MADHAV INSTITUTE OF TECHNOLOGY & SCIENCE, GWALIOR

(A Govt. Aided UGC Autonomous & NAAC Accredited Institute Affiliated to RGPV, Bhopal)

Project Report

on

Intruder Detection and Automatic Email Alerting System

Submitted By:

Ashi Barsaiya

0901CS191023

Ayush Gupta

0901CS191028

Faculty Mentor:

Mir Shahnawaz Ahmad

Assistant Professor, Computer Science And Engineering

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

MADHAV INSTITUTE OF TECHNOLOGY & SCIENCE

GWALIOR - 474005 (MP) est. 1957

MAY-JUNE 2022

MADHAV INSTITUTE OF TECHNOLOGY & SCIENCE, GWALIOR

(A Govt. Aided UGC Autonomous & NAAC Accredited Institute Affiliated to RGPV, Bhopal)

Project Report

on

Intruder Detection and Automatic Email Alerting System

A project report submitted in partial fulfilment of the requirement for the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

Submitted By:

Ashi Barsaiya

0901CS191023

Ayush Gupta

0901CS191028

Faculty Mentor:

Mir Shahnawaz Ahmad

Assistant Professor, Computer Science And Engineering

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

MADHAV INSTITUTE OF TECHNOLOGY & SCIENCE

GWALIOR - 474005 (MP) est. 1957

MAY-JUNE 2022

MADHAV INSTITUTE OF TECHNOLOGY & SCIENCE, GWALIOR

(A Govt. Aided UGC Autonomous & NAAC Accredited Institute Affiliated to RGPV, Bhopal)

CERTIFICATE

This is certified that **Ashi Barsaiya**(0901CS191023) and has submitted the project report titled **Intruder Detection and Automatic Email Alerting System** under the mentorship of **Mr. Mir Shahnawaz Ahmad,**Professor,Computer Science and Engineering in partial fulfilment of the requirement for the award of degree of Bachelor of Technology in Computer Science and Engineering from Madhav Institute of Technology and Science, Gwalior.

09/05/22

Mir Shahnawaz Ahmad
Faculty Mentor
Assistant Professor
Computer Science and Engineering

09/05/22

Dr. Manish Dixit
Professor and Head
Computer Science and Engineering

Dr. Manish Dixit
Professor & HOD
Department of CSE
M.I.T.S. Gwalior

MADHAV INSTITUTE OF TECHNOLOGY & SCIENCE, GWALIOR

(A Govt. Aided UGC Autonomous & NAAC Accredited Institute Affiliated to RGPV, Bhopal)

CERTIFICATE

This is certified that and **Ayush Gupta** (0901CS191028) has submitted the project report titled **Intruder Detection and Automatic Email Alerting System** under the mentorship of **Prof. Mir Shahnawaz Ahmad** in partial fulfilment of the requirement for the award of degree of Bachelor of Technology in Computer Science and Engineering from Madhav Institute of Technology and Science, Gwalior.

09/05/22

Mir Shahnawaz Ahmad
Faculty Mentor
Assistant Professor
Computer Science and Engineering

09/05/22

Dr. Manish Dixit
Professor and Head
Computer Science and Engineering

Dr. Manish Dixit
Professor & HOD
Department of CSE
M.I.T.S. Gwalior

MADHAV INSTITUTE OF TECHNOLOGY & SCIENCE, GWALIOR

(A Govt. Aided UGC Autonomous & NAAC Accredited Institute Affiliated to RGPV, Bhopal)

DECLARATION

We hereby declare that the work being presented in this project report, for the partial fulfilment of requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering at Madhav Institute of Technology & Science, Gwalior is an authenticated and original record of my work under the mentorship of **Mir Shahnawaz Ahmad,** Assistant Professor, Computer Science & Engineering.

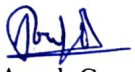
We declare that we have not submitted the matter embodied in this report for the award of any degree or diploma anywhere else.

Ashi Barsaiya

0901CS191023

3rd Year

Computer Science and Engineering



Ayush Gupta

0901CS191028

3rd Year

Computer Science and Engineering

MADHAV INSTITUTE OF TECHNOLOGY & SCIENCE, GWALIOR

(A Govt. Aided UGC Autonomous & NAAC Accredited Institute Affiliated to RGPV, Bhopal)

ACKNOWLEDGEMENT

The full semester project has proved to be pivotal to our career. We are thankful to our institute, **Madhav Institute of Technology and Science** to allow us to continue our disciplinary/interdisciplinary project as a curriculum requirement, under the provisions of the Flexible Curriculum Scheme (based on the AICTE Model Curriculum 2018), approved by the Academic Council of the institute. I extend my gratitude to the Director of the institute, **Dr. R. K. Pandit** and Dean Academics, **Dr. Manjaree Pandit** for this.

I would sincerely like to thank our department, **Department of Computer Science and Engineering, for allowing** us to explore this project. We humbly thank **Dr. Manish Dixit**, Professor and Head, Department of Computer Science and Engineering, for his continued support during the course of this engagement, which eased the process and formalities involved.

We are sincerely thankful to our faculty mentors. We are grateful to the guidance of **Mir Shahnawaz Ahmad,** Assistant Professor, Computer Science & Engineering, for his continued support and guidance throughout the project. We are also very thankful to the faculty and staff of the department.

Ashi Barsaiya
0901CS191023
3rd Year
Computer Science and Engineering

Ayush Gupta
0901CS191028
3rd Year
Computer Science and Engineering

ABSTRACT

Abstract:- Security has become an important factor nowadays. Intruders have become prominent factors for all the data/property theft. This project aims to design and implement a security system with human detection capability. Traditional home security systems, i.e., Closed-Circuit Television (CCTV) can only capture and record videos without the ability of giving warning feedback if there is any suspicious object. Therefore, an additional object detection and warning method is required. If the suspicious object is detected, then the alarm is activated and sends an email to warn the house owner about the existence of the intruder. A camera placed at the locality is trained such that it can identify the familiar people and it is "on" all the time. Whenever an unknown/unidentified person comes to the vicinity of the camera, this intruder detection system gets activated. Based upon this, the incident responder can investigate the issue and take the necessary action at the instant. The captured image is compared with the saved image of the authorized person in the database. The system can distinguish an authorized and unauthorized person by comparing. If it is found to be an unauthorized person, then system sends the recognized image to the owner whose authorized number we feed in the system, through email. The idea can be applied in many real-life situations, like thief identification near the house.

Keywords: Intruder detection · Alerting owner · Machine learning · Image processing · Thief identificatio

सार

सुरक्षा आजकल एक महत्वपूर्ण कारक बन गया है। सभी डेटा/संपत्ति की चोरी के लिए घुसपैठिए प्रमुख कारक बन गए हैं। इस परियोजना का उद्देश्य मानव पहचान क्षमता के साथ एक सुरक्षा प्रणाली को डिजाइन और कार्यान्वित करना है। पारंपरिक घरेलू सुरक्षा प्रणालियाँ, यानी क्लोज्ड-सर्किट टेलीविज़न (सीसीटीवी) केवल वीडियो कैप्चर और रिकॉर्ड कर सकती हैं, अगर कोई संदिग्ध वस्तु है तो चेतावनी प्रतिक्रिया देने की क्षमता के बिना। इसलिए, एक अतिरिक्त वस्तु का पता लगाने और चेतावनी विधि की आवश्यकता है।

यदि संदिग्ध वस्तु का पता चलता है, तो अलार्म सक्रिय हो जाता है और घर के मालिक को घुसपैठिए के अस्तित्व के बारे में चेतावनी देने के लिए एक ईमेल भेजता है। इलाके में लगे एक कैमरे को इस तरह प्रशिक्षित किया जाता है कि यह परिचित लोगों की पहचान कर सके और यह हर समय "चालू" रहता है। जब भी कोई अनजान/अज्ञात व्यक्ति कैमरे के आसपास आता है, तो यह घुसपैठिए का पता लगाने वाला सिस्टम सक्रिय हो जाता है।

इसके आधार पर, घटना प्रतिवादी मामले की जांच कर सकता है और तत्काल आवश्यक कार्रवाई कर सकता है। कैप्चर की गई छवि की तुलना डेटाबेस में अधिकृत व्यक्ति की सहेजी गई छवि से की जाती है। सिस्टम एक अधिकृत और अनधिकृत व्यक्ति की तुलना करके भेद कर सकता है। यदि यह एक अनधिकृत व्यक्ति पाया जाता है, तो सिस्टम मान्यता प्राप्त छवि को उस स्वामी को भेजता है जिसका अधिकृत नंबर हम सिस्टम में ईमेल के माध्यम से फीड करते हैं। इस विचार को कई वास्तविक जीवन स्थितियों में लागू किया जा सकता है, जैसे घर के पास चोर की पहचान।

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

Abbreviation	Description
MIME	MIME is a kind of add-on or a supplementary protocol that allows non-ASCII data to be sent through SMTP
SMTP	SMTP transfers the mail being a message transfer agent from the sender's side to the mailbox of the receiver side and stores it

Chapter 1: INTRODUCTION

1.1 Project Overview

Security has become an important factor. Intruders have become prominent factors for all the data/property theft. The basic idea is to identify the intruder and alert owner/administrator in different possible ways, i.e., Intruder Detection System. This paper discusses different ways such as "a message (SMS)", "WhatsApp message", "location of intruder", "an immediate call", and "intruder's image to owner's/administrator's WhatsApp" to alert owner/administrator. For identifying the intruder, image recognition is used. A camera placed at the locality is trained such that it can identify the familiar people and it is "on" all the time. Whenever an unknown/unidentified person comes to the vicinity of the camera, all the above-said features get activated and the owner gets alerted

1.1.1 What is an Intruder Detection System?

An intruder detection system is a system that alerts when any intruder (unknown person) comes under the view of the designated camera. It stores the known faces and compares them with the faces recognised from the camera. If any unknown face is detected it alerts the user. It uses open_cv and face_recognition library for face detection and recognition.

1.2 Problem Definition:

The number of cases of theft are increasing and occur frequently, either in organizations or some locality of your house. So, to reduce these problems we can use the Intruder Detection System and identify the intruders and investigate upon them and increase the security.

1.3 Objective:

The general objective is to identify the intruder and alert the owner/administrator through Automatic Email Alerting System. Intruders are mostly the ones, who does not belong to the same locality/does not belong to the same institution.

The Specific Objectives are listed below:

- Identify the intruders.
- Alert the owner.
- Increase the security.

1.4 Scope

Scope: Intrusion detection systems primarily use two key intrusion detection methods: signature-based intrusion detection and anomaly-based intrusion detection. Signature-based intrusion detection is designed to detect possible threats by comparing given network traffic and log data to existing attack patterns.

1.5 Required Tools and Languages

Required Tools: Visual Studio Code, OpenCV, Webcam

i) Visual Studio Code : Visual Studio Code, also commonly referred to as VS Code, is a source-code editor made by Microsoft for Windows, Linux and macOS. Features include support for debugging, syntax highlighting, intelligent code completion, snippets, code refactoring, and embedded Git. Users can change the theme, keyboard shortcuts, preferences, and install extensions that add additional functionality.

In the Stack Overflow 2021 Developer Survey, Visual Studio Code was ranked the most popular developer environment tool, with 70% of 82,000 respondents reporting that they use it.

ii) OpenCV: Computer vision is a space of computer programming which bases on making PC's fit for interpreting pictures. It got out during the 70's when Martin Minsky asked is student to interface a computer to a camera and getting the PC to evaluate what it saw. During this time the state of art of computer vision transformed into reality. Today CV is consistently used with AI which setup to recognize certain features or things like remembering the portion of people.

iii) Webcam: To identify the user and capture the images in case of the intruder.

Coding Language: Python

Python: Python is a globally reputed language which is proposed to be significantly coherent. It is an interpreted language. It is very interactive in nature and has a user -friendly interface. It is set to be object oriented which maintains a procedure of programming that optimizes code inside objects.

Other Libraries: NumPy, face_recognition, smptlib,glob, Time, datetime, collections, MIME libraries.

1.6 Feasibility

1.6.1 Operational Feasibility

In Operational Feasibility the degree of providing service to requirements is analysed along with how easy the product will be to operate and maintain after deployment. Along with this other operational scopes are determining usability of product, Determining suggested solution by software development team is acceptable or not etc.

The project is feasible in terms of operations as it can be implemented easily.

1.6.2 Economic Feasibility

In the Economic Feasibility study, the cost and benefit of the project are analysed. This means under this feasibility study a detailed analysis is carried out of what will be the cost of the project for development which includes all required costs for final development like hardware and software resources required, design and development cost and operational cost and so on. After that, it is analyzed whether the project will be beneficial in terms of finance for the organization or not.

Chapter 2: PRELIMINARY REVIEW

A facial recognition system is a technology capable of matching a human face from a digital image or a video frame against a database of faces, typically employed to authenticate users through ID verification services, works by pinpointing and measuring facial features from a given image.

Development began on similar systems in the 1960s, beginning as a form of computer application. Since their inception, facial recognition systems have seen wider uses in recent times on smartphones and in other forms of technology, such as robotics. Because computerized facial recognition involves the measurement of a human's physiological characteristics, facial recognition systems are categorized as biometrics. Although the accuracy of facial recognition systems as a biometric technology is lower than iris recognition and fingerprint recognition, it is widely adopted due to its contactless process. Facial recognition systems have been deployed in advanced human–computer interaction, video surveillance and automatic indexing of images.

Computer Vision: Computer vision is a process by which we can understand the images and videos how they are stored and how we can manipulate and retrieve data from them. Computer Vision is the base or mostly used for Artificial Intelligence. Computer-Vision is playing a major role in self-driving cars, robotics as well as in photo correction apps.

OpenCV: OpenCV is the huge open-source library for computer vision, machine learning, and image processing and now it plays a major role in real-time operation which is very important in today's systems. By using it, one can process images and videos to identify objects, faces, or even handwriting of a human. When integrated with various libraries, such as NumPy, python is capable of processing the OpenCV array structure for analysis. To Identify image pattern and its various features we use vector space and perform mathematical operations on these features.

The first OpenCV version was 1.0. OpenCV is released under a BSD license and hence it's free for both academic and commercial use. It has C++, C, Python and Java interfaces and supports Windows, Linux, Mac OS, iOS and Android. When OpenCV was designed the main focus was real-time applications for computational efficiency. All things are written in optimized C/C++ to take advantage of multi-core processing.

Chapter 3: DETAILED DESIGN

3.1 Procedure:

Step-1 : Encode the picture using the HOG algorithm to create a simplified version of the image.
Step-2 : Finding the main landmarks in the face like nose, mouth and ears.
Step-3 : Encoding Faces. Here we use a pre-trained Convolution Neural Network developed by OpenFace.
Step-4 : Finding the person's name from the encoding.Compare which person has the closest measurements to our face's measurements.

3.2 Detailed Study:

Facial recognition is a way of identifying or confirming an individual's identity using their face. Facial recognition systems can be used to identify people in photos, videos, or in real-time.

Facial recognition is a category of biometric security. Other forms of biometric software include voice recognition, fingerprint recognition, and eye retina or iris recognition. The technology is mostly used for security and law enforcement, though there is increasing interest in other areas of use.

Many people are familiar with face recognition technology through the FaceID used to unlock iPhones (however, this is only one application of face recognition). Typically, facial recognition does not rely on a massive database of photos to determine an individual's identity — it simply identifies and recognizes one person as the sole owner of the device, while limiting access to others.

Beyond unlocking phones, facial recognition works by matching the faces of people walking past special cameras, to images of people on a watch list. The watch lists can contain pictures of anyone, including people who are not suspected of any wrongdoing, and the images can come from anywhere — even from our social media accounts. Facial technology systems can vary, but in general, they tend to operate as follows:

Step 1: Face detection

The camera detects and locates the image of a face, either alone or in a crowd. The image may show the person looking straight ahead or in profile.

Step 2: Face analysis

Next, an image of the face is captured and analyzed. Most facial recognition technology relies on 2D rather than 3D images because it can more conveniently match a 2D image with public photos or those in a database. The software reads the geometry of your face. Key factors include the distance between your eyes, the depth of your eye sockets, the distance from forehead to chin, the shape of your cheekbones, and the contour of the lips, ears, and chin. The aim is to identify the facial landmarks that are key to distinguishing your face.

Step 3: Converting the image to data

The face capture process transforms analog information (a face) into a set of digital information (data) based on the person's facial features. Your face's analysis is essentially turned into a mathematical formula. The numerical code is called a faceprint. In the same way that thumbprints are unique, each person has their own faceprint.

Step 4: Finding a match

Your faceprint is then compared against a database of other known faces. For example, the FBI has access to up to 650 million photos, drawn from various state databases.

On Facebook, any photo tagged with a person's name becomes a part of Facebook's database, which may also be used for facial recognition. If your faceprint matches an image in a facial recognition database, then a determination is made.

Of all the biometric measurements, facial recognition is considered the most natural. Intuitively, this makes sense, since we typically recognize ourselves and others by looking at faces, rather than thumbprints and irises. It is estimated that over half of the world's population is touched by facial recognition technology regularly.

3.3 Data Flow Diagram:

When the camera detects an unknown person's face, the images of the intruder are sent to the server and the intruder detection system gets activated and the alerts in the form of automatic emails are then sent to the registered email.

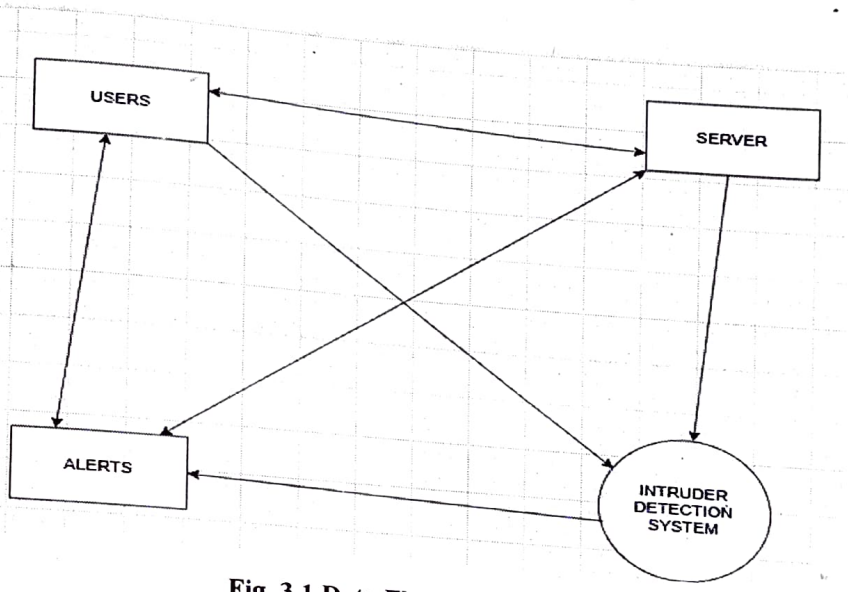


Fig. 3.1 Data Flow Diagram

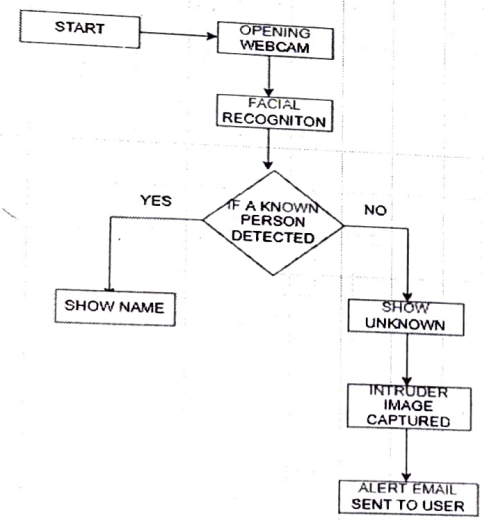


Fig. 3.2 Flow Chart

3.4 Software Development Life Cycle Model:

A software project can be implemented using this Rapid Application Development Model if the project can be broken down into small modules wherein each module can be assigned independently to separate teams. These modules can finally be combined to form the final product.

Development of each module involves the various basic steps as in waterfall model i.e analyzing, designing, coding and then testing,etc

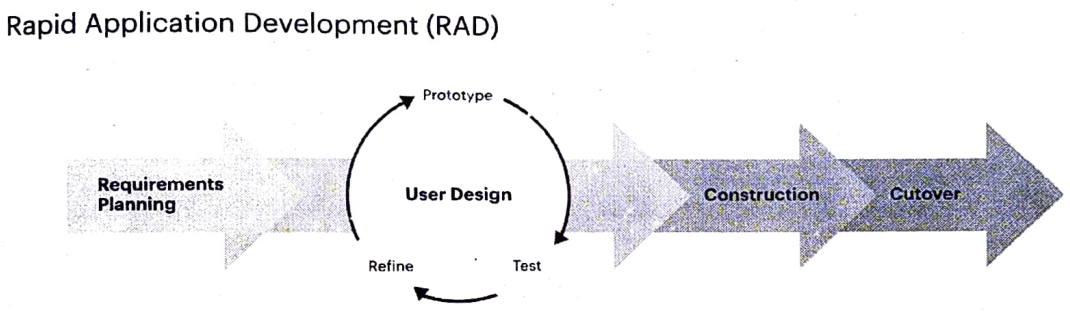


Fig. 3.3 Rapid Application Development Model

This model consists of 4 basic phases:

1. **Requirements Planning –**

It involves the use of various techniques used in requirements elicitation like brainstorming, task analysis, form analysis, user scenarios, FAST (Facilitated Application Development Technique), etc. It also consists of the entire structured plan describing the critical data, methods to obtain it and then processing it to form final refined model.

2. **User Description –**

This phase consists of taking user feedback and building the prototype using developer tools. In other words, it includes re-examination and validation of the data collected in the first phase. The dataset attributes are also identified and elucidated in this phase.

3. **Construction –**

In this phase, refinement of the prototype and delivery takes place. It includes the actual use of powerful automated tools to transform process and data models into the final working product. All the required modifications and enhancements are too done in this phase.

4. **Cutover –**

All the interfaces between the independent modules developed by separate teams have to be tested properly. The use of powerfully automated tools and subparts makes testing easier. This is followed by acceptance testing by the user.

Chapter 4: FINAL ANALYSIS AND DESIGN

4.1 Results: We have added the picture of Elon Musk in the database of the system. When the webcam captures a random image, it compares it to the pictures in the database and it is matched with the most accurate picture. As shown in the figure below Fig., System is detecting the picture as Elon Musk as a known person and displaying the name.

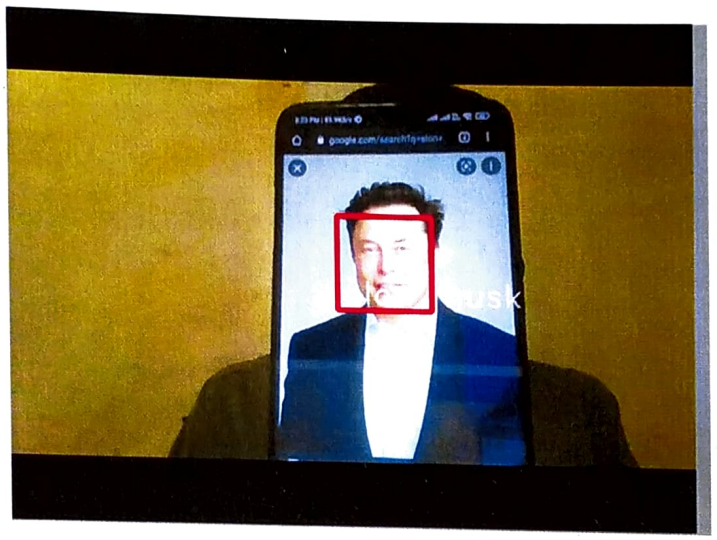


Fig 4.1.1. Known Face Detected

Similarly, when a picture of another person is shown who is not in our database, the system displayed unknown as it doesn't matches with the pictures in the database.

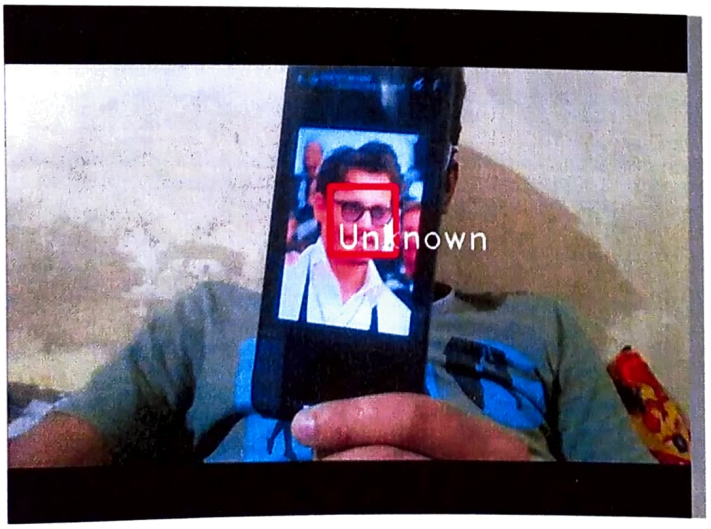


Fig. 4.1.2 Unknown Face Detected

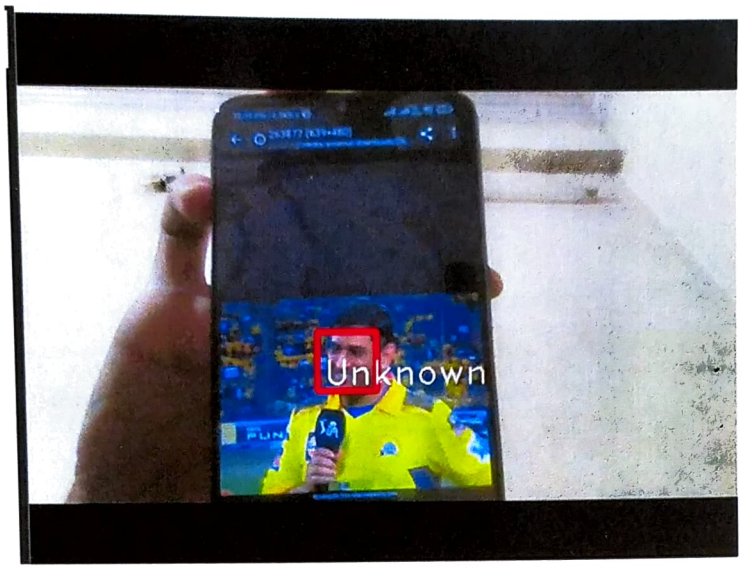


Fig. 4.1.3 Unknown Face

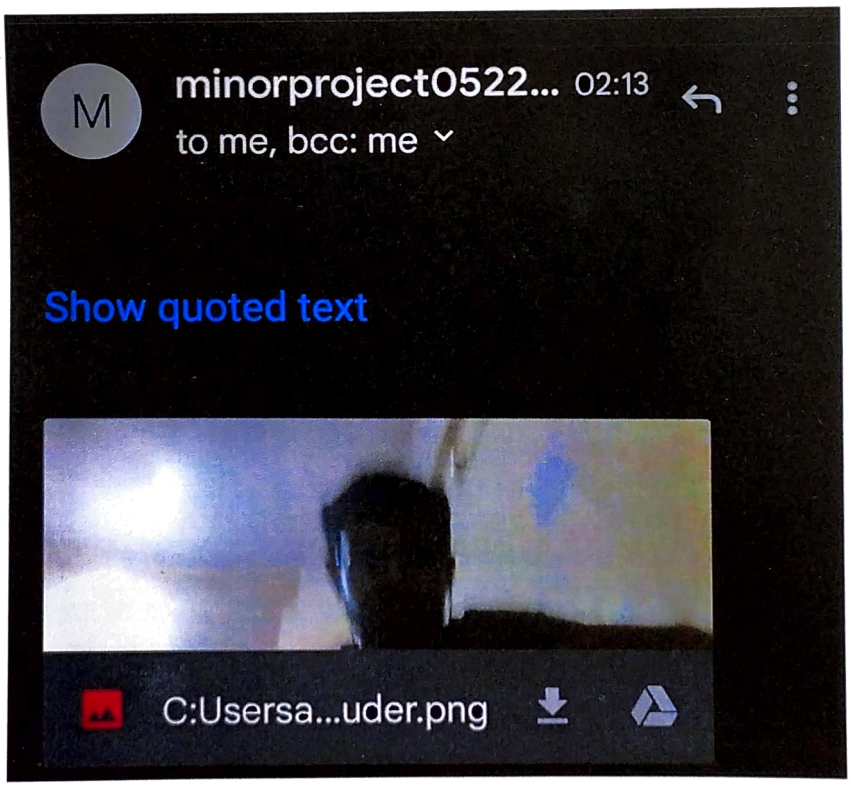


Fig. 4.1.4 Emailed Intruder Image

4.2 Results Analysis:

This application/project detects unknown people entered into a specific camera view and sends an alert email to the admin/owner along with sample intruder images.

* Here we used face_recognition python module.
* It is a dlib's state-of-the-art face recognition module built with deep learning backend.
* The model has an accuracy of 84%(approx) in detecting intruders.

4.3 Application:

The project can be used at various places where security is concerned such as:

- Departmental stores
- Shopping Malls
- Houses
- Mobile phones
- Face recognising lock system

4.4 Problems Faced:

- It faces difficulty in recognising similar faces.
- Low accuracy when the movement of the user is fast.
- Blurred images and low light causes difficulty.

4.5 Limitations:

There can be an error in recognizing the person during fast movement and also if the faces are similar, the system might get confused.

CHAPTER 5: CONCLUSION AND FUTURE WORK

5.1.1 Conclusion:

This project is a proof of concept on how to create an application that can detect human motion in a room, which also saves images to the local machine. The created project yields a good detection result with greater accuracy on labeling the acquired images. In case of recognising the owner or registered user, it displays the saved name of the user and if the face is unknown, it displays unknown with the face and sends it to the registered mail.

5.2.2 Future Scope:

- Can create an interface for the code.
- An alarm can be added when the intruder is detected.
- An ensembled learning can be deployed for increasing the efficiency of the project.
- We will optimise the model so that it can work on low processing power computers.
- We will try to incorporate the system with voice command features.

REFERENCES:

1. M. Piccardi (October 2004). "Background subtraction techniques: a review". IEEE International Conference on Systems, Man and Cybernetics 4. pp. 3099–3104.doi:10.1109/icsmc.2004.1400815
2. Yoshida, T., 2004. Background differencing technique for image segmentation based on the status of reference pixels." International Conference on Image Processing ICIP'04, pages 3487–3490, Singapore, October 24-27, 2004
3. Papert, The summer vision project, Massachusetts Institute of technology, 1996