SMART HOME SECURITY SYSYTEM WITH FACE RECOGNIZATION AND WEAPON DETECTION

MINI PROJECT REPORT

18CSC305J - ARTIFICIAL INTELLIGENCE

Submitted by

KAYYALA PRASANNANJANEYULU (RA2011026010358)
VADDU SRUJAN REDDY (RA2011026010352)
RUDRA PRATAP SINGH (RA2011026010377)

Under the guidance of

Dr.K.Suresh

Assistant Professor, Department of Computational Intelligence

in partial fulfillment for the award of the degreeof

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

of

FACULTY OF ENGINEERING AND TECHNOLOGY

S.R.M. Nagar, Kattankulathur, Chengalpattu District

MAY 2023

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Under Section 3 of UGC Act, 1956)

BONAFIDE CERTIFICATE

Certified that Mini project report titled **"SMART HOME SECURITY WITH FACE RECOGNIZATION AND WEAPON DETECTION"** is the bona fide work of **KAYYALA PRASANNANJANEYULU (RA2011026010358),VADDU SRUJAN REDDY(RA2011026010352) AND RUDRA PRATAP SINGH(RA2011026010377)** who carried out the minor project under my supervision. Certified further, that to the best of my knowledge, the work reported herein does not form any other project report or dissertation on the basis of which a degree or award was conferred on anearlier occasion on this or any other candidate.

SIGNATURE

Dr.K.Suresh
GUIDE
Assistant Professor
Department of Computational Intelligence

SIGNATURE

DR.R.Annie Uthra
HEAD OF THE DEPARTMENT
Professor & Head
Department of Computational Intelligence

1.TITLE :

SMART HOME SECURITY SYSTEM WITH FACE RECOGNITION AND WEAPON DETECTION

TABLE OF CONTENTS

2.ABSTRACT :

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 doesnot 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.INTRODUCTION:

The main problem of face recognition is its high dimension space, which is to be reduced by any dimension reduction techniques. The pattern recognition approach then tries to match the facial features, which are extracted from all the images present in the database. Therefore, there are two major problems one is feature extraction and then pattern recognition. Before this image, registration of all the faces is required to enhance the recognition rate of the whole system. So these all motivates to search for a new method to solve all these problems and then integrate them to make a fully functional system with high accuracy.

The recent trends in home market security indicate that focus is now shifting to providing large scale solutions. The number of devices that can be connected are increasing multi fold. The systems are able monitor indoors and give high quality surveillance feed. They provide protection to the home owners by monitoring levels of humidity, temperature, presence of toxic gases like carbon monoxide, etc. Hence, with the use of improved data driven algorithms, the security systems can be can be enhanced and made even smarter than existing systems in future.

- To do face recognition in real time.
- Enhance the Speed i.e. frames/sec.
- Do recognition on high Camera resolution.

4. LITERATURE SURVEY :

1.Viola, P., & Jones, M. J. (2001). Rapid object detection using a boosted cascade of simple features. Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 1, I-I.

2.Dalal, N., & Triggs, B. (2005). Histograms of oriented gradients for human detection. Proceedings of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 1, 886-893.

3.Viola, P., Jones, M., & Snow, D. (2003). Detecting pedestrians using patterns of motion and appearance. International Journal of Computer Vision, 63(2), 153-161.

4.Yang, M. H., Kriegman, D. J., & Ahuja, N. (2002). Detecting faces in images: A survey. IEEE Transactions on Pattern Analysis and Machine Intelligence, 24(1), 34-58.

5.Zhang, Z., & Zhang, H. (2010). A survey of recent advances in face detection. Microsoft Research Asia Technical Report.

6.Jain, A. K., & Ross, A. (2004). Multibiometric systems. Communications of the ACM, 47(1), 34-40.

7.Rowley, H. A., Baluja, S., & Kanade, T. (1998). Neural network-based face detection. IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(1), 23-38.

8.Yang, M. H., Roth, D., & Ahuja, N. (2000). A framework for joint face detection and tracking. Proceedings of the 2000 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2, 712-718.

9.Li, S. Z., & Jain, A. K. (2005). Handbook of face recognition. Springer Science & Business Media.

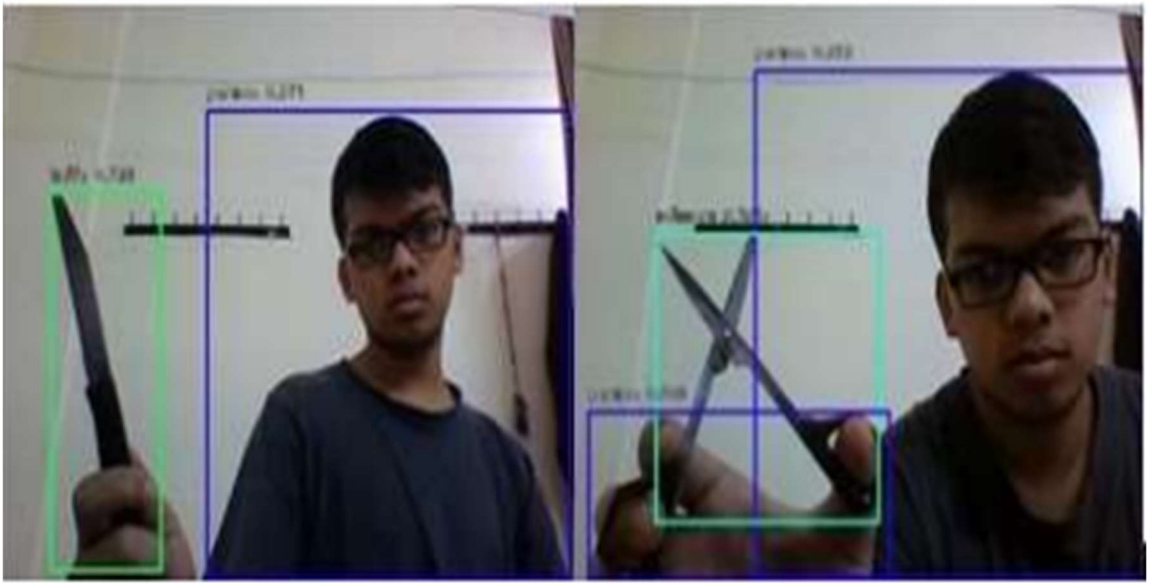
10.Li, S. Z., Zhu, J., & Zhang, Z. (2005). Face detection: A survey. International Journal of Image and Graphics, 5(3), 371-390.

5. DATA DESCRIPTION :

5.1 Images Data Sets For Traing Our Model :

6. TESTING :

6.1. MODEL RECOGNIZES AFTER TRAINING :



7.CHALLENGES IN EXISTING SYSTEM :

For an average household owner, there is no means of monitoring the indoor activities remotely. Most houses don't have intrusion detection systems. Thus cases of theft have increased day by day. Surveillance systems are largely used by offices of banks, organisations, educational institutions and product based industries. The existing systems are capable of delivering good performance at much higher costs. There is a scope of reducing costs in terms of both capital and computational performance. Presently, systems are able to do simple object detection for only surveillance and no market solution is offering face access control in home space. In the recent years, more number of solutions relied on cloud services than on edge computing platforms which have seen their entry only recently. Cloud services are unable to deliver low latency. Most systems which are able to offer good speed and accuracy have never been em- 3 ployed in home security space. The most sophisticated large scale surveillance systems to do recognition are employed to monitor road traffic and public spaces. Like any other software, AI powered systems are prone to attacks by using AI powered attacks. Images looking very similar to each other but having differences in pixels can be used to create GAN based attacks. This could cause even a high accuracy system to misclassify an otherwise authorized person. This can be tackled by performing adversarial training on the algorithm using hard negative examples. The security of smart homes can be compromised very easily by means of D.D.o.S, P.D.o.S and device hijacking attacks. The identity theft of a person allows an intruder to bypass a system. This can be solved by multi factor authentication.The tampering of the system can be detected. If the above challenges are not addressed then, there could be catastrophic consequences including threat to lives of the inhabitants.

8.NEED OF THE 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 (vibration) is there, when the door or window is moved and an alert signal in case of any emergency.

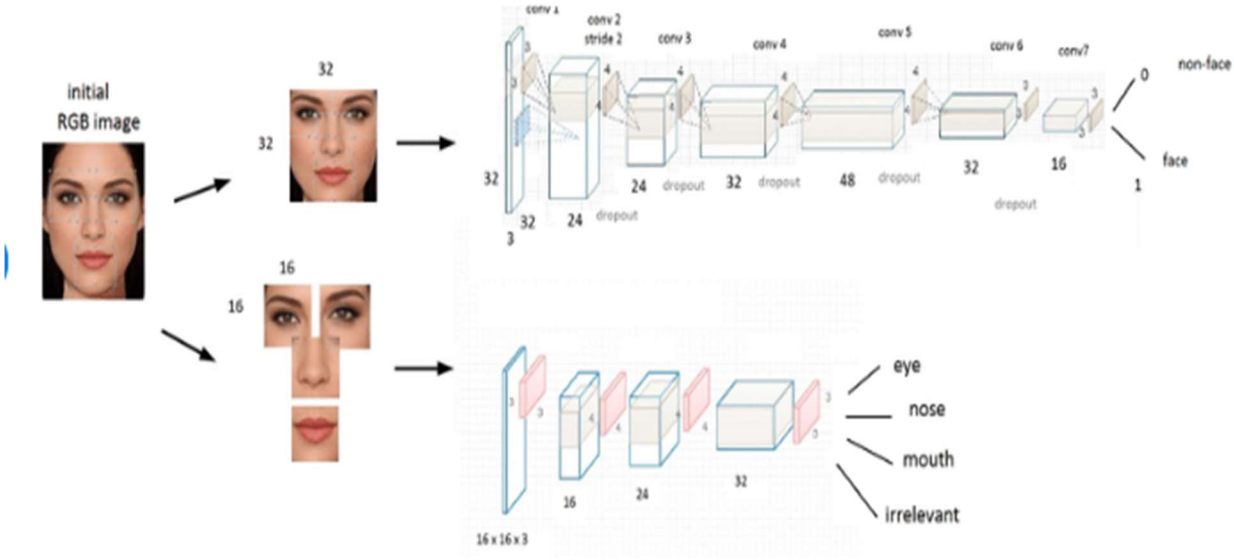
9.ALGORITHMS USED :

There are different types of algorithms which can be used for Face Recognition that are PCA (Principal Component Analysis), LDA (Linear Discriminant Analysis), ICA (Independent Component Analysis), EBGM (Elastic Bunch Graph Matching), Fisherfaces.

The most common type of machine learning algorithm used for facial recognition is a deep learning Convolutional Neural Network (CNN). CNNs are a type of artificial neural network that are well-suited for image classification tasks.

CNNs learn to extract features from images and use those features to classify the images into different categories. The depth of a CNN is important for facial recognition because it allows the CNN to learn more complex facial features.

9.1. An example of a convolutional neural network architecture



The 3 steps of facial recognition

Face recognition is divided into three steps:

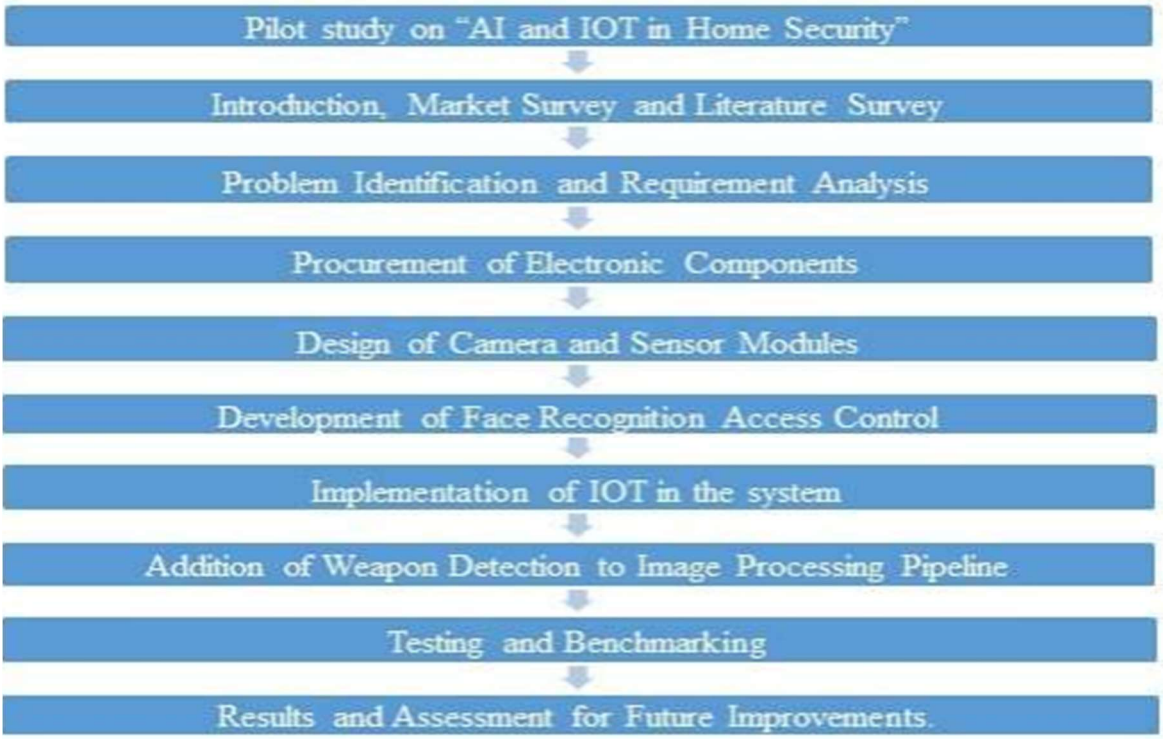
1. **Face Alignment and Detection** – The first step is to detect faces in the input image. This can be done using a Haar Cascade classifier, which is a type of machine learning algorithm that is trained on positive and negative images. The machine must locate the face in an image or video. By now, most cameras have an in-built face detection function. Face detection is also what Snapchat, Facebook and other social media platforms use to allow users to add effects to the photos and videos that they take with their apps.

   A challenge in the context of face detection is that often the face is not directed frontally to the camera. Faces that are turned away from the focal point look totally different to a computer. One way to accomplish this is by using multiple generic facial landmarks. For example, the bottom of the chin, the top of the nose, the outsides of the eyes, various points around the eyes and mouth, etc. A machine learning algorithm needs to be trained to find these points on any face and turn the face towards the center.

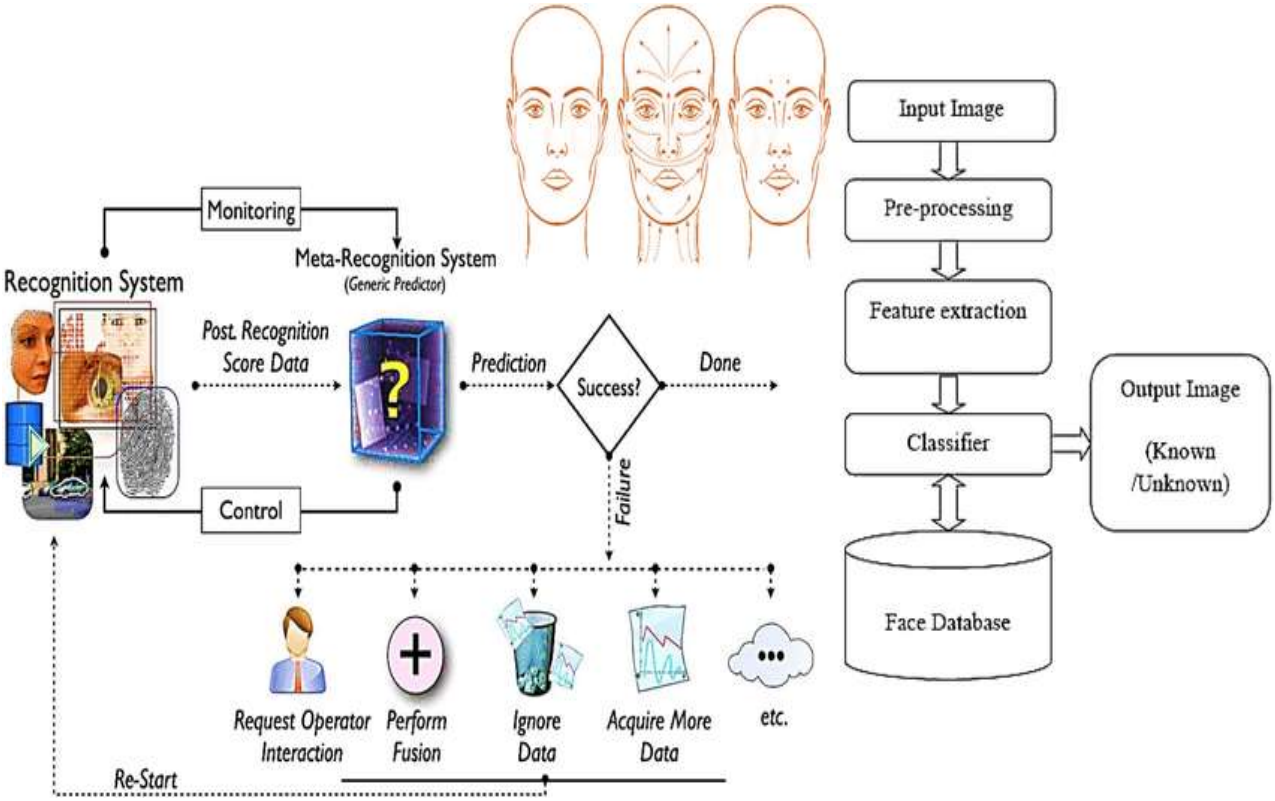
2. **Feature Measurement and Extraction** – Once faces have been aligned and detected, the next step is to extract features from them. This is where the Convolutional Neural Network (CNN) comes in. A CNN is able to extract high-level features from an image, which are then used to identify faces in a database.

3. **Face Recognition** – The last step is to match the extracted features with faces in a database. This is usually done using a Euclidean distance metric, which measures the similarity between two vectors.

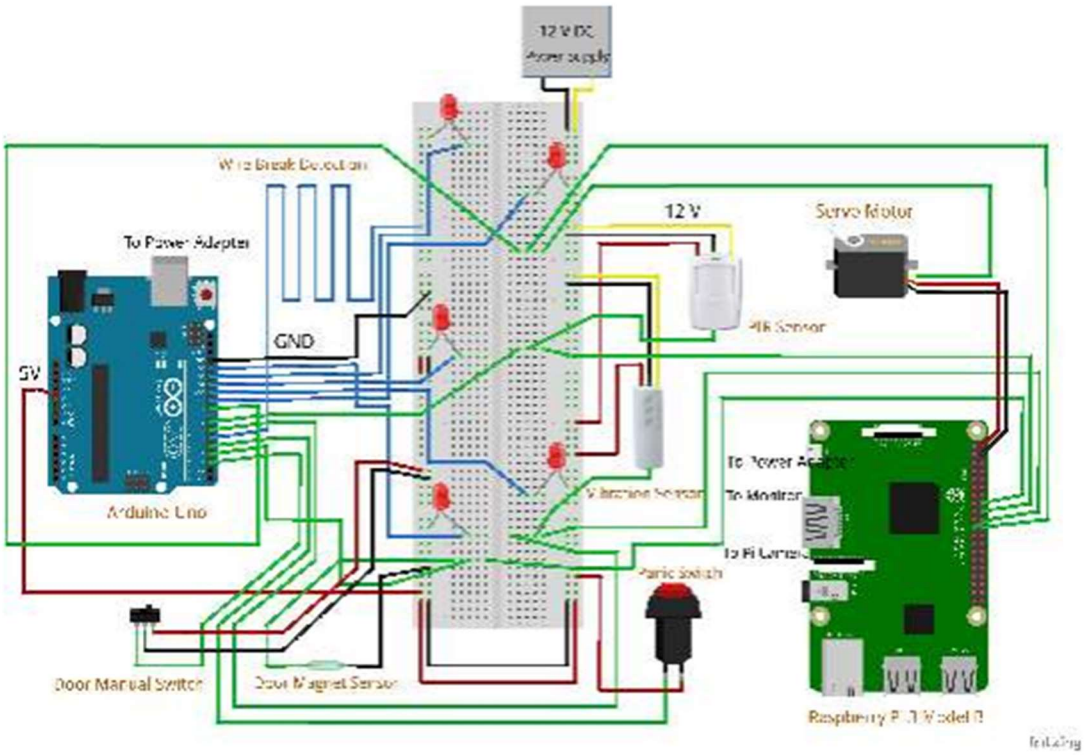
10. METHOLOGY :



11. ARCHETECTURE DIAGRAM :



12. CIRCUIT DIAGRAM :



13. REQUIREMENTS AND SPECIFICATIONS :

13.1.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.

The Python Programming Language :

Python was developed by Guido van Rossum in the early 1990s. It has a lot of advantages over other object-oriented programming languages like C++ and Java.

Raspbian OS :

Raspberry Pi uses a Debian-based operating system. The project uses Raspbian Stretch among other options like Ubuntu MATE and Windows 10 IOT Core as it is the native OS and more stable. The OS highly suited for the Raspberry PiâA˘ Z´s lowperformance ARM CPUs. The user interface supports GUI with Python pre-installed. It is oriented to help users who do not use Linux for development. The file system, networking, process handling and access to peripherals using Linux kernel.

OpenCV Library :

OpenCV (Open Source Computer Vision Library) is an image processing library made by Willow Garage of Intel. It was built for real-time computer vision applications. It was designed for efficient computation. It is written in C/C++ and can take advantage of multi-core processing

13.2.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.

PIR Sensor :

PIR sensor (Passive Infrared) sensor measures the change in temperature when an object radiating heat (human in this case) passes in front of it. It is a passive sensor which means it can only read the values.

Raspberry Pi 3 Model B Development Board :

The Raspberry Pi is a small single-board computer used in many other applications such as robotics, image processing, security systems, etc

Hikvision Network Camera (Wired) :

The Hikvision Network Dome Camera is a 1.3 Megapixel Dome shaped, CMOS based Vandal-proof camera. It is used for surveillance and video data is stored using DVR or NVR. It has support for IR for a range of approx. 10 to 30 metres. It also features intrusion and motion detection. It is powered via PoE using a network switch.

14. CONCLUSION AND FUTURE SCOPE :

14.1. 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. This project clearly shows how state-of-the-art methods can be used even with limitations on hardware. The design of the system for achieving the âA˘Ÿsweet spotâA˘ Z´ between speed and performance is an iterative process. 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. The primary advantage of it is that it helps avoid expenditure on any physical components, thus reducing costs significantly. However, it is an experimental feature which cannot be incorporated into a single model alongside face recognition. 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 and forms an essential avenue for building smart cities. The system can be further used in other industrial areas such as logistics, schools and ATM facilities for improving security. This will reduce the amount of time taken to identify threats to the buildings where the system is employed

14.2. FUTURE SCOPE :

Even though, the final design was found as satisfactory, it was realized there is always scope for improvement. The system is not entirely break-proof in spite of providing fail-safe method.

Some of the aspects worth noting for future improvements are as follows-

- Liveness Detection System: During the process of development of Face Recognition system, it was observed that the system can be spoofed by using a photo of the owner for access. Hence, a liveness detection system was incorporated during the testing of the system. The system is able to distinguish faces as valid or invalid based on the whether the captured face is from a phone or the person himself. However, the disadvantage of the systemwas that it doesnâA˘ Z´ t generalise well on all faces. Actual methods also include detection eyes blinking, motion sensing, how pixels change and 3D depth sensing. Depth sensing required cameras with depth sensors for determining if the face is a 2D image or a 3D solid object. Due to lack of suitable hardware and low recall of the method, it was discarded in the final design of the system. Nonetheless, it forms a crucial part in improving the system.
- Non-Frontal Face Detection: Only front faces were detected in the final model. The alternative model using DeepFace could allow for non-frontal faces as well. The descriptor of the current model can be combined with it to achieve recognition of non-frontal faces with very low latency.
- System Performance: The lower performance of the system can be compensated by using dedicated GPUs present in embedded platforms like Nvidia Jetson boards and Google Coral TPU board.
- Camera Tampering Detection: It can be created by using image processing and predicting by rate at which frames change.

15. CODING /PROGRAM PART :

Before Executing the code we need to install :

❖ OpenCV:

OpenCV (Open Source Computer Vision Library) is a widely used library for computer vision tasks, including face detection. Install OpenCV using the following command:

pip install opencv-python

❖ NumPy:

NumPy is a fundamental package for scientific computing in Python. It provides support for multi-dimensional arrays and mathematical operations on arrays. OpenCV depends on NumPy for handling image data efficiently. Install NumPy using the following command:

pip install numpy

Face detection.py :

```
import cv2
import numpy as np
import dlib

# Load the pre-trained face detection model
face_detector = dlib.get_frontal_face_detector()

# Load the pre-trained face recognition model
```

```
face_recognizer = dlib.face_recognition_model_v1("shape_predictor_68_face_landmarks.dat")

# Load the input image
image = cv2.imread('input_image.jpg')

# Convert the image to grayscale
gray = cv2.cvtColor(image, cv2.COLOR_BGR2GRAY)

# Detect faces in the image
faces = face_detector(gray)

# Iterate over detected faces
for face in faces:
    # Get the facial landmarks
    landmarks = face_recognizer.predictor(gray, face)

    # Perform face recognition on the face
    # (Here, you would typically compare the face features with a database of known faces)
    # For demonstration purposes, we'll simply draw a rectangle around the face
    x, y, w, h = face.left(), face.top(), face.width(), face.height()
    cv2.rectangle(image, (x, y), (x + w, y + h), (0, 255, 0), 2)

# Display the image with face detection results
cv2.imshow('Face Recognition', image)
cv2.waitKey(0)
cv2.destroyAllWindows()
```

In this code:

1.The **cv2.CascadeClassifier** class is used to load the pre-trained face detection model. The path to the **haarcascade_frontalface_default.xml** file is provided to specify the Haar cascade classifier for face detection.

2.The input image is loaded using **cv2.imread()** and stored in the **image** variable.

3.The image is converted to grayscale using **cv2.cvtColor()**.

4.The **detectMultiScale()** function is used to perform face detection on the grayscale image. The function takes several parameters, such as **scaleFactor**, **minNeighbors**, and **minSize**, which can be adjusted to control the sensitivity and accuracy of the face detection.

5.The detected faces are stored in the **faces** variable as rectangles, where each rectangle represents the coordinates (x, y, width, height) of a detected face.

6.The code then iterates over the detected faces and draws green rectangles around them using the **cv2.rectangle()** function.

7.Finally, the image with the face detection results is displayed using **cv2.imshow()**. The program waits for a key press (**cv2.waitKey(0)**) and then closes the window (**cv2.destroyAllWindows()**).

weapon_detection.py :

```
import cv2


# Load the pre-trained weapon detection model

weapon_cascade = cv2.CascadeClassifier('weapon_cascade.xml')


# Load the input video
```

```
video = cv2.VideoCapture('input_video.mp4')


# Loop over frames in the video
while video.isOpened():
    # Read the current frame
    ret, frame = video.read()


    # Break if no frame is captured
    if not ret:
        break


    # Convert the frame to grayscale
    gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)


    # Perform weapon detection
    weapons = weapon_cascade.detectMultiScale(gray, scaleFactor=1.1,
minNeighbors=5, minSize=(30, 30))


    # Draw rectangles around the detected weapons
    for (x, y, w, h) in weapons:
        cv2.rectangle(frame, (x, y), (x+w, y+h), (0, 0, 255), 2)


    # Display the frame with weapon detection results
```

```
    cv2.imshow('Weapon Detection', frame)

    # Break if 'q' key is pressed
    if cv2.waitKey(1) & 0xFF == ord('q'):
        break

# Release the video capture and close the window
video.release()
cv2.destroyAllWindows()
```

16. REFERENCES

- ✓ Dubal, P., Mahadev, R., Kothawade, S., Dargan, K., and Iyer, R. (2018). "Deployment of customized deep learning based video analytics on surveillance cameras." arXiv preprint arXiv:1805.10604.
- ✓ Hinton, G. E., Osindero, S., and Teh, Y.-W. (2006). "A fast learning algorithm for deep belief nets." Neural computation, 18(7), 1527–1554.
- ✓ Kazemi, V. and Sullivan, J. (2014). "One millisecond face alignment with an ensemble of regression trees." Proceedings of the IEEE conference on computer vision and pattern recognition. 1867–1874.
- ✓ Lin, T.-Y., Goyal, P., Girshick, R., He, K., and Dollár, P. (2017). "Focal loss for dense object detection." Proceedings of the IEEE international conference on computer vision. 2980–2988.
- ✓ Liu, W., Anguelov, D., Erhan, D., Szegedy, C., Reed, S., Fu, C.-Y., and Berg, A. C. (2016). "Ssd: Single shot multibox detector." European conference on computer vision, Springer. 21–37.
- ✓ Mao, J., Lin, Q., and Bian, J. (2018). "Application of learning algorithms in smart home iot system security." Mathematical Foundations of Computing, 1(1), 63–76.
- ✓ Parkhi, O. M., Vedaldi, A., Zisserman, A., et al. (2015). "Deep face recognition.." bmvc, Vol. 1. 6.
- ✓ Schroff, F., Kalenichenko, D., and Philbin, J. (2015). "Facenet: A unified embedding for face recognition and clustering." Proceedings of the IEEE conference on computer vision and pattern recognition. 815–823.
- ✓ Wen, Y., Zhang, K., Li, Z., and Qiao, Y. (2016). "A discriminative feature learning approach for deep face recognition." European conference on computer vision, Springer. 499–515.