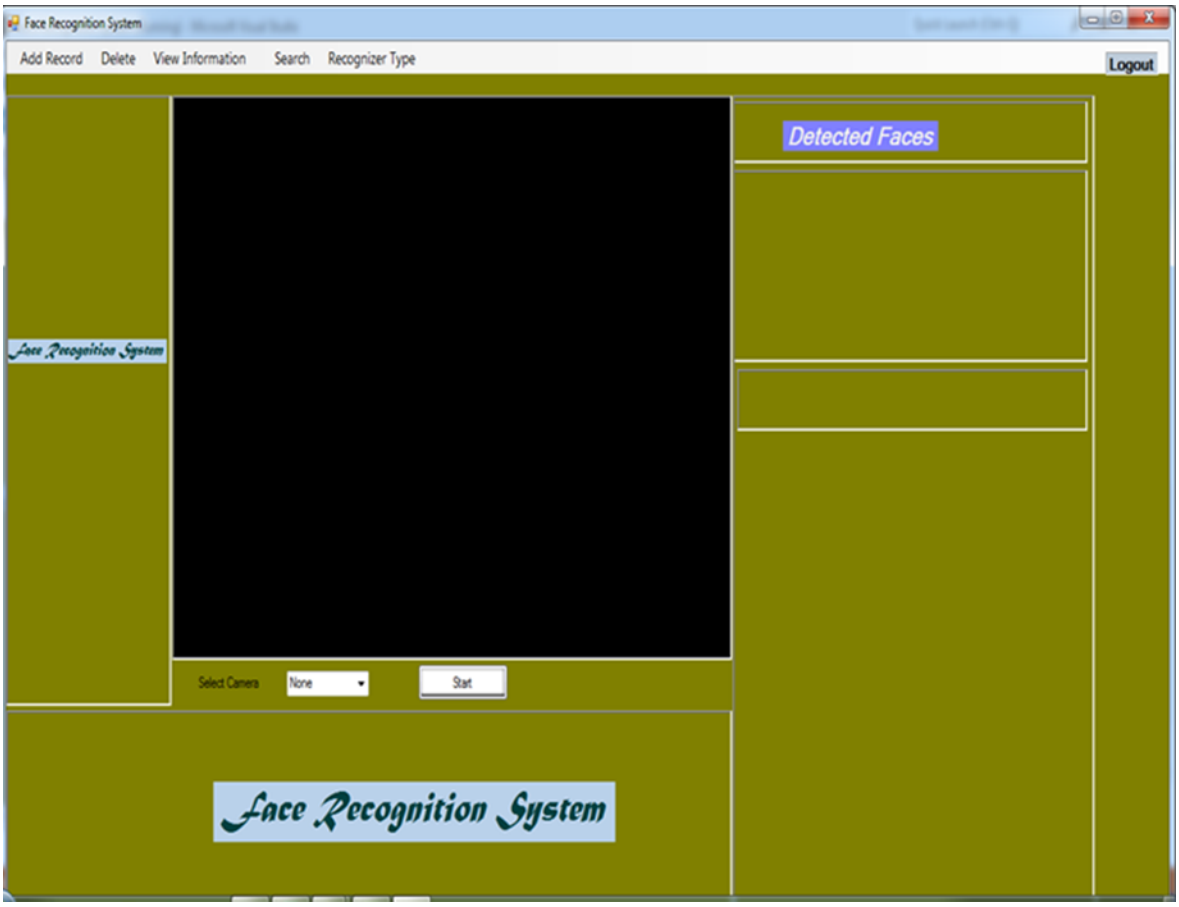


Figure 6.3. User Main Interface Screen

The Face Recognition System interface shown above is the main page that will open after successfully login into the system. Here, the user needs to press the "Start" button to enable the program start.

6.5. Capturing Images

To acquire face images from any person, the (USB) camera or webcam is used. The USB camera was used to continuously capture the person as they enter into the room. In capturing process, the person should be frontal to the camera (within 1 to 3 feet or one meter distance for better result), since the system could only identify the face image frontally.

6.6. Training Process

The system could only recognize the person once it was already trained. Training process is the first step of the system. To obtain training image, the person should face in front of the camera within a limited distance (1 to 3 feet from the camera) to have a good result and then image of the

person is captured. Figure 6.4 shows how to train the image of the person in the system. It also shows how to add new training record to the system and data that must be identify the image which includes name, surname, face features, and etc. This information will be used for future recognition purpose.

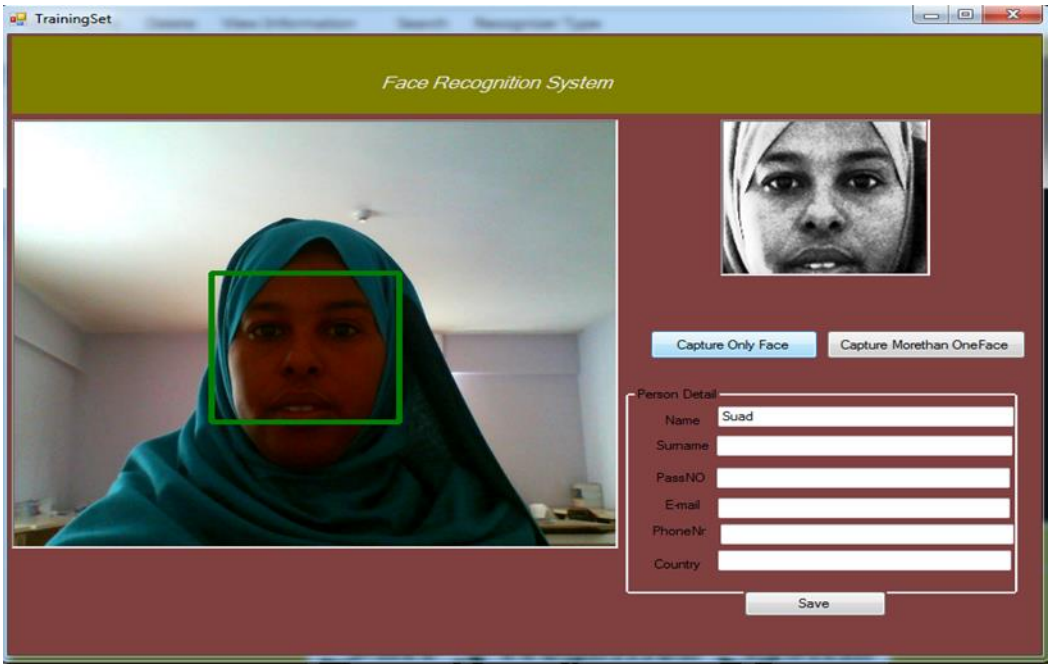


Figure 6.4. Training Process

All trained images should have corresponding information saved into the database, since this information was used by the system in recognition process. The information must be composed of Identification number (FaceId), Name, Surname, Phone Number, Counrty, Passport Number, and Email. The trained face images should be saved into the folder name “TrainedFaces”. We used different images from different persons in training process, each image contained an identification number of person. The Identification number was then used to retrieve the personal information saved in the database. Figure 6.5 shows some trained images of selected individuals.

Figure 6.5. Trained Images

6.7. Face Detection

Using preprocessing technique, the image became equal in intensity and more noticeable. The EmguCV that is used for detecting the human faces from captured image called Haar Cascade Classifier also known as the Viola-Jones Method [24]. Using the Voila – Jones Algorithm the system could easily detect the face images from a captured device.

The first option on the main menu is the Face Detection. This part of the application is able to find faces in real-time images from a camera. The detection of faces is done automatically. When the detection occurs, a green rectangle appears on the windows surrounding the face as shown in Figure 6.6.

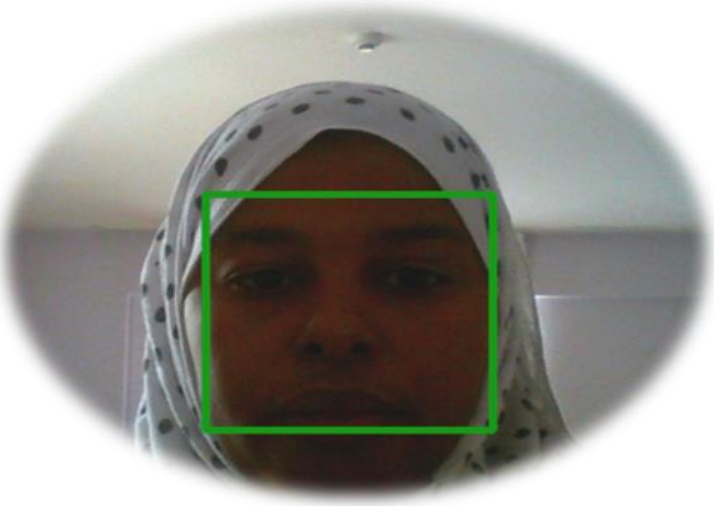


Figure 6.6. Face Detection

6.8. Face Recognition

After person's face image is detected, next step of the process which is face recognition will be executed. The recognition process compares the geometrical features of detected face to facial images already stored in a database. If stored and detected features match to each other, the face would be recognized and the information of that person will be displayed back to the screen.

In this final step maybe we can have different purposes, whether it is identification or verification. As we mentioned in the previous sections, if identification takes place the image will be compared with all images in a database. If verification takes place, the image will be compared one to one into the database.

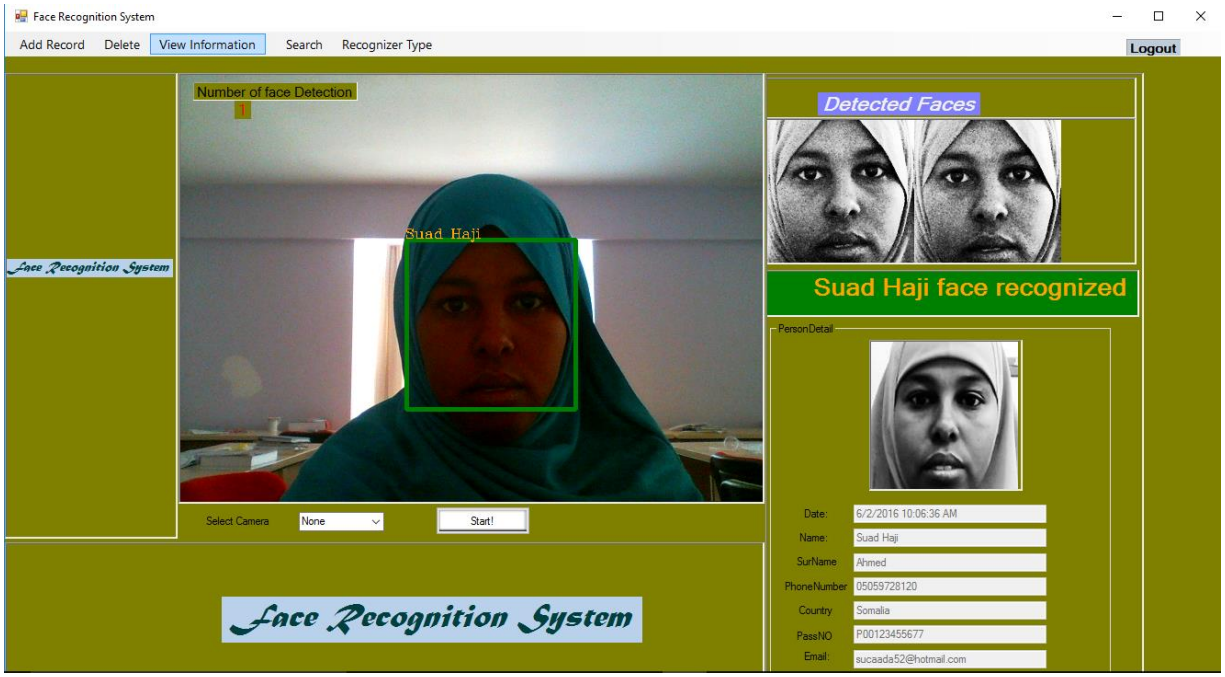


Figure 6.7. Face Recognition

Lastly, the image in Figure 6.8 shows how to search using by name, here the system takes a name to search. The system will return the details that has been saved if the name search is registered. However, the system will return nothing if the search name is not in the system's database.

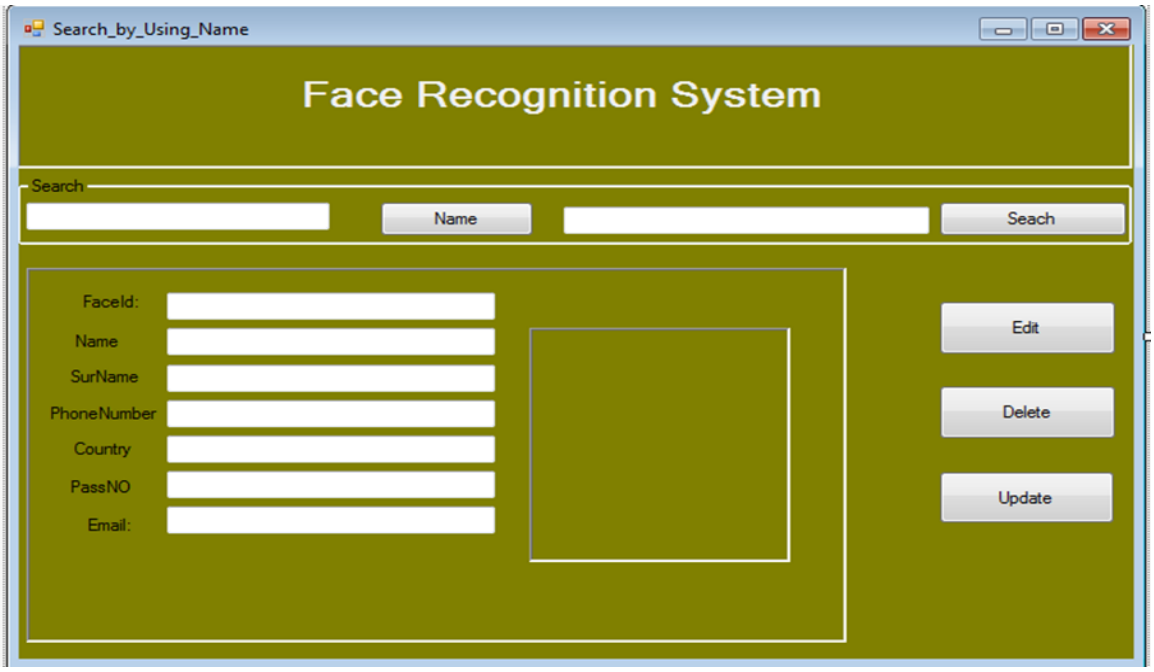


Figure 6.8. User Search Using by Name

6.9. Screen Object and Action

The main function of face base recognition security is to recognize the face, if the user login is able to keep tracking of face and save their record in the database. The user is able to delete, add new detected face, search, view information and edit record inside of the system.

6.10. Database Development

We used the following tools in developing a system which were: EmguCv 2.4.10.1940 version (a wrapper for Intel's open source OpenCV Library for computer vision), Microsoft Visual Studio Ultimate 2012, MS Access 2013 served as database, C/C# as Programming languages, and Universal Serial Bus (USB) camera for acquiring face images.

6.11. Test

The main purpose of the test report for the Face Recognition System is to discuss the testing details such as editing record, adding record, deleting record, searching record and etc. The software project test report also describes the objective, scope and approach of the software testing effort for the Face Recognition System project. The test report for the Face Recognition System also indicates the personnel responsibility for each task and also specifies the risks associated with the test report.

6.11.1. Test Items

- Registration
- Login (authentication)
- Extraction of quality image for training the system.
- Known Person
- Unknown Person

6.11.2. Unit Testing

Unit testing is the section that tests the programs to check for errors in all the code. The main aim of this part of the test is to detect any error in the Face Recognition System source code. All the classes, windows forms, functions will be tested to make sure that they reach all the expectations, like Training the system, Detection, Recognition and Taking records. Among the benefits of Unit Testing:

- Easy to modify code.

- Allow testing in bottom up fashion or approach.

One of the disadvantages of Unit Testing is that it might not identify each person properly.

6.11.3. Integration Testing

The aim of Integration Testing is to make sure that after Unit Testing all the units will be collected and integrated to make one single system or application (Face Recognition System), after that it will be tested to make sure that it performs all the functionalities and performance that is expected.

6.11.4. Acceptance Testing

This testing is generally performed when the Face Recognition System is nearing its end. This test mainly qualifies the Face Recognition Based Security System and decides if it will be welcome by the clients. The users or customers of the Face Recognition Based Security System are responsible for the Acceptance Testing.

6.11.5. System Testing

One of the most important test sections is the System Testing; the whole integrated system will be tested to make sure that all the functionalities and the requirements that were described in the requirement report and design report.

6.11.6. Test Case 1 – User Login

Table 6.1 describes how a user logging to the system based on user login authentication. In face based recognition security each user has an account and a corresponding ID in the database. Users are able to login the system based on the login authentication that analyzes and determines users ID as well as his permissions to the system.

Table 6.1 shows how the system can allow a user to login if the user uses the correct login data and the table also explains how the system deny access if the login details are wrong.

Table 6.1. User Login Test Table

Incorrect Input	Pass Criteria	Correct Input	Pass Criteria
Users input incorrect UserName, passport.	An invalid message will appear to show that an invalid username has been used.	The correct input for login to the system is username and password	The users are able to access the main page.

6.11.7. Test Case 2 – User Registration

In Face Recognition System the users are able to get access to the system if the users have accounts. Before accessing into the system user must register with correct information. Registration standards for evaluating the significance properties are given in Table 6.2.

Table 6.2. User Registration Test Table

Incorrect Input	Pass Criteria	Correct Input	Pass Criteria
Interring incorrect format in registration page. For example, typing email address in the field of user name and vice versa.	Immediate message will appear to indicate wrong format.	Entering correct format in user registration page.	The pass criteria for this user will successfully complete. The user will be able to login and get access to the system.

6.11.8. Test Case 3 – User Registration

This section covers how the user left an empty field in the registration page which the user must fill all the required information before registration successfully. Table 6.3 illustrates the criteria of leaving empty space in user registration field.

Table 6.3. User Registration Test Table

Incorrect Input	Pass Criteria	Correct Input	Pass Criteria
User left empty field in the new user registration page or user inter no recognizer character.	Immediately the message will be showed in the empty space.	In correct input the user must not leave any empty space and must fill all the required.	The user will be registered successfully. The system will detect all user details and also user will be able to login into the system.

6.11.9. Test Case 4 – Search

Table 6.4 illustrates how the user is able to search in the system. Searching means to look for something in a list or an array where you search the list from beginning to end, however in searching the user must follow some criteria in order to get correct results.

Table 6.4. Search Record Test Table

Incorrect Input	Pass Criteria	Correct Input	Pass Criteria
Incorrect input in this test case. User searches username. In Face Recognition System user is able to search using by name.	Message will be appeared to indicate that user makes wrong entering in the field.	User searches using by name, the user enters correct format.	Results of searching will show that the user enters correctly.

6.11.10. Test Case 5–Add New Detected Face

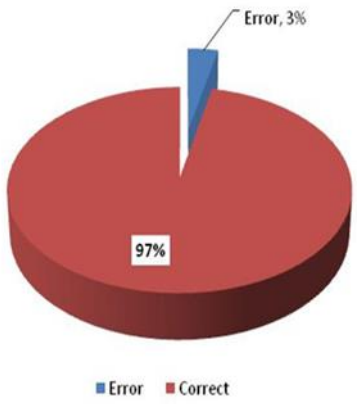
In face based recognition system the user is able to add detected face into the database and the Error should be handled when adding the detected face by entering the correct detail of detected face and without leaving empty field. As long as a person was in the camera's view, his face would be accurately detected and tracked and if it's new face, this new face will appear immediately on the screen. Table 6.5 shows the test case of adding new face.

Table 6.5. Add New Detected Face Test Table

Incorrect Input	**Pass Criteria**	**Correct Input**	**Pass Criteria**
In incorrect input, user must not leave empty field.	Message will appear immediately if the uses left any empty field.	In correct input, user must fill all the field.	In pass criteria, user will add new face successfully.

7. RESULTS AND CONCLUSION

In general, the developed application of FRS works fine, it shows accuracy (recognition ability) of more than 97% under the normal conditions such as light, distance from camera, same camera (for training and recognition). However, if the distance from detection and recognition camera is different or the types of the cameras are not the same, the recognition capability of the system is reduced to 90%. The Figure 7.1 and Figure 7.2 show graphical explanation of the results.



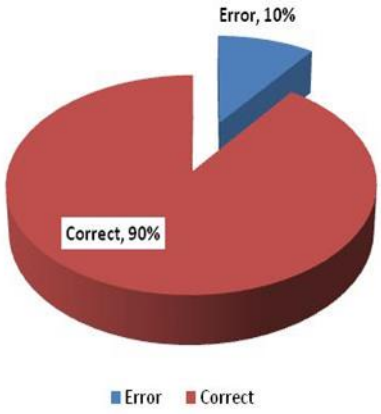


Figure 7.1. Accuracy ratio under inconvenient conditions **Figure 7.2.** Accuracy rate under normal conditions

From the result, it is easy to see that if the recognition constraints are fulfilled there is no any reason for the application (FRS) to fail to recognize a person as know or unknown person. However, even a slight change in the described constraints such as light, camera type and image distance the application's accuracy can be negatively affected.

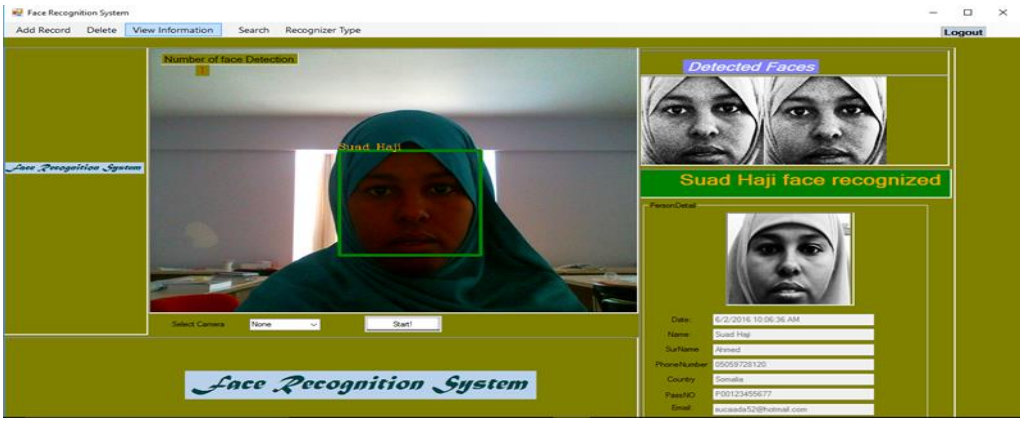


Figure 7.3. Recognized Test Images Taken From Webcam

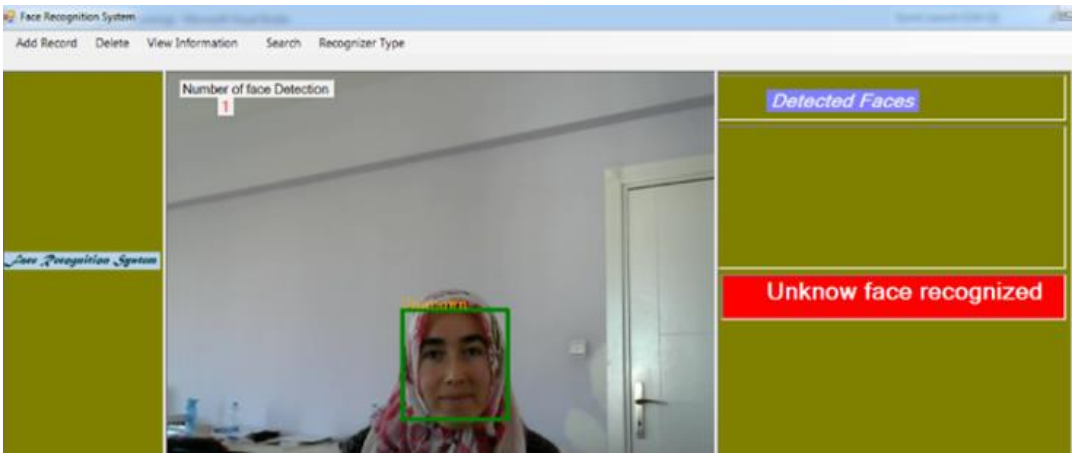


Figure 7.4. Unknown Face

In conclusion, the developed face recognition based security system described in this thesis can be used to maintain security in an organization, schools and general public with the help of cameras. EmguCV library with C# programming language were used in developing the application. The FRS collects a number of images for each and every individuals to be used as training sets; so that in the future, if that particular person appears this system will detect and recognize him/her. If person's record is not added into the system, that particular person will be classified as an unknown person. Eigen Faces and LBP were the algorithms used in the recognition process, both Eigen Faces and LBP yielded excellent results. Furthermore, if there is frequent change in the lighting conditions, LBP seems to be the better choice.

Based on the results, the developed FRS application performs satisfactorily, with an accuracy rate (recognition ability) of more than 97% under conducive conditions such as good lighting ambience, sufficient distance from the camera, using the same camera for training and recognition, and etc. However the accuracy is reduced if any of these environment conditions is partially met. Figure 7.1 and Figure 7.2 shows graphical explanation of the results, where Figure 7.3 and Figure 7.4 shows different dialog boxes of the system.

Project Source Code:

Connection to Database

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <startup>

    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5"/>
  </startup>
  <connectionStrings>

   <add name="Connet" connectionString="Data
Source=(LocalDB)\v11.0;AttachDbFilename=|DataDirectory|\Userdatabase.mdf;"
providerName="System.Data.SqlClient"/>
  </connectionStrings>
</configuration>
```

A. User Login Code.

```
private void btn_login_Click(object sender, EventArgs e)
      {
         if (textBox1.Text == "")
         {
            MessageBox.Show("Please enter user name", "Error", MessageBoxButtons.OK,
MessageBoxIcon.Error);
            textBox1.Focus();
            return;
         }
         if (textBox1.Text == "")
         {
            MessageBox.Show("Please enter password", "Error", MessageBoxButtons.OK,
MessageBoxIcon.Error);
            textBox2.Focus();
            return;
         }
         try
         {
            SqlConnection myConnection = default(SqlConnection);
            myConnection = new SqlConnection(FR);

            SqlCommand myCommand = default(SqlCommand);

            myCommand = new SqlCommand("SELECT UserName,Password FROM
AccountTable WHERE UserName = @UserName AND Password = @Password",
myConnection);

            SqlParameter Name = new SqlParameter("@Username", SqlDbType.VarChar);
```

```
            SqlParameter Password = new SqlParameter("@Password", SqlDbType.VarChar);

            Name.Value = textBox1.Text;
            Password.Value = textBox2.Text;

            myCommand.Parameters.Add(Name);
            myCommand.Parameters.Add(Password);

            myCommand.Connection.Open();

            SqlDataReader myReader =
myCommand.ExecuteReader(CommandBehavior.CloseConnection);

            if (myReader.Read() == true)
            {
               MessageBox.Show("You have logged in successfully " + textBox1.Text);
               //Hide the login form
               this.Hide();
               Form1 f2 = new Form1();
               f2.ShowDialog();
            }
            else
            {
               MessageBox.Show("Login Failed...Try again !", "Login Denied",
MessageBoxButtons.OK, MessageBoxIcon.Error);

               textBox1.Clear();
               textBox2.Clear();
               textBox1.Focus();
            }
            if (myConnection.State == ConnectionState.Open)
            {
               myConnection.Dispose();
            }
         }
         catch (Exception ex)
         {
            MessageBox.Show(ex.Message, "Error", MessageBoxButtons.OK,
MessageBoxIcon.Error);

         }
      }
```

B. Start Camera Connection Code:

```
private void btnStart_Click(object sender, EventArgs e)
      {
          if (capture == null)
```

```
        {
            try
            {
                capture = new Capture();
            }
            catch (NullReferenceException excpt)
            {
                MessageBox.Show(excpt.Message);
            }
        }
        if (capture != null)
        {
            if (captureInProgress)
            {
                btnStart.Text = "Start!";
                Application.Idle -= ProcessFrame;
                DetectFaces();
            }
            else
            {

                btnStart.Text = "Stop";
                Application.Idle += ProcessFrame;
                DetectFaces();
            }
            captureInProgress = !captureInProgress;
            DetectFaces();
        }
    }
```

E. Detection and Recognition Code:

```
private void DetectFaces()
    {
        using (Image<Bgr, byte> nextFrame = capture.QueryFrame())
        {
            if (nextFrame != null)
            {

                Image<Gray, byte> grayframe = nextFrame.Convert<Gray, byte>();
                MCvAvgComp[][] facesDetected =
                    grayframe.DetectHaarCascade(
                        haar, 1.2, 3,
                        HAAR_DETECTION_TYPE.DO_CANNY_PRUNING,
                        new Size(60, 60)
                        );
                foreach (MCvAvgComp f in facesDetected[0])
                {
```

```
                result = nextFrame.Copy(f.rect).Convert<Gray, byte>().Resize(160, 160,
Emgu.CV.CvEnum.INTER.CV_INTER_CUBIC);
                result._EqualizeHist();
                nextFrame.Draw(f.rect, new Bgr(Color.Green), 4);
                if (EigenRecog.IsTrained)
                {
                   string name = EigenRecog.Recognise(result);
                   //Draw the label for each face detected and recognized
                   nextFrame.Draw(name, ref font, new Point(f.rect.X - 2, f.rect.Y - 2), new
Bgr(Color.Orange));

                   //nextFrame.Draw(f.rect, new Bgr(Color.Orange), 3);

                   labelandimageaddedtopenal(result, name);
                   textBox1.Text = name;
                   label12.Text = facesDetected[0].Length.ToString();
                   label12.Visible = true;
                   label13.Visible = true;
                   //if (name == " Unknown ")
                   //{
                   //    nextFrame.Draw(f.rect, new Bgr(Color.Orange), 3);
                   //}
                   //else {
                   //    nextFrame.Draw(f.rect, new Bgr(Color.Red), 3);
                   //}

                   //string recorgnizedface = "face Recognized";
                   //string recorgnizedname2 = "Unknow face Recognized";
                   if (textBox1.Text == "Unknown")
                   {

                      //label11.Font = 12;
                      label11.Text = "Unknow face recognized";
                      label11.ForeColor = Color.White;
                      label11.Visible = true;
                      panel6.BackColor = Color.Red;


                   }
                   else
                   {
                      label11.ForeColor = Color.Orange;
                      label11.Text = textBox1.Text + " " + "face recognized";
                      label11.Visible = true;
                      panel6.BackColor = Color.Green;
                   }
                }
```

```
            }
            CamImageBox.Image = nextFrame;
        }
    }
}
```

REFERENCES

[1] **Zhao, W., Chellappa R, . Phillips PJ and Rosenfeld A,** 2003. Face recognition: A literature survey, *ACM Comput. Survey,* cilt 35, no. 4, pp. 1-61.

[2] **Shah, D. H, Shah, T. V. and Shah, J. S.,** 2015 Recognition and Authentication by Biometric Techniques, *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering,* cilt 3, no. 8, p. 2015, 1-4.

[3] **GAO-15-621 Report,** 2015 Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law, United States, 2015.

[4] **Computer Vision,** 2016 https://en.wikipedia.org/wiki/Computer vision Last Accessed data: May 30, 2016.

[5] **Anot, N. and Singh, K., . K.,** 2016 A Review on Biometrics and Face Recognition Techniques, *International Journal of Advanced Research,* cilt 4, no. 5, pp. 1-4, 2016.

[6] **Eze, A. O. and Gozie, I.,** 2013 Facial Verification Technology for Use In Atm Transactions, *American Journal of Engineering Research (AJER),* cilt 02, no. 05, pp. 1-6, 2013.

[7] **Hobbing, P. and Koslowski , R.,** 2009 A Comparıson of Border Securıty Systems in The EU and in The US, Under the coordination of the Justice and Home Affairs Section of the Centre for European Policy Studies (CEPS), 2009.

[8] **Schwartz, W. R., Guo , H. and Davis, L. S.,** 2010 A Robust and Scalable Approach to Face Identification, *Computer Vision – ECCV 2010,* cilt 6316, no. 2010, pp. 1-14, 2010.

[9] **Jafri .R. and Arabnia, H. R.,** 2009 "A Survey of Face Recognition Techniques," *Journal of Information Processing Systems,* cilt 5, no. 2, pp. 1-28, 2009.

[10] **Babich, A.,** 2012 Biometric Authentication. Types of biometric identifiers, 2012, pp. 1-56.

[11] **Gaur, S., Shah .V. A. and Thakker, M.,** 2012 Biometric Recognition Techniques: A Review, *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering,* cilt 1, no. 4, pp. 1-9, 2012.

[12] **Thakur, A. S. and Rai, M.,** 2016 Automatic Multiple Face Recognition and Annotation Based on Principle Component Analysis cum Least Mean Square Error (PLMSE), *International Journal of Innovative Research in Science, Engineering and Technology,* cilt 5, no. 4, pp. 1-13, 2016.

[13] **Kumar, A. and Bansal, M.,** 2015 Facial and Voice Recognition System using Biometrics Techniques, *IJIRST –International Journal for Innovative Research in Science & Technology,* cilt 2, no. 03, pp. 1-4, 2015.

[14] **Shinde, A. A. and Ruikar, D. S.,** 2013 Face Recognition using PCA and Eigen Face Approach, *International Conference on Recent Trends in engineering & Technology - 2013(ICRTET'2013),* India, 2013.

[15] **Kochar, B., Saggar .S. and Gupta, N.,** 2011 Designing Facial Recognition System Using Combo Approach, *Proceedings of the 5th National Conference; INDIACom-2011 Computing For Nation Development, March 10 – 11, 2011 Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi*, New Delhi, 2011.

[16] **Paul, C. L. and Sumam, A. A.,** 2012 Face Recognition Using Principal Component Analysis Method, *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* cilt 1, no. 9, pp. 1-5, 2012.

[17] **Imran ,A. M., Miah, U. S. and Rahman, H.,** 2015 Face Recognition using Eigenfaces *International Journal of Computer Applications (0975 – 8887),* cilt 118, pp. 1-5, 2015.

[18] **Gupta, K. R. and Sahu, K., U.,** 2013 Real Time Face Recognition under Different Conditions, *International Journal of Advanced Research in Computer Science and Software Engineering,* cilt 3, no. 1, pp. 1-8, 2013.

[19] **Arora, K.,** 2012 Real Time Application of Face Recognition Concept, *International Journal of Soft Computing and Engineering (IJSCE),* cilt 2, no. 5, pp. 1-6, 2012.

[20] **Kumar,S. K., Prasad. S., Semwal .B. V. and Tripathi .C. R.,** 2011 Real Tıme Face Recognıtıon Usıng Adaboost Improved Fast Pca Algorıthm, *International Journal of Artificial Intelligence & Applications (IJAIA),* cilt 2, no. 3, pp. 1-14, 2011.

[21] **Ghatge, S., S. and Dixit ,V. P. V.,** 2013 Face Recognition under varying illumination with Local binary pattern, *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering,* cilt 2, no. 2, pp. 1-8, 2013.

[22] **Alam, S.,** 2013 Design of Face Recognition System Design of Face Recognition System Design of Face Recognition System, *2013 IEEE 3rd International Conference on System Engineering and Technology*, Malaysia, 2013.

[23] **Tripathi, K., P.,** 2011 A Comparative Study of Biometric Technologies with Reference to Human Interface, *International Journal of Computer Applications,* cilt 14, no. 5, pp. 1-6, 2011.

[24] **Lumbay, R., P.,** 2015 Video – Image Based: Face Recognition for Automated Attendance System in Caraga State University Library,pp. 1-80, 2015.

CURRICULUM VITAE

Suad Haji Ahmed was born in 1988 at Beledweyne, Somalia. She completed bachelor's degree in Information Technology (IT) at Somali Institute of Management & Administration Development (SIMAD) in 2008-2011. She has been working at Simad University as an administrative staff from 2012 till date. She has been a Master Student at Software Engineering Department of Firat University. She is married with two daughters.