Abstract

This project is part of Microsoft Hack the Home initiative, which provides the makers with free, open-source components for effortless interfacing with devices and services that makers use most to hack their homes. Home security systems are a growing field of projects for Makers. A self based system is not only less expensive than a bulky professional installation, but it also allows for total control and customization to suit personal needs. This project deals with the design and implementation of Secure locking Automation using Raspberry Pi for Door unlocking to provide essential security to our homes, bank lockers and associated control operations and send security alert through the GSM module. Raspberry Pi operates and controls the video camera for capturing it for turning ON a relay for door unlock. The module contains a secured face recognizer for automatic door opening. Since Raspberry Pi is not compatible with GSM we use an Arduino Controller to control the operation of GSM to send interruption messages to the owner.

Contents

List of Figures

Chapter 1

INTRODUCTION

Face, the most distinguishable feature of human body, making you the "unique you", not only gives you an individual identity, but can also save you from security breaches and fraud transactions, can take care of your personal data, and prevent your PC, wireless network from plausible security threats. Unlike the world of facebook, where you can wear different face every day, here it is the uniqueness of your face that makes all the difference. Face Recognition is the fast track technology which has brought the world at your finger tips. The easier life is getting day by day, the more complex it is becoming to escape from the traps intended to crack and get access to your private data. The ubiquitous methods of user id and password combinations, access cards are no longer free from security threats. Such scenario demands an infallible solution, the one that cannot be hacked, shared or stolen and that solution is present with us, as an innate gift of nature, the human biological characteristics. 'Biometrics' is the study of measurable biological characteristics. It also consists of several authentication techniques based on unique physical characteristics such as face, fingerprints, iris, hand geometry, retina, veins, and voice. "Face recognition" is a computer based security system capable of automatically verifying or identifying a person. It is one of the various techniques which are Biometrics. Biometrics identifies or verifies a person based on individual's physical characteristics by matching the real time patterns against the enrolled ones.

1.1 MOTIVATION

The motivation behind this project is that facial detection has amplitude of possible applications. From common household objects like digital cameras that automatically focus on human faces to security cameras that actually match a face to a person's identity. Webcams are often used as a security measure for locking a personal computer. The webcam's facial recognition technology allows for the computer to be accessible to the user only if it recognizes their face.

Cameras can also use this technology to track human faces and keep a count of the number of people in a shot or in a certain location or even coming in through an entrance. This technology can be further narrowed down to the recognition and tracking of eyes. A switch or a button would save power by dimming a screen if viewer is not looking.

1.2 INTRODUCTION TO THE AREA OF WORK

Facial recognition is a biometric method of identifying an individual by comparing live capture or digital image data with the stored record for that person. Most current facial recognition systems work with numeric codes called faceprint. Such systems identify nodal points on a human face. In this context, nodal points are end points used to measure variables of a person's face, such as the length or width of the nose, the depth of the eye sockets and the shape of the cheekbones. These systems work by capturing data for nodal points on a digital image of an individual's face and storing the resulting data as a faceprint. The faceprint can then be used as a basis for comparison with data captured from faces in an image or video.

1.3 PROPOSED WORK

The aim of our project is to provide a high security system using face recognition on Raspberry Pi board and send an alert to the authorised person via GSM module, this will increase the security of our project. The proposed work is as follows:

1. Interfacing of camera module to capture live Face image.
2. Create a database of authorized person
3. Capture current face, save it and compare with data base image.
4. Interfacing Raspberry Pi with Arduino Controller to interface GSM module to send security alert to Authorized person while unlocking the locked door.
5. Interface relay as an output module.

1.4 REASON FOR CHOOSING FACE RECOGNITION

There is multiple reasons that make us choose Face Recognition System from all the kinds of biometric, these are:

1. Physical interaction is not needed from the user.
2. It is more accurate and more secure.
3. We can use image capture device or any camera can be used.

Biometric-based techniques have emerged as the most promising option for recognizing individuals in recent years since, instead of authenticating people and granting them access to physical and virtual domains based on passwords, PINs, smart cards, plastic cards, tokens, keys and so forth, these methods examine an individual's physiological and/or behavioral characteristics in order to determine and/or ascertain his identity. Passwords and PINs are hard to remember and can be stolen or guessed; cards, tokens, keys and the like can be misplaced, forgotten or duplicated. Magnetic cards can become corrupted and unreadable. However, an individual's biological traits cannot be misplaced, forgotten, stolen or forged. Biometric-based technologies include identification based on physiological characteristics such as face, fingerprints, finger geometry, hand geometry, hand veins, palm, iris, retina, ear and voice and behavioral traits.

Chapter 2

HISTORICAL DEVELOPMENT AND LITERATURE SURVEY

2.1 HISTORICAL DEVELOPMENT[1]

Pioneer of Facial Recognition include Woody Bledsoe, Helen Chan Wolf, and Charles Bisson. During 1964 and 1965, Bledsoe, along with Helen Chan and Charles Bisson, worked on using the computer to recognize human faces. This project was labeled man-machine because the human extracted the coordinates of a set of features from the photographs, which were then used by the computer for recognition. Using a graphics tablet (GRAFACON or RAND TABLET), the operator would extract the coordinates of features such as the center of pupils, the inside corner of eyes, the outside corner of eyes, point of widows peak, and so on. From these coordinates, a list of 20 distances, such as width of mouth and width of eyes, pupil to pupil, were computed. These operators could process about 40 pictures an hour. When building the database, the name of the person in the photograph was associated with the list of computed distances and stored in the computer. In the recognition phase, the set of distances was compared with the corresponding distance for each photograph, yielding a distance between the photograph and the database record. The closest records are returned. Because it is unlikely that any two pictures would match in head rotation, lean, tilt, and scale (distance from the camera), each set of distances is normalized to represent the face in a frontal orientation. To accomplish this normalization, the program first tries to determine the tilt, the lean, and the rotation. Then, using these angles, the computer undoes the effect of these transformations on the computed distances. To compute these angles, the computer must know the three-dimensional geometry of the head. Because the actual heads were unavailable, Bledsoe (1964) used a standard head derived from measurements on seven heads. After Bledsoe left

PRI in 1966, this work was continued at the Stanford Research Institute, primarily by Peter Hart. In experiments performed on a database of over 2000 photographs, the computer consistently outperformed humans when presented with the same recognition tasks (Bledsoe 1968). Peter Hart (1996) enthusiastically recalled the project with the exclamation, "It really worked!" By about 1997, the system developed by Christoph von der Malsburg and graduate students of the University of Bochum in Germany and the University of Southern California in the United States outperformed most systems with those of Massachusetts Institute of Technology and the University of Maryland rated next. The Bochum system was developed through funding by the United States Army Research Laboratory. The software was sold as ZN-Face and used by customers such as Deutsche Bank and operators of airports and other busy locations. The software was "robust enough to make identifications from less-than-perfect face views. It can also often see through such impediments to identification as mustaches, beards, changed hair styles and glasses (even sunglasses)". In about January 2007, image searches were "based on the text surrounding a photo," for example, if text nearby mentions the image content. Polar Rose technology can guess from a photograph, in about 1.5 seconds, what any individual may look like in three dimensions, and claimed they "will ask users to input the names of people they recognize in photos online" to help build a database[citation needed]. Identix, a company out of Minnesota, has developed the software, FaceIt. FaceIt can pick out someone's face in a crowd and compare it to databases worldwide to recognize and put a name to a face. The software is written to detect multiple features on the human face. It can detect the distance between the eyes, width of the nose, shape of cheekbones, length of jawlines and many more facial features. The software does this by putting the image of the face on a faceprint, a numerical code that represents the human face. Face recognition software used to have to rely on a 2D image with the person almost directly facing the camera. Now, with FaceIt, a 3D image can be compared to a 2D image by choosing 3 specific points off of the 3D image and converting it into a 2D image using a special algorithm that can be scanned through almost all databases. In 2006, the performance of the latest face recognition algorithms was evaluated in the Face Recognition Grand Challenge (FRGC). High-resolution face images, 3-D face scans, and iris images were used in the tests. The results indicated that the new algorithms are 10 times more accurate than the face recognition algorithms of 2002 and 100 times more accurate than those of 1995. Some of the algorithms were able to outperform human participants in recognizing faces and could uniquely identify identical twins. U.S. Government-sponsored evaluations and challenge problems have helped spur over two orders-of-magnitude in face-recognition system performance. Since 1993, the error rate of automatic face-recognition systems has decreased by a factor of 272. The reduction applies to systems that match people with face images captured in studio or mugshot environments. In Moore's law terms, the error rate decreased by

one-half every two years. Low-resolution images of faces can be enhanced using face hallucination. Further improvements in high resolution, megapixel cameras in the last few years have helped to resolve the issue of insufficient resolution.

2.2 LITERATURE SURVEY

- The book “Art Of Electronics” by Paul Horowitz and Winfield Hill provides complete description of the basic electronic components and their working. This book covers many areas of circuit design, from basic DC voltage, current and resistance, to active filters and cillators, to digital electronics, including microproccessors and digital bus interfacing.
- “Face Recognition Using Eigenface Apporach” by Marijeta Slavkovic, Dubravka Jevtic published at “Serbian Journel Of Electrical Engineering” Vol. 9, No. 1, February 2012, 121-130. This paper gives detailed description about eigen values and Principle Component Analysis.

Chapter 3

COMPONENT SPECIFICATION[2]

3.1 RASPBERRY PI

3.1.1 HARDWARE

Raspberry Pi is the series of small single board computers developed in the United Kingdom by the Raspberry Pi, to promote the teaching on basic computer science in developing countries. The original model was far more popular than the anticipated selling, outside of its target market for uses such as robotics. The Peripheral is not included with the Raspberry Pi. But some of the accessories however have been included in the several official and unofficial bundles.

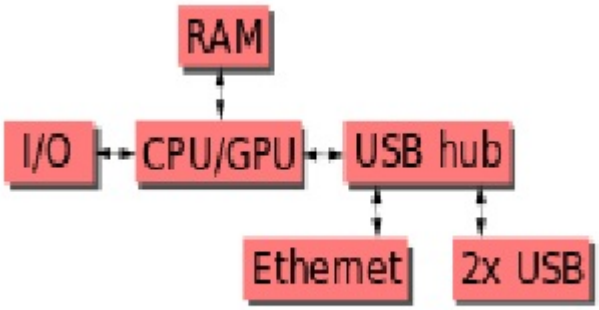


Figure 3.1: Hardware component.

Raspberry Pi hardware has been evolved through the several versions that the feature variations in memory capacity and peripheral device support. The block diagram shown in figure 3.1. depicts Models A, B, A+, and B+. The model A and A+, and the Pi Zero which lack the Ethernet and USB hub components. Ethernet adapter which is internally connected to the additional USB port. In the Model A, A+ and the Pi Zero, the USB port is connected directly to the

system on chip (SoC). On the Pi 2 Model B+ and the higher models contains the USB/Ethernet chip contains a five-point USB hub, of which the four ports are available, while the Pi 2 Model B only provides two ports. In the Pi Zero, the USB port is also connected directly to the SoC, but it also uses a micro USB (OTG) port.

3.1.2 PROCESSOR

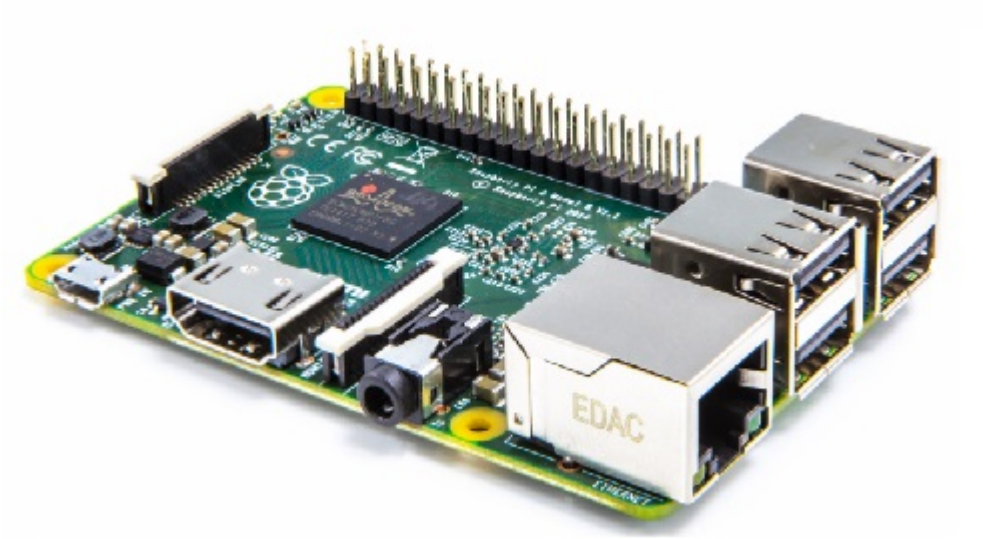


Figure 3.2: Raspberry Pi 2 processor

Raspberry Pi 2 processor in the figure 3.2. uses a 32-bit, 900 MHz quad core ARM Cortex-A7 processor. The Broadcom BCM2835 SoC which is used in the first generation Raspberry Pi that is somewhat equivalent to the chip that is used in the first generation Smartphone's which includes a 700 MHz, ARM1176JZF-S processor, a Video Core IV graphics processing unit (GPU), and also the RAM. It has the level 1 (L1) cache of 16 KB and a level 2 (L2) cache of 128 KB. Level 2 cache is used primarily by the GPU.

3.1.3 SPECIFICATIONS

Technical Specification:

1. 1GB RAM is available
2. Bluetooth Low Energy (BLE) on the board
3. 40pin extended GPIO

4. Upgraded switched Micro USB power source (now supports up to 2.4 Amps)
5. 4 x USB 2 ports
6. 4 pole Stereo output and Composite video port
7. Full size HDMI
8. CSI camera port for connecting the Raspberry Pi camera
9. DSI display port for connecting the Raspberry Pi touch screen display
10. Micro SD port for loading your operating system and storing data
11. Expected to have the same form factor has the Pi 2 Model B, however the LEDs will change position
12. Broadcom BCM2837 64bit Quad Core Processor powered Single Board Computer running at 1.2GHz.

3.2 GSM

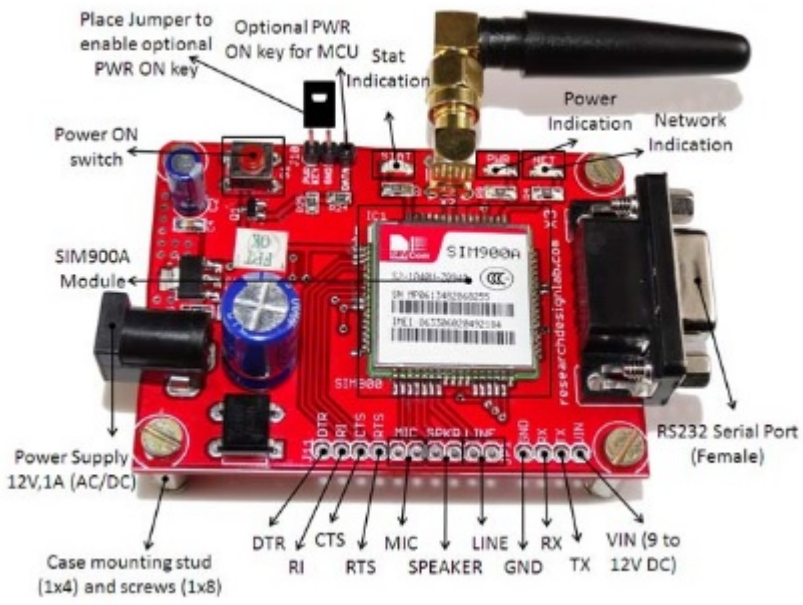


Figure 3.3: GSM module

GSM (Global System for Mobile Communications) is originally developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second generation

(2G) digital cellular networks which is used by mobile phones, was first deployed in Finland in December 1991. As of 2014, it has become the de-facto global standard for mobile communications with over 90% market share, it is operating in over 219 countries and territories. 2G networks are developed as a replacement for the first generation (1G) analog cellular networks, the GSM standard originally described as a digital, circuit-switched network optimized for full duplex voice telephony. This expanded over the time to include data communications, it was first expanded by circuit-switched transport, then by packet data transport via GPRS (General Packet Radio Services) and EDGE (Enhanced Data rates for GSM Evolution, or EGPRS). Subsequently, the 3GPP developed the third-generation (3G) UMTS standards, followed by the fourth-generation (4G). LTE Advanced "GSM" is a trademark owned by the GSM Association. It may be also referred to the most common voice codec used.

3.2.1 NETWORK STRUCTURE

The network is structured into number of discrete sections:

- Operations support system (OSS) – network maintenance
- GPRS Core Network – optional part allows packet-based Internet connections
- Network and Switching Subsystem – part of the network is most similar to the fixed network, sometimes just called the "core network"
- Base station subsystem – base stations and their controllers are explained

3.2.2 SPECIFICATIONS

- Quad-Band 850/ 900/ 1800/ 1900 MHz
- Weight: 3.4g Control via AT commands (GSM 07.07 ,07.05 and SIMCOM enhanced AT Commands)
- Compliant to GSM phase 2/2+

1. Class 4(2 W @850/ 900 MHz
2. Class 1(1 W @ 1800/1900MHz)

- Dimensions: 24*24*3mm
- Low power consumption: 1.0mA(sleep mode)

- Operation temperature: -40°C to +85 °C
- GPRS multi-slot class 10/8

3.2.2.1 Specifications for Data

- GPRS class 10: maximum 85.6 kbps (downlink)
- PBCCH support Coding schemes CS 1, 2, 3, 4
- CSD up to 14.4 kbps
- USSD Non transparent mode
- PPP-stack

3.2.2.2 Specifications for SMS via GSM/GPRS

- SMS cell broadcast Text and PDU mode
- Point to point MO and MT

3.2.2.3 Software features

- embedded TCP/UDP protocol FTP/HTTP
- 0710 MUX protocol

3.2.2.4 Special firmware

- MMS Java (cooperate with Isolation)
- Embedded AT

3.3 ARDUINO CONTROLLER

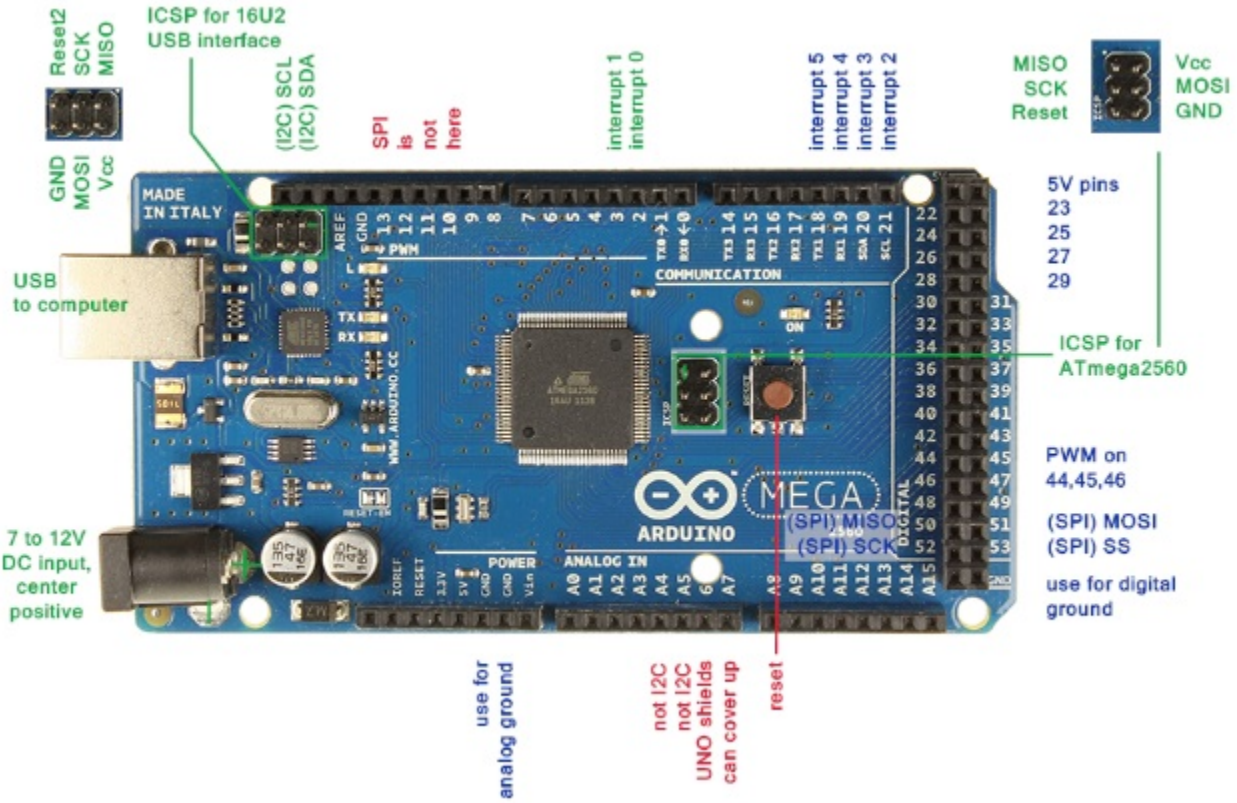


Figure 3.4: Arduino mega controller

Arduino Uno is a microcontroller board based on the ATmega328P as shown in the figure 3.4. It has 14 digital IO pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz quartz crystal, a USB connection, a power jack, an ICSP header and a reset button. It also contains everything needed to support the microcontroller; simply connect it to any computer with a USB cable or power it with AC-to-DC adapter or battery to get it started. Now you can tinker with your UNO without worrying too much about doing something wrong, worst case scenario is that you can replace the chip for a few dollars and start over again.

"Uno" means one in Italian and it was chosen to mark the release of Arduino Software (IDE) 1.0. The Uno board and version 1.0 of Arduino Software (IDE) is the reference versions of Arduino Uno, now it is evolved to newer releases. The Uno board is the first in the series of USB Arduino boards, and the reference model for the Arduino platform; for an extensive list of current, past or outdated boards see to the Arduino index of boards.

3.3.1 TECHNICAL SPECICATIONS

Microcontroller ATmega328P

- Operating Voltage 5V
- Input Voltage (recommended) 7-12V
- Input Voltage (limit) 6-20V
- Digital I/O Pins 14 (of which 6 provide PWM output)
- PWM Digital I/O Pins 6
- Analog Input Pins 6
- DC Current per I/O Pin 20 mA
- DC Current for 3.3V Pin 50 mA
- Flash Memory 32 KB(ATmega328P) of which 0.5 KB used by bootloader
- SRAM 2 KB(ATmega328P)
- EEPROM 1 KB(ATmega328P)
- Clock Speed 16 MHz
- Length 68.6 mm
- Width 53.4 mm
- Weight 25 g

Chapter 4

METHODOLOGY

4.1 HARDWARE WORKING[3][5]

4.1.1 BLOCK DIAGRAM

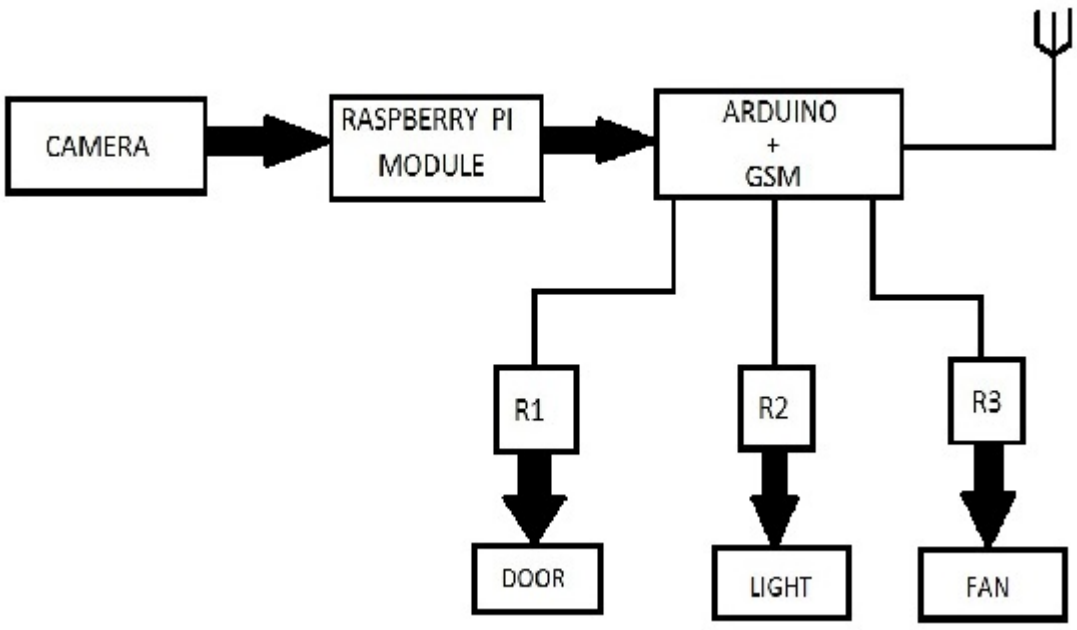


Figure 4.1: Block Diagram

The figure shown above is the basic block diagram of the raspberry Pi based face recognition system for door unlocking. Our project system can be operated in two different sections, i.e. one for capturing and creating data base and the other section is to capture the image and which is used for identifying or comparing the images in the data base. Here in the second section, we use Eigen faces methodology of face recognition for finding the matches.

- Camera module: Camera module is Pi camera which is interfaced to the raspberry Pi module. It is used for capturing an image and to send the captured image to the raspberry pi model.
- Raspberry Pi module: Raspberry Pi B+ module is a small computer board. When image is taken by the raspberry pi, it is then compared to Eigen face image. First time when we capture the image to create data base raspberry pi module captures six types of images to create a data base in the system and this data base is compared with the live captured images. After comparing two images, the output is positive or negative and then it gives command to GSM module through Arduino Controller.
- Arduino controller: Since Raspberry Pi used here is not compatible with GSM, we use Arduino Controller to control the operation of GSM to spend interrupt message to the owner.
- GSM module: GSM module is used to send a message to the authorities after analyzing the output. If the output is negative then a message, “An unauthorized person is trying to access the door” is sent to the authority person.
- Once the face is recognised, the lights and fan of the house will turn ON.

4.1.2 FLOWCHART

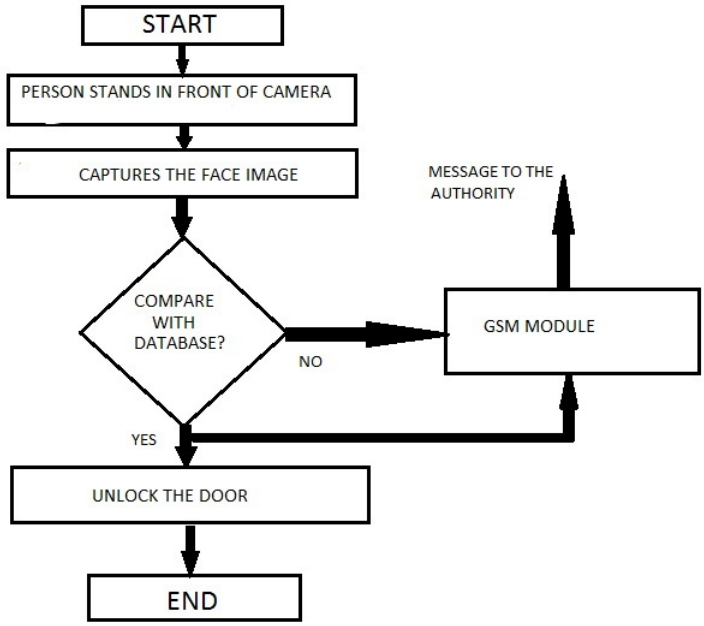


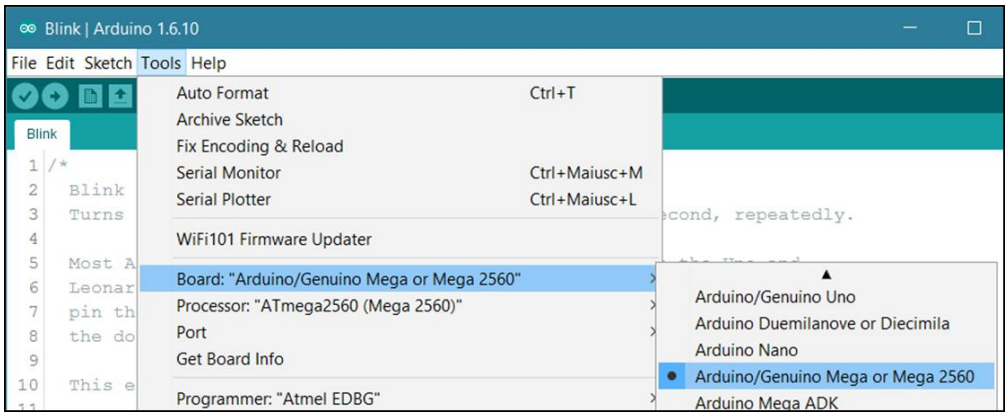
Figure 4.2: Flowchart

4.2 SOFTWARE WORKING[4][6]

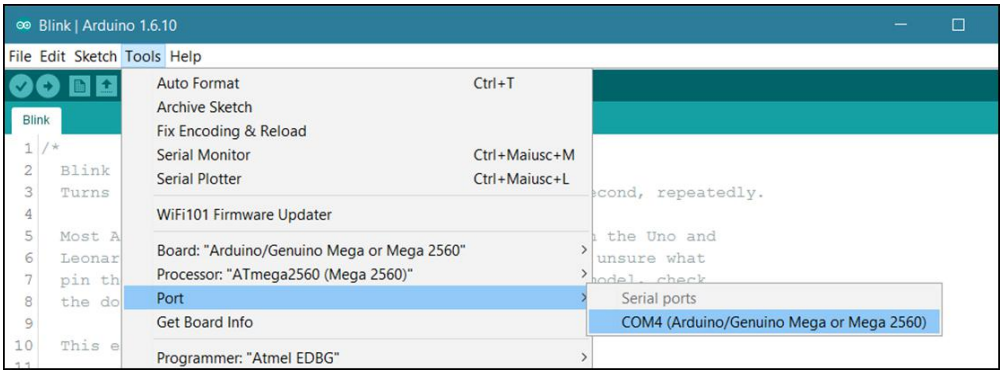
4.2.1 SOFTWARE PART OF AUDRIUNO

Connect your Mega2560 board with an A B USB cable; sometimes this cable is called a USB printer cable. The USB connection with the OC is necessary to program the board and not just to power it up. The Mega2560 automatically draw power from either the USB or an external power supply. Connect the board to your computer using the USB cable. The green power LED (labeled PWR) should go on.

Select your board type and port. You will need to select the entry in the Tools Board menu that corresponds to your Arduino or Genuino board. You have a Mega2560, therefore it has an ATmega2560 microcontroller, selected by default as processor.



Then select the serial device of the board from the Tools Serial Port menu. This is likely to be COM3 or higher(COM1 and COM2 are usually reserved for hardware serial ports). To find out, you can disconnect your board and re-open the menu; the entry that disappears should be the Arduino or Genuino Board. Reconnect the board and select that serial port.



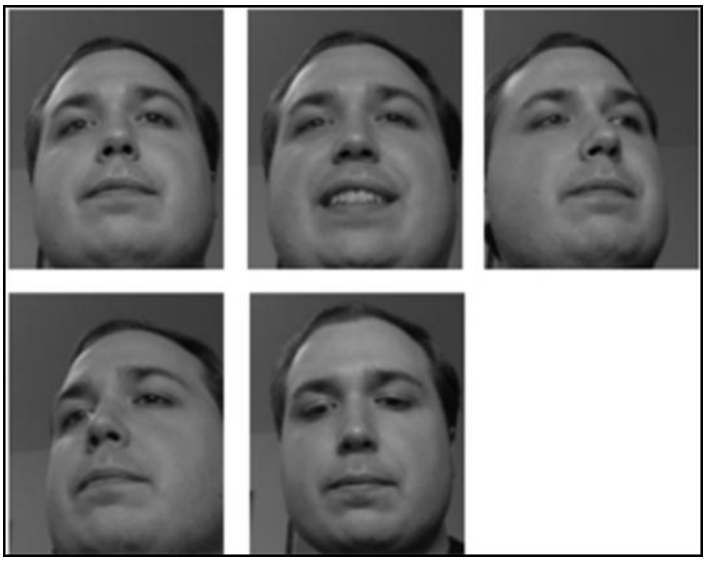
Upload the program now, simply click “upload” button in the environment. Wait a few seconds- you should select see the RX and TX leds on the board flashing. If the upload is successful, the messsage “done uploading” will appear in the status bar.

A few seconds after the upload finishes, you should see pin13 LED on the board start to blink(orange light).

4.2.2 SOFTWARE PART OF RASPBERRY PI

This project uses the Eigen faces algorithm in OpenCV to perform face recognition. To use this algorithm you will need to create a set of training data with pictures of face that are and are not allowed to open the door Included in this project is a large set of face images that are tuned for training with the face recognition algorithm. These faces make up the set of negative images which represent faces that are not allowed to open the door. You can see these images in the training/negative subdirectory of the project. To generate images of the person who will be allowed to open door, or positive training images, you can use the included b. This script will take pictures with the hardware and write them to the traini9ng/positive sub-directory (which will be created by the script if it does not exist). Open the file **capture.pgm** (located in the directory with scripts) in image editors to see the last image that was captured. Capturing positive training images. Press button or type c (and press enter) to capture an image. Press Ctrl-C to quit.

Try to take pictures of the face with different expressions, under different lighting conditions, and at different angles to build a better face recognition model. You can see the images I captured for my positive training data below.



Once you have captured a number of positive training images, you can run **train.py** script to perform the training. If it is still running, exit the **capture-positive.py** script by pressing Ctrl-C in the terminal session. Run **python train.py**

If you are curious you can examine image that are output by the training to visualize the Eigen faces of the model. Open the mean.png, positive_eigenface.png. And **negative_eigenface.png** files in an image viewer.

Mean Image

Positive Eigenface Image

Negative Eigenface Image

Eigenfaces generated from my training data.

The positive eigenface is a summary of the features that differentiate my face from the average or mean face. This face will be allowed to unlock the box.

The negative eigenface represents all the other faces in the training set. This face will not be allowed to unlock the box.

With the training.xml file which is generated, you will be ready to move on to configure the servo latch and software for the project. Once you have captured a number of positive training images, you can run the train.py script to perform the training. If it is still running, exit the **capture-positive.py** script by pressing Ctrl-C in the terminal session. Run **python tarin.py**

You can examine images that are output by the training to visualize the eigenfaces of the model. Open the mean.png, positive_eigenface.png, and negative_eigenface.png files in an image viewer.

.

4.2.3 PCA Approach to Face Recognition[4]

Principal component analysis transforms a set of data obtained from possibly correlated variables into a set of values of uncorrelated variables called principal components. The number of components can be less than or equal to the number of original variables. The first principal component has the highest possible variance, and each of the succeeding component has the highest possible variance under the restriction that it has to be orthogonal to the previous component. We want to find the principal components, in this case eigenvectors of the covariance matrix of facial images.

Chapter 5

ADVANTAGES AND DISADVANTAGES[8]

5.1 ADVANTAGES

5.1.1 Offers a Non-Contact Process

One of the top benefits of using bio metric face recognition over other forms of face technology is that this type of biometrics offers a non-contact process. This science makes it easy to capture information from people with biometrics facial technology, since images of the person's face can easily be captured, even from a distance.

5.1.2 Fast and Accurate Results:

Another of the benefits that can be enjoyed with facial recognition biometrics is fast and accurate results. When using biometric face recognition systems, users are able to enjoy high recognition rates and short processing times, making these systems an effective option. Most biometric systems also provide the ability to recognize someone's face regardless of facial changes, which may include a different expression, the addition of a beard, or even the addition of glasses. Systems also can recognize you even if your face is captured from a different vantage point. This advance in biometrics facial technology has made this type of biometrics more user friendly than before.

5.1.3 Reliable Matching:

Reliable face matching is offered by biometric face recognition systems, which is another advantage of choosing this type of technology. Individual facial biometrics features are used

by face recognition technology to provide identification and authentication.

5.1.4 No More Time Fraud:

One of the big benefits of using facial biometric systems is that you won't have to worry about time fraud .It will be impossible for somebody to enter , since everyone has to go through face scanning biometrics devices to clock in.

5.1.5 High Success Rate:

Facial biometrics technology today has a high success rate, especially with the emergence of 3D face recognition technologies. It is extremely difficult to fool the system, so you can feel secure knowing that your biometrics computer security system will be successful at tracking time and attendance while providing better security.

5.2 DISADVANATAGES

1. Cannot handle pose variations.
2. The face can be obstructed by hair, glasses, hats, scarves, etc.
3. Also changes in lighting or facial expressions can throw off the device.
4. Sensitive to lighting variations, shadows etc. Cameras are still expensive.
5. Takes time to reconstruct models.
6. Unavailability of large collection of 3D data.
7. Isn't always accurate due to the quality of the camera.

Chapter 6

APPLICATIONS[7]

1.Civil␣applications␣and␣law␣enforcement.

- National ID, passport, driver's license, border control.
- Surveillance of public places (airports, metro stations, etc)..
- Forensic applications.
- Security applications for electronic transactions and access control.

2.Physical access

- Secure access to networks and infrastructures
- e-health, e-commerce, e-banking.

3.Ambient␣Intelligence

- Smart house.
- Natural human-machine interaction.

3.Wearable␣systems

- Memory aids and context-aware systems.

4.Entertainment

- Interactive films, computer games.

5.Search

1. Picasa 3.5 face recognition application for finding and managing photos.

CONCLUSION

The design of the face recognition system using Raspberry pi can make the smaller, lighter and with lower power consumption, so it is more convenient than the PC-based face recognition system. Because of the open source code, it is free to do software development on Linux. We use Eigen Face Matrix for the face recognition and detection process. Also send a security alert message to the authorized person utilities. The developed scheme is cheap, fast, highly reliable and provides enough flexibility to suit the requirements of different systems.

FUTURE SCOPE

Using Raspberry pi the current project can be modified by an infrared camera. Interfacing it can be used in Smart Surveillance Monitoring Security System in which any type of public security can be achieved by using living body detection or spying. Also it can be used in ttendance system of the class. Also some profound applications can be implemented using interfacing of Raspberry pi and Arduino UNO board like sensor application of smartcard swapping, finger detection, alcohol detection, agriculture humidity sensing, Temperature sensing using web server, and many more.

Bibliography

[1] http://forensicpsych.umwblogs.org/research/criminal-justice/face-recognition-software

[2] The book “Art Of Electronics” by Paul Horowitz and Winfield Hill

[3] Real-Time Face Detection on a Configurable Hardware Platform by Rob McCready

[4] “Face Recognition Using Eigenface Apporach” by Marijeta Slavkovic, Dubravka Jevtic published at “Serbian Journel Of Electrical Engineering” Vol. 9, No. 1, February 2012, 121-130

[5] Hardware Implementation of Facial Recognition on Android Platform Jonathan Hoffpauir and Andy Nguyen EE 4780 – Introduction to Computer Vision May 4, 2012

[6] https://learn.adafruit.com/raspberry-pi-face-recognition-treasure-box

[7] Face Recognition and its Applications by Andrew W. Senior and Ruud M. Bolle, IBM T.J. Watson Research Centre, NY 10598,

[8] www.biometric-security-devices.com/biometric-face-recognition.html