

**A DEEP LEARNING APPROACH TO DETECT UNAUTHORIZED  
PERSON**

**BY**

**MD. HASAN HABIB  
ID: 172-15-9675**

**SHAKIB MAHAMUD  
ID: 172-15-9606**

**And**

**OWALI ULLAH SHAWON  
ID:172-15-9763**

This Report Presented in Partial Fulfillment of the Requirements for the  
Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

**Shadaab Kawnain Bashir**  
Lecturer  
Department of CSE  
Daffodil International University

Co-Supervised By

**Mr. Abdus Sattar**  
Assistant Professor  
Department of CSE  
Daffodil International University



**DAFFODIL INTERNATIONAL UNIVERSITY**

**DHAKA, BANGLADESH**

**MAY 2021**

## APPROVAL

This Project/internship titled “A Deep Learning Approach to Detect Unauthorized Person”, submitted by Md. Hasan Habib, Shakib Mahamud and Owali Ullah Shawon, ID No: 172-15-9675, 172-15-9606 and 172-15-9763 to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 2<sup>nd</sup> June 2021.

### BOARD OF EXAMINERS



**Chairman**

---

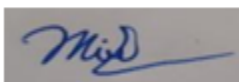
**Dr. Touhid Bhuiyan**

**Professor and Head**

Department of Computer Science and Engineering

Faculty of Science & Information Technology

Daffodil International University



**Internal Examiner**

---

**Moushumi Zaman Bonny**

**Assistant Professor**

Department of Computer Science and Engineering

Faculty of Science & Information Technology

Daffodil International University



**Internal Examiner**

---

**Md. Sazzadur Ahamed**

**Senior Lecturer**

Department of Computer Science and Engineering

Faculty of Science & Information Technology

Daffodil International University



**External Examiner**

---

**Dr. Md Arshad Ali**

**Associate Professor**

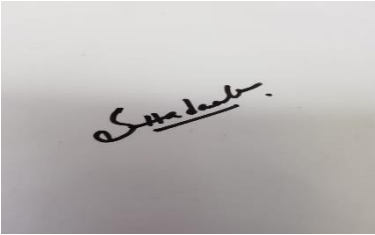
Department of Computer Science and Engineering

Hajee Mohammad Danesh Science and Technology  
University

## DECLARATION

We hereby declare that, this project has been done by us under the supervision of **Shadaab Kawnain Bashir, Lecturer, Department of CSE** Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

### Supervised by:



---

**Shadaab Kawnain Bashir**

Lecturer

Department of CSE

Daffodil International University

### Co-Supervised by:



---

Mr. Abdus Sattar

Assistant Professor

Department of CSE

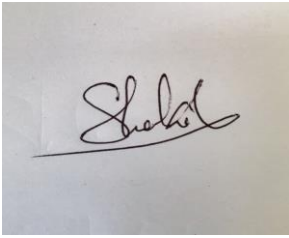
Daffodil International University

**Submitted by:**



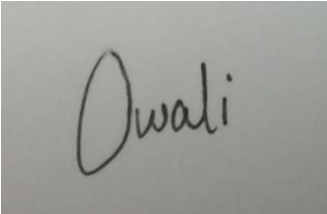
---

**Md. Hasan Habib**  
ID: 172-15-9675  
Department of CSE  
Daffodil International University



---

**Shakib Mahamud**  
ID: 172-15-9606  
Department of CSE  
Daffodil International University



---

**Owali Ullah Shawon**  
ID: 172-15-9763  
Department of CSE  
Daffodil International University

## ACKNOWLEDGEMENT

First, we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year project/internship successfully.

We really grateful and wish our profound our indebtedness to **Shadaab Kawnain Bashir, Lecturer**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of “Computer Vision” to carry out this project. Her endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to Professor **Dr. Touhid Bhuiyan**, Professor, and Head, Department of CSE, for his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

We would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

## **ABSTRACT**

This analysis aims to identify Unauthorized Persons to ensure the protection of an organization. Essentially, this is a hybrid of two forms of detection. The first detects known and unknown faces, while the second detects ID cards. An image dataset should be connected with the model. Using the dataset images, we were able to identify faces and ID cards. The face recognition library and Histogram of Oriented Gradients (HOG) were used to recognize the faces, and the You Only Look Once (YOLO) V3 model was used to detect the ID card. From the test image our model will be able to recognize both the face and the object. Our model will show the person's name and draw a rectangular green shape around the face region if it recognizes faces. If the face does not match the encoded faces, the system will mark it as unknown, and if the face has covered by a hand or other object, the system will mark it as unknown and draw a red shape around the face area. If our model detects the Id card, it will make a rectangle shape in the detected region and color it green, just as it does with faces. If the model is unable to detect the identification card, it will draw a rectangle below the neck and paint it red.

# TABLE OF CONTENTS

<b>CONTENTS</b>	<b>PAGE</b>
Board of examiners	2
Declaration	4
Acknowledgements	6
Abstract	7
List of figures	10
<b>CHAPTER</b>	
<b>CHAPTER 1: INTRODUCTION</b>	<b>1-4</b>
1.1 Introduction	1
1.2 Motivation	2
1.3 Rationale of Study	3
1.4 Expected Outcome	3
1.5 Report Layout	4
<b>CHAPTER 2: Background</b>	<b>5-6</b>
2.1 Related Works	5
2.2 Comparative Analysis and Summery	5
2.3 Problems and Challenges	6
<b>CHAPTER 3: METHODOLOGY</b>	<b>7-22</b>
3.1 Research Subject and Instrument	7
3.2 Data Collection Procedure	7
3.3 Proposed Methodology	9
3.4 Implementation Requirement	22



<b>CHAPTER 4: EXPERIMENTAL RESULT AND ANALYSIS</b>	23-25
4.1 Experimental Setup	23
4.2 Experimental Result and Analysis	23
4.3 Model Testing	25
<b>CHAPTER 5: IMPACT ON SOCIETY, ENVIRONMENT AND SUSTAINABILITY</b>	26 – 28
5.1 Impact on Society	26
5.2 Impact on Environment	26
5.3 Ethical Aspects	27
5.4 Sustainability Plan	28
<b>CHAPTER 6: CONCLUSION AND IMPLICATION OF FUTURE RESEARCH</b>	29
6.1 Conclusions	29
6.2 Implication for Further Study	29
<b>REFERENCES</b>	30-31
<b>PLAGIARISM REPORT</b>	32

## LIST OF FIGURES

<b>FIGURES</b>	<b>PAGE NO</b>
Figure 3.1: Dataset Images Snapshot	8
Figure 3.2: Histogram of Oriented Gradient working process	11
Figure 3.3: Test image face location and encoding detection code	11
Figure 3.4: Detecting know face	12
Figure 3.5: Example of multi-face detection at a time	13
Figure 3.6: Example of unauthorized Face	13
Figure 3.7: Labeling Id Card	14
Figure 3.8: YOLO working process	15
Figure 3.9: Detecting Id card	16
Figure 3.10: Creation of Model Flowchart	17
Figure 3.11: System architecture	18
Figure 3.12: Authorized Person Detection	20
Figure 3.13: Unauthorized Person Detection	21
Figure 4.1: Confusion Matrix	23
Figure 4.2: Accuracy Parentage	24

# Chapter 1

## Introduction

### 1.1 Introduction

We are now investing a significant amount of money to secure our company. We used a CCTV camera, biometric fingerprint recognition, and security guards to accomplish this. We cannot, however, regulate the rate of crime. Gradually the crime rate is increasing. For most businesses, this is becoming a significant issue. We designed unique protection technology called A Deep Learning Approach to Detect Unauthorized Person to make the security system more sophisticated.

Most of the organization has their unique authorized card or ID cards for their employees. Employees used these ID cards to verify their identity. Many businesses use employee passes to obtain access to their facilities. For that showing the cards to the machine or the guards are compulsory to ensure security. These cards can easily be stolen, and any unauthorized individual can use them to regain access to the organization. It poses a significant risk to a company. We can see that tons of crimes are happening with the help of an organization's ID cards. In addition, this company uses closed-circuit television (CCTV) to track employee movement. However, this is ineffective in reducing crime.

The use of conventional security systems is less effective and also much less efficient. It is because checking individual persons by security guards is more time-consuming and is often tedious. Even though there is a closed-circuit camera to monitor one's movements, someone can easily defraud the guards by using a fake ID card. However, in organizations with a large number of employees, identifying unauthorized individuals is nearly impossible. Monitoring the surveillance camera for every moment is difficult. Some dishonest people take this as their advantage. Using this as their advantage, those people easily got into the organization and performed their illegal tasks.

Addressing this form of security issue, we developed a system that can recognize faces along with detect approved Id cards. For face detection and recognition, OpenCV and Face Recognition libraries are used. The You Only Look Once (YOLO) V3 object detection model is used to detect the ID cards. If the machine recognizes the face, it will classify as a recognized face, is if the face does not match the known faces, it will mark as unknown. When the device detects an id card in one's neck, it creates a rectangle in the detected region. If the id card is not there, a red color rectangle will appear below the neck with the message "id card not found."

## **1.2 Motivation**

Security is always a concern for an institute. For example, an outsider can enter our university by using someone's id card without any assurance that he is a student or that this id card belongs to him. There is a significant risk that someone with a bad intention will cause harm to the university. Once we've identified the problem, we want to make sure that no one outside the institute can harm us [1]. However, a developing country like Bangladesh has a weak security system, which allows nefarious people with bad intent to take advantage of this and engage in criminal activity. For instance, we don't have enough protection systems to detect unauthorized individuals. To ensure a safe environment for any institute, computer vision and AI are required to recognize approved people. In addition, we proposed an identification model that uses a face recognition method to validate a person's details while also detecting an item (ID card) [2]. Recognizing a face and object requires a fraction of a second or less, resulting in a faster recognition method. It will improve the effectiveness of identification while also identifying an unwanted or unauthorized individual.

### **1.3 Rationale of the Study**

In this research area, we present an impactful model for detecting and recognizing a human and an object by using some known algorithm. [3] The existence of research and systems in this field is quite low and different kinds of techniques have been proposed based on machine learning techniques, artificial neural networks, and Support Vector Machine. [3] Here, proposes a deep learning approach in which we record an impressive result using OpenCV, face recognition, Histogram of Oriented Gradients (HOG) algorithm, and YOLO V3 algorithm. For low resources fields while working with both face recognition and object detection most researchers avoid working with both at the same time. Being such a complex system and new to researchers is the main reason for fewer contributors and inventors.

### **1.4 Expected Outcome**

Our main contributions include,

- Developed a model for face recognition and object detection
- A Novel Dataset in perspective of Bangladesh
- An initial experimental system for an organization for security purposes.
- Smarter Monitoring System
- Automation of identification
- Identify Unauthorized Persons
- Enhanced security

## **1.5 Report Layout**

In this chapter, we looked at the introduction, which included the Unauthorized Person Detection Platform, motivation, the study's logic, and the thesis's conclusion. The report layout is then followed.

The context of our research will be discussed in Chapter 2.

The approach of our complete thesis work will be discussed in Chapter 3.

We'll go over the experimental findings and analyze them in Chapter 4.

The influence on society, the environment, and sustainability will be discussed in Chapter 5.

We'll talk about the summary, conclusion, and implications of future study in Chapter 6.

## **Chapter 2**

### **Background**

#### **2.1 Related Works**

This research presents a proficient strategy for identifying an acknowledgment of the unauthorized human face dependent on some intermediate calculations. We have found many related works like this one, but they are not exactly like it. We use some techniques based on these papers.

"Face Detection System Based Viola-Jones Algorithm" is a title of a paper by researchers [4] Jamal M.Al-Tuwaijari and Saja A. Shaker. Where they detect faces using biometric facial face image details. "A Comparative Study between LBP and Haar-like features for Face Detection Using OpenCV" author characteristics and the Local Binary Pattern are two approaches of face detection that are evaluated. [5] "A Review of Person Recognition Based on Face Model" this review looks at all of these methods with characteristics that make face identification difficult, such as lighting, position variation, and facial expressions. [1] "Face Detection and Recognition" on this thesis paper they mostly discuss about face and facial feature detection.

KLT Algorithm, Viola-Jones Algorithm face detection which detects human face using Haar cascade classifier, although camera is continuously detecting the face every frame, PCA algorithm for feature selection were utilized in the "Face Recognition System." To mimic the geometric aspects of the human face, we use a model combining technique. [4]

#### **2.2 Comparative Analysis and Summery**

As we see the related works comparative to our research, we can say that we have developed some to secure the system on entry security system process. [6] In this research comparing to related papers, we have some improvement according to their development. By the end of this process, [7] there is one most important thing to see here about security systems where an unauthorized person can detect very easily. [2]

We've introduced a face detection method that reduces error rate while maintaining a high detection rate. The method was used to create a face recognition device that is faster than any previous method. [8] This paper puts together a diverse series of new algorithms, representations, and perspectives.

### **2.3 Problems and Challenges:**

We encountered a variety of obstacles and problems while conducting this research, including determining what type of data we require, collecting data, and implementing the findings. Because research in this topic is limited in our country, working in this field was more challenging than working in other fields. [9] Comprehending the ecosystem was difficult as a relatively new topic, as was understanding algorithms and selecting methods for identifying both face and object at the same time. We also struggled with components for training the model as we need a high-end GPU. Here are main challenges that we faced:

1) Understanding problem and facts to be solved

2)Collecting Data

3)Choosing algorithm

4) Combining algorithm

5) Implementing and testing



## **Chapter 3**

### **Methodology**

#### **3.1 Research Subject and Instrument**

The main research subject of our research is detection and recognition in which we are detecting a human and an object. For that a good level of understanding about algorithms and specification knowledge is need. Like how OpenCV works and what we need to implement it. Different types of instruments are required for implementation, including:

A good GPU base Computer

OpenCV installation

A webcam

A dataset

Capable computer for training with time

#### **3.2 Data Collection Procedure**

Our main objective is to develop the “A Deep Learning Approach to Detect Unauthorized Person” is for securing the industries or the academic institutions from unauthorized or unengaged persons from that institution. People who are not connected to this institution cannot enter. If he/she wants to enter then he/she has to show Identification. But it is difficult for a person to person checks these identities.

So, we want to develop a system where the system has access to the authentication data of the people who are engaged with the institution. It can be a digital or analog identity card. The card has the information of the person.

During this pandemic situation, it was very difficult to collect these data sets. First, we approach some institutions for the data collection which they have on their database.

But they did not agree with us for the purpose of their security. Then we approach our own institution but they also decline as their privacy policy.

Moreover, we switch to our own approach. We request our friends and teacher to help us in our process. We use social networking to collect data from some people. We make a google form for collecting the data. But most of the people were not interested in it. In the end, we approached many of them physically to take a picture with an identity card.

That is how we collect about 700 people's photo data with their identity cards. From this data, we make another 300-dummy data which makes a total of 1000 data.

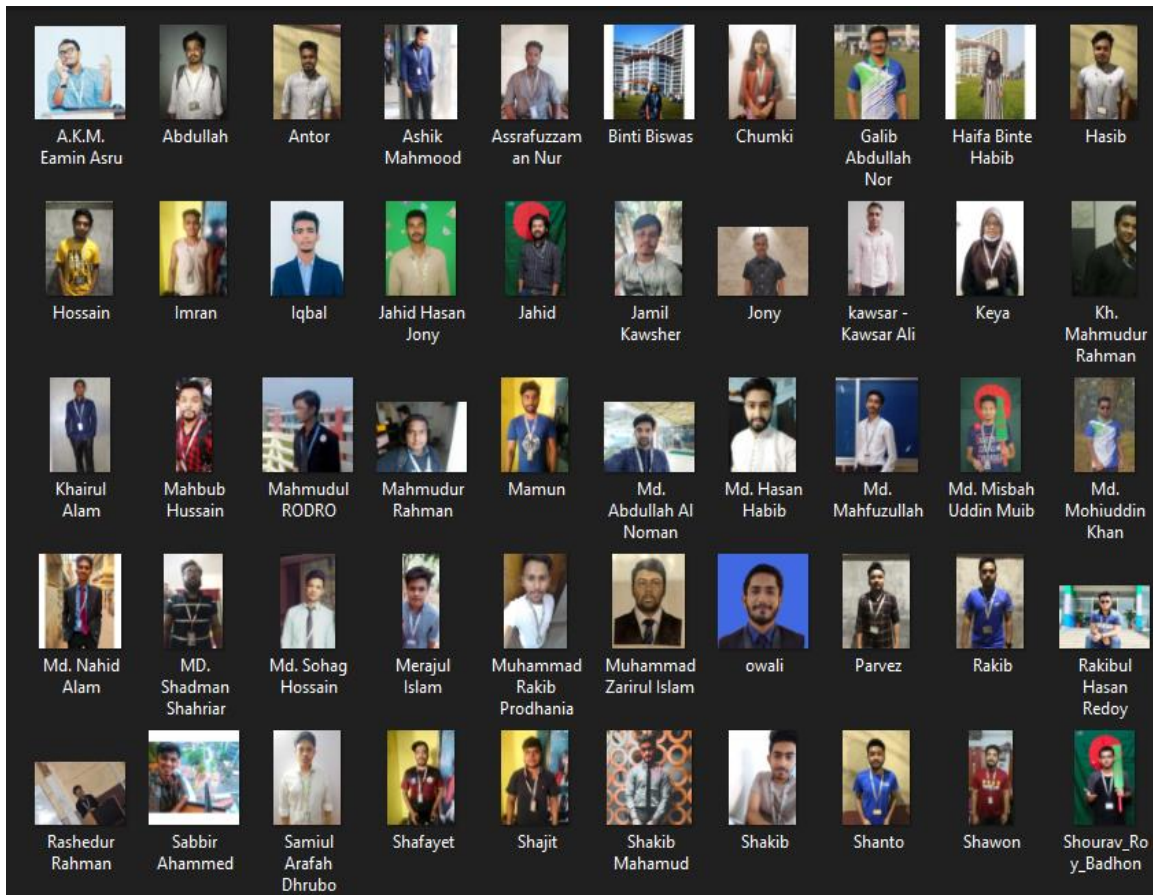


Figure 3.1: Dataset Images Snapshot

### 3.3 Proposed Methodology

The parous of our research is to bring a system that will improve the security system of an organization by using OpenCV, face recognition, Hog algorithm, and YOLO v3 algorithm and successfully recognize authorized persons of an institution. For this novel approach is successful this below steps are taken:

- Existing systems that are present in this field are well studied for constructing this system.
- Feature-based and image-based approaches are well studied.
- Existing image-based systems that were proposed recently studied.
- Various papers on Face Detection, Object Detection, Computer Vision, and Neural Network algorithms were studied.
- Went through different organizational systems to have an understanding research idea.
- Various IT fairs were visited and studied the need of an organization.
- The main aspects of this research are being identified like recognition approach, detection approaches, distance factor, and feature approach.
- Relevant to those aspects' questionnaires are pointed out.
- Standard answers were provided for questionnaires.
- Difficulties were being faced in our core points (recognition approach, detection approaches, distance factor, and feature approach) and relevant solutions were studied.
- Based on an organization's want step by step organized plan was made.

- Eventually, a final plan was made and a model is proposed and in the long run

Here we have divided the whole system into three main parts. These are the ones:

1. Recognition of people's faces
2. Detection of objects
3. Face and object recognition in combination

Let's describe more about these methodologies.

### **1. Recognition of people's faces:**

At first, we need to measure the face encodings using the face recognition library. The algorithm takes note of important measurements on the face, such as the color, height, and slant of the eyes, the distance between the brows, and so on, to recognize the individual. Face encoding is specified by the combination of both of these factors. It will construct a model of the encoded faces after calculating all of the face encodings in the data set. Then the system will detect the number of faces present in the current frame using the HOG algorithm. Histogram of Oriented Gradients (HOG), is a function descriptor for extracting features from image info. It is widely used in target recognition activities in computer vision. Let's take a look at some of the main features of

HOG that set it apart from other function descriptors:

- The HOG descriptor is concerned with an object's structure or form. How is this different from the edge features we extract for photographs, you may wonder? In the case of edge features, we only determine whether or not a pixel is an edge. The edge orientation can also be generated by HOG. These are obtained by extracting the edges' gradient and orientation.
- These orientations are therefore computed in concentrated sections. This signifies that the whole picture has broken into different smaller regions, with gradients and alignment determined for each. In the following pages, we'll go through this in greater depth.

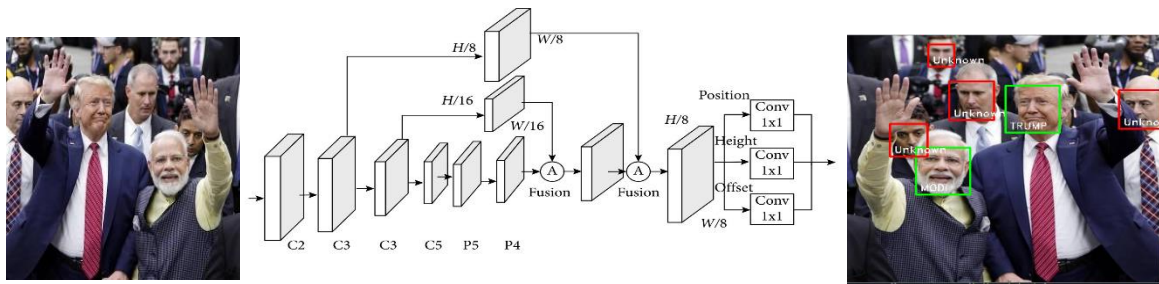


Figure 3.2: Histogram of Oriented Gradient working process

- Finally, the HOG will create a different Histogram for each of these areas. The term Histogram of Oriented Gradients comes from the fact that the histograms generated using the gradients and orientations of the pixel values. [9]

Then the system will record the current frame face encodings. Following that, a for loop with the face positions and face encodings as parameters has called. The values of the top, right, bottom, and left positions of the faces in the current frame spot. [9] After that, it will compare those values with the known face encoding. If those values match any of the recognized face encodings, the program will return the person's name and draw a rectangular form around the face with a green border. And also, the number of faces present in that frame.

```

all_face_location = face_recognition.face_locations(original_image, number_of_times_to_upsample=1, model='hog')
all_face_encoding = face_recognition.face_encodings(original_image, all_face_location)

print("There are {} no of Faces".format(len(all_face_location)))

for current_face_location,current_face_encoding in zip(all_face_location,all_face_encoding):

    top_pos, right_pos, bottom_pos, left_pos = current_face_location

    all_matches = face_recognition.compare_faces(known_face_encodings,current_face_encoding )
    face_dis =face_recognition.face_distance(known_face_encodings, current_face_encoding)
    matchIndex = np.argmin(face_dis)

```

Figure 3.3: Test image face location and encoding detection code

The following is an example of face recognition:

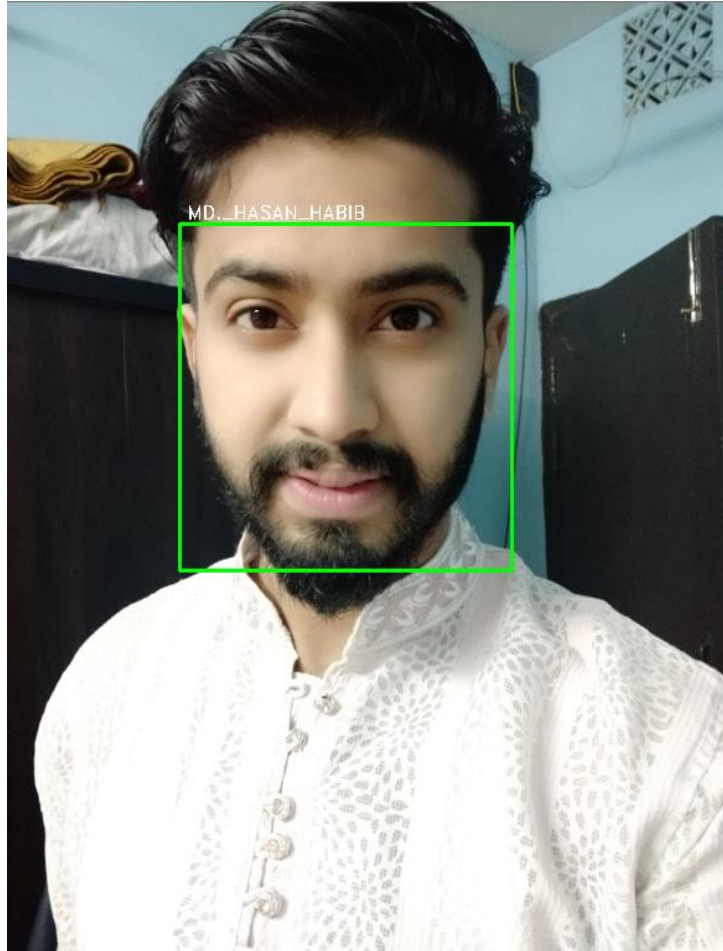


Figure 3.4: Detecting know face

In the dataset one face encoding has matched with this test data image so that the system returns it as the known face. It has done so by adding a green frame to the face locations and displaying the person's name from the dataset.



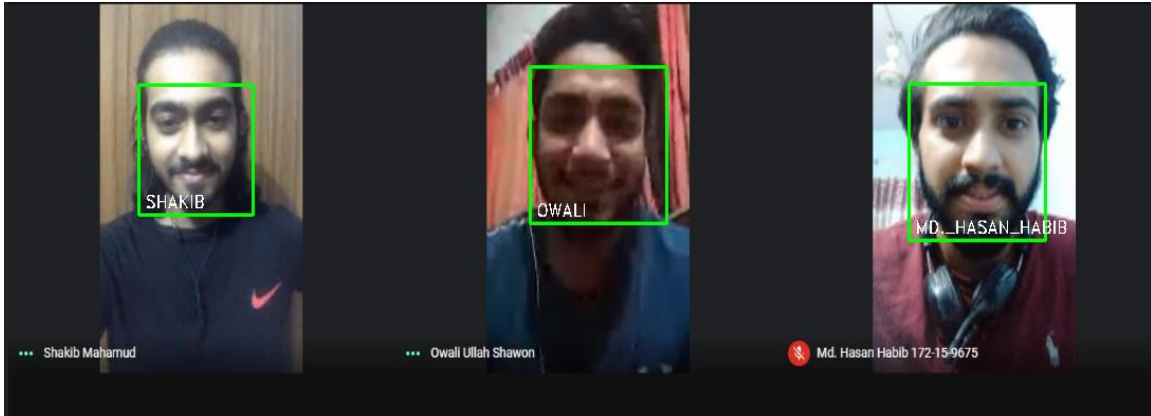


Figure 3.5: Example of multi-face detection at a time

If the detecting detected face is not in the dataset, after that, the system will mark it as unknown and frame it in red. An example of such a case shown below:

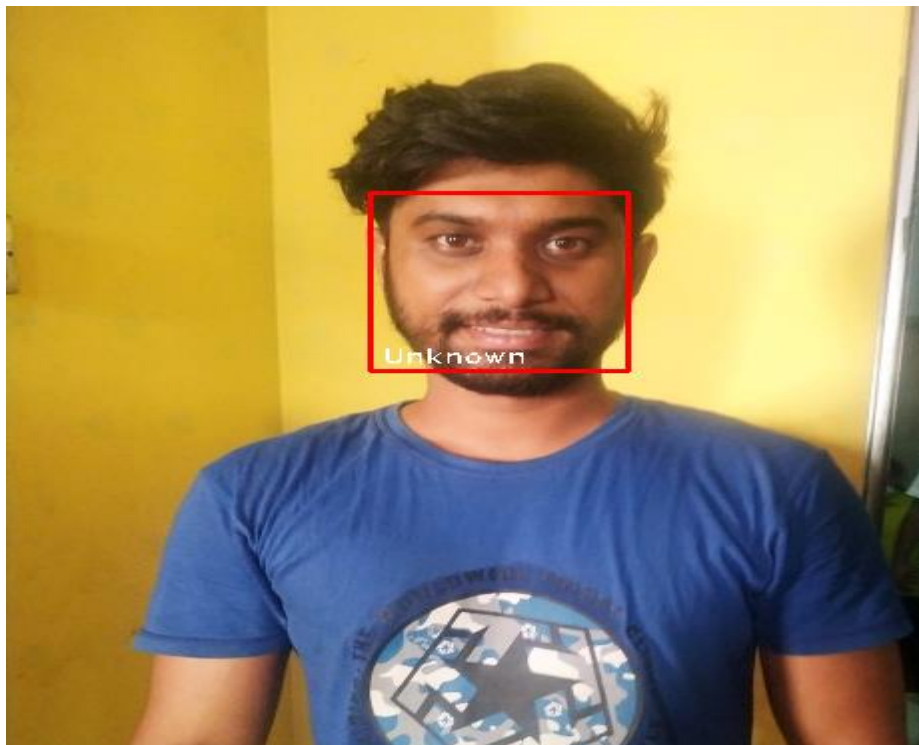


Figure 3.6: Example of unauthorized Face

The system has successfully detected the face positions. Here this person image is not in the data set so it has labeled it as unknown and frame it as red box.

In, this way the face recognition system will work.

## 2.Detection of objects:

Now after recognizing the face, we are going to detect a custom object like our university id card by using Yolo V3. Before applying our selected algorithm, we are leveling our data by one class ID using labelImg.exe for training our model for applying in the testing dataset. [7]

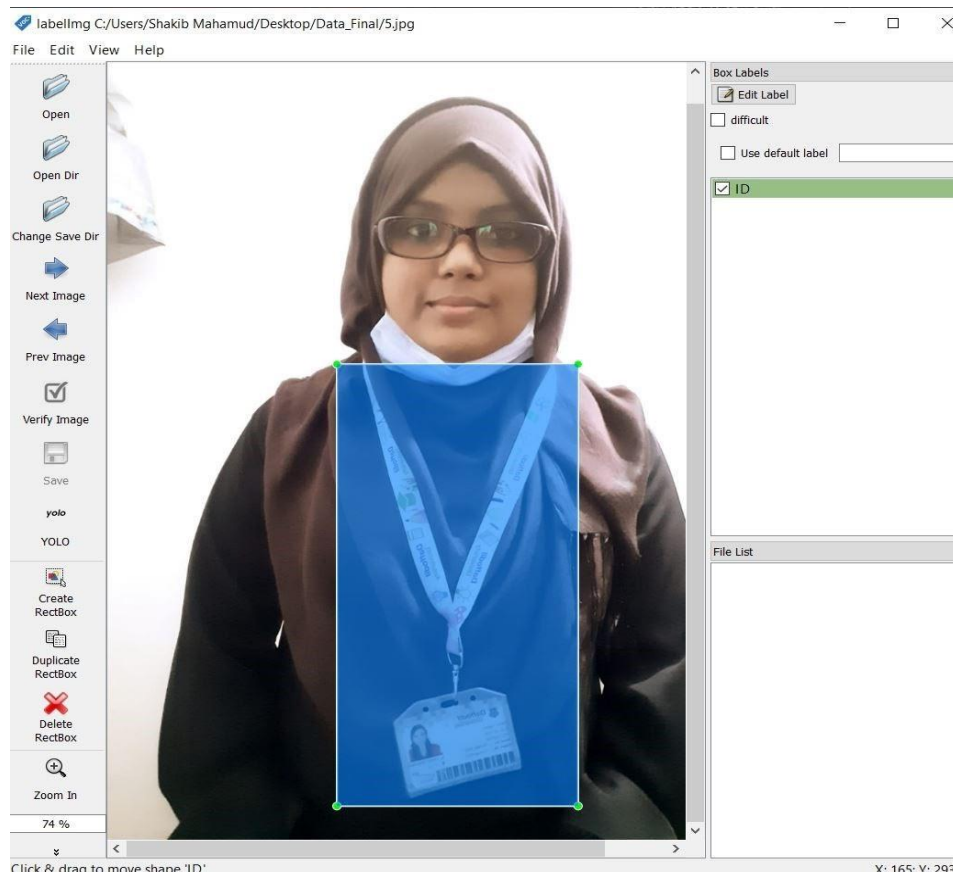


Figure 3.7: Labeling Id Card

We chose YOLO V3 because detecting a custom object performs better than other detecting algorithms. YOLO is a Convolutional Neural Network (CNN) for identifying objects where CNNs are classifier-based frameworks that can interact with input photos



as ordered types of information and discover patterns between them. YOLO V3 has the advantage of being far faster than other networks while maintaining accuracy. [10]

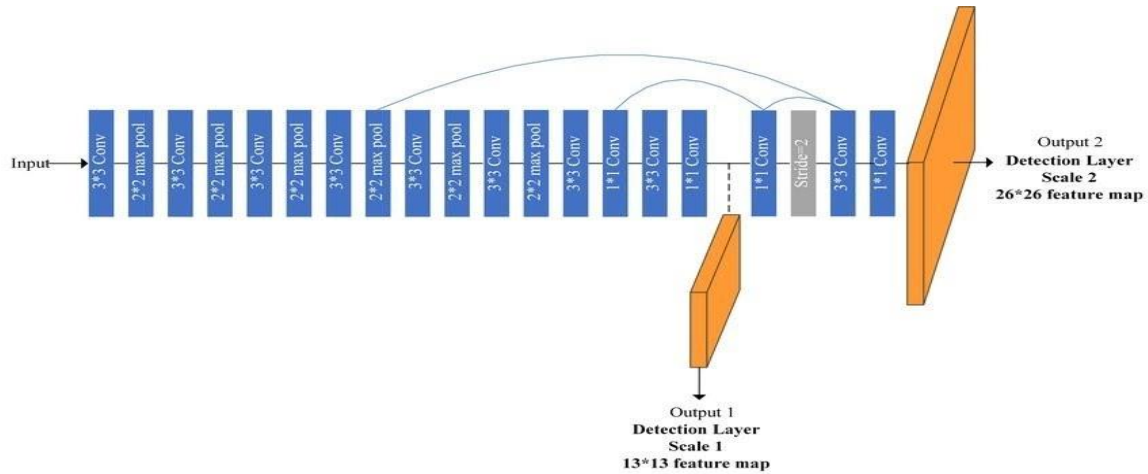


Figure 3.8: YOLO V3 working process

It enables the model to look at the complete picture at test time, allowing its forecasts to be influenced by the global setting in the picture. Locale's "score" in YOLO V3 and other convolutional neural organization computations based on their similarity to specified classes. High-scoring regions are given as specific identifications of the class to which they are most closely related. [11]

YOLO V3 separates a photo into a framework because we're working with a custom object and leveling data with a single class ID. Every network cell predicts a certain number of limit boxes (also known as anchor boxes) surrounding objects that excel in the previously described preset classes, such as our ID Class. Every limit box has its own certainty score for how precise it anticipates that expectation to be, and each leaping box only includes one item. To find the most generally recognized forms and sizes, the limit boxes are generated by grouping the components of the ground truth boxes from the first dataset. YOLO V3 is quicker than previous versions in terms of speed, accuracy, and class specificity. [11]

During training, YOLO V3 employs for class predictions, independent logistic classifiers and binary cross-entropy loss are used., which allows us to deal with a dataset as

complicated as ours. We employ a multilabel method in YOLO V3, which allows classes to be more precise and have several bounding boxes.



Figure 3.9: Detecting Id card

### 3.Face and object recognition in combination:

It is the final proposed model. Here we are going to detect the faces and also the id cards. The system will detect the face position and determine if the person is known or unknown in the face detection part. The system will detect the Id card position during the object detection process. At first, the system will prepare the face and object detection model for testing. Creating the model process is shown in the below diagram.

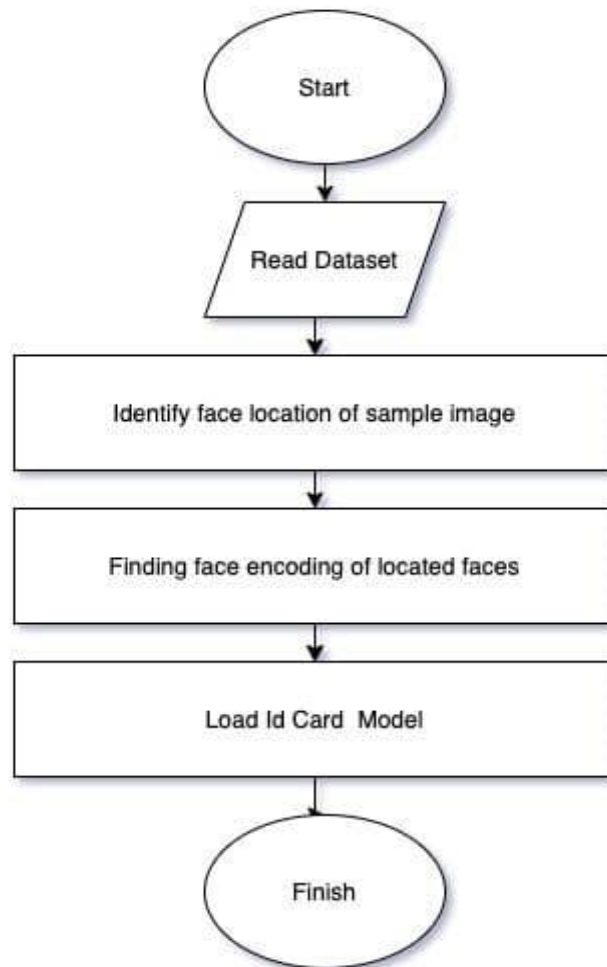


Figure 3.10: Creation of Model Flowchart

When the system first boots up, it loads all of the dataset images. After loading all of the images from the dataset, the system will use the face recognition library to locate the faces in those example photographs. Then it will move on to the face encoding part. It will generate face encoding for each face image and save the person's name associated with that encoding. After loading the face encodings then it will load the object detection model that we have created by the YOLO V3.

Let's discuss the whole working procedure of our system. The diagram of the system architecture is shown below.

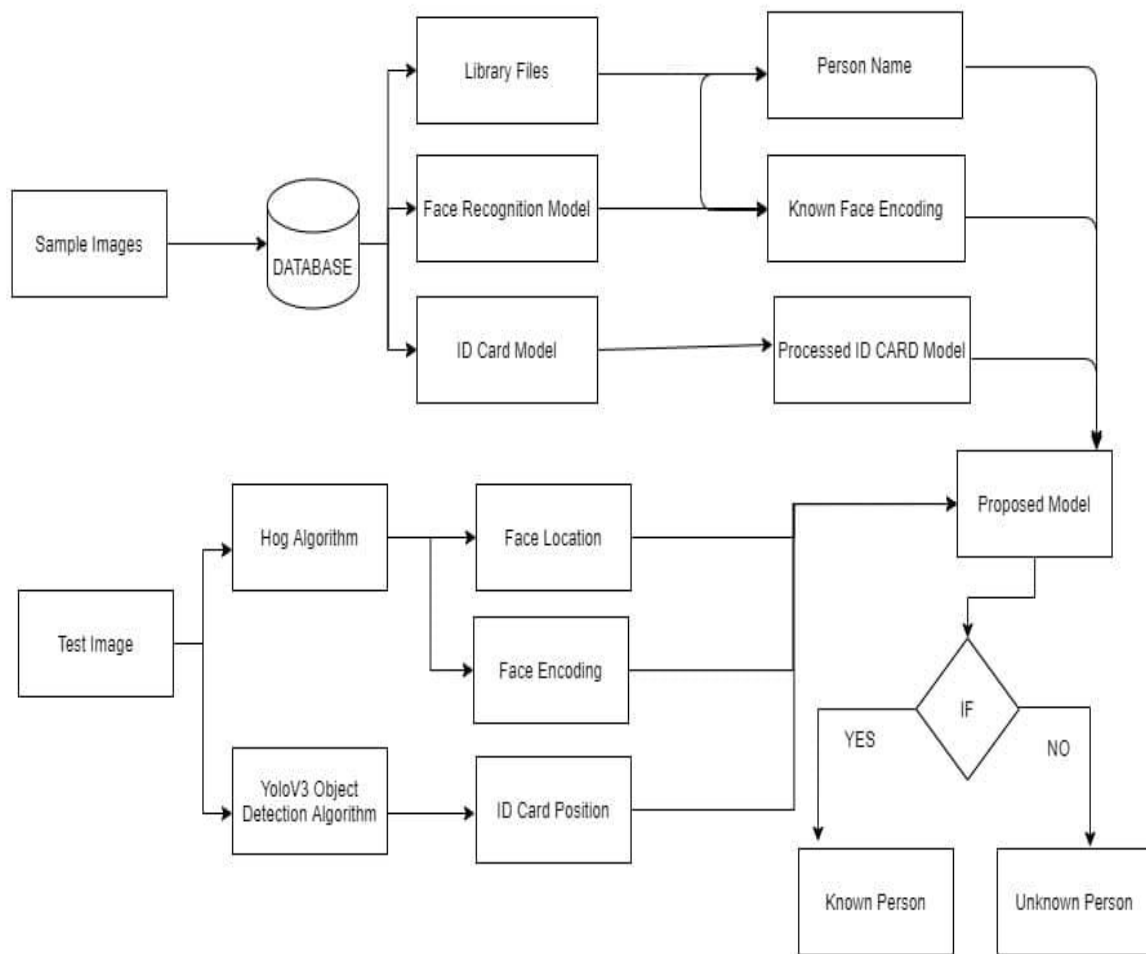


Figure 3.11: System architecture

First, the database would be loaded with all of the known face data. Then the program will import all the necessary library files, face recognition model, and the object detection model. After that, the system will apply those in the know face image dataset. From that, the system will find the face encodings of those known faces. It will also store the name of that known person. And also generate the final id card detection model. That is how the system will prepare for the final proposed model for face and Id card detection.

For testing an image for detection, at first, load the test image. The system will apply the Histogram of Oriented Gradients (HOG) algorithm and YOLO V3 object detection algorithm to that test image. HOG algorithm will generate the face location of the test image and using the face recognition library, test image face encoding will identify. And using the YOLO V3 algorithm, the id card position of that image will be detected. All those detections will be inserted in the proposed model for the outcome. When the data from the test image is analyzed for detection. The system will loop through the test image data with the known dataset. If the test image data match the known dataset the system will return the face position of the person along with the person's name. And detect the id card position of that image and label it as an id. If the face does not match the known dataset and the id card is not visible in the image, the system will flag the individual as unauthorized.

Let's see the outcome of our system. Example of the test image outcome is given below.

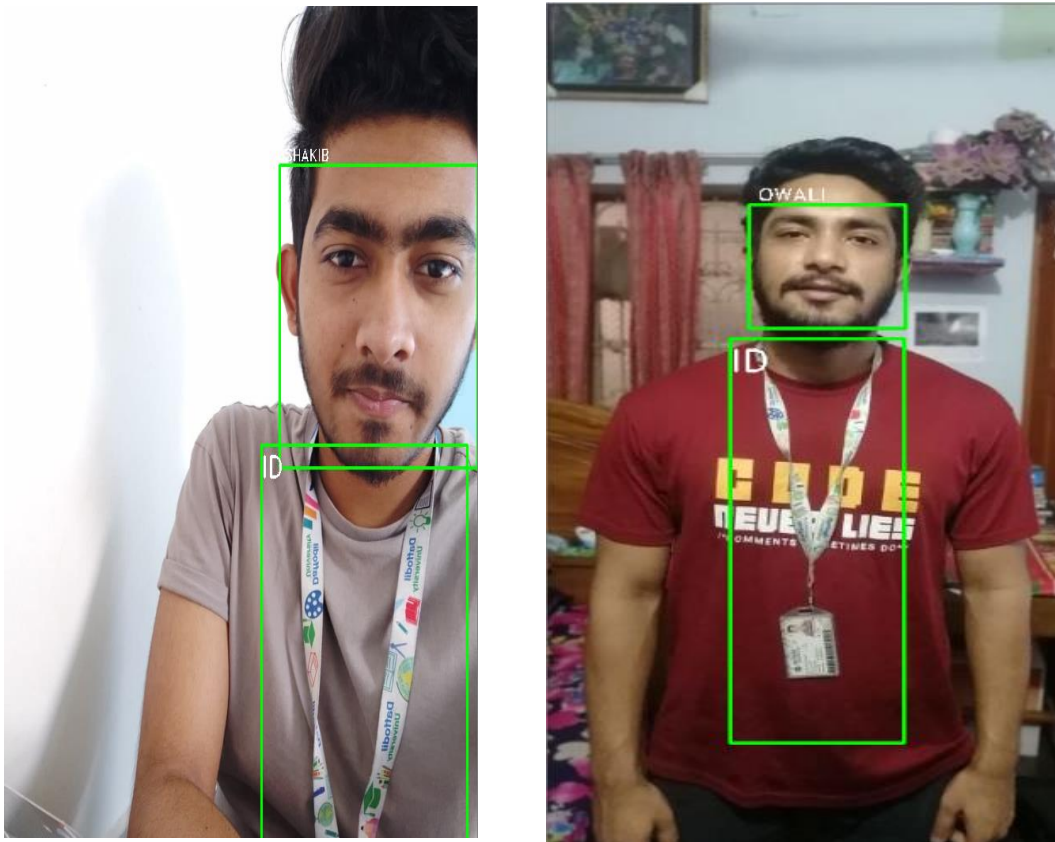
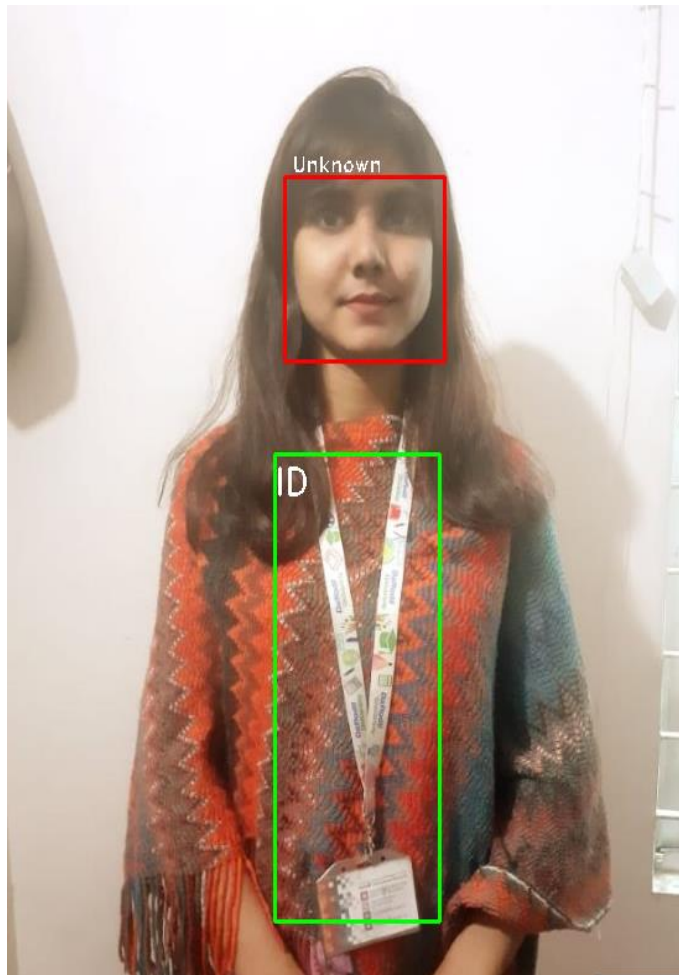


Figure 3.12: Authorized Person Detection

Those two test image face data is already existing in the dataset. The system has successfully detected those faces and also showing the names of those person. It has also successfully detected the id card position.



Let's also see an example of unauthorized person.



3.13: Unauthorized Person Detection

Here this person has wear the authorized id cand but her image is not in the database that why the system has recognized has as an unauthorized person.

### **3.4 Implementation Requirement**

The requirements of our proposed system are given below:

1. GPU base Computer (Laptop or Desktop)
2. Integrated Development Environment (Spyder, Google Colab)
3. Python
4. Face Recognition and YOLO V3 model
5. Open CV
6. LabelImg
7. Database



## Chapter 4

### Experimental Result and Analysis

#### 4.1 Experimental Setup

The required experimental setup is given below:

- 1.Spyder
- 2.Google colab
- 3.Database

#### 4.2 Experimental Result and Analysis

In order to understand how efficient our proposed model is, we trained our model with 700 data's and we tested on 300 data, including 220 known persons with Id card data and 80 unknown person data. We were able to discover the majority of known people since our trained model learned well and identified them, and our model also performed well when detecting unknown persons. Detecting the known person error has the lowest potential error, and detecting an unknown person error is also low. Our systems predicted confusion matrix is given below:

	NO	YES	
Unknown-	<b>TN</b> 58	<b>FP</b> 22	NO
Known-	<b>FN</b> 20	<b>TP</b> 200	YES
	Unknown-	Known-	

4.1: Confusion Matrix

	Precision	Recall	F-1 score
Known	0.900900	0.900901	0.9009005
Unknown	0.725000	0.743589	0.7341919
Accuracy			0.86

Figure 4.2: Accuracy Parentage

By examining our findings, we can observe that the percent of accurate positive known classification form instances we forecasted as known had a precision of 0.900900, whereas the percent of accurate positive unknown classification form instances had a precision of 0.725. As a result, our suggested model's prediction for known data performed similarly to recall, making our model exceptionally good at spotting known people. Furthermore, our model worked well for unknown data. Despite the fact that our model's overall accuracy is 0.86 percent, which is fairly excellent, we discovered that our model performs best at identifying known and does better in identifying unknown. We developed such an effective and helpful model by investigating and studying human face and object feature extraction. Stopping unauthorized access in any company is one of the biggest flaws of our current security system, according to Bangladesh's view. Our approach also solves a missing aspect of our current security system: by adopting our suggested model in a corporate organization, we can detect practically every authorized individual and stop roughly 70-75% of unauthorized access attempts.

### **4.3 Model Testing**

Our Model should be tried appropriately from start to finish before freely accessible as a framework for the end-clients. There is a couple of essential testing and these are:

- **Functionality Testing:** check every one of the connections in the system, database connection, structures utilized for monitoring.
- **Usability Testing:** particularly human-PC connections and shortcomings are estimated during this test.
- **Interface Testing:** This is finished by checking that correspondence is done appropriately.
- **Compatibility Testing:** Making sure it works the same in all pc operating systems.
- **Performance Testing:** Testing speed that is easily manageable for end users.
- **Security Testing:** Unauthorized access is not allowed in any situation.

## Chapter 5

### Impact on Society, Environment and Sustainability

#### 5.1 Impact on Society:

The effect of our research on society is astounding. Monitoring has reached new heights thanks to facial recognition technology. It allows authorities to monitor your every move by enabling automatic and indiscriminate live monitoring of people while they're in their everyday lives. But here we will check if the person is the true one or not. So that we can find out the real person who has access to the specific place. As a result of this operation, society is more stable against fraud and bad people. And the institution that verified people is secured.

Using facial recognition, police and security services can process photographs from a wide range of sources, like body-worn, smartphone, and also in cameras, to detect person investigations.

When we arrive, this facial recognition lets the immigration and baggage pickup processes go smoothly and stress-free.

It can be used to supervise booking and security tests to ensure optimum service levels, as well as to identify suspicious individuals and send automatic warnings to security personnel on the ground.

In the retail industry, it can be used to expedite fraud and theft investigations or to process photos from various sources to recognize people of interest. It's also used to identify consumers in a loyalty program and provide outstanding care.

#### 5.2 Impact on Environment

By comparing images and video with databases like driver's license records, law enforcement authorities and certain businesses can identify offenders and victims. However, civil liberties organizations claim that facial recognition compromises privacy and is vulnerable to violence. So, without the business or the government organization the product should not be open to the market for the general public.

### **5.3 Ethical Aspect**

Ethics is a commentary on nature and a concept of "what is right." If we talk about ethics, then organizations are most responsible for it. The organizations that will use this have to play an honest role. They should not use the data in the wrong way. It is an honor for them to act reasonably. If anyone steals data from any institution then it is against the ethical aspect. General public has less to deal with these but sometimes they have to cooperate if any wrong doing happens.

Need, complicity, impartiality, bias, and responsibility are all topics that have come up, and oversight when it comes to ethics. Some software engineers are hesitant to work on public-safety-related technology. Many jurisdictions exist at the local, state, and federal levels under governance systems such as the United States. Outside groups are concerned that a haphazard rollout may lead to unethical use without control. The topic of privacy raises many problems. Who will control the data on facial images? How will this information be shared between the police and the public security team? Is it going to be stored safely or is it going to be vulnerable to hostile actors?

Face recognition has the ability to make it easier to discover known or suspected terrorists, especially in crowded places, in the absence of responsible development, reducing the risk of racial profiling. It might also help speed up time-consuming administrative tasks like paperwork, line-ups, and minimal security. On the plus side, face recognition and AI in general might be used to rapidly clear overturned convictions by matching people to booking photographs linked to records.

As a result, surveillance systems may be faulty when modeling and comparing the faces of persons of color, women, and the elderly. The racial component is extremely disturbing, especially in developed countries like the USA. In comparison to other demographics, black males and gay women of color are significantly imprisoned. Inaccurate face recognition software has the ability to exacerbate this difference; further, it has the ability to grow the number of misidentified identities owing to false matches.

## **5.4 Sustainability Plan**

The ability to maintain indefinitely across different realms of life is referred to as sustainability. The stability will be maintained as the institution requires.

This ground is especially relevant to bodies and organizations performing public-interest responsibilities. To rely on it, the system administrator must demonstrate that it is acting with authority and judgment. Furthermore, the mission or function of the data controller must be defined under State legislation. While specific legislative provision is not required, the data controller's responsibilities, duties, or powers must be sufficiently clear and specific. As a result, corporate entities can only use this ground to a limited extent.

Furthermore, the administration should apply the following rules to sustain the plan of the security system. They have to assign a responsible person for the specific task who will be responsible for the information they provide.

## **Chapter 6**

### **Conclusion and Implication of Future Research**

#### **6.1 Conclusion**

This study developed a model for face recognition and id card detection to ensure protection. The system will detect the position of the face and id card. If the face is in the dataset, the system will recognize the individual and display their name, as well as detect the image's id card location. If the face is not in the dataset, then it will mark the face position of that face and label it as an unknown person. With the dataset, our proposed model's face recognition and object detection accuracy are about to 86 percent.

#### **6.2 Implication for Further Study**

The goal for the future is to increase the success rate by improving the detection conditions for faces and objects, as well as improving area segmentation. Extracting a new feature also will help to increase the success rate. Moreover, adding new features like tracking a human for his unacceptable activity can also be a scope. Where it can play a vital role in avoiding any kind of harmful situation. Based on our model a monitoring system can be developed where we can optimize a safer, more efficient, and secure environment for our people.

## References

- [1] A. S. M. ., A. M. Asif Anjum Akash, "Improvement of Haar Feature Based Face Detection in OpenCV Incorporating Human Skin Color Characteristic," 2016.
- [2] A. N. Georgy Kukharev, "Visitor Identification - Elaborating Real Time Face Recognition System".
- [3] D. A. Dwi Ana Ratna Wati, "Design of Face Detection and Recognition System," in 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), 2017.
- [4] X. Z. Z. L. X. W. H. S. S. Z. L. Shifeng Zhanga, "Detecting Face with Densely Connected Face Proposal Network," Elsevier, 2018.
- [5] R. N. C. S. Diana Martinez-Mosquera, "Matlab Simulation of Algorithms for Face Detection in Video Surveillance".
- [6] A. H. M. Z. U. R. F. A. A. A. M. P. Danish Ali Chowdhry, "Smart Security System for Sensitive Area," in IEEE Conference, 2013.
- [7] J. Du, "Understanding of Object Detection Based on CNN Family and YOLO," 2018.
- [8] G. K. M. P. Harihara Santosh Dadi, "Improved Face Recognition Rate Using HOG Features and SVM Classifier," IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) , 2016.
- [9] G. K. M. P. M. L. M. Harihara Santosh Dadi, "Face Recognition and Human Tracking Using GMM,HOG and SVM in Surveillance Videos," Springer, 2017.
- [10] L. D. J. Y. Z. W. J. Lin Zheng Chun, "YOLOv3: Face Detection in Complex Environments," 28 July 2020.
- [11] Z. H. Z. W. C. L. B. G. Wangpeng He, "TF-YOLO: An Improved Incremental Network for Real-Time Object Detection," 21 July 2019.
- [12] S. Ouhbi, J. . L. Fern ´andez-Alem ´an, A. Toval, A. Idr and J. R. Pozo, "Free Blood Donation Mobile Applications," Springer Science+Business Media New York, 2015.
- [13] P. L. C. C. L. X. T. Shuo Yang1, "WIDER FACE: A Face Detection Benchmark," IEEE Xplore, p. 9.



- [14] Z. Z. Z. L. Y. Q. Kaipeng Zhang, "Joint Face Detection and Alignment Using Multitask," IEEE, p. 5, 2016.
- [15] H. Peng, "Application Research on Face Detection Technology based on," International Journal of Signal Processing, Image Processing and Pattern Recognition, 2015.
- [16] S. A. S. Jamal M.Al-Tuwaijari, "Face Detection System Based Viola-Jones Algorithm," in 6th International Engineering Conference , 2020.
- [17] M. S.KALAS, "REAL TIME FACE DETECTION AND TRACKING USING OPENCV," 2014.
- [18] H. T. W. Y. ZHENG XIANG, "The Excellent Properties of a Dense Grid-Based HOG Feature on Face Recognition Compared to Gabor and LBP," IEEE, p. 12, 2018.
- [19] J. R. M. Ian R. Fasel, "A Comparison of Face Detection Algorithms," 2015.
- [20] M. K. K. H. N. S. I. S. Kushsairy Kadir, "A Comparative Study between LBP and Haar-like features for Face Detection Using OpenCV," 2014.
- [21] K. A. ., R. K. Kruti Goyal, "Face Detection and Tracking," 2017.
- [22] K. M. S. I. M. Hassaballah, "Face detection evaluation: a new approach based on the golden ratio  $\Phi$ ," Springer, 2011.
- [23] Q. Z. J. N. W. J. Li Cuimei, "Human face detection algorithm via Haar cascade classifier combined with three additional classifiers," in IEEE 13th International Conference on Electronic Measurement & Instruments, 2017.
- [24] T. B. N. Z. M. N. Sirine Ammar, "Towards an Effective Approach for Face Recognition with DCGANs Data Augmentation," 2020.
- [25] Š. K. Zuzana Képešiová, "An Effective Face Detection Algorithm," 2018.
- [26] L. W. P. R. WEI FANG, "Tinier-YOLO: A Real-Time Object Detection Method for Constrained Environments," IEEE Access, 2020.

# PLAGIARISM REPORT

---

**ORIGINALITY REPORT**

---

<b>13%</b> SIMILARITY INDEX	<b>13%</b> INTERNET SOURCES	<b>4%</b> PUBLICATIONS	<b>%</b> STUDENT PAPERS
--------------------------------	--------------------------------	---------------------------	----------------------------

---

**PRIMARY SOURCES**

---

<b>1</b>	<a href="https://dspace.daffodilvarsity.edu.bd:8080">dspace.daffodilvarsity.edu.bd:8080</a> Internet Source	<b>12%</b>
<b>2</b>	<a href="http://www.ijert.org">www.ijert.org</a> Internet Source	<b>&lt;1%</b>
<b>3</b>	<a href="http://www.mdpi.com">www.mdpi.com</a> Internet Source	<b>&lt;1%</b>
<b>4</b>	<a href="http://utpedia.utp.edu.my">utpedia.utp.edu.my</a> Internet Source	<b>&lt;1%</b>
<b>5</b>	Dwi Ana Ratna Wati, Dika Abadianto. "Design of face detection and recognition system for smart home security application", 2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), 2017 Publication	<b>&lt;1%</b>
<b>6</b>	<a href="http://link.springer.com">link.springer.com</a> Internet Source	<b>&lt;1%</b>

---