TITLE:

SMART HOME SECURITY SYSTEM WITH FACE RECOGNITION AND WEAPON DETECTION

TEAM MEMBERS :

- K.DINESH (RA2111003011858)
- D.PAVAN KUMAR (RA2111003011863)
- D.SAI SIDDARDHA(RA2111003011887)

1.INTRODUCTION:

Image processing is a method to perform some operations on an image, in order to get an enhanced image or to extract some useful information from it. It is a type of signal processing in which input is an image and output may be image or characteristics/features associated with that image. Nowadays, image processing is among rapidly growing technologies. It forms core research area within engineering and computer science disciplines too. Image Processing is a humungous field and has variety of applications in different disciplines of technology such as Artificial Intelligence, medical sciences, forensics, robotics etc. We targeted a daily life problem which we thought if solved could be of major use to people.

2.PROBLEM STATEMENT:

Today home automation systems are popular in households. The control of electric fixtures like fans and lights is possible with the help of Internet of Things (IOT). The problem arises due to intrusion of burglars. The security of such systems has been done using computer vision and IOT. Here we aim to enhance this system by use of image processing for object detection. The system uses cameras at the door for face recognition as access control. Also, vibration and door magnet sensors are installed at the entry points to detect when the burglar tries to barge inside. PIR sensors are employed to detect human presence. A vibration sensor is also used to give alert if any shock nearby is detected. The system allows entry only if authorized person like owner or person registered on the database arrives. The person may be identified through valid proof of identity. It sends a message to the owner in case it doesn´t recognize the person within 20 seconds and the owner can monitor the activities via live feed from the camera. All sensor signals are checked and status of the system is updated continuously. In case the burglar tries to break inside, siren is activated and alert messages are redirected to the owner and the police.

3.WHY THIS PROJECT:

The existing systems offer multifactor authentication via biometrics which means more number of parameters for access. To simplify this, we introduce a single factor of authentication using face recognition. Security systems have provided protection against camera tampering, but it is a late response to a potential intruder. This can be improved using weapon detection along with it. The primary idea was to develop a system with state of the art algorithm on a low end embedded device. The concept can then be used to make efficient security cameras and thereby reducing costs without compromising on accuracy. The need of a system arises as the video data captured can be used for analytics to give details of activities in a timely manner.

- Most state of the art algorithms have a bottleneck when processing in real time without dedicated hardware. Hence, a need for the system to achieve a reliable result even without high end hardware appeared. The instrumentation of the sensors has to be done so that the house is secured from all sides and not just a single point of entry. This requires the system to be able to detect human presence, if any shock is there, when the door or window is moved and an alert signal in case of any emergency.

4.OBJECTIVES:

- The primary objectives of the system are:
- Perform Face Recognition using higher accuracy models
- Detect weapons in video stream
- Send timely alerts triggered by sensors
- Detect tampering of the system

The evaluation of the system was done by using simple metrics such as speed, latency, accuracy, etc. All the parameters considered depend highly on the methodology followed.

4.1 Face Recognition Model :

The Face Recognition model uses deep metric learning present in Dlib C++ Library. The model reached an accuracy of 99.38% on the Labelled Faces in the Wild (LFW) dataset. This network was trained on 3 million images. It uses a ResNet having 29 convolutional layers. The number of frames per second was considered as evaluation metric. The time taken to generate a frame also includes the time required to perform inference on a single frame. The trained model for face recognition is converted to inference model

Figure 4.1.1: Authorized person recognized with name as

Figure 5.2: Unauthorized person labelled as unknown

4.2 WEAPON DETECTION MODEL :

Weapon Detection uses the RetinaNet object detection model adapted in Keras library. It is an extension to SSD-ResNet model with an additional convolutional neural network called Feature Pyramid Network as backbone which is used for bounding box regression. The performance was poor for this model. This model architecture being computationally intensive and with a mAP score of 32 on the COCO dataset requires high performance GPUs with lots of memory to give faster throughput results. It is a highly accurate model. However, there were difficulties during classification for various orientation of the same object. This could be improved with retraining.

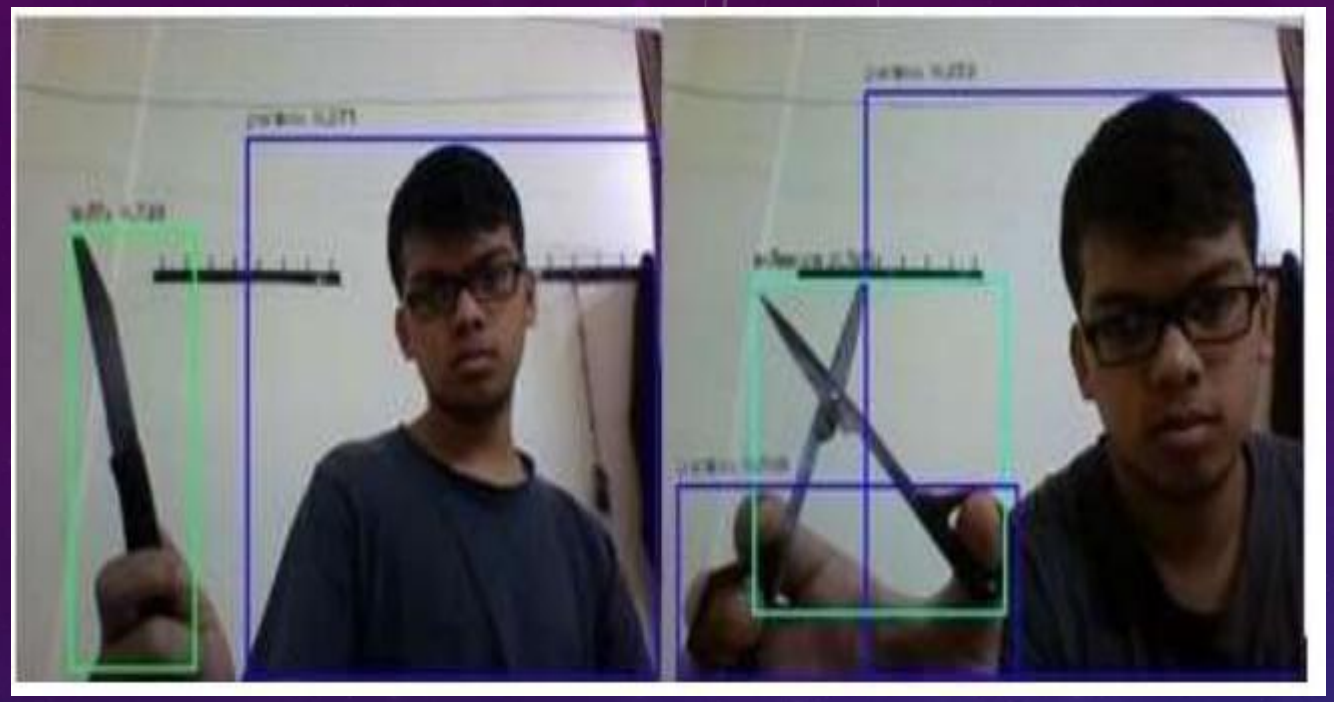

Figure 4.2.1: Weapons detected and labelled with their names

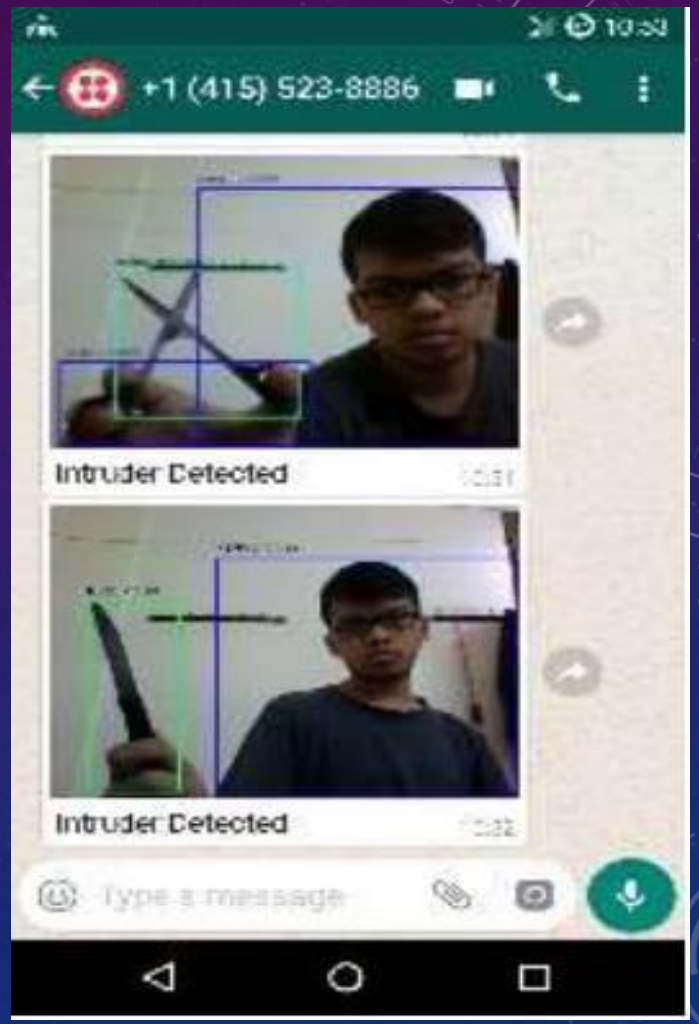

Figure 4.2.2: Notification alerts received via Twilio API

5. REQUIREMENTS :

5.1 Software Requirements : The project was developed using Python. This chapter describes about the software packages and libraries which were used in the project. The project uses Raspberry Pi 3 Model B, hence, the operating system is Linux based Raspbian OS. Image Processing was implemented with the help OpenCV. Intel OpenVINO Toolkit R5.1 for Linux is used for hardware acceleration of image processing. IOT was implemented using IFTTT android application.

5.2 Hardware Requirements : The components required for the project include PIR sensor, Door Magnet sensor, Vibration sensor, circuit break detection module for wire connections, panic switch, Raspberry Pi 3 Model B board, Pi Camera module, Neural Compute Stick 2, servo motor, Hikvision Network Camera (Wired), Network Switch, PoE cables, Ethernet cables, DVR, JioFi device(router), SD card, monitor, keyboard, mouse, breadboards, jumper wires, extension wires, LED modules, buzzers, 12V DC battery, Arduino Uno board and 5V Power Supply.

6.CONCLUSION:

The system developed in this work proposes a simplified way to handle access control and intrusion detection in smart homes. The use of face recognition for access control is an efficient way for this environment. The sensors used are capable of providing instant alerts, so that the owner is never left to unforeseen circumstances.It requires further investigation with customized models and training on large datasets. Therefore, the best performance can be achieved by redefining image processing algorithms and not using off-the-shelf models. One of the important highlights of the system is weapon detection using image processing.This method promises to improve the detection rates of a potential intruder and improve the overall efficiency of the access control system. The system also implements a fail-safe method by having extra components powered by electric power backup in case there is a circuit failure. The tampering of the circuit is also detectable, which makes it suitable for emergencies. With all the above features, the system is apt for use in modern homes.

Thank You