

DESIGN AND IMPLEMENTATION OF IoT BASED WIRELESS REAL-TIME VIDEO SURVEILLANCE

A Project Report Phase – II

Submitted in partial fulfilment of the requirements for the award of
Bachelor of Engineering degree in Electronics and Communication Engineering

by

RAHINI RAJASEKAR (39130364)

SANGEETHA K (39130395)



DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

SCHOOL OF ELECTRICAL AND ELECTRONICS

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with Grade “A” by NAAC

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119.

APRIL - 2023



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with "A" grade by NAAC

Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai – 600 119

www.sathyabama.ac.in

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is a bonafide work of **RAHINI RAJASEKAR** (REG NO: 39130364) and **SANGEETHA K** (REG NO: 39130395) who carried out the project entitled "**DESIGN AND IMPLEMENTATION OF IoT BASED WIRELESS REAL-TIME VIDEO SURVEILLANCE**" under our supervision from November 2022 to April 2023.

Internal Guide

Dr. T BERNATIN, M.E., Ph.D.

Head of the Department

Dr. T. RAVI, M.E., Ph.D.

Submitted for Viva Voce Examination held on 21.04.2023

Internal Examiner

External Examiner

DECLARATION

We, **RAHINI RAJASEKAR** (REG NO: 39130364) and **SANGEETHA K** (REG NO: 39130395) hereby declare that the Project Report entitled “**DESIGN AND IMPLEMENTATION OF IoT BASED WIRELESS REAL-TIME VIDEO SURVEILLANCE**” done by us under the guidance of **Dr. T BERNATIN, M.E., Ph.D.** is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Electronics and Communication Engineering.

DATE:

PLACE:

1.



2.



SIGNATURE OF THE CANDIDATES

ACKNOWLEDGEMENT

We are pleased to acknowledge our sincere thanks to **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. We are grateful to them.

We convey our thanks to **Dr. N.M. NANDHITHA, M.E., Ph.D., Dean, School of Electrical and Electronics** and **Dr. T. RAVI M.E., Ph.D., Head, Department of Electronics and Communication Engineering** for providing us necessary support and details at the right time during the progressive reviews.

We would like to express my sincere and deep sense of gratitude to our **Project Guide Dr. T BERNATIN, M.E, Ph.D.**, for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of our project work.

We wish to express our thanks to all Teaching and Non-teaching staff members of the Department of Electronics and Communication Engineering who were helpful in many ways for the completion of the project.

ABSTRACT

Internet of Things offers user interoperability and connectivity between devices, systems, services, networks and in particularly control systems. Smart video surveillance is an IOT based application as it uses Internet for various purposes. IOT based Video Surveillance is the latest technology used in wide range of places. Video surveillance serves as the remote eyes for management and the security force. In the existing technique, AdaBoost algorithm needs a quality data set. And also, noisy data and outliers have to be avoided before adopting this algorithm. So, In this project Machine Learning Techniques are Haar-Cascade and Local Binary Pattern Histogram algorithms are used to overcome the above disadvantage to detect the face clearly. The camera module capturing an image of a person as soon as the smart home switches is being pressed and sends the still image to the android device through telegram app and alerts the owner about the person standing at the door. The entire systems programming has been established in python and the Embedded C for a controller.

KEYWORDS: IoT, Arduino, AdaBoost, Haar-Cascade, LBPH, ML, Telegram

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	ABSTRACT	vii
	LIST OF FIGURES	x
	LIST OF TABLES	xi
	LIST OF ABBREVIATIONS	x
1.	INTRODUCTION	1
	1.1 MACHINE LEARNING TECHNIQUES	2
	1.2 PROBLEM STATEMENT	3
	1.3 OBJECTIVE	3
2.	LITERATURE REVIEW	4
	2.1 LITERATURE SURVEY	4
	2.2 UNIQUENESS OF THE PROJECT COMPARED TO EXISTING ONE	7
3.	METHODOLOGY	9
	3.1 EXISTING METHODOLOGY	9
	3.2 PROPOSED METHODOLOGY	9
	3.3 DIFFERENCE BETWEEN EXISTING AND PROPOSED SYSTEM	9
	3.4 BLOCK DIAGRAM OF PROPOSED WORK	10
	3.5 FLOW CHART OF PROPOSED WORK	12
	3.6 EXISTING ALGORITHMS	13
	3.7 PROPOSED ALGORITHMS	14
4.	REQUIREMENT ANALYSIS	26
	4.1 HARDWARE USED	26

4.2	SOFTWARE USED	28
4.3	PROJECT MANAGEMENT PLAN	32
4.4	FINANCIAL REPORT ON ESTIMATED PLAN	34
4.5	SOFTWARE TO OPERATION PLAN	35
4.6	DEVELOPMENT AND DEPLOYMENT	37
4.7	TESTING	38
5.	RESULTS AND DISCUSSION	40
6.	CONCLUSION	49
6.1	FUTURE WORK	50
6.2	PERFORMANCE ANALYSIS	50
	REFERENCES	53

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE NO.
3.1	BLOCK DIAGRAM OF PROPOSED WORK	10
3.2	FLOW CHART OF PROPOSED WORK	12
3.3	HAAR FEATURES	16
3.4	INTEGRAL IMAGES	17
3.5	LBPH MECHANISM	19
3.6	LBPH FLOW CHART	21
3.7	FLOW CHART OF LBPH AND HAAR CASCADE	22
3.8	FACE RECOGNITION	24
3.9	FEATURE EXTRACTION	25
4.1	FACE DETECTION USING OPENCV	30
4.2	CAPTURING VIDEO USING OPENCV	31
5.1	HARDWARE SETUP	40
5.2	DATA SET	41
5.3	TRAINING DATA	41
5.4	FACE RECOGNITION	42
5.5	LIVE PERMISSION GRANTED	43
5.6	LIVE PERMISSION DENIED	44
5.7	MANUALLY OPENING DOOR	45
5.8	MANUALLY CLOSING DOOR	46
5.9	MANUALLY TAKING LIVE PHOTO	47
5.10	MANUALLY LIVE VIDEO	48

LIST OF TABLES

TABLE NO	TITLE	PAGE NO
4.1	SPECIFICATIONS OF MOTOR	27
4.2	PIN DETAILS OF MOTOR	27

LIST OF ABBREVIATIONS

IOT	Internet of Things
ML	Machine Learning
LBPH	Local Binary Pattern Histogram
LCD	Liquid Crystal Display
DVD	Digital Versatile Disc
RFID	Radio Frequency Identification
PCA	Principal Component Analysis
CV	Computer Vision
XML	Extensible Markup Language
TTL	Transistor-Transistor Logic
API	Application Programming Interface

CHAPTER 1

INTRODUCTION

Ensuring security is crucial in day-to-day life as well as work environment. Typically, security systems are deployed in an intended area, and are standalone systems. Recently Internet of Things (IOT) has been used in various fields such as smart homes, smart cities, transportation and creating a smart environment. The advantage of IOT based systems is remote access, collecting crucial data which in turn helps in tracking, increasing efficiency and saving costs. An IOT based smart door locking system can alleviate the shortcomings of a conventional locking mechanism. IoT technology is used to improve or perhaps create a new security system. In this project, we chose the latter option and built a smart and safe door lock system. In this paper machine learning techniques to improve security (machine learning is the construction of computers and systems capable of self-adapting based on the study of patterns in training input data). By using the principles of computer vision in facial recognition, to create a security system that not only relies on standard authorization practices but also has an added layer of impenetrable security while still maintaining the basic concept of easy-to use minimal interaction IoT system. This project stemmed from the idea that in the modern-day and age standard locks, no matter how well made cannot live up to the full potential in terms of the security provided without the use of the tools that technology provides. A standard lock and key mechanism have several problems such as the compulsory requirement of carrying a physical key, which can get lost or if fallen into wrong hands easily duplicated. Furthermore, the complete lack of tracking systems makes it so that if anyone was to enter the home, the owner will not have the faintest idea as to who that person may be. This system aims to combat these scenarios by creating a lock system, which replaces the need for physical keys and keeps track of which person has been granted access at what time.

In this project a practical locking system for doors that can be used in buildings. The major components of the system consist of the motor (L298N) to control the locking and unlocking of the door, LCD, DVD loader, switch and Microcontroller.

Internet of Things: The internet of Things additionally called the internet of articles,

refers to a remote system between items. The term IOT has come to portray various advances and research teach that empower the web to connect into this present reality of physical articles. There are various technologies that enable IOT:

- RFID and near-field communication
- Optical tags and quick response codes
- Bluetooth low energy
- ZigBee

1.1 MACHINE LEARNING TECHNIQUES

WHAT IS MACHINE LEARNING?

IoT and machine learning deliver insights otherwise hidden in data for rapid, automated responses and improved decision making. Machine learning for IoT can be used to project future trends, detect anomalies, and augment intelligence by ingesting image, video and audio.

WHY USE MACHINE LEARNING FOR IOT?

Machine learning can help demystify the hidden patterns in IoT data by analyzing massive volumes of data using sophisticated algorithms. Machine learning inference can supplement or replace manual processes with automated systems using statistically derived actions in critical processes.

With machine learning for IoT, you can:

- Ingest and transform data into a consistent format
- Build a machine learning model
- Deploy this machine learning model on cloud, edge and devices

1.2 PROBLEM STATEMENT

Security and safety are becoming more and more popular day by day. Hence, it is getting improved and used for the ease in our life. Nowadays, technology has become an integrated part of people's lives therefore the security of one's home, office or organization must not be left behind. Our goal is to design a system with minimum human intervention. Smart Receptionist with smart lock system is mainly designed and developed for security and safety purposes. This smart security system is used to see a visitor when the main door of the office or organization is closed. The purpose of this system is to control the door lock and authorization using Telegram Application. In this system, whenever a person rings the bell, image of the person is captured by the camera. If person's image is present in database, he/she will be allowed in else if image is not present in the database, then the smart lock system will send the image to Telegram App for Authorization. Once the image is sent to the Telegram Application, option will be available with user of either locking or unlocking the door. If the user clicks on unlock button the door will open and person standing on the door will be allowed in and if the user clicks on lock button the door will remain locked and person will not be allowed in door.

1.3 OBJECTIVE

Our main objective of the project is to build a robust IOT based security solutions which could be used in multiple scenarios like for class rooms during pandemic situations, bank locker rooms, women's hostel, confidential meeting rooms to authenticate only authorized person by using embedded 'c' & python language integrated with telegram chat-bot.

CHAPTER 2

LITERATURE REVIEW

2.1 LITERATURE SURVEY

Jing-Ming Guo et al. [1] (2011) proposed the Ada boosting has attracted attention for its efficient face-detection performance. Probability-based Face Mask Pre-Filtering (PFMPF) is presented to reserve the face candidates with a higher accuracy. The two stages both provide far less training time than that of the cascade Ada boosting and thus reduce the computation complexity in face-detection tasks. The performance of a face detection system is normally evaluated based four metrics: 1) training time, 2) detection time, 3) detection rate, and 4) false positive rate. Although the detection rate and false positive rate are somewhat inferior to that of Haar-like feature

Y. Januzaj. et al. [2] (2011) proposed real time access control for face recognition using, Raspberry pi instead of GSM services and relay. The limitation of the work was it couldn't control the background light situation and ambient light conditions.

H Lwin.et al. [3] (2015) has proposed a door lock access system which consists of three subsystems: to be specific face recognition, face detection, and automated door access control. Face recognition is actualized by using the Principal Component Analysis. The door will open itself for the known person in command of the microcontroller and caution will ring for the unknown person. Demerit of this system is input images are taken through a web camera continuously until the 'stop camera' button is pressed. Somebody is required at the location to check unauthorized person's images or status of the system and take further appropriate action. Personal computer (PC) is associated with the microcontroller, The entire system will not work if PC is crashed or non-Function.

M. Chowdhury.et al. [4] (2013) had implemented security system where if any person came at the door it was notified to the home owner via e-mail and twitter then the user could see the person standing at the door using camera from remote location. The image of the person got captured and sent to twitter and e-mail. They stated that user couldn't control the door remotely. They had concluded that this system was useful for

preventing unauthorized access. The limitation of this work was that the alert generated was sent to the mail and twitter account but if the user didn't have internet connection on his/her phone, he/she couldn't check the mail and couldn't recognise that any unauthorized person was trying to access the door.

G. senthilkumar.et.al. [5] (2014) proposed a work on Embedded Image Capturing System Using Raspberry Pi. In this work, they captured the image and compared it with the database but the limitation was the system couldn't work properly in the ambient light condition.

S. Jogdand.et.al [6] (2015) proposed a work on Implementation of Automated Door Accessing System with Face Design and Recognition in which they used Viola Jones method for face detection and PCA (Principal Component Analysis) for the comparison of images. The limitation of this work was that it is not robust and the efficiency is less.

U. Sowmiya.et al [7] (2015). Developed to connect any door with internet. In this system user also implemented PIR sensor and camera. PIR sensor used for detecting person and camera used for capturing the video of the person who comes at the door. The video was sent through 3g dongle to authorized person. They had also discussed some advantages of this system. They had concluded use of this system in banks, hospitals etc. But their proposed model didn't provide the facility of sending messages to the authorized people.

Karthik A Patil et al [8] (2020). This paper proposed biometric locks over traditional keyed locks to improve the security of their homes or workplaces. In contrast to the conventional lock, a cutting-edge biometric lock requires no key to bolt or open the door and instead uses a biometric sensor. Even though bio-metric is used this system is cost-effective.

J. Kartik et al [9] (2013). Have proposed two systems are proposed, one is based on GSM technology and other uses a web camera to detect the intruder. The first security system uses a web camera, installed in house premises, which is operated by software installed on the PC and it uses the Internet for communication. The camera identifies movement of any intruder before the camera measurements or camera range. The

product imparts to the planned client through Internet arrange and, in the meantime, it gives a sound alarm. The second security system is SMS based and utilizes GSM innovation to send the SMS to the owner. But the user cannot able to view the unauthorized person's image who try to intrude.

Taewan Kim et al. [10] (2013) proposed a smart door phone system to automatically turn a narrow angle camera in the direction of a voice source to improve the face recognition rate. But the surrounding noise will affect the system.

Ni Ni San Hlaing and San SanLwin [11] (2019) proposed "Arduino based electronic lock using RFID and password". This digital door lock runs on the technology of audio-frequency identification and passcode-based with the help of an Arduino Uno MCU. Just like traditional keys, you can forget your keycards. It is possible the system can be hacked or bypassed by someone who is tech savvy so they are not fool proof. One major problem is that electric RFID systems may malfunction during power outages.

Arpita Mishra et al. [12] (2020) proposed "Secured password-based lock system". This methodology is targeted to prevent unlocking of the door by unknown individuals. The formation of the home safety Service consists of the numeric keypad, the hook which is used for lifting, and a GSM module to establish dependable connection for communication conferred with the MCU. The control panel conferred with the device is employed because the passcode access combination opens/closes the door. It will be high in cost and prone to jamming and hacking.

Shrinidhi Gindi et al. [13] (2020) proposed Room security solution supported IoT using RFID, the system is often monitored from anywhere within the world thanks to the continual updating of the status of the door. But the RFID tags can be read without the user's knowledge.

Mr. L. David William Raj et al. [14] (2021) proposed "An OTP-based wireless smart door locking system". In this innovation, the key phrase for security is initially put away within the Electrically Erasable Programmable ROM [EEPROM]. At the purpose when the client enters the proper secret phrase then the two-way confirmation of a haphazardly produced OTP is shipped off the client gadget. On the off chance that the OTP is

coordinated, the framework is going to be opened, and therefore the required capacity is often started. Process of OTP password generation can be cumbersome.

K. Jayanth et al. [15] (2022) proposed Smart television systems controlled by the owner via an Android mobile are frequently operated remotely as well as locally. When an intrusion is detected at the entrance, the system will send a notification to the android mobile using an IoT application for remote control. But This system needs electricity to run. In areas where there is a shortage of electricity people can't use this software because the electricity can go at any time.

Prashanth Balraj Balla et al. [16] (2022) The main objective of this system is to implement for a particular face and distinguishing it from a number of stored faces with some real time variations as well. But when there is no proper lighting, the facial features can't be viewed clearly.

Hteik Htar Lwin et al. [17] (2003) proposed "Automatic Door Access System Using Face Recognition". In this system, automatic face recognition and detection is done by MATLAB program on PC. Microcontroller is used to control the door access system depending on incoming data sent from PC. Door is opened immediately after confirming that the person is authenticated. After 2 seconds, door is closed automatically. However, 2 seconds are not enough time for a person to enter. So, longer time should be set for real-time conditions. Viola Jones algorithm is used for face detection. Since, this algorithm can only detect frontal view of the face correctly, this system has limitations.

Sandesh Kulkarni et al. [18] (2017) proposed "Face Recognition System Using IoT". The system developed was cost and power efficient. In this system, Viola Jones Algorithm is used for face detection that eliminates face candidates using a cascade of stages but the structural information captured by it is limited.

2.2 UNIQUENESS OF THE PROJECT COMPARED TO THE EXISTING ONE:

Compared to existing solutions, this project integrates face detection technology with Telegram chatbot functionality to provide a more comprehensive and automated approach to intruder detection. The use of face detection technology allows for accurate

and quick detection of unauthorized individuals, while the integration with a Telegram chatbot enables immediate notification and verification of the intruder.

Additionally, the use of a chatbot allows for real-time communication and updates on the status of the intruder, as well as the ability to control and manage the detection system remotely. This project also offers increased security and privacy by sending footage to a private Telegram chatbot, rather than storing it on a third-party server.

Overall, the uniqueness of this project lies in its combination of various technologies and its focus on real-time detection and verification, which provides a more comprehensive and automated approach to intruder detection compared to existing solutions.

CHAPTER 3

METHODOLOGY

3.1 EXISTING METHODOLOGY

Existing methodology used face detection and face recognition algorithms such as AdaBoosting algorithm and Principal Component Analysis as well as a wireless interface are used to recognize the visitor and send the information to the home owner's phone.

3.2 PROPOSED METHODOLOGY

In this Project program is developed using Python where facial recognition plays a major role and we connect this powerful machine learning tool with the hardware (Embedded Systems) to make in more efficient, effective and to provide real time solution. Our Concept works this way we have a button connected to the microcontroller of the project once when the button is pressed the camera gets activated and starts detecting the face using Haar-cascade and LBPH algorithm and the result is transmitted through serial communication which is connected to the microcontroller through pc once the face matches python will write the data to the Arduino microcontroller and that in turn will open the door automatically if the face is recognized and if the face is not recognized then the footage will be captured and will be sent to Telegram mobile Application through Bot Father once that process is completed the user now has the authority either to authenticate or not to authenticate that person if authentication is successful then the door opens else the door remains closed.

3.3 DIFFERENCE BETWEEN EXISTING AND PROPOSED SYSTEM

In an existing methodology after the theft only people come to know about the incident. But in this proposed system it can find it in advance if suspicious people try to get in by capturing their images and the images will be sent to the user's telegram via telegram chat-bot.

3.4 BLOCK DIAGRAM OF PROPOSED WORK

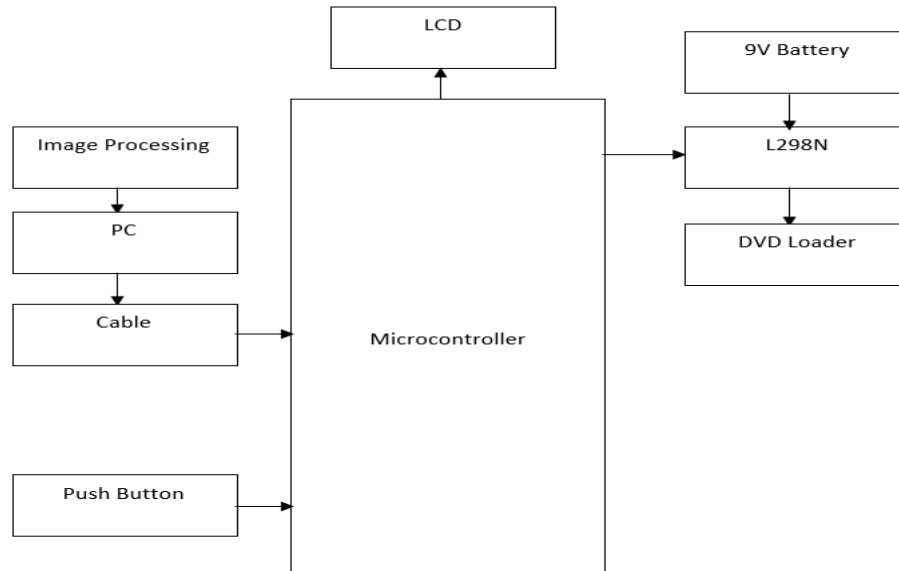


Fig:3.1: Block Diagram of Proposed Work

3.4.1 BLOCK DIAGRAM EXPLANATION

Arduino Uno which contains Atmega328P is used as the brain of the project which will help us to authorize and control the Motor Drive which will open the door based on the facial Recognition Matching System and an Capture Button is also integrated along with that upon pressing the capture button the camera gets activated and compares the Facial and Hardware process takes place to implement this concept we have used two programming language, one python to capture face to recognize and differentiate the known and unknow person once that process is completed the authorization takes place using Telegram BOT (Chat-bot)) system which helps us to give access and apart from that a hardware device is connected to reflect the hardware process to show us the door mechanism.

3.4.2 List of Modules:

Module 1: Hardware Integration.

Module 2: Python Programming for Facial Recognition with Integration with Telegram Chat-bot.

Module 3: Embedded 'C' Programming & Testing.

Module Description:

Module 1:

We Will be Using Arduino Microcontroller Integrated with 16 * 2 Lcd Display, Motor Driver and DVD Loader, Battery to control the hardware based on the Inputs received from the python for Authentication.

Module 2:

In This Model we will be creating Program to Detect and Recognize Face for Authentication Purpose. For Efficient Facial Frontal Face Recognition, we will be Using Haar-Cascade Algorithm with LBPH Operators which helps in extracting local features in the face and match it with the most similar face image in the database. Upon Completion we will send the Footage to the Integrated Telegram Chat-Bot.

Module 3:

We will be creating Program to receive serial values from python and perform operations in the hardware based on the received feed-back by using Embedded 'C' Language to control the Hardware Systems.

3.5 FLOW CHART

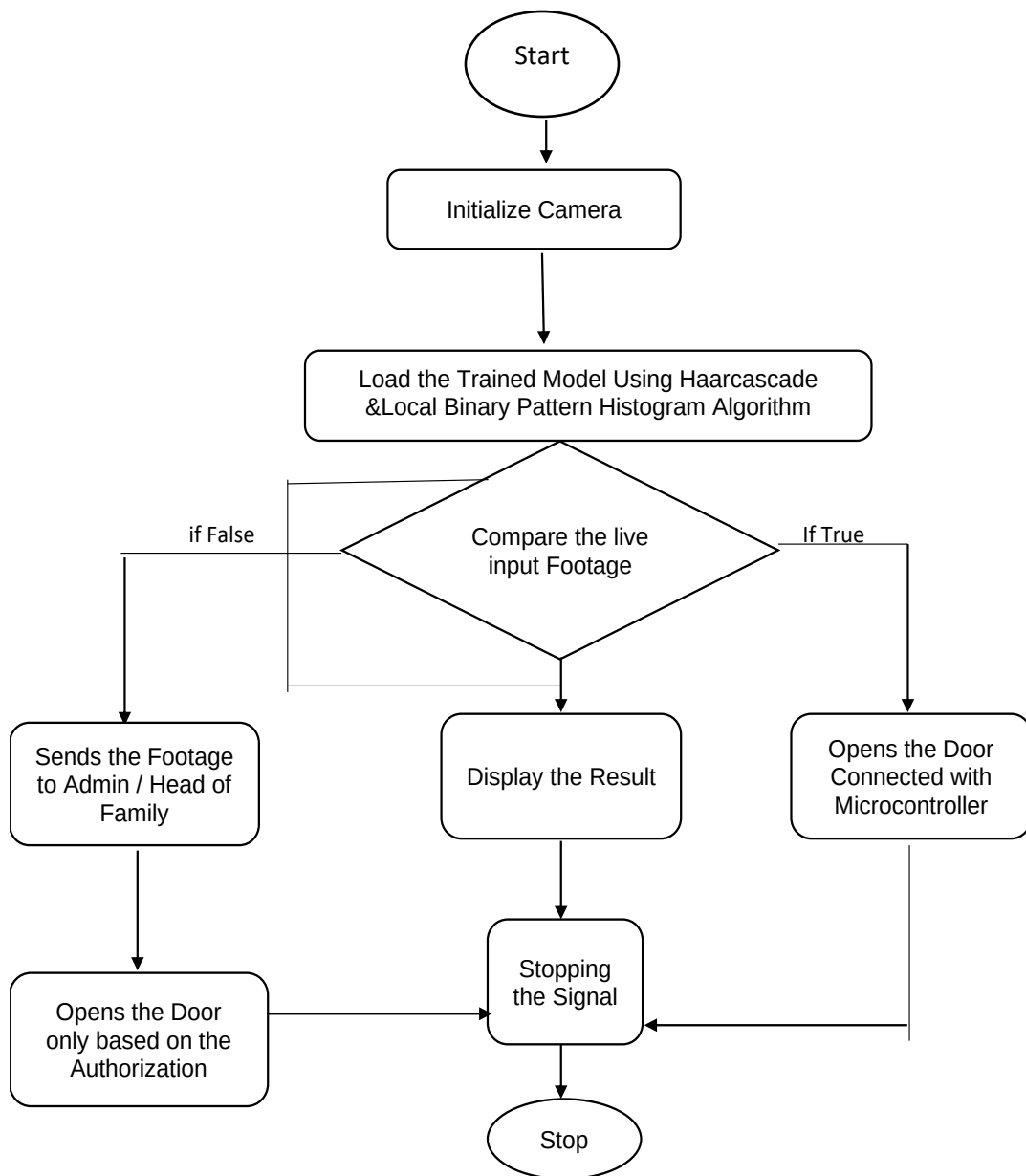


Fig:3.2: Flow chart

3.5.1 Image Processing Using Python:

Image processing allows us to transform and manipulate thousands of images at a time and extract useful insights from them. It has a wide range of applications in almost every field. Python is one of the widely used programming languages for this purpose.

3.5.2 Embedded Systems:

An embedded system is a combination of computer hardware and software designed for a specific function. Embedded systems may also function within a larger system. The systems can be programmable or have a fixed functionality. An embedded system is a microcontroller or microprocessor-based system which is designed to perform a specific task.

Embedded systems consist of a microcontroller with on-board memory, a power supply, and communication ports for transmitting data to other devices. Embedded software programs tell the microcontroller how to respond in real time to data collected from the environment through peripheral sensors and devices.

3.5.3 Telegram Chat-Bot:

A chatbot is an automated multifunctional assistant, that can receive send and send triggered messages, and with Send Pulse, your bot can save information as variables for future usage.

3.6 EXISTING ALGORITHMS

3.6.1 ADABOOSTING ALGORITHM:

Boosting is an ensemble modeling technique that attempts to build a strong classifier from the number of weak classifiers. It is done by building a model by using weak models in series. Firstly, a model is built from the training data. Then the second model is built which tries to correct the errors present in the first model. This procedure is continued and models are added until either the complete training data set is predicted

correctly or the maximum number of models are added. AdaBoost was the first really successful boosting algorithm developed for the purpose of binary classification. AdaBoost is short for Adaptive Boosting and is a very popular boosting technique that combines multiple “weak classifiers” into a single “strong classifier”. It was formulated by Yoav Freund and Robert Schapire. They also won the 2003 Gödel Prize for their work.

3.6.2 PRINCIPAL COMPONENT ANALYSIS (PCA) ALGORITHM:

Principal Component Analysis (PCA) is a statistical procedure that uses an orthogonal transformation that converts a set of correlated variables to a set of uncorrelated variables. PCA is the most widely used tool in exploratory data analysis and in machine learning for predictive models. Moreover, PCA is an unsupervised statistical technique used to examine the interrelations among a set of variables. It is also known as a general factor analysis where regression determines a line of best fit.

3.7 PROPOSED ALGORITHMS

3.7.1 HAAR CASCADE ALGORITHM

Object Detection is a computer technology related to computer vision, image processing and deep learning that deals with detecting instances of objects in images and videos. We will do object detection in this article using something known as haar cascades.

The algorithm can be explained in four stages:

- Calculating Haar Features
- Creating Integral Images
- Using Adaboost
- Implementing Cascading Classifiers

It's important to remember that this algorithm requires a lot of **positive images** of faces and **negative images** of non-faces to train the classifier, similar to other machine learning models.

Haar Cascade Classifier

- Loading the input image using built in function `cv2.imread(img_path)`, here the passing the image path as an input parameter
- Converting it to gray scale mode and then displaying it
- Loading the haar cascade classifier

Haar value calculation:

Pixel value = (Sum of the Dark pixels/Number of Dark pixels)

- (Sum of the Light pixels/Number of Light pixels)

Haar classifier is an object detection algorithm. In order to detect the object and to identify what it is, the features will be extracted from the Image. Using the above equation haar pixel value can be calculated.

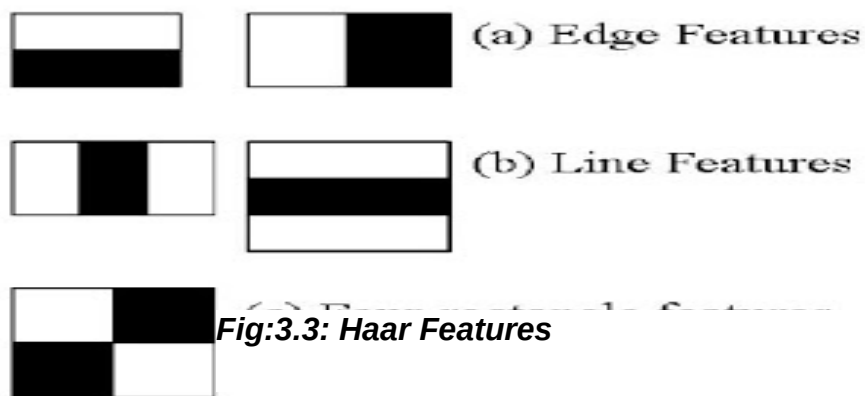
It is an Object Detection Algorithm used to identify faces in an image or a real time video. The algorithm uses edge or line detection features proposed by Viola and Jones in their research paper “Rapid Object Detection using a Boosted Cascade of Simple Features” published in 2001. The algorithm is given a lot of positive images consisting of faces, and a lot of negative images not consisting of any face to train on them. These include models for face detection, eye detection, upper body and lower body detection, license plate detection etc.

The haar feature continuously traverses from the top left of the image to the bottom right to search for the particular feature. This is just a representation of the whole concept of the haar feature traversal. In its actual work, the haar feature would traverse pixel by pixel in the image. Also, all possible sizes of the haar features will be applied. Depending on the feature each one is looking for, these are broadly classified into three categories. The first set of *two rectangle features* are responsible for finding out the edges in a horizontal or in a vertical direction (as shown above). The second set of *three rectangle features* are responsible for finding out if there is a lighter region surrounded by darker regions on either side or vice-versa. The third set of *four rectangle features* are responsible for finding out change of pixel intensities across diagonals.

Calculating Haar Features

The first step is to collect the Haar features. A **Haar feature** is essentially calculations that are performed on adjacent rectangular regions at a specific location in a detection window. The calculation involves summing the pixel intensities in each region and calculating the differences between the sums.

These features can be difficult to determine for a large image. This is where **integral images** come into play because the number of operations is reduced using the integral image.



Creating Integral Images

Without going into too much of the mathematics behind it (check out the paper if you're interested in that), integral images essentially speed up the calculation of these Haar features. Instead of computing at every pixel, it instead creates sub-rectangles and creates array references for each of those sub-rectangles. These are then used to compute the Haar features.

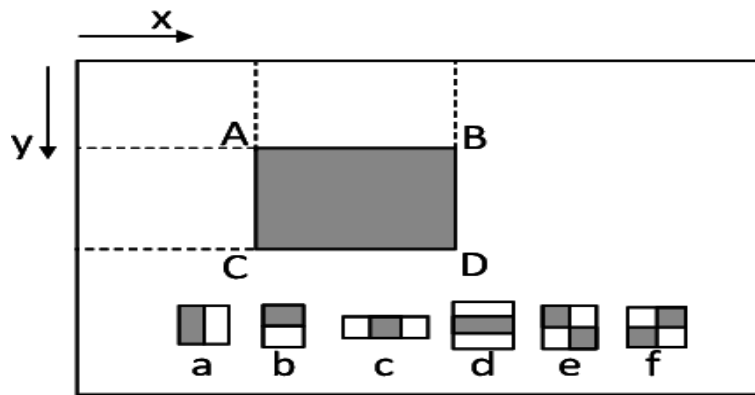


Fig:3.4: Integral Images

It's important to note that nearly all of the Haar features will be **irrelevant** when doing object detection, because the only features that are important are those of the object. However, how do we determine the best features that represent an object from the hundreds of thousands of Haar features. This is where **Adaboost** comes into play.

Rectangular Haar like Features:

A simple rectangular Haar-like feature can be defined as the difference of the sum of pixels of areas inside the rectangle, which can be at any position and scale within the original image. This modified feature set is called 2-rectangle feature. Viola and Jones also defined 3-rectangle features and 4-rectangle features. The values indicate certain characteristics of a particular area of the image

Applications of Haar Cascades

A few of the most important applications are listed below:

- **Facial Recognition:** Similar to how iPhone X uses facial recognition, other electronic devices and security protocols can use Haar cascades to determine the validity of the user for secure login.
- **Robotics:** Robotic machines can “see” their surroundings to perform tasks using object recognition. For instance, this can be used to automate manufacturing tasks.

- **Autonomous Vehicles:** Autonomous vehicles require knowledge about their surroundings, and Haar cascades can help identify objects, such as pedestrians, traffic lights, and sidewalks, to produce more informed decisions and increase safety.
- **Image Search and Object Recognition:** Expanding off facial recognition, any variety of objects can be searched for by using a computer vision algorithm, such as Haar cascades.
- **Agriculture:** Haar classifiers can be used to determine whether harmful bugs are flying onto plants, reducing food shortages caused by pests.
- **Industrial Use:** Haar classifiers can be used to allow machines to pick up and recognize certain objects, automating many of the tasks that humans could previously only do.

3.7.2 LOCAL BINARY PATTERNS HISTOGRAM (LBPH)

Local Binary Patterns Histogram algorithm was proposed in 2006. It is based on local binary operator.

It is widely used in facial recognition due to its computational simplicity and discriminative power.

The steps involved to achieve this are:

- face acquisition
- feature extraction
- creating dataset
- classification

The LBPH algorithm is a part of OpenCV.

1. **Parameters:** the LBPH uses 4 parameters:

- **Radius:** the radius is used to build the circular local binary pattern and represents the radius around the central pixel. It is usually set to 1.
- **Neighbors:** the number of sample points to build the circular local binary pattern. Keep in mind: the more sample points you include, the higher the computational cost. It is usually set to 8.

- **Grid X:** the number of cells in the horizontal direction. The more cells, the finer the grid, the higher the dimensionality of the resulting feature vector. It is usually set to 8.
- **Grid Y:** the number of cells in the vertical direction. The more cells, the finer the grid, the higher the dimensionality of the resulting feature vector. It is usually set to 8.

2.Training the Algorithm: First, we need to train the algorithm. To do so, we need to use a dataset with the facial images of the people we want to recognize. We need to also set an ID (it may be a number or the name of the person) for each image, so the algorithm will use this information to recognize an input image and give you an output. Images of the same person must have the same ID. With the training set already constructed, let's see the LBPH computational steps.

3. Applying the LBP operation: The first computational step of the LBPH is to create an intermediate image that describes the original image in a better way, by highlighting the facial characteristics. To do so, the algorithm uses a concept of a sliding window, based on the parameter's **radius** and **neighbors**.

The image below shows this procedure:

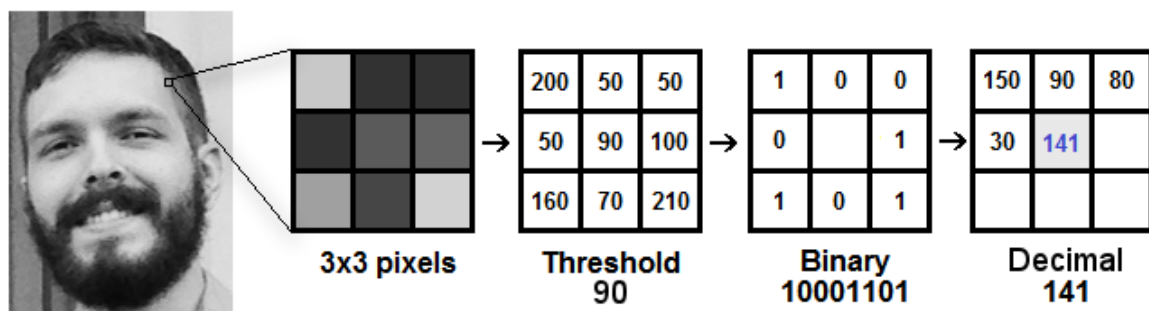


Fig: 3.5: LBPH Mechanism

Based on the image above, let's break it into several small steps so we can understand it easily:

- Suppose we have a facial image in grayscale.
- We can get part of this image as a window of 3x3 pixels.
- It can also be represented as a 3x3 matrix containing the intensity of each pixel (0~255).
- Then, we need to take the central value of the matrix to be used as the threshold.
- This value will be used to define the new values from the 8 neighbors.
- For each neighbor of the central value (threshold), we set a new binary value. We set 1 for values equal or higher than the threshold and 0 for values lower than the threshold.
- Now, the matrix will contain only binary values (ignoring the central value). We need to concatenate each binary value from each position from the matrix line by line into a new binary value (e.g., 10001101). Note: some authors use other approaches to concatenate the binary values (e.g., clockwise direction), but the final result will be the same.
- Then, we convert this binary value to a decimal value and set it to the central value of the matrix, which is actually a pixel from the original image.
- At the end of this procedure (LBP procedure), we have a new image which represents better the characteristics of the original image.
- **Note:** The LBP procedure was expanded to use a different number of radius and neighbors, it is called Circular LBP.

LBPH Flow chart :

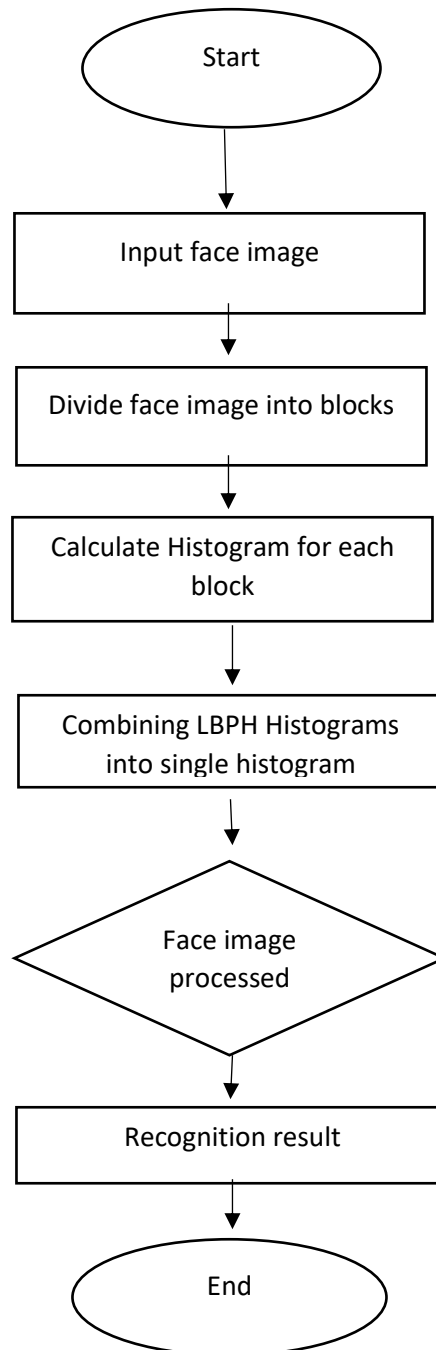


Fig:3.6: LBPH Flow chart

3.7.3 FLOW CHART OF HAAR CASCADE AND LBPH ALGORITHM

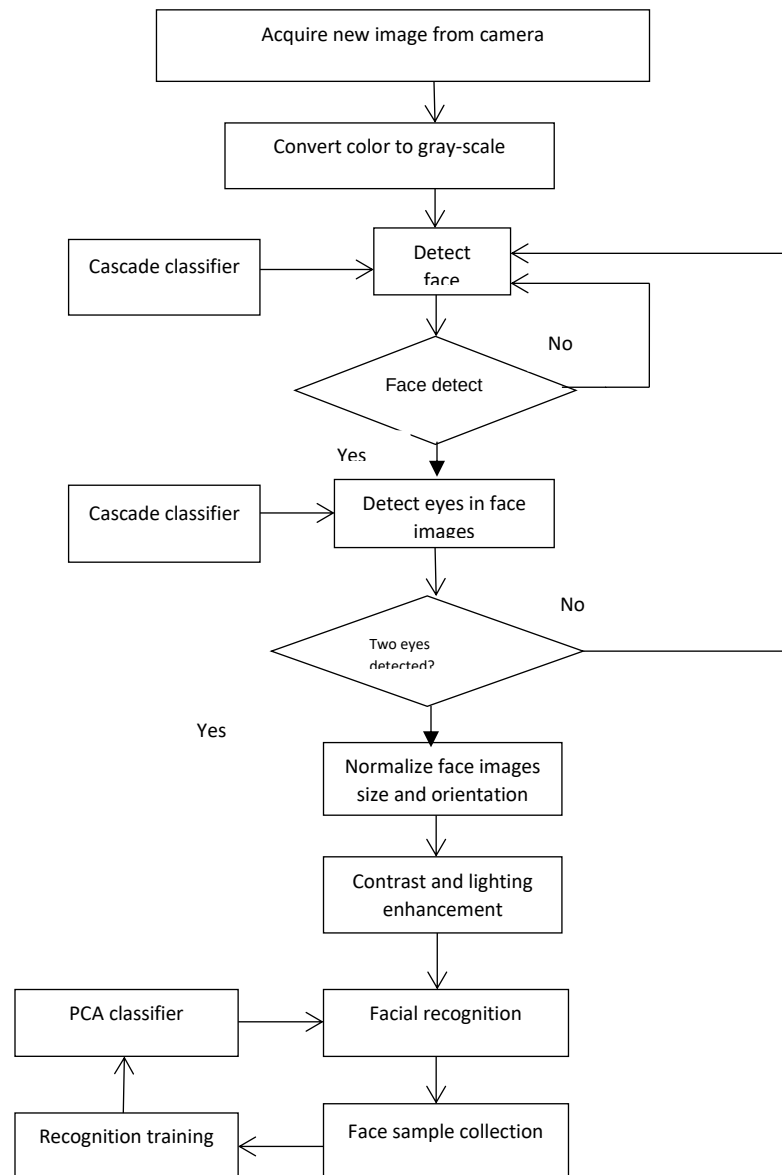


Fig:3.7: Flow chart of Haar cascade and LBPH

Haar uses a set of features called Haar features to detect objects in an image. These features are calculated by computing the difference between the sums of pixel intensities in adjacent rectangular regions of the image. The algorithm uses a trained classifier to scan the image for these features and identify the object of interest.

It works by extracting local binary patterns from an image and constructing a histogram of these patterns. The histogram is then used to classify the face by comparing it to a set of known faces in a database.

3.7.4 FACE DETECTION

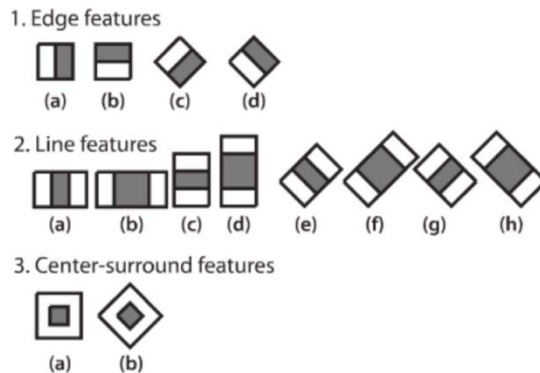
Face detection is one particular application type classed under "computer vision" technology. It is the method by which computer programs are developed and instructed to precisely recognize faces or objects (in the related technique of object detection) in images. They may come from real-time video or still photos that were captured by a camera. In order to assess whether or not something in a photograph is a face, face detection uses classifiers, which are algorithms (0). The ability to recognize faces in tens of thousands to millions of photographs has been trained into classifiers in order to increase accuracy.

In order to recognize a face, the camera software must first detect it and identify the features before making an identification. Likewise, when Facebook makes tagging suggestions to identify people in photos it must first locate the face. On social media apps like Snapchat, face detection is required to augment reality which allows users to virtually wear dog face masks using fancy filters. Another use of face detection is in smartphone face ID security.

Face detection uses **classifiers**, which are algorithms that detects what is either a face (1) or not a face (0) in an image. Classifiers have been trained to detect faces using thousands to millions of images in order to get more accuracy. OpenCV uses two types of classifiers, LBP (Local Binary Pattern) and Haar Cascades.

A sequence of rescaled “square-shaped” functions which together form a wavelet family or basis.

It is based on the Haar Wavelet technique to analyze pixels in the image into squares by function. This uses machine learning techniques to get a high degree of accuracy from what is called “training data”.



Face Detection determines the locations and sizes of human faces in arbitrary (digital) images.

In **Face Recognition**, the use of Face Detection comes first to determine and isolate a face before it can be recognized.

Fig: 3.8: Face Detection

This is a brief illustration of Features Extraction and the difference between Face Detection and Face Recognition. Face detection is about locating, while face recognition is about identifying.

3.7.5 FEATURE EXTRACTION

Haar Cascades use machine learning techniques in which a function is trained from a lot of positive and negative images. This process in the algorithm is feature extraction.

In feature extraction, the algorithm uses training data to best identify features that it can consider a face.

The training data used in this project is an XML file called:

haarcascade_frontalface_default.xml

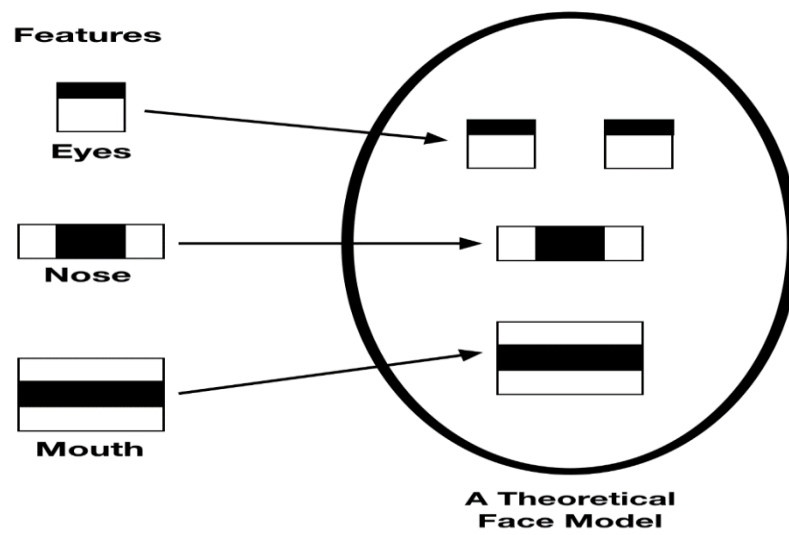


Fig:3.9: Feature Extraction

CHAPTER 4

REQUIREMENT ANALYSIS

4.1 HARDWARES USED:

4.1.1 ARDUINO

Arduino is a single-board microcontroller to make using electronics in multidisciplinary projects more accessible. The hardware consists of a simple open-source hardware board designed around an 8-bit Atmel AVR microcontroller, or a 32-bit Atmel ARM. The software consists of a standard programming language compiler and a boot loader that executes on the microcontroller.

Arduino microcontrollers are pre-programmed with a boot loader that simplifies the uploading of programs to the on-chip flash memory. The default bootloader of the Arduino Uno is the Optiboot bootloader. Boards are loaded with program code via a serial connection to another computer. Some serial Arduino boards contain a level shifter circuit to convert between RS-232 logic levels and transistor–transistor logic (TTL) level signals. Current Arduino boards are programmed via Universal Serial Bus (USB), implemented using USB-to-serial adapter chips such as the FTDI FT232. Some boards, such as later-model Uno boards, substitute the FTDI chip with a separate AVR chip containing USB-to-serial firmware, which is reprogrammable via its own ICSP header.

4.1.2 L298N MOTOR

The L298N Driver is a dual full bridge driver with high voltage and high current that is designed to drive inductive loads such relays, solenoids, DC motors, and stepping motors. Moreover, it accepts standard TTL logic levels. There are two enable inputs provided to enable or disable the device independently of the input signals. This motor operates the door's opening and closing when the face is verified.

SPECIFICATIONS

Table 4.1 Specifications of motor

PARAMETER	VALUE
Operating voltage	Up to 46v
DC Current	4A

PIN DETAILS

Table 4.2 Pin details of motor

PIN	NAME	DETAILS
1	GND	Ground
2	+12V	Power supply input
3	IN1	Direction of motor 1
4	IN2	Direction of motor 1
5	ENA	Controlling motor 1
6	ENB	Controlling motor 2
7	IN3	Direction of motor 2
8	IN4	Direction of motor 2

The L298 integrates two power output stages (A,B).The power output stage is a bridge configuration and its outputs can drive an inductive load in common or differential mode, depending on the state of the inputs. The current that flows through the load comes out from the bridge at the sense output: an external resistor (RSA, RSB.) allows detecting the intensity of this current.

4.1.3 LCD DISPLAY

Liquid crystal displays (LCDs) have materials which combine the properties of both liquids and crystals. Rather than having a melting point, they have a temperature range within which the molecules are almost as mobile as they would be in a liquid, but are grouped together in an ordered form similar to a crystal.

4.1.4 SWITCH OR BUTTON

A push-button (also spelled pushbutton) or simply button is a simple switch mechanism to control some aspect of a machine or a process. Buttons are typically made out of hard material, usually plastic or metal. The surface is usually flat or shaped to accommodate the human finger or hand, so as to be easily depressed or pushed. Buttons are most often biased switches, although many un-biased buttons (due to their physical nature) still require a spring to return to their un-pushed state.

4.1.5 DVD PLAYER

In this project DVD Player is used as a door. It will open and close based on the conditions.

4.2 SOFTWARE USED:

4.2.1 ARDUINO IDE:

The Arduino Integrated Development Environment - or Arduino Software (IDE) - contains a text editor for writing code, a message area, a text console, a toolbar with buttons for common functions and a series of menus. It connects to the Arduino hardware to upload programs and communicate with them.

Programs written using Arduino Software (IDE) are called **sketches**. These sketches are written in the text editor and are saved with the file extension.ino. The editor has features for cutting/pasting and for searching/replacing text. The message area gives feedback while saving and exporting and also displays errors.

4.2.2 PYTHON

Python is considered as the language of preference in the market. It is simple to learn, has clean syntax, and has a large online community supporting it. Python becomes a great choice when it comes to IoT.

Python recognizes the needs regardless of whether we create the IoT project from scratch or interact with actuators, sensors, and accessories.

Some of the many benefits of working with Python for IoT devices are a large number of libraries for all types of platforms and the speed it offers at which we can develop the code.

4.2.4 OpenCV IN PYTHON (*Open-Source Computer Vision*):

OpenCV is a Python library which is designed to solve computer vision problems. OpenCV was originally developed in 1999 by Intel but later it was supported by Willow Garage.

Face Detection Using OpenCV

This seems complex at first but it is very easy. Let me walk you through the entire process and you will feel the same.

Step 1: Considering our prerequisites, we will require an image, to begin with. Later we need to create a cascade classifier which will eventually give us the features of the face.

Step 2: This step involves making use of OpenCV which will read the image and the features file. So, at this point, there are NumPy arrays at the primary data points.

All we need to do is to search for the row and column values of the face NumPy ndarray. This is the array with the face rectangle coordinates.

Step 3: This final step involves displaying the image with the rectangular face box

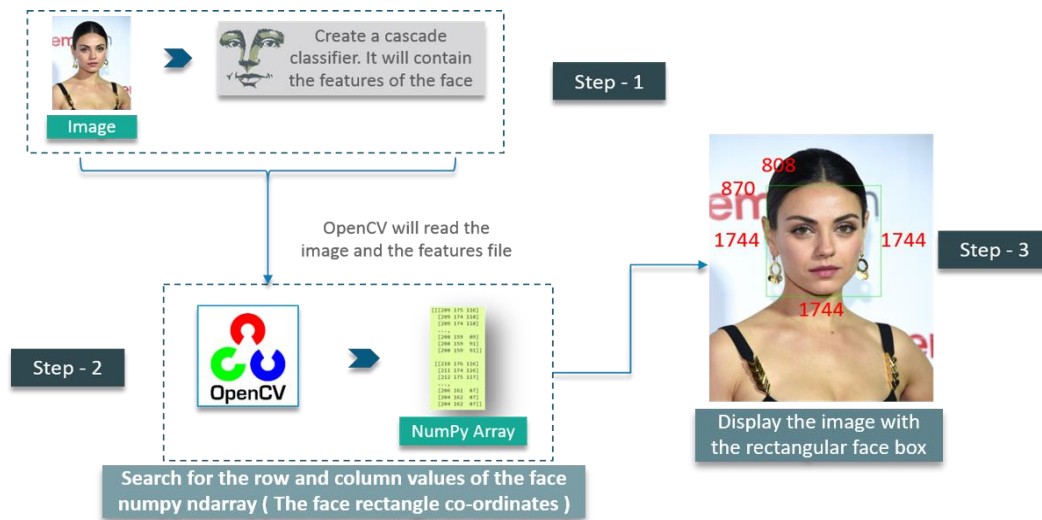


Fig:4.1: Face Detection Using OpenCV

First, we create a **Cascade Classifier** object to extract the features of the face as explained earlier. The path to the XML file which contains the face features is the parameter here. The next step would be to read an image with a face on it and convert it into a black and white image using **COLOR_BGR2GREY**. Followed by this, we search for the coordinates for the image. This is done using **detect Multiscale**. It's the coordinates for the face rectangle. The **scale Factor** is used to decrease the shape value by 5% until the face is found. So, on the whole – Smaller the value, greater is the accuracy.

Capturing Video Using OpenCV

Capturing videos using OpenCV is pretty simple as well. the following loop will give you a better idea.

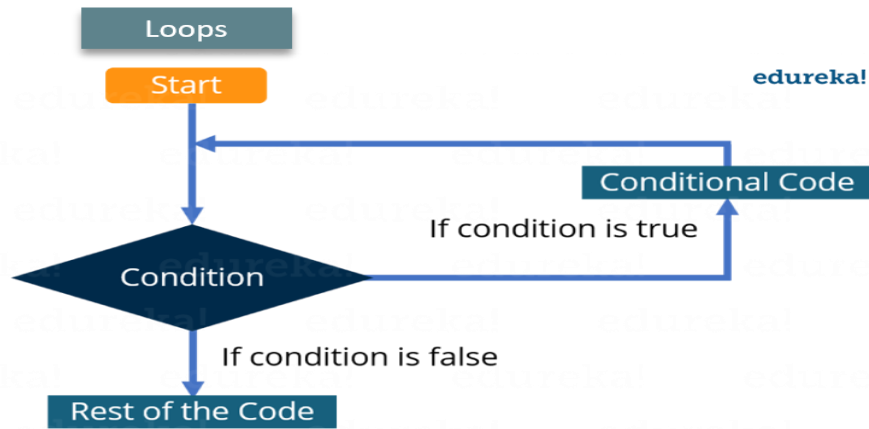


Fig:4.2: Capturing Video Using OpenCV

Capturing Video:

First, we import the OpenCV library as usual. Next, we have a method called **Video Capture** which is used to create the Video Capture object. This method is used to trigger the camera on the user's machine. The parameter to this function denotes if the program should make use of the built-in camera or an add-on camera. '0' denotes the built-in camera in this case. And lastly, the **release** method is used to release the camera in a few milliseconds.

PYTHON MODULES USED

Python Date-time Module:

Python time module provides many ways of representing time in code, such as objects, numbers, and strings. It also provides functionality other than representing time, like waiting during code execution and measuring the efficiency of your code.

Python Telepot Module:

Telepot helps to build applications for Telegram Bot API. To use the Telegram Bot API, first have to get a bot account by chatting with BotFather. BotFather will give a token,

something like 123456789:ABCdefGhIJKlmNoPQRsTUVwxyZ. With the token in hand, one can start using telepot to access the bot account.

Python Subprocess Module:

Subprocess in Python is used to run new programs and scripts by spawning new processes. And it enables the user to launch new programs right from the current Python program thanks to the subprocess module.

Python serial Module:

This module encapsulates the access for the serial port. It provides backends for Python running on Windows, OSX, Linux and BSD. The module named "serial" automatically selects the appropriate backend.

Python cv2 Module:

cv2 is the module import name for opencv-python, "Unofficial pre-built CPU-only OpenCV packages for Python". The traditional OpenCV has many complicated steps involving building the module from scratch, which is unnecessary. cv2 access our webcam using pass 0 in the function parameter. If you want to capture CCTV footage then we can pass RTSP url in the function parameter, which is really useful for video analysis.

4.3 PROJECT MANGEMENT PLAN

Project management is an important aspect of any engineering project, including the development of IoT based video surveillance using telegram chat-bot. A well-executed project management plan can help ensure that the project is completed on time, within budget, and meets the desired performance requirements.

The following is a general project management plan for IoT based video surveillance using telegram chat-bot.

Scope and Objectives:

The project scope and objectives define the specific requirements of IoT based video surveillance using telegram chat-bot. This includes the desired speed range, accuracy, response time, and other performance metrics. The scope and objectives should be clearly defined at the beginning of the project and communicated to all stakeholders.

Project Planning:

The project planning phase includes identifying the specific hardware and software components required for the video surveillance, developing a detailed project schedule, and defining the roles and responsibilities of the project team. This phase should also include risk management planning, where potential risks and mitigation strategies are identified and addressed.

Hardware and Software Development:

The hardware and software development phase includes the design and development of the Arduino, L298N Motor, OpenCV, machine learning algorithms and other components required for the video surveillance. The software development includes coding, testing, and debugging of the code to ensure that it meets the project requirements such as lighting conditions, less setup time and maximum of face accuracy.

Integration and Testing:

Once the hardware and software components have been developed, the integration and testing phase begins. This involves integrating the different components and conducting various lighting based conditions such as dark and light mode as well as determining the face detection accuracy to ensure that the system meets the project requirements for video surveillance.

Deployment and Maintenance:

Once the IoT based video surveillance system has been tested and validated, it can be deployed. The deployment phase includes installing the system at home, banks, hostels and other places where security is a crucial thing and providing training to the end-users. The maintenance phase includes ongoing support and maintenance to ensure that the system continues to operate at various lighting condition irrespective of the number of people entering.

Project Closure:

The project closure phase includes conducting a final project review to assess the success of the project and identify areas for improvement in future projects. It also includes documenting the project, archiving project materials, and releasing resources.

In conclusion, the development of IoT based video surveillance using machine learning algorithm requires careful planning, development, testing, and deployment. A well-executed project management plan can help ensure that the project is completed on time, within budget, and meets the desired performance requirements.

PROJECT DELIVERABLES

- A functional facial recognition algorithm using Python.
- A working serial communication protocol between Python and Arduino.
- An Arduino code that will control the motor to open and close the door.
- A complete system that will integrate all the above deliverables.
- A Complete Control System using Telegram Chatbot System.

4.4 FINANCIAL REPORT ON ESTIMATED PLAN

It is important to note that the actual cost of the project may vary depending on several factors such as the cost of the hardware components, the availability of the components, and unexpected expenses. Therefore, it is recommended to regularly monitor and adjust the budget as necessary throughout the project's lifecycle.

In addition, it is also important to consider the cost of labor, which is not included in the estimated budget. The project management plan outlines the tasks and timeline for the development of the system, and the cost of labor will depend on the amount of time spent on each task.

Overall, the estimated costing for this project is reasonable and will depend on the specific hardware and labor costs associated with the project.

4.5 SOFTWARE TO OPERATION PLAN

Installation and setup of software:

- Install Python and necessary libraries for facial recognition such as OpenCV and face recognition.
- Install the Arduino IDE and necessary libraries for motor control.
- Set up the development environment for Python and Arduino.

Facial recognition algorithm development:

- Develop and test the facial recognition algorithm using Python.
- Integrate the algorithm with the camera to capture and process images of faces.
- Determine the threshold for recognizing authorized faces.

Serial communication protocol development:

- Develop and test the serial communication protocol between Python and Arduino.
- Determine the communication method and protocol, such as UART or I2C.
- Test the communication between the two systems.

Arduino code development:

- Write and test the code to control the motor using the Arduino board.
- Determine the direction and speed of the motor for opening and closing the door.
- Test the functionality of the Arduino program.

System integration:

- Integrate the Python and Arduino programs into a complete system.
- Test the system thoroughly to ensure all components are working together.
- Conduct user acceptance testing to verify the system's functionality and usability.

Deployment and Operations:

- Deploy the system to the desired location and mount the camera and motor for the door.
- Configure the system to operate according to the user's requirements.
- Monitor the system's performance and make necessary adjustments as needed.
- Provide user training on how to operate the system.

Telegram Chat Bot**Create a Telegram account:**

- Download the Telegram app or use the web version.
- Create a new account or sign in to an existing one.

Set up a bot account:

- Search for the Bot Father account on Telegram and send a message to it.
- Follow the Bot Father's instructions to create a new bot account and obtain an API key.

Choose a programming language and development environment:

- Decide which programming language you want to use to build the chatbot.
- Choose a development environment that supports the chosen programming language.

Develop the chatbot:

- Use the Telegram Bot API to interact with the Telegram server and receive messages from users.
- Write code to parse incoming messages and provide appropriate responses.
- Implement desired features such as commands, inline mode, and callbacks.

Test the chatbot:

- Test the chatbot's functionality and make any necessary adjustments to the code.
- Test the chatbot with different inputs and edge cases to ensure it works as intended.

Deploy the chatbot:

- Deploy the chatbot to a server or hosting platform that supports the chosen programming language.
- Ensure the chatbot is accessible and functional from the Telegram app or web version.

Operations:

- Monitor the chatbot's performance and usage.
- Respond to user feedback and make improvements to the chatbot's functionality and design.
- Ensure the chatbot remains up-to-date and compatible with the latest version of the Telegram Bot API.

4.6 DEVELOPMENT & DEPLOYMENT TESTING:

Development environment:

- Install the latest version of Python and the necessary libraries for facial recognition, such as OpenCV and face recognition.
- Install the Arduino IDE and necessary libraries for motor control.
- Set up the development environment for Python and Arduino on your computer.

Hardware components:

- Connect the camera to your computer and ensure it is working correctly.

- Connect the Arduino board to your computer and ensure it is working correctly.
- Connect the motor to the Arduino board and ensure it is working correctly.

Code development:

- Develop and test the facial recognition algorithm using Python.
- Integrate the algorithm with the camera to capture and process images of faces.
- Develop and test the serial communication protocol between Python and Arduino.
- Write and test the code to control the motor using the Arduino board.
- Test Telegram Chatbot System

Deployment environment:

- Choose a hosting platform or server to deploy the system.
- Install the necessary software and libraries on the server.
- Ensure the server has sufficient resources to handle the system's requirements.

Deployment process:

- Transfer the code and necessary files to the server.
- Set up the system on the server and configure it to operate according to the user's requirements.
- Test the system thoroughly to ensure all components are working together.

Ongoing maintenance:

- Monitor the system's performance and make necessary adjustments as needed.
- Keep the software and libraries up-to-date with the latest versions to ensure compatibility and security.
- Respond to user feedback and make improvements to the system's functionality and design.

4.7 TESTING

Unit testing:

Unit testing involves testing individual components or modules of the system to ensure they are working as intended. For example, testing the facial recognition algorithm, serial communication protocol, or motor control code separately.

Integration testing:

Integration testing involves testing how the individual components or modules of the system interact with each other. For example, testing how the facial recognition algorithm communicates with the motor control code through serial communication and telegram chatbot.

Functional testing:

Functional testing involves testing the system's functionality against the user's requirements. For example, testing whether the system can accurately recognize authorized users and open the door, and deny access to unauthorized users through telegram chatbot.

Performance testing:

Performance testing involves testing the system's ability to handle a large number of users or requests without slowing down or crashing. For example, testing the system's response time under heavy load or stress.

Security testing:

Security testing involves testing the system's ability to prevent unauthorized access or hacking attempts. For example, testing the system's authentication and authorization mechanisms, encryption, and access controls.

User acceptance testing:

User acceptance testing involves testing the system with real users to ensure it meets their needs and is easy to use. For example, testing the system's interface, usability, and accessibility

CHAPTER 5

RESULTS AND DISCUSSION

To assess the system's accuracy, face recognition is tested on two different types of data: image data and real-time data. For authorized users, the tested image will be tagged with an ID number, while it will be unlabeled for unauthorized users. With a web camera, real-time facial recognition is accomplished. The system can identify an authorized person and vice versa.

The door will automatically open when the technology recognizes a person's face. The user will receive the video footage via a Telegram Chat Bot if the system is unable to recognize the user's face. Otherwise, the door will remain closed. A User can also manage door access with a help of Telegram Chat Bot.

HARDWARE SETUP:



Fig:5.1: Hardware Setup

DATA SET

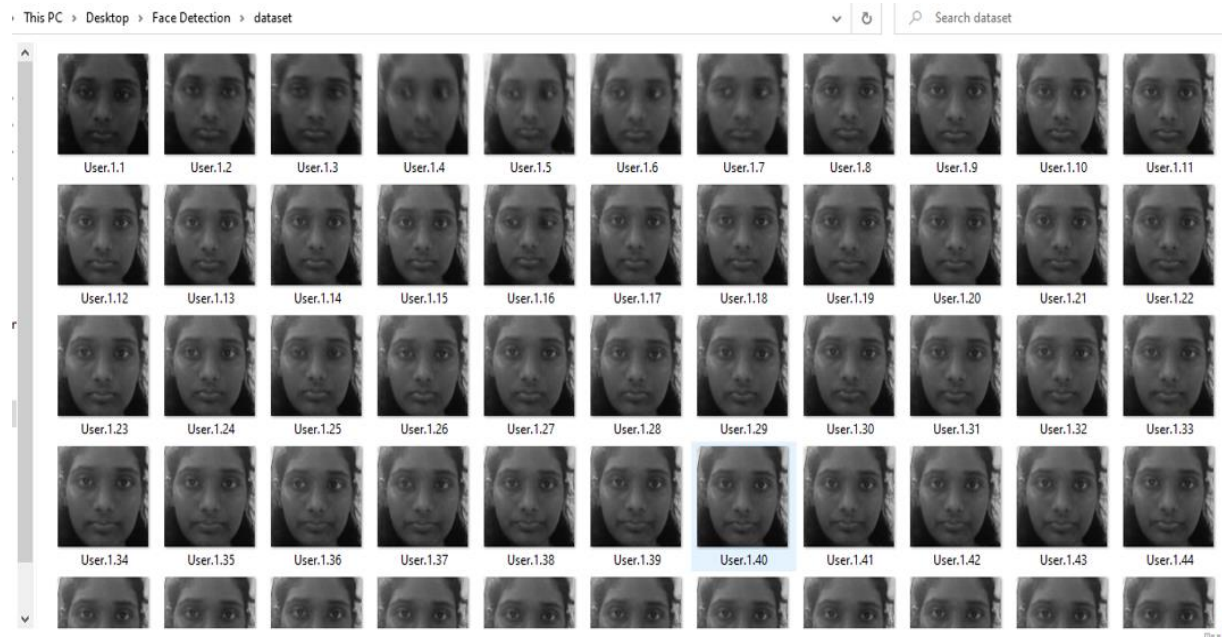


Fig:5.2: Data set

For Training the data, there are 200 images of a person has been collected with an id number. The images will be trained using *trainer.yml* file.

TRAINING DATA

```
opencv_lbphfaces:
  threshold: 1.7976931348623157e+308
  radius: 1
  neighbors: 8
  grid_x: 8
  grid_y: 8
  histograms:
    - !opencv-matrix
      rows: 1
      cols: 16384
      dt: f
      data: [ 3.82653065e-03, 1.02040814e-02, 0., 0., 2.55102036e-03,
3.82653065e-03, 0., 1.53061226e-02, 0., 0., 0., 0., 0., 0.,
0., 0., 7.65306130e-03, 8.92857090e-03, 0., 0.,
1.27551018e-03, 1.27551018e-03, 0., 8.92857090e-03, 0., 0.,
0., 0., 1.53061226e-02, 1.27551018e-03, 2.55102036e-03,
2.04081628e-02, 0., 0., 0., 0., 0., 0., 0., 0., 0.,
0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0.,
0., 0., 0., 0., 0., 5.10204071e-03, 5.10204071e-03, 0.,
0., 1.27551018e-03, 0., 0., 0., 0., 0., 0., 0., 0., 0.,
0., 5.10204071e-03, 2.55102036e-03, 0., 0., 1.27551018e-03,
0., 0., 0., 0., 0., 0., 2.55102036e-03, 1.27551018e-03,
0., 2.55102036e-03, 0., 0., 0., 0., 0., 0., 0., 0.,
0., 0., 0., 0., 0., 5.10204071e-03, 2.55102036e-03, 0.,
0., 2.55102036e-03, 0., 0., 3.82653065e-03, 2.55102036e-03,
0., 0., 0., 1.53061226e-02, 1.27551018e-03, 1.27551018e-03,
6.37755077e-03, 0., 0., 0., 0., 0., 0., 0., 0., 0.,
0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0.,
0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0.,
0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0.,
0., 0., 0., 9.43877548e-02, 0., 1.40306121e-02, 0.,
8.92857090e-03, 0., 6.50510192e-02, 0., 0., 0., 0., 0.,
0., 1.27551018e-03, 1.27551018e-03, 1.78571418e-02, 0.,
```

Fig:5.3: Training Data

FACE RECOGNITION

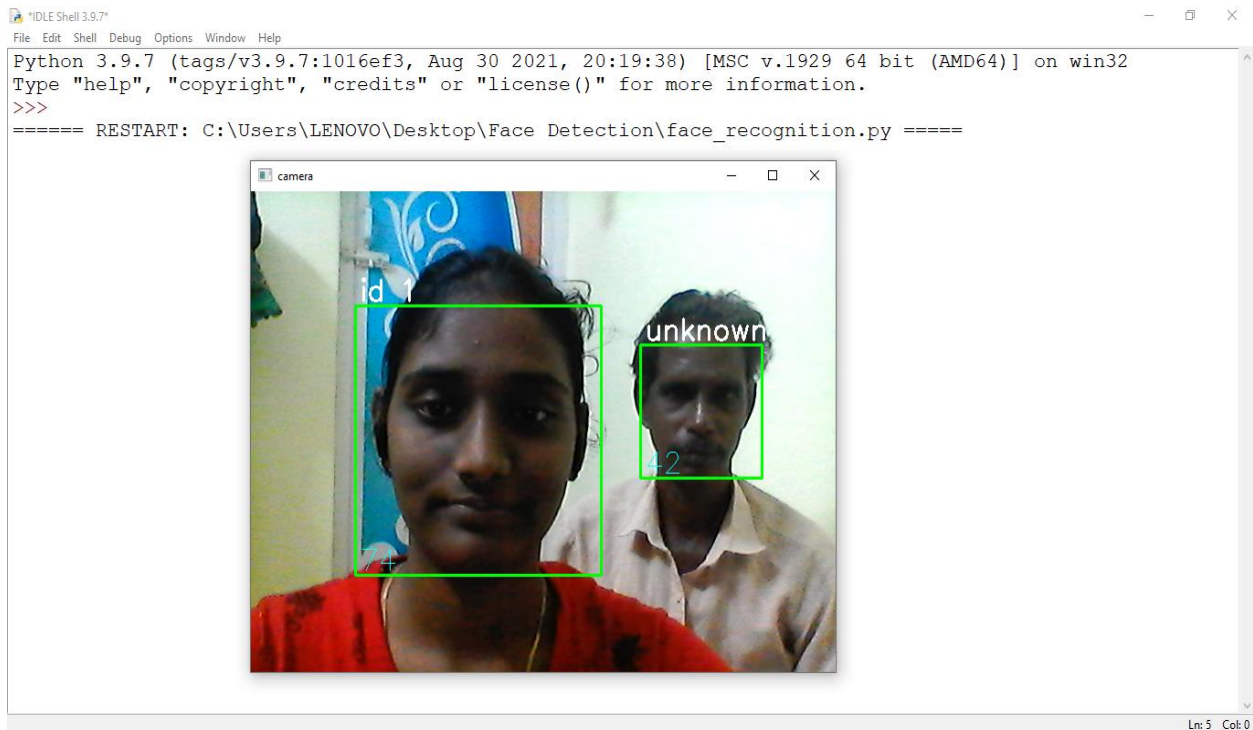


Fig:5.4: Face recognition

ID's have been given to respective person and the person's face has already been trained and stored in a database. The person faces whose ID number 1 is already presented in our database. So, it is displaying as "id 1". For the unknow faces it will display as "Unknown".

Two types of operations performed:

- 1) Automatically
- 2) Manually

1) Automatically

Automatically opening the door based on face detection and recognition

Live Permission Granted:

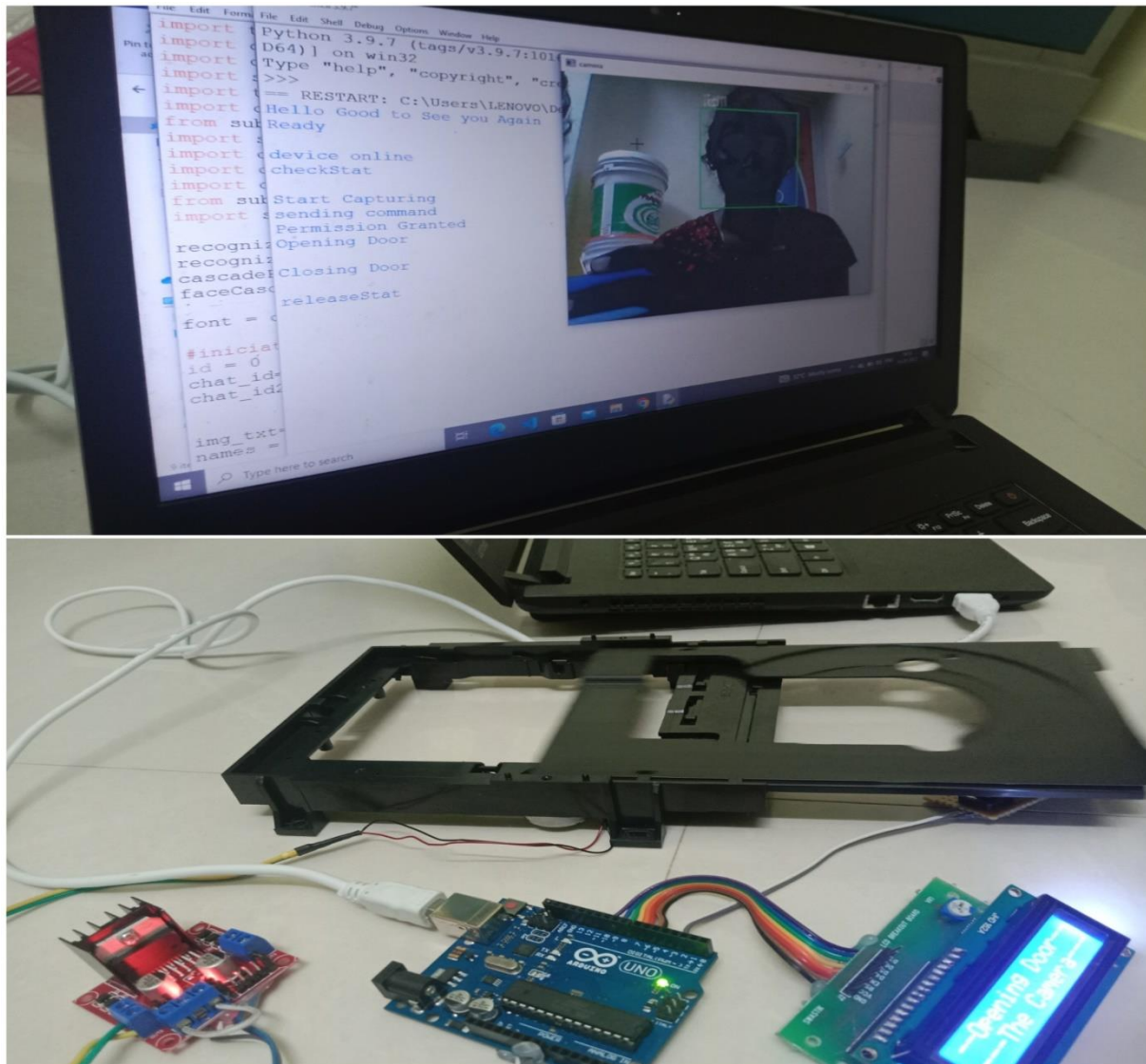


Fig:5.5: Live Permission Granted

The above person's face is already trained and stored in our database. So, the door has opened for the above person.

Live Permission Denied:

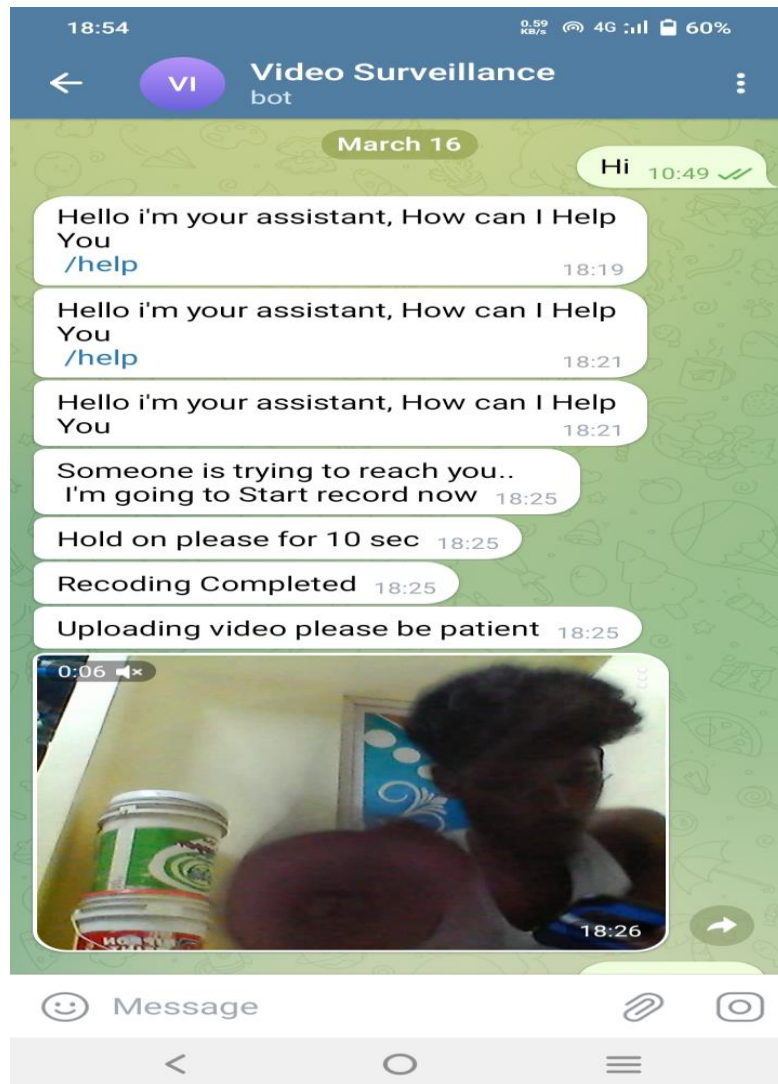


Fig:5.6: Live Permission Denied

The above person's face is not stored in our database. So, the system sends a video of an intruder to a user via telegram chat bot.

2) Manually

i. *Manually opening the door*

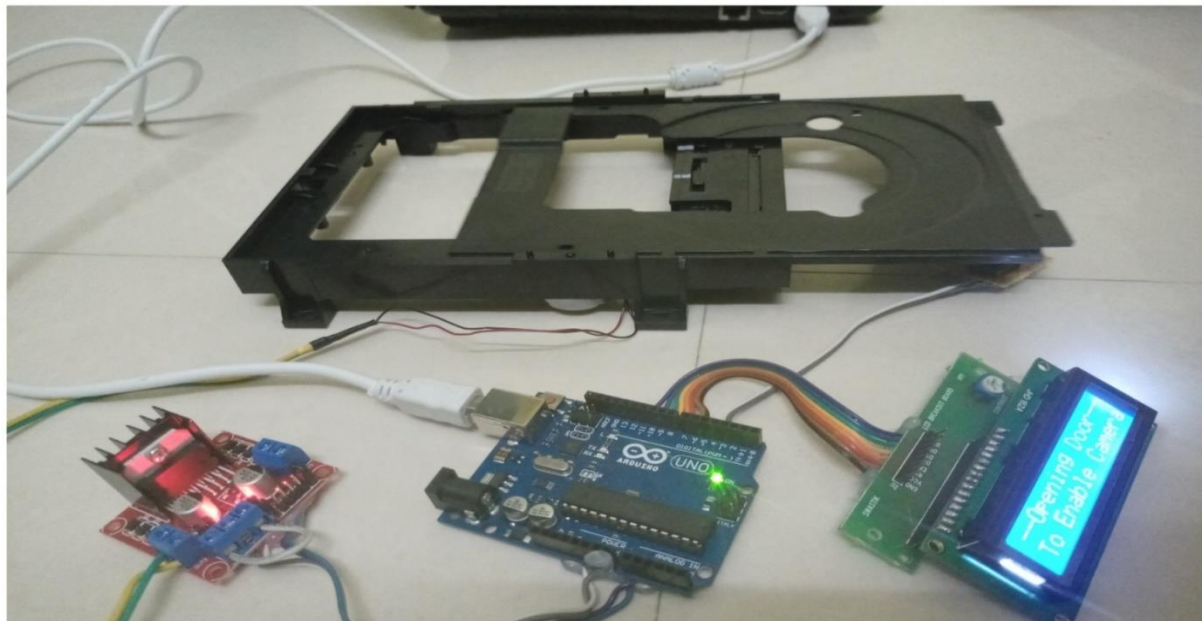


Fig:5.7: Manually Opening door

The person we know is coming and this person's face is not stored in our database. So, we can manually open the door using Telegram Chat bot

ii. *Manually closing the door*



Fig:5.8: Manually Closing Door

This system allows us to close the door manually

iii. Manually taking image



Fig: 5.9: Manually taking Live Photo

iv. *Manually taking video:*

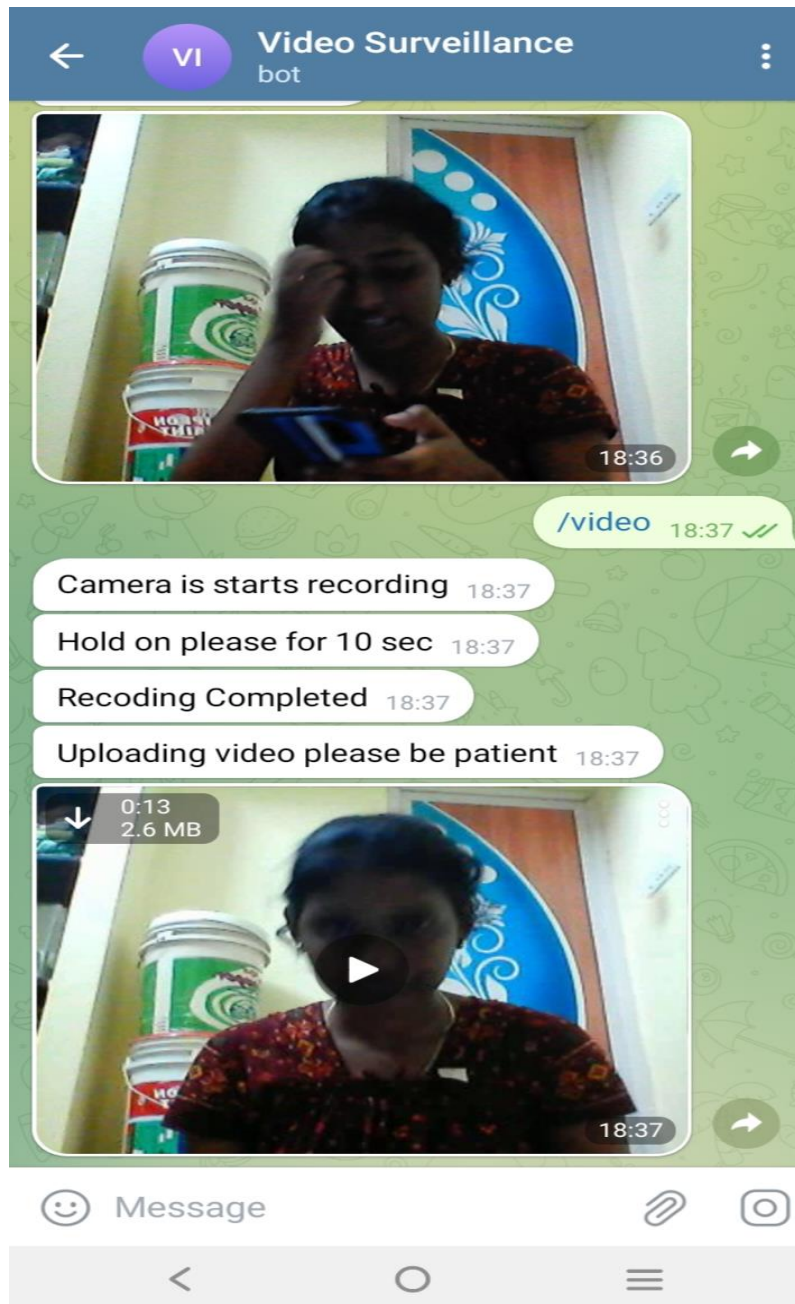


Fig:5.10: Manually Live Video

Same like Image we can also view what is happening outside by taking video (about 10s). The time period is set in the programming.

ADVANTAGES OF OUR PROPOSED SYSTEM

- We get an immediate response from our setup before the intruder try to intrude.
- Smart locks allow you to leave the hindrance of house keys behind and can allow you to lock and unlock using face recognition.
- Instead of appointing a watchman we can use our proposed method.
- Face recognition verifies who you are, not what you carry (key card) or what you know (PIN). Hence, it's inherently more secure for controlling access to buildings.
- Hands free – You can simply walk up and look at the reader and the door unlocks. It's one of the most convenient forms of building access. No need to fumble to look for your key cards.
- Easy to use by all demographics – Face recognition access is one of the most intuitive forms of access and can be used by people of all ages, even when they are not tech-savvy.
- Cannot be cloned like key cards – Proximity key cards and fobs can be cloned easily with cheap online cloners on Amazon. Face recognition provides a higher safety system that does not have those risks.
- You can remotely enroll people – In the world of flexible office post covid, security and IT teams may not come onsite every day. Face recognition access can be enrolled now remotely using a mobile app.
- Reduces ongoing cost and operational overhead of giving out keys and key cards to people in person.

APPLICATIONS

- Banks
- Hostels
- Home Security
- Meeting Halls
- Exam Centres
- Industries & Factories

CHAPTER 6

CONCLUSION

This paper reviewed the machine learning techniques used in facial recognition. More specifically the existing methods of Ada-boosting and Principal Component Analysis are reviewed. In these two algorithms the detection rate and false positive rate are somewhat inferior to that of Haar like feature. Haar cascade is an algorithm that can detect objects in images, irrespective of their scale in image and location. This algorithm is not so complex and can run in real-time. Local Binary Pattern Histogram is known for its ability to recognize the front face and side face of a person. They are also very efficient for feature selection through the use of the Ada-boost algorithm. The proposed system is a great way of ensuring security. It goals at creating minimal human intervention. It combines two modern technologies face recognition and IOT. It is low cost and power efficient system.

6.1 FUTURE WORK

In Future we have decided to detect multiple faces in the same frame and provide authentication based on their face recognition integrated for ensuring more enhanced security via chat bot systems and IoT being the future our work will ensure more security not only for home but in industries, colleges etc.

6.2 PERFORMANCE ANALYSIS

A performance analysis can be done based on various factors, such as accuracy, speed, and reliability.

1. Face detection accuracy: The success of the project depends on the accuracy of face detection. The face detection algorithm used in the paper should be accurate enough to differentiate between authorized individuals and intruders. If the algorithm has a high false positive rate, it could result in authorized individuals being denied access, which could be frustrating for users. On the other hand, if the algorithm has a high false negative

rate, it could result in unauthorized individuals gaining access, which could compromise the security of the system.

2. Speed: The speed of the face detection algorithm is also crucial. The system should be able to identify faces fast and respond in a short amount of time. If the system is slow, it could lead to delays in accessing the building, which could be inconvenient for users.

3. Reliability: The reliability of the system is another critical factor. The system should be able to operate reliably under varying lighting conditions and different types of faces. It should also be able to handle false positives and false negatives gracefully without compromising the security of the system.

In general, face detection algorithms perform best under well-lit conditions with minimal shadows and glare. In low-light conditions, such as at night or in dimly lit areas, the algorithm may struggle to detect faces accurately, resulting in false positives or false negatives.

To address this issue, the system can be equipped with additional lighting sources, such as infrared lights or motion-activated floodlights, to improve visibility and increase the accuracy of the face detection algorithm. Additionally, the system can be programmed to adjust the camera's settings automatically based on lighting conditions to optimize detection accuracy.

Another potential issue is glare from direct sunlight or other light sources, which can cause overexposure and wash out facial features, making it difficult for the algorithm to detect faces. This issue can be mitigated by positioning the camera in a location that minimizes glare, such as in a shaded area or using a camera with a built-in sunshield.

Finally, it's important to note that the accuracy of face detection algorithms can vary depending on the quality of the camera and the algorithm used. Therefore, it's important to choose a high-quality camera and algorithm that are optimized for face detection in a variety of lighting conditions.

Overall, while lighting conditions can impact the performance of face detection-based authorization and sending footage to a Telegram chat bot for unauthorized person

verification, there are several strategies that can be employed to improve accuracy and minimize false positives and false negatives.

REFERENCES

- [1] Jing-Ming Guo, Chen-Chi Lin, Min-Feng Wu, Che-Hao Chang, and Hua Lee. IEEE SIGNAL PROCESSING LETTERS, VOL. 18, NO. 8, AUGUST 2011. "Complexity Reduced Face Detection Using Probability-Based Face Mask Prefiltering and Pixel-Based Hierarchical-Feature Adaboosting".
- [2] Januzaj, Y., Luna, A., Ramaj, V. 2015 Real time access control based on Facial Recognition. Review Article, J Nucl Ene Sci Power Generat Technol Vol: 10 Issue: 9.
- [3] Lwin, H., Khaing, A., Tun, H. 2015. Automatic door access system using face recognition. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 4, ISSUE 06, JUNE 2015 ISSN 2277-8616.
- [4] Chowdhury, M., Nooman, S. 2013. Access Control of Door and Home Security by Raspberry Pi through Internet. International Journal of Scientific & Engineering Research, Volume 4, Issue 1 october-2013 ISSN 2229-5518.
- [5] Senthilkumar, G., Gopalkrishnan, K., Sathish Kumar, V. 2014 Embedded Image Capturing System Using Raspberry Pi System. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 2, March – April 2014 ISSN 2278-6856.
- [6] Çarıkçı, M., Özen, F. 2012 A Face Recognition System Based on Eigen faces Method. Procedia Technology 1 (2012) 118 – 123 2212-0173 © 2012 Published by Elsevier Ltd. doi: 10.1016/j.protcy.2012.02.023.
- [7] Jogdand, S., Karanjkar, M. 2015 Implementation of Automated Door Accessing System with Face Design and Recognition. Corpus ID: 16518189 Published 2015 Computer Science.
- [8] Sowmiya, U., shafiq mansoor, J. 2015 Raspberry pi-based home door security through 3g dongle. International Journal of Engineering Research and General Science Volume 3, Issue 2, March-April, 2015 ISSN 2091-2730.

- [9] Kartik J. Srimadhavan V. 2013 SMS Alert and Embedded Network Video Monitoring Terminal. October 2013 International Journal of Security Privacy and Trust Management 2(5):9-19 DOI:10.5121/ijspmt.2013.2502.
- [10] Sahani, M., Nanda, C., Sahu, A., Pattnaik, B. 2015 Web Based Online Embedded Door Access Control and Home Security System Based on Face Recognition. © 2018 IJCRT | Volume 6, Issue 1 February 2018 | ISSN: 2320-2882.
- [11] Mulla, M., Patil, R. 2015 .Facial Image Based Security System using PCA. International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064.
- [12] Gubbi, Jayavardhana, (2013) Internet of Things (IOT): A vision, architectural elements, and future directions. Future Generation Computer Systems. 29, 1645-1660. <http://dx.doi.org/10.1016/j.future.2013.01.010>.
- [13] Karthik A Patil, Niteen Vittalkar, Pavan Hiremath, Manoj A Murthy. Volume: 07 Issue: 05 | May 2020. "Smart Door Locking System using IoT".
- [14] Ni Ni San Hlaing, San San Lwin, "Electronic Door Lock using RFID and Password Based on Arduino" International Journal of Trend in Scientific Research and Development (IJTSRD) Volume: 3 | Issue: 3 | Mar-Apr 2019.
- [15] Arpita Mishra, Siddharth Sharma, Sachin Dubey, S.K. Dubey, "PASSWORD BASED SECURITY LOCK SYSTEM" International Journal of Advanced Technology in Engineering and Science www.ijates.com Volume No.02, Issue No. 05, May 2014 ISSN (online): 2348 – 7550.
- [16] Shrinidhi Gindi, Naiyer Shaikh, Kashif Beig, Abdeali Sabuwala, "Smart Lock System Using RFID" International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 07 Issue: 07 | July 2020.
- [17] Mr. L. David William Raj, M. Deepika, V. Bhuvaneshwari, R. Harshitha, K. Haripriya, "A DESIGN OF OTP BASED WIRELESS SMART DOOR LOCKING SYSTEM" International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 08 Special Issue Apr 2021.

[18] K. Jayanth, Kamjula Manikanteswar Reddy, B. Harshith, S Sathyalakshmi “IoT based Visitor Identification System” 2022.

[19] Prashanth Balraj Balla, Prof.K.T. Jadhao “IoT BASED FACIAL RECOGNITION SECURITY SYSTEM” 2022.

LETTER OF ACCEPTANCE



8th International Conference on
Communication and Electronics Systems
ICCES-2023
1-3, June 2023 | Coimbatore, India

<http://icoecs.org/2023/>
icces2022@gmail.com

Letter of Acceptance

Details of Accepted Paper

Paper ID	Paper Title	Author(s)
ICCES376	IoT based Intruder Detection System Integrated with Telegram Chat bot System for Authentication	Bernatin T, Sangeetha K, Rahini Rajasekar, P. Chitra

Author(s):

On behalf of the Conference committee, I would like to congratulate you on having your article accepted by the ICCES 2023 IEEE Conference, which will be held from 1-3, June 2023 at PPG Institute of Technology, Coimbatore, India. You have been selected to deliver your oral presentation at the International Conference on Communication and Electronics Systems.

ICCES 2023 is an internationally-recognized IEEE conference, which dedicated solely for recommendation for inclusion in IEEE Xplore. Please visit the conference website for further updates [\[http://icoecs.org/2023/index.html\]](http://icoecs.org/2023/index.html).

As a result of the review and results, we are pleased inform that you can now submit the full-length paper for inclusion into the ICCES proceedings. We appreciate if you could send the final version of your research paper at your earliest convenience, in order to ensure the timely publication. When submitting your final paper, please highlight the changes made according to the review comments.

Thank you for your contribution to the ICCES 2023 conference.

Yours sincerely,

V. B. L.

Dr. V. Bindhu

Conference Chair
ICCES- 2023.



IEEE XPLORE COMPLIANT ISBN: 979-8-3503-9663-8
IEEE DVD ISBN: 979-8-3503-9662-1

Previous Publications
[2022](#), [2021](#), [2020](#), [2019](#), [2018](#), [2017](#), [2016](#)