A CAL Project Report

on

CRIMINAL DETECTION USING FACIAL RECOGNITION TECHNIQUES

to be submitted in partial fulfilling of the requirements for the course on

Object Oriented Software Development – CSE4028

(G1)

By

Baibhav Singh 17BCE2359

Zisan Aalam 17BCE2361

Yominesh Giri 17BCE2363

Rinoj Raj Nakarmi 17BCE2364

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Fall Semester 2020-2021

TABLE OF CONTENTS

ABSTRACT

1. Introduction ……. 04
2. Survey, Analysis ……....…….…… 05
3. Design of Diagrams & Prototype Design ……..…….. 14
4. Development of Model …….....……. 22
5. Conclusion ……....…… 32
6. References ……. 33

ABSTRACT

Facial recognition is an area of biometric based technology that's been the center of research for many years. Facial recognition can be used in the area of security, for recognition etc. This project is for the facial recognition done for the criminal recognition where the security expert will input an image of the person and based on databases, image processing algorithm and training process identifies the criminal. The sole purpose of this software is to detect the facial structure of an individual with high accuracy.

1. INTRODUCTION

This project is for the facial recognition done to recognize criminals where the security expert/admin inputs an image of an individual and based on databases, image processing algorithm and training process identifies whether the individual has a criminal record or not. The system will first preprocess the image which will cause unwanted elements such as noise to be removed from the image. After that, the system will then classify the image based on its landmarks for example, the distance between the eyes, the length of the jaw line, etc. Then, the system will run a search through the database to find its perfect match and display the output. This work is focusing on implementing the system for criminal identification.

The sole purpose of this software is to detect the facial structure of an individual with high accuracy. This software as being user-friendly and simple to maneuver will help all the detective companies or any other company for that matter which cannot afford expensive hardware and software to detect whether their employee or an individual has a criminal record or not. Its objective is to spot a criminal face in the internet database and the records of the criminal database or in a crowd of unknown individuals. The goal is that it could be used by companies all around to secure themselves and small crime investigation companies all around the world could use it as well.

2. SURVEY and ANALYSIS

a. A Survey of Face Recognition Techniques

Rabia Jafri* and Hamid R. Arabnia*

Facial Recognition is challenging topic in the field of image processing and computer vision, and has received great attention from researchers in past years. In this paper, an outline of a portion of the notable strategies in every one of these classifications is given and a portion of the advantages and disadvantages of the plans referenced in that are analyzed. Besides, a conversation laying out the motivator for utilizing face acknowledgment, the uses of this innovation, and a portion of the problems afflicting current frameworks with respect to this undertaking has likewise been given. This paper additionally makes reference to the absolute latest calculations created for this reason and endeavors to give a thought of the best in class of face recognition technology.

b. Face Recognition: A Survey

Muhammad Sharif1, Farah Naz1, Mussarat Yasmin1, Muhammad Alyas Shahid1 and Amjad Rehman2

Facial recognition has gained lots of importance in the application of image processing furthermore availability of viable technologies in the filed have contributed a great deal of it. Despite of different challenges in this field it has gained huge amount of recognition and attention from researcher from different fields. His part also highlights the most commonly used databases, available as a standard for face recognition tests. AT & T, AR Database, FERET, ORL and Yale Database have been outlined here. While in the second part of this survey a detailed overview of some important existing methods which are used to dealing the issues of face recognition have been presented. Said methods include Eigen face, Neural Network (NN), Support Vector Machine (SVM), Gabor Wavelet and Hidden Markov Model (HMM).

c. Facial Recognition in Criminal Investigation

Samuel Ehidiamen Agaga

There is no doubt one of the major social economic vices of this century is the crime. The government alone cannot find criminals on time, with available number of officers as compared to population density in developed cities. Technology advancement has shown hope to mitigate these problems. In this research paper, we have discussed about how facial recognition technologies can be used in different places so that it is easy to find the criminals. The motivation behind the criminal act is reinforced if the culprit is aware there are no ways of making his or identity known. Achieving a face recognition technology that can recognize humans will certainly be a lion stride against the emergence of crime in today's world. The goal of this study is to research into facial recognition technologies and evaluate how well they are fit for use in criminal investigation.

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

Nurul Azma Abdullaha), Md. Jamri Saidi, Nurul Hidayah Ab Rahmanb), Chuah Chai Wenc), and Isredza Rahmi A. Hamidd

In developed countries of identification of criminal is basically done by thumbprint identification. However, this type of technique is easily exploited because criminals are getting clever and don't leave any finger prints on the scene. With the help of CCTV surveillance, installed in public and private the footage can be used to identify suspect on scene.

e. Advanced Facial Recognition for Digital Forensics

Hiba Al-kawaz!", Nathan Clarke, Steven Furnell' , Fudong Lit. and Abdulrahman

Forensic facial recognition has become an essential requirement in criminal investigations due to the advent of electronic devices such as CCTV, digital cameras, mobile phones, and computers and the huge volume of content that exists. Forensic facial recognition goes beyond facial recognition in that it deals with facial images under unconstraint and non-ideal conditions, such as poor image resolution, facial orientation, illumination, expression, and the presence of accessories. A large variety of facial recognition algorithms exist; each condition have a huge impact on the recognition performance.

Companies and cities all over world are experimenting with artificial intelligence to reduce and prevent crime, and to more quickly respond to crimes in progress. The ideas behind many of these projects is that crimes are relatively predictable; it just requires being able to sort through a massive volume of data to find patterns that are useful to law enforcement. This type of technology was not possible a few decades ago. With the advancement of machine learning in recent years, we have seen a rise in technology in this particular area *("AI for Crime Prevention and Detection – 5 Current Applications", 2019, February 2)*. We are going to focus solely on crime detection software which uses face detection techniques. We look at the existing systems/software that already exists in the market.

a) Neurotechnology is a product based company providing software and services in the field of biometric based recognition. Verilook is one of their products that offers face detection, simultaneous multiple face recognition and fast face matching features. It can recognize partially occluded faces (accessories), recognizes emotion. It can configure a 180 degree head roll.

For reliability tests, they have used many public datasets like the NIST Special Database 32.

Verilook has the same architecture as that of PCA-SVM, DCT-GMM. It uses normalized and cropped face images of size 64 x 80 to train a PCA vector space. This leads to a system where the original image space of 5120 dimensions is reduced to 249 dimensions *(Vera-Rodriguez, J. Fierrez, P. Tome, and J. Ortega-Garcia, 2010)*. Similarity scores are computed in this PCA vector space using a SVM classifier with linear kernel.

To analyze this product, three scenarios are considered: close distance in which the shoulders may be present, medium distance which includes the upper body and far distance includes the full body. For this analysis, NIST MBGC v2.0 dataset is used. The results shows the segmentation errors increase significantly across scenarios, from only 1.43% in close distance to 82.57% in far distance. Segmentation errors mean that the Verilook software could not find a face in the image. Another data statistic that was computed for the three scenarios was the average face quality index provided by Verilook (0=lowest, 100=highest), and according to that 73.93 for close, 68.77 for medium and 66.50 for far distance was observed *(Vera-Rodriguez, J. Fierrez, P. Tome, and J. Ortega-Garcia, 2010)*.

For verification test, three protocols were designed.

a) The close2close gives an idea of how the system performs when a close distance image is used.

b) Close2medium and close2far use medium distance and far distance images.

The results show that Verilook is the best in close2close with an EER of around 7%. It is worst for closettofar with an EER of 40%.

b) Amazon Rekognition is a fully managed web service that provides image and video analysis using deep learning models.

Rekognition Image uses deep neural network models to detect and label thousands of objects and scenes in your images. Rekognition Video is a video recognition service that detects activities; understands the movement of people in frame; and recognizes objects, celebrities, and inappropriate content in videos stored in Amazon *S3 (Amazon Rekognition FAQs)*.

The face detection algorithm is most effective on frontal faces. It uses DetectFaces API of AWS that returns the facial landmarks of the face.

Analysis

The control experiment provides a basis for understanding how well these commercial systems perform by using standardized photography from publically available facial databases. The results of this experiment can then be directly compared to experiment two which focusses upon using more forensically realistic images – where numerous facial recognition challenges are likely to co-exist simultaneously. The whole experiment is divided into three categories *(Hiba Al-kawaz, N. Clarke, Abdulrahman Alruban, 2018)*.

a) For the first experiment the CAS-PEAL-R1 Chinese face dataset was utilized as it simulates several facial recognition challenges (i.e., pose, expression, lighting, and accessories).

b) In the second experiment, a more realistic dataset is required that challenges al the conditions (lighting variation, accessories). Also the images used are varying to different constraints (day and night, photo taken between different time periods, far and close).

Results:

a) For the accessories category, Amazon Rekognition achieved an IR score of 98.76% while Neurotechnology achieved a score of 92.61%. Regarding the lighting and poses condition, Neurotechnology received an IR score of 63.42% and Amazon Rekognition received an IR score of 83.95%. Neurotechnology performance dropped significantly to 31.31% for the pose condition while Rekognition received a score of 85.73%.

Subset	**IR at Rank1 (%)**	
	Neurotechnology	**Amazon Rekognition**
Accessories	92.61	98.76
Expression	98.31	99.78
Lighting	63.42	83.95
Pose	31.31	85.73

b) For the second experiment, realistic datasets were used and hence Neurotechnology got the lowest of 6.6% and amazon Rekognition received the score of 48.24% *(Hiba Al-kawaz, N. Clarke, Abdulrahman Alruban, 2018).*

System needed:

The system we are searching for is a small, portable, cheap system that can be used in mobile devices as well as PCs and laptops and which don't require extensive software installation with minimal features. The only feature we are interested is to detect a face and run through the database to check whether the individual has had a criminal record or not. The software is for organizations and crime department that may need to run background checks on employees or people inside their workplace. The organization can register a criminal (feature for criminal departments) or just check through the database to see if the individual is a criminal or not.

Survey Analysis

We have distributed a survey to see how our potential users may react to the system proposed or such software for that matter. The survey paints a picture on how seriously or securely people take their security and how much they know about their colleagues and employees. Through the survey, we can analyze the security arrangements or an individual's perspective towards their own security in different parts of sectors (private, public, corporate, etc.). By knowing our potential user on somewhat private level, we can understand their requirement and understanding which can help us build a system and add features accordingly.

We concluded that more than 60 percent of our potential users are employed under corporate or small privately owned organizations. Rest of them either works for government organizations or in service sectors like hotels and hospitals. We wanted to know how well do they know about their colleagues. 38.5% knew almost everyone. That concludes that they are confident about their workplace being safe. In corporate sectors and governmental organizations, 34.6% were aware about their colleagues limited to their specialization. We found that mostly technical people in the survey knew very limited people from their workplace.

Also, another secure things was that 53.8% people admitted that their workplace deployed CCTV cameras. It may be important for our software as the CCTV footage can be used in a beneficial way. The CCTV cameras were deployed mostly in corporate, NGO sectors and government sectors. Though, more than 45% of the people admitted that their company commits

to background research before hiring an employee, it was shocking to find out that most small organizations and some service sectors including a government organization commit to background research often and no policy exist on the same. The survey also concluded that most people (80%) use devices like laptops or workplace PC. We can design our software around that.

Now after basic information, we wanted to find some specific answers related to our field of interest. Our software after detecting the image (and if criminal) displays a page with all information on the particular individual. So, 69.2% of them agreed that the important information must be displayed first in the page and the additional/advanced information should be displayed in the page that follows. An interface designed around the same can be beneficial. We also wanted to know how often people use their camera on their phone (for our camera feature) and found that 69.2% of them take pictures when the weather favors them.

Now, we questioned people about their detective instincts and how often they go to the web to investigate on an individual. More than 60% agreed they investigated an individual online depending on the reason and out of them most people agreed that their search result were barely accurate but found information they could narrow down to.

Now for our facial recognition database feature, we asked couple of questions regarding how sensitive they felt about their own security. More than 50% felt very sensitive and valued privacy more but at the same time 73% of them couldn't care less when their face was captured in CCTV or their reaction when they found a CCTV in public. Regarding their safety, 34.6% barely checked on their digital footprint online meaning they have no idea what they can find on themselves on the internet. Only 11.5% were really serious about their digital footprints though earlier, more than 50% were very sensitive towards their privacy.

At last, we ended the survey by asking whether they had committed any minor crimes knowingly/unknowingly. We framed the options around crimes that could be captured by CCTV or their internet history. 46.2% of them generally crossed lanes and most of them were related to driving. Only about 19% of them indulged in illegal downloading/piracy.

After the survey results, we came up with the following conclusion. Our software may be appreciated in organizations that are small/startups and few of the corporate sectors. People limited to their specialization in government and service sectors could also appreciate our

software (mostly technical people). Also, most people are around their laptops and workplace PC most of the time so more effort can be made towards developing a system that runs of those platforms. Also more than 60% users use their camera most often so we could build a system that can also run on mobile platforms. Designing the user interface, we can agree on the result that more than 69% of them wants the information with multiple pages.

We can insure the information is accurate and to the point to solve their accuracy problems. At last but not the least, our software could really prove beneficial to organizations that conduct no background research on their potential employee. It could be helpful to them to secure their workplace from any criminal environment.

3. Design of Diagrams

USE CASE

Criminal detection system allows the security expert or the user to input an image of the suspected person and find out if the person is criminal or not. We are focusing mostly in workplace that don't follow background research policy or do not have CCTV according to the survey done earlier.

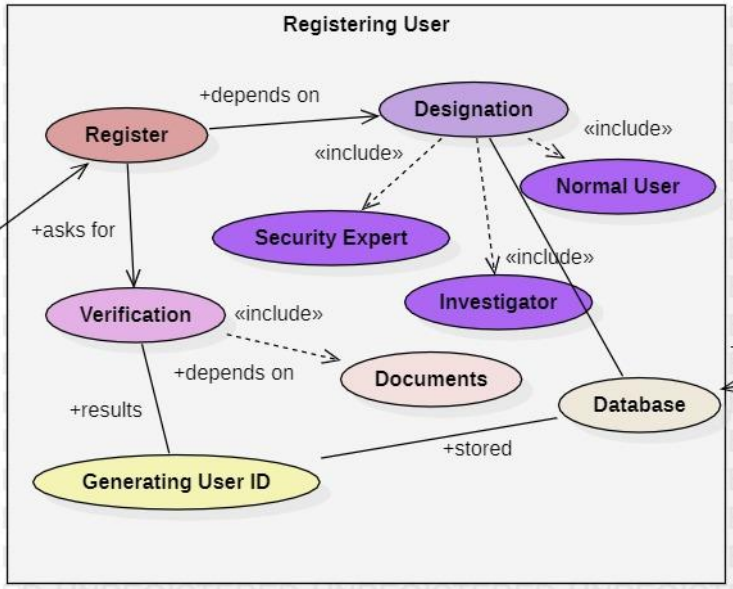
We have divided our user classes to three categories.

i) **Security Expert:** They may be the head of a criminal investigation department or a security consultant. They can register criminal into the system.

ii) **Normal User:** They are usually the head of private companies or small organization that we are mostly focusing on. They can use the image input and the video input features of the software but cannot register a criminal.

iii) **Investigator:** They may be a private investigator assigned to look out for a suspected person or a member of the criminal department of the city. He/she is also eligible to register criminal into the system.

Now, the first and foremost use case is to register the users into the system. As we have divided our users into three categories, we need to verify them to assign them roles and eligibility. We can verify them with the help of KYC based verification to confirm their designation.



Use case for registering user

After the confirmation is done, the system returns a user ID which can now be used to login into the system.

The system has three main features.

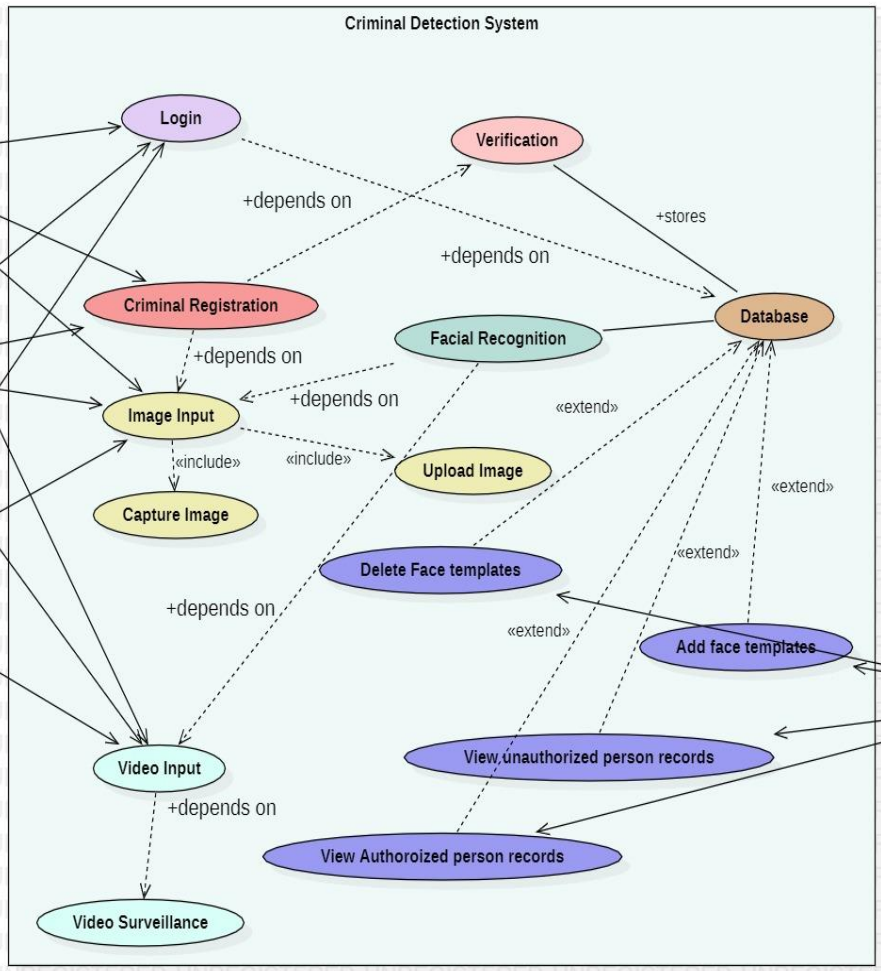
i) **Register Criminal:** This can only be accessed by the security expert and the investigator. To complete the process of this feature, the user needs to fill the required information and attach image.

ii) **Detect through image:** This is a feature through which we can detect the face of the suspected using an image. It can be both captured and attached. So we have two use case that is included in the image input.

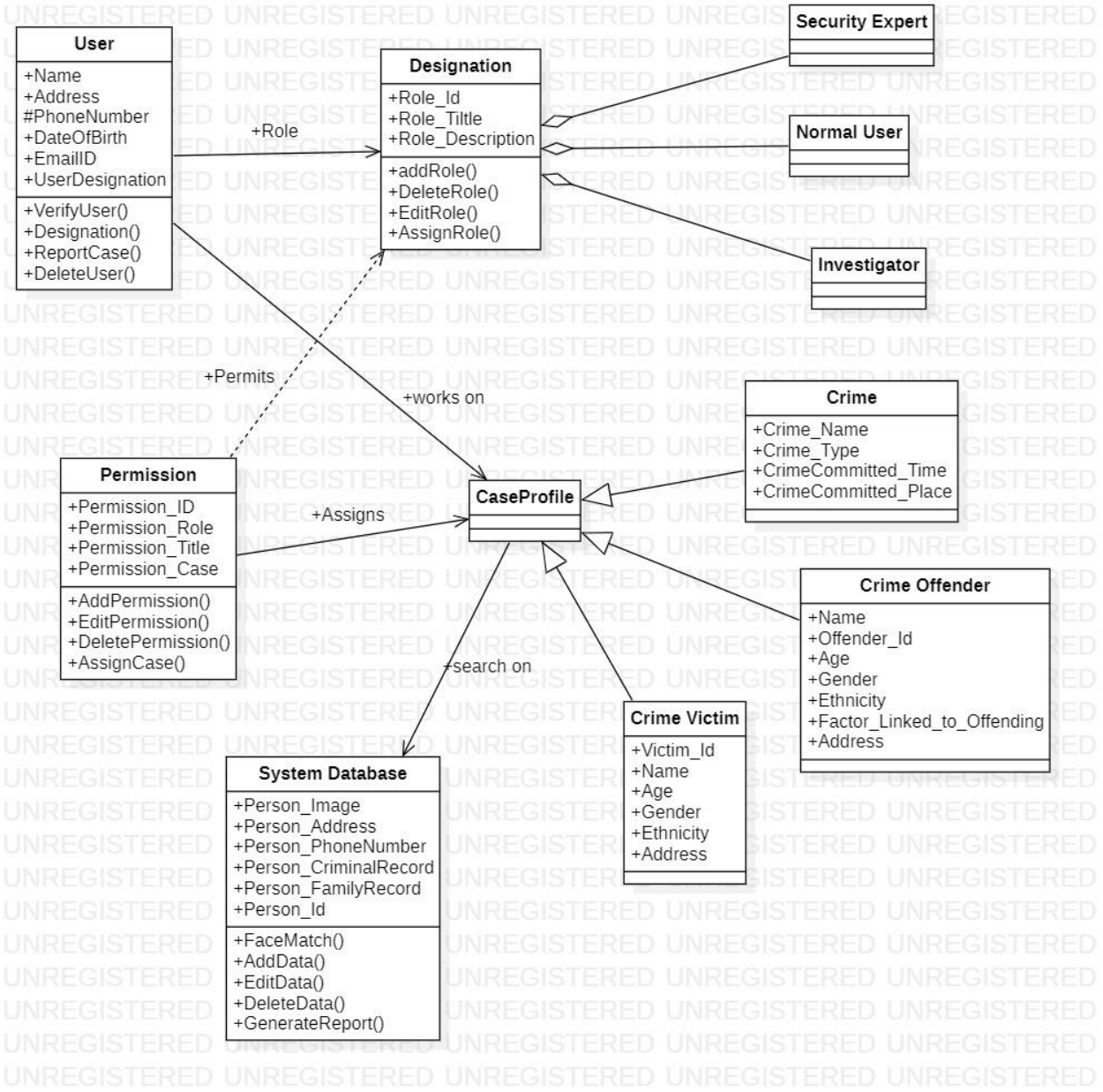
iii) **Detect through video:** This is a feature through which we can detect the face of the suspected using video surveillance. For that, we need to pause the surveillance before capturing the image and sending it for verification.

The system admin can retrieve the records from the database and add or delete the facial templates from the database. He/she can also view the authorized and unauthorized personnel records.

The complete use case is shown below:



CLASS DIAGRAM



Class Description

User class: This class contains the user information on user like name, address, phone number, designation etc. It performs operation like verification of user, check designation, report a case and delete user details.

Designation Class: This class gives us details about user role, user title and description and performs operation like addRole, editRole, deleteRole and assign role. This class is composition of three other classes meaning the roles can be:

a. **Security Expert Class**
b. **Normal User Class**
c. **Investigator Class**

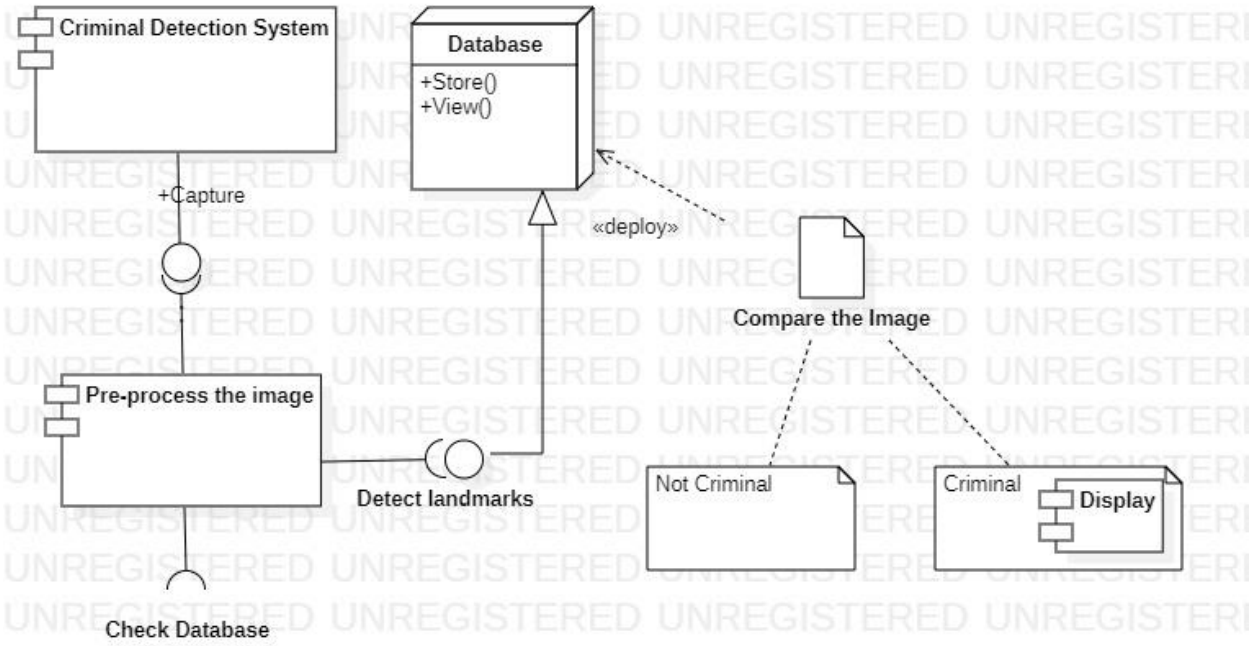
Permission Class: This class depends on Designation Class. Based on user role, user will be handed a permission on what cases to handle and kind of role to perform on cases.

Case Profile: This class gives us complete details about crime, crime offender and crime victim. It consists of three class:

a. **Crime:** This class tells us about crime name and type and it further explains about crime committed time and place
b. **Crime Offender:** This class tells us about offender who committed the crime like name, age, address etc.
c. **Crime Victim:** This class gives details about victim like name, age, address etc.

System Database: This is the class where many people data are stored in the form of image as well. It contains person face, name, address and age. So when we have to search offender, we run that offender face on our system and in case of matching face we retrieve the information. we can add new data into this class.

COMPONENT DIAGRAM



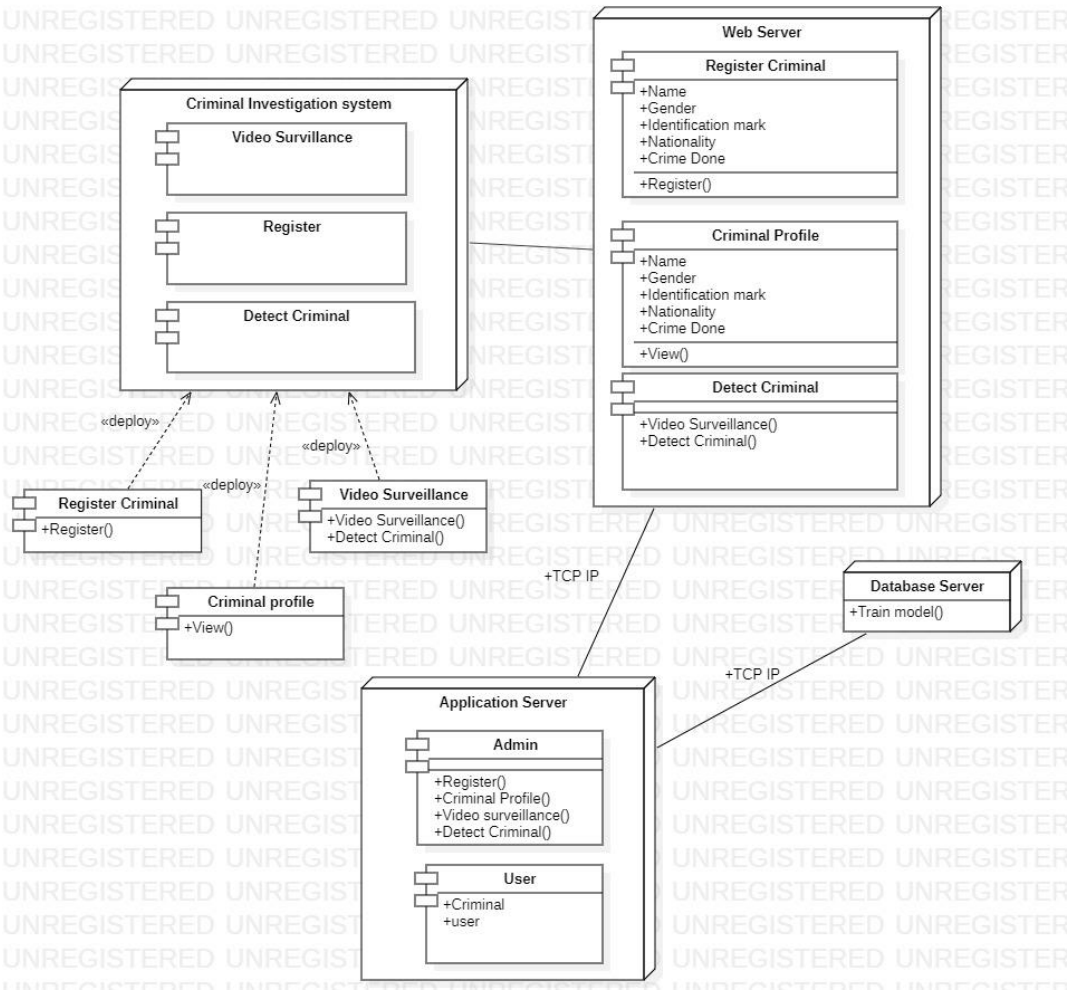
The component diagram basically depicts how components are wired together to form larger components or software systems.

Here the criminal detection system component diagram shows components, provided and required interfaces, ports and relationships between, system, processing model, and database. The basic components of component diagrams are:

- Criminal Detection System
- Database
- Processing model

The features of this system component diagram are you can easily register new criminal into database with few sample images to train the database. We can also view any criminal's details from the database. When criminal is identified from the live footage their details can be displayed easily. If there is no criminal in live footage then it will be discarded. The main Database is going to have store and view function.

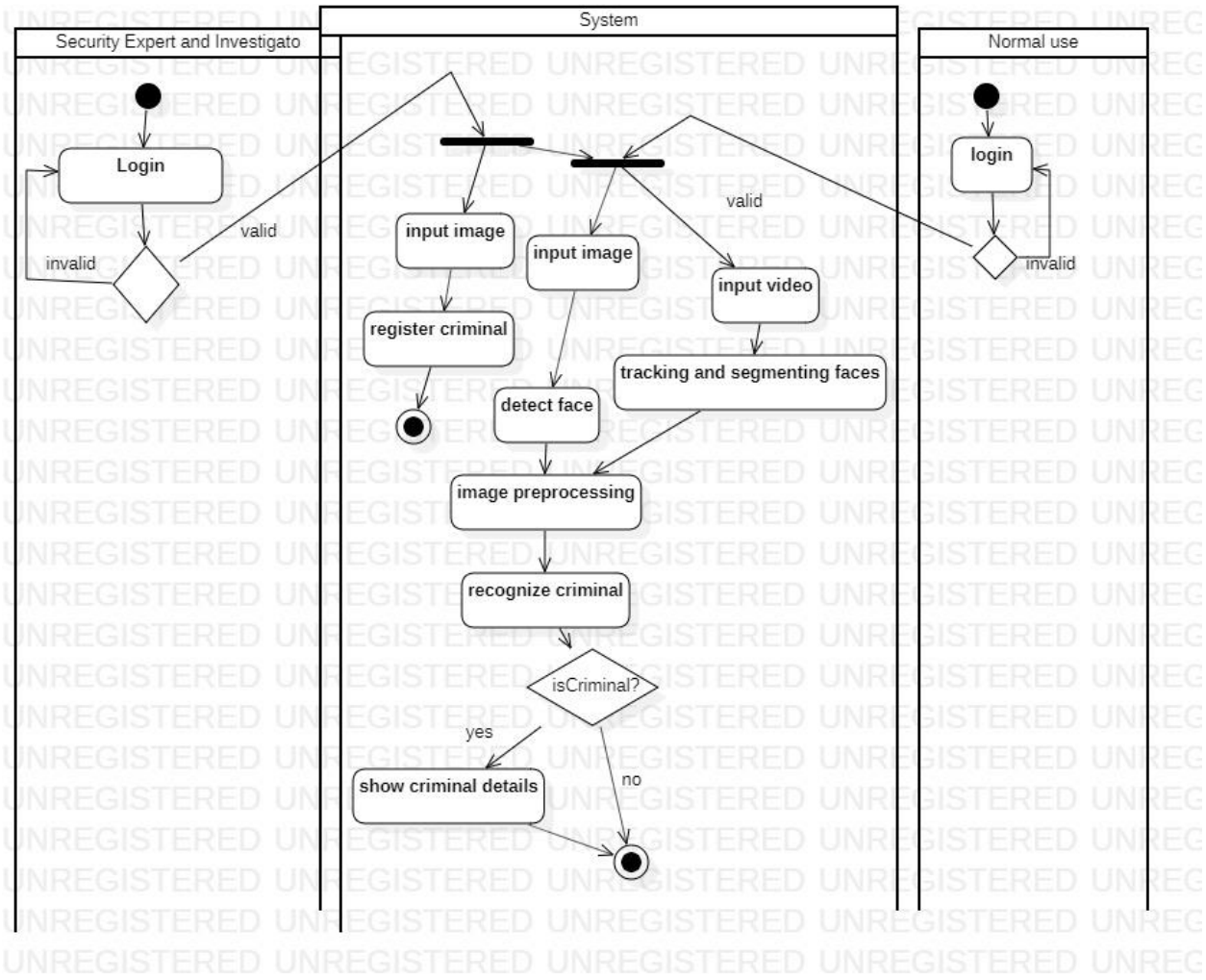
DEPLOYMENT DIAGRAM



The deployment diagram in models the physical deployment of artifacts on nodes.

The deployment diagram consists of execution architecture of the system. So basically, the main execution architecture of Video Surveillance, registering the criminal, and finally detecting the criminal etc. The backend architecture of this system consists of Web server, Application server, and database. The video surveillance is going to contain get live footage from the Web cam and then it will do identify the image in the surveillance with the database trained images to check whether there are any criminals in live footage or not. Second, we have registering new criminal with required information like name, gender, identification mark, nationality, crime done until that date. There is function like register which can be deployed. The last one is detecting criminal from the input image.

ACTIVIY DIAGRAM



The user roles are divided into three categories.

a) Security Experts
b) Investigators
c) Normal User

Security Experts and Investigators have the permission to register criminal while the normal users can only use the facial recognition feature.

After the criminal is registered in the database, the users can finally use the detect face by image or by video feature which is shown in the diagram above.

4. Development of a Model

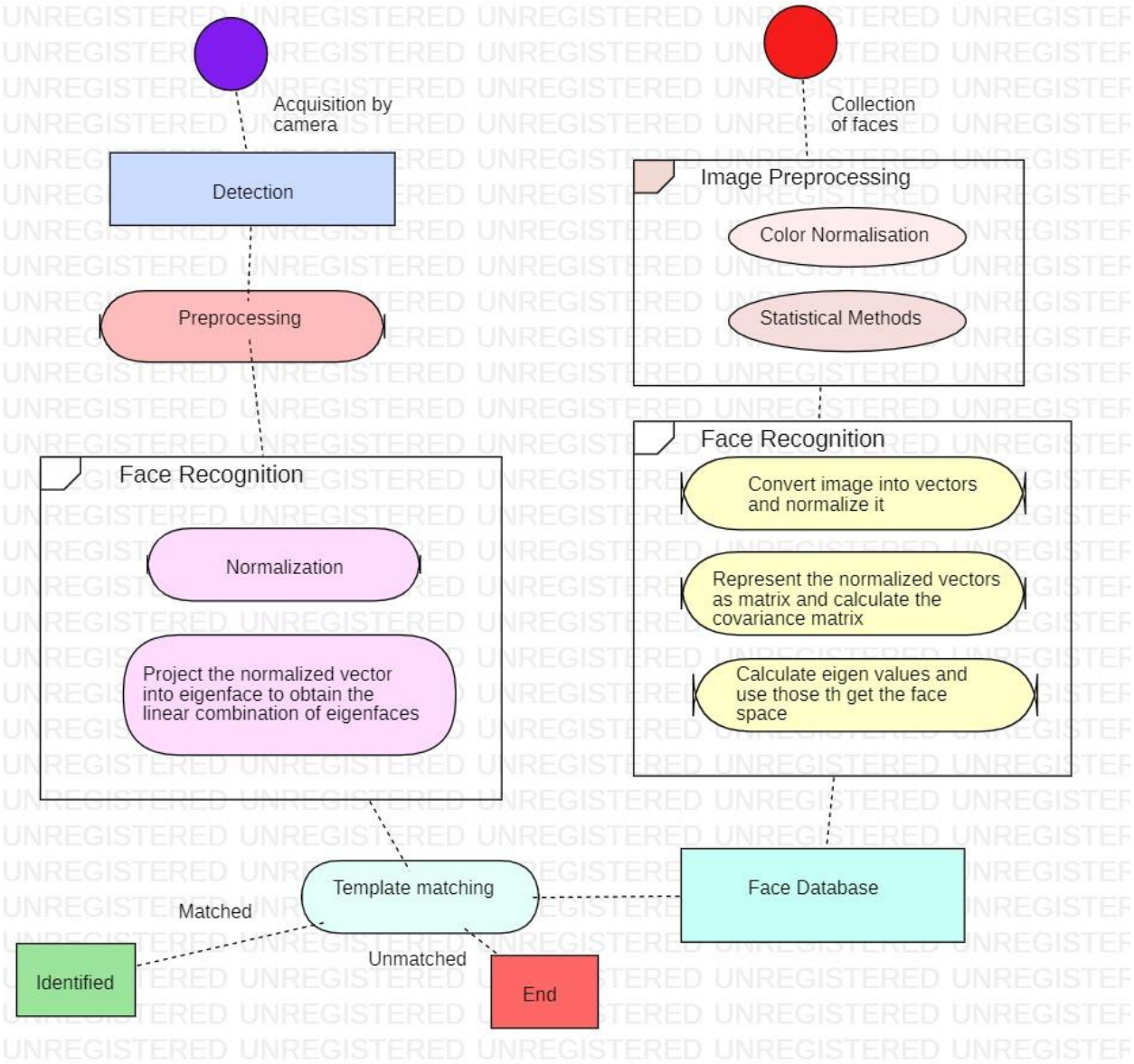


Fig. Architectural Model

The model revolves around two modules of the system. First and foremost is the collection of the images i.e., register criminal from the interface. The image taken is first preprocessed using color normalization methods that normalize the RGB values of the image. As the intensity of the lighting source increases by a factor, each RGB component of each pixel in the image is scaled by the same factor. We remove the effect of this intensity factor by dividing by the sum of the

three color components. Since the pixels of the resulting image have equal intensity, summing the three color channels would result in a blank image. Therefore, to create an image with single scalar values for each pixel (as required by our Eigen face system), we can either take a single color channel or sum just the red and green components (the chromaticity) (Thomas Heseltine, Nick Pears and Jim Austin, 2002). After the preprocessing is completed, our next phase is to recognize the face. Here, we use the Eigen face and PCA analysis.

The flowchart/architecture of the Eigen face looks like below:

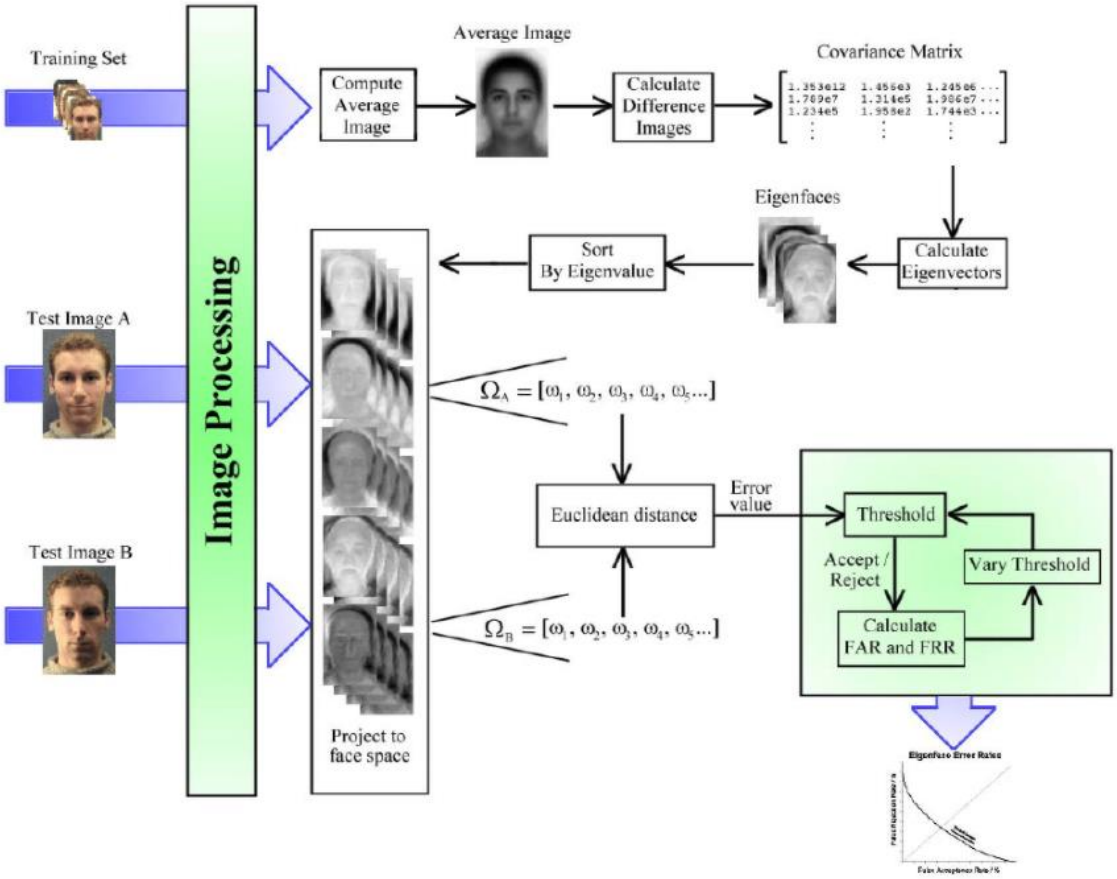


Fig. Flow model of Eigen Face

After the representing the training faces in the form of a vector of the coefficients of eigen faces, the first module of the model is completed.

The second module of the system is the acquisition phase that takes the images using camera or simply by uploading. This module is represented in our system with detect criminal and video surveillance interface. In the video surveillance, the object is detected using the HAAR Cascade which is simply an object detection algorithm. After the detection, the image goes through the preprocessing.

In the face recognition phase, we first preprocess the image to make it centered and have the same dimension as the training face. We then subtract the face from the average face and project the normalized vector into Eigen face to obtain the linear combination of Eigen faces. The vector of the Eigen Face's coefficients is generated. Now, we take the vector generated and subtract it with the vector of the training face to get a minimum distance. If this distance is below the threshold then it is recognized with face from training set. The process is represented by the template matching phase in the architecture.

Testing

We employ manual testing so we know the experience from the user's perspective. Each tests case are handpicked so we know that the system works as documented. Our system is divided into two components. Image acquisition for recognition and Image collection for registration. Each test cases ensures that system works as expected. Moreover, we do not have much knowledge on automated testing as of now so we preferred manual testing.

Manual testing is a software testing process in which test cases are executed manually without using any automated tool. All test cases executed by the tester manually according to the end user's perspective. It ensures whether the application is working, as mentioned in the requirement document or not.

Log-in page

Test Case	Check-Item	Test Case Objective	Steps to Execute	Test Data Input	Expected Result	Note
TC01	Log-in	Leave all field blank and click on log in button	Select the log-in button		By leaving all the fields blank, a mandatory symbol (*) should appear in front of Username and Password fields.	
TC02	Username	Provide Valid Username	Select the Username field and type in the username	Username: 1100N	It should accept the entered username	
TC03	Username	Provide Invalid Username	Select the Username field and type in the username	Username: Ram001	Entering invalid username, then an error message must be displayed saying "Please Enter Valid Username" (Must start with a digit and end with a letter N,S or I)	
TC04	Password	Enter Valid Password	Select the Password field and type in the password	Password: r@123456R67	It should accept the entered password	Password should have a minimum length of 10 and must contain at least 1 special character and at least 1 lowercase and uppercase character and at least 3 digits
TC05	Password	Enter Invalid Password	Select the Password field and type in the password	Password: r@123456	Entering invalid password, then an error message must be displayed saying "Please enter correct Password"	
TC06	Log-in button	Correct Inputs	Click the log-in button		It should lead the user to the main page	
TC07	Registration		Click the registration link		It should direct the user to the registration page	

Register Criminal

Pre-conditions: User needs the clear image of the person from a reliable source. A proper angled photo if possible.

Test Case	Check-Item	Test Case Objective	Steps to Execute	Test Data Input	Expected Result
TC01	Register Criminal	To register criminal	Log in and then select the Register Criminal link from the interface		Directs to registration page
TC02	Register Criminal	To leave all the form fields blank	Click the Register button		By leaving all the text fields blank, the borders of the text field must turn red and not allow the user to proceed
TC03	Register Criminal	Leaving the image section blank	Click the Register button	Enter all the details and not upload the image	Pop-up a box saying image not uploaded.
TC04	Register Criminal	Uploading only one image	Click the Register button	Enter all the details and not upload only one image	Minimum 5 images required
TC05	Register Criminal	Filling all the required details	Click the Register button	Enter all required details and upload minimum 5 images	Display a message saying "Criminal registered successfully"

Detect Criminal

Pre-Conditions: Try to upload an image that is clear and well illuminated, not blurred.

Test Case	Check-Item	Test Case Objective	Steps to Execute	Test Data Input	Expected Result
TC01	Detect Criminal	To detect criminal	Select the detect criminal link from the interface		Directs to the detect criminal page
TC02	Detect Criminal	To not upload the image and try to recognize the criminal	Click the Recognize button		Displays a error which says "Image not uploaded"
TC03	Detect Criminal	Upload image which is in the database	Click the select image button	Select an image	If the image is recognized in the database, it displays the profile link at the right side of the screen.
TC04	Detect Criminal	Upload image which is not in the database	Click the select image button	Select an image	It pops out a box displaying "No criminal recognized"

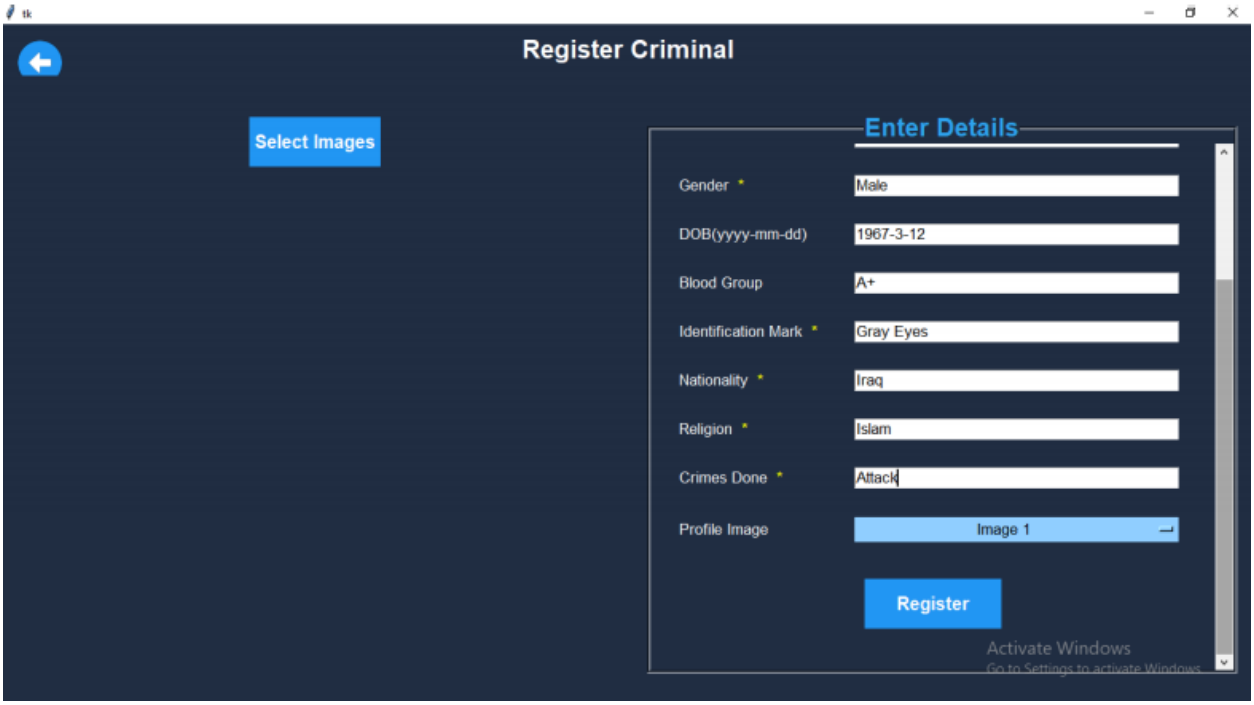
Video Surveillance

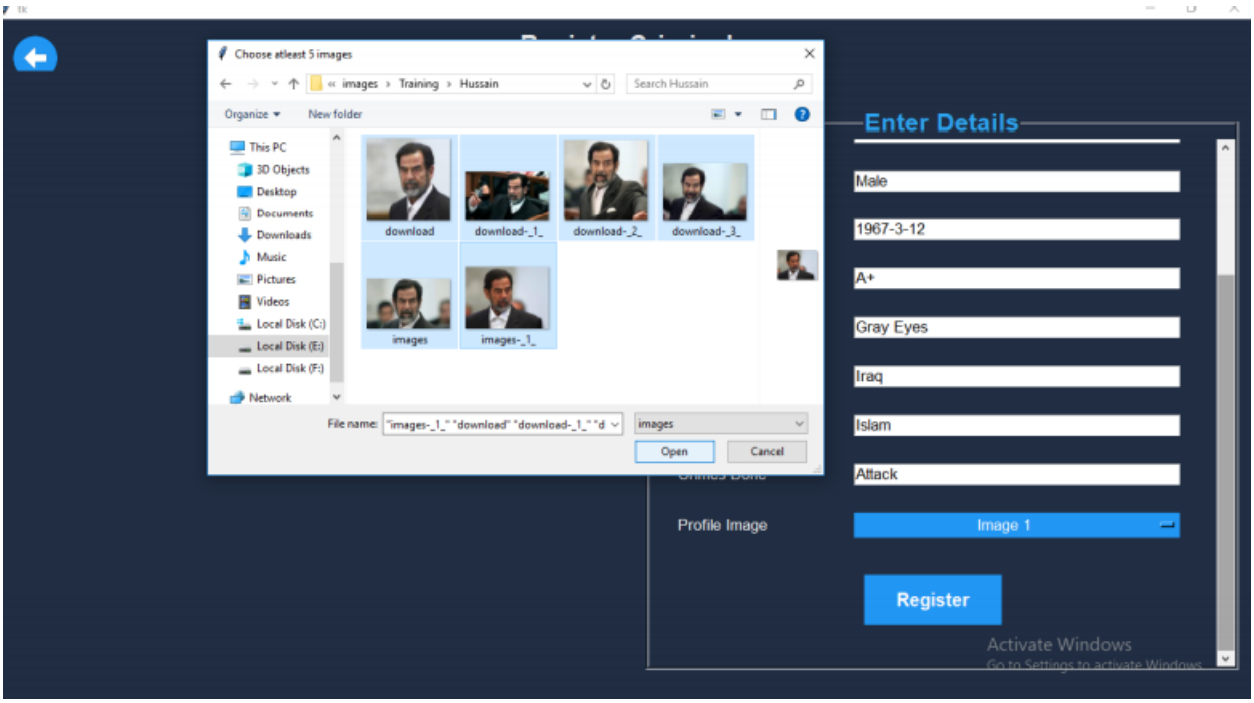
Pre-Conditions: Try to make the subject still. Fast moving objects are not detected.

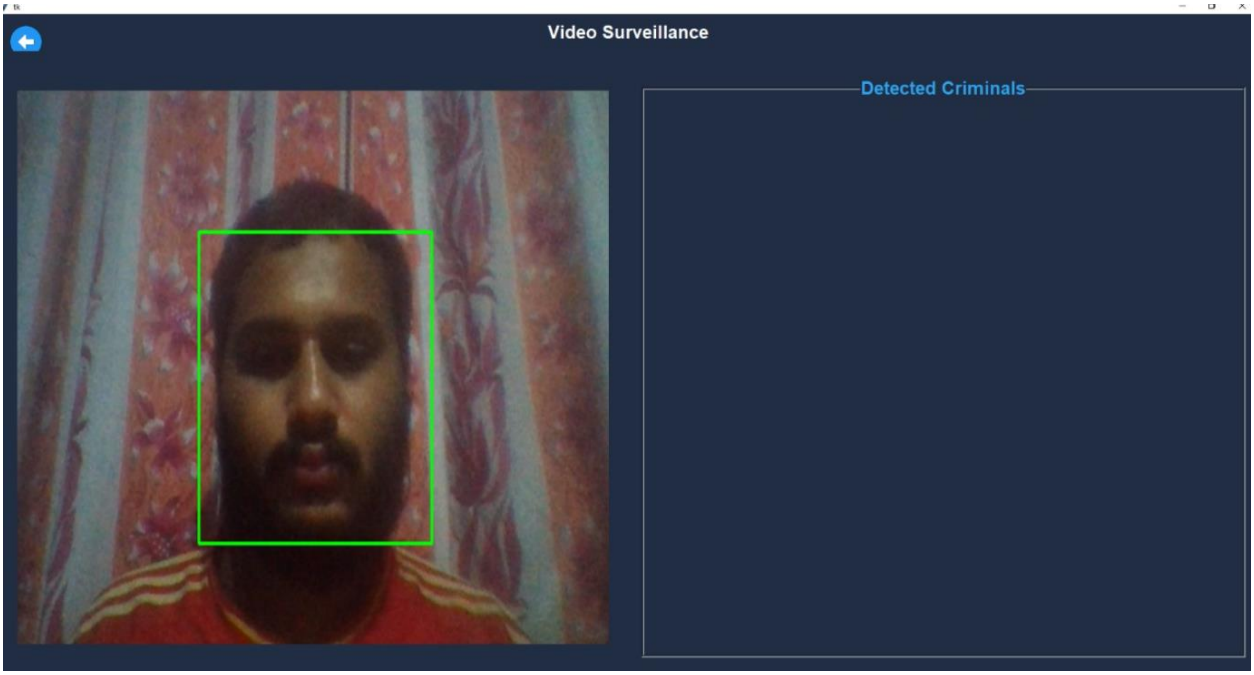
Test Case	Check-Item	Test Case Objective	Steps to Execute	Test Data Input	Expected Result
TC01	Video Surveillance	To detect criminal using video surveillance	Select the Video surveillance link from the interface		Directs to the video surveillance page.
TC02	Video Surveillance	To disturb the camera by moving the subject.		Through webcam	Cannot recognize the subject and hence displays a pop-up saying "No criminal recognized"
TC03	Video Surveillance	Stay still by the camera		Through webcam	If the subject is in the database, it displays the profile link at the right side of the screen.
TC04	Video Surveillance	To view the profile of the criminal	Click the profile link		It displays a page with all the details available on the subject.


Criminal Identification System
Video Surveillance
Register Criminal
Detect Criminal
Activate Windows
Go to Settings to activate Windows.


Register Criminal
Select Images
Enter Details
* Required Fields
Name *
Hussain
Father's Name
Hussain Junaid
Mother's Name
ADBS
Gender *
Male
DOB(yyyy-mm-dd)
1967-3-12
Blood Group
A+
Identification Mark *
Gray Eyes
Nationality *
Iraq
Religion *
Islam
Crimes Done *
Attack
Activate Windows


Register Criminal
Select Images
Enter Details
Gender *
Male
DOB(yyyy-mm-dd)
1967-3-12
Blood Group
A+
Identification Mark *
Gray Eyes
Nationality *
Iraq
Religion *
Islam
Crimes Done *
Attack
Profile Image
Image 1
Register
Activate Windows


Choose atleast 5 images
images › Training › Hussain
Search Hussain
Organize
New folder
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Local Disk (E:)
Local Disk (F:)
Network
download
download-_1_
download-_2_
download-_3_
images
images-_1_
File name: "images-_1_" "download" "download-_1_" "d
images
Open
Cancel
Enter Details
Male
1967-3-12
A+
Gray Eyes
Iraq
Islam
Attack
Profile Image
Image 1
Register
Activate Windows



5. CONCLUSION

Many advances have been going on in the field of face detection and other biometric related technologies. We have tried to present a detailed description of a software that we have tried to developed and give its features, documentation followed by the survey of related software in this field. We have also tried to highlight the security requirements of workplace and offices through our small survey. At last but not the least, we have tried to showcase our project by testing its components.

6. REFERENCES

Muhammad Sharif, Farah Naz1, Mussarat Yasmin, Muhammad Alyas Shahid and Amjad Rehman, *Face Recognition: A Survey JOURNAL OF Engineering Science and Technology Review*, {March 2017}

Samuel Ehidiamen Agaga, *Facial Recognition in Criminal Investigation*, {January 2018}

Nurul Azma Abdullaha, Md. Jamri Saidi, Nurul Hidayah Ab Rahmanb, Chuah Chai Wenc and Isredza Rahmi A. Hamidd, *Face Recognition for Criminal Identification: An implementation of principal component analysis for face recognition*, {03 October 2017}

Hiba Al-kawaz, Nathan Clarke, Steven Furnell, Fudong Li1, Abdulrahman Alruban, *Advanced Facial Recognition for Digital Forensics* ,{June 2018}

Daniel Faggella, *AI for Crime Prevention and Detection – 5 Current Applications*, {February 2, 2019}

Rabia Jafri* and Hamid R. Arabnia*, *A Survey of Face Recognition Techniques*, Journal of Information Processing Systems, Vol.5, No.2, {June 2009}

R. Vera-Rodriguez, J. Fierrez, P. Tome, and J. Ortega-Garcia, *Face Recognition at a Distance: Scenario Analysis and Applications*, {January 2010}

Thomas Heseltine, Nick Pears and Jim Austin, *Evaluation of image pre-processing techniques for Eigen face based face recognition*, Proceedings of SPIE - The International Society for Optical Engineering, {July 2002}