SCHOOL OF ELECTRICAL ND ELECTRONIC ENGINEERING

MINI PROJECT REPORT
ON

"AI TRAINED SECURITY SYSTEM FOR BETTER SECURITY ON PRIVATE PROPERTY"

Submitted in partial fulfillment of the requirements for the award of the Degree of

Bachelor of Technology
In
Electrical and Computer Engineering

Submitted by

Ashish K Jacob(R20EL007)
Heba Yusuf(R20EL022)
Rakshitha Megha S(R20EL037)

Under the guidance of

Prof.Seema Magadum
DESIGNATION
REVA UNIVERSITY

2022-2023

Rukmini Knowledge Park, Kattigenahalli, Yelahanka, Bengaluru-560064
www.reva.edu.in

DECLARATION

We, **Mr. Ashish K Jacob(R20EL007), Miss.Heba Yusuf(R20EL022) Miss.Rakshitha Megha S(R20EL037)** students of B. Tech, belongs to the School of Electrical and Electronics Engineering, REVA University, declare that this Project Report entitled **"AI TRAINED SECURITY SYSTEM FOR BETTER SECURITY ON PRIVATE PROPERTY "** is the result the of project work done by me under the supervision of **Prof.Seema Magadum** in School of Electrical and Electronics Engineering.

We are submitting this Project Report in partial fulfillment of the requirements for the award of the degree of Bachelor of Technology in Electrical and Electronics Engineering by the REVA University, Bengaluru during the academic year 2022-23.

We further declare that this project report or any part of it has not been submitted for the award of any other Degree / Diploma of this University or any other University/ Institution.

(Signature of the Students)

*Certified that this project work submitted by **Ashish K Jacob, Heba Yusuf, Rakshitha Megha S*** ha*s been carried out under my / our guidance and the declaration made by the candidate is true to the best of my knowledge.*

Signature of Guide
Date …….

Signature of Director
Date …….
Official Seal of the School

SCHOOL OF ELECTRICAL AND ELECTRONICS ENGINEERING

CERTIFICATE

Certified that the project work entitled **"AI TRAINED SECURITY SYSTEM FOR BETTER SECURITY ON PRIVATE PROPERTY"** carried out under my / our guidance by **Ashish K Jacob(R20EL007), Heba Yusuf(R20EL022), Rakshitha Megha S(R20EL037)** are Bonafede students of REVA University during the academic year 2022-23, are submitting the project report in partial fulfillment for the award of Bachelor **of Technology in Electrical and Electronics Engineering** during the academic year **2022–23**. The project report has been approved as it satisfies the academic requirements in respect of Project work prescribed for the said Degree.

Prof.Seema Magadum
Asst. Professor, School of EEE
REVA University

Dr. Raghu C N,
Deputy Director, School of EEE, REVA University

Dr. M Dhanamjaya,
Vice Chancellor,
REVA University

External Examine

Name of the Examiner with affiliation Signature with Date

1.

2.

ACKNOWLEDGMENTS

This satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of the people who made it possible with constant guidance and encouragement and crowned our efforts with success.

A hearty thanks to our Project Guide **Prof.Seema Magadum,** School of EEE, for his guidance and support throughout the course.

We are grateful to **Dr. Raghu C N**, Deputy Director, School of Electrical and Electronics Engineering, REVA University, Bangalore, for his valuable support and encouragement.

We also thank all the staff members of the School of Electrical and Electronics Engineering and all those who have directly or indirectly helped us with their valuable suggestions in the successful completion of this project.

We express our thanks to **Dr. M Dhanamjaya**, Vice-Chancellor, REVA University, Bangalore, for extending his support.

We also thank our Honorable **Chancellor**, **Dr. P. Shyama Raju** for his support and encouragement and wonderful infrastructure/resources.

Finally, yet importantly we would like to thank our beloved parents for their blessings, love, and encouragement to successfully complete the task by meeting all the requirements.

Ashish K Jacob(R20EL007)

Heba Yusuf(R20EL022)

Rakshitha Megha S(R20EL037)

ABSTRACT

The project uses OpenCV for displaying video and image formats, PYQT6 is used to display all the UI elements present in the project for it to be used by the user. For the facial recognition to take place we need the presence of face recognition software known as DLIB library

OpenCV is a library of programming functions mainly aimed at real-time computer vision. Originally developed by Intel, it was later supported by Willow Garage then Itseez. The library is cross-platform and free for use under the open-source Apache 2 License.

The code is written in python, XML, Arduino IDE.

The GUI (graphical user interface) used in this project is PTQT6 to let the user decide between what to use and what not to use

The main Idea of the algorithm are as follows:

most of the statistics recorded is idle facts in which no pastime takes place. It uses action reputation to clear out the idle movement records and trims the component where pastime has been recorded the usage of movement detection and diverse movements.

Run the given data through the video processor and use that to run facial recognition software on the data being fed to us by the system.

Once the data is available it is then sent to the base system for it to be recorded and stored in a server (mostly plan on using MySQL or MongoDB.)

Then once all the needed information is processed and stored in the database, we can use all this data to run the overall security system starts to work.

A basic system can be tested using the Arduino uno project that is being made. The only time the door will

LIST OF TABLES

LIST OF FIGURES

Contents

Appendix

Program Code

Paper published

Data sheets

CHAPTER 1
INTRODUCTION

1.1 History

The use of artificial intelligence (AI) in security has a relatively short history, but it has already had a significant impact on the field. In the early days of AI, researchers focused on developing systems that could perform specific tasks, such as playing chess or solving math problems. However, as AI technology has advanced, it has been applied to a wide range of security applications.

One of the earliest examples of AI being used in security was in the development of expert systems, which were designed to replicate the decision-making abilities of human experts in a particular domain. These systems were used in a variety of security contexts, including intrusion detection, risk assessment, and fraud detection.

In recent years, AI has been used to improve the effectiveness of security systems in a number of ways. For example, AI-powered security cameras can analyze video feeds in real-time to identify suspicious activity, while AI-based intrusion detection systems can analyze network traffic to identify and alert on potential cyber threats.

AI has also been used to improve the accuracy and efficiency of security operations centers (SOCs). By analyzing large amounts of data and using machine learning algorithms, AI-powered SOCs can identify patterns and trends that may indicate a security incident is imminent.

1.2 Project overview

Over the previous couple of years because of globalization a major exchange has been came about in exceptional sectors global including enterprise, protection, fitness, etc. one of their key sectors that are now challenge global is security and privateness. Because of the emergence of shielding premises, offering security is one of the most important Obligations in recent times.

This Project aims to make securing a house automated task and to not require constant attention or invigilation. The more the security system is used the more it autonomous it becomes making it the perfect candidate to be used in big houses with old people in it.

CHAPTER 2
LITERATURE SURVEY

[1] The Impact of Artificial Intelligence on Data System Security: A Literature Review

Ricardo Raimundo 1and Albérico Rosário

Abstract:

Diverse forms of artificial intelligence (AI) are at the forefront of triggering digital security innovations based on the threats that are arising in this post-COVID world. On the one hand, companies are experiencing difficulty in dealing with security challenges with regard to a variety of issues ranging from system openness, decision making, quality control, and web domain, to mention a few. On the other hand, in the last decade, research has focused on security capabilities based on tools such as platform complacency, intelligent trees, modeling methods, and outage management systems in an effort to understand the interplay between AI and those issues. The dependence on the emergence of AI in running industries and shaping the education, transports, and health sectors is now well known in the literature. AI is increasingly employed in managing data security across economic sectors. Thus, a literature review of AI and system security within the current digital society is opportune. This paper aims at identifying research trends in the field through systematic bibliometric literature review (LRSB) of research on AI and system security. The review entails 77 articles published in the Scopus database, presenting up-to-date knowledge on the topic. The LRSB results were synthesized across current research subthemes. Findings are presented. The originality of the paper relies on its LRSB method, together with an extant review of articles that have not been categorized so far. Implications for future research are suggested

Introduction:

The assumption that the human brain may be deemed quite comparable to computers in some ways offers the spontaneous basis for artificial intelligence (AI), which is supported by psychology through the idea of humans and animals operating like machines that process information by devices of associative memory [1]. Nowadays, researchers are working on the possibilities of AI to cope with varying issues of systems security across diverse sectors. Hence, AI is commonly considered an interdisciplinary research area that attracts considerable attention both in economics and social domains as it offers a myriad of technological breakthroughs with regard to systems security [2]. There is a universal trend of investing in AI technology to face security challenges of our daily lives, such as statistical data, medicine, and transportation [3]. Some claim that specific data from key sectors have supported the development of AI, namely the availability of data from e-commerce [4], businesses [5], and government [6], which provided substantial input to ameliorate diverse machine-learning solutions and algorithms, in particular with respect to systems security [7]. Additionally, China and Russia have acknowledged the importance of AI for systems security and competitiveness in general [8,9]. Similarly, China has recognized the importance of AI in terms of housing security, aiming at becoming an authority in the field [10]. Those efforts are already being carried out in some leading countries in order to profit the most from its substantial

Conclusion:

This piece of literature allowed illustrating the AI impacts on systems security, which influence our daily digital life, business decision making, e-commerce, diverse social and legal issues, and neural networks. First, AI will potentially impact our digital and Internet lives in the future, as the major trend is the emergence of increasingly new malicious threats from the Internet environment; likewise, greater attention should be paid to cyber security. Accordingly, the progressively more complexity of business environment will demand, as well, more and more AI-based support systems to decision making that enables management to adapt in a faster and accurate way while requiring unique digital e-manpower. Second, with regard to the e-commerce and manufacturing issues, principally amidst the world pandemic of COVID-19, it tends to augment exponentially, as already observed, which demands subsequent progress with respect to cyber security measures and strategies. The same, regarding the social applications of AI that, following the increase in distance

[2] Camera based Smart Surveillance System-Literature Survey Ishan Kokadwar, Anurag Kulkarni, Sayali Khare, Vaibhav Limbhore, Swati Chandurkar

Abstract:

Over the last few years due to globalization a major change has been occurred in different sectors worldwide such as business, security, health, etc. One of their key sectors which are now concern worldwide is security and privacy. Due to the emergence of protecting premises, providing security is one of the most important tasks. Thus, to provide security, the video surveillance system was introduced. A video surveillance system is used for the monitoring of the behavior, activity or other information generally of people in a specific area. The application of video surveillance is now not only limited to provide security for area but expanded to the various sectors. This paper aims to elaborate the various techniques in video surveillance, automated video analysis and insight generation. These techniques were used to build the Software System for Automated Surveillance for Academic Institution's Campus premises.

Introduction:

Nowadays, security is measure concern in every organization. To this satisfy issue the organizations use surveillance cameras. The limitation in using them is that there must be an operator to watch the stream from the cameras and take respective decisions. The use of camera-based surveillance has extended from security to tracking, environment and threat analysis and many more. By using the power of modern computing and hardware it is possible to automate the process. The emergence of machine learning, Deep learning, and computer vision tools have made this process efficient and feasible for general purpose use. So instead of using human support for monitoring and insight generation, we can let the processor and machine learning system do the task in a more efficient and errorless way. Here we have mentioned few approaches which had helped us in solving this problem.

Conclusion:

In this paper we have discussed data collecting, storing and analysis technique for CCTV Camera Surveillance. We found that for feature extraction and tuning system to work hand in hand with deep learning model hear cascade was useful. By using Image Mosaicking technique images could be stitched and camera position limitation were removed. Thus, among many methods of collecting camera input we found IP based camera technique on distributed network us useful and CNN model was useful for detail analysis.

[3]: AI enabled smart surveillance system (J. Phys.: Conf. Ser. 1916 012034)

Abstract:

The conventional household door locking system has lot of drawbacks and it is still yet not resolved. Most of the security systems so far in our markets includes video surveillance or vigilance system. In order to improve security level facial recognition and object detection technique using CNN algorithms can be used which is also provides remote proctoring facilities to owners. The proposed system detects the object and identifies the anomalous activity near the door by applying Convolutional Neural Network. Electric door lock solenoid is used to unlock the door. An ultrasonic sensor is utilized to measure the distance between a person and door through the facial recognition when it reaches a certain threshold value that has been kept to detect the person reaching the doors and it tries to capture the human image only if it is mismatched from database. When a stranger tries to access the door, an alert message might be triggered to registered mobile number and the proprietor would be able to control the door locking system and inspect the image of person which has been mailed.

Introduction:

Nowadays, the safety and security are most challenges issues in modern time society to stop people life and their valuables assets from illegal handling. As a result, the safety and security extending to personal social security to protect every individual's personal information, valuable things and their day-to-day activities. Hence, the private security services moving towards to integration of video surveillance, door lock access conflicts in personalized monitored areas [1, 2]. The personal authorization or network based remote authorization or smart devices based on local authorization, or the illegal access risk within the building facility. In recent era, the network based centralized electronic access system developed for security gate and control and door access control in smart buildings with different user authorization interfaces like wireless communication technology like Near-Field communication (NFC), Contactless Communication Technology like Radio-Frequency Identification (RFID), fingerprint recognizer, and face recognizer, etc. [3-7] to limit the physical access of the people within the buildings or assets. The building facility localized electronic access system receives the user specific authentication and authorization information from a centralized access system server and performs the automated gate or door lock open or close control for the precise individuals to access control system user authentication interfaces are subject to the security compromising by exposing the password or digital keys to strangers. Also, the RF-based

available user interfaces are susceptible to security threats. However, the installation cost of remote proctored system would be high and also has the weakness of access distance, security and network access efficiency issue. Recent advancement in IoT plays vital role in remote monitoring and security systems. These security systems can be improved by providing intelligence to the hardware components. AI based Jetson Nano device supports to integrate intelligence to detect anomalous activities by enabling deep learning concept. It will increase the efficiency of the security system

Conclusion:

Our proposed system is to provide safety and security. This proposed system helps people to secure house from an unauthorized person. To lock and unlock the smart door we don't need any keys it will open only for an authorized person and it doesn't open for an unauthorized person. In bounding boxes an algorithm was implemented and its process is to distinguish the authorized and unauthorized person. The bounding boxes marking green and red for detected person. In future we can enhance the execution time delay which is useful for identifying the burglars quickly and taking action according to the situation

CHAPTER 3
PROPOSED WORK

3.1 Security module

3.1.1 Introduction

The camera already present can access the data for the face of the person present in the front door. This image taken from the front door can be used by the facial recognition AI allowing it to run it through the existing system to make a decision. This decision can lead us to multiple different options that are available for the use of the system.

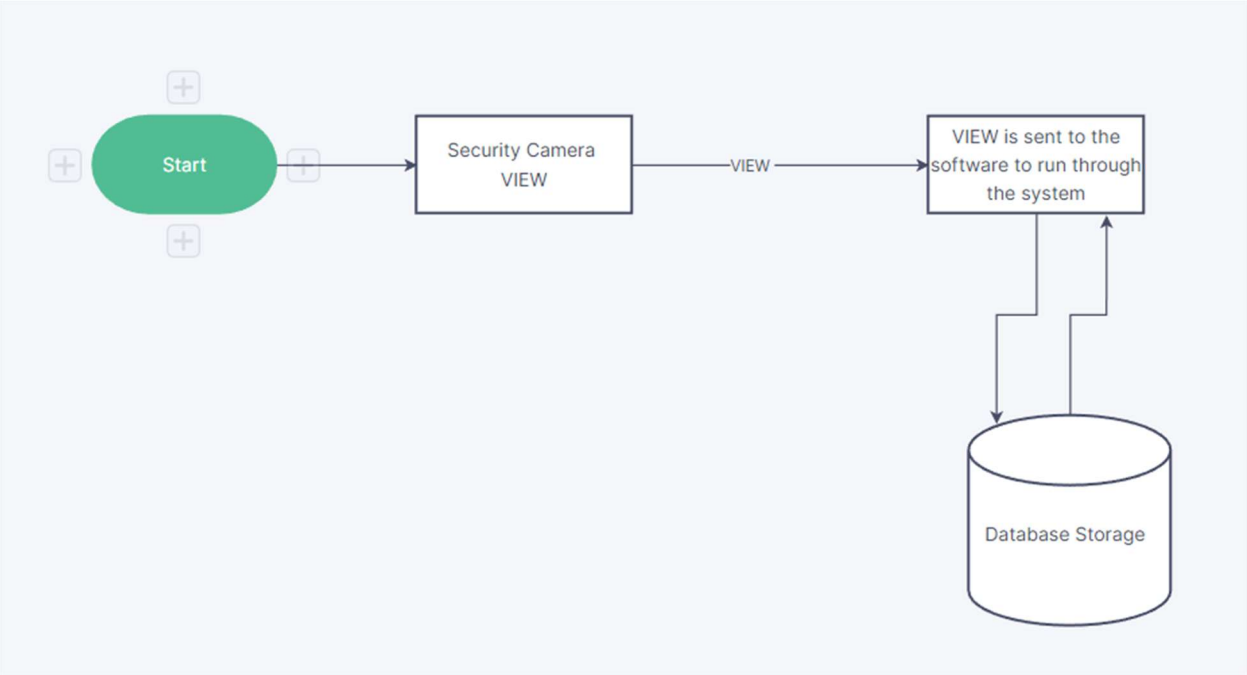


Fig 1: Basic Idea of the Security System

The needed information can be taken and stored in a database present in a remote location or in a Networked server allowing us to keep work with the data.
All the needed information is automatically stored and can be accessed by the AI to run and will give us the necessary output

3.1.2 OpenCV2 and its implementation

OpenCV (Open-Source Computer Vision) is a popular computer vision library containing a large collection of image processing functions. It was originally developed by Intel and is now maintained by Willow Garage and Itseez.

The library is cross-platform and free for use under the open-source BSD license. It has C++, Python, and Java interfaces, and it supports Windows, Linux, Mac OS, iOS, and Android.

OpenCV's Python module is a wrapper for the original C++ library. It is implemented using the Python's ctypes library, which is used to invoke functions in a dynamic link library (DLL). The cv2 module is the second version of the original cv module. It is recommended to use cv2, as it has more features and better support for newer versions of OpenCV.

OpenCV provides many useful functions for loading, displaying, and processing images, videos, and webcam feeds. It also has a number of functions for feature detection and extraction, such as edge detection, object detection, and template matching. It can be used in a variety of applications, including security and surveillance, image and video processing, and computer vision-based human-computer interaction.

3.1.3 PYQT6 and its implementation

PyQt is a set of Python bindings for the Qt application framework and Qt GUI library. Qt is a cross-platform application framework that is widely used for developing applications with a graphical user interface (GUI) in C++. PyQt6 is a set of Python bindings for Qt version 6. It is implemented as a Python extension module (native code) that wraps the popular Qt library, which is written in C++. PyQt6 provides bindings for all of the Qt classes and functions, and it is available for use under the GPL and commercial licenses. PyQt is available for Windows, Linux, and macOS. It is a popular choice for building GUI applications in Python, as it allows developers to use the same codebase for all three major platforms. PyQt6 is compatible with Python 3.

3.1.4 Facial Recognition working

Facial recognition is a technology that can identify or verify a person from a digital image or video frame. It typically involves comparing a detected face in a photograph or video with a database of faces to find a match.

Dlib is a machine learning library in C++ that provides tools for facial recognition. It contains algorithms that can be used to detect and track faces in images and videos, as well as extract facial landmarks such as the eyes, nose, and mouth. It also has a number of pre-trained models for facial recognition that can be used out of the box.

To perform facial recognition using dlib, you would first need to detect faces in an image or video frame using the face detection functions provided by the library. You can then use the detected facial landmarks to align and normalize the face, and finally compare the normalized face to a database of known faces using a similarity measure. If a match is found, the person's identity can be determined.

Dlib is a powerful library with many features and options, but it can be complex to use and requires some programming knowledge. It is well-suited for applications that require robust and accurate facial recognition, but may be overkill for simpler tasks.

3.2 Door Handling

3.2.1 Arduino Uno

Arduino Uno is a microcontroller board based on the ATmega328P (datasheet). It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analogue inputs, a 16 MHz quartz crystal, a USB connection, a power jack, an ICSP header and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with an AC-to-DC adapter or battery to get started.

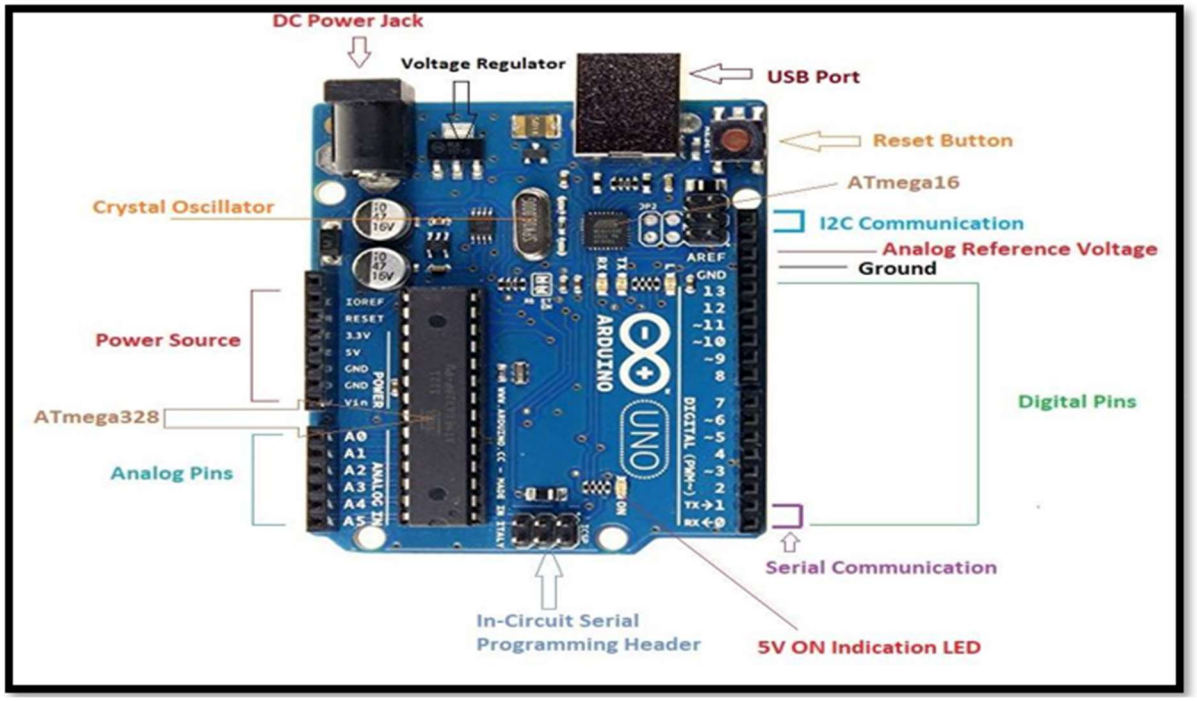


Fig 2: Arduino UNO

Microcontroller	ATmega328P
Operating Voltage	5V
Input Voltage (recommended)	7-12V
Input Voltage (limit)	6-20V
Digital I/O Pins	14 (of which 6 provide PWM output)
PWM Digital I/O Pins	6
Analog Input Pins	6
DC Current per I/O Pin	20 mA

Table 1 : Arduino Specification

3.3 Communication between the different Libraires

This Code Works by dividing all the code into separate modules. These Modules then combine together to give us the required output. Each module can be divided into two categories and those are as follows

- Frontend : OpenCV library, PYQT6
- Backend : OpenCV library, DLIB library

3.3.1 OpenCV2 to PYQT6

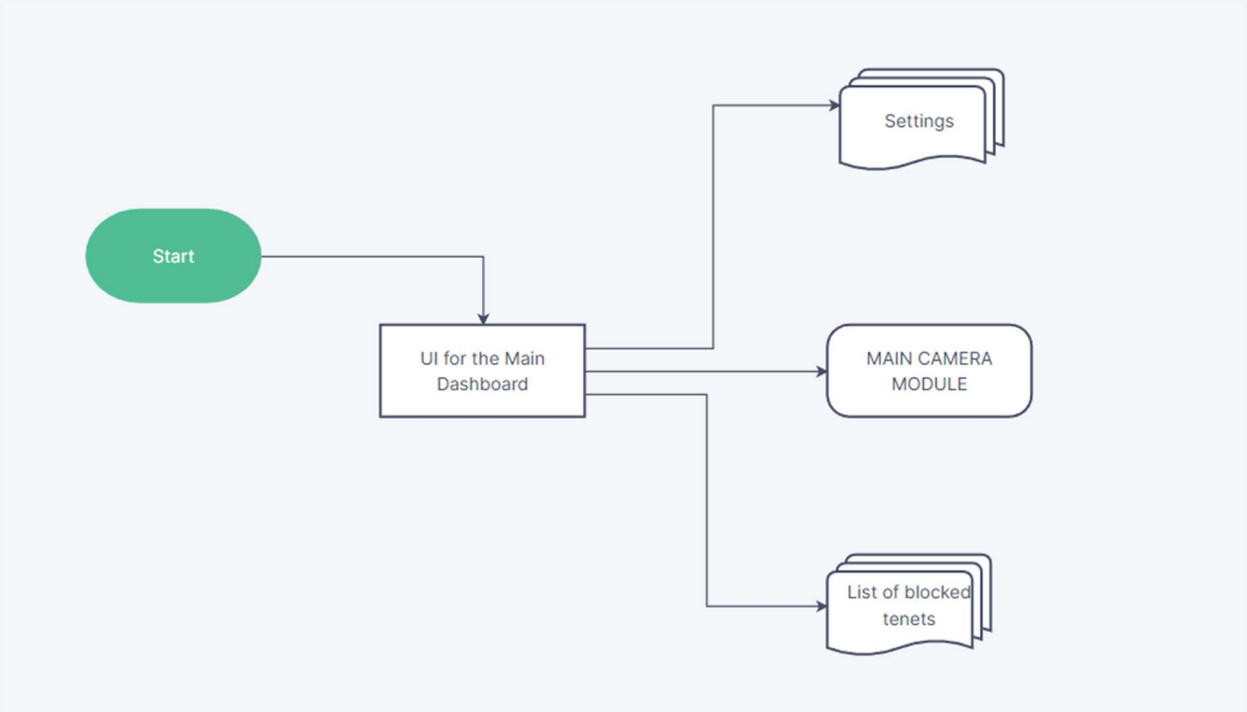


Fig 3: Front End Flowchart for the user

UI : this is the main UI of the overall security system shown to the user
Settings : different settings available to the user
Main Camera Module : Allows for the data to be recorded to the system
Block List : this shows the list of people who are blocked from the system and cannot

3.3.2 OpenCV2 to Facial Recognition Module

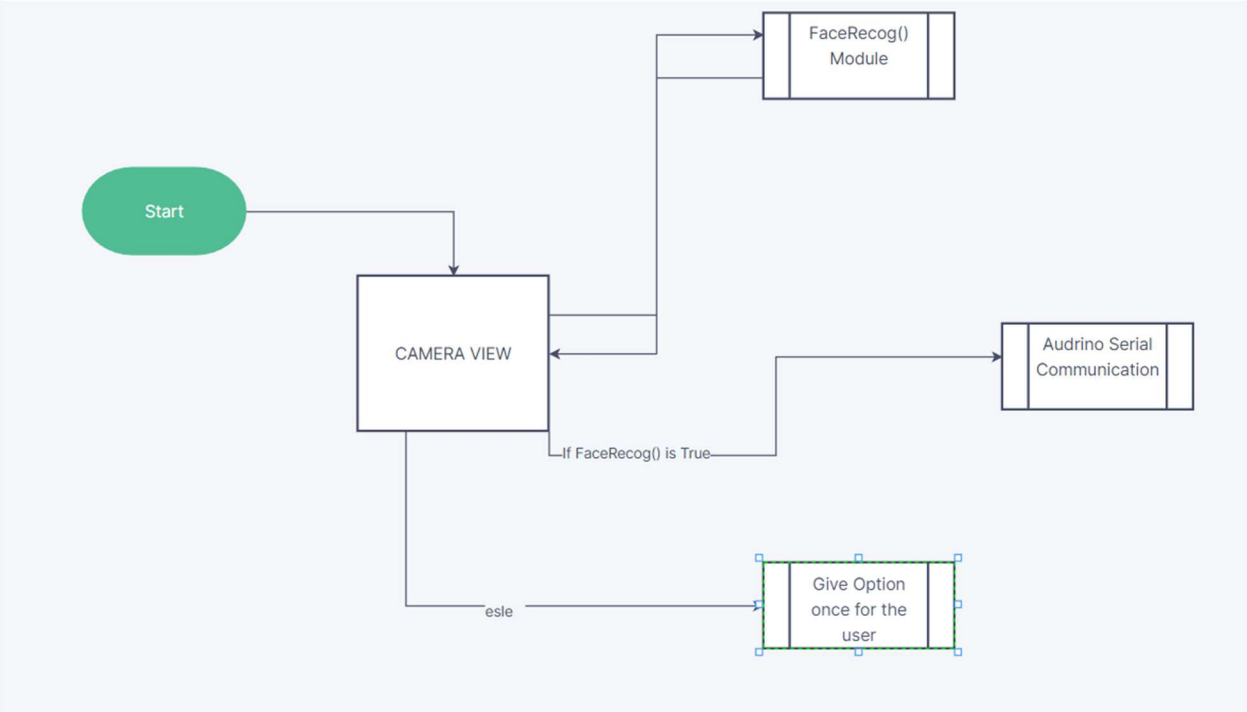


fig 4: facial recognition back end

3.3.3 The Arduino Communication

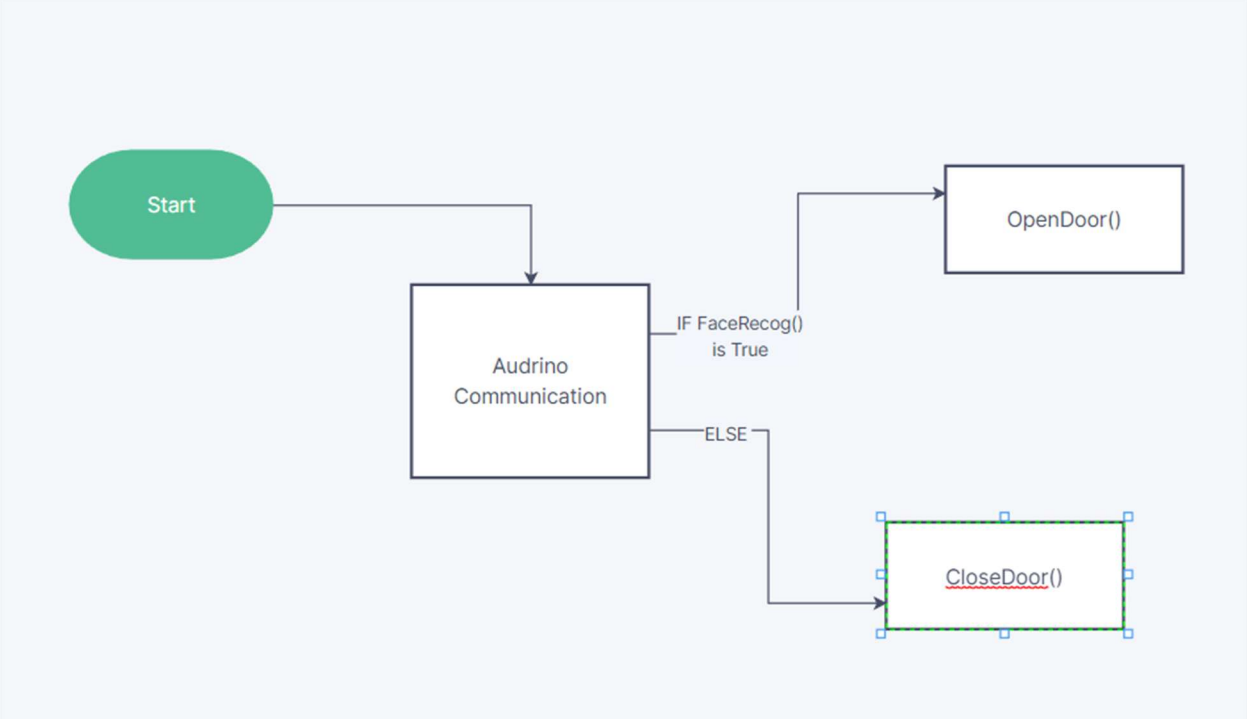


Fig 5 : Arduino cases present

3.4 Additional features available

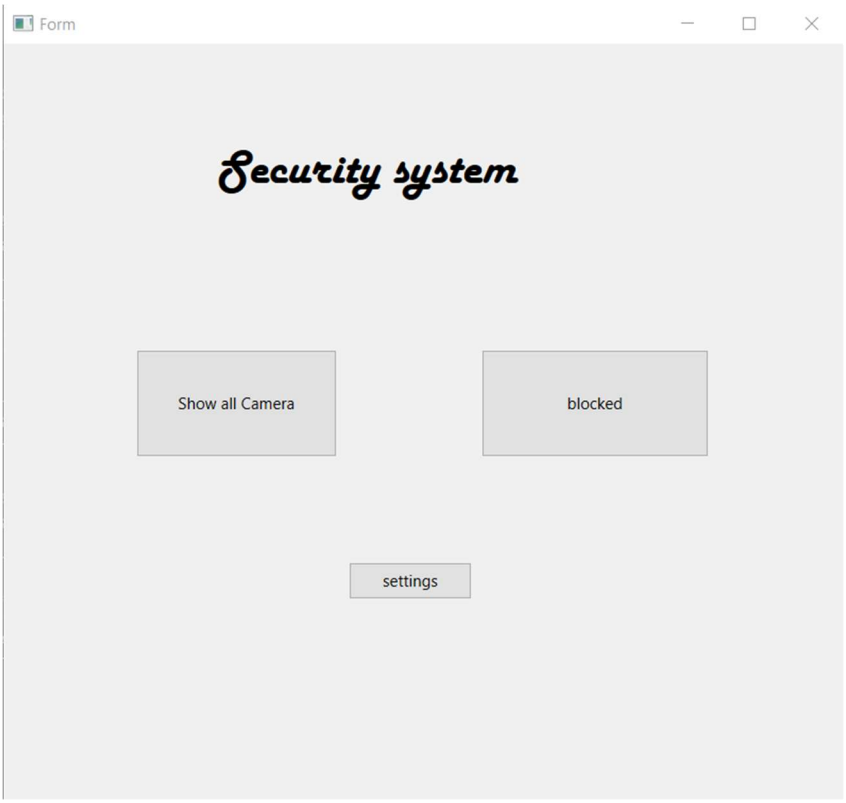
- Allows hand tracking to make needed decision
- Block list can be used to automatically contact the authorities
- Live Video can be sent to any source

3.5 Final Project Outlook

The interpretation drawn after completion of the full-fledged project is that it's an Automated security robot that allows for the completion. The robot is equipped with many applications that will ease the institutional workload and improve education handling. The software interacts with Arduino to decide who can and who cannot access the needed data.

CHAPTER 4
RESULT ANALYSIS

4.1 Automatic Security System

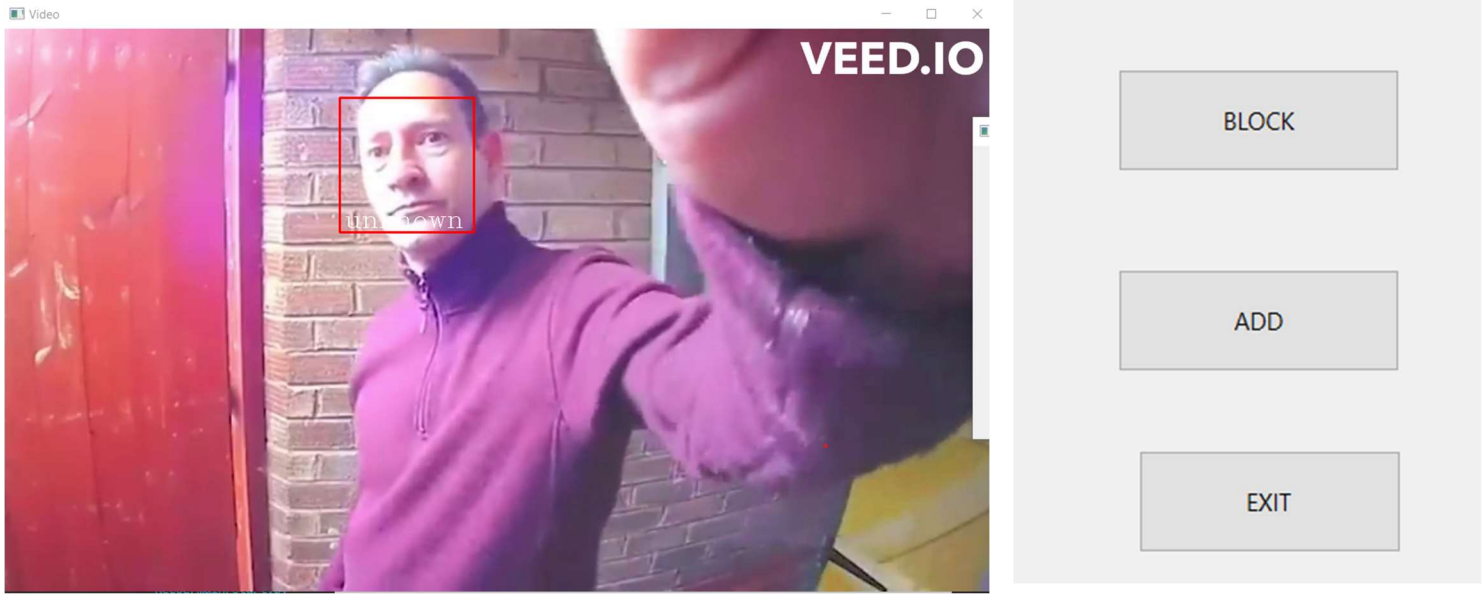


This is the main dash board of the programme being used by the software providing the user with all the necessary details required for the functioning of the programme and all the options from there can then be shown to the user allowing for us to get all the necessary details.

4.2 Usage of the software

Once the show all button of the camera is pressed, we can see that all the problems happening with the front door camera will be shown to the user and until and unless the person in the entrance is trusted it doesn't allow for the door to be opened

4.2.1 “Show all Camera” option



As you can see an unknown person has tried to use the automated system but the AI recognized that this person is not allowed to enter a locked itself

The photo will be sent to the emails of the owner of the house and the necessary authorities can also be called and they can do the necessary work required to stop the intruder too.

CHAPTER 5
CONCLUSION AND FUTURE SCOPE

5.1 conclusion

In conclusion, AI powered security cameras offer a number of benefits over traditional security cameras. They are able to analyze footage in real-time, alerting users to any potential threats or unusual activity. This not only improves the efficiency of security systems, but also allows for a quicker response to any incidents that may occur. In addition, AI technology is constantly improving, which means that these security cameras will only become more advanced and effective over time. Overall, the use of AI in security cameras represents a significant step forward in the field of security and surveillance.

5.2 future scope

There are a number of potential future developments that could be implemented in AI-based security systems:

Improved facial recognition technology: Currently, facial recognition systems are not always accurate, particularly when it comes to identifying individuals with certain characteristics (such as people of color or those wearing masks). However, as AI technology continues to improve, it is likely that these systems will become more reliable and accurate.

Integration with other smart home devices: AI security systems could potentially be integrated with other smart home devices (such as smart locks, thermostats, and lighting systems) to create a more comprehensive and seamless security system.

Predictive analytics: AI could potentially be used to analyze historical data and predict when and where potential security threats may occur, allowing for proactive measures to be taken.

Enhanced surveillance capabilities: AI could be used to improve the resolution and clarity of surveillance footage, as well as increase the range and coverage of security cameras.

Improved cybersecurity: As AI-powered security systems become more prevalent, it will be important to ensure that they are secure against potential cyber threats. AI could be used to detect and prevent cyber-attacks on security systems