Dedan Kimathi University of Technology

Better Life through Technology

THE DESIGN AND IMPLEMENTATION OF FACIAL RECOGNITION SECURITY SYSTEM AT GEARBOX, NAIROBI

By

Benson Githutha Gathitu

E022-01-1071/2018

BSc. In Mechatronics Engineering

4th Year

Supervisor: Dr. Titus Mulembo

Attachment Period: 6th October 2021 – 10th October 2021

ABSTRACT

Security has always been a vital agenda in any workplace be it a commercial space, manufacturing plant or government offices. In the modern world, aside from human labour, electronic gadgets have aided in improving security through the use of video surveillance technology. The Facial Recognition System is focused on greatly improving security by facial image scanning and processing hence allowing entry to a workplace on recognition of one`s face or alerting security department on detection of strangers.

TABLE OF CONTENTS

Contents

LIST OF FIGURES

LIST OF TABLES

CHAPTER ONE

General Background

Automation of most human functions is rapidly increasing in the present day. Up to date, guards have to monitor and manage entry of people to places like commercial spaces, government offices and warehouses.

The advancements in Machine Learning have enabled the process of precise image processing and recognition. The cost of implementation is viable even in household application.

New innovative technology revolves around economic feasibility of a product in terms of its cost and ease of implementation. The Raspberry pi crosses both criteria in that it is a cheap, effective computer which ca be interfaced with other modules to realize systems with immense functionality. It can be very useful in applications such as motor speed control, automatic lighting, VPN server and security system.

Major modules to be integrated with a Raspberry pi in a security system are a camera (piCamera or webcam), proximity and motion sensors which are all affordable. The whole security system circuitry is simple and easy to implement. This makes it easy to implement a cost-effective security system to provide comfortable and safe environment for households and workplaces.

The security system cannot wholly replace the role of security guards but will make their life easier.

Image processing means taking an input of an image or video frame, processing it and output a set of related parameters of an image. Machine learning aids in the tracking, detections and recognition of an image.

Problem Statement

The need to develop a cost effective facial recognition system was immensely influenced by the fact that Gearbox had not implemented a digital register of the people entering the premises. Also there were many people entering the premises (employers, employees, interns and attachees). Most of the interns and attachees were not recognized by the security guards and were deemed as strangers hence denied entry till their identity was confirmed.

The facial recognition system would solve these problems as it would recognize everyone provided that their images and details have been logged into the company's database. Also it would register entry time of every individual in the company.

Objectives

The main aim of this project is to design and develop a security system that includes features as proximity and motion detection, image processing and recognition and entry into a database.

The system had to:

- detect a human being close to it,
- activate a camera to capture a facial image
- process the image and recognize the face.
- Log entry time of an individual to a database.
- Alert security officials on failure in recognizing an individual.

The specific objectives were:

- To study and describe how the Raspberry Pi can be interfaced with a proximity sensor and PiCamera/webcam.
- To study communication protocols between the Raspberry Pi and the company's database.
- To develop and build the security system.
- To design and 3D print casing if the system.
- To install the system in the company's reception area.

Scope of the Project

Face identification is one of the most developing research zones because of increasing demands for security in numerous applications. This project is focused on developing a security system that detects and recognizes faces and logs entry time of a recognized individual to a database.

However, the system will not include a video surveillance module.

CHAPTER TWO

LITERATURE REVIEW

Introduction

Face recognition has gained tremendous attention over the last three decades since it is considered a simplified image analysis and pattern recognition application. There are at least two reasons for understanding this trend:

1. the large variety of commercial and legal requests
2. the availability of the relevant technologies (e.g., smartphones, digital cameras).

Although the existing machine learning/recognition systems have achieved some degree of maturity, their performance is limited to the conditions imposed in real-world applications. For example, identifying facial images obtained in an unconstrained environment (e.g., changes in lighting, posture, or facial expression, in addition to partial occlusion, disguises, or camera movement) still poses several challenges ahead. This means that the existing technologies are still far removed from the human visual system capabilities.

Referential databases are used to match and compare a respondent's facial images (e.g., perpetrator, witness, or victim).

Besides, the broad use of digital cameras and smartphones made facial images easy to produce every day; these images can be easily distributed and exchanged by rapidly established social networks such as Facebook and Twitter.

Face recognition has a long history; it stirs neurologists, psychologists, and computer scientists. The human face is not an ideal modality compared to other biometric traits; it is typically less precise than other biometric modalities such as iris or fingerprint, and can potentially be influenced by cosmetics, disguises, and lighting. However, the face has the advantages that make it one of the most favored biometric characteristics for identity recognition, we can note:

Natural character: The face is a very realistic biometric feature used by humans in the individual's recognition, making it possibly the most related biometric feature for authentication and identification purposes. For example, in access control, it is simple for administrators to monitor and evaluate approved persons after authentication, using their facial characteristics. The support of ordinary employers (e.g., administrators) may boost the efficiency and applicability of recognition systems. On the other hand, identifying fingerprints or iris requires an expert with professional competencies to provide accurate confirmation.

Nonintrusive: In contrast to fingerprint or iris images, facial images can quickly be obtained without physical contact; people feel more relaxed when using the face as a biometric identifier. Besides, a face recognition device can collect data in a friendly manner that people commonly accept.

Less cooperation: Face recognition requires less assistance from the user compared with iris or fingerprint. For some limited applications such as surveillance, a face recognition device may recognize an individual without active subject involvement.

First attempts at identifying a facial subject by comparing a part of a facial photograph were reported at a British court in 1871. Face recognition is one of the most significant law enforcement techniques in cases where video material or pictures on a crime scene are available. Legal specialists do a manual facial image test to match that of a suspect. Automated facial recognition technologies have increased the efficiency of judicial employees and streamlined the comparison process.

Today facial recognition, associated with artificial intelligence techniques, enables a person to be identified from his face or verified as what he claims to be. Facial recognition can analyze facial features and other biometric details, such as the eyes, and compare them with photographs or videos. With accusations of widespread surveillance, this controversial technology raises many concerns among its opponents, who fear breaches of data privacy and individual liberties. Face recognition for its defenders enables accurate, fast, and secure authentication to protect against all fraud forms. According to a report by the analytical company Mordor-Intelligence, the face recognition market was estimated at 4.4 billion dollars worldwide in 2019 and would surpass 10.9 billion in 2025. This technology has already become popular in some countries, such as China.

Because of artificial intelligence technologies, significant advances in face recognition have occurred. In early times, research interests were mainly focused on face recognition under controlled conditions where simple classical approaches provided excellent performance. Today, the focus of research is on unconstrained conditions in which deep learning technology has gained more popularity as it offers strong robustness against the numerous variations that can alter the recognition process.

In addition, many academics struggle to find robust and reliable data sets for testing and to evaluate their proposed method: finding an appropriate data set is an important challenge especially in 3D facial recognition and facial expression recognition. To check the effectiveness of these methods, accurate datasets are required that

i. contain a large number of persons and photographs,

ii. follow real-world requirements

iii. are open to the public.

Face Recognition History

This section reviews the most significant historical stages that have contributed to the advancement of face recognition technology:

Table 1: Face Recognition History

YEAR	
1964	The American researchers studied facial recognition computer programming. They imagine a semi-automatic method, where operators are asked to enter twenty computer measures, such as the size of the mouth or the eyes.
1977	The system was improved by adding 21 additional markers (e.g., lip width, hair color).
1988	Artificial intelligence was introduced to develop previously used theoretical tools, which showed many weaknesses. Mathematics (“linear algebra”) was used to interpret images differently and find a way to simplify and manipulate them independent of human markers.
1991	Alex Pentland and Matthew Turk of the Massachusetts Institute of Technology (MIT) presented the first successful example of facial recognition technology, Eigenfaces, which uses the statistical Principal component analysis (PCA) method.
1998	To encourage industry and the academy to move forward on this topic, the Defence Advanced Research Projects Agency (DARPA) developed the Face recognition technology (FERET) program, which provided to the world a sizable, challenging database composed of 2400 images for 850 persons.

2005	The Face Recognition Grand Challenge (FRGC) competition was launched to encourage and develop face recognition technology designed to support existent facial recognition initiatives.
2011	Everything accelerates due to deep learning, a machine learning method based on artificial neural networks. The computer selects the points to be compared. It learns better when it supplies more images.
2014	Facebook knows how to recognize faces due to its internal algorithm, Deepface. The social network claims that its method approaches the performance of the human eye near to 97%.

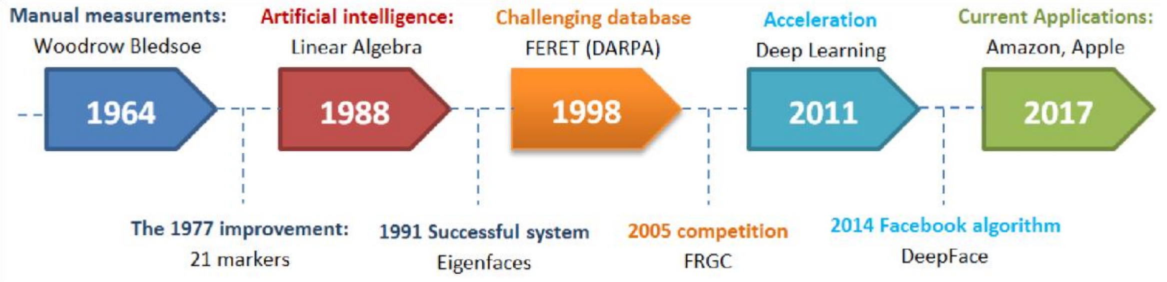


Figure 1: Primary stages in the history of face recognition

Today, facial recognition technology advancement has encouraged multiple investments in commercial, industrial, legal, and governmental applications. For example:

In its new updates, Apple introduced a facial recognition application where its implementation has extended to retail and banking.

Mastercard developed the Selfie Pay, a facial recognition framework for online transactions.

From 2019, people in China who want to buy a new phone will now consent to have their faces checked by the operator.

Chinese police used a smart monitoring system based on live facial recognition; using this system, they arrested, in 2018, a suspect of “economic crime” at a concert where his face, listed in a national database, was identified in a crowd of 50,000 persons.

Face Recognition Systems

Main Steps in Face Recognition Systems

In engineering, the issue of automated face recognition includes three key steps

1. approximate face detection and normalization

2. extraction of features and accurate face normalization
3. classification (verification or identification).

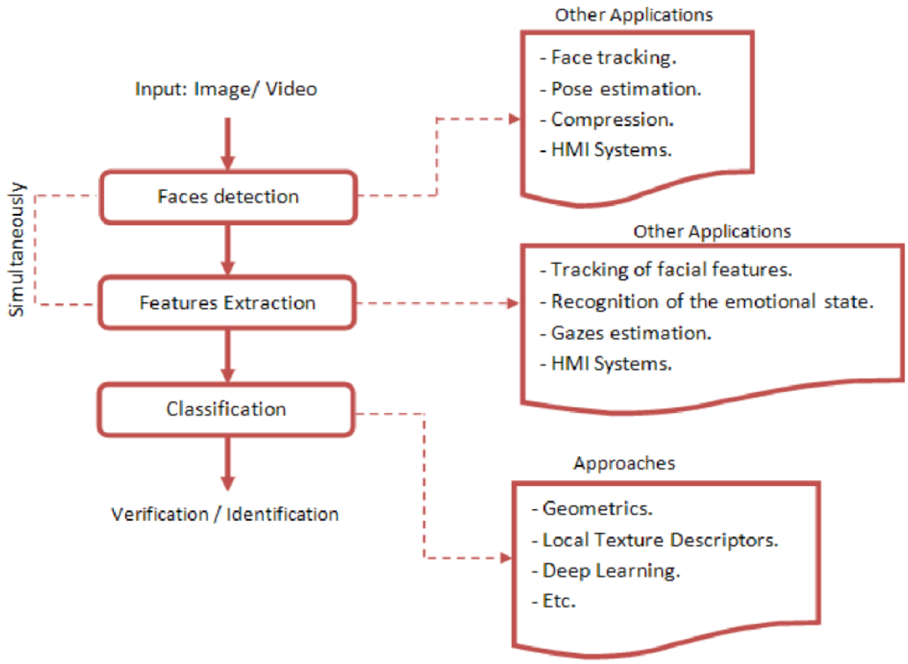


Figure 2:The standard design of an automated face-recognition system.

Face detection is the first step in the automated face recognition system. It usually determines whether or not an image includes a face(s). If it does, its function is to trace one or several face locations in the picture.

Feature extraction step consists of extracting from the detected face a feature vector named the signature, which must be enough to represent a face. The individuality of the face and the property of distinguishing between two separate persons must be checked.

Classification involves verification and identification. Verification requires matching one face to another to authorize access to a requested identity. However, identification compares a face to several other faces that are given with several possibilities to find the face's identity. Sometimes, some steps are not separated.

For example, the facial features (eyes, mouth, and nose) used for feature extraction are frequently used during face detection. Detection and extraction of features can be performed simultaneously, as shown in the figure above.

Depending on the application environment's complexity, some external factors can cause highly intra-face identity distributions (or lowly inter-face identity distributions) and degrade the accuracy of recognition. Among these factors, the database size, low or high lighting, presence of noise or blur, disguises, partial occlusion, and certain secondary factors that are often common, unavoidable, and very challenging. In a noisy environment, image pre-processing may prove necessary.

Although automated face recognition systems must perform the three steps mentioned above, each step is considered a critical research issue, not only because the techniques used for each step need to be improved and because they are essential in several applications, as shown in the figure above. For example, face detection is necessary to activate facial monitoring, and the extraction of facial features is crucial to identify the person's emotional state, which is, in turn, essential in human–machine interaction systems (HMI). The isolation of each step facilitates the evaluation and state-of-the-art evolution.

Assessment Protocols in Face Recognition

As stated in the previous sub-section, an automated face recognition system can operate either in the mode of verification or identification, depending on each application.

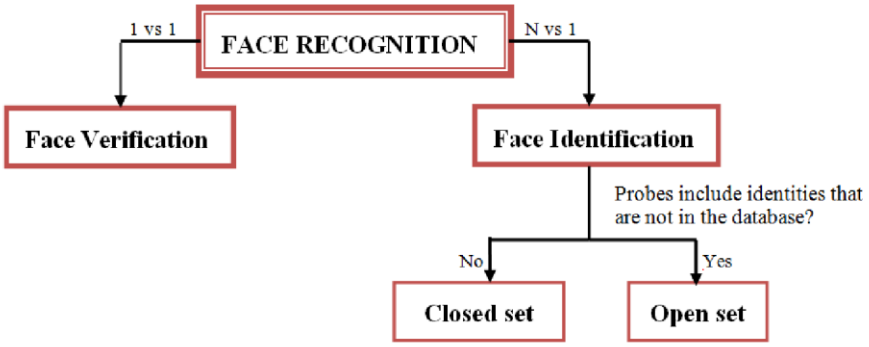


Figure 3: Categorization of various assessment protocols in face recognition.

In verification mode, the system evaluates a person's identity by comparing his/her registered model(s) in the database with the captured face. A one-to-one comparison is performed by the system to decide whether the proclaimed identity is true or false. Habitually, verification is used for positive recognition to avoid different individuals using the same identity. Face verification systems are classically assessed by the receiver operating characteristic (*ROC*) and the estimated mean accuracy (*ACC*).

Two types of errors are assessed for *ROC* analysis: true accept rate (*TAR*) and false accept rate (*FAR*). The *TAR* is defined as the fraction of valid comparisons exceeding the similarity score (threshold) correctly:

$$TAR = \frac{TP}{(TP + FN)} \quad (1)$$

TP: true positive.

FN: false negative.

Moreover, *FAR* is defined as the fraction of the impostor comparisons exceeding incorrectly the same threshold:

$$FAR = \frac{FP}{(FP + TN)} \quad (2)$$

FP: false positive.

TN: true negative.

However, *ACC* is a simplified metric, which shows the percentage of correct classifications:

$$ACC = \frac{TP + TN}{(TP + TN + FP + FN)} \quad (3)$$

In identification mode, the system identifies an individual by searching for the enrolled model representing the best match between all facial models stored in the database. Therefore, a one-against-all comparison is performed by the system to determine this individual (or failure if that individual does not exist in the database), without providing a prior declaration of identity.

Identification is an essential task for harmful recognition applications; the purpose of this type of recognition is to prevent multiple identities by one single individual. For two different scenarios, two test protocols may be used, which are: open-set and closed-set (as shown in the figure above).

For open-set, the training set cannot include test identities. Different metrics are established in the open-set face identification scenario to measure the model's accuracy such as the false negative identification rate (FNIR) and the false positive identification rate (FPIR). FNIR measures the ratio of cases wrongly classified as false, although they are true cases, while FPIR measures the ratio of cases wrongly classified as true despite being false.

Whereas closed-set retrieves images from the same identities for training and testing. Rank-N is a fundamental performance metric used in closed-set face identification to measure the model's accuracy, where the valid user identifier is returned within the N-Top matches.

Applications

1. **Face ID:** Instead of traditional key and password-based identification is replaced with identify people by their face images, it also ensures the physical presence of an authorized person. Such applications are Driver licenses, entitlement programs, immigration, national ID, passports, voter registration, and welfare registration.
2. **Access Control:** The access and restriction to a place or resource is control in this field. Face recognition applies on numerous areas for example: Border-crossing control, facility access, vehicle access, ATM, computer, program, database, network access, online transactions, long distance education and online examinations.
3. **Security:** The face recognition secures the number of systems from life threading damage such as terrorist identification, flight boarding, stadium, audience scanning, computer-based application i.e. database, file encryption, Internet, medical records, and trading terminals security.
4. **Surveillance:** Numbers of advanced surveillance applications are implemented on different locations such as park, power grid, patrol control, nuclear plant to secure the public.
5. **Law enforcement:** This area covers the crime stopping and suspect alert, tracking, suspect background checking, investigation, identifying fraud and cheats and etc.
6. **Human computer interaction (HCI):** Intelligent gaming and proactive processing are the examples in HCI class. Other than this, antique photo verification, low bit rate video and image transmission and so on are some advance applications of face recognition systems.

Face Recognition Techniques

To take advantages of facial based identification, a framework should have the capacity to distinguish an uncooperative face in uncontrolled condition and a discretionary circumstance without notice of the subject. In this section, the recent research in face recognition has been overviewed that apply mostly to frontal faces.

I. **Local binary pattern (LBP)**

In this technique, the face picture is partitioned into the areas (pieces) and every district relates with every focal pixel.

At that point it inspects its pixel neighbor in view of the dark scales estimation of focal pixel to change its neighbor to 0 or 1. Later on extended LBP operator in the view of Weber‘s law was proposed. A new bit of knowledge into three dynamics regarding iris location method on K-means algorithm; Sobel and LBP methods was introduced. Another LBP based approach in face recognition applies form the perspective of various lighting conditions. In this scheme Difference of Gaussian (DoG) and LBPs has been utilized to extract the images for recognition.

Ahonen etal. connected nearby paired example of local binary patterns. This new method was extracted by binarising the gradients of centre point. Moreover, the sub-division has been applied on several parts of face image. The approach proved more robust in pose and illumination changes because of its versatile abilities.

II. Principal Component Analysis PCA or Eigenfaces:

To deal with face recognition, eigenface is one of a very famous approach.

Principal component analysis (PCA) technique is totally based on lower dimensions. In this method a statistical calculation is applied which converts the maximum number of co-related variables into a smaller no. of uncorrelated variables. The fruitful use of PCA was analyzed effectively on face representations. The advance method known as D2DPCA was proposed specifically to overcome illumination changes which normally a main issue in face recognition system. The approach was based on new feature and a fusion of two half-face images. Singular Value Decomposition was utilized to manage encompassing light. The wavelets have been employed to combine KPCA for Multi Scale Features.

III. Neural network:

The non-linearity of neural network makes it more famous and attractive in various field of image processing. It is very tricky to design and implement of a neural network-based recognition successfully. Its criticalness totally depends on future application. Neural networks have been applied for face detection, multilayer perceptron and convolution. In face verification system multi-resolution pyramid structure has been implemented. Moreover, a hybrid approach of neural network was proposed in which local image sample, a self-organizing map and convolutional network. Another approach based of probabilistic decision based neural network (PDBNN) has been applied. The approach inherited the modular structure from its predecessor, a decision based neural network (DBNN). The extended version of NN from the multi-view face representation was adopted via multiband feature technique.

A systolic architecture has been introduced for large scale-based integration of face recognition. A hierarchical method of decision-based neural networks DBNN was adopted with the combination of nonlinear basis functions and a competitive credit-assignment scheme A contrast-adjustment based technique for face recognition has been introduced. The correlation and statistical independence functions were used to set the parameter problems.

IV. Hidden Markov Models (HMMs)

The HMM based Stochastic modelling of non-stationary vector time series has been proved effective for speech-based applications. Recently, this new dimension references in human face recognition. One way to associate and apply HMM was to divide the face regions such as eyes, nose and mouth etc. while in a spatial based observation sequence a band sampling were adopted for face images.

V. Template Matching

Various methods have been proposed in the literature for template matching.
The Euclidean distance has been adopted for template matching. In which the whole image was represented in the intensity values of a two-dimensional array and compared via approximate metric.

Recently, the face templates were compared of an individual. While from single view point but multiple distinctive smaller templates have been adopted for face recognition. Furthermore, the different parts of the template were utilized for matching such as eyes, nose and mouth. The main limitation appeared in template matching is computational complexity. In general, it is more logical as compared to feature matching based approaches for face recognition.

VI. Wavelet transform

Generally believed that neighborhood based features are more reliable while spatial frequency analysis concentrate such features . In this regards wavelet is most popular tool used in characteristics of space–frequency localization. The wavelet transform based face recognition technique has been proposed by calculating the shape and texture of the face images. Moreover, discrete wavelet transform based scheme was introduced via probability distribution functions through various color channels. Specifically, among different wavelet bases Gabor functions provide the higher resolution in spatial and frequency domains/

A Gabor based dynamic link framework and other advance techniques were proposed for face recognition. Later on, the DT-CWT and ST-CWT based face recognition performed better than Gabor wavelets.

VII. Multi algorithm approach:

Nowadays, most of the research is focusing on mutli-modeling and multi-algorithm techniques. In this approach more than one technique are combined to extract features from different perspective in face images. The four kind of schemes like principal component analysis (PCA), Discrete Cosine Transform (DCT), Template Matching using Correlation (Corr) and Partitioned Iterative Function System (PIFS) have been implemented in multi algorithm approach. Along with the multi-algorithm, multi biometric was introduced via merging gray level correlation and principle component analysis (PCA).

VIII. 3D model

The utilization of 3D data in face recognition has recently been pulling in consistently expanding levels of consideration in the biometric group. The reflected light caught by the camera is a complex capacity of the surface geometry, albedo, brightening and the spatial characteristics.

The use of 3D information in face recognition has lately been attracting ever increasing levels of attention in the biometrics community. The reflected light captured by the camera is a complex function of the surface geometry, albedo, illumination and the spectral characteristics of the camera. The unique way to deal with these issues of face recognition is come up with 3D properties based approaches. Along with the 3D geometry a multiple texture maps was adopted to detect the parts and then align model which cover wide range of pose and appearances.

IX. Biomechanical models.

In this approach, the structure and musculature of the face is used mostly for computer animation based applications. Biomechanical model based on 3D shape and color, biomechanical properties of skin and structure beneath the skin and anthropometric statistics along with natural changes in facial appearances adopted to combine 3D and 2D data of face images and proof the success in recognizing the faces.

X. Infrared

Infrared image or thermal images or thermograms shows the heat discharged from an object. These thermal changes represent uniqueness of every object according to their different characteristic of material and its temperature. Thermal imaging becomes more popular in face recognition field via analyzing the temperature generated by blood vessels under the facial skin. Hence, for thermal based face verification systems, particular kind of sensor or camera known as IR is utilized to capture the images which show the thermal changes among faces of various skin types and colors. NIR spectrum has been powerfully provide a detection rate for faces and adopted in numerous face recognition systems via computing feature extraction technique on thermal images.

Security System

Security literally means a way or method by which something is secured through a system of interworking components and devices.

On the other hand, **security systems** are networks of integrated electronic devices working together with a central control panel to protect against burglars and other potential intruders. Security systems work on the simple concept of securing entry points into a home with sensors that communicate with a control panel or command center installed in a convenient location. The sensors are typically placed in entrances as well as easily accessible windows.

Current Security Technologies

Arduino Based Home Security System

This security system project deals with the design and development of a theft control system for home, which is being used to prevent/control any theft attempt.

The developed system makes use of an embedded system comprising of an open hardware microcontroller(Arduino) and a modem based on Global System for Mobile communication (GSM) technology.

The designed and developed system can be installed in the home. An interfacing intrusion detector unit is also connected to the microcontroller-based security system. The system thus incorporates a passive infrared sensor (PIR) for motion detection. In case of an intrusion attempt, a warning message is being transmitted by the system (as an sms) to the owner’s mobile phone, or to any pre-configured mobile phone number for further processing.

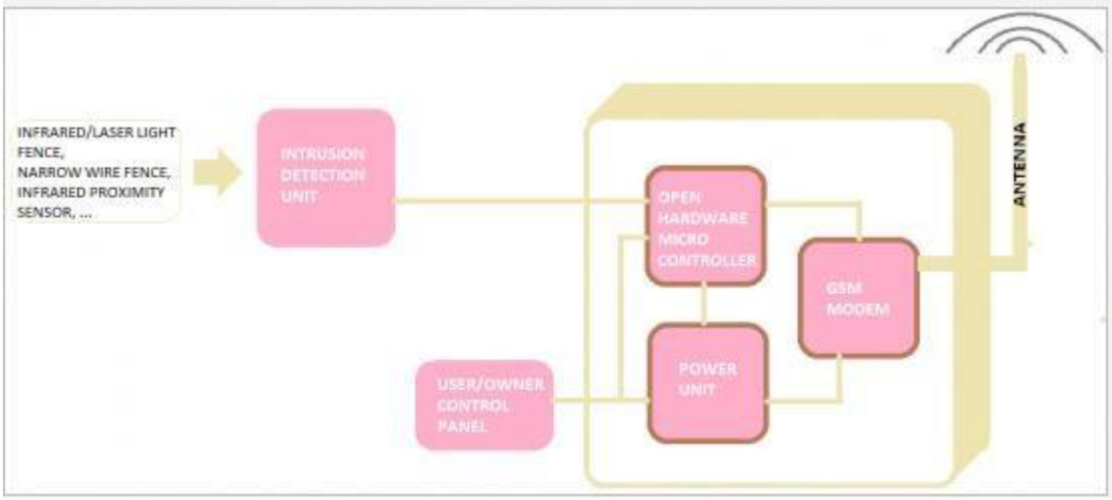


Figure 4: Arduino based home security system block diagram

The security system comprises of an Arduino Uno microcontroller, a standard SIM900A based GSM/GPRS modem and PIR sensor. The whole system can be powered from any 12VDC/2A power supply unit/battery.

How it works

Its working principle can be analyzed from the block diagram above. When input power is applied to the system, the system goes into standby mode. However, when the terminals of connector joining PIR with the Arduino microcontroller are short circuited, the pre-programmed warning message is automatically transmitted to the concerned mobile number. This system however does not transmit the image of the intruder. It only conveys a notification message.

Closed-circuit television (CCTV) Security System

Video surveillance is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors. It differs from broadcast television in that the signal is not openly transmitted, though it may employ point to point (P2P), point to multipoint, or mesh wireless links.

Operation of a CCTV Security System

The simplest system is a camera connected directly to a monitor by a coaxial cable with the power for the camera being provided from the monitor. The outdoor or indoor camera take several images per second and thus cannot be differentiated by human eye. The images are then transferred via a coaxial cable or optic fibre to a computer placed in a secure location. These computers are monitored by security personnel and responds to any improper behaviours. These systems have been incorporated with alarm systems so as to send out an alert in case of a security bridge.

Two types of CCTV storage exist; VCR and DVR. The DVR system is more superior as it can be able to transmit digitized video signals over the data networks and thus can allow for remote control and monitoring of the system.

Remote Surveillance IP System

IP surveillance is a digitized and networked version of closed-circuit television (CCTV). In an IP surveillance system, an IP camera records video footage and the resulting content is distributed over an IP (Internet protocol) network. Adding networking capability to digital CCTV provides additional benefits, including:

i. Improved ability for remote viewing and control. Anyone on the network can potentially see video from any camera connected to the network.

ii. IP storage makes it possible to store data in any geographic location.

iii. Greater ease of distribution. An image of a crime suspect, for example, can be immediately distributed to officials.

iv. The ability to connect to email and other communications systems so that alerts can be sent automatically.

Raspberry Pi Based Surveillance System

A raspberry pi can be used to implement a security system with motion detection, image processing and alert mechanism. The alert ought to contain a time lapse photo or video and transmitted over the internet. This thus will enable the users to monitor the homes from anywhere in the world.

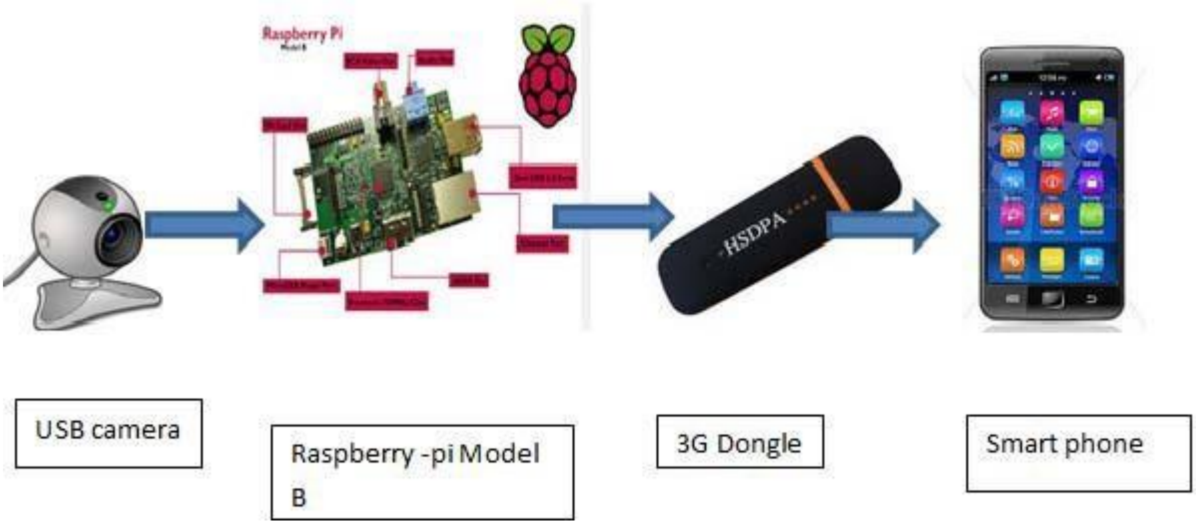


Figure 5: Raspberry Pi based Security System

As shown in the figure above, the whole architecture of the system is composed of five modules namely:

i. Raspberry Pi SBC model
ii. Pi camera/USB Camera
iii. PIR sensor
iv. Wi-Fi Dongle
v. Monitor/laptop

Why Raspberry Pi based Security Systems?

- Cost of implementation of such a system.
- The Raspberry Pi is also a very versatile device whose functionality is not limited. It can be extended from being merely a security device to temperature control device, automatic lighting and proxy server.
- An IP Camera system has the ability to distribute alarm messages over the internet as well as the Raspberry Pi based security system. However, the cost of an IP Camera makes it not easily affordable to small home owners. Thus they can be deployed in large industrial set ups, defence forces, police departments etc.

- Larger memory capacity compared to other microcontroller rendering it more effective especially when trying to interface with other modules e.g. camera, monitors, motion sensors, mouse and keyboard.
- Raspberry Pi has an extendable SD card storage and can be expanded to suit the needs of an individual.
- The Raspberry Pi has a ethernet port and Wi-Fi module to connect it to the internet.
- A CCTV surveillance system is expensive to purchase and install compared to the system in question. It requires a DVR system to connect it to the data networks through TNP/IP. A DVR on its own is very expensive. Hence such a system may not be afforded by low income home owners.

The Raspberry Pi

A raspberry pi microcontroller is a fully functional credit sized computer which can be plugged into a monitor. It is based on a Broad-com system on chip with an ARM processor of around 1-2 GHz, a GPU and a RAM.
It also has Wi-Fi enabled which is necessary for most IoT application and TCP/IP communication. This type of communication is used intensively when attempting to SSH (log) into the Raspberry pi server and be able to access the microcontroller files.

Raspberry Pi Pinout

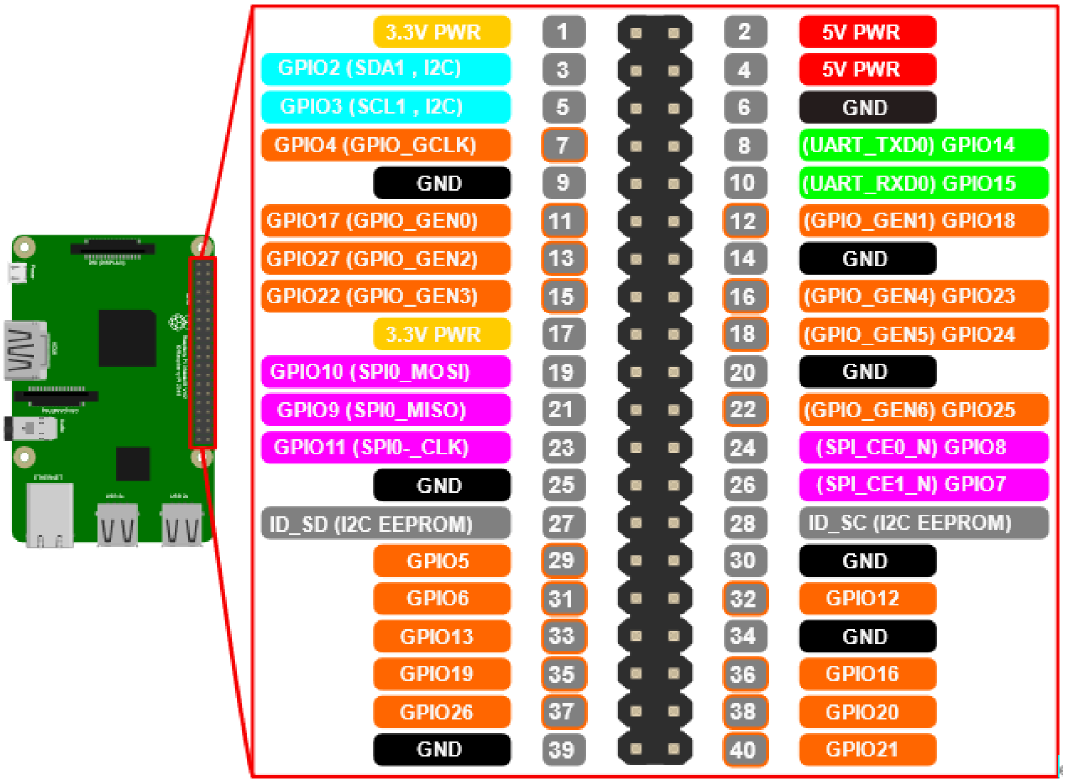

3.3V PWR 1 2 5V PWR
GPIO2 (SDA1 , I2C) 3 4 5V PWR
GPIO3 (SCL1 , I2C) 5 6 GND
GPIO4 (GPIO_GCLK) 7 8 (UART_TXD0) GPIO14
GND 9 10 (UART_RXD0) GPIO15
GPIO17 (GPIO_GEN0) 11 12 (GPIO_GEN1) GPIO18
GPIO27 (GPIO_GEN2) 13 14 GND
GPIO22 (GPIO_GEN3) 15 16 (GPIO_GEN4) GPIO23
3.3V PWR 17 18 (GPIO_GEN5) GPIO24
GPIO10 (SPI0_MOSI) 19 20 GND
GPIO9 (SPI0_MISO) 21 22 (GPIO_GEN6) GPIO25
GPIO11 (SPI0-_CLK) 23 24 (SPI_CE0_N) GPIO8
GND 25 26 (SPI_CE1_N) GPIO7
ID_SD (I2C EEPROM) 27 28 ID_SC (I2C EEPROM)
GPIO5 29 30 GND
GPIO6 31 32 GPIO12
GPIO13 33 34 GND
GPIO19 35 36 GPIO16
GPIO26 37 38 GPIO20
GND 39 40 GPIO21

Figure 6: Raspberry Pi Pinout

PINS	FUNCTIONALITY
2 and 4	5V Power Input
1 and 17	3.3V Power Input
6, 9, 14, 20, 25, 30, 34, 39,	Ground pins
The rest	GPIO pins

Table 2: Raspberry Pi Pins Functionality

GPIO2 and GPIO3 have fixed pull-up resistors.

Software PWM can be used on any pin but hardware PWM can only be used on GPIO12, GPIO13, GPIO18 and GPIO19

SPI communication can be used on GPIO14 and GPIO15

I2C communication can be used on GPIO2 (Data) and GPIO2 (Clock)

GPIO18 (PCM_CLK) regulates data transfer speed between raspberry and other external devices.

Programming the Raspberry Pi

To enable communication with the outside world, the Raspberry Pi has to be programmed with a suitable programming language. These languages include Java, FOTRAN, Pascal, Python, C, C++ . Each language has its own syntax and semantics. Python was used as it is the language used in Linux systems.

Raspberry Pi Operating Systems

An operating system makes Raspberry Pi run. Since Raspberry Pi is based on Linux, optimum performance of Raspberry Pi can be achieved if it is therefore operated in this environment. Raspbian provides more than a pure OS: it comes with over 35,000 packages, precompiled software bundled in a nice format for easy installation on Raspberry Pi.

Ultrasonic Proximity Sensor

It works at a frequency of 40 kHz. It uses two specially made ultrasonic transducers: One transducer emits 40kHz sound, while the other receives 40kHz sound and converts it into electrical variation of the same frequency. Ultrasonic proximity sensors operate by emitting and receiving high-frequency sound waves.

Operating Principle

There are two basic modes of operation: opposed mode and diffuse (echo) mode. In opposed mode, one sensor emits the sound wave and another, mounted opposite the emitter, receives the sound wave. In diffuse mode, the same sensor emits the sound wave and then listens for the echo that bounces off an object.

Pros and Cons

Pros

Ultrasonic proximity sensors can detect a variety of objects regardless of its material or surface properties. They are useful for object detection over intermediate distances, on the order of several feet. They can also operate in a wide variety of operating conditions.

Cons

At close proximity they possess a blind spot where objects are not detected.

Network Protocols

They enable the exchange of information across the internet and work in the of every web application.

The raspberry would be able to update the database using the company’s API. Therefore it would use HTTPS protocol to establish secure and encrypted communication between it and the API. HTTPS is based on TCP/IP network protocol.

There are 12 common network protocols. Network protocols related to HTTPS are:

Internet Protocol (IP)

It provides a unique identity to each node on the computer network. The identity is an IP address of when a node sends and receives data. the data gets spliced into packets; one for the sender and one for the recipient. After the packet leaves the sender, it goes to a gateway that directs it in the through gateways until they reach the proper direction. Packets continue to travel reach their destinations.

There are 2 versions of IP protocol: IPv4 and IPV6. IPv4 uses 32 bits to create an IP address while IPv6 to create an IP address.

Transmission Control Protocol (TCP)

It arranges packets in order so that IP can deliver them to their destination. This is because IP can send the packets out of order, therefore TCP amends this before IP delivers the packets. TCP also detects errors in the sending process (if any packets are missing based on TCP's numbered system) and requires IP to retransmit those packets before IP delivers the data to its destination.

User Datagram Protocol (UDP)

Just like TCP, it works with IP to transmit time-sensitive data. However, it doesn't wait for all packets to arrive or organize the packets. It transmits all pockets even if some haven't arrived.

File Transfer Protocol (FTP)

It is used to connect to remote computers, list shared files, and either upload or download files between local and remote computers.

It runs over TCP, which provides a connection-oriented, guaranteed data delivery service.

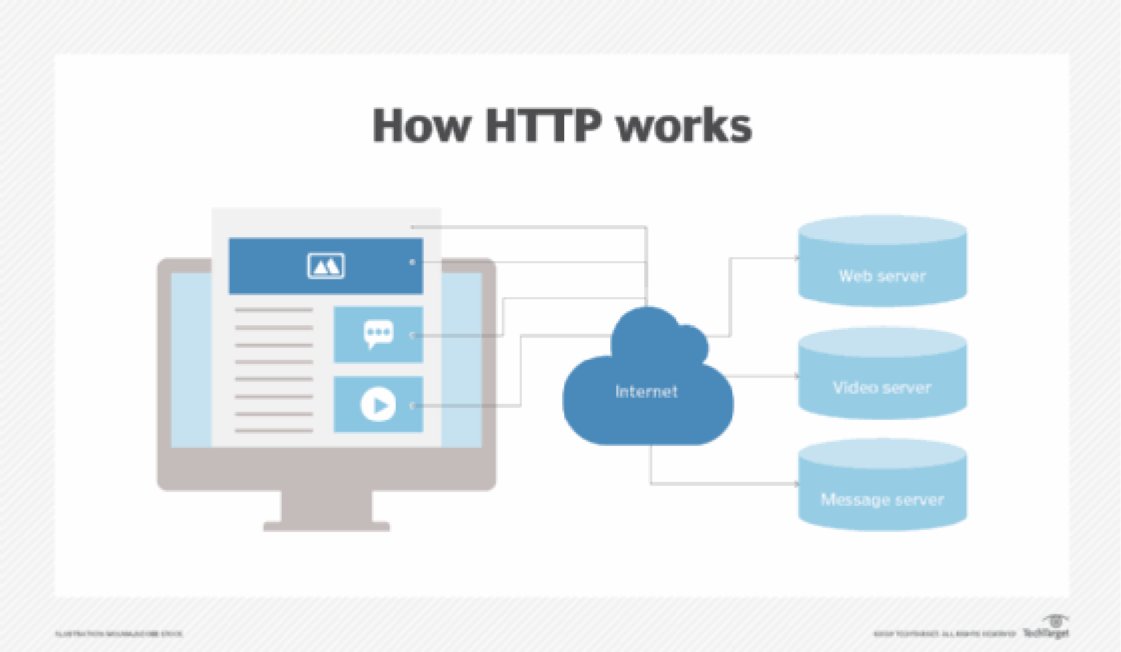
This is a command channel and a data channel to communicate and exchange files respectively. Request of files is through the command channel and access to download, edit and copy files is. data channel through the data channel.

Hypertext Transfer Protocol (HTTP)

It is a file sharing protocol that runs over TCP/IP, although primarily works over the web browsers.

When a user requests a web Resource, it is requested using HTTP. When this resource /address is entered into a web browser. DNS is called to resolve the Fully Qualified Domain Name (FDQN) to an IP address.

When the address is resolved, a HTTP get request is sent to the web Server. The web server responds with a HTTP send an IP address. - HTTP uses TCP for communication between client's response. servers. It operates on port 80.



Hypertext Transfer Protocol Secure (HTTPS)

It offers certificate-based mutual authentication between the client and the server. It validates both client and server identities and encrypts all data packets sent during a session.

CHAPTER THREE

METHODOLOGY

Design Hardware (System Modules Set Up and Configuration)

The system modules consist of:

- Raspberry Pi Model B+ controller,
- Ultrasonic proximity sensor
- Webcam
- 32 GB MicroSD card
- 220 Ohms resistor
- USB powered cable.

The model Raspberry Pi Model B+ was chosen to implement the project. It has merits over other models in that it has increased number of USB ports and large number of GPIO pins. Moreover, this piece of hardware was available.

Setting Up Operating System, Internet connection and SSH access on the Pi

Raspbian Debain ‘Buster’ image was written into the 32GB Micro SD card. This was the operating system chosen to run on the Pi because the OS has been optimized and ported to the Raspberry Pi ARM architecture. This OS has very good integration with the hardware and comes preloaded with a GUI and development tools.

Internet was necessary in so that the Pi can communicate over network protocols and thus allow for installation of necessary Python packages. The Pi would be using one of the Wi-Fi routers at the company.

Since the broadcast router uses Dynamic Host Configuration Protocol (DHCP) to dish out IP addresses to devices connected to it, it was necessary to change the IP address of the Pi from static to dynamic. This was done by editing the network interface file in the root folder of the Pi’s local storage.

<u>Steps carried out</u>

- ❖ A terminal was opened in the memory card's root folder.
- ❖ Using the terminal, a file named ssh was created. Its purpose was to start the server when the memory card would be inserted into the raspberry pi.

- A configuration file by the name "wpa_supplicant.conf" was created and Wi-Fi configuration code entered into the file. This was to help the raspberry pi access local Wi-Fi.
- The memory card was ejected from the PC and inserted into the raspberry pi.
- Using a software called Advanced IP scanner, the Ip address of the raspberry pi was found.
- Using command terminal on pc, the pi server was accessed using the command line "ssh pi@ ipAddressofpi". This was to allow it communicate with the Raspberry Pi.

Using Putty software (an SSH client) or command terminal one can remotely access and control a raspberry.

Format of the network interface file “wpa_supplicant.conf” was:

```
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev
update_config=1
country=KE
network={
ssid="GEARBOX MEMBERS"
psk="123456789"
scan_ssid=1
}
```

Where ssid is the name of Wi-Fi that raspberry is to connect to and psk is the Wi-Fi’s password.

After the Pi boots up, it would save the file in its local storage at location /etc/network/

Enabling the Webcam

It was hooked to the raspberry pi through USB port which is an extremely fast port. To configure and enable the webcam, the following commands were executed at the Command line interface (CLI) of the raspberry pi:

```
sudo apt_get update
sudo apt_get upgrade
sudo raspi-config
sudo apt install fswebacam
```

The following line of code was used to capture images using the USB webcam.

```
fs webcam -r 1920 x1080 -p YUYV - S30 -D2 -F2 test.jpg
```

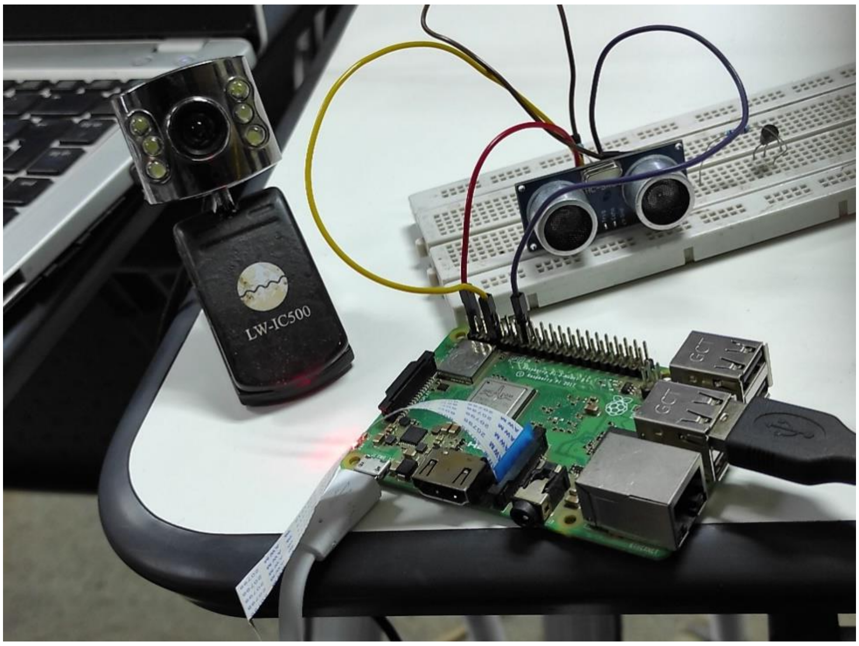
-r 1920 x1080	is the resolution one wanted the webcam to use while capturing an image
-p YUYV	is for the webcam to capture an image using its maximum resolution.
- S30	is to skip the first 30 frames for clarity of the image
-D2	is for the webcam to delay for 2 seconds before capturing an image.
-F2	is to capture 2 frames and combine to one image. This could reduce visual noise on stationary objects.

Table 3: Capture image using webcam Code Explanation

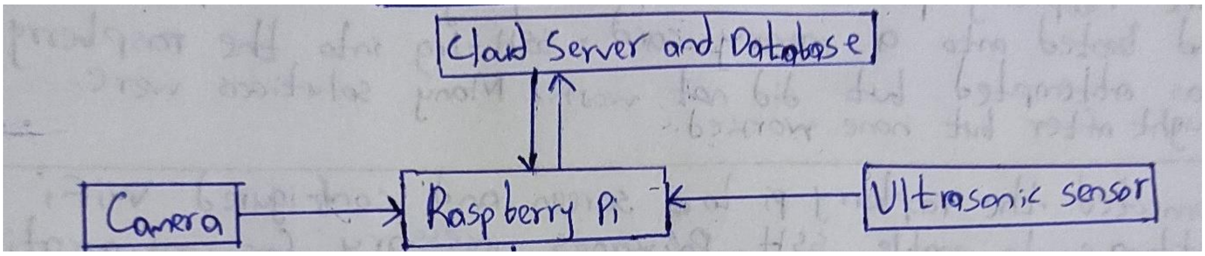
Hardware Architecture

Hardware System

- Raspberry Pi
- Cooling fan
- Memory Card
- HC-SR04 Ultrasonic proximity sensor
- 220 Ohms resistor
- Plastic casing

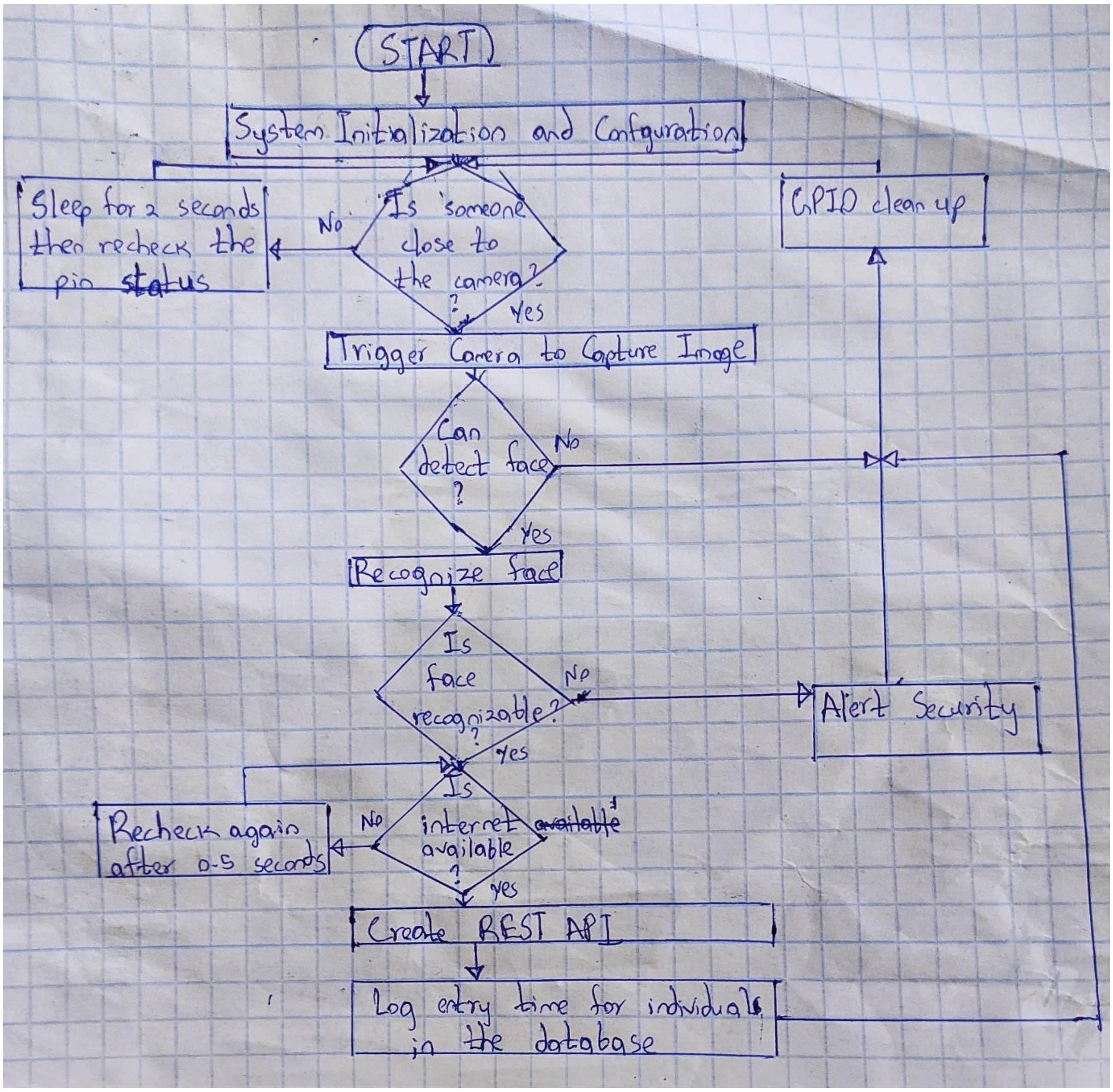


Block Diagram for Raspberry Pi Based Facial Recognition Security System



Design Software

Flowchart of the Raspberry pi based Facial Recognition Security System


START
System Initialization and Configuration
Sleep for 2 seconds then recheck the pin status
No
Is someone close to the camera?
Yes
GPIO clean up
Trigger Camera to Capture Image
Can detect face?
No
Yes
Recognize face
Is face recognizatle?
No
Yes
Alert Security
No
Is internet available?
~~available~~
Yes
Recheck again after 0.5 seconds
Create REST API
Log entry time for individuals in the database

<u>System initialization and configuration</u>

This involved the following tasks:

- Importing Python libraries and packages. These libraries are predefined and help in making the interfaced modules work properly.
- Webcam setting and configuration.
- GPIO settings and pin initialization: (The echo pin of the ultrasonic proximity sensor was set to input mode while the trigger pin was set to output mode.
  - In order read the value of any GPIO pin, this command is used; GPIO.input(pin).
  - In order read the value of any GPIO pin, this command is used; GPIO.output(pin)

Also creation of a server that would be able to communication with the company's API.

Code Listing for Integration of Ultrasonic Sensor and Webcam using Pi

```
import RPi.GPIO as GPIO
import time

GPIO.setmode(GPIO.BCM)
TRIG = 4
ECHO = 18

GPIO.setup(TRIG, GPIO.OUT)
GPIO.setup(ECHO, GPIO.IN)

GPIO.output(TRIG, True)
time.sleep(0.0001)
GPIO.output(TRIG, False)

while GPIO.input(ECHO) == False:
    start = time.time()

while GPIO.input(ECHO) == True:
    end = time.time()

sig_time = end-start

#cm:
distance = sig_time / 0.000058   #inches: 0.000148
print('Distance: {} cm'.format(distance))
fswebcam -r 1920x1080 -p YUYV -S 30 -D 2 -F 2 test3.jpg
time.sleep(3)

GPIO.cleanup()
```

OpenCV – Python Image Processing

OpenCV is a very powerful machine learning tool used to analyse images and video files.
It aids a lot in the execution and accuracy of facial image detection and recognition.
The basic processing procedure to be followed is detailed in the code listing below.

Full Code Listing

Face Detection

```
import numpy as np
import cv2
faceCascade = cv2.CascadeClassifier('Cascades/haarcascade_frontalface_default.xml')
cap = cv2.VideoCapture(0)
cap.set(3,640) # set Width
cap.set(4,480) # set Height
while True:
    ret, img = cap.read()
    img = cv2.flip(img, -1)
    gray = cv2.cvtColor(img, cv2.COLOR_BGR2GRAY)
    faces = faceCascade.detectMultiScale(
        gray,
        scaleFactor=1.2,
        minNeighbors=5,
        minSize=(20, 20)
    )
    for (x,y,w,h) in faces:
        cv2.rectangle(img,(x,y),(x+w,y+h),(255,0,0),2)
        roi_gray = gray[y:y+h, x:x+w]
        roi_color = img[y:y+h, x:x+w]
    cv2.imshow('video',img)
    k = cv2.waitKey(30) & 0xff
    if k == 27: # press 'ESC' to quit
        break
cap.release()
cv2.destroyAllWindows()
```

Face Recognition Trainer

```
import cv2
import numpy as np
from PIL import Image
import os
# Path for face image database
path = 'dataset'
recognizer = cv2.face.LBPHFaceRecognizer_create()
detector = cv2.CascadeClassifier("haarcascade_frontalface_default.xml");
# function to get the images and label data
def getImagesAndLabels(path):
    imagePaths = [os.path.join(path,f) for f in os.listdir(path)]
    faceSamples=[]
    ids = []
    for imagePath in imagePaths:
        PIL_img = Image.open(imagePath).convert('L') # convert it to grayscale
        img_numpy = np.array(PIL_img,'uint8')
        id = int(os.path.split(imagePath)[-1].split(".")[1])
        faces = detector.detectMultiScale(img_numpy)
        for (x,y,w,h) in faces:
            faceSamples.append(img_numpy[y:y+h,x:x+w])
            ids.append(id)
    return faceSamples,ids

faces,ids = getImagesAndLabels(path)
recognizer.train(faces, np.array(ids))
```

Face Recognition

```
import cv2
import numpy as np
import os
recognizer = cv2.face.LBPHFaceRecognizer_create()
recognizer.read('trainer/trainer.yml')
cascadePath = "haarcascade_frontalface_default.xml"
faceCascade = cv2.CascadeClassifier(cascadePath);
font = cv2.FONT_HERSHEY_SIMPLEX
#iniciate id counter
id = 0
# names related to ids: example ==> Marcelo: id=1,  etc
names = ['None', 'Ben', 'Frank, 'Liza', 'Mary', 'Mercy']
# Initialize and start realtime video capture
cam = cv2.VideoCapture(0)
cam.set(3, 640) # set video widht
cam.set(4, 480) # set video height
# Define min window size to be recognized as a face
minW = 0.1*cam.get(3)
minH = 0.1*cam.get(4)
while True:
    ret, img =cam.read()
    img = cv2.flip(img, -1) # Flip vertically
    gray = cv2.cvtColor(img,cv2.COLOR_BGR2GRAY)

    faces = faceCascade.detectMultiScale(
        gray,
        scaleFactor = 1.2,
        minNeighbors = 5,
        minSize = (int(minW), int(minH)),
       )
    for(x,y,w,h) in faces:
        cv2.rectangle(img, (x,y), (x+w,y+h), (0,255,0), 2)
        id, confidence = recognizer.predict(gray[y:y+h,x:x+w])
        # Check if confidence is less them 100 ==> "0" is perfect match
        if (confidence < 100):
            id = names[id]
            confidence = "  {0}%".format(round(100 - confidence))
        else:
            id = "unknown"
            confidence = "  {0}%".format(round(100 - confidence))
        cv2.putText(img, str(id), (x+5,y-5), font, 1, (255,255,255), 2)
        cv2.putText(img, str(confidence), (x+5,y+h-5), font, 1, (255,255,0), 1)

    cv2.imshow('camera',img)
    k = cv2.waitKey(10) & 0xff # Press 'ESC' for exiting video
    if k == 27:
        break
cam.release()
cv2.destroyAllWindows()
```

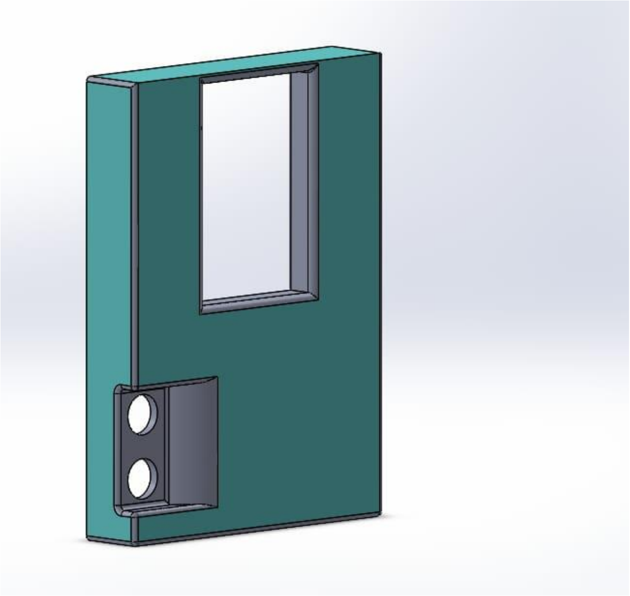
Casing Design and 3D print

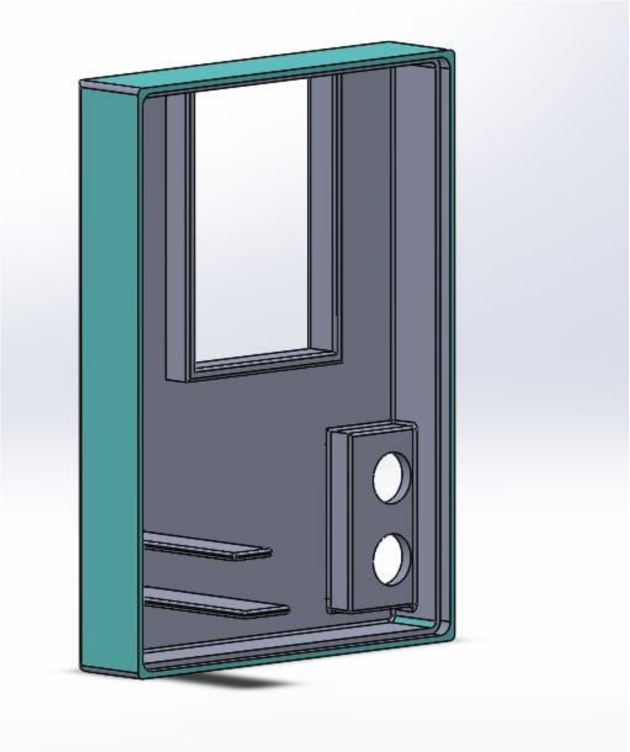
Production of a 3D model using computer aided design (CAD) software is referred to as CAD Design. Solidworks was used to model a 3D casing for the facial recognition security system.
After completion an thorough review of the CAD model, it was 3D printed. 3D printing process:

- The CAD file was converted to STL format(Standard tessellation language).
- The STL file was copied to an AMMachine(a computer that controls the 3D printer). The size and orientation for printing iwas selected.
- Machine Setup. Each machine has its own requirements for how to prepare for a new print job. This includes refilling the polymers, binders and other consumables the printer will use. It also covers adding a tray to serve as a foundation.
- Automatic Build. The machine melts the polymer supplied to it, then cools it to produce a layer of polymer on the path pre-configured to draw on. Each layer is usually about 0.1 mm thick, though it can be much thinner or thicker. Depending on the object’s size, the machine and the materials used, this process could take hours or even days to complete. The machine is checked periodically to make sure there are no errors.
- After completion of printing, the painted object was removed from the machine.
- Post processing of the printed object. This could include brushing off any remaining powder or bathing the printed object. The new print may be weak during this step since some materials require time to cure, so caution might be necessary to ensure that it doesn’t break or fall apart.

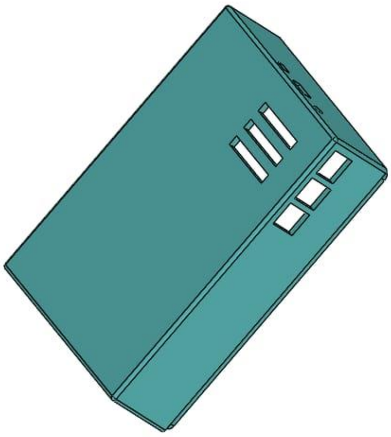
Casing Design

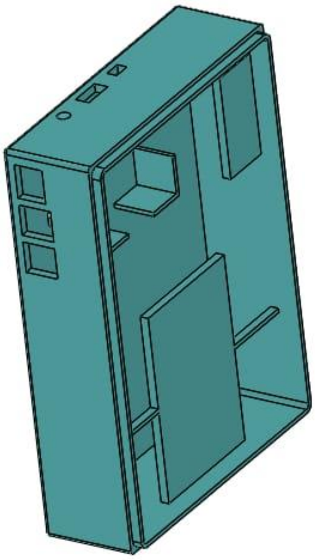
Male Half



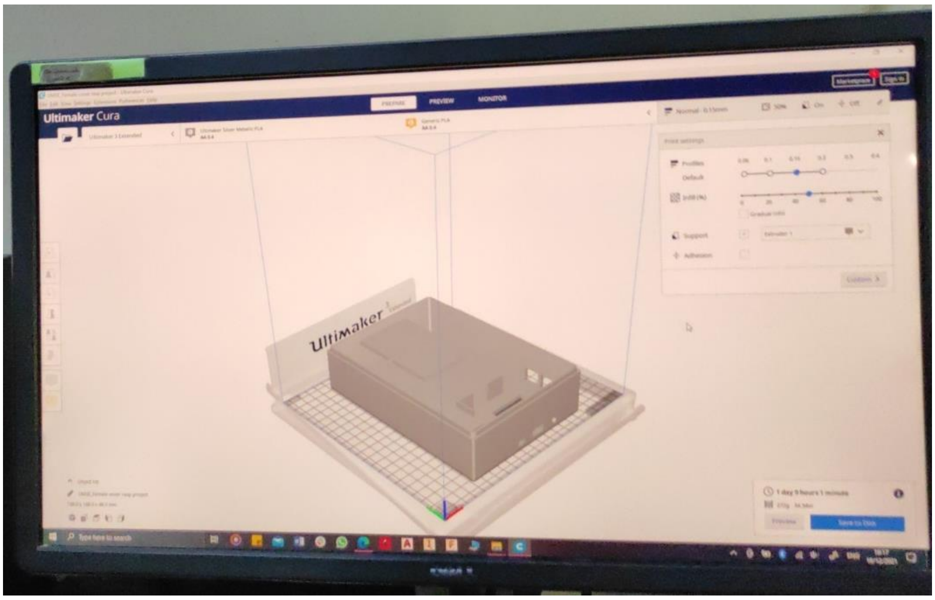


Female Half





Joined



Normal - 0.15mm 50% On Off

Print settings

Profiles 0.06 0.1 0.15 0.2 0.3 0.4
Default

Infill (%) 0 20 40 60 80 100
□ Gradual infill

Support ☑ Extruder 1

Adhesion □

1 day 9 hours 1 minute

CHAPTER FOUR

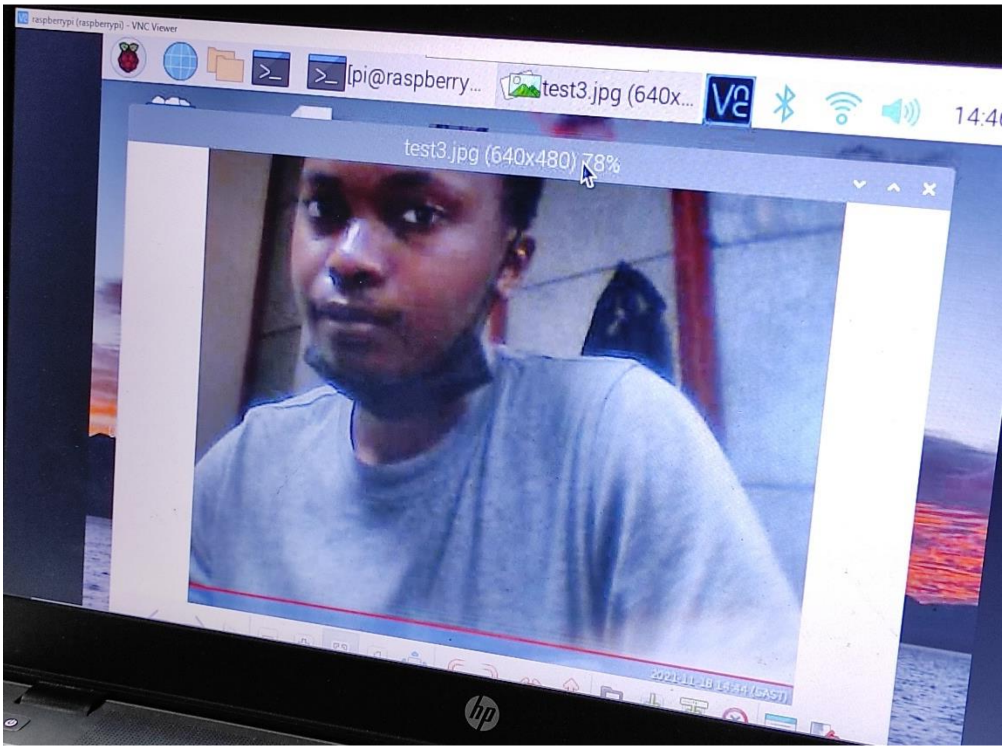
RESULTS

Ultrasonic sensor Receiver and Face Detection and Recognition success against distance from system

Table 4: Modules success against distance from security system

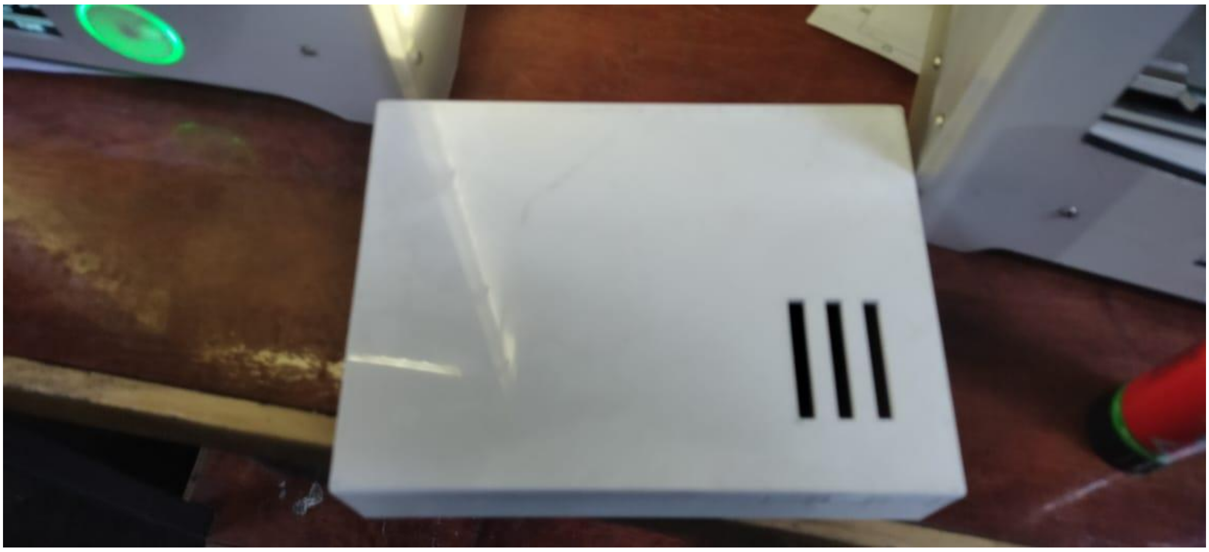
Distance in meters	Ultrasonic sensor receiver	Face Detection Successful	Face Recognition Successful
0.25	HIGH	YES	YES
0.5	HIGH	YES	YES
0.75	HIGH	YES	YES
1.0	HIGH	YES	YES
1.25	HIGH	YES	YES
1.5	HIGH	YES	YES
2.0	HIGH	YES	NO
2.5	HIGH	YES	NO
3.0	HIGH	YES	NO
3.5	HIGH	YES	NO
4.0	HIGH	YES	NO
4.5	LOW	NO	NO
5.0	LOW	NO	NO

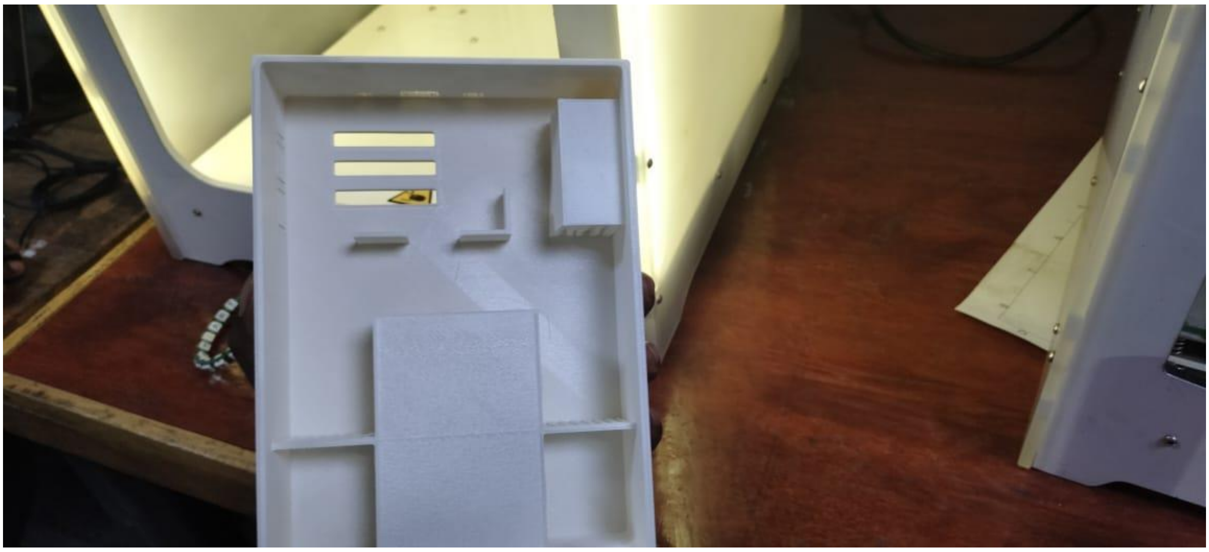
Face Detection using webcam maximum resolution



Casing Design

The casing design was successfully 3D printed.





ANALYSIS OF THE RESULTS

As from the table;

Python scripts for face detection, face recognition trainer and face recognition worked.
It can be depicted that after 1.5 metres, face recognition is not successful as the clarity of the frame taken is not that clear.
The HC-SR04 maximum range is 4m.
Face detection is no longer successful after 4 metres as accuracy of face detection decreases with increase in distance from the camera.

This shows that the HC-SR04 is critical in the system as it is used to find the perfect balance where face detection and face recognition will be precise and successful. This is by setting a distance value that will turn on the webcam and bring out perfection in face detection and recognition. As all the other modules depend on the HC-SR04, if it fails, the whole security procedure as designed shall fail.

CONCLUSION

The project designed and implemented a security system based on the Raspberry Pi. The aspects of the system are: proximity detection using a ultrasonic sensor, image processing using a Pi Camera and sending out JSON data through web RPC. The goals of the project were achieved.

Also, the attachees developed soft skills such as critical thinking and team work by solving the problems occurred in the project in teams and by using specifications and constraints provided to them.

RECOMMENDATIONS

The following are recommended**:**

- Major improvements on the system and webRPC security features.
- Major improvements on the system processor speed for live video streaming for surveillance by the security department.
- The system requires to be remotely controlled. Hence, future explorations should focus much more on the same.

CHAPTER FIVE

REFERENCES

1. B. J. Glenn, *Computer Science: An Overview,* 11th ed. Edwards Brothers.
2. F. C. Mahima and A. Prof. Gharge, “Design and Develop Real Time Video Surveillance System Based on Embedded Web Server Raspberry PI B+ Board. International Journal of Advance Engineering and Research Development (Ijaerd), NCRRET.,” pp. 1–4, 2015.
3. Zhichao Lian, Meng Joo Er, and Juekun Li ―A Novel Face Recognition Approach under Illumination Variations Based on Local Binary Pattern―A. Berciano et al. (Eds.): CAIP 2011, Part II, LNCS 6855, pp. 89–96, 2011.
4. Zhihua Xie1, Guodong Liu1, and Zhijun Fang2 ―Face Recognition Based on Combinationof Human Perception and Local Binary Pattern ‖ Y. Zhang et al. (Eds.): IScIDE 2011, LNCS 7202, pp. 365–373, 2012.© SpringerVerlag Berlin Heidelberg 2012
5. Zhiming Qian, Chaoqun Huang, and Dan Xu, ―Automatic Face Recognition Systems Design and Realization ‖ The Sixth ISNN 2009, AISC 56, pp. 323–331. Springer-Verlag Berlin Heidelberg 2009