ENHANCED FACE DETECTION USING COST EFFECTIVE HOME AUTOMATION

Nagaraj Doddam[1*], EN. Ganesh[2]

Article History: Received: 12.12.2022 **Revised:** 29.01.2023 **Accepted:** 15.03.2023

Abstract

Advancement in IoT based application has become the cutting edge innovation among the researcher due to the accessibility of Internet all over. In order to make the application user friendly, many new age technologies, web based and android based technologies have acquired their significance in this cutting edge technology. In recent years, the world has seen a lot of progress in automated home systems. The existing home automation systems are basic: turning switches on/off, etc. over the Internet. But this leaves a lot to be desired in the Home Security department. While there are systems that let you view your security camera feed, this is highly time consuming and counter-productive. There are numerous electrical equipment's available in market which could be integrated together to create a robust solution which will address the security gaps and provide automation at finger tips. The currently available Home automation systems are very expensive and not within the reach of common man. This paper helps in providing cost effective robust Home Security automation using Raspberry. It also helps in energy conservation and empowering user to control using smart phone. Thus, main objective of this work is to make our home much secure along with energy conservation

Keywords: Face Detection, Haar Classifier

[1*]Department of Computer Science, Vels University Chennai India
[2]Department of Computer Science, Dean, Vels University Chennai India

Email: [1*]rajureddy10@gmail.com

DOI: 10.31838/ecb/2023.12.s3.241

1. Introduction

Human-Machine Interaction (HMI) has turned into the more realistic in everyday life because of the advancement in the technology. Today, HMI research has moved one step ahead and exchanged onto the Internet, which was previously utilized for correspondence and presently utilized for IoT (Internet of Things). IoT applications are not restricted to one specific field. It has shown the huge commitment from small scale applications to the enormous scope applications, for example, E-trade, Coal Mine, Wearable gadget, Smart Grid, Laboratory Monitoring, Agriculture and many different areas.

Home automation allows us to focus on getting our work done without worrying about the safety and security of our home, while enabling us to control the appliances in our home on the go. All of our devices and appliances are networked together to provide us with a seamless control over all aspects of our home and more. Home automation has been around from many decades in terms of lighting and simple appliance control, and only recently has technology caught up for the idea of the interconnected world, allowing full control of your home from anywhere, to become a reality. With home automation, you dictate how a device should react, when it should react, and why it should react. Home automation is a necessity these days as it helps save up on power consumption, makes our homes more secure, provides a way to monitor our home when we are away, and makes our home secure in every way possible.

Home Security and Home automation are often overlooked and least addressed when compared to the technological advancements in the world. Smartphones are widely available for every common man, but Smart homes concept is still under developed and is far from the reach of the common man.

A Home can be considered as a Smart Home only when it is equipped with right gadgets and is able to operate, communicate with each other smart devices and fulfill the common human needs with minimal human interference. With the current Covid situation most of the urban homes are equipped with WiFi technology. Leveraging the existing WiFi network power and adding few smart devices in the home network can not only enhance the security, but will also help in monitoring and controlling the same using Smartphones.

The general daily needs of a common man are Safety, Security and intelligent Smart devices which can help in saving energy and empowering the user to have greater control by click of a button. Automated Home Security can be designed using Smart Locks for main door, surveillance Camera and sensors to control the various needs of the common man. Experts predict that there is going to be an exponential increase in Internet of Things (IoT) devices in the next couple of years. The IoT helps in connecting the various Smart devices and helps in providing access to specific data required for intelligent decision making. Raspberry Pi is a mini computer which enables smoother communication with smart devices and connecting the same with Internet for greater efficiency and control. This Home automation will enhance the security with high latency and low cost. The key objective of this paper is to develop Home Security and Home enhance automation using Raspberry Pi minicomputer through IoT and provide monitoring and controlling capability to the common man using simple application in Smartphone.

Accordingly, saving of the power is the principal concern, which is the essential point of this paper. To save the power consumption, we have proposed the efficient, energy effective home automation framework utilizing IoT. Hence, point of this exploration to save the power utilization and simultaneously give the wellbeing and security of the home appliances. This paper is divided into six sections. Section I gives the basic idea of the system. Section II describes the existing system and its Gaps. Section III describes the proposed system. Section IV describes about the Hardware used. Section V describes the experimental results and Section six is conclusion..

Exsisting System

In one of the existing papers a ZigBee module was embedded in digital door lock and the door lock acts as a central main controller of the overall home automation system [1].

In another paper based on embedded system Aurdino microcontroller is use for home security. The system was operating using cellular phone with the help of GSM technology [2].

In one of the existing paper advanced alert home security system with Fingerprint and Password authentication to open or close the door system and also sending the message if any miss operation will be performed by others using GSM Technology with smart mobile [3].

In another paper a door locking system is proposed which makes the locking or unlocking of a door more reliable to the user than the conventional system. This paper uses Short messaging service to operate the main door from any part of the world [4].

In one of the paper various types of sensors such as PIR motion sensor, Gas Leakage sensor and Fire Sensor to detect the change in surrounding of the home and notify the user by sending an SMS via GSM module [5].

In another paper a home automation and home security technique. The sensors were integrated using Arduino. The status of our home appliances will get uploaded to a cloud platform through wireless module. The sensors were able to enable or disable the sensors which will be in control of the user. The gestures of our fingers to control the appliances were achieved using Flex sensor [6].

In one of the papers A Wi-Fi based Home security system which alerts the owner using a PIR module which constantly monitors the Home. ESP8266 Wi-Fi module is used to control the security system from the user's mobile phone with a potential internet connection [7].

In another paper the proposed system design is based on a microcontroller device Arduino. It was used to develop both stand-alone interactive objects, or can operate efficiently with software co-design [8].

In one of the paper build for monitoring the unauthorized in the home using raspberry pi 3 model. The Raspberry pi foundation uses the python language for coding. It is made of software called New out of box software which is easier to installing an operating system [9] .

In another paper it has been mentioned that everything around us is getting smarter with whole new world of technology called smart device that has changed the way we interact in our daily lives. Smart Devices comprise of both high-end and low-end devices with respect to software and hardware platform [10].

In another paper it has been mentioned that Internet of things (IOT) paradigm is changing day to day lives towards sophisticated automation and enhancing living standards of our societies. Therefore data is collected, manipulated and stored in the clouds [11] ..

Exsisting Architecture

The existing Home automation architectures available in the market today are:

A. Bluetooth Based Home automation: It is cheap and secure. It has a low range (10 to 100 meters). It uses 2.4GHz bandwidth and the speed can be up to 3Mbps. The key drawbacks are its low range, the fact that it takes a long time to discover and connect to devices, and that real time access is not possible using Bluetooth. [12]

B. Phone based Home automation:

In this, the system can be accessible from anywhere with a telephone line. It doesn't provide Real time control. It is fast, but because DTMF has only 12 frequencies, maximum of 12 devices can only be controlled. Two phones are required: one to which the circuit is connected, and the other from which the call is to be made [13].

C. ZigBee based Home automation:

ZigBee based architecture provides high security because of end-to-end encryption. It uses two microcontrollers- one on the transmitter side, another on receiver side. It has a low range and isn't that fast. [14] [15] [16]

D. Wireless based Home automation:

In this architecture, IoT and Wi-Fi are used to communicate between the controller and the devices. Several devices can be connected using multiple networking techniques. It also provides the added benefit of providing speech based command support. [17] [18] [19]

E. Existing IoT based Home automation:

These use internet servers to communicate between controller and devices. If there is a server overload, or if the server crashes, the system can be rendered useless. Therefore, there is a need to overcome this problem. [20] [21]

As we can see, the existing home automation architectures have something or the other working against them, making them either unreliable, or limited in some way. Therefore, there is a need to address these issues in order to make a stable, more expansive home automation system that can be used by everyone in their homes. [22]

Proposed System

As demand for power is expanding day-by-day, therefore, smart home is the impending area of exploration to provide the remote access for controlling the home appliance using IoT. This permits the client to control the home automation gadget, for example, fan, bulb and so on, without even making any actual association. [23] [24]

In this paper we are proposing Home Security and Home Automation using Raspberry Pi and Internet of Things with full control using Smart Android Application. The Smart Application developed will allow the owner to view live video of the guest at the door and remotely authorize to unlock the main door to allow the guest to enter the main door by controlling through Smart Android Application from anywhere in the world. [25]

The Smart Application will also be enabled to control the key components in the house like AC, Lights, Fan and Electrical Water Motor Switch along with user defined timer. The Smart application will be enabled to display the status of the current components in the smart Home and provide frequent notifications to the owner.

Smart Application will also address energy savings and conserving natural resources by prompting the user on the water level in Sump and overhead water level indicator and raise alarm in case of over flow.

The Smart Home features in this paper are broadly classified into three main areas 1. Main Security Enhancement 2. Smart Accessibility & Protection 3. Energy Savings Automation

The proposed system architecture uses a Raspberry Pi (microprocessor) as the core of the system. The

Pi is a tiny computer about the size of a credit-card, and it features a processor, RAM and all the important hardware ports that can be found in a computer. Then there is also a iOS-based Mobile application with a User Interface to control the device in specific rooms of the home. Along with this, a PIR sensor is used, which is linked to a PiCamera (an 8MP camera). This is then linked to the Facebook account of the user to provide an accurate identification of the person who has triggered the sensor, provided the user has them on their friends' list.

Relays are used instead of normal switches as they can be triggered with a low voltage change. A temperature and humidity sensor is also used to measure and communicate the readings of the home to the user's mobile application directly. Raspberry Pi, cloud server and the mobile app are connected using lower latency network which is called Pubnub network. Pubnub is a secure global Data Stream Network (DSN) and easy to use API that enables its customers to connect, scale, and manage real time applications and IoT devices. Raspberry Pi controls all the IOT devices and gets the input from the cameras and sensors and processes them for real time communication.

A. Main Security Enhancements

The Smart home Security enhancement includes setting up digital smart lock to main door which controllable using Smart Phone Application. The Keyless door unlock will help the owner to unlock the door using either through fingerprint or through smart phone unlock. When the guest presses the bell switch at the main door, the camera will be activated and alert call will be triggered to the owner prompting the owner to take necessary action. The owner can view the video of the person at the main door using the smart application, and will be able to unlock the smart door lock allowing the guest to come in. The Figure 1. Showcases the Proposed Architecture of the system

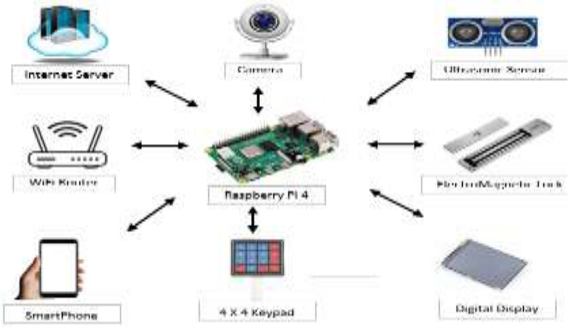


Fig 1. Proposed Architecture of the System

B. Smart Accessibility & Protection

Smart Home accessibility empowers the user to control key appliances using mobile application. With click of the button on the android application, the user is able to control the fan light and other key appliances in the house.

C. Energy Saving Automation

Smart Homes are not just automating the daily activities, but also will focus in conserving the natural resources and saving the power consumption by intelligent decision making. Gadgets are strategically placed in the house to enhance the security and automation feasibility

Hardware Used

The Hardware used for this paper are as follows 1. Raspberry Pi3, 2. Electro Magnetic Lock, 3. PIR Motion Sensor 4. Door Open Sensor 5. Fire Sensor 6. Ultra-sonic Distance Sensor 7. Finger Print Sensor 8. Smart Phone.

D. Raspberry Pi

Raspberry Pi 3 is a single board computer which is in the size of the debit card with 1.2GHz working on Linux Operating system, it has 64-bit quad core CORTEX processor with built in wifi. It has internal memory of 1GB. This Raspberry pi consists of I/O, CPU, Ethernet, 2x USB Hub, HDMI Port, audio Jack and memory slots. The version of Raspberry Pi is best suited for this project as it meets the requirement of the project

E. Electro Magnetic Lock

Electro Magnetic lock consists of Electro magnet an armature plate. This needs to be fixed to the main door. It becomes magnetized when electric current passes through that. This magnetic field secures the door and electronically controls the door when locked and unlocked.

F. PIR Motion Sensor

PIR is the Passive Infra-Red Motion Sensor which detects the motion. The PIR Motion Sensors are placed in strategical point in the house. When the door is locked and if there is any motion is identified in the house, a trigger is initiated to the owner Smart Phone through the Raspberry Pi.

G. Door Open Sensor

The Magnetic Door Sensors MC 38 needs to be placed in strategic areas in the house to provide regular alerts to the owner. The most critical area in the house is the area of the safety locker which will hold the expensive items in the house. But often this area is ignored with mere belief of Lock and Key.

The Locks can be easily broken and valuables can be stolen and can lead to great loses. A simple door sensor in the Safety locker connected to the Raspberry can alert the owner with message every time the locker is accessed. This will give full control to the owner and protect the house from Thefts

H. Fire Sensor

Fire Sensor (MQ2) needs to be placed in most critical fire prone zones in the house. This will help in detecting smoke and high temperatures and send immediate alerts to Raspberry microcontroller, which in turn alerts the owner with a message to take the mitigation actions. This will protect the damages from fire by taking timely mitigation actions

I. Ultrasonic Distance Sensor

The Ultra Sonic Distance sensor HCSR04 is used to measure the water level in the overhead tanks. The Water in the overhead tanks are filled daily and often there is wastage of water and electricity. This is often caused by negligence to switch off the water motor. This Ultra Sonic Distance sensor HCSR04 is fit above the overhead tank to measure the level of water. When the water reaches the overflow level, the Ultra sonic distance sensor sends immediate alerts to Raspberry microcontroller, which in turn alerts the owner with a message to tale actions by switching off the water motor.

J. Finger Print Sensor

Finger Print sensor is used at the main door to authorize the people to enter the house. Key less unlock is made possible by using the Finger Print Sensor. The residents of the house can have their finger print captured as one time set up initially and subsequently will enable the authorize the residents using key less unlock of the main door.

K. Smart Phone

Smart Phone is a common device which is available to everyone. The complete control of the user is enabled using the smartphone. The smart phone enables the user to open the main door lock, control the electrical devices in the network, and check the alert messages from the microcontroller to take necessary actions. The Raspberry microcontroller constantly keeps posting the alerts and information to the user through the smartphone. All the devices connected to the Raspberry can be controlled using the smartphone

The Blynk android application is used to connect the Smartphone with the Raspberry Pi. The various control features required for this project are created in Blynk applications and is configured to send the signals to the Raspberry pi microcontroller.

Raspberry PI requires Linux operating system to be enabled on the computer, once the Linux operating system is installed, Raspberry Pi could be easily controller from the home page. Raspbian\Noobs Operating system is installed on to the Raspberry Pi microcontroller. All the devices specified in section 3.1 is connected to Raspberry Pi. The C++ \ Python programing Language is used to control the devices connected to the microcontroller. All devices are connected to the GPIO Pins in the Raspberry PI

The Raspberry Pi Camera, Finger Print Sensor and Matrix Keyboard is installed in the outdoor unit and is connected to the microcontroller placed inside the house. The Electromagnetic Door lock is installed in the main door and the electrical circuit is connected to the microcontroller. The Door sensor is connected to the locker door and the connection is made to the Raspberry Pi. The PIR Motion sensor and the Fire sensor is placed in strategic places in the house and is then connected to the micro controller

The Ultra Sonic Distance sensor is connected to the overhead water tank and the sump. The Ultrasonic distance sensor output line is connected to the Raspberry Pi Microcontroller. The Ultra sonic Distance sensor measures the level of water and sends the alert message to the Raspberry pi when the water level in the Tank is full. The Raspberry Pi will send the alert message to the smartphone for the owner to take the necessary action

Working Model

A. PIR sensor and PiCamera:

Having a camera monitor the home 24x7 can be really expensive, considering the storage and power consumption. This can be overcome by using the PIR sensor as a trigger to start running the camera. When there is a visitor at the door, the PIR sensor detects the movement. If there is movement for a specific amount of time (say, 2-3 secs), the PIR sensor triggers the PiCamera, which then takes a photo of the visitor and sends it to the owner of the home. This helps the owner monitor what is going on around his/her home without spending a fortune on the storage and power consumption.

B. The Temperature and Humidity sensor:

When triggered, the temperature and humidity sensor record the temperature and humidity in their location for a specified number of times (say, 10 times), since the readings might not be accurate on the first try. The system is then programmed to take a mode of the readings, which is, isolate the reading occurring the highest number of times and sending it to the user.

C. Face recognition using machine learning

In our project, we'll be using Facial recognition that is linked with the Facebook account of the user, in order to provide access to people whom the user is acquainted with, and thereby eliminating the need for duplicate keys.

Nowadays, we can see that Facebook automatically recognizes the faces of our friends whenever we post any photo. With almost 98% accuracy, it is probably as good as any human. Merely recognizing faces is easy in terms of today's technological prowess. But the challenge lies in distinguishing between similar looking people, like sibling or direct relatives.

But before tackling that, we need to look at how face recognition actually works.

- Firstly, finding all the faces in the picture.
- Secondly, making sure that the machine recognizes a face as that of the same person, even if it is turned in a weird direction, or is in bad lighting.
- Thirdly, picking out the unique features of the face, like size of eyes, shape of the face, etc, to tell the person apart from other people.
- Lastly, comparing the unique features of that face to all the people we already know to determine the person's name.

Our brain is hardwired to do all this subconsciously and instantly. But computers aren't able to do such computations. So each step has to be considered a problem, and then be solved. A *pipeline* is required to solve each of these steps, and to pass the result to the next step. Hence, the following steps are followed:

1. Finding all the faces- First, the image is made black and white, as color data is not needed to find faces. Next, every pixel is scrutinized by looking at the pixels surrounding it. This is done to figure out the comparative darkness of the pixel when compared with its surrounding pixels. An arrow is used to show the direction in which the image is getting darker. This process is repeated for every pixel in the image.

Figure.4 sample image (black and white)

Figure.5 analyzing pixels and replacing them with white arrows

These arrows signify the gradients in an image, showing the flow from light to dark in the image. This is done so that difference in lighting of the image doesn't hinder the facial recognition. Thus, dark and light images will end up with the exact same representation.

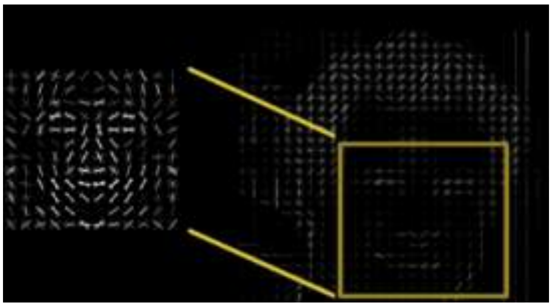
Figure.6 the eye before and after being replaced by arrows

Since this is way too much data to be stored, the image is divided into 16x16 square pixels. Each square is then replaced with an arrow pointing in the direction that occurred the most in it. This leaves us with a very simple representation that captures the basic face structure. The idea is to reduce the entire data acquired through the scanning and reading of the face into data that the computer can easily analyze in a short period of time to reduce the computation delay.

Figure.7 the upper half of the face as an HOG Image

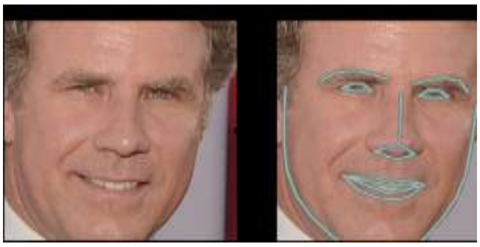
This is a Histogram of oriented Gradients image, or HOG image. By generating many HOG images of the same person, a HOG pattern can be derived, which can be used to correlate with the face that is to be detected and thereby recognizing it.

Figure.8 The HOG Image received by analyzing multiple images of the same Person.

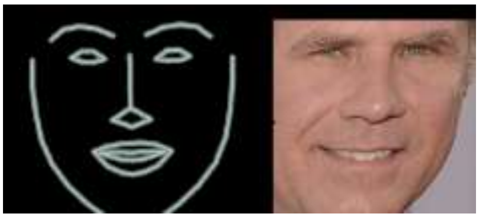


2. Faces turned in different directions- To overcome this, we need to represent the face in such a way that the eyes and lips are always in the same place in the image, thereby making comparing of faces easier. This is done by Face Landmark Estimation (invented by Vahid Kazemi and Josephine Sullivan in 2014). What this does is it comes up with 68 specific points (or landmarks) that occur on every face, like the edge of the lips, or the tip or the nose, etc. Then the machine is trained to find these points on the face of any person. This gives us the exact location of the eyes and mouth, enabling us to rotate, scale and shear the image so that these are as centered as possible. What this does is it gives all the pictures of any given person a specific orientation. So, whatever the pose of the person is in that image, the face can still be easily recognized as the basic features will always be positioned in the same manner. This is a necessary step, as the computer cannot process faces like humans do. It needs data to be presented in a way that it understands and can analyze easily. Since a large delay in recognizing the face is counter-productive, it is mandatory that the image be presented in as simple a data as possible for the computer to easily process it in a minimal amount of time

Figure.9 The basic 68 Landmarks that can be found on any given face.



(a) (b)



(c) (d)

Figure.10 (a) Face area detected in image. (b) Face landmarks detected. (c) Perfectly centered result that's wanted. (d) Face transformation to be as perfectly centered as possible.

3. Distinguishing faces- Rather than always going through old images of the same person to compare with the given image to come up with a match, which is both time consuming and counter-productive, a method needs to be used to recognize faces in the blink of an eye.

For this, some measurements of each face have to be extracted. Then, the unknown face can be measured in the same way, and the known face with the closest measurements can be found. The extraction of themeasurements have to be done by the computer on its own. This is done using Deep Convolution Neural Network. This will be used to train the system to generate 128 measurements for each face.

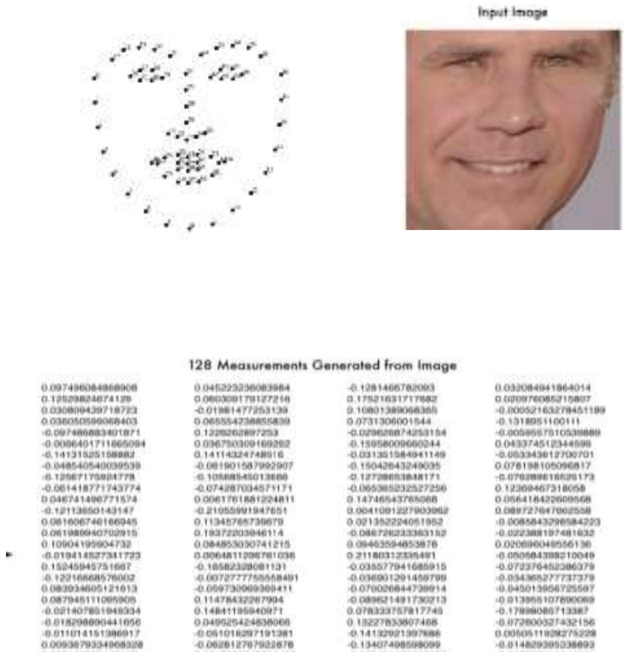
This works as follows:

1. Take the training image of known person.
2. Take another picture of same person.
3. Take the picture of different person.

Then, the algorithm tweaks the neural network to make sure that the measurements for #1 and #2 are closer and that of #2 and #3 are slightly different. This machine learning of the 128 measurements of each face is known as an Embedding. It helps break down complicated data like images into a series of computer generated numbers.

The next step is to train the neural network to output a face embedding. This is time consuming and requires a lot of computing power and data. But it can generate measurements of any face once it has been trained. This training is a one-time thing. Then we can run any face through the trained network and the 128 measurements are generated.

We don't really know what measurements are being generated, but the fact that the neural network gives us nearly the same numbers for different images of the same person tells us that it is pretty accurate.



128 Measurements Generated from Image

0.097496084868908
0.12529824674129
0.030809439718723
0.036050599068403
-0.097486883401871
-0.0066401711665094
-0.14131525158882
-0.048540540039539
-0.12567175924778
-0.061418771743774
0.046741496771574
-0.12113650143147
0.061606746166945
0.061989940702915
0.10904195904732
-0.019414527341723
0.15245945751667
-0.12216668576002
0.083934605121613
0.087945111095905
-0.021407851949334
-0.018298890441656
-0.011014151386917
0.0093679334968328
0.058139257133007
-0.024210374802351
-0.057223934680223
0.023535015061498
-0.0098039731383324
0.020220354199409
0.0040337680839002
0.051597066223621

0.045223236083984
0.060309179127216
-0.01981477253139
0.065554238855839
0.1226262897253
0.036750309169292
0.14114324748516
-0.061901587992907
-0.10568545013666
-0.074287034571171
0.0061761881224811
-0.21055991947651
0.11345765739679
0.19372203946114
0.084853030741215
0.0064811296761036
-0.16582328081131
-0.0072777755558491
-0.059730969369411
0.11478432267904
0.14841195940971
0.049525424838066
-0.051016297191381
-0.062812767922878
0.0048638740554452
-0.11443792283535
0.014683869667351
-0.081752359867096
0.037022035568953
0.12788131833076
-0.094398014247417
-0.10034311562777

-0.1281466782093
0.17521631717682
0.10801389068365
0.0731306001544
-0.029626874253154
-0.15958009660244
-0.031351584941149
-0.15042643249035
-0.12728653848171
-0.065365232527256
0.14746543765068
0.0041091227903962
0.021352224051952
-0.086726233363152
0.09463594853878
0.21180312335491
-0.035577941685915
-0.036901291459799
-0.070026844739914
-0.089621491730213
0.078333757817745
0.13227833807468
-0.14132921397686
-0.13407498598099
-0.039491076022387
0.071997955441475
0.05228154733777
-0.031709920614958
0.11009479314089
0.18632389605045
-0.11768248677254
-0.040977258235216

0.032084941864014
0.020976085215807
-0.00052163278451189
-0.1318951100111
-0.0059557510539889
0.043374512344599
-0.053343612700701
0.078198105096817
-0.076289616525173
0.12369467318058
0.056418422609568
0.089727647602558
-0.0085843298584223
-0.022388197481632
0.020696049556136
-0.050584398210049
-0.072376452386379
-0.034365277737379
-0.045013956725597
-0.013955107890069
-0.17898085713387
-0.072600327432156
0.0050511928275228
-0.014829395338893
-0.043765489012003
-0.012062266469002
0.012774495407939
0.069833360612392
0.11638788878918
-0.015336792916059
0.10281457751989
-0.082041338086128

Figure.11 Input image, and the 128 measurements that are generated.

4. Finding the name of the person from the Encoding**:** For this, we need to run the measurements through the database of the people known to the user, and isolate the person with the closest measurements. This can be done by any machine learning classification algorithm. A classifier can get the measurements from any image and tell us who is the closest match.

Haar Cascades are machine learning object detection algorithms that are used to identify faces in an image or a real-time video. The Haar Cascade algorithm uses edge or line detection features that are proposed by Viola and Jones within their research paper named "Rapid Object Detection employing Boosted Cascade of Simple Features"

Steps involved in algorithm.

- Importing OpenCV
- Importing XML file
- Importing test Image
- Converting the image to greyscale
- Detecting Multi-scale faces
- Mentioning sides of the rectangle for face detection
- Displaying the detected image

Facial recognition works in three steps: detection, analysis, and recognition.

- Detection. Detection is the process of finding a face in an image. ...
- Analysis. The facial recognition system then analyzes the image of the face. ...
- Recognition.

The facial recognition process normally has four interrelated phases or steps. The first step is face detection, the second is normalization, the third is feature extraction, and the final step is face recognition. Nowadays, face detection systems are increasingly common since they may be far more secure than fingerprint and written passwords. Face detection is also utilized for surveillance in various locations, including airports, train stations, and roadways. Due to the portability of the Raspberry Pi as a surveillance system, we will develop a face recognition system using the OpenCV library. It comes with two Python scripts, one of which is a training programme that will examine the collection of images of a certain person and produce a dataset (YML File), much like every other Face Recognition system. The second software in this group is called Recognizer, which finds faces and utilizes an YML file to identify them so it can say the person's name. These apps have been specially designed for Raspberry Pi (Linux).

OpenCV

OpenCV is a free and open-source toolkit for image processing, computer vision, and machine learning. It now has a significant impact on real-time functioning, which is crucial for modern systems. Anyone may process photos and videos to recognize items, people, and even handwriting by utilizing this library. When combined with other libraries, such NumPy and Python, the OpenCV array structure may be processed for analysis. It recognizes the properties of visual patterns that will be utilized to conduct mathematical operations in vector space. You may read this article to learn more about OpenCV. This will need to be done in order to install OpenCV and prepare it for face detection

Dlib

Dlib is a cutting-edge C++ toolkit that includes machine learning techniques and tools for developing sophisticated software to address real-world issues. It is employed in a variety of fields, including robots, embedded technology, mobile phones, and huge high performance computer systems, in both business and academics. Dlib may be used for free in any application thanks to its open source license.

Pillow

Python Imaging Library, popularly known as Pillow or PIL, is a programme that may be used to open, modify, and save pictures in a variety of different formats.

Face recognition

It is believed that the face recognition library for Python is the only library capable of recognizing and manipulating faces. This collection will be used to train and identify faces.

Haar cascade classifier

Face detection is a hot topic with many practical applications. Modern smartphones and laptops have facial detection software built in that can verify the user's identification. Numerous applications have the ability to record, recognize, and process faces in real time while also determining the user's age and gender and applying some very amazing filters. The list is not just restricted to these mobile applications because face detection has several uses in surveillance, security, and biometrics. The original Object Detection Framework for Real Time Face Detection in Video Footage was proposed by Viola and Jones in 2001, however, and that is where its Success stories have their roots.

Haar cascade 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. The models are kept in the repository as XML files and may be read using OpenCV techniques. These comprise models for detecting faces, eyes, upper and lower bodies, license plates, and so on. Here are a few ideas that Viola and Jones put out in their research.

The equation of recognition rate is: Recognition Rate =

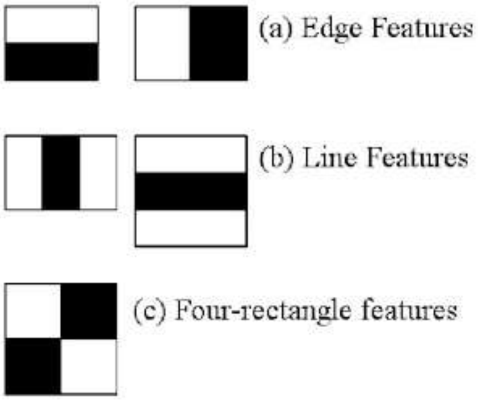
$$\frac{Number\ of\ correctly\ identified\ images}{\text{Total Number of Images}} \text{ X } 100$$

The system has been trained by running each algorithm ten times and then an average is taken. The training time obtained is 7.2282 seconds. The test results are mentioned in Table 1, wherein Eigenface recognizer has been used for feature extraction process.

Distance Between Person and Camera (cm)	**Recognition Rate using Eigenface**		
	Day	Night	With Expression
35	100%	100%	100%
40	100%	100%	100%
45	100%	100%	100%
50	100%	100%	100%
60	100%	100%	100%
80	45%	35%	45%
Total	90.83%	89.16%	90.83%

The objective here is to find out the sum of all the image pixels lying in the darker area of the haar feature and the sum of all the image pixels lying in the lighter area of the haar feature. And then find out their difference. Now if the image has an edge separating dark pixels on the right and light pixels on the left, then the haar value will be closer to 1. That means, we say that there is an edge detected if the haar value is closer to 1. In the example above, there is no edge as the haar value is far from 1. This is just one representation of a particular haar feature separating a vertical edge. Now there are other haar features as well, which will detect edges in other directions and any other image structures. To detect an edge anywhere in the image, the haar feature needs to traverse the whole image. 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. 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. Now, the haar features traversal on an image would involve a lot of mathematical calculations. As we can see for a single rectangle on either side, it involves 18 pixel value additions (for a rectangle enclosing 18 pixels). Imagine doing this for the whole image with all sizes of the haar features. This would be a hectic operation even for a high performance machine. To tackle this, they introduced another concept known as The Integral Image to perform the same operation. An Integral Image is calculated from the Original Image in such a way that each pixel in this is the sum of all the pixels lying in its left and above in the Original Image. The calculation of a pixel in the Integral Image can be seen in the above GIF. The last pixel at the bottom right corner of the Integral Image will be the sum of all the pixels in the Original Image.



With the Integral Image, only 4 constant value additions are needed each time for any feature size (with respect to the 18 additions earlier). This reduces the time complexity of each addition gradually, as the number of additions does not depend on the number of pixels enclosed anymore. This is a case where there is a sudden change of pixel intensities moving vertically from the left towards the right in the image. Again repeating the same calculation done above, but this time just to see what haar value is calculated when there is a sudden change of intensities moving from left to right in a vertical direction. The haar value here is 0.54, which is closer to 1 in comparison to the case earlier.

Procedure

Before we start, it's important to grasp that Face Detection and Face Recognition are two different things. In Face Detection, only the face of an individual will be detected by the software. In Face Recognition, the software won't only detect the face but will recognize the person. Now, it should be clear that we'd like to perform Face Detection before performing Face Recognition A video feed from a webcam is nothing but a long sequence of images being updated one after the other and each of those images is simply a set of pixels of various values put together in its respective position. There are plenty of algorithms behind detecting a face from these pixels and further recognize the person in it and trying to explain them is beyond the scope of this tutorial, but since we are using the OpenCV library, which is incredibly simple to perform, face Recognition can be understood without getting deeper into the concepts.

Train face

The get face.py programme opens every image in the Face Images directory and looks for faces in them. When a face is found, it is cropped, made grayscale, and then converted to a NumPy array. Then we ultimately coach and save it as a file named face-trainner.yml using the face recognition library that we installed previously. The data in this file can subsequently be used to become acclimated to recognizing the faces. By importing the predetermined modules, we launch the application. The OS module is used to traverse through directories, the cv2 module is used for image processing, Numpy is used to translate images into mathematical equivalents, and PIL is used to manage images.

The haarcascade frontal face default.xml classifier must then be used to find faces in photos. Go to your project folder to make sure this XML is there; else, issues will occur. Then, we create a Local Binary Pattern Histogram (LBPH) Face Recognizer using the recognizer variable. Then, in order to view the images contained there, we must navigate to the Face Images Directory. Your current working directory should contain this directory (CWD). The next line is used to access the folder that is kept inside the CWD. Since the BGR values will be ignored, it is well known that grayscale photos are much simpler for OpenCV to analyses than colorful ones. To reduce the image's values while maintaining consistency across all photos, we convert the image to grayscale and shrink it to 550 pixels.

Make sure the face is in the center; else, it will be chopped out. In order to assign a numerical value to the photos, convert them to a NumPy array. Then, use the cascade classifier to find faces in the images and save the results in a variable named faces. the face is found, we'll crop the region around it and designate it as our Region of Interest (ROI). The face recognizer is trained using the ROI region. Every ROI face must be added to a variable named x train. Then we provide the recognizer, which can give us the training data, these ROI values together with the Face ID value. After compiling this application, the information received is stored, although you might notice that the face-trainner.yml file is occasionally modified.

Therefore, be careful to build this programme each time you make modifications to the images in the Face Images directory. For debugging reasons, the Face ID, pathname, person's name, and NumPy array may be output after compilation.

Test face

We may utilize the training data to recognize faces now that it is available. We'll import a live video stream from a USB camera into the Face Recognizer application and turn it into a picture. Then, using our face detection method, we must find faces in those photographs and compare them to all of the Face IDs we've already established. If a match is found, we will box the face and note the name of the person who was identified. The programme and the trainer programme are quite similar, so import the exact modules we used before and utilize the classifier since we want to conduct face detection once more.

2. Output Results

The Main aim of the project is to build affordable security system for common man, to conserve the natural resources like water, electricity and to provide easy access control to the key electrical equipment's in the house. The Component Cost table (Table 1) showcases the cost of each of the component used.

Table1. Component Cost Table

Total Components Cost	
Component	***Cost (INR)***
Raspberry Pi3	3020
Electro Magnetic Lock	1100
PIR Motion Sensor	66
Door Open Sensor MC 38	70
Fire Sensor - MQ2	95
Ultra-sonic Distance Sensor HC SR04	64
Finger Print Sensor R307	935
Outdoor 4 x 4 Matrix Keypad	159
Outdoor Raspberry Camera Unit	325
Total Cost	5834

The Home Security system is not widely used because of the price factors set at higher margin by the marketers. The cost of installing the basic Home security system is more than fifty thousand rupees.

By installing the home security system proposed in this paper, the cost of installing the various components is around five thousand eight hundred and thirty-four. This cost is just one tenth of the cost quoted in the market.

Home Thefts can be totally eradicated if this system is installed. The owner of the house is intimated immediately in vase of any unauthorized entry with the help of motion sensor and door sensor. Fire Accident loses can also be mitigated because of the early detection of the smoke and heat with the help of the IR Heat sensors.

According to Niti Ayaog Water Management, half of India is facing water crisis. Chennai, Bangalore already having water crisis because of delayed monsoon. More than 50% of the water is being wasted on daily basis, because of waterflow from overhead tanks, by installing this project, the user will be able to switch off the water motor in timely manner because of the alert message and is able to save water and electricity.

The electrical energy consumption in the house can also be monitored and controlled using the smart phone. The appliances which are not required can be switched off using smart phone, thus enabling the user to conserve the electrical energy consumption

Output Results

In this paper, we have introduced the step-by-step procedure of smart home automation regulator unit. With the help of the plan control unit, home machine can be converted into a savvy and insightful gadget utilizing IoT.

The key goal of the project to build affordable secure Home Security system for common man usage. Even if the user is away from the home a sense of security is made available because of building the Raspberry Pi integration. The overall cost also has been kept low so that maximum benefit is provided to the end user.

The system has been successfully integrated using Raspberry Pi and the aim has been achieved without any deviation. The limitations of this research is limited only to the sensors specified in this paper. There is lot of scope for future enhancement in inclusion of additional sensors to provide new controls to the user in cost effective method.

3. Acknowledgment

I wish to thank E.N.Ganesh Dean of Vels University for supporting and guiding me through the entire process of research

J. Kaur, "Operating systems for low-end smart devices: a survey and a proposed solution framework," *International Journal of Information Technology*, vol. 2, no. 5, 2018.

Y. T. Park, "Smart digital door lock for the home automation," *IEEE,* 2009.

Y. Sharma, "Cloud based Intelligent Plant Monitoring Device," International Research Journal of Engineering and Technology, vol. 2, p. 16, 2019.

A. A. Shankar, "Finger Print Based Door Locking System," *International Journal Of Engineering And Computer Science,* vol. 4, no. 3, pp. 10810-10814, 2015.

E. J. O. Oke A. O., "Development of a GSM based Control System for Electrical Appliances," *International Journal of Engineering and Technology,* vol. 3, no. 4, 2013.

N. N. Mahzan, "Design of an Arduino-based home fire alarm system with GSM module," *Journal of Physics: Conference Series,* vol. 4, no. 3, 2017.

S. Wadhwani, "Smart Home Automation and Security System using Arduino and IOT," *International Research Journal of Engineering and Technology (IRJET),* vol. 5, no. 2, 2018.

U. Singh, "Smart Home Automation System Using Internet of Things," in *IEEE,* 2019.

U. Singh, "Smart Home Automation System Using Internet of Things," in *IEEE,* 2019.

N. David, "Design of a Home Automation System Using," *International Journal of Scientific & Engineering Research,* vol. 6, no. 6, 2015.

R.Chandana, "Smart Surveillance System using Thing Speak," *International Journal of Advanced Research in Computer and Communication Engineering,* vol. 4, no. 7, 2015.

J. Kaur, "Operating systems for low-end smart devices: a survey and a proposed solution framework," *International Journal of Information Technology,* vol. 2, no. 5, 2018.

A. A. A. Sen, "Preserving privacy in internet of things: a survey," *International Journal of Information Technology,* no. 10, 2018.

D.NARESH, "Bluetooth Based Home Automation and Security System Using," *International Journal of Engineering Trends and Technology (IJETT,* vol. 4, no. 9, 2013.

V. Gunge, "Smart home automation: a literature review," *Journal of Computer Applications,* 2016.

K. Gill, "A zigbee-based home automation system," *IEEE Transactions on Consumer Electronics,* vol. 55, no. 1, 2018.

A. Alkar, "An Internet based wireless home automation system for multifunctional devices," *ieee,* vol. 51, no. 4, 2015

A. ElShafee, "Design and Implementation of a WiFi Based," *World Academy of Science, Engineering and Technology,* vol. 6, no. 3, p. 2177, 2012.

N. K. Suryadevara, "Wireless Sensor Network Based Home Monitoring System for Wellness Determination of Elderly," *ieee,* vol. 6, no. 3, p. 4592, 2017.

V. Namboodiri, "Toward a Secure Wireless-Based Home Area Network for Metering in Smart Grids," *ieee,* vol. 8, no. 2, p. 5672, 2016.

J. Bangali, "Energy efficient Smart home based on Wireless Sensor Network," *American Journal of Engineering Research (,* vol. 2, no. 12, p. 2320, 2013.

P. Manojkumar, "A novel home automation distributed server management system using Internet of Things," *International Journal of Ambient Energy,* vol. 43, no. 1, p. 5478, 2021.

T. Chaurasia, "Enhanced Smart Home Automation System based on Internet of Things," *IEEE,* 2019.

H. Mehta1, "IOT BASED HOME AUTOMATION SYSTEM USING ARDUINO BOARD," *International Research Journal of Engineering and Technology,* vol. 4, no. 1, 2017.

S. K. A. Shah, "Smart Home Automation Using IOT and its Low," *I. J. Engineering and Manufacturin,* vol. 5, no. 2, p. 28, 2020.

L. M. Gladence, "Recommender system for home automation using IoT and artificial intelligence," *Journal of Ambient Intelligence and Humanized Computing* , vol. 12, no. 5, p. 3252, 2020.