MULTI-TIER AUTHENTICATION MODEL BASED HOME AUTOMATION

Nagaraj Doddam[1*], E. N. Ganesh[2]

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

Abstract

Automation is a key driver in reducing the scope of human error. Inter can be viewed as advancement rather than an uprising. Quick response systems using automation will provide more accurate and real time data. The main idea for this research work is to effectively manage the tasks of a home through an integrated control system .The existing Home Security Automation available in Market is at high cost and is not affordable for common man .The proposed system brings in the strengths of the IOT and providing a robust cost effective automation solution. It will have several key functions like Smoke sensor Alarm based smart lock, Finger Print sensor authentication, Face detection authentication, Intruder sensing, smart water tank. The Home security system helps in controlling household appliances from far-off Location.

Keywords: Raspberry, Sensors, Haar Cascade 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.s3.093

1. Introduction

The technological advances has made life easier by improving the ways to communicate with the objects. The world is moving towards smart things and improving the quality of life by use of technology .To strive in this smarter world everyone has to do daily things in a smart way. For implementing smarter way the smart technologies we are using are IOT & smart home automation. It consists of everything which includes smart homes, smart cities, smart energy, intelligent transportation, etc., IOT (Internet of things) is the communication between the humans and objects and also it is the interface of physical devices like electronics, software, sensors, actuators, and network connectivity that enables the devices to transfer the data. The human force, time and cost must be reduced. In IOT distance never matters. We can operate it anywhere from the world. This is the main reason why to use this technology in the project. Research studies estimate that will internet of Things consists of almost 40 billion of objects by 2020. Automation performs a gradually crucial role in daily experience and global economy. Engineers strive to combine automated devices with mathematical and organizational tools to create complex systems for a gradually increasing range of applications and human activities.

Home automation systems suffers from main challenges these are poor flexibility ,difficulty, manageability in achieving security & it is high cost .The main objective of this project is to design and implement a home automation system using IOT that is capable of controlling & monitoring the home appliances in an easy way through web interface .The proposed system has good flexibility, and no difficulty while using through Wi-Fi technology to connect with the different sensors to home automation system. This will decrease the cost gradually and will increase the ability of upgrading the system to be reconfigurable

Bluetooth based home automation system using Mobile:
In Bluetooth based home automation system the home appliances are connected to the Raspberry board, by using the relay at input and output ports. A high level interactive C language is used for programming and can be dumped into Raspberry BT board by using Bluetooth we made connection path available. The protection is provided by making use of OTP (One Time Password) so that the selected users are allowed to control the appliances. By using wireless Bluetooth communication we can establish the connection between Raspberry boards and Mobile, it is portable and environmental friendly. To indicate the status of the device we can receive the feedback from the mobile by using the signals from the designed circuit.

2. Zigbee based home automation system using Mobile:
By making use of Zigbee the monitoring and controlling of home appliances can be designed and implemented. By using the network coordinators the device performance is recorded and stored. In this the Wi-Fi network is used with standard wireless ADSL modern Router. The security Wi-Fi parameter and the network SSID are saved previously. The message is sent to network device of the home only when it is to be declared safe and it is re-encrypted. By using Zigbee network the Zigbee controller sent messages to it. The virtual home algorithm receives the security messages. In Zigbee communication we can decrease the cost of the system.

3. Home automation using RF module:
The main aim of Home Automation is to develop a home automation system using RF controlled remote. Now technology is increasing so that homes are getting smarter with these new technologies. Modern homes are changing from switches to centralized control systems which contain RF controlled switches. In every house there are traditional wall switches in various parts of the home it makes difficult for the users to go near them to control and operate. It becomes difficult for the old people and for physically handicapped people to do so. Home Automation using remote implements an easier solution with RF technology. For this RF remote is combined to the microcontroller on transmitter side that sends ON/OFF signals to receiver where the devices are connected.

4. GSM based home automation system using Mobile:
GSM based Home automation become an attractive due to the Mobile phone and GSM technology. In GSM communication can be done by considering the SMS based home automation, GPRS based home automation and dual tone multi frequency (DTMF) based home automation. To convert machine signals into electrical signals a device named transducer is used and these signals are given as inputs to the microcontroller. The physical quantities like sound, temperature and humidity can be converted into other quantities like voltage and current by using sensors. Since the GSM module can understand only commands so that microcontroller converts signals into commands. Based on the command which is received by the actions will be performed

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

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 one 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 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].

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

In another 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 existing 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 one of the 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

There are many existing Home automation architectures available in the market today. The most famous ones are listed below:

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. Some of its 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 due to 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. Various devices can be connected using different 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, and 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.

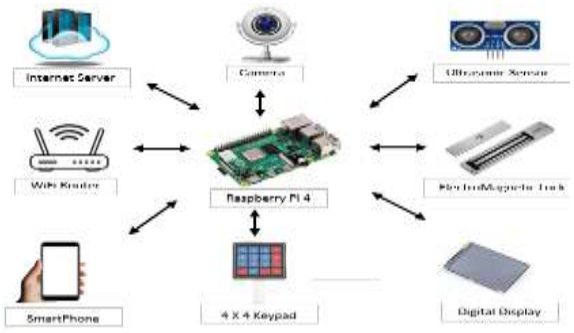
The Smart Home features in this paper are broadly classified into three main areas 1. Main Security Enhancement 2. Smart Accessibility & Protection 3. Energy Savings Automation

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 an 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



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.

B. 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 Wi-Fi. It has internal memory of 1GB. This Raspberry pi consists of I/O, CPU, and Ethernet, 2 x USB Hub, HDMI Port, and audio Jack and memory slots. The version of Raspberry Pi is best suited for this project as it meets the requirement of the project

C. **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.

D. **PIR Motion Sensor**

PIR is the Passive Infra-Red Motion Sensor which detects the motion. The PIR Motion Sensors are placed in strategically 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.

E. **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

F. **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

G. **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.

H. **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.

I. **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

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.

Features

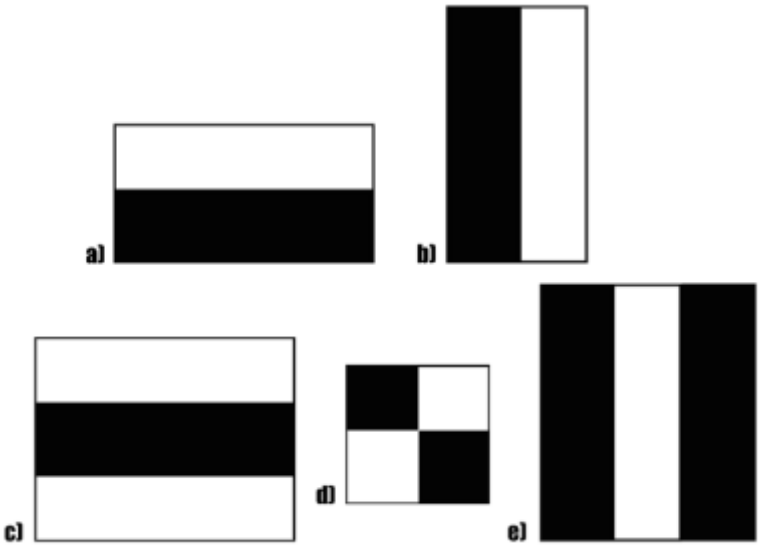


Fig. a sample of Haar features used in the Original Research Paper published by Viola and Jones.The first contribution to the research was the introduction of the haar features shown above. These features on the image makes it easy to find out the edges or the lines in the image, or to pick areas where there is a sudden change in the intensities of the pixels.

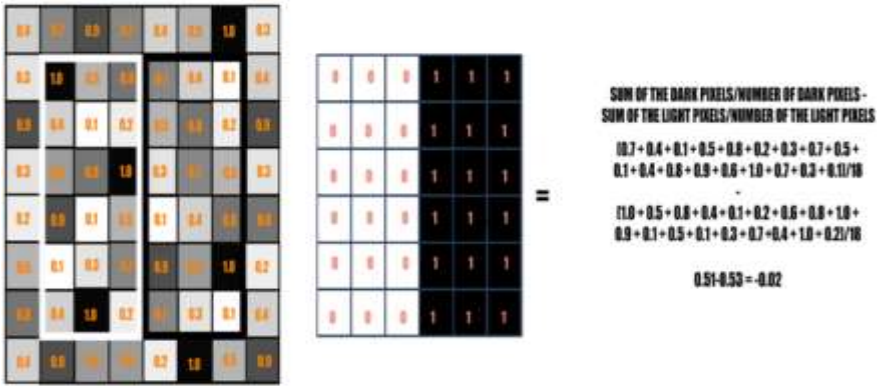


Fig. The rectangle on the left is a sample representation of an image with pixel values 0.0 to 1.0. The rectangle at the center is a haar kernel which has all the light pixels on the left and all the dark pixels on the right. The haar calculation is done by finding out the difference of the average of the pixel values at the darker region and the average of the pixel values at the lighter region. If the difference is close to 1, then there is an edge detected by the haar feature. A sample calculation of Haar value from a rectangular image section has been shown here. The darker areas in the haar feature are pixels with values 1, and the lighter areas are pixels with values 0. Each of these is responsible for finding out one particular feature in the image. Such as an edge, a line or any structure in the image where there is a sudden change of intensities. For ex. in the image above, the haar feature can detect a vertical edge with darker pixels at its right and lighter pixels at its left.

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. Also 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.

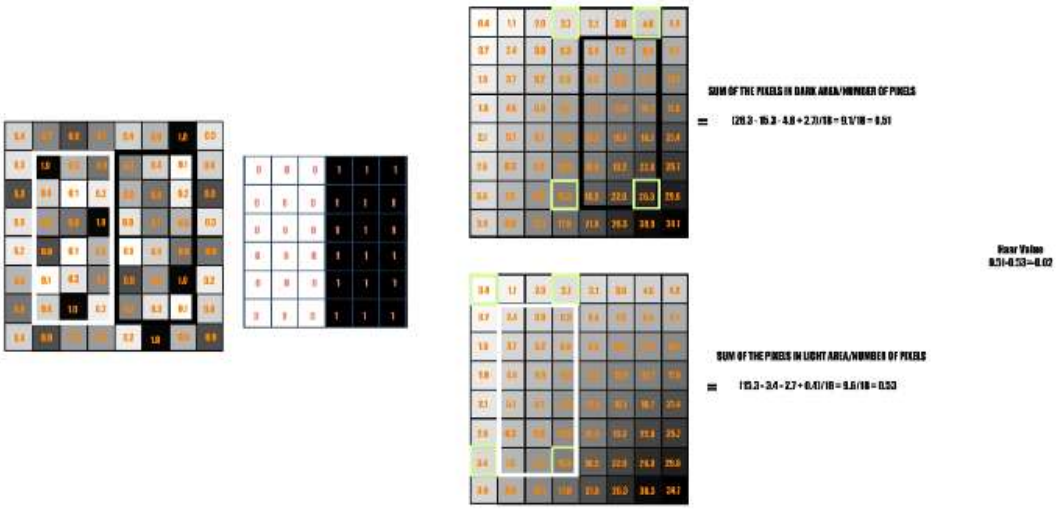


Fig. Integral Image is used here to calculate the haar value.

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. In the above image, there is no edge in the vertical direction as the haar value is -0.02, which is very far from 1. Let's see one more example, where there might be an edge present in the image.

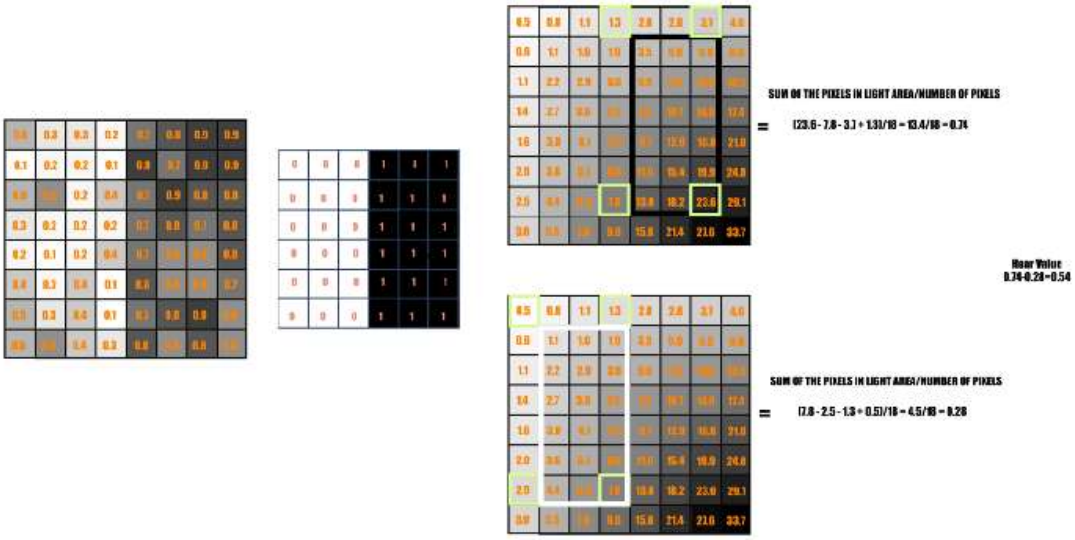


Fig. Haar calculation from Integral Image.

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.

This paper basically consists of three important parts i.e. sensing, monitoring, and controlling system. The first part sensing is done by sensors like flex sensor, accelerometer etc. the monitoring task is done by the cloud platform and the controlling part is done by our microcontroller unit i.e. i.e. Raspberry.The sensors, appliances and Wi-Fi module are interfaced with Raspberry. The value of sensors brings a change in the status of our appliances. The flex sensor depends on the gestures of our fingers to control the appliances. The accelerometer controls the opening and closing of door. The magnetic sensor alerts us if the door lock brakes. The flame sensor alerts us if there is fire in the house. The status of our appliances are uploaded on the cloud platform and the user can see the status on his laptop and smartphone as well. The Aurdino UNO controls the appliances on the basis of value given by sensors.

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 IOT facilitates numerous benefits to the society and from our paper we can provide and prove the strength of IOT that is capable to contribute the services for the purpose of building vast no. of applications and help to implement them on the public platform. This design provides moderate and less expensive way of sensing, monitoring and controlling system in the field of domestic and as well as industrial standard to implement IOT. At a final note, we conclude that IOT leads to become universal in every aspect. This paper will be very beneficial in our normal day to day life and will bring much needed innovation in his fast changing world of technology where people prefer to have control over things using the smartphones which will bring ease to their routine life.

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

3. References

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.

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.