UNIVERSITY of RWANDA

DEPARTMENT OF COMPUTER SCIENCE

MUSANZE CAMPUS

COLLEGE OF SCIENCE AND TECHNOLOGY

SCHOOL OF ICT

PROJECT REPORT:

CRIMINAL INVESTIGATION USING FACE RECOGNITION BASED ON DEEP LEARNING ALGORITHMS

Submitted by:

MUROKOZI Jackson: 219006818

BYIRINGIRO Bertin: 219000535

KASINE Peninah: 219003832

Under supervision of:

Mr. BIZIMUNGU Theogene

Submitted in partial fulfillment of the requirements for the award of

BACHELOR OF SCIENCE DEGREE IN INFORMATION SECURITY.

January 2023

CERTIFICATION

This is to certify that the Project Work entitled, **"CRIMINAL INVESTIGATION USING FACE RECOGNITION BASE ON DEEP LEARNING ALGORITHMS"** *is a record of the original bona fide work done by* **Mr. *MUROKOZI Jackson Reg. No 219006818,* Mr. *BYIRINGIRO Bertin Reg. No* 219000535, and Ms. *KASINE Peninah Reg. No* 219003832** *in partial fulfillment of the requirement for the award of Bachelor Degree in Computer science with an option of information security in UNIVERSITY OF RWANDA, COLLEGE OF SCIENCE AND TECHNOLOGY during the Academic Year 2021-2022.*

Supervisor **Mr. BIZIMUNGU Theogene**

Signature: Date: --/--/2023

Head of Department of Computer Science Mr. MURANGIRA Theoneste

Signature……Date: ……. /……./……..

DECLARATION

We do hereby declare that the project work " **CRIMINAL INVESTIGATION USING FACE RECOGNITION BASE ON DEEP LEARNING ALGORITHMS** " submitted in partial fulfillment of the requirements for the bachelor degree in computer science with options information security conducted under the guidance of **Mr. BIZIMUNGU Theogene**, is the record of our own work and has never been presented or submitted for any academic award in any University or Institution as a whole or in part.

Declared By

MUROKOZI Jackson …….....

BYIRINGIRO Bertin .....

KASINE Peninah …….....

University of Rwanda -CST

Date…… /……../…..... And Signature……

DEDICATION

We dedicate this work to:

- The Almighty God,
- Our families,
- Our friends and colleagues,
- Rwanda National Police,
- University of Rwanda,
- Our Lecturers,
- Our supervisor

ABSTRACT

Our project aims to improve the efficiency and effectiveness of criminal investigations by utilizing state-of-the-art face recognition technology. We have developed an Android-based system that utilizes CCTV cameras installed in public areas to continuously capture and analyze images of individuals in real-time. The system employs deep learning algorithms to perform facial recognition, which are trained using a large dataset of criminal photos and faces collected and accessible at the Rwanda Investigation Bureau (RIB).

The system is designed to improve the current process of criminal identification by automating the facial recognition process and providing swift and targeted response. It can identify criminals by comparing the image captured by CCTV cameras with the criminal data in the database in real-time, even if the person is wearing a mask, or the lighting conditions are poor. If a match is found, the system sends an alert to the RIB and police agents, displaying the identified person's image, name and other details on the admin's screen.

Additionally, our system also includes additional security measures such as access controls, encryption of data and logging of every action taken on the system which guarantees the protection of individuals' privacy rights and ensures compliance with the regulations and laws that protect citizens' rights and privacy. Our system is not only beneficial for criminal investigations but also for other areas such as identification of missing person, crowd management and surveillance.

Our system is an innovative solution that utilizes the unique characteristics of a person's face to assist in the identification and detection of criminals, and ultimately aims to enhance the current system of criminal identification and improve its efficiency and effectiveness.

TABLE OF CONTENT

CERTIFICATION i

DECLARATION ii

DEDICATION iii

ABSTRACT iv

LIST OF FIGURES viii

LIST OF ABBREVIATIONS AND ACRONYMS x

CHAPTER 1: GENERAL INTRODUCTION 1

1.1 Introduction 1

1.2 Problem Statement 2

1.3 Objective of the Study 2

1.3.1 General Objectives 2

1.3.2 Specific objectives 2

1.4 General Interests 3

1.5 Scope and Limitations of the System 3

1.6 Technologies 4

1.7 Organization of the report 5

1.8 Project Gantt Chart 6

CHAPTER 2: LITERATURE REVIEW 7

2.1 Introduction 7

2.2 Definition of Terminologies 7

2.2.1 Criminal 7

2.2.2 Face Recognition 7

2.2.3 Open-CV 7

2.2.4 Convolution Neural Network 8

2.3 Related studies 8

2.4 Computer Vision Algorithms used 8
2.4.1 CNN Algorithm 8
2.4.2 TensorFlow 10
2.4.3 Eigen faces Approach using PCA Algorithm 10
CHAPTER 3: RESEARCH METHODOLOGY 12
3.1 Introduction 12
3.2 Methodological Approach 12
3.2.1 Documentation method 12
3.2.2 Observation method 13
3.3 Requirement Analysis 14
3.4 Class diagram 16
3.4.1 Symbol Used for Class diagram 16
3.5 Sequence Diagram 19
3.6 System Requirements 19
3.6.1 Hardware requirements 19
3.6.2 Software requirements and development tools 20
CHAPTER 4: ANALYSING, DESIGN, AND IMPLEMENTATION OF THE PROJECT 21
4.1 Introduction 21
4.2 Existing System 21
4.3 Proposed System 22
4.4 Entity relationship diagram 23
4.5 Database schema 24
4.6 System Analysis 24
4.7 Working Principle of the System 25
4.8 System Implementation 27
4.8.1 Overview of system interface for CCTV Camera application 27
4.8.2 Overview of system interface for agent's android mobile application 31

4.8.3 Overview of system interface for admin's website dashboard 35

CHAPTER 5: CONCLUSION & RECOMMENDATION 44

5.1 Conclusion 44

5.2 Recommendation 44

REFERENCES 46

LIST OF FIGURES

Figure 1: Types of Identification system 1
Figure 2: Gantt chart 6
Figure 3: CNN - Convolutional neural networks 9
Figure 4: Face Recognition Using Eigenfaces 10
Figure 5: Waterfall model 15
Figure 6: Use Case diagram 18
Figure 7: Sequential diagram 19
Figure 8: Existing System 21
Figure 9: Proposed System 22
Figure 10: Entity relationship diagram 23
Figure 11: Database Schema diagram 24
Figure 12: Landmarks on Every Face 25
Figure 13: Block Diagram of face recognition 26
Figure 14: CCTV Camera - Options 28
Figure 15: CCTV Camera - Training 29
Figure 16: CCTV Camera - Scanning 31
Figure 17: Agent - Login screen 32
Figure 18: Agent - Dashboard screen 33
Figure 19: Agent - Notification alert 34
Figure 20: Admin - Login page 35
Figure 21: Admin - Dashboard page 36
Figure 22: Admin – Criminals list page 36
Figure 23: Admin - Face Database page 37
Figure 24: Admin - Tracking page 38
Figure 25: Admin - CCTV Camera page 38
Figure 26: Admin - Reports page 39
Figure 27: List of Admins with access 40
Figure 28: Admin registration 41
Figure 29: Admin - Agent Access page 41
Figure 30: Admin – Add/Edit an Agent 42

Figure 31: Admin - Statistics page..... 43

LIST OF ABBREVIATIONS AND ACRONYMS

AES:	Advanced Encryption System
AI:	Artificial Intelligence
AIS:	Automatic Identification System
ATM:	Automated Teller Machine
CCTV:	Closed-Circuit Television
CNN:	Convolutional Neural Network
CV:	Computer Vision
DPU:	District Police Unit
IDE:	Integrated Development Environment
JDK:	Java Development Kit
MD5:	Message-Digest algorithm 5
MIS:	Manual Identification System
ML:	Machine Learning
NPC:	National Police College
Open-CV:	Open-Source Computer Vision Library
OS:	Operating System
PCA:	Principal Component Analysis
RIB:	Rwanda Investigation Bureau
RNP:	Rwanda National Police
SDK:	Software Development Kit
SQL:	Structured Query Language

CHAPTER 1: GENERAL INTRODUCTION

1.1 Introduction

Criminal identification is the most vital work for the investigation bureau who are looking for criminals, but it is also the most difficult and time-consuming task since they must locate it everywhere. It is more challenging in densely populated cities or public locations. In certain circumstances, manual identification allows for the gathering of additional information about criminals.

Criminal identification can no longer be a challenge because of existing of advanced technologies in computer vision and images processing where machine learning and artificial intelligence are used with different computer vision algorithms to detect, recognize and identify objects and human faces from a picture or video. As a solution, this research presents an automated criminal identification method based on identifying criminals' faces.

This will help the investigation bureau in identifying and apprehending offenders in public locations [1]. Criminal identification can be accomplished in two methods, as seen in Figure 1.1 Identification in the Manual Identification System (MIS) is done by the investigation bureau officers searching them in public locations. It takes a long time to offer sufficient attention, and it also carries the risk of missing criminals because they would be alerted by seeing officers and quickly escape from there. Because the MIS is taking extra time, we will not be able to adequately focus on everyone. When it comes to an automatic identification system (AIS), however, there is no requirement for public surveillance. All of the processes in this system are automated.

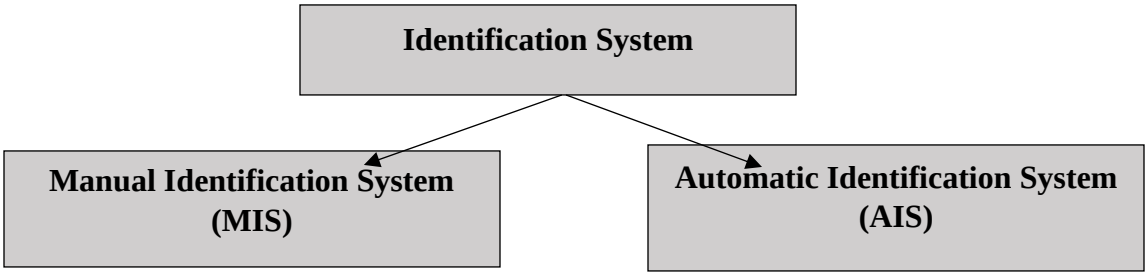


***Figure 1**: Types of Identification system*

1.2 Problem Statement

It is still a difficult and challenging for the investigation bureau to track and find people who have committed sins or people who have been suspected of a certain crime. There was a burden in using manual or analog ways of posting pictures of criminals on different platforms, social media or in public and waited for someone to recognize and identify a criminal and called the investigators to come to catch the identified criminal. The processing of the current used strategy was very slow, budget and time consuming. As bad results, it took too long to track and find the criminals which sometimes gave a chance to those criminals to commit crimes again resulted to loss of life and properties. The investigation bureau also spent a lot of money during the process which could end up in a loss. On the other hand, criminals could hide or change their identifications and they could no longer be identified easily. These are caused by not using advance technology to support the investigation and criminals' identification such as using Computer Vision, AI (Artificial Intelligence), and Machine Learning.

1.3 Objective of the Study

1.3.1 General Objectives

The general objectives of our project are to develop an advanced system which identify criminals using face recognition technologies provided by computer vision and enhanced by deep learning algorithms. The system captures and analyses images extracted from different real-time surveillance camera and are handled by image processing, and then compared with the images stored in the database. If images match, the alert sent to the administration of the system and to the nearest police station so that the identified criminal gets caught.

1.3.2 Specific objectives

The specific objectives of our project are to:

- Utilize advanced technologies to make tracking and identifying suspects more efficient.
- Apply computer vision, artificial intelligence, and machine learning to improve the accuracy of investigations.
- Provide law enforcement with more reliable tools for identifying suspects.

- Use advanced technologies to speed up the process of tracking and arresting suspects.
- Improve the ability to identify suspects who may have changed their identification or are attempting to hide.

1.4 General Interests

The interests of our project are:

- Developing a system which can be used by RIB.
- Using advanced technologies in criminal identification system.
- Applying knowledge, we covered in information security to give our hands in the existing challenge of identifying criminals in a secured, safe and fast way.
- Extending the application of computer vision technology by implementing it in our developed android based secured criminals' identification system.

1.5 Scope and Limitations of the System

The developed system has some scope and limitation. The area in which our research is based in Rwanda. And our case study focused on conducting a research based on Rwanda Investigation Bureau. We shall investigate the current strategy done by RIB and RNP to track and identify criminals who are suspect of a crime or criminals who have committed illegal activities in a way of improving the current used system.

The function of the developed system is to recognize and identify criminals based on recognizing their faces. The system uses a real-time camera which capture video and the system process it into continuous pictures and the by using computer vision algorithms as Open CV and Convolution Neural Network, the captured pictures are processed and compared with those stored in the database.

In the development of our system, we have used the camera of android devices as CCTV camera in our demonstration and working principle of our system.

1.6 Technologies

To achieve the desired output of the system, it is developed using different technologies, different programming languages, algorithms and security.

Proposed programming languages to use are:

- Java
- JavaScript
- XML
- HTML
- CSS

Database and query scripts used:

- MySQL
- Firebase

Computer vision algorithms used:

- CNN (Convolutional Neural Network)
- Open CV

The system security measures taken to enforce security on our system by protecting data sent within the system:

- The administration dashboard is secured so that only users with admin privileges can access it through the website dashboard.
- In case a criminal is detected, the system alerts automatically the system admins and the nearest police stations and the policemen so that they can catch the identified criminal.
- The passwords are encrypted using MD5 hashing
- They system uses computer vision technology to detect and identify human face
- The system easily adapts to environment changes with the help of Artificial Intelligence and Machine Learning

1.7 Organization of the report

This document is composed of 5 chapters classified as follows:

Chapter 1, this chapter provides an overview of the entire project where it contains the general introduction, background, statement of the problem, choice and motivation of the study, general objective, specific objectives, scope of the study.

Chapter 2, this chapter focuses on describing the current system environment mentioning the and analyzing how it works and the problems related to it.

Chapter 3, this chapter describes the methodology used by the researcher to achieve the stated objectives and techniques used to collect data. It helped us the researcher by proving real data from documents and people's experience provided guidance to the system solution.

Chapter 4, this chapter presents proposed implementation of the system by explaining how it works, expected results and different diagrams.

Chapter 5, this chapter provide conclusion basing on the conducted research and the outcomes and recommendations to different parties that could be interested in or get advantages from the system.

1.8 Project Gantt Chart

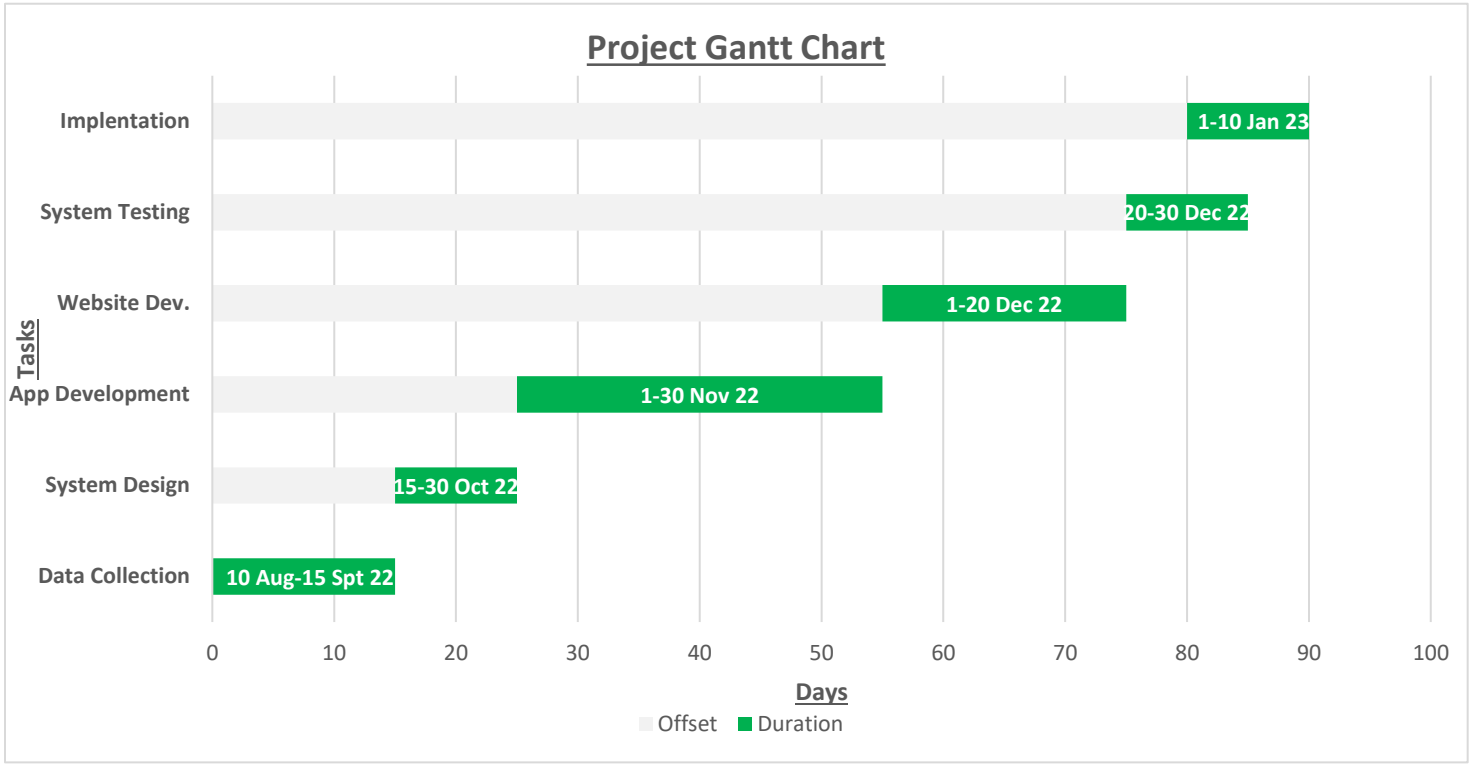


Figure 2: *Gantt chart*

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

A literature review on the use of face recognition in criminal investigations is a comprehensive examination of the existing research and studies on the topic. The purpose of the review is to provide an overview of the current state of knowledge on the topic, highlighting key findings, trends, and gaps in the existing research.

In terms of the use of face recognition technology in criminal investigations, research has generally focused on the accuracy and reliability of the technology, as well as its potential biases and limitations. Studies have also examined the ethical and legal implications of using the technology in criminal investigations, such as issues related to privacy and civil rights.

2.2 Definition of Terminologies

2.2.1 Criminal

What qualifies someone as a criminal? A criminal is a common phrase for someone who has committed a crime or has been legally convicted of committing a crime. Criminal also refers to being involved in a crime. Criminal activities or individuals are those who are involved in or connected to a crime. [2]

2.2.2 Face Recognition

A facial recognition system is a technology that can match a human face from a digital image or video frame against a database of faces. It is often used to verify users via ID verification services and works by locating and measuring facial characteristics from a given image. [3]

2.2.3 Open-CV

OpenCV is an acronym for Open-Source Computer Vision. The library includes a wide range of optimized algorithms, including both traditional and cutting-edge computer vision and machine learning techniques. It provides interfaces in C++, Python, Java, and MATLAB that work on Windows, Linux, Android, and MacOS. OpenCV is free to use for both commercial and non-commercial purposes. It is commonly used for capturing photos and videos in public places. [4]

2.2.4 Convolution Neural Network

CNN is a powerful algorithm for image processing. Their algorithms are currently the best existing algorithms for the automated processing of images. They are being used in different place to do things like identifying the objects in an image.

2.3 Related studies

"Face Recognition in Criminal Investigations" by Anil K. Jain, Karthik Nandakumar and Abhishek Nagar. In this project, the authors provide an overview of the use of face recognition technology in criminal investigations, including its technical aspects, legal and ethical considerations, and future research directions. The project covers the history and technical development of the technology, as well as its applications in criminal investigations and forensic science. The authors also examine the limitations and challenges of the technology, including issues related to accuracy, security, and privacy. Finally, they discuss the future of face recognition technology in criminal investigations and highlight areas for further research. [5]

"Assessing the accuracy of face recognition technology in forensic applications" by M.A.Bruce, C.H.Burton, J.W.Wilson. This study examined the accuracy and reliability of face recognition technology in forensic applications. The study found that face recognition technology can be an effective tool for forensic investigations when used in conjunction with other forms of evidence, but that its accuracy is influenced by a number of factors, such as image quality and the age of the face being matched. The study also highlighted that the technology can be less accurate for certain groups of people, such as women and people with darker skin tones, and may also be susceptible to errors due to lighting conditions and facial expressions. [6]

2.4 Computer Vision Algorithms used

2.4.1 CNN Algorithm

Convolutional neural network is a particular kind of neural network for working with images which takes input from an image, extracts feature from the image, and then provides learnable parameters to effectively do the tasks of classification, detection, and many other things. It utilizes something called "filters" to extract the features from the photographs; different filters are used to extract different information from the images.

CNN is widely used for a variety of computer vision applications, including image classification, object recognition, picture segmentation, and many more. It uses binary classification or multi-class classification to extract information from the images and labelling or categorizing the images following a couple of steps:

Step: - 1: Importing the necessary libraries

Step: - 2: Loading the data and basic EDA

Step: - 3: Preparing the training and testing data

Step: - 4: Building the Model

Step: - 5: Compile and Train the Model

Step: - 6: Evaluating the model

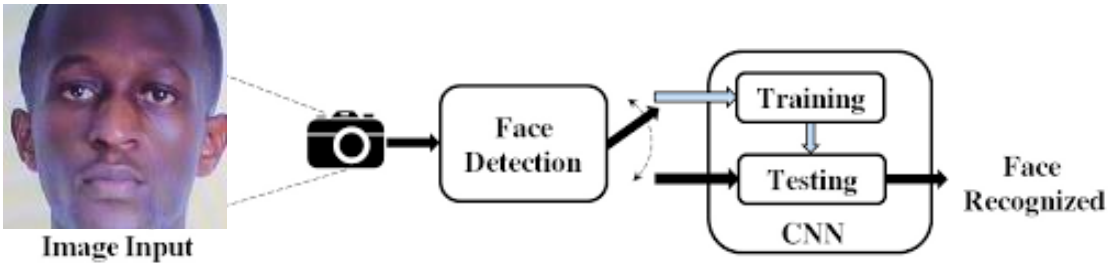


Figure 3: *CNN - Convolutional neural networks*

In our project, we used the following CNN models:

VGGFace: This model was trained on a large dataset of faces and was used for face recognition and verification tasks. Its high accuracy and ability to handle large datasets made it an ideal choice for our project.

ResNet: This model was known for its high accuracy on image classification tasks and was fine-tuned on a dataset of faces. Its ability to achieve high accuracy made it a suitable choice for our project.

2.4.2 TensorFlow

TensorFlow is a widely used and highly regarded open-source Python package from Google that makes building computer vision deep learning models straightforward and easy. With TensorFlow, the process of gathering data, training models, delivering predictions, and improving future outcomes is made easier by Google Brain Tensor-Flow. It is an open-source library for numerical computation and large-scale machine learning.

2.4.3 Eigen faces Approach using PCA Algorithm

Dimensionality reduction and linear algebra techniques are used in this approach for face recognition. This method was employed at the time in a variety of applications, including handwriting recognition, lip reading, medical picture analysis, etc. since it was simple to use and had lower processing costs. It reduces dimensionality and projects training sample/data into tiny feature space using Eigenvalues and Eigenvectors.

Figure 4: *Face Recognition Using Eigenfaces*

Advantages:

- Simple to implement and less expensive in terms of computing.
- No prior knowledge of the image is necessary, such as face features
- Simple to use and has lower processing costs compared to other methods.
- Can be applied to a variety of applications, not only face recognition.
- Can be used to reduce dimensionality and project training data into a small feature space.
- Highlight the most distinctive features of a face.

Limitations:

- For training/testing, a correctly cantered face is necessary.
- The algorithm is sensitive to the amount of light and shadow in an image as well as the size of the face.
- This algorithm must have a front view of the face in order to function effectively. It assumes that the face images are well-aligned and that the lighting conditions are similar across all images.
- It may not perform well when there is significant facial expression variation in the images.
- It may not be robust to changes in lighting conditions or facial poses.
- The performance of the algorithm may decrease when there is a high degree of overlap among the classes.
- It is sensitive to noise, so the images need to be pre-processed.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

A research method is a specific process or method used to identify, select, process, and analyze information about a topic. Scientifically it must be forced to be analyzed and consider their causes, solutions, explanations and applications. Analysis in particular helps us to understand nature and natural phenomena. And we use "qualitative research".

This chapter describes the development side of “Criminal Investigation Using Face Recognition Based on Deep Learning Algorithms” it encloses a brief overview of the technologies used to make our system, tests have been applied. And also specify software compatibility requirements.

3.2 Methodological Approach

A methodology is a broad research approach that describes how the study will be carried out and, among other things, specifies the method to be employed. Methodology describes these approaches, which specify the means or method of data gathering or the way of obtaining a certain outcome. The methodology does not identify a specific methodology, but significant emphasis is placed on the type and type of process, or objective, to be followed in a certain procedure.

In our study we are expecting to use the following data collection methods:

1. Documentation

2. Observation

3.2.1 Documentation method

Documentation, as you know, is the process of reading a library book and browsing the Internet. Information about them relevant to our topic or inquiry. To obtain a bibliographic search on a topic, use this procedure. Some researchers are interested in researching on a subject that shares some similarities with ours. The information gathered will assist us in developing your project.

3.2.2 Observation method

One key aspect of our observation methodology was the use of real-world case studies to assess the effectiveness of face recognition in criminal investigations. We worked closely with law enforcement agencies to identify cases where face recognition was used, and we collected data on the performance of the algorithms and the outcomes of the investigations. This allowed us to directly observe the impact of face recognition on real-world investigations and to understand the challenges and limitations of using these algorithms in practice. Additionally, we conducted interviews with law enforcement personnel and stakeholders to gather additional insights into the use of face recognition in criminal investigations. This mixed-methods approach allowed us to gain a comprehensive understanding of the strengths and weaknesses of face recognition in this context.

In our criminal investigation project using face recognition, we employed a mixed-methods approach to gather information from different sources and gain a comprehensive understanding of the use of face recognition in criminal investigations. This approach included:

Experimental Design: We created controlled conditions in which to test the face recognition algorithms and measure their effectiveness in identifying suspects. We used a database of known individuals and compared the results of the face recognition algorithms to manual identification methods.

Case Study: We analyzed real-world examples of criminal investigations in which face recognition was used. We collected data on the performance of the algorithms and the outcomes of the investigations, as well as conducted interviews with law enforcement personnel and stakeholders to gather additional insights.

Survey: We gathered data from a sample of law enforcement personnel to gather information on their experiences and perceptions of using face recognition in criminal investigations.

Simulation: We created a simulated scenario in which to test the face recognition algorithms. We created a virtual environment in which the algorithms were used to identify suspects and measured the accuracy of the results.

By using a mixed-methods approach, we were able to gain a more thorough understanding of the strengths and limitations of face recognition in criminal investigations. This approach allowed us to triangulate the data from different sources and validate the findings. The combination of methods allowed us to have a comprehensive and reliable results.

3.3 Requirement Analysis

Software Development Life Cycle

The process that serves as the framework for software development is known as the SDLC, or software development lifecycle. The SDLC serves as a guide for project managers and business organizations as they complete each phase of the software development lifecycle. A phase is the name for each stage of the SDLC. The SDLC's initial step is the requirements collecting and analysis phase.

Waterfall model

The waterfall approach was the first SDLC model widely used in software development to ensure project success. The "waterfall" approach divides the entire software development process into individual phases. In this waterfall model, the result of one phase typically serves as the input for the next sequential phase.

The following figure shows the different phases of the waterfall model.

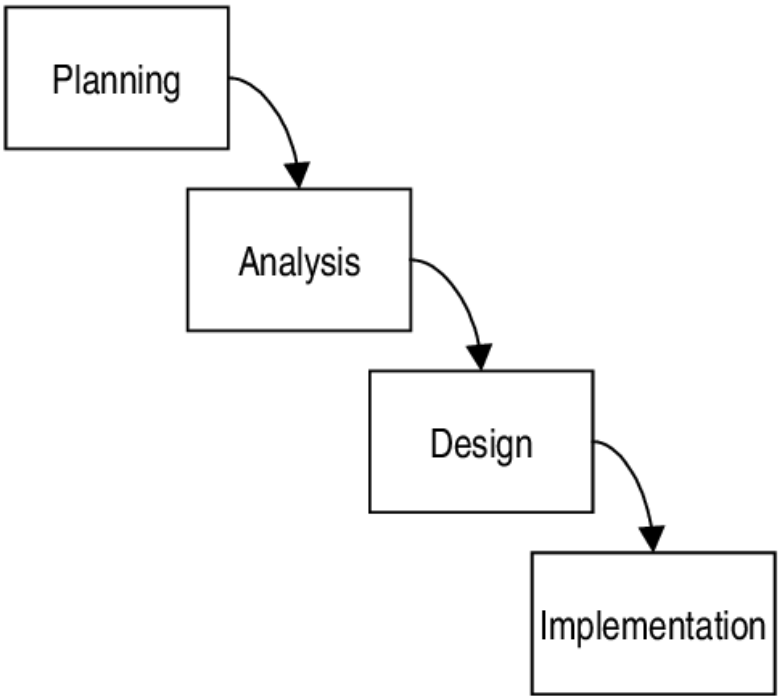


Figure 5: *Waterfall model*

The successive phases of the waterfall model are 7:

- ✓ **Requirement's extraction and analysis**: In this phase, all possible requirements for the system to be developed are recorded and documented in the specifications.
- ✓ **System design**: In this phase, the specifications of the first phase are investigated and the system design is prepared. This system design helps specify hardware and system requirements and helps define the overall system architecture.
- ✓ **Implementation**: With input from the system design, the system is first developed in small programs, so-called units, and integrated in the next phase. Each unit is developed and tested for its functionality. This is called a unit test.
- ✓ **Integration and testing**: All units developed during the implementation phase will be integrated into the system after each unit has been tested. After integration, the entire system is tested for errors and failures.
- ✓ **System offering**: As soon as functional and non-functional tests are completed. The product is used in your environment or put on the market.

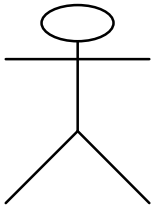
- ✓ **Maintenance**: There are some issues with the client environment. Patches have been released to address these issues. Also, some better versions will be released to improve the product. Maintenance is performed to bring these changes to your environment.

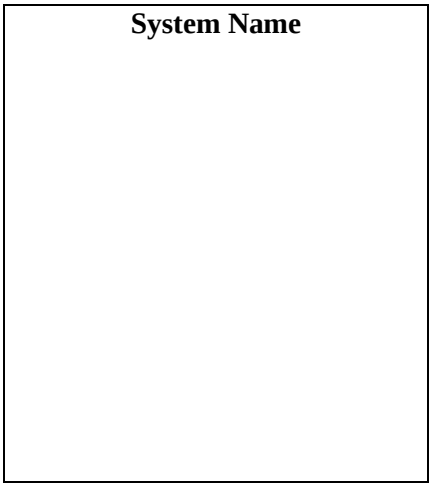
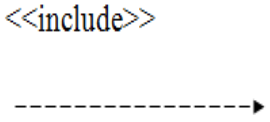
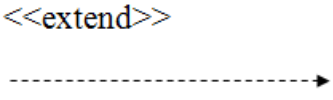
All of these phases are cascaded and progress is considered to be steadily flowing downwards (like a waterfall) through the phases. The next phase is named "Waterfall Model" because it only starts when the goals defined in the previous phase are achieved and approved. In this model, the phases do not overlap.

3.4 Class diagram

A class diagram in the Unified Modeling Language is a form of static structural diagram that illustrates a system's classes, their properties, operations, and relationships between objects in order to describe the system's structure.

3.4.1 Symbol Used for Class diagram

An actor: ➢ Is a person or system that derives benefit from and is external to the subject. ➢ Is depicted as either a stick figure (default) or, if a nonhuman actor is involved, a rectangle with "Actor" in it (alternative). ➢ Is labeled with its role. ➢ Can be associated with other actors using a specialization/super class association, denoted by an arrow with a hollow arrowhead. Is placed outside the subject boundary.	 Actor Name

A subject boundary: ➢ Includes the name of the subject inside or on top. ➢ Represents the scope of the subject, ○ e.g., a system or an individual business process.	
An include relationship: ➢ Represents the inclusion of the functionality of one-use case within another. ➢ It has an arrow drawn from the base Use Case to the used Use Case.	
An extend relationship: ➢ Represents the extension of the Use Case to include optional behavior. ➢ Has an arrow drawn from the extension Use Case to the base Use Case	

A generalization relationship: ➢ Represents a specialized Use Case to a more generalized one. ➢ Has an arrow drawn from the specialized Use Case to the base Use Case?	
An association relationship: ➢ Links an actor with the Use Case (s) with which it interacts.	

Table 1: *Use Case tools description*

Design of the diagram: Use Case

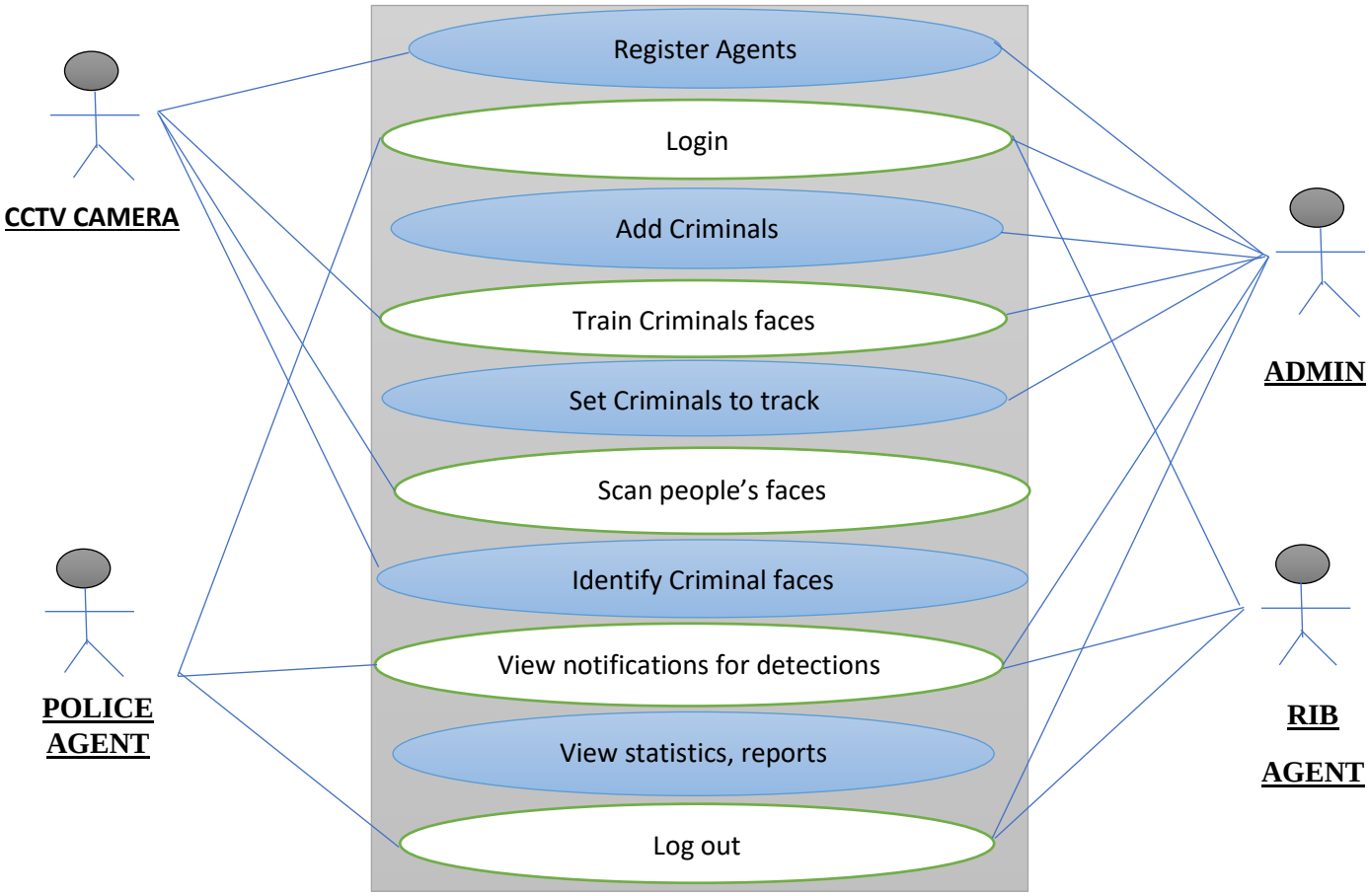


Figure 6: *Use Case diagram*

3.5 Sequence Diagram

The Sequence Diagram model is the collaboration of objects based on a time sequence. That shows how the objects interact with others in a particular scenario of a use case. With the advanced visual modeling capability, you can create complex sequence diagram without an obstacle.

This figure explains the sequence of user interaction with a system

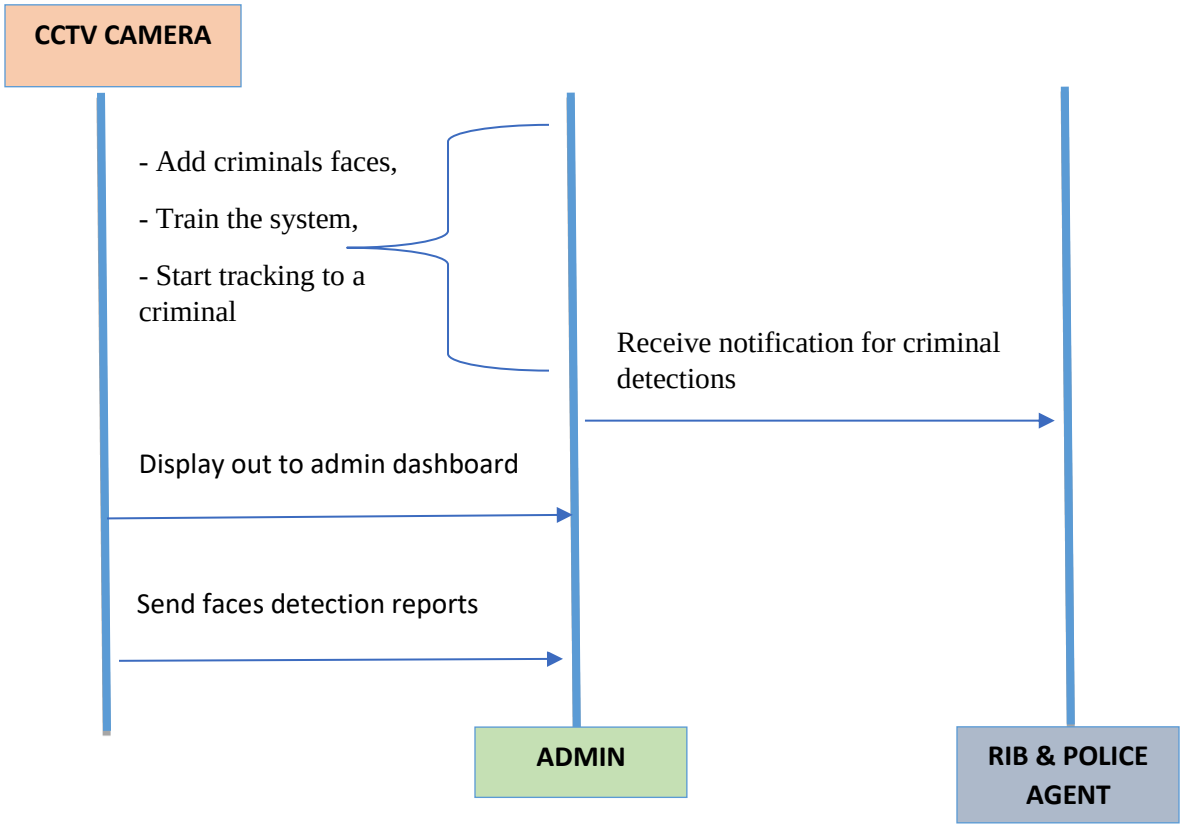


Figure 7: *Sequential diagram*

3.6 System Requirements

3.6.1 Hardware requirements

The system hardware required are:

- Computers such as laptops, desktop, android phones
- RAM with 4GB minimum

- Processor: Intel core or i3 of 2.9HZ minimum, etc
- Hard Disk with 500GB minimum

3.6.2 Software requirements and development tools

The software required are:

- Android studio
- Android SDK
- Open-CV library
- JDK
- VS Code
- Firebase
- Realtime database
- Operating System (OS): Windows 8,8.1,10, and windows 11

CHAPTER 4: ANALYSING, DESIGN, AND IMPLEMENTATION OF THE PROJECT

4.1 Introduction

This chapter contains two main parts: the design and implementation of the criminal investigation using face recognition based on deep learning algorithms for RIB as the administrators and the CCTV application for scanning. This chapter explains and demonstrate the projects using screenshots and diagrams including user case diagrams, ER diagrams, and user interfaces.

4.2 Existing System

Normally the current system in Rwanda, we have RIB (Rwanda Investigation Bureau) which is the agency responsible to tracking and finding criminals who have committed illegal activities and it can assign tasks to RNP (Rwanda National Police). The way criminals' identification is performed, is that RIB posts the picture of criminals on the platforms, social media and also, they put different publication in the news, and post banners of their faces in different places so that when someone recognize a criminal basing on the posted photo, he/she can call the investigation bureau. In this case, there can be no accuracy because it is hard to remember someone you saw in a picture, memorize him/her and be able to match the identification with someone you saw in the public. Also, the identification can take too long to find the criminals. [7]

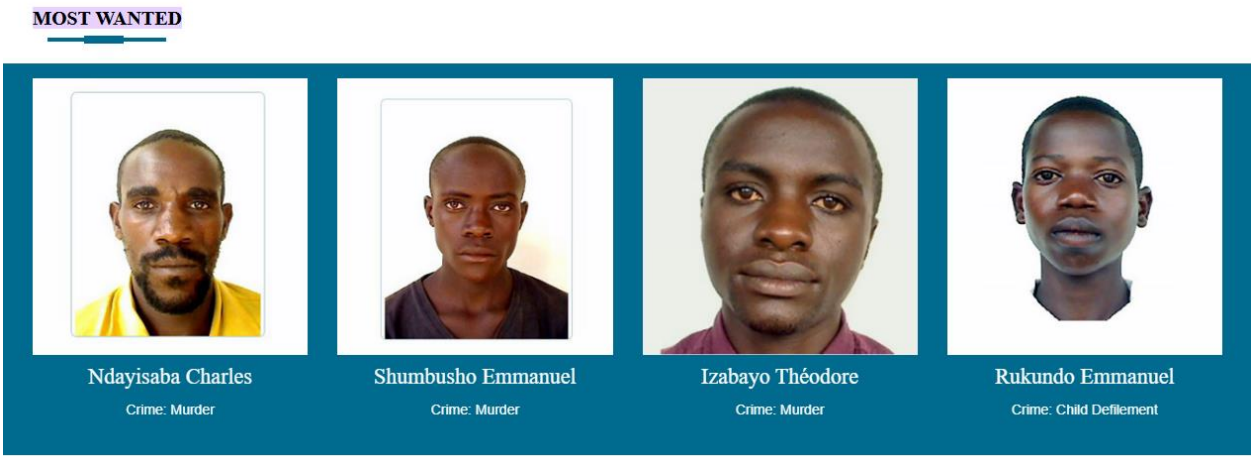


Figure 8: *Existing System*

4.3 Proposed System

In this project, we use CCTV cameras that are always recording in a public setting. During the system's implementation, we will save criminal photos data with their names on photographs in the database. We will process those photos and extracting features from them, and during feature extraction, and we will be grabbing the face encodings from the current images and storing them into a single file using Android device technology. Using open-CV while capturing CCTV footage and captured images face encodings are placed and compared with our saved face encodings of the criminal database if any match is found then automatically on screen it will display an image of that criminal whose face matches and display the message with his name that criminal found and give an alert to the concerned agency of investigation bureau and also notify the nearest policemen so that they can catch the identified criminal.

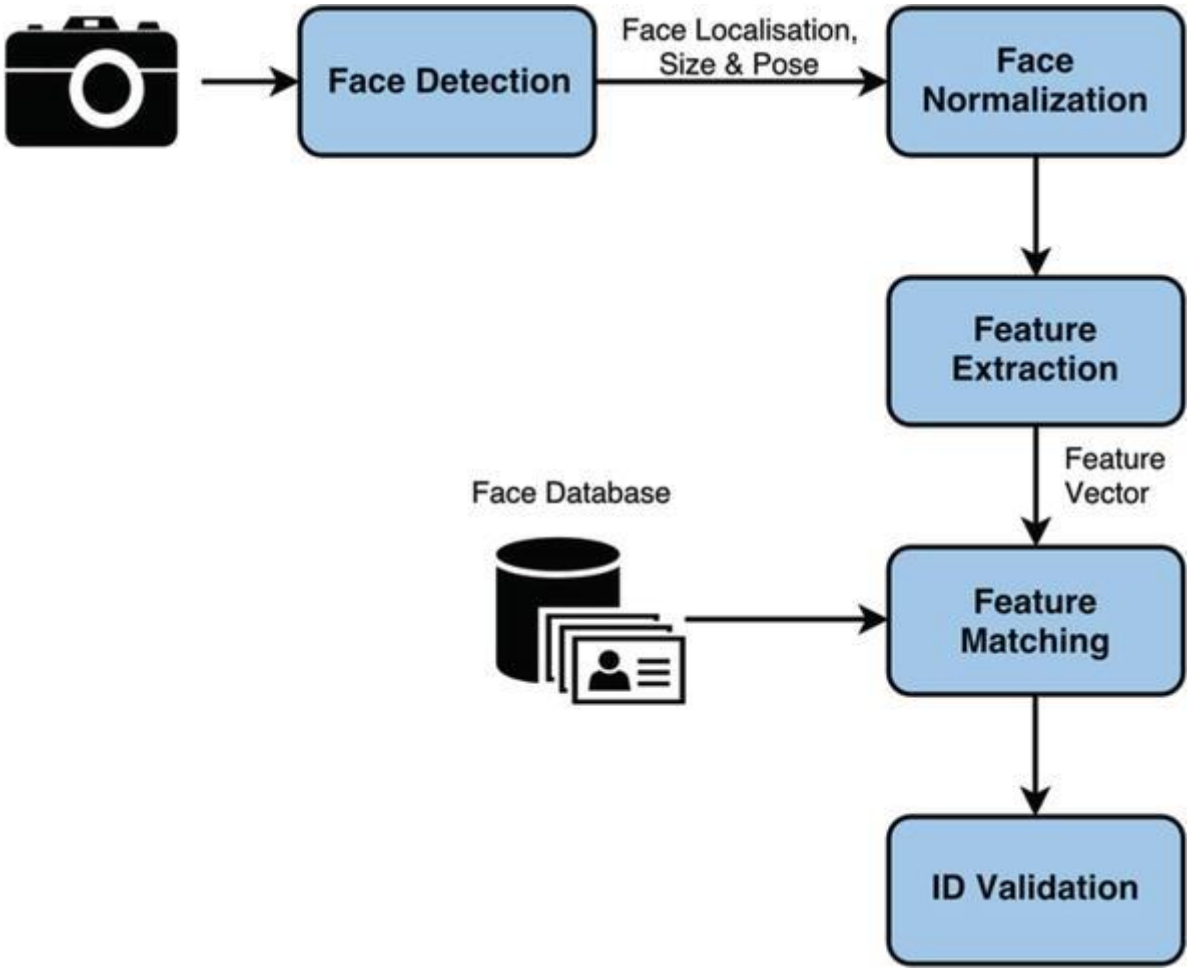


Figure 9: *Proposed System*

4.4 Entity relationship diagram

This entity relationship diagram details the tables in the database, the entities, and a description of each table.

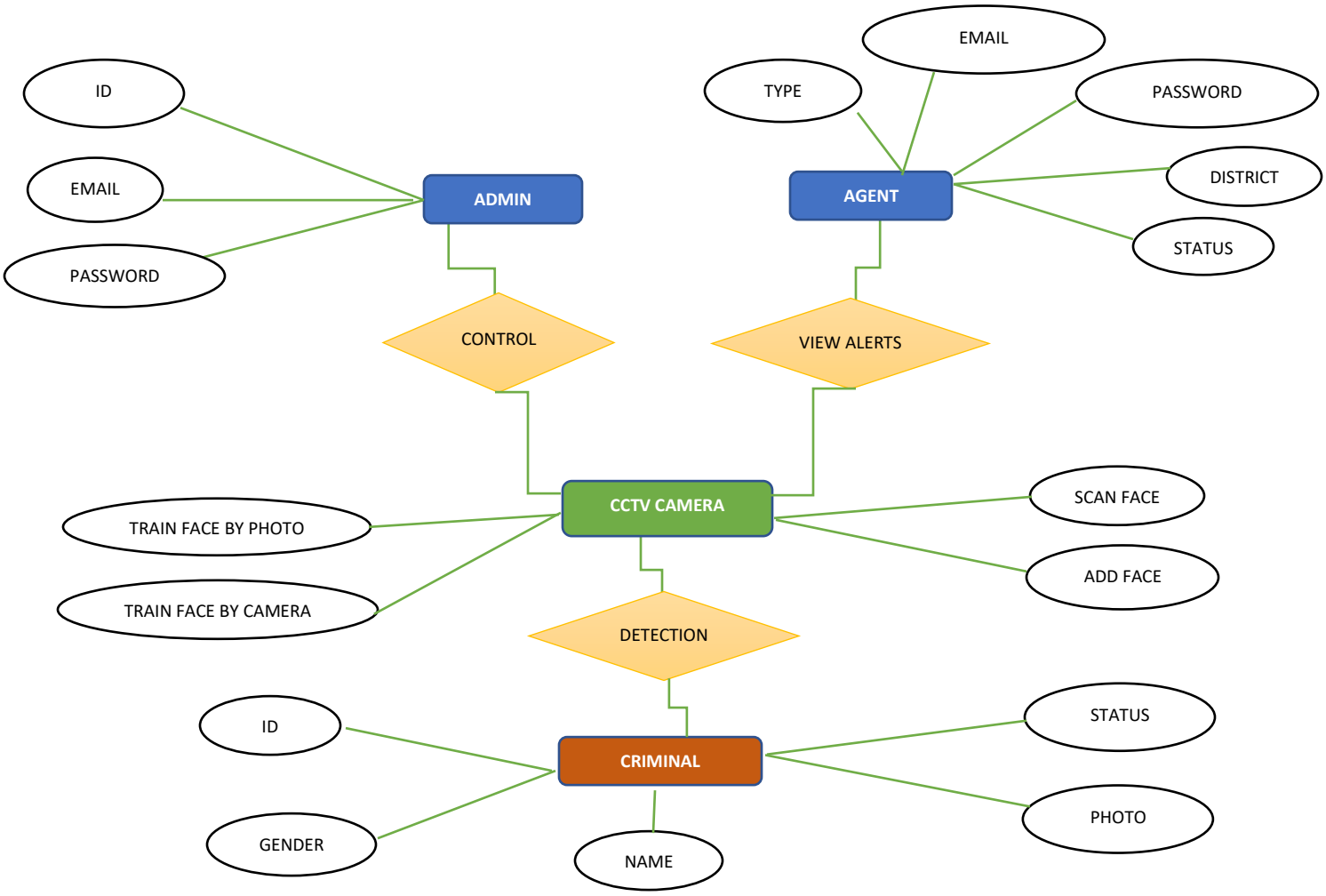


Figure 10: *Entity relationship diagram*

4.5 Database schema

A database schema is the logical representation of a database, which shows how the data is stored logically in the entire database. It contains list of attributes and instruction that informs the database engine that how the data is organized and how the elements are related to each other.

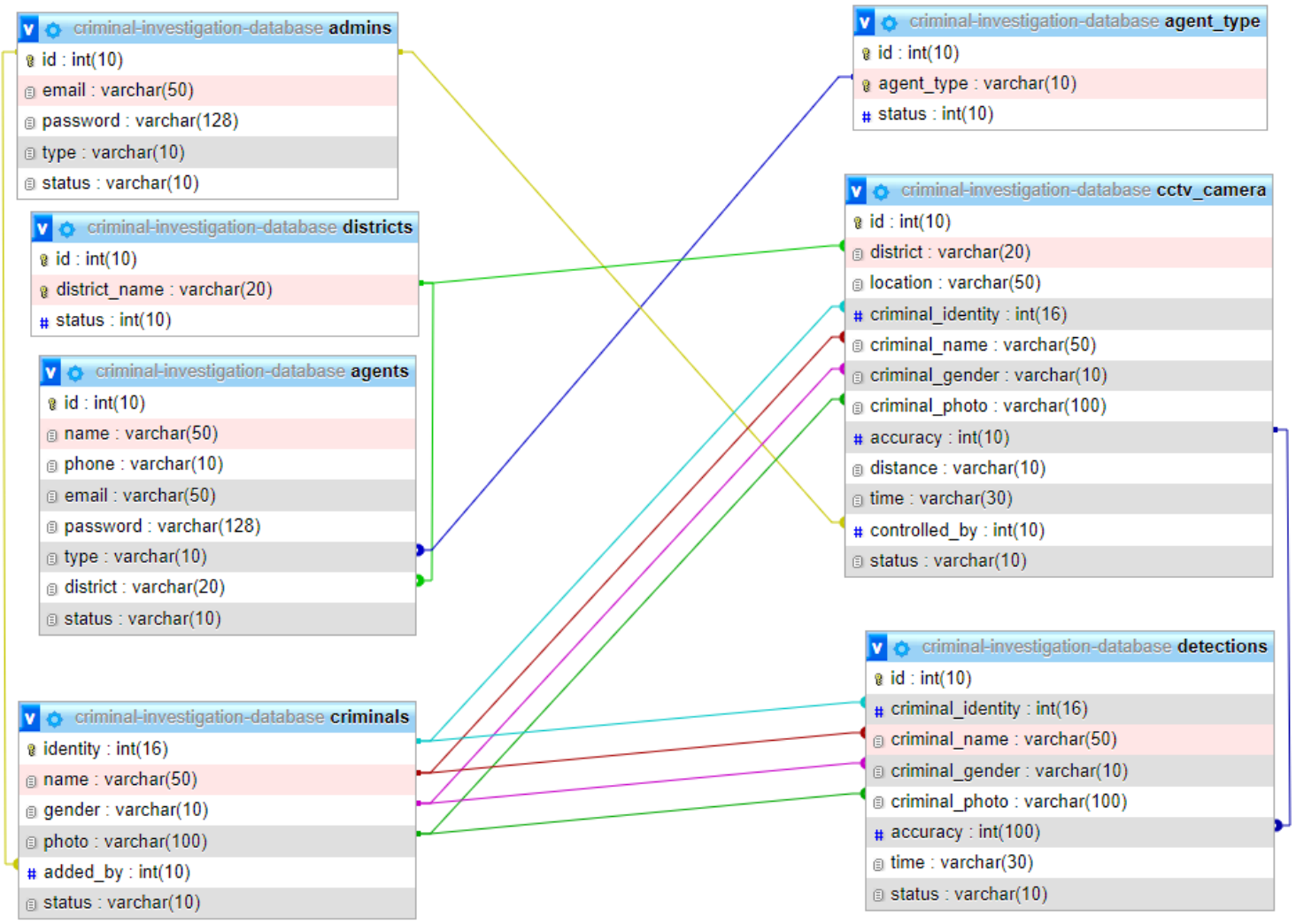


Figure 11: *Database Schema diagram*

4.6 System Analysis

Criminal enrollment is the first stage in recording criminal information in the criminal database. Criminal identities, names gender and images are recorded in the database then face recognition and identification is conducted using the recorder images and information. Using the face detection

algorithms, picture of criminals' face encodings will be used. The database procedure is criminal enrollment, but the major step begins with facial detection. As seen in Figure below, face detection takes into account 68 landmarks on the face. CCTV camera collected film or picture is saved, and its properties, such as encodings, are extracted before being compared to image encodings in the database. The face will be matched in the database, and the name and the criminal detected message will be shown beside the criminal image on the screen in the CCTV Room.

[8]

Figure 12: *Landmarks on Every Face*

In this project we used a large dataset containing tens of hundreds of images of faces, specifically the Labeled Faces in the Wild dataset. Our models achieved high accuracy levels, typically in the range of 91-97%. However, the performance of the models may vary depending on the specific dataset and conditions used during testing. We also considered other factors such as computational resources, real-time performance, and privacy concerns. Overall, our project's results were in line with industry standards, achieving high levels of accuracy while considering other important factors.

4.7 Working Principle of the System

We are employing CCTV cameras to capture photographs of members of the public in order to identify the appropriate person who has a criminal record in the database to apprehend.

1. First, we extract the facial encodings from the criminal database photos and save them in one list, while dividing the name recorded with the criminal image into another list.

2. Then the CCTV Camera are deployed to collect public pictures in order to identify and easily apprehend criminals who are present in public places.

3. Taking the acquired photos' face-encodings and extracting the features from them.

4. Using our database image encoding values to compare captured picture encoding values.

5. If the encoding values match those of the taken image, the criminal image, name, and message are shown on the screen.

6. The image of that individual are saved to a separate folder, allowing investigation bureau to readily identify the criminal whose identification matches.

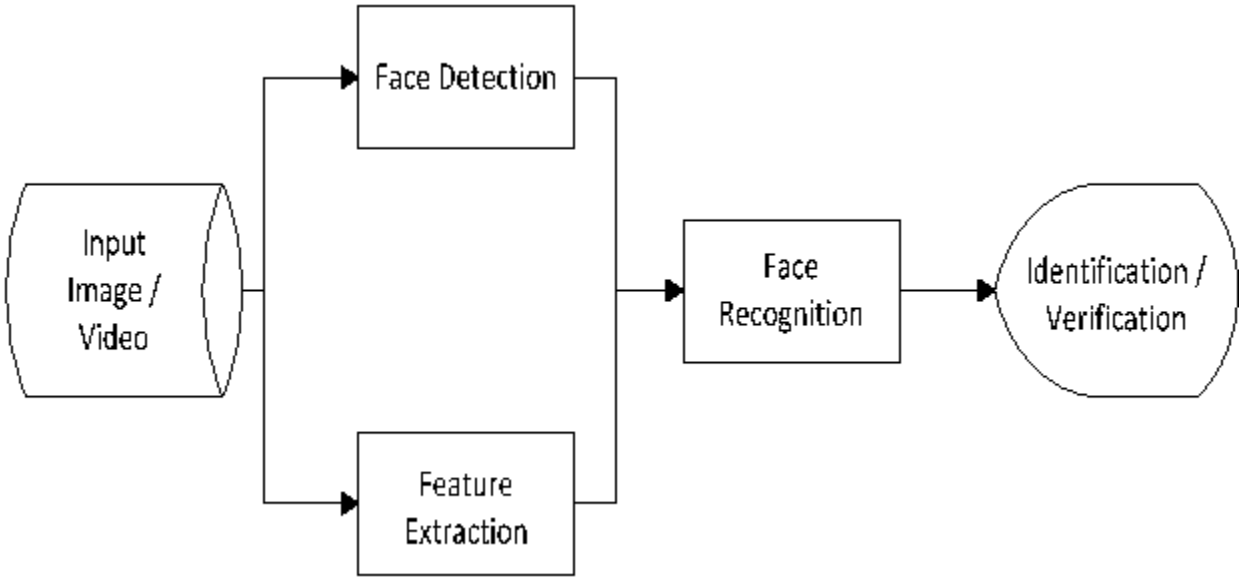


Figure 13: *Block Diagram of face recognition*

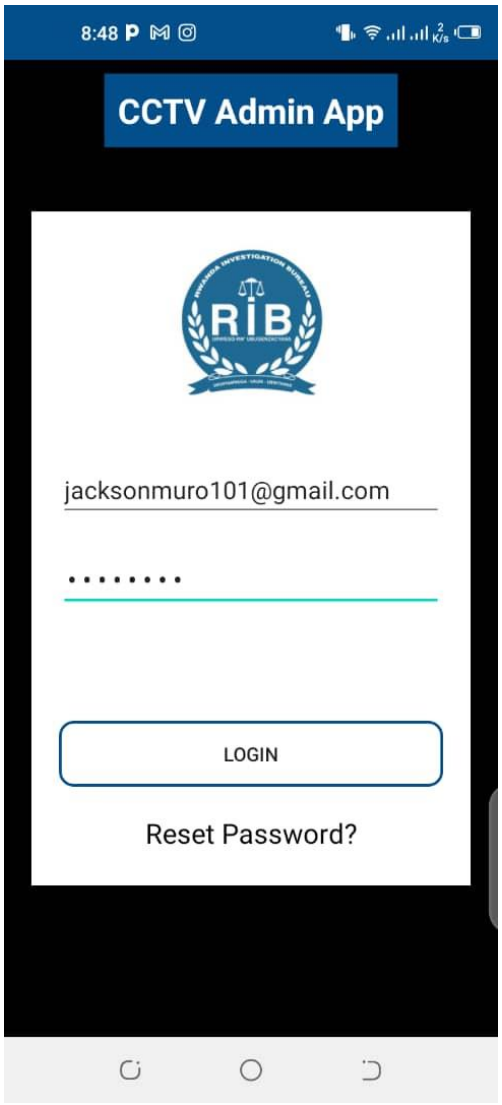
4.8 System Implementation

4.8.1 Overview of system interface for CCTV Camera application

The interfaces to be demonstrated are implemented in the android mobile application which act as a CCTV camera device. It is used to capture people's faces and use the computer vision algorithm to identify and recognize criminals.

CCTV Camera – Admin login

For the agents to access the agent mobile application, It typically requires an email and password to log in.The purpose of an admin login page is to provide a secure way for administrators to manage and maintain the website or application.



CCTV Camera – Options

The CCTV Camera provide different options mainly its purpose is to train criminals face for further recognitions and saving recognitions data in the database.

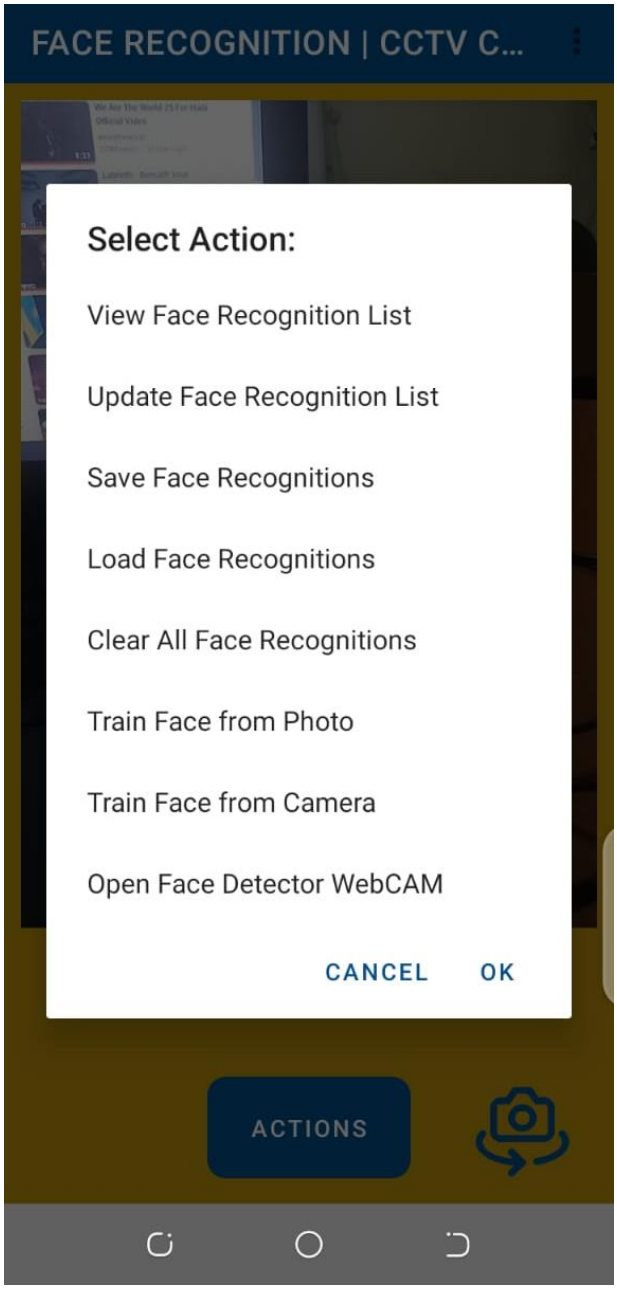


Figure 14: *CCTV Camera - Options*

CCTV Camera – Training

From the CCTV Camera, that's where the admin can register faces of criminals either by using a camera or saved photos. After training the criminal, you provide the information corresponding to the trained face such as the identity, the name and the gender to be saved in the database.

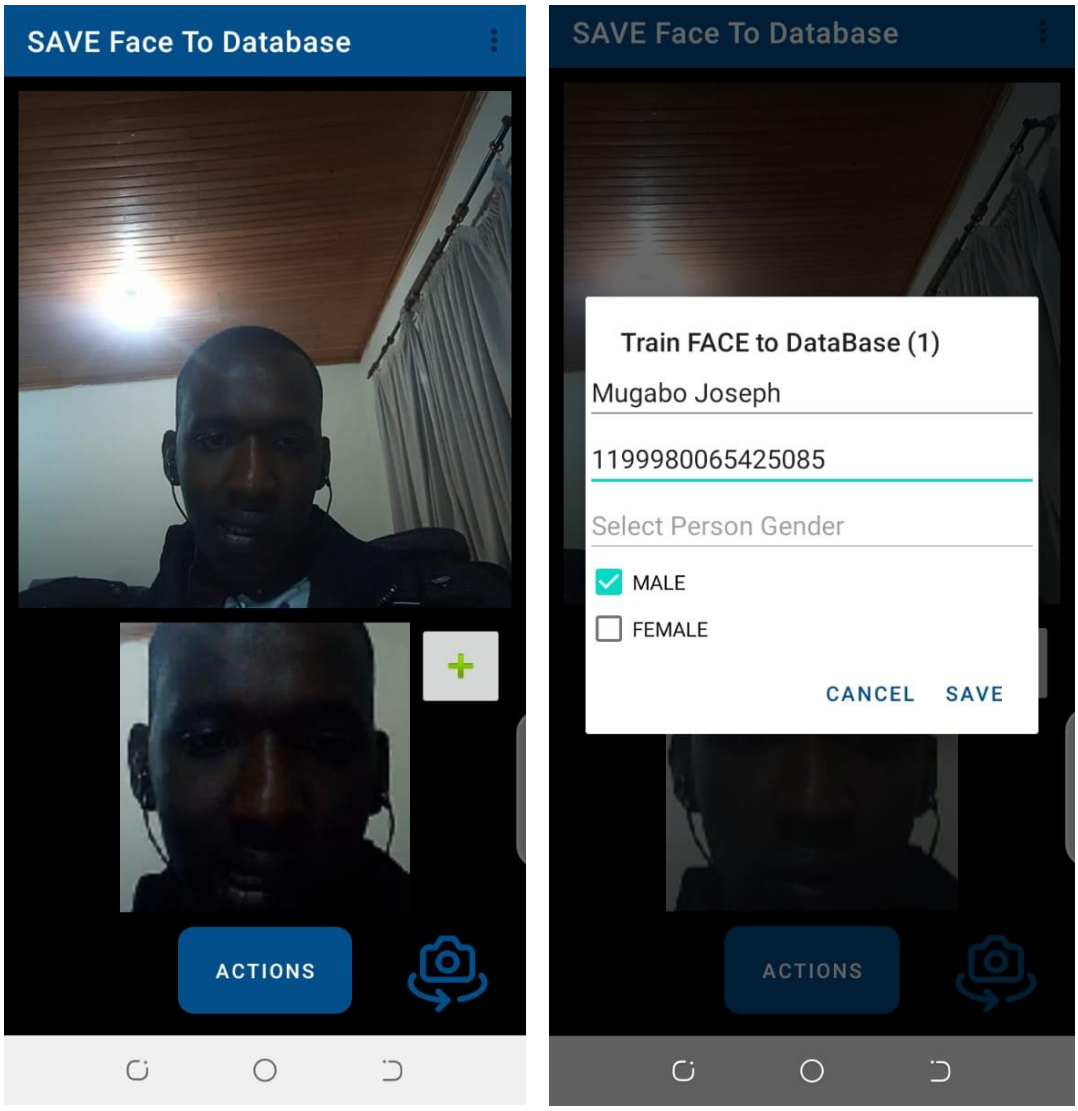
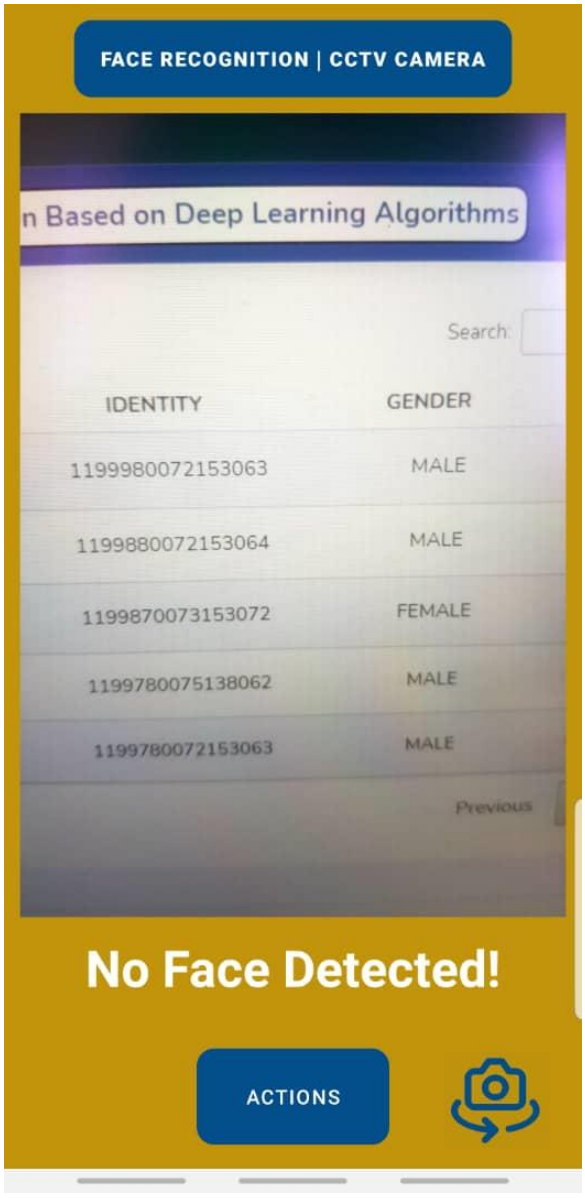


Figure 15: CCTV Camera - Training

CCTV Camera – Scanning

The CCTV Camera also performs the scanning of people face with a live video scanning, and by using computer vision algorithm, it is able to identify a human face and compare it with the

registered faces in the database and hence it recognizes criminals and send the information to the administration dashboard.



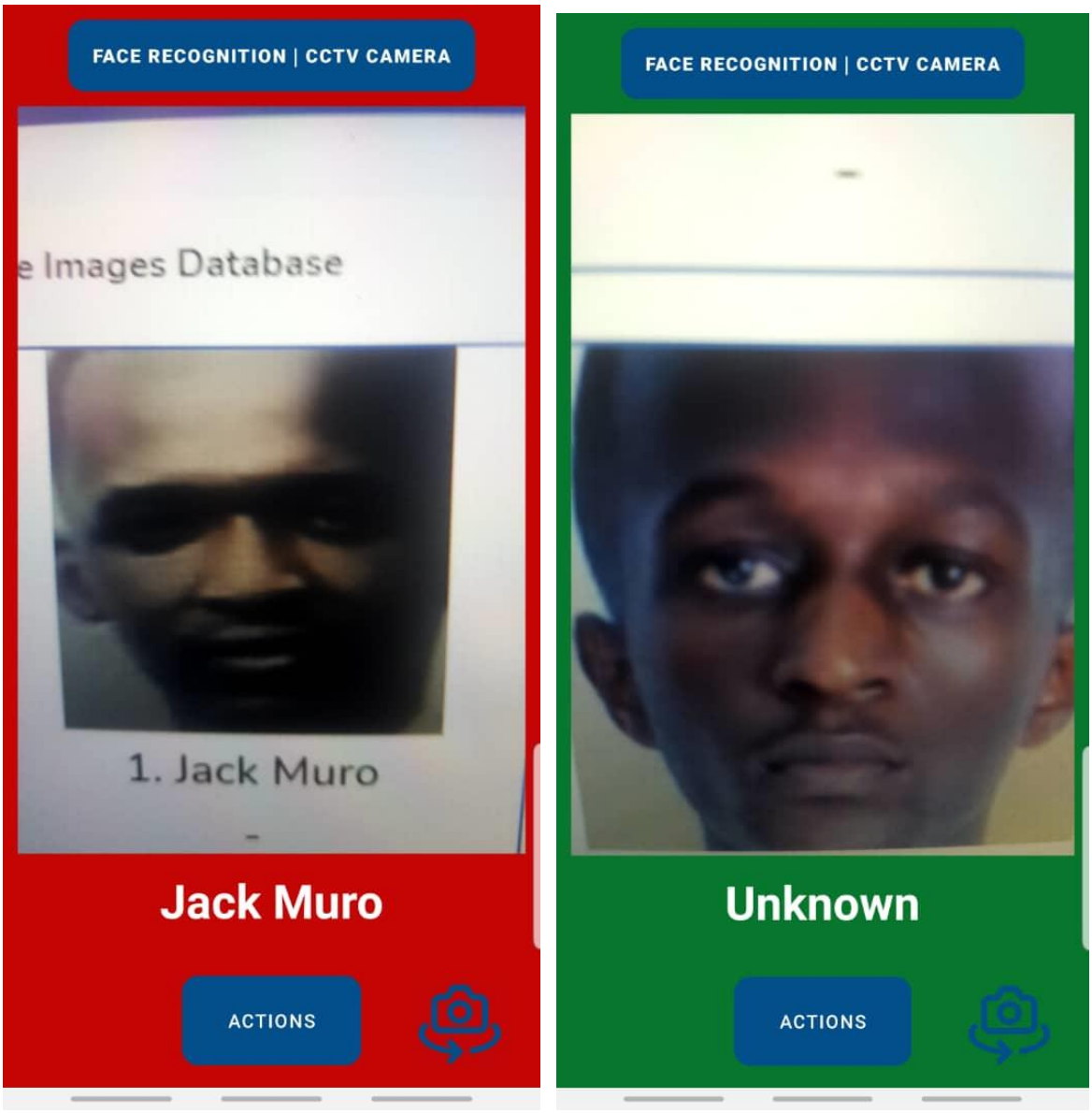


Figure 16: *CCTV Camera - Scanning*

4.8.2 Overview of system interface for agent's android mobile application

The interfaces to be demonstrated are implemented in the android mobile application of the agents, which is gives registered and authorized RIB and police agents to access information in the system.

Agent – Login screen

For the agents to access the agent mobile application, they have to be registered by the admin and verify their email and also get approved by the admin. To be authenticated, the agent must provide their email and password.

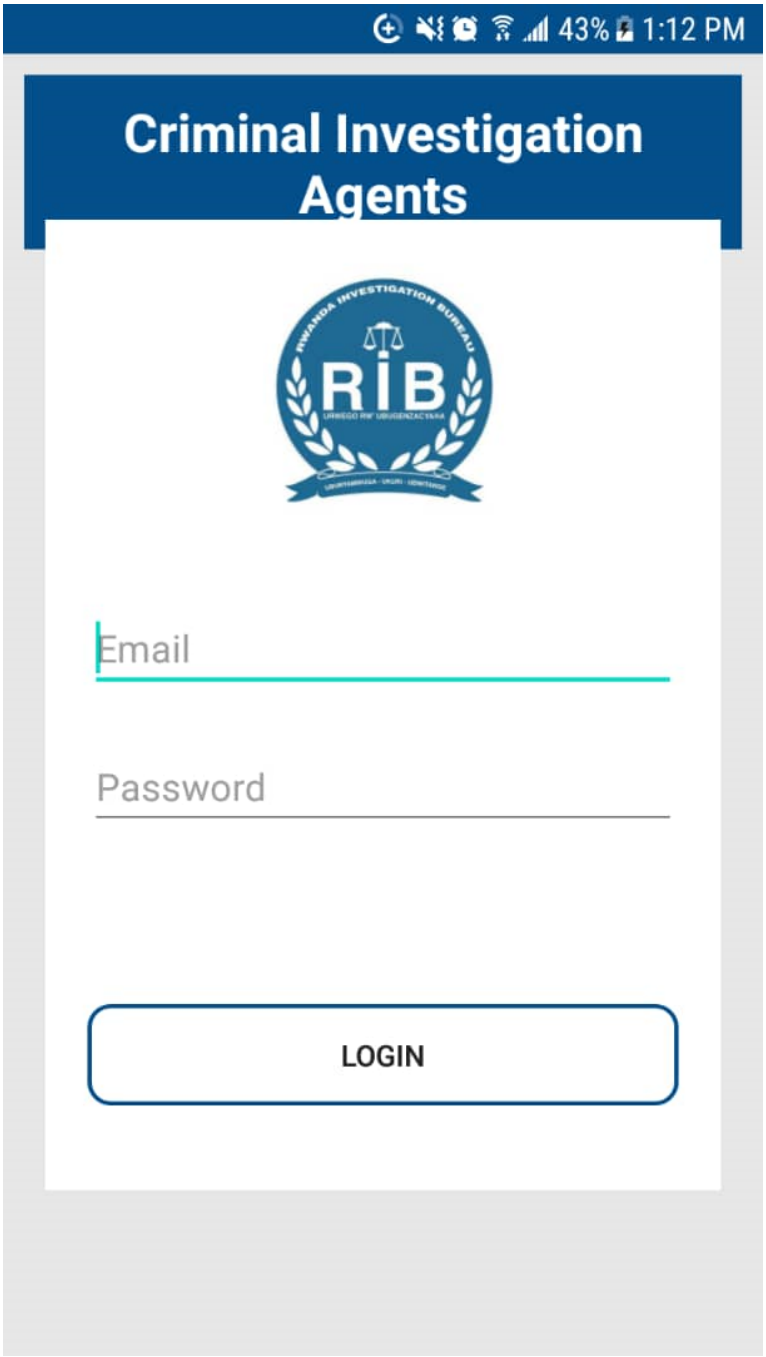


Figure 17: *Agent - Login screen*

Agent – Dashboard screen

After logging in, the agents are taken to their dashboard screen in the application where they can be able to view data captured by the CCTV Camera is the location that are assigned to. In case a tracked criminal is detected, the agents of RIB or Police are be able to see it on their smartphones.

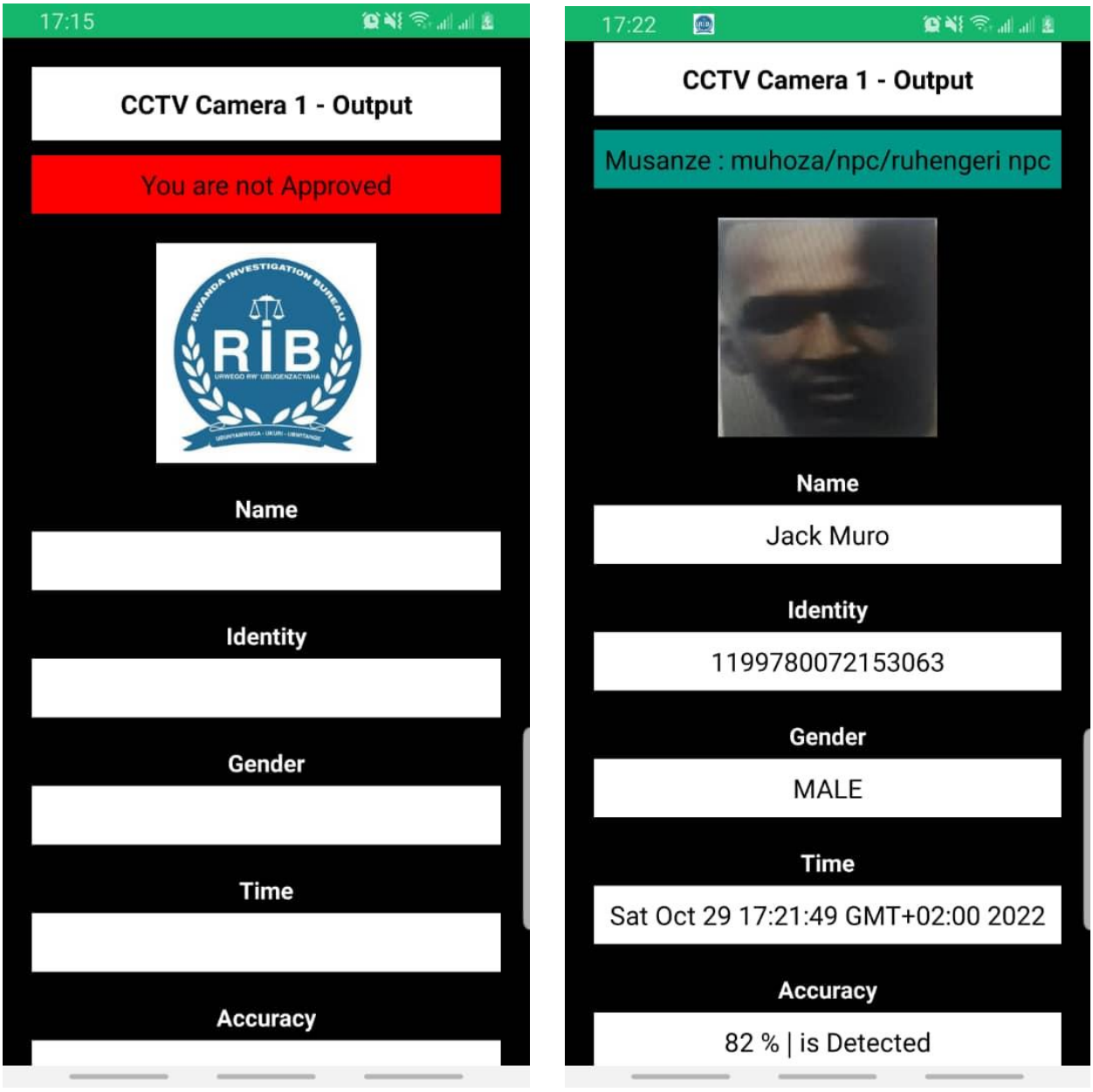


Figure 18: *Agent - Dashboard screen*

Agent – Notification alert

On the agent application, once a criminal who is being tracked is detected and recognized, a notification alert is sent to all approved agents with in the CCTV Camera location.

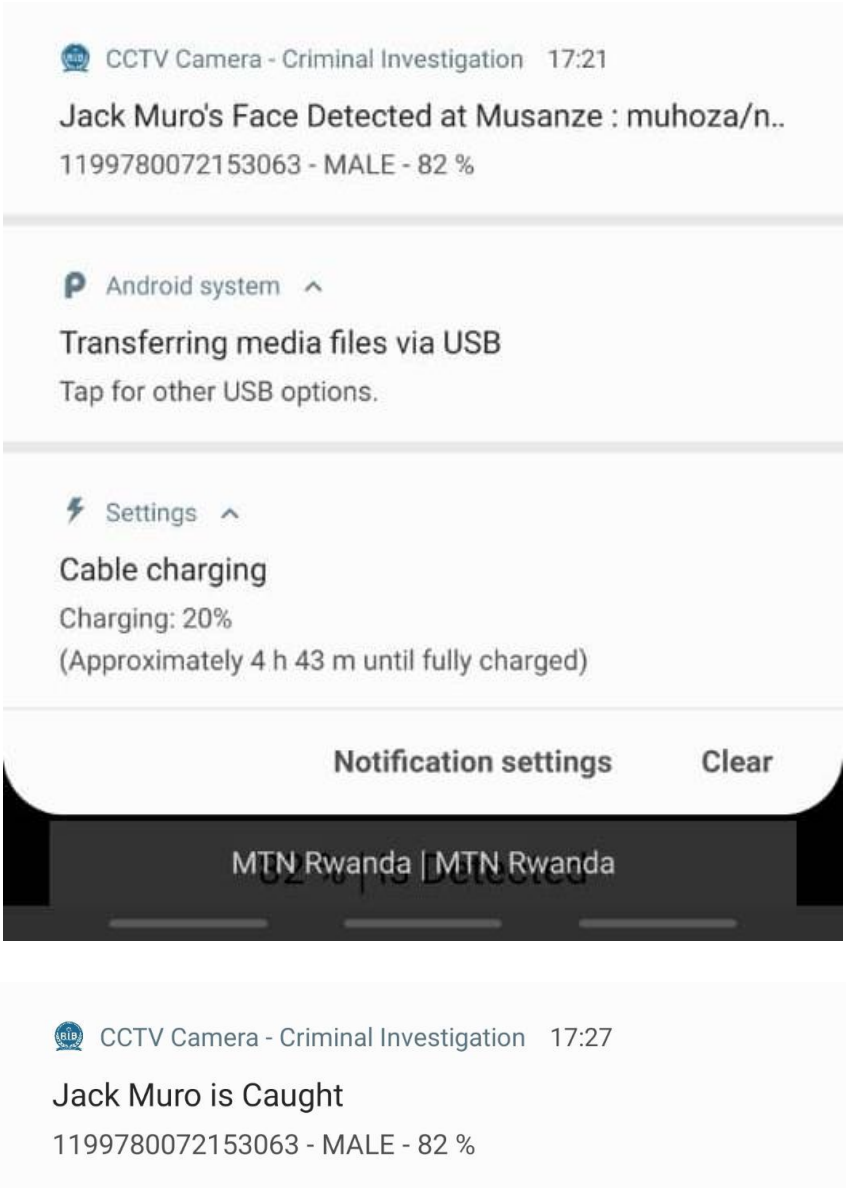


Figure 19: *Agent - Notification alert*

4.8.3 Overview of system interface for admin's website dashboard

The interfaces to be demonstrated are implemented in the website dashboard which is used by only the administrators of RIB to select criminals to be tracked, to view reports of tracked and detected criminals and other statistics.

Admin – Login page

This is the entrance page for the administration of the system, where the admin must provide a valid email address and a security password to be able to login in the dashboard. And only registered emails with admin privileges can have access to the dashboard. In case an admin forget the password, there is also an option to reset the email where a rest password link is sent to the entered admin email address.

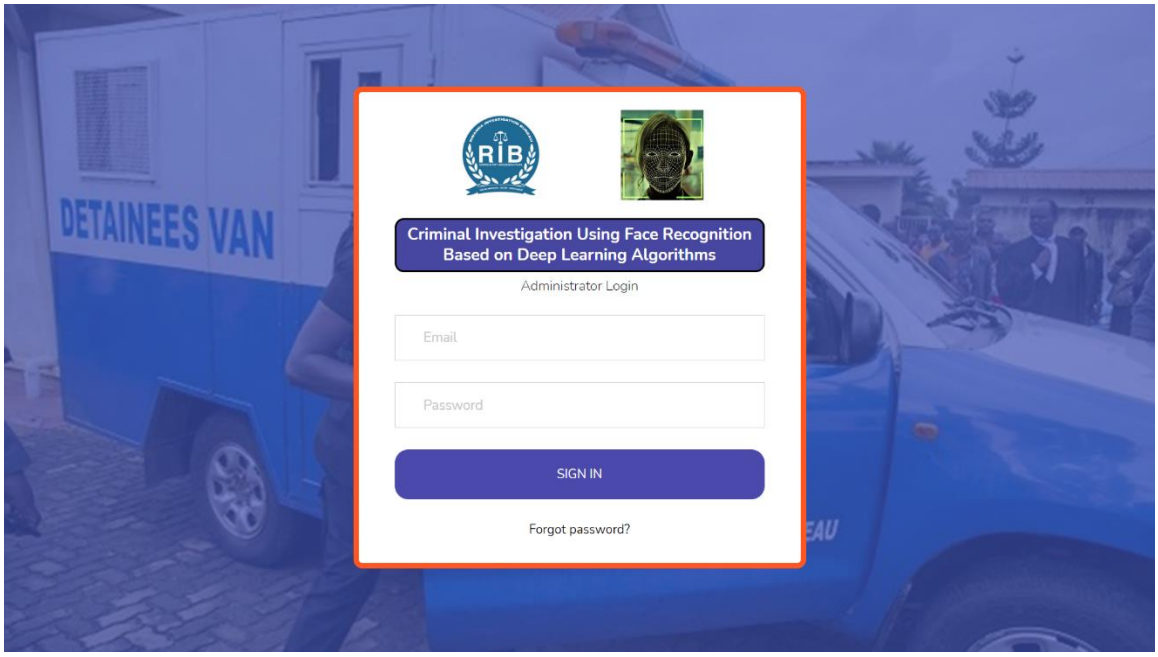


Figure 20: *Admin - Login page*

Admin – Dashboard page

This dashboard page is designed to provide an overview of the key metrics and performance indicators for a website or application. An admin dashboard page includes a variety of different components, such as criminals page, tracking page, deleted page, and other visualizations that help administrators to quickly understand the status and performance of the website.

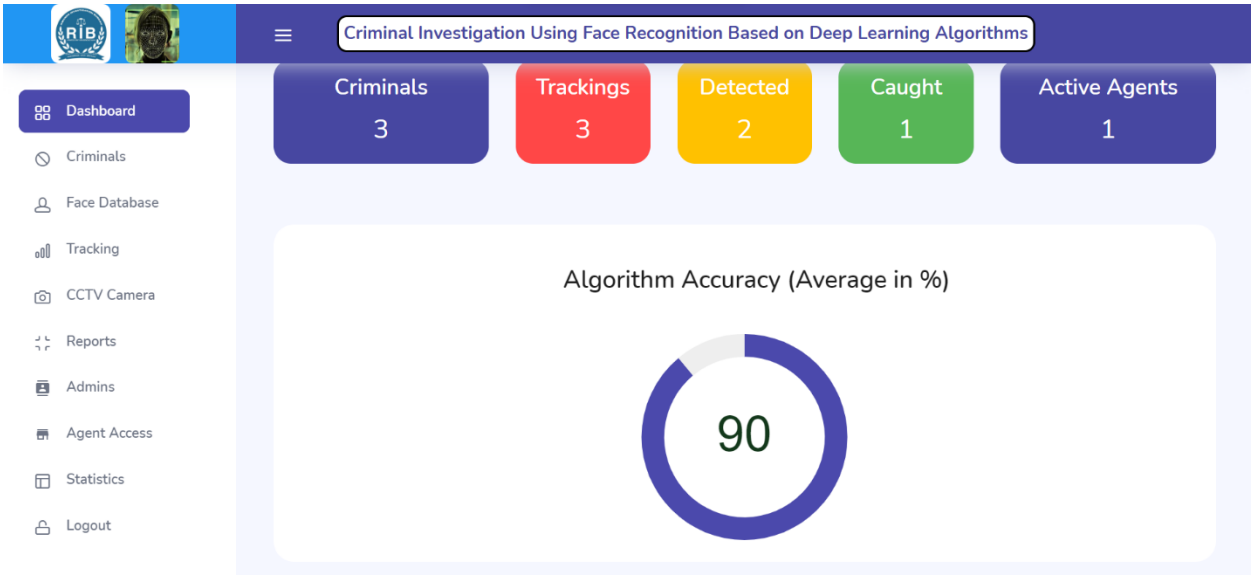


Figure 21: *Admin - Dashboard page*

Admin – Criminals' list page

This is the page which list all registered criminals and their information like the photo, name, identity, the gender with an option to delete a criminal and to export or print the list of criminal.

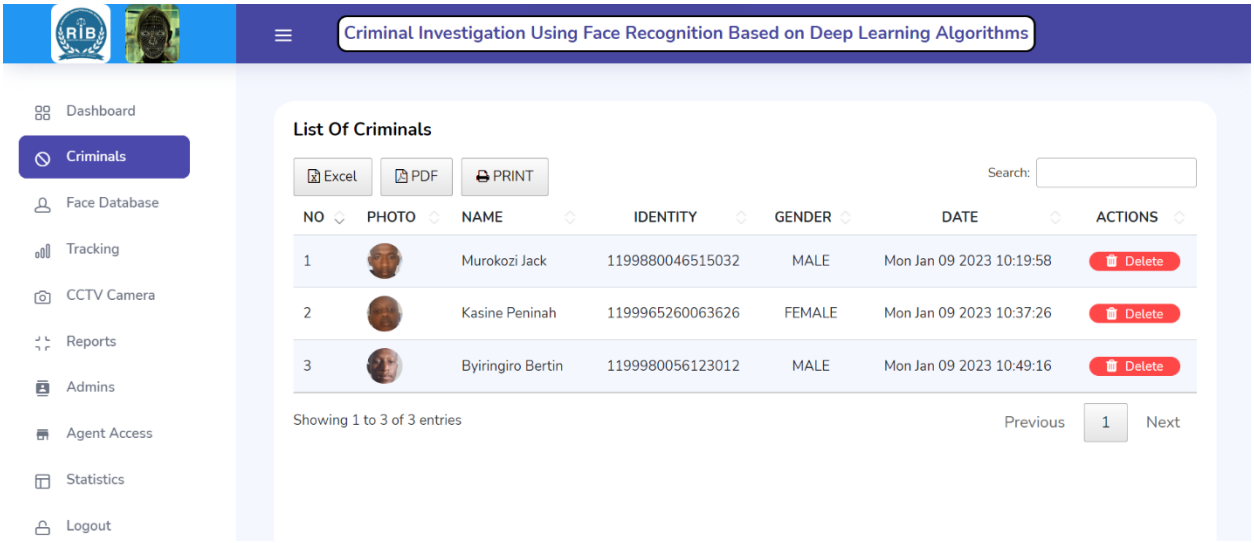


Figure 22: *Admin – Criminals list page*

Admin – Face Database page

The face page retrieves all faces of the registered criminals in the database by showing the last trained picture of each criminal, the name and the status whether a criminal is wanted or not.

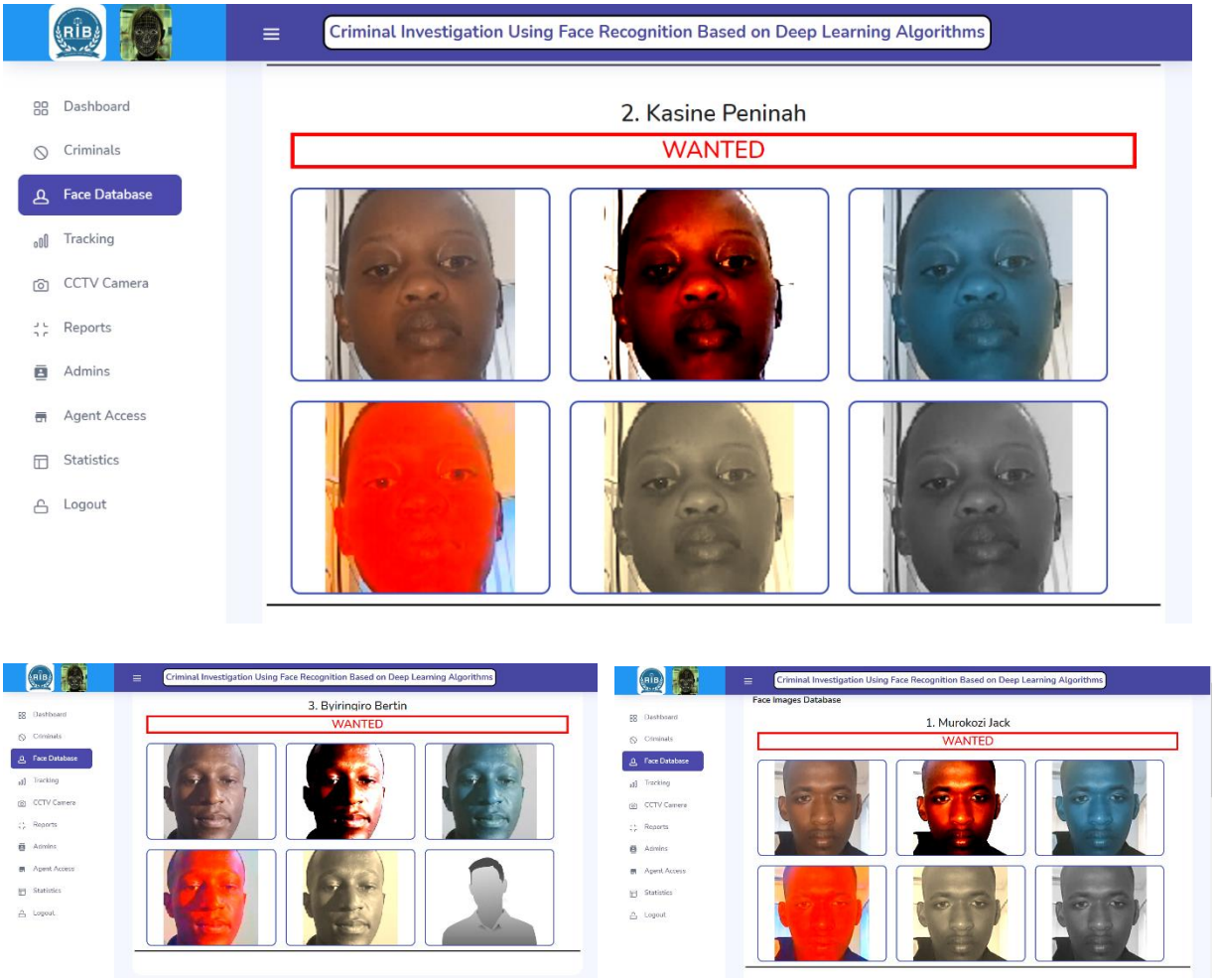


Figure 23: *Admin - Face Database page*

Admin – Tracking page

This a page which gives the administrator the option the start tracking a criminal and to view the status of criminals where is being tracked, detected or found.

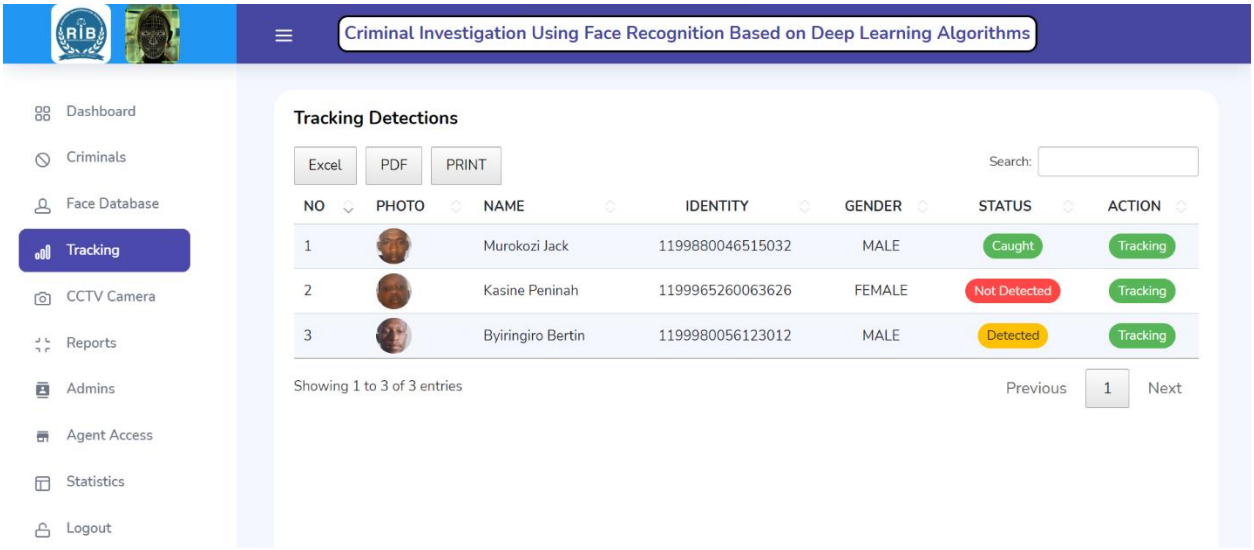


Figure 24: *Admin - Tracking page*

Admin – CCTV Camera page

This page shows the live output the CCTV Camera by showing the last time of detection and the information of the last recognized person like the name, gender, identity, photo and more importantly the accuracy at which the algorithm has detected and recognized that person on.

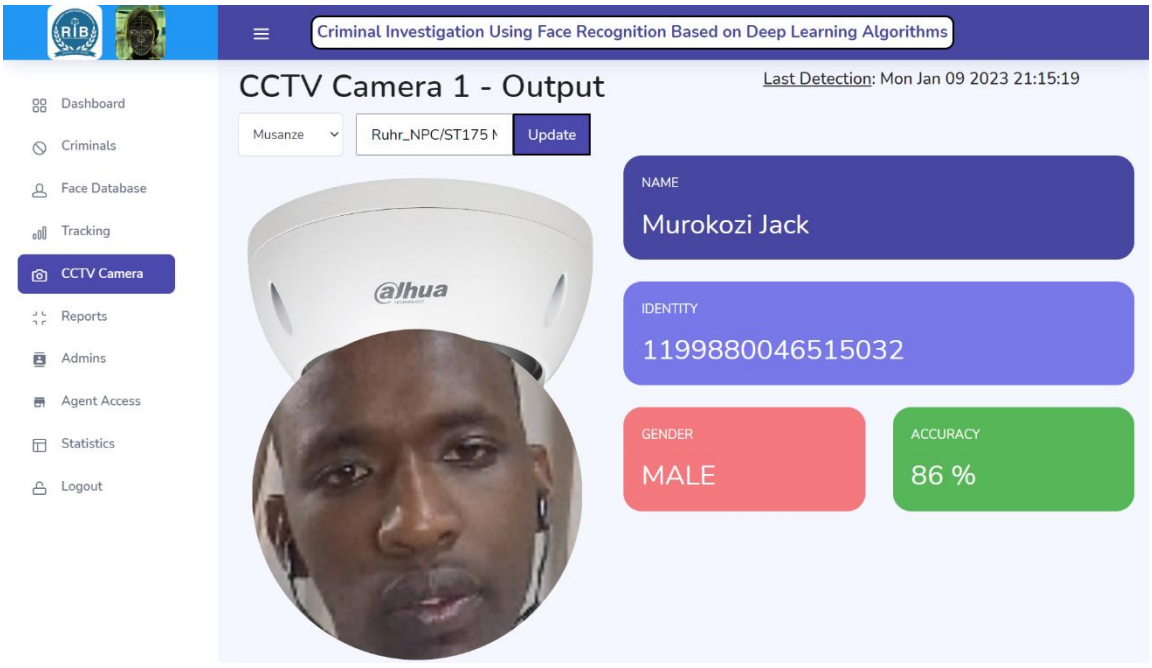
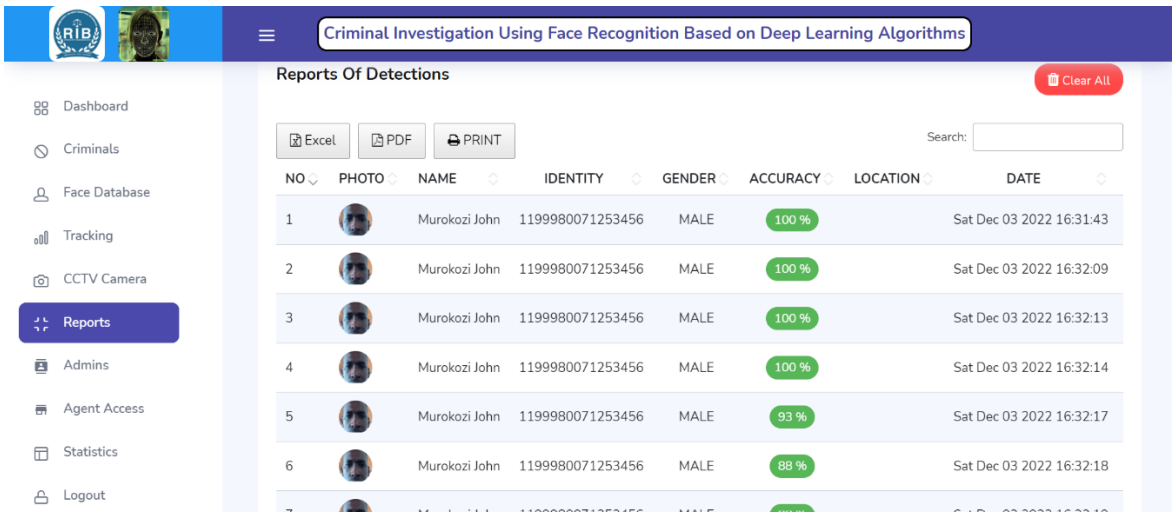
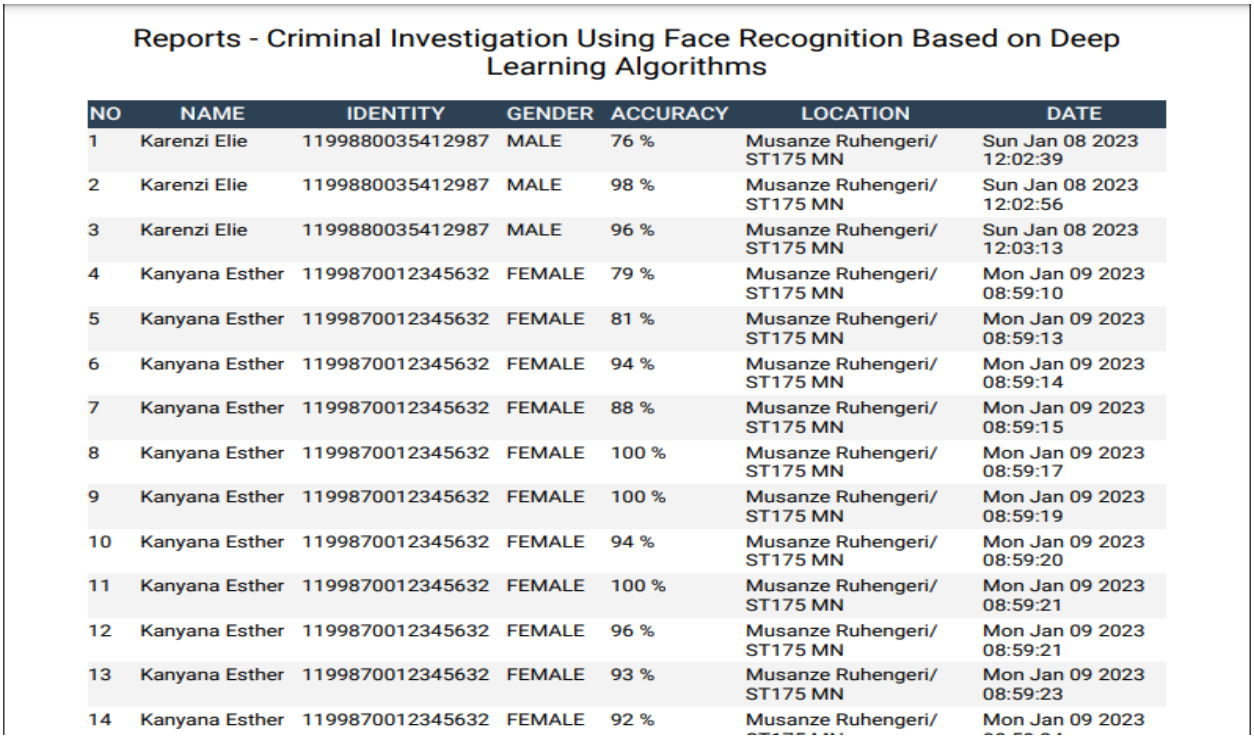


Figure 25: *Admin - CCTV Camera page*

Admin – Reports page

The reports page shows a list of all occurred detections from the CCTV Camera by showing all retrieved information of the person or the criminal including the photo, the name, the identity, the gender, the time & date of detection, the accuracy at which the algorithm recognized the face on, and the location of CCTV Camera. There is even an option to print or download a report as PDF or Excel file.





Reports - Criminal Investigation Using Face Recognition Based on Deep Learning Algorithms

NO	NAME	IDENTITY	GENDER	ACCURACY	LOCATION	DATE
1	Karenzi Elie	1199880035412987	MALE	76 %	Musanze Ruhengeri/ ST175 MN	Sun Jan 08 2023 12:02:39
2	Karenzi Elie	1199880035412987	MALE	98 %	Musanze Ruhengeri/ ST175 MN	Sun Jan 08 2023 12:02:56
3	Karenzi Elie	1199880035412987	MALE	96 %	Musanze Ruhengeri/ ST175 MN	Sun Jan 08 2023 12:03:13
4	Kanyana Esther	1199870012345632	FEMALE	79 %	Musanze Ruhengeri/ ST175 MN	Mon Jan 09 2023 08:59:10
5	Kanyana Esther	1199870012345632	FEMALE	81 %	Musanze Ruhengeri/ ST175 MN	Mon Jan 09 2023 08:59:13
6	Kanyana Esther	1199870012345632	FEMALE	94 %	Musanze Ruhengeri/ ST175 MN	Mon Jan 09 2023 08:59:14
7	Kanyana Esther	1199870012345632	FEMALE	88 %	Musanze Ruhengeri/ ST175 MN	Mon Jan 09 2023 08:59:15
8	Kanyana Esther	1199870012345632	FEMALE	100 %	Musanze Ruhengeri/ ST175 MN	Mon Jan 09 2023 08:59:17
9	Kanyana Esther	1199870012345632	FEMALE	100 %	Musanze Ruhengeri/ ST175 MN	Mon Jan 09 2023 08:59:19
10	Kanyana Esther	1199870012345632	FEMALE	94 %	Musanze Ruhengeri/ ST175 MN	Mon Jan 09 2023 08:59:20
11	Kanyana Esther	1199870012345632	FEMALE	100 %	Musanze Ruhengeri/ ST175 MN	Mon Jan 09 2023 08:59:21
12	Kanyana Esther	1199870012345632	FEMALE	96 %	Musanze Ruhengeri/ ST175 MN	Mon Jan 09 2023 08:59:21
13	Kanyana Esther	1199870012345632	FEMALE	93 %	Musanze Ruhengeri/ ST175 MN	Mon Jan 09 2023 08:59:23
14	Kanyana Esther	1199870012345632	FEMALE	92 %	Musanze Ruhengeri/	Mon Jan 09 2023

Figure 26: *Admin - Reports page*

Admin – Admins page

This page list of admins which are registered in the system and allow some operations on them like activation and deletion of any admin. All these operations on the admins can be performed by super admin only. Admins have access to control the CCTV Camera device which is responsible for scanning criminals faces.

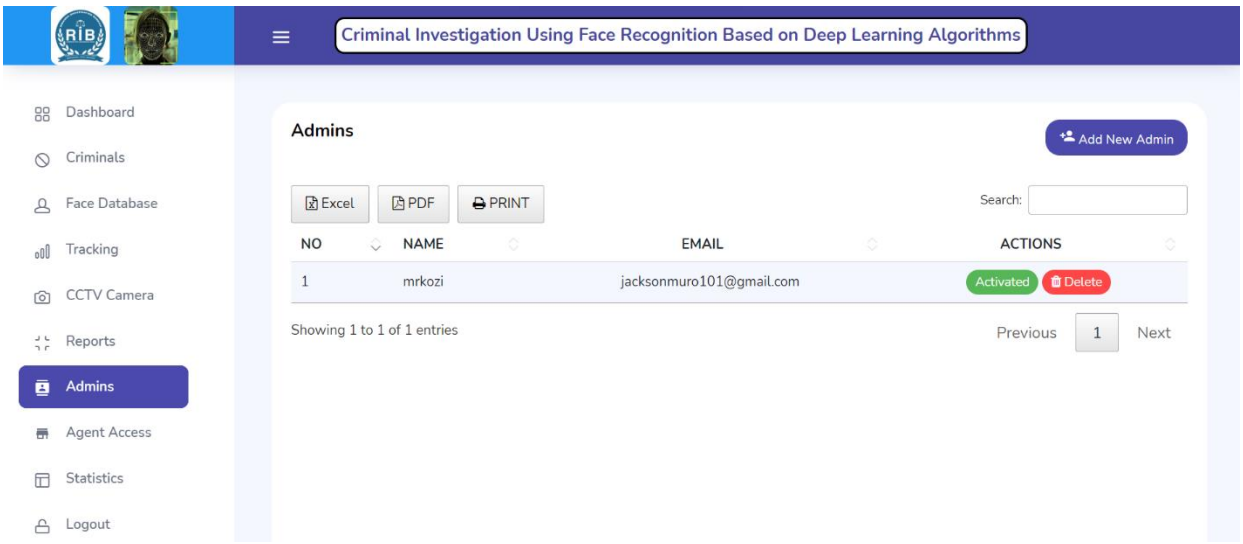


***Figure 27**: List of Admins with access*

Admin registration

The registration page is used to add new admins in the system which gives them access to control the CCTV Camera devices. The registration requires the name, email and default password. Then a password reset email is sent to the admin to be able to change his password.

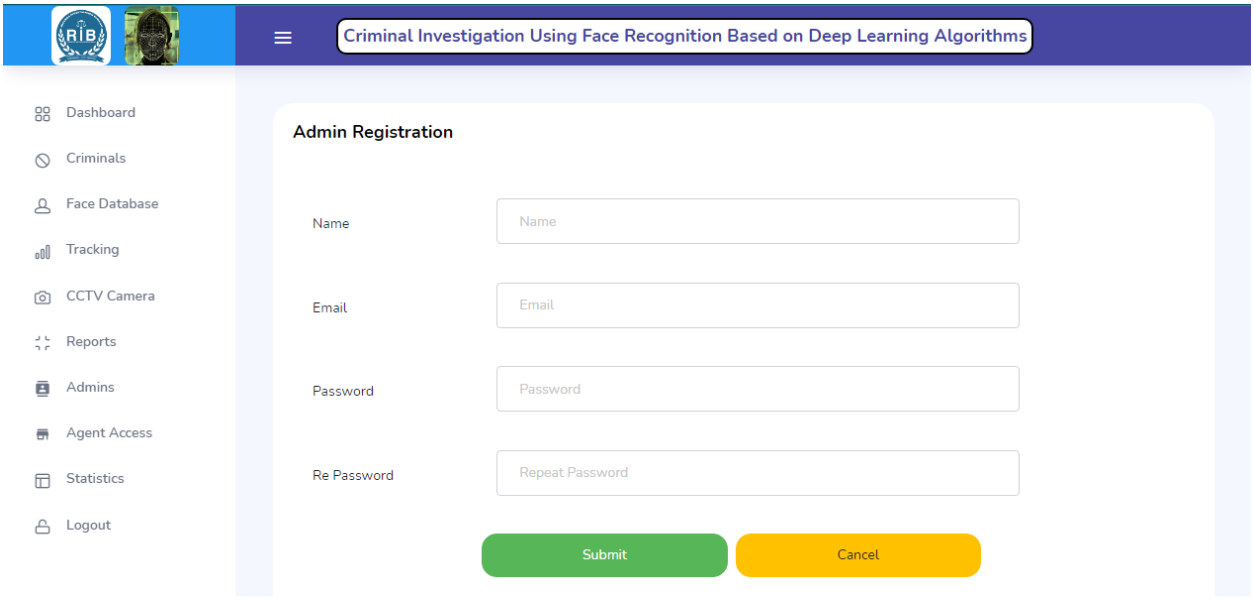


***Figure 28**: Admin registration*

Admin – Agent Access page

The agent access page shows a list of registered agents with their email, type and DPU with an option to active each agent as a way of giving them access to the agent mobile application.

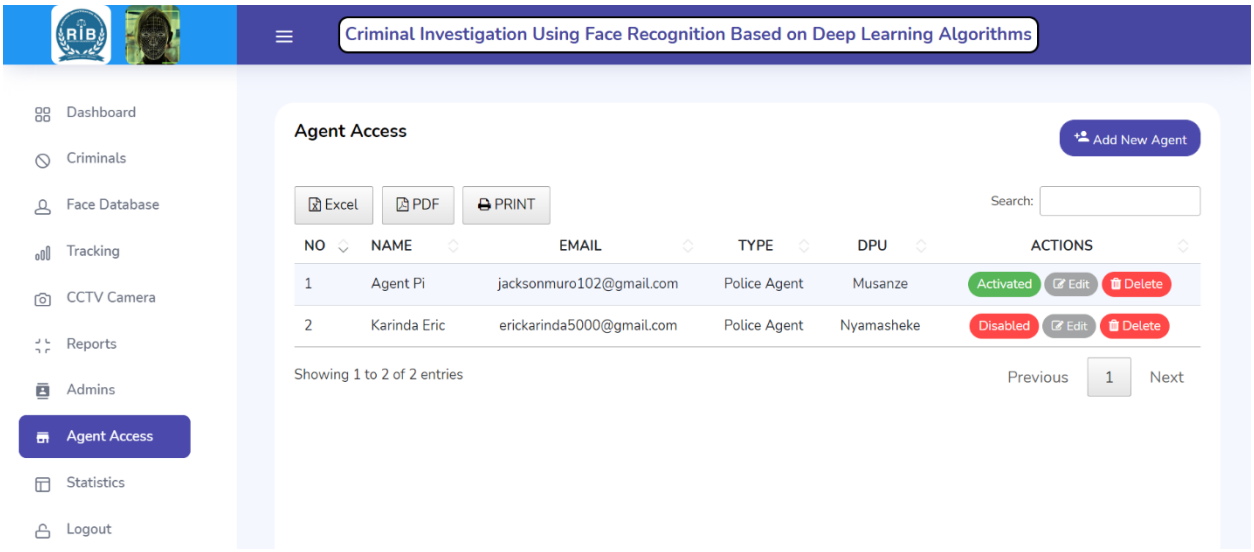


***Figure 29:** Admin - Agent Access page*

Admin – Add/Edit an Agent

This page gives the admin an option to add a new agent by providing the agent's name, email, type, DPU and the password. And then the system sends a rest email link for the agents to change to their own password. The admin can also use this form to modify data of an existing agent.

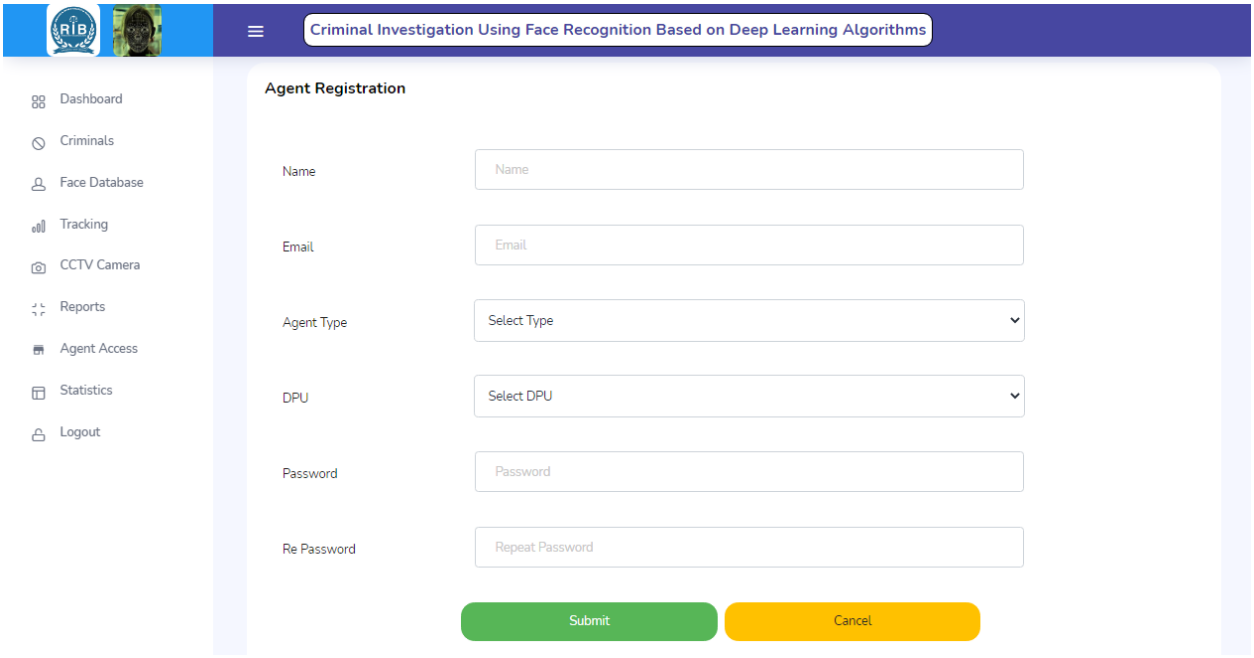


Figure 30: *Admin – Add/Edit an Agent*

Admin – Statistics page

The statistics page provides an overview of the system in form of graphs and analytics for instance here the pie chart shows the accuracies of the algorithm whereas the line graph show the rate at which the system is detecting on.

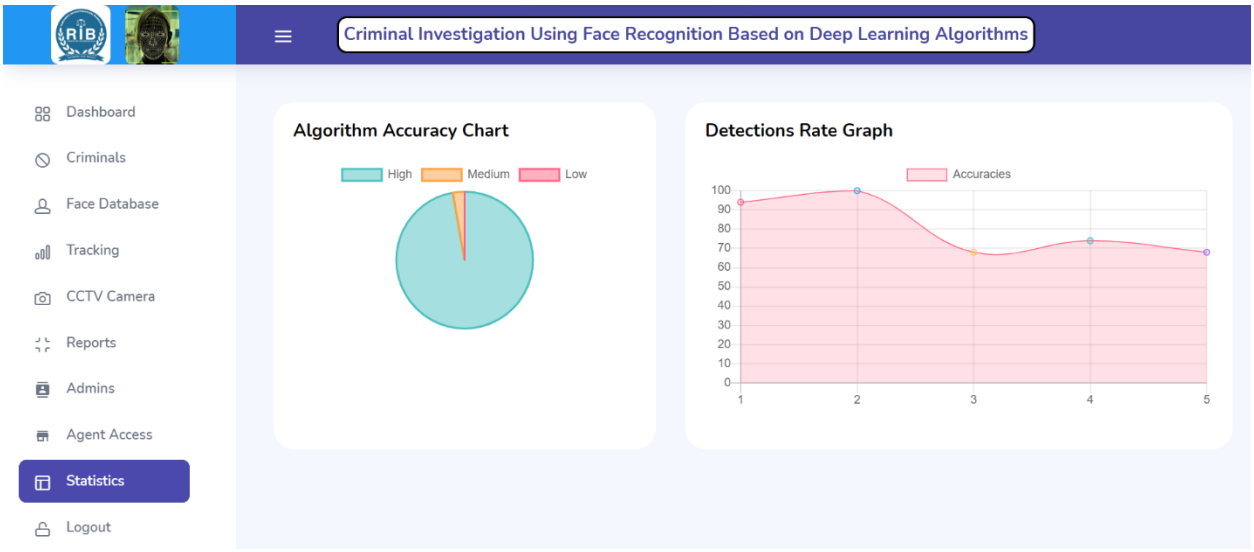


Figure 31: *Admin - Statistics page*

CHAPTER 5: CONCLUSION & RECOMMENDATION

5.1 Conclusion

Face Recognition Technology has the ability to aid in the resolution, prevention, and prosecution of crimes. More precisely, it might be beneficial for a variety of investigations, such as determining the identity of an ATM fraud suspect, searching for a terrorist in public places, combating child abuse, or even locating missing individuals. On the other hand, early evidence suggests that without sufficient control, face recognition technology might result in human rights violations and hurt civilians. That is why the government must be involved to ensure that it is used legally.

Face recognition based on deep learning algorithms has the potential to significantly improve the efficiency and effectiveness of criminal investigations. By automating the process of identifying suspects, face recognition can help law enforcement agencies solve cases more quickly and bring perpetrators to justice. However, it is important to carefully consider the potential limitations and biases of these algorithms and to develop clear guidelines and policies for their use. By increasing the diversity of the training data, regularly evaluating and updating the algorithms, increasing transparency, and providing training and support for law enforcement, we can ensure that face recognition is used responsibly and ethically in criminal investigations.

5.2 Recommendation

This improved version of the criminal detection system not only makes it easier for the investigation bureau to identify criminals, but also saves them time because the processes are automated in the system. Face detection utilizing Face Encodings is the innovative aspect of this Research Project. Another aspect is to increase training data diversity by improving the accuracy and fairness of face recognition algorithms, it is important to increase the diversity of the training data. This can be achieved by including a wider range of facial features, skin tones, and other characteristics in the training data. Also, to regularly evaluate and update algorithms, as face recognition algorithms continue to evolve, it is important to regularly evaluate and update them to ensure they are performing accurately and ethically. This can be done through the use of independent testing and by incorporating feedback from stakeholders.

For further research, we recommend that, because CCTV are static and not dynamic, we can incorporate drones which have camera to support the tracking and they might be moving around scanning people instead of waiting for the criminals to reach the place where CCTV are statically installed.

REFERENCES

[1] Ratnaparkhi, S. T., Tandasi, A., & Saraswat, S. (2021, January). Face Detection and [Recognition for Criminal Identification System. In 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 773-777). IEEE.

[2] Tappan, P. W. (1947). Who is the Criminal?. American Sociological Review, 12(1), 96-102.

[3] Tolba, A. S., El-Baz, A. H., & El-Harby, A. A. (2006). Face recognition: A literature review. International Journal of Signal Processing, 2(2), 88-103.

[4] Bradski, G., & Kaehler, A. (2000). OpenCV. Dr. Dobb's journal of software tools, 3, 120.

[5] "Face Recognition in Criminal Investigations" by Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar, IEEE Transactions on Information Forensics and Security, Vol. 12, No. 6, pp. 1466-1477, 2017.

[6] "Assessing the accuracy of face recognition technology in forensic applications" by M.A.Bruce, C.H.Burton, J.W.Wilson, Science & Justice, Vol.50, pp. 127–135, 2010.

[7] https://www.rib.gov.rw/index.php?id=371#:~:text=US%20ON%20TWITTER-,MOST%20WANTED

[8] The 68 specific human face landmarks, ResearchGate, https://www.researchgate.net/publication/331769278/figure/fig4/AS:756348480417792@1557338938468/The-68-specific-human-face-landmarks.ppm

[9] Jain, A. K., Dass, S., & Nandakumar, K. (2019). Face recognition: A comprehensive study. Pattern Recognition Letters, 116, 3-20.

[10] Wang, H., & Liu, X. (2020). Deep learning-based face recognition: A survey. ACM Computing Surveys, 53(3), 1-34.

[11] Li, H., Li, Y., & Chen, S. (2019). Face recognition using deep learning: Challenges and prospects. IEEE Access, 7, 48958-48975.

[12] Chen, X., Huang, K., & Li, Z. (2018). A survey on deep learning-based face recognition. Frontiers of Information Technology & Electronic Engineering, 19(2), 195-212.

[13] Zhang, D., Chen, S., & Li, H. (2019). Face recognition: A survey of challenges and solutions. ACM Computing Surveys, 52(1), 1-36.

[14] Patel, V. M., & Patel, D. R. (2020). A review of deep learning techniques for face recognition. Neural Computing and Applications, 32(4), 1265-1278.

[15] Du, Y., & Li, J. (2018). Face recognition using deep learning methods: A survey. IEEE Access, 6, 45151-45169.

[16] Liu, W., Chen, X., & Li, Z. (2019). Deep

[17] Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). Imagenet classification with deep convolutional neural networks. In Advances in neural information processing systems (pp. 1097-1105).

[18] Girshick, R., Donahue, J., Darrell, T., & Malik, J. (2014). Rich feature hierarchies for accurate object detection and semantic segmentation. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 580-587).

[19] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444.

[20] Simonyan, K., & Zisserman, A. (2014). Very deep convolutional networks for large-scale image recognition. arXiv preprint arXiv:1409.1556.

[21] He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 770-778).

[22] Szeliski, R. (2010). Computer vision: algorithms and applications. Springer Science & Business Media.

[23] Bradski, G., & Kaehler, A. (2008). Learning OpenCV: Computer vision with the OpenCV library. O'Reilly Media, Inc.

[24] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.

[25] Géron, A. (2017). Hands-on machine learning with Scikit-Learn and TensorFlow: concepts, tools, and techniques to build intelligent systems. O'Reilly Media, Inc.

[26] Karpathy, A., & Li, F. (2014). Deep visual-semantic alignments for generating image descriptions. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 3128-3137).

[27] Kingma, D. P., & Ba, J. (2014). Adam: A method for stochastic optimization. arXiv preprint arXiv:1412.6980.

[28] Bojarski, M., Del Testa, D., Dworakowski, D., Firner, B., Flepp, B., Goyal, P., ... & Jackel, L. D. (2016). End to end learning for self-driving cars. arXiv preprint arXiv:1604.07316.