1.INTRODUCTION

Robbery and illegal entrance are both common occurrences in today's society. As a result, security is crucial in everyday life. People are typically preoccupied with their daily activities, but they also want to ensure the safety of their valuable items. They are prone to misplacing important goods such as keys, wallets, and credit cards. If they don't have these, they won't be able to get to their residence or any other destination. A lock opener, an authentication password, a RFID tag, or an ID swipe card are mostly required for getting into a typical security system. On the other side, many security measures have flaws, such as the danger of being forgotten or stolen by unauthorized individuals. As a result, enhanced authentication solutions that provide a greater level of security as a template are required. Biometric Authentication is one of them. The word "Biometrics" refers to the measuring of human characteristics. In computer science, biometric authentication is a method of identity and access control. It's also used to figure out who's who in a group of people that are being watched. Individuals are identified using unique biometric identifiers with measurable qualities. Physiological biometric indicators are commonly used to identify and categorize persons. In contrast to behavioural attributes, the shape of the body has an impact on physiological characteristics. Fingerprints, palm veins, facial recognition, DNA, palm print, hand geometry, iris identification, retina, and odour/scent are only a few examples. In today’s world by using smart devices we are make our needs smart. By following trends and updates we have to consider and remove drawbacks in existing system and add more features and updates. Face detection system is more complex because of unstable characteristics. Example: let us consider glasses and beard will show some impact to detect the faces. So by considering the different angles and multiple images of faces and it will influence on detection process.

The study of OpenCV and its inbuilt library functions helps to generate a code will do correct and authentic facial recognition system with new and more efficient use of hardware. Human body will identified as an input within environment by capturing live video from a web camera and the process will be done on captured video frames. The images will run through raspberry pi3 and check with the stored data base, in this case, used an 8 GB memory card. The compilation process will be performed in VNC Viewer which helps to run Raspbian OS and the response will send to the micro controller which is connected to Zigbee receiver and power is supplied to this micro controller by the transformer and a keyboard is connected

to this micro controller and display board is also connected to it. This will control the motor driver to lock and unlock the door. To run this model there are different algorithms in that we took LBPH because it will provide more accuracy results when compared to other algorithms.

Face recognition is the technique in which the identity of a human being can be identified using ones individual face. Such kind of systems can be used in photos, videos, or in real time machines. The objective of this article is to provide a simpler and easy method in machine technology. With the help of such a technology one can easily detect the face by the help of dataset in similar matching appearance of a person. The method in which with the help of python and OpenCV in deep learning is the most efficient way to detect the face of the person. This method is useful in many fields such as the military, for security, schools, colleges and universities, airlines, banking, online web applications, gaming etc. this system uses powerful python algorithm through which the detection and recognition of face is very easy and efficient.

1.1. BIOMETRIC SECURITY:

1.1.1. Definition :

Technology is integrated into just about every aspect of modern life – and with the ever-increasing digitization of our world, it has become more difficult to safeguard confidential information. Keys and passwords are no longer sufficient data security measures. Passwords, in fact, pose a huge vulnerability in a company's security system due to their shareability and ease of cracking.

With the abundance of and network security breaches and the rise of identity theft, it is clear that stronger authentication methods are necessary. One such method is biometric security systems. In this article, we'll take a close look at what biometric security is and why it's the future of identification and authentication.

Biometric security is a security mechanism that identifies people by verifying their physical or behavioral characteristics. It is currently the strongest and most accurate physical security technique that is used for identity verification. Biometrics are mainly used in security systems of environments that are subject to theft or that have critical physical security requirements. Such systems store characteristics that remain constant over time – for instance, fingerprints, voice, retinal patterns, facial recognition, and hand patterns.

These characteristics are stored as "templates" in the system. When somebody tries to access the system, the biometric security system scans them, evaluates the characteristics, and

attempts to match them with stored records. Then, if a match is found, the person is given access to the facility or device.

The most commonly used kind of biometric security system in physical access is fingerprint sensors. This is due to their lower cost; however, for the best accuracy, high-security environments often use iris recognition systems.

1.1.1.1. BIOMETRIC IDENTIFIERS:

Biometrics are unique physical identifiers that are used by automated recognition systems. For instance, the veins in your palm, the minutiae of your fingerprints, and the shape and pattern of your iris are all your unique biometric identifiers. For a full breakdown of biometrics, read our detailed guide, "What Is Biometrics?"

1.1.1.2. BIOMETRIC IDENTIFICATION AND AUTHENTICATION:

While biometric security systems can combine identification and authentication, the two functions are not the same. With biometric identification, a person's features are compared to an entire database. With biometric authentication, on the other hand, the system is checking to see if the person is who they say they are – so their attributes are compared against one particular profile from the database.

For a practical example: Facial recognition security systems might use video surveillance to identify known shoplifters when they enter the premises of a store. The store might also have a separate fingerprint system that authenticates an employee and gives them access to a restricted room upon scanning their fingerprint – the scanned data is compared to the stored, approved template.

If you want a more detailed look at the difference between the two functions of biometrics, check out our article, "Biometric Authentication, Identification, and Verification in 2020."

1.1.2. Importance of Biometric Nowadays:

More and more companies are recognizing the benefits that biometric security devices can bring – not just in securing physical environments but also computers and business assets. In corporate buildings, it is crucial that unauthorized people are restricted from accessing secure networks and systems. Furthermore, due to compliance regulations, it must be ensured that only certain employees have access to sensitive files and that workflow processes are followed to the letter. For sensitive data, passwords aren't ideal, as co-workers can share them. Instead, organizations can use biometrics to regulate server or computer access.

Companies that use biometric security systems can benefit from extreme accuracy and unparalleled security of restricted information. Fingerprints, retinal scans, and iris patterns, when captured correctly, produce totally unique data sets. When an employee or a user is enrolled in a biometric security system, automatic identification can be performed uniformly, quickly, and with only minimal training.

1.1.3. WORKING OF BIOMETRIC SYSTEMS:

The importance of biometric security in modern society is ever-growing. Physical characteristics are unique and fixed – including among siblings and even twins. An individual's biometric identity is able to replace (or, at the very least, supplement) password systems for phones, computers, and restricted areas.

After a person's biometric data is gathered and matched, the system saves it to be matched with subsequent access attempts. Usually, the biometric data is encrypted and then stored either in the device itself or in a remote server.

Hardware known as biometrics scanners captures physical characteristics for identity verification and authentication. The hardware's scans are compared to the saved database – and, depending on whether a match is found, access is granted or restricted. You can think of your own body as a key to unlock secure areas.

Biometrics brings two major benefits: they are convenient, and they are difficult to impersonate. While such systems aren't perfect, they bring huge potential to the future of cybersecurity.

1.1.4. DESIGN OF BIOMETRIC SECURITY SYSTEMS:

When designing a biometric system, the primary goal is to encrypt the private cryptographic code with biometric technologies – each of those technologies should produce a limited number of information vectors – which, in turn, will be considered as biometric cryptographic keys. Next, the systems must calculate a hash function for every key. Hashes may be stored on a USB token, a server, a smart card, or another form of storage. One benefit of this process is that the storage method won't actually contain any sensitive data since the biometric attributes features themselves are not stored.

Each part of the private key is encrypted with all biometric vectors produced in the biometric attribute encryption phase. The entirety of the information (i.e., hashes and encrypted values) is saved on the database. Since the database doesn't contain secret information, access to it does not need to be limited. The biometric key encryption is only stored in volatile RAM.

Identity verification is done via the hash values. When an individual attempts to log in, they claim their identity and then present one of their features for biometric authentication. If just verification is performed, one biometric attribute is plenty – for instance, a fingerprint scan. A certain set of features is acquired from this biometric attribute. Then, from that set, a subset of vectors is generated. That subset is considered to be the biometric cryptographic key. Lastly, the hash function is calculated from this vector – and the calculation's result is compared to stored hash values.

1.1.5. TYPES OF BIOMETRIC SECURITY SYSTEM:

There are two main types of biometrics used for security: physical and behavioral. Physical biometrics analyze facial features, eye structure, hand shape, and other things involving your body's physical form.

A. Physical:

- Facial geometry
- Fingerprints
- Skull shape
- Retina
- Iris
- Hand geometry
- Palm or finger veins
- DNA

B. Behavioural

- Speaker recognition
- Signature
- Keystroke dynamics
- Gait

1.1.6. EXAMPLES OF POPULAR BIOMETRIC SECURITY:

Some forms of biometrics are more popular than others, either due to their affordability (fingerprint scans) or their high levels of accuracy (iris recognition). Let's take a look at some of the most widespread forms of biometric security systems.

1.1.6.1. Facial Recognition:

Facial recognition is done by analysing the ratios of an individual's facial features: for instance, the distance between the eyes, the nose, the lips, the ears, the chin, and the eyebrows. Facial recognition is highly accurate, and results only take a split-second.

1.1.6.2. Iris Scanning:

Iris authentication technology photographs a person's iris and analyses its texture. The software uses approximately 260 anchor points when creating a sample – which is much higher than, say, fingerprint systems, which have 60-70 anchor points.

1.1.6.3. Retinal Scan:

Each retina has its own unique network of capillaries – and, in most cases, the retina remains unchanged throughout a person's lifetime. Retina scanning occurs when a beam of infrared light is projected into somebody's eye via an eyepiece. The retina's capillaries absorb the light better than other parts of the eye, so the scan is able to create a pattern of blood vessels – which is then measured and verified.

1.1.6.4. Finger Printing:

Fingerprint systems are very commonly used due to their affordability, security, and relative accuracy. A fingerprint scanner produces a digital image of the print, and a computer turns the minutiae into a code via pattern-matching software. That code is then compared to the database of approved identities.

1.1.6.5. Voice Recognition:

A speaker's voice is used to verify their claimed identity. It is a 1:1 match, in which their voice is compared to a voice model (also known as a voiceprint). Such systems usually give access to secure systems like telephone banking. Voice recognition typically operates with an individual's knowledge and cooperation.

1.1.6.6. Vein Recognition:

This kind of biometrics is used to identify people based on their unique vein patterns within their palm or finger.

1.1.6.7. Hand Geometry:

Geometrics features of a person's hand are assessed and compared to a template. Features assessed may include the length of the fingers, the distance between knuckles, and the width of the hand.

1.1.7. Uses of Biometric Security Systems:

You have likely noticed biometric security systems showing up more and more often in retail and banking environments, as well as mobile devices. Let's take a closer look at where you can see biometrics in use today – some will be familiar to you, but others may come as a surprise.

1.1.7.1. Banking Systems:

Banking customers have grown weary of the constant need to prove their identity – yet, without this, the threat of identity theft will continue to rise. Therefore, biometric security systems for banks are in demand. Many banks that have mobile apps allow user authentication via biometrics such as facial recognition, fingerprint scanning, and voice verification. And other banks use a combination of these biometrics; multi-factor authentication, when combined with biometrics, can create a nearly impenetrable layer of security.

1.1.7.2. Business Security:

Many companies nowadays are installing access control and time tracking systems that incorporate biometric authentication. Take, for instance, Id-Time from RecFace. This software automatically records employees' working hours and compliance with labor regulations, and it uses biometric data to do so. Identification takes less than 1 seconds, and 7 kinds of reports are generated during the execution.

1.1.7.3. Self Check-In:

Single sign-on is a method of authentication in which a user logs in to multiple software systems with just one ID and password. For instance, you can use your Google login information to access Gmail, Google Drive, YouTube, and many more applications.

Single sign-on is also often used in healthcare services to give doctors access to many systems easily and quickly. However, the healthcare industry is often subject to data breaches – which means that there is a pressing need for the industry to begin integrating biometric authentication into single sign-on procedures.

1.1.7.4. Device Security:

Over the last few years, iOS and Android devices have added biometric authentication features. The first smartphone to feature fingerprint scanning was the Motorola Atrix back in 2011. At the time, the technology was quite flawed; nowadays, though, almost every modern smartphone uses fingerprint scanning.

However, device biometrics has also moved beyond mere fingerprints. Take Face ID, for example; it was introduced in 2017 with Apple's iPhone X. This feature projects more than 30,000 infrared points onto a user's face, assessed the resulting pattern, and then generates a "facial map." That map is then used to authenticate later login attempts.

Samsung has a biometric security feature of its own: Intelligent Scan. It combines facial recognition with an iris scan, thus providing biometric multi-factor authentication.

1.1.7.5. Money Security:

We mentioned how biometrics are used by banks; however, there is another financial application: biometric payment security. This technology is integrated during transaction authorization processes and, for now, mostly involves a fingerprint scan

1.1.7.6. Home Security:

Biometric technology can allow an individual to enter a home once its scanning unit has verified their identity. Access to office buildings, entire houses, or particular rooms can be controlled via biometrics. Biometric locks negate the need for a key and are operated with the swipe of a fingerprint instead.

1.1.8. Safety of Biometric Security System:

While biometric technology has been growing by leaps and bounds, and it certainly an exciting industry, you must keep in mind that it doesn't guarantee absolute cybersecurity. While biometric security is much harder to fool than passwords, it is still possible to be breached. For instance, criminals can "lift" fingerprints off of surfaces and use them to access biometrically secured systems.

Furthermore, you must consider whether the database that holds your biometric data is secure. Take, for instance, when the US Office of Personnel Management was breached in 2015. Over 5 million fingerprints were stolen. If your data is compromised, it isn't as if you can change your fingerprints.

It is also possible to "trick" biometric scanners that use facial recognition technology. Researchers from the University of North Carolina at Chapel Hill constructed 3-D models of 2D face photographs. The researchers then tried to access five security systems using those 3-D models, and they successfully breached four of the systems.

So, as you can see, while biometric security is highly accurate, it is not invulnerable to breaches.

1.1.8.1. HOW TO PROTECT YOUR BIOMETRIC DATA:

1. Only share your biometrics with highly trusted organizations;
2. Before sharing your biometrics with organizations, make sure that they have necessary cybersecurity measures in place;
3. Only share biometric data when it's absolutely necessary. Ask if it's worth it; for instance, is enabling facial recognition on Facebook truly necessary?
4. Use strong passwords to make it difficult for hackers to steal your stored biometrics;

5. Use reputable cybersecurity software to safeguard your digital life.

1.1.8.2. HOW COMPANIES SHOULD PROTECT YOUR BIOMETRIC DATA:

1. Keep all systems and software up-to-date;
2. Use multi-factor authentication and strong internal passwords;
3. Use reputable, strong cybersecurity software;
4. Use anti-spoofing technology to protect the system from breaches.

1.1.9. Advantages and Disadvatages of Biometric Security Systems:

To sum up what we've presented about biometric security systems so far, we've compiled their advantages and disadvantages.

1.1.9.1. Advantages of Biometric Security Systems:

1. Biometrics are inherent to the user**.** In the vast majority of cases, a person's fingerprints, retinal patterns, and facial geometry will never change;
2. Biometrics are difficult to duplicate**.** Most modern biometric security systems use liveliness checks to protect against spoofing attempts;
3. Permissions are easily managed**.** With many systems, administrators can instantly give or restrict permissions to employees, and the list of accepted templates is automatically modified;
4. Efficiency is increased**.** Most biometric systems can authenticate users in less than one second – thus strongly cutting down on time delays caused by PINs, passwords, and manual identity checks;
5. Fewer security staff**.** A biometrics system can do the work of multiple security employees – meaning that companies can save money since there is less need for assigning dedicated security staff to access points;
6. No replacement costs. Lost fobs and cards occur at a high rate, and this often comes with a replacement cost. Biometrics, on the other hand, can't be lost.

1.1.9.2. Disadvantages of Biometric Security Systems:

1. The environment can impact biometric security**.** For instance, a higher error rate may occur in a very cold environment;
2. There could be a false acceptance or a false rejection. Both have been known to happen; even though biometric security may have a 99% accuracy rate**,** the 1% rate of inaccurate authentication could have detrimental results;

3. They require hardware and integrations. Not only does a biometric security system rely on having a computer, a sensor, and the necessary software, but it also needs the expertise of a programmer for system management;
4. Scanning challenges may occur**.** For instance, if you are wearing glasses during an iris scan, this could cause difficulties and slow down an otherwise quick process;
5. They come at a high cost. Even though biometric systems are cheaper than they used to be, they are still much more expensive than traditional security devices;
6. Biometric data can't be reset if it is compromised**.** If your fingerprints are stolen, you can't change them like a password.

1.2. FACE RECOGNITION:

Face recognition technology is not new – you are probably already using it in your daily life. Most of us use smart phones nowadays, which often employ face recognition technology to unlock the device. This technology provides a powerful way to protect personal data and ensure that even if the phone is stolen, sensitive data remains inaccessible by the perpetrator. The use of face recognition technology is being applied to an ever-expanding set of domains, including safety, security, and payments.

So, what exactly does face recognition do? Face recognition is a broad problem of identifying or verifying a person in digital images or video frames through the facial biometric pattern and data. The technology collects a set of unique biometric data of each person associated with their face and facial expression to authenticate a person. Face recognition technology is mostly used for two types of tasks:

- Face Verification: given a face image, match it with known images in secure database, give a yes/no decision (for example, is this the person who claims he/she is?). Does the person exist in the database?
- Face Identification: given a face image, match it with known images in secure database, detect whose image it is (for example, who is this person?). Identifying the person such as the image is John Doe's or Mark Twain's, and so on.

End-to-end face recognition system for biometrical authentication

Ericsson's Global Artificial Intelligence Accelerator (GAIA) team has been working on a Proof of Concept that aims to make the authentication more secure. While there are other companies in the market that offer commercial products or services to help build face recognition applications, the GAIA team mostly leveraged open-source tools to build an AI-powered solution that can be used on mobile or edge devices. With the resource constraints

(limited storage and memory on a device, for example), it is critical to find a good balance among the model complexity, performance and response time when selecting the best candidate AI models. One more important factor that needs to be considered is trustworthiness of AI models for face recognition. Ericsson developed guidelines for trustworthy AI development to support these initiatives.

Figure 1 shows the architectural design of the end-to-end face recognition system for biometrical authentication. It takes a reasonably small number of images or video frames as the input, detects human faces, and determines if the human faces match any of the face images in the database of enrolled users. If a match is determined the person is biometrically verified, otherwise they are not verified. The system consists of four basic modules: face detection, face alignment, face encoding, and face matching. In addition, a face liveness check is added as an optional module in the pipeline to ensure the authenticated person is a real person, and the system is not fooled by a photograph of a targeted person.

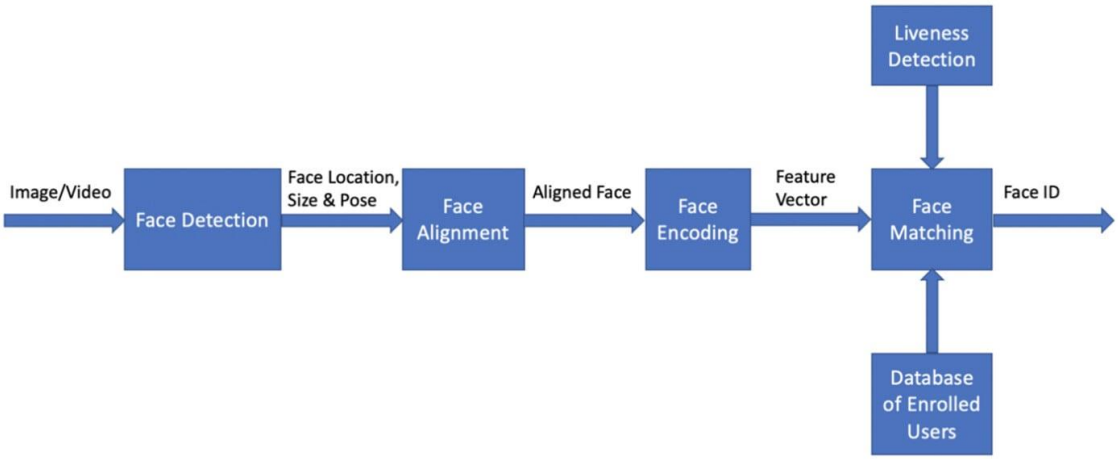

Fig.1.1 Architecture of end-to-end face recognition system for biometrical authentication

1.2.1. FACE DETECTION:

Face detection is the first step in the pipeline. It is the process of finding a face in an image. This step only focuses on finding a face and does not concern identity determination. Ultralight detector is set as the default face detection model, as it gives excellent performance in detecting faces from different angles (i.e., it is not restricted by detecting front face only). Furthermore, the detector is a lightweight model (with size <2MB) and can detect faces very

fast (with inference time 50 +/- 6 ms on a MacBook Pro 2.6GHz Intel Core i7 with 32GB DDR4).

1.2.2. FACE ALIGNMENT:

Face alignment is the next step, after a face is detected in an image. Quite often when a person takes a picture, he or she may not be facing directly towards the camera. However, face alignment can deal with the problem. Even if a face is turned in different directions, the system is still able to tell if it is the same person. More specifically, an algorithm called "face landmark estimation" is applied to locate facial landmarks, i.e., the specific points that exist on every face, such as top of chin, outside edge of each eye, inner edge of each eyebrow, etc.

Figure 2 shows an example of the 68-point face landmark model that is used in the pipeline to locate specific points on every face. Once the locations of those key geometric face structures are identified, any rotation, translation and scale representation of the face can be normalized. No matter how the face is turned, the eyes and mouth can be centered in roughly the same position in the image. With the face aligned, the later step of the face matching process will become more accurate.

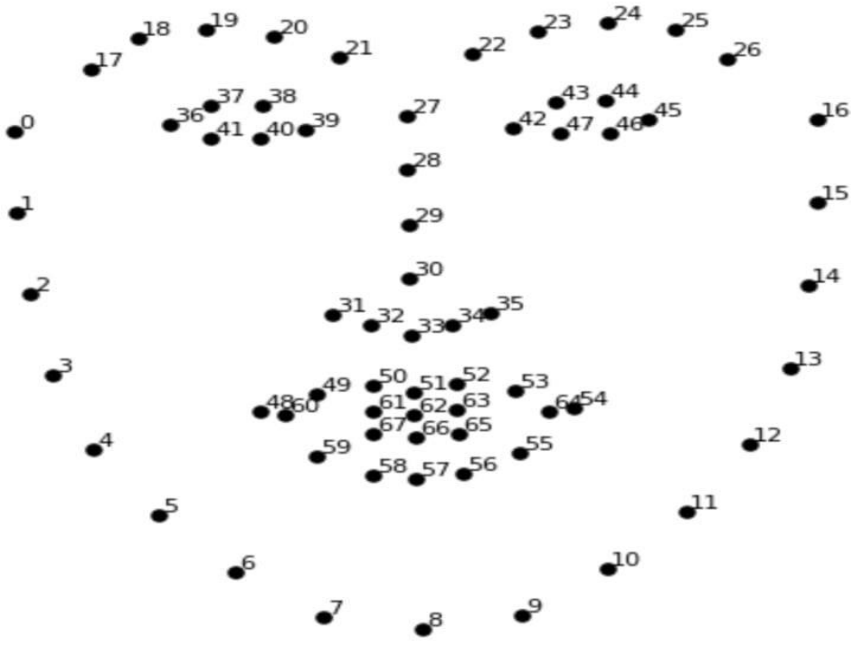

Fig.1.2. Example of the 68-point face landmark model

1.2.3. FACE ENCODING:

The third step is face encoding. This process identifies key parts of a face through the "eyes of a computer." As computers can only recognize numbers, a reliable way of converting face images to numbers/measurements was needed to represent each face. Finding a good method of face encoding was a challenging task. Quite often deep

learning models, such as the "Convolutional Neural Network (CNN)" model, are trained by using a large database of face images to calculate the best face representation of each face. The goal of this training is to generate nearly the same encodings when looking at two different pictures of the same person, whilst generating quite different measurements when looking at pictures of different people.

After exploring many different models, a pre-trained Resnet model provided in Dlib was chosen for the face encoding model of the pipeline. This model was essentially a ResNet-34 model, which was modified by dropping some layers and re-building with 29 convolution layers. This Resnet model takes an image inputs with size 150 x 150 x 3 and represents/encodes each face image as 128-dim measurements. Once the model network was designed, the pretrained model was trained on a dataset of about 3 million faces. The face dataset was mainly derived from the two open-source face databases, the face scrub dataset and the VGG dataset. The design of the ResNet-34 model is shown in Figure 3.

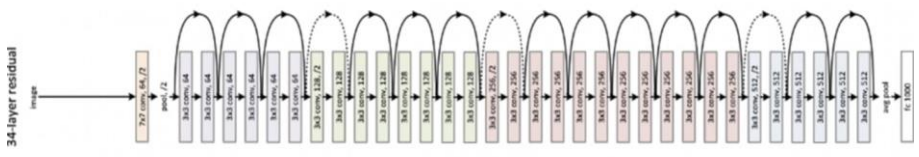

Fig.1.3. Design of ResNet-34 model

1.2.4. FACE MATCHING:

After encoding of a face, the final step is to perform face matching. This entails calculating the distance of two encodings/measurements corresponding to two faces and compare the distance against a threshold. If the distance is smaller than the threshold, then the two faces are determined to belong to the same person; otherwise, the two faces are from two different people.

There are two major types of face matching tasks:

Face identification: the process involves finding the person in the database of known enrolled users who has the closest encoding (i.e., smallest distance) to the test face image.

Face verification: compares the encoding of the test face image with the targeted encoding (i.e., encoding of the authorized user). If the two encodings are close enough (i.e., smaller than the threshold), the test person is verified.

1.2.5. FACE LIVENESS DETECTION:

In addition to the main functionality of the face recognition pipeline, liveness detection has been incorporated into the pipeline. This is an optional feature to make sure the authenticated face is from a real person, not from a photograph or from a video frame. The movement-based models such as "eye-blink detection" and "mouth-moving detection" are used as part of the liveness check. Once the liveness detection feature is triggered, the system detects eye-blinks followed by the mouth close-open-close pattern to verify if it is a live person.

1.2.6. EYE-BLINK DETECTION:

A real person will unconsciously blink their eyes. The eye-blink detection model tries to detect the eyes' open-close-open pattern across different frames. Eyes are located by the face alignment step, and then used to calculate the eye aspect ratio. The ratio is further used to predict the open or closed status of eyes using a ML model based on "Support Vector Machine (SVM)", as the machine-learning model provides more robust detection of eyes' status compared to a prefix threshold-based approach.

1.2.7. MOUTH-MOVING DETECTION:

Similarly, once the location of a mouth is determined by the face alignment step, the mouth aspect ratio is calculated to determine the open or closed status of mouth. Since a mouth is less sensitive than eyes, a fixed threshold is good enough to make the decision. The mouth is classified as open if the mouth aspect ratio is larger than a threshold.

1.3. IMAGE:

An image is defined as a two-dimensional function, F(x,y), where x and y are spatial coordinates, and the amplitude of F at any pair of coordinates (x,y) is called the intensity of that image at that point. A digital image is a two-dimensional array of pixels. Each pixel has an intensity value (represented by a digital number) and a location address (referenced by itsrow and column numbers).When x, y, and amplitude values of F are finite, we call it a digital image. The images may be analog or digital. Aerial photographs are examples ofanalog

images while satellite images acquired using electronic sensors are examples of digital images. A digital image is a two-dimensional array of pixels.

A digital image is an image composed of picture elements, also known as pixels, each with finite, discrete quantities of numeric representation for its intensity or gray level that is an output from its two-dimensional functions fed as input by its spatial coordinates denoted with x, y on the x-axis and y-axis, respectively.

1.3.1. TYPES OF DIGITAL IMAGES:

Generally, we consider four type of images:

- Binary images
- Gray-scale images
- Colour images
- Multispectral images

1.3.1.1. Binary Images:

Binary images can take one two value 0 and 1 or typically black and white. Binary images take only 1 binary digit to represent each pixel so it is also known as 1-bit image. e.g. – optical character recognition (OCR).

Through threshold operation from the grey-scale images binary images are created. In threshold operation, every pixel above the threshold value is turned white (1), and those below the threshold are turned black (0).

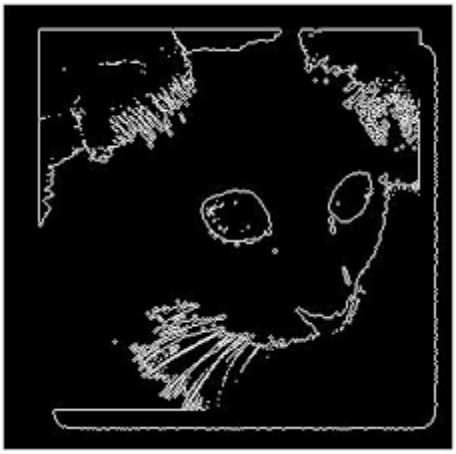

Fig.1.4.Example of Binary Image

1.3.1.2.Grayscale Image:

These images are also known as monochrome or one-color images. Gray-level images only contain grey level information they do not contain any colour information. Available number of different grey levels is determined by the number of bits used for each pixel.

For example: for 256 different grey level grey scale image should contain 8bits/pixel data.

12 or 16bits/pixel data are used for the medical imaging and astronomy.

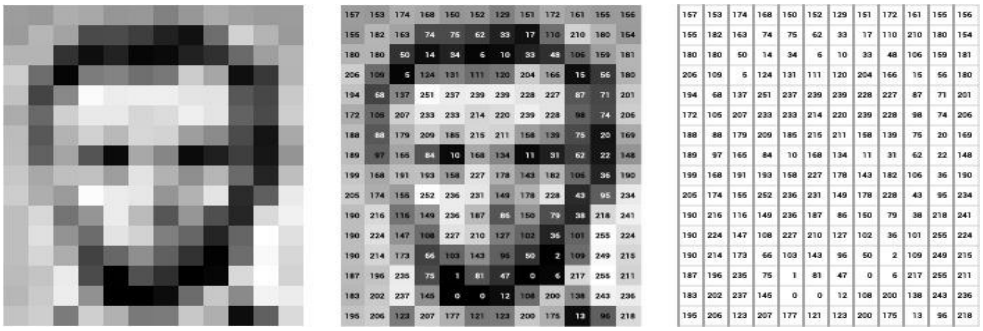

Fig.1.5. Example of Grayscale Image

1.3.1.3. Colour Image:

Colour images are created as three-band monochrome image data, in which each band of image data corresponds to a different colour. In each spectral band there is a grey-level information which is the actual information stored in the digital image. Colour images are also known as the RGB image because colour images are represented as there green, and blue. Colour images would have 24-bits/pixels by using 8-bitmonochrome standard as a model and 8-bits for each of the three-colour band (red, green and blue).

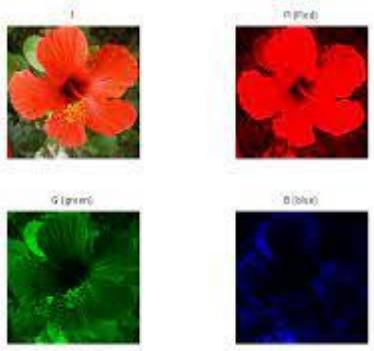

Fig.1.6.Example of Colour Image

1.3.1.4. Multispectral Image:

This type of images contain the information outside the normal human perceptual range. Information represented is not directly visible by human system so, these are not images in the usual sense. However by mapping the different spectral band to RGB

components the information is represented in visual form. Multispectral images include the ultraviolet, infrared, X-ray, radar data and acoustic.

1.3.2. OPERATIONS ON IMAGE:

1.3.2.1. Image Resolution:

The term resolution is often used as a pixel count in digital imaging. When the pixel counts are referred to as resolution, the convention is to describe the pixel resolution with the set of two numbers. The first number is the number of pixel columns (width) and the second is the number of pixel rows (height), for example as 640 by 480. Another popular convention is to cite resolution as the total number of pixels in the image, typically given as number of megapixels, which can be calculated by multiplying pixel columns by pixel rows and dividing by one million. An image that is 2048 pixels in width and 1536 pixels in height has a total of 2048×1536 = 3,145,728 pixels or 3.1 megapixels. One could refer to it as 2048 by 1536 or a 3.1-megapixel image. Other conventions include describing pixels per length unit or pixels per area unit, such as pixels per inch or per square inch.

Below is an illustration of how the same image might appear at different pixel resolutions.

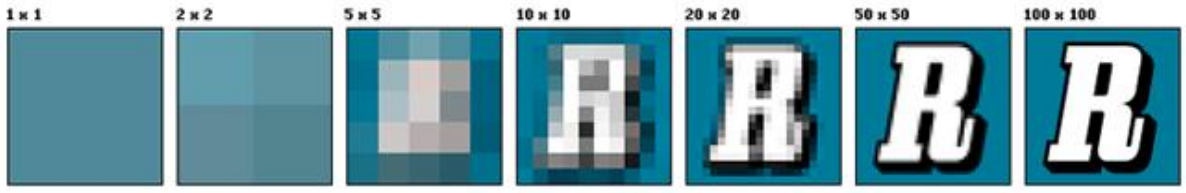

Fig.1.7.Different forms of Image Resolution

As the megapixels of a camera increase so does the ability of a camera to produce a larger image; a 5-megapixel camera is capable of capturing a larger image than a 3-megapixel camera. Larger monitor screens usually have higher screen resolution, measured in pixels.

1.3.2.2. Image Processing:

Image processing is a method to perform some operations on an image, in order to get an enhanced image or to extract some useful information from it. It is a type of signal processing in which input is an image and output may be image or characteristics/features associated with that image. Digital Image Processing is a software which is used in image processing. For example: computer graphics, signals, photography, camera mechanism, pixels, etc. Image analysis involves processing an image into fundamental components to extract meaningful information. Image analysis can include tasks such as finding shapes,

detecting edges, removing noise, counting objects, and calculating statistics for texture analysis or image quality. In electrical engineering and computer science, image processing is any form of signal processing for which the input is an image such as a photograph or video.

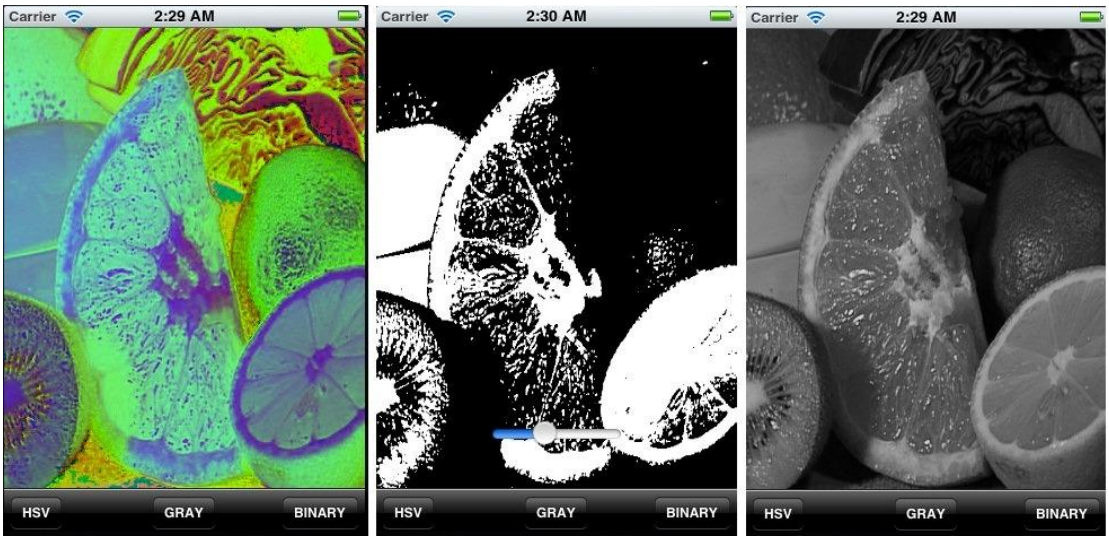

Fig.1.8.Image Conversion to GrayScale Image

Most image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal-processing techniques to it. Digital image processing is the use of a digital computer to process digital images through an algorithm. As a subcategory or field of digital signal processing, digital image processing has many advantages over analogy image processing.

1.3.2.3. Image Transformation:

Image transformation is a function that produces an image as output and takes an image as input. The input and output image may have different interpretation or may appear entirely different, depending on the transform chosen. Example of image transformation are principal component analysis; Fourier transform and various spatial filter.

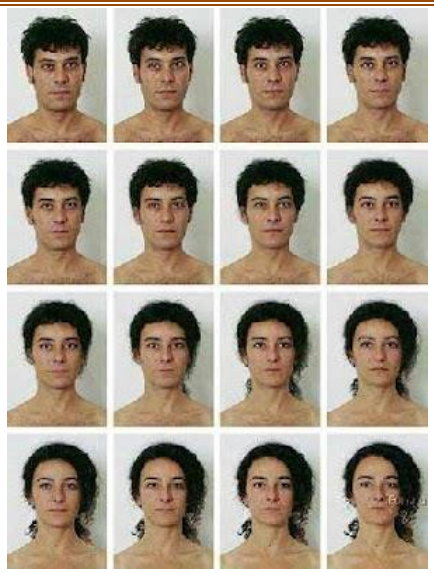

Fig.1.9. Example of Image Transformation

From the two or more sources image transformation generates the new image which highlights the particular feature of interest, better than the original input images.

1.4. PIXEL:

In digital imaging, a pixel(or picture element) is the smallest item of information in an image. Pixels are arranged in a 2-dimensional grid, represented using squares. Each pixel is a sample of an original image, where more samples typically provide more-accurate representations of the original. The intensity of each pixel is variable; in colour systems, each pixel has typically three or four components such as red, green, and blue, or cyan, magenta, yellow, and black. The word *pixel* is based on a contraction of *pix* ("pictures") and *el* (for "element").

Pixels are normally arranged in a 2-dimensional grid, and are often represented using dots or squares. Each pixel is a sample of an original image; more samples typically provide more accurate representations of the original. The intensity of each pixel is variable. For example, a 2.1 megapixels picture contains 2,073,600 pixels since it has a resolution of 1920 x 1080. The physical size of a pixel varies, depending on the resolution of the display. The total number of pixels within the region defines the area of that region. However, the perimeter refers to the boundary of the region, given the number of pixels. A ‘pixel’ (short for ‘picture element’) is a tiny square of colour. Lots of these pixels together can form a digital image. Each pixel has a specific number and this number tells the computer what colour the pixel should be. The process of digitisation takes an image and turns it into a set of pixels.

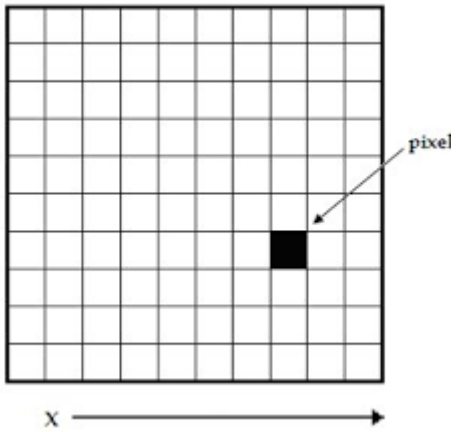

Fig.1.10.Example of Pixel

1.4.1.Matrix Of Pixel:

An image matrix, like any matrix, is a mathematical object. Typically, computers display greyscale images on a screen by producing values between 0 and 255 for each pixel, as this makes one byte of data when encoded in binary. Each pixel is made up of red, blue, and green lighting elements that are used in different combinations and intensities to make millions of different colours. An image is an array, or a matrix, of square pixels (picture elements) arranged in columns and rows. An image — an array or a matrix of pixels arranged in columns and rows. In a (8-bit) grey scale image each picture element has an assigned intensity that ranges from 0 to 255.

P1	P2	P3
P4	P5	P6
P7	P8	P9

Fig.1.11.Matrix of Pixel Representation

Essentially, pixels are the building blocks of the digital world, allowing designers to manipulate and set them to specific coordinates to bring an image to life. In visual design, it is important to understand the overall structure of a pixel and how it can be manipulated to benefit the quality of your designs.

1.5.BGR:

BGR stands for Blue (255, 0, 0), Green (0, 255, 0), Red (0, 0, 255). OpenCV uses BGR colour as a default colour space to display images, when we open an image in OpenCV using cv2.imread() it displays the image in BGR format. And it provides colour-changing methods using cv2.cvtColor() for transforming a BGR image into other Colour spaces.

When the image file is read with the OpenCV function imread() , the order of colours is BGR (blue, green, red). On the other hand, in Pillow, the order of colours is assumed to be RGB (red, green, blue). RGB stands for Red Green Blue. Most often, an RGB colour is stored in a structure or unsigned integer with Blue occupying the least significant "area" (a byte in 32-bit and 24-bit formats), Green the second least, and Red the third least. BGR is the same, except the order of areas is reversed. The BGR is used because the early developers at OpenCV chose BGR colour format is that back then BGR colour format was popular among camera manufacturers and software providers. BGR (subpixels), blue, green, red, an RGB display pixel layout. Boy Genius Report, a weblog that specializes in technology and consumer gadgets. The main difference between RGB versus BGR is the arrangement of the subpixels for Red, Green, and Blue. RGB is arranged like that, but BGR is essentially in reverse with no adverse effect on colour vibrancy and accuracy. … The majority of modern monitors use the RGB subpixel layout, so this flaw doesn't affect you.

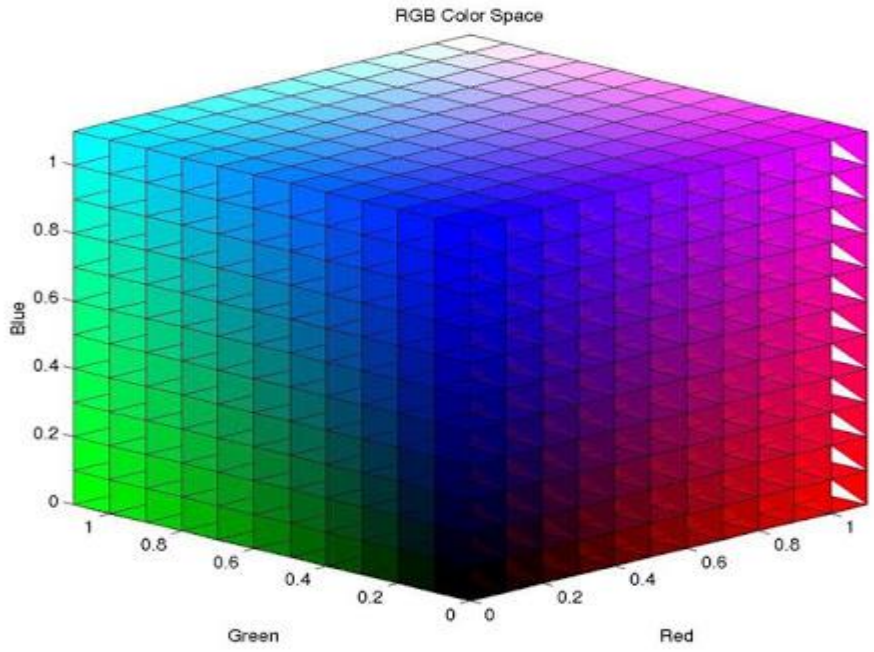

Fig.1.12.RGB Representation

1.6.GRAY SCALE:

Gray scaling is the process of converting an image from other colour spaces e.g. RGB, CMYK, HSV, etc. to shades of grey. It varies between complete black and complete white a series of regularly spaced tones ranging from black to white through intermediate shades of grey also an image composed solely of grey scale tones. The main reason why grayscale representations are often used for extracting descriptors instead of operating on colour images directly is that grayscale simplifies the algorithm and reduces computational requirements. Grayscale images are distinct from one-bit bi-tonal black-and-white images, which, in the context of computer imaging, are images with only two colours: black and white (also called bilevel or binary images). Grayscale images have many shades of grey in between. Grayscale images can be the result of measuring the intensity of light at each pixel according to a particular weighted combination of frequencies (or wavelengths), and in such cases they are monochromatic proper when only a single frequency (in practice, a narrow band of frequencies) is captured. The frequencies can in principle be from anywhere in the electromagnetic spectrum.

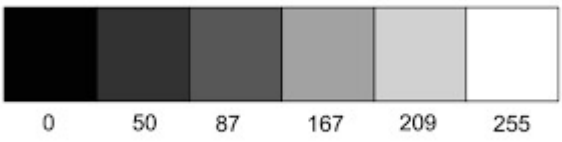

Fig.1.13.Gray Scale

The grey level or grey value indicates the brightness of a pixel. … In a binary image a pixel can only take on either the value 0 or the value 255. In contrast, in a greyscale or colour image a pixel can take on any value between 0 and 255. Mean grey value – Average grey value within the selection. This is the sum of the grey values of all the pixels in the selection divided by the number of pixels. Because a byte is composed of 8 bits, such images are known as 8-bit grayscale images. Some high-end scanners can scan with a finer intensity scale. They use 12 or 16 bits to represent the intensity values of the image, making it possible to register 4096 or 65,536 different grey levels. Gray level slicing is a technique used to highlight a specific. Range of grey levels in a given image. – Similar to thresholding. – Other levels can be suppressed or maintained. – Useful for highlighting features in an image.

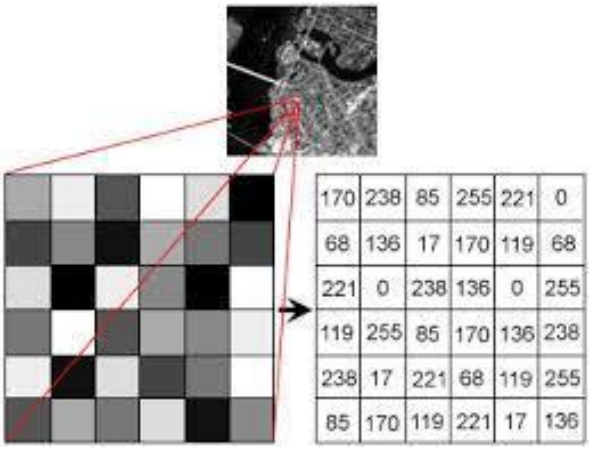

Fig.1.14.Gray scale in Matrix

Gray-level slicing is being done by two approach One approach is to give all grey level of a specific range high value and a low value to all other grey levels. Second approach is to brighten the pixels gray-value of interest and preserve the background. Both iOS and Android offer the option to set your phone to grey scale, something that can help those who are colour-blind as well as let developers more easily work with an awareness of what their visually impaired users are seeing. For people with full colour vision, though, it just makes your phone drab.

Gray Level Slicing. Grey level slicing is equivalent to band pass filtering. It manipulates group of intensity levels in an image up to specific range by diminishing rest or by leaving them alone. This transformation is applicable in medical images and satellite images such as X-ray flaws, CT scan.

The digital image created by a scientific camera shows the level of light that falls on every pixel as an intensity value, this value is known as a gray level. ... For example, an 8-bit camera is capable of displaying 256 gray levels, a 12-bit camera 4096 gray levels, and a 16-bit camera 65,535 gray levels.

Grey level thresholding is a simple lookup table, which partitions the gray levels in an image into one or two categories - those below a user-selected threshold and those above. Thresholding is one of many methods for creating a binary mask for an image.

2.LITERATURE SURVEY

Door lock security systems are classified based on technology used 1) GSM based, 2) smart card based, 3) Password based, 4) Biometric based, 5) RFID based, 6) Door phone based, 7) Bluetooth based, 8) Social networking sites based, 9) OTP based, 10) Motion detector based, 11) VB based, 12) Combined system.

2.1. BASE PAPERS:

Door lock security systems are classified based on technology used 1) GSM based, 2) smart card based, 3) Password based, 4) Biometric based, 5) RFID based, 6) Door phone based, 7) Bluetooth based, 8) Social networking sites based, 9) OTP based, 10) Motion detector based, 11) VB based, 12) Combined system.

2.1.1. FACE RECOGNITION USING IOT:

The basic idea behind the project is to use a Raspberry PI micro-controller board for system development, a Webcam and Zigbee module for face recognition and a programmable stepper motor to open door locks. We will install an appropriate Linux based Raspberry pi operating system on raspberry pi micro-controller board. For the door unlocking system, place a stepper motor at the door latch. This motor will be programmed in such a way that when the system authenticates the person in front of the camera, the motor will rotate to open latch. The image processing technology is used to authenticate the person to enter home. For image processing, the Webcam and Zigbee module. The Webcam and Zigbee module is attached to Raspberry pi, and it aids in storing various faces in the databases. When someone wants to enter home, he should stand in front of the camera. Camera will recognize the face and compare it with the faces stored in the LFW database. If the face matches, the door will be automatically unlocked, otherwise a warning call will be sent to the owner of the house.

2.1.2. BUILDING A RASPBERRI PI SECURITY SYSTEM WITH FACIAL RECOGNITION:

The basic idea behind the project is to use a Raspberry PI micro-controller board for system development, a Webcam and Zigbee module for face recognition and a programmable stepper motor to open door locks. We will install an appropriate linux based Raspberry pi operating system on raspberry pi micro-controller board. For the door unlocking system, place a stepper motor at the door latch. This motor will be programmed in such a way that

when the system authenticates the person in front of the camera, the motor will rotate to open latch. The image processing technology is used to authenticate the person to enter home. For image processing, the Webcam and Zigbee module. The Webcam and Zigbee module is attached to Raspberry pi, and it aids in storing various faces in the databases. When someone wants to enter home, he should stand in front of the camera. Camera will recognize the face and compare it with the faces stored in the LFW database. If the face matches, the door will be automatically unlocked, otherwise a warning call will be sent to the owner of the house.

2.1.3. FACE RECOGNITION USING OPENCV ON IOT FOR SMART DOOR:

This paper discusses a face recognition system which is designed and implemented for doors resulting in smart doors based on IoT. The paper intends to provide the information to the user using open source technology which comprises OpenCV2, LBPH algorithm, SMTP, raspberry pi3, Webcam and Zigbee. The implementation area is categorized more on a local level like home, offices and campus. The system provides real time face detection and recognition once the bell is triggered. The captured image is analysed with the available database and if it is a match, the access is granted and the door will open. On the contrary if the face did not match the captured image is then sent to the user mail using SMTP. The system will then wait for the response from the user within stipulated time with appropriate messages. The message is retrieved on raspberry pi using IMAP. Based on the retrieved message context either access will be granted or denied. The system is acting as a base station. The wireless communication is achieved using SMTP and IMAP. The aim of the system is to develop a real time face recognition model having low-cost solutions in security.

2.1.4. FACE RECOGNITION-BASED DOOR LOCKING SYSTEM WITH TWO-FACTOR AUTHENTICATION USING OPENCV:

This project develops a face recognition-based door locking system with two-factor authentication using OpenCV. It uses Raspberry Pi 4 as the microcontroller. Face recognition-based door locking has been around for many years, but most of them only provide face recognition without any added security features, and they are costly. The design of this project is based on human face recognition and the sending of a One-Time Password (OTP) using the Twilio service. It will recognize the person at the front door. Only people who match the faces stored in its dataset and then inputs the correct OTP will have access to unlock the door. The Twilio service and image processing algorithm Local Binary Pattern Histogram (LBPH) has been adopted for this system. Servo motor operates as a mechanism to access the door. Results show that LBPH takes a short time to recognize a face.

Additionally, if an unknown face is detected, it will log this instance into a "Fail" file and an accompanying CSV sheet.

2.2. SUMMARY OF RELATED WORK:

The summary of methods used in literature is in given Table. Table Summary of literature survey

Literature	Advantage	Disadvantage
[1] Sandesh Kulkarni, Minakshee Bagul,Akansha Dukare ,"Face recognition system using IoT" , IJARCET Publications, 2017	New connection like cascade connections, parallel connection, series connection to extend the system. The system can work on both modes online and offline mode. In online mode, the system can use internet at its working time. In offline mode, the system does not use any internet connection.	It does not have a second method for unlocking the incase the face recognition does not work on the authorized user.
[2]Thulluri Krishna Vamsi, Kanchana Charan Sai, Vijayalakshmi M, "Face recognition based door unlocking using raspberry pi" IJARIIT Publications, Feb 2019	LBPH is one of the easiest face recognition algorithms. It can represent local features in the images. It is possible to get great results (mainly in a controlled environment). It is robust against monotonic gray scale transformations.	Algorithm used is LBPH. first, the method is very sensitive to scale, therefore, a low-level preprocessing is still necessary for scale normalization. Secondly, since the eigenface representation is, in a least squared sense, faithful to the original images, its recognition rate decreases for recognition under varying pose and illumination.
[3]David Gsponer, "Building a raspberry pi security system using facial	The sole purpose of this project was to develop a security system at very low	It does not have a second method for unlocking the incase the face recognition

recognition", Haaga-Helie publications,2018.	cost. It will provide a way for anyone to implement a solution with low-budget hardware. The project's facial recognition is developed in 3 parts: 1. Data gathering 2. Machine learning 3. Facial recognition	does not work on the authorized user.
[4]A.D.Deshmukh, M.G.Nakrani, D.L.Bhuyar, U.B.Shinde, "Face recognition using OpenCV on IoT for smart door ",Elsevier SSN publications, February 2019	Face Detection method used is haar classifiers, The key advantage of a Haar-like feature over most other features is its calculation speed. Due to the use of integral images, a Haar like feature of any size can be calculated in constant time	Its speed of detection by using haar is fast but the accuracy is less than that of the CNN.
[5] Muhammad Arif Azhari Halim, Mohd. Fairuz Iskandar Othman, Aa Zezen Zaenal Abidin, Erman Hamid, Norharyati Harum, Wahidah Md Shah " Face Recognition-based Door Locking System with Two-Factor Authentication Using OpenCV " IEEE Publications December 2021	Face Detection method used is haar classifiers. It have a second method for unlocking the incase the face recognition does not work on the authorized user. The twilo services is used to generate OTP for password recognition.	Its accuracy is high but the twilo service is used to generate OTP it will increase cost it is not effective to identify the person for verification request to unlock the door.

3.SYSTEM ANALYSIS

3.1. PROBLEM STATEMENT:

As with any technology, there are potential drawbacks to using facial recognition, such as threats to privacy, violations of rights and personal freedoms, potential data theft and other crimes. There's also the risk of errors due to flaws in the technology.

Facial recognition isn't perfect. For example, it's less effective at identifying women and people of color than White males. The technology depends upon algorithms to make facial matches. Those algorithms are more robust for White men than other groups because the databases contain more data on White men than women and people of color. This creates unintentional biases in the algorithms.

There are inherent dangers in false positives. Facial recognition software could improperly identify someone as a criminal, resulting in an arrest. This issue is exasperated when you add that the technology struggles with people of color, which increases the potential for racial profiling accusations.

3.2. EXISTING SYSTEM:

In the world of emerging technology, security became an essential component in day to day life. Information theft, lack of security and violation of privacy etc. are the essential components which are needed to be protected. Using smart secure systems for door lock and unlocking became popular nowadays. This is system is being adapted by many countries and first grade countries such as USA, Japan etc. already makes use of this system. This system provides either a facial recognition security feature or a keypad is provided to enter the pass code to unlock the door. Although it provides security to the doors, it also has its own drawbacks: Firstly, if the system mainly uses a facial recognition module, there might be a slight chance that sometimes the face may not be detected and hence the door cannot be unlocked. Secondly, if the system uses a keypad to enter the pass code to unlock the door, there might be a chance that the key maybe is recorded or can be observed by others without users consent. Hence, two-step verification is developed which makes use of facial recognition as the first step and pass code as its following step. But the same issues pertain in the newly developed system.

The Previous techniques used for Image Detection is:

1. Face Recognition-based Door Locking System using OpenCv

2. Intelligent Secure Smart Locking System Using Face Biometrics

3. IoT-Based Security with Facial Recognition Smart Lock System

3.2.1. Face Recognition-Based Door Locking System Using Opencv:

This project develops a face recognition-based door locking system with two-factor authentication using OpenCV. It uses Raspberry Pi 4 as the microcontroller. Face recognition-based door locking has been around for many years, but most of them only provide face recognition without any added security features, and they are costly. The design of this project is based on human face recognition and the sending of a One-Time Password (OTP) using the Twilio service. It will recognize the person at the front door. Only people who match the faces stored in its dataset and then inputs the correct OTP will have access to unlock the door. The Twilio service and image processing algorithm Local Binary Pattern Histogram (LBPH) has been adopted for this system. Servo motor operates as a mechanism to access the door. Results show that LBPH takes a short time to recognize a face. Additionally, if an unknown face is detected, it will log this instance into a "Fail" file and an accompanying CSV sheet. The model of an intelligent door locking system was constructed. Application for Android-based smartphones was created with the ability to decide on face similarity. To set up facial recognition, the OpenCV library was used. The Android app was written in Java. And OpenCV library was written in C++; for this reason, a JAVA binding version of OpenCV was set up. In the end, this library was running in C++ under the hood, but function calls were in JAVA. To train a recognition model, at first dataset must be trained using the LCA algorithm and then applied on an extracted face picture.

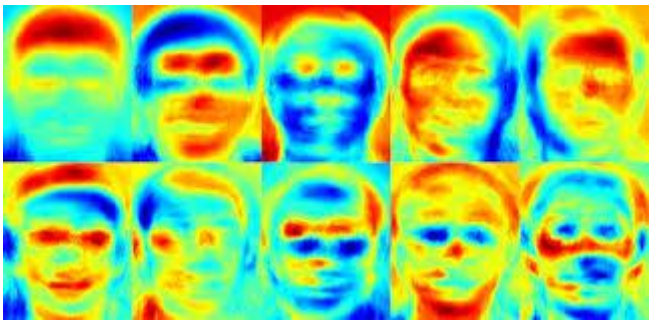

Fig.3.1.Face Recognition with OpenCV

OpenCV has built-in faces dataset; however, they mostly contain European faces. And after training on the provided dataset, the accuracy was 60 % on testing on four teammates. For this reason, it was decided to collect its own dataset. To add a person to the dataset the

application has a “New Person” button, and then the application takes 20 consecutive photos of a face every 200 Ms.

3.2.2. Intelligent Secure Smart Locking System Using Face Biometrics:

The rapid growth of technology in the modern society has raised many questions on the terms like security and privacy. Due to the evolution in the technology and industrialization the terms like security and privacy has become imperative for a common person. Authentication is a key factor which helps for the identification of authorized people and helps in eradicating fraudulent activities, robberies, and many other social crimes. Most of the crimes are due to the vulnerabilities in the door locking systems which can be easily accessible by the outsiders. Though there are solutions like smart doorbells and video streaming, which have limitations like heavy cost, complex and have loopholes in the security issues. To diminish the limitations and to enhance the security Smart door unlock systems using face recognition is proposed. The proposed system consists of a camera sensor popularly known as esp32-cam for storing the pictures of persons and for live streaming. The proposed system recognizes the face of the person standing in front of the door with the help AI-Thinker in the esp32-cam. The face of the person is compared with the faces of the authorized persons which are stored in the SD card of esp32-cam.

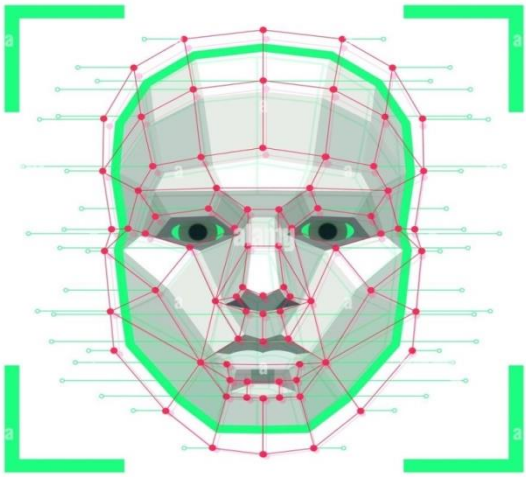

Fig.3.2.Face Recognition using Face Biomertrics

If the person is an authorized person then the door gets unlocked which can be achieved with the hardware component solenoid lock. If the person is an unauthorized person then the door will be locked. The proposed system helps in adapting from traditional mechanical lock methods to enhanced security methods. It also helps in case of losing keys and helpful for

disabled persons with easier access. It is a method of biometric identification that uses that body measures, in this case face and head, to verify the identity of a person through its facial biometric pattern and data. A facial recognition system uses biometrics to map facial features from a photograph or video. It compares the information with a database of known faces to find a match. That's because facial recognition has many commercial applications. It can be used for everything from surveillance to marketing.

3.3.3. IOT-Based Security with Facial Recognition Smart Lock System:

Face recognition door lock system uses camera to capture image which is connected to the Raspberry Pi module for face recognition. If the image is known door will open and if the image is unknown then it will send the image to the website where owner of the house will decide based on the image whether to open the door or not. If the bell is pressed, it activates the camera which captures the image. The image captured is checked against images in the database. If the image matches then the door will be opened and if the image is not recognized then the image of the person is sent to the website http://iotgecko.com/. From where owner of the house can lock or unlock the door. Login credentials are provided to the owner of the house by which he/she has to login and get complete access to the door lock mechanism.

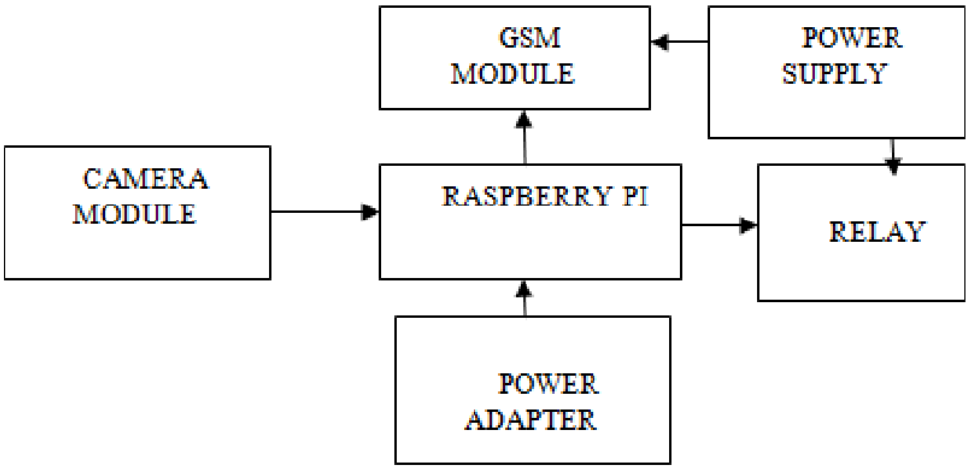

Fig.3.3.IoT Based Faced Recognition

Ones we system is turned on for the first time. LCD display will show you three options: Registration, Start, clear data for the first time, we have to select first option i.e. Registration. When we click on the Registration, camera will open and it will capture images of owner and save it in database. Now, as the owner images are stored in database, we can start the system by selecting second option i.e. Start When we click on start, system will boot up and now if owner presses the bell, camera will recognize the face of the owner and it will

open the door without any human intervention. And if the unknown person comes in front of door and he/she presses the bell then the image will be sent to the website where we provided the facility to the user of locking and unlocking the door. We used Haar cascade Frontal Face to Detect object in video stream and we have created Local Binary Patterns Histograms for face recognition. Proteus is the software we used to generate the PCB design of this model.

3.3. DRAWBACKS OF EXISTING SYSTEM:

By using above mentioned methods in the existing system we get several drawbacks inthose methods. Some important drawbacks are mentioned below:

1. It does not have a second method for unlocking the door in case the face recognition does not work on the authorized user.

2. Algorithm used is LBPH, first, the method is very sensitive to scale, therefore, a low-level pre-processing is still necessary for scale normalization. Secondly, since the eigenface representation is, in a least squared sense, faithful to the original images, its recognition rate decreases for recognition under varying pose and illumination.

3.Its speed of detection by using haar is fast but the accuracy is less than that of the CNN.

4. Its accuracy is high but the twilo service is used to generate OTP it will increase cost it is not effective to identify the person for verification request to unlock the door.

3.4. PROPOSED SYSTEM:

In this project develops a face recognition-based door locking system with two-factor authentication using OpenCV. It uses Raspberry Pi 4 as the microcontroller. Face recognition-based door locking has been around for many years, but most of them only provide face recognition without any added security features, and they are costly. The design of this project is based on human face recognition and the sending of a One-Time Password (OTP) along with image of person through email. It will recognize the person at the front door. Only people who match the faces stored in its dataset and then inputs the correct OTP will have access to unlock the door. The Email service and image processing algorithm Local Binary Pattern Histogram (LBPH) has been adopted for this system. Servo motor operates as a mechanism to access the door. Results show that LBPH takes a short time to recognize a face. Additionally, if an unknown face is detected, it will log this instance into a "Fail" file and an accompanying CSV sheet. It is totally cost efficient when compared to previous systems. By using Twilio it demands some charges to be paid every time to get the one time

password so in this project totally the one time password with image is sent to the mail it is very useful as compared to previous project.

3.5. BLOCK DIAGRAM:

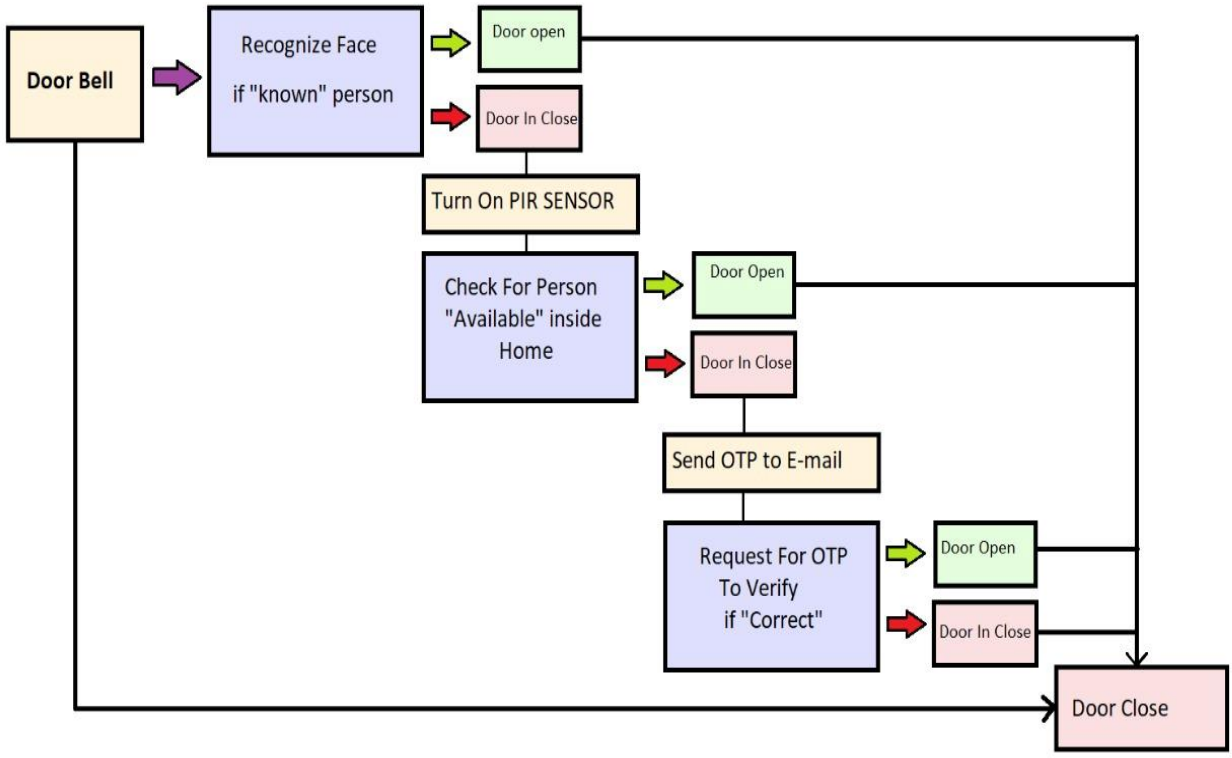

Fig.3.4.Block Diagram of Proposed System

3.6. IMPLEMENTATION:

This paper mainly consists Data Gathering, Training the Recognizer, and Face Recognition. In the first phase, the authorized data of face samples will be collected. For this, we have to take a frame and detect faces. For detecting images, we are using open cv and dlib with Raspberry Pi. After detecting the faces, we will extract the face along with resizing the image. Then, the extracted image will be saved in the database.

In the second phase, the training of recognizers will be done for the saved face samples. for this process, we will take each image from the database and encode that particular face. Finally, the facial encodings of each person will be saved in binary files with the names of the persons. Now, these encodings will be used in the recognition process to identify the owner and the intruder.

In the last phase, the real-time face recognition will be done using trained data. For this process, a real-time frame will be taken and the face will be detected. To capture images, we are using a camera module with Raspberry Pi. Now the face sample is preprocessed and

analyzed. After analysis, the data will be stored in the database. Now the process of comparison of all the stored samples with the newly obtained sample will be carried out. It will search out for the best matching person id. If the match is found, then the person standing outside is authorized hence the lock will get unlocked otherwise a security alert will be sent to the authorized person through SMS along with the image of the intruder.

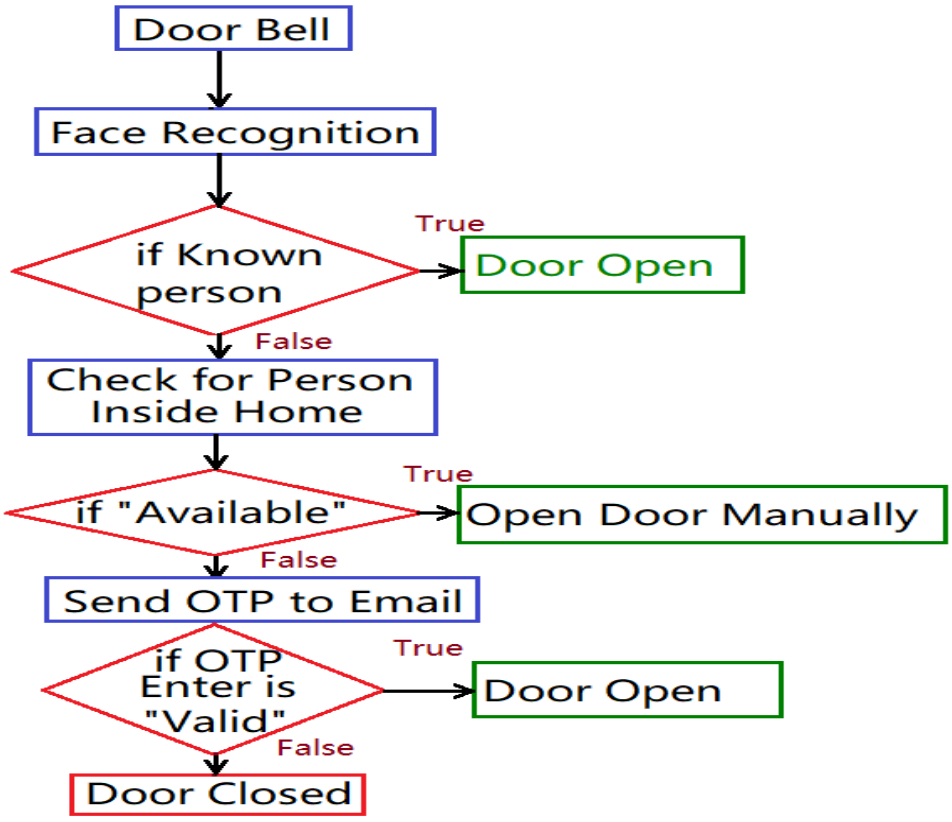

Fig.3.5.Flow chart of Proposed Face Recognition System

3.7. METHODOLOGIES:

3.7.1. Image Processing:

Image processing is a method to perform some operations on an image, in order to get an enhanced image or to extract some useful information from it. It is a type of signal processing in which input is an image and output may be image or characteristics/features associated with that image. Image processing is any form of processing for which the input is an image or a series of images or videos, such as photographs or frames of video. The output of image processing can be either an image or a set of characteristics or parameters related to the image. It also means Analyzing and manipulating images with a computer. There are some examples which are processed on image processing.

Examples:

1. Normalization
2. Edge Filters
3. .Soft focus, selective focus
4. Binning
5. User-specific Filter

3.7.2. Image Segmentation:

Segmentation is the process of partitioning a digital image into multiple segments (sets of pixels, also known as super pixels). The goal of segmentation is to simplify and/or change the representation of an image into something that is more meaningful and easier to analyze. Image segmentation is typically used to locate objects and boundaries (lines, curves, etc.) in images. More precisely, image segmentation is the process of assigning a label to every pixel in an image such that pixels with the same label share certain visual characteristics. The result of image segmentation is a set of segments that collectively cover the entire image, ora set of contours extracted from the image (see edge detection). Each of the pixels in a region is similar with respect to some characteristic or computed property, such as color, intensity, or texture. Adjacent regions are significantly different with respect to the same characteristic(s)when applied to a stack of images, typical in medical imaging, the resulting contours after image segmentation can be used to create 3D reconstructions with the help of interpolation algorithms like Marching cubes.

3.7.3. Local Directional Pattern(LDP):

LDP is a gray-scale texture pattern which characterizes the spatial structure of a local image texture. A LDP operator computes the edge response values in all eight directions at each pixel position and generates a code from the relative strength magnitude. Since the edge responses are more illumination and noise insensitive than intensity values, the resultant LDP feature describes the local primitives including different types of curves, corners, and junctions, more stably and retains more information. Given a central pixel in the image, the eight directionaledge response values {}, 0, 1...,7 i m i= are computed by Kirsch masks i M in eight different orientations centered on its position. The masks are shown in below figure.

The response values are not equally important in all directions. The presence of a corneror edge causes high response values in some directions. Therefore, we are interested in the k mostprominent directions to generate the LDP.

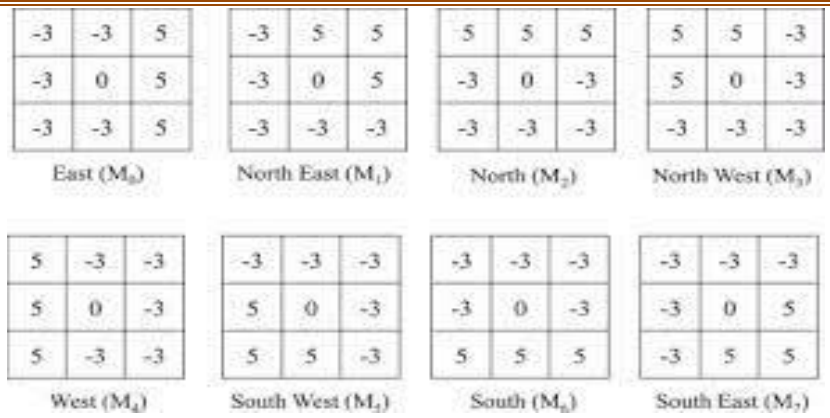

Fig.3.6. Kirsch Edge masks in all Eight Directions

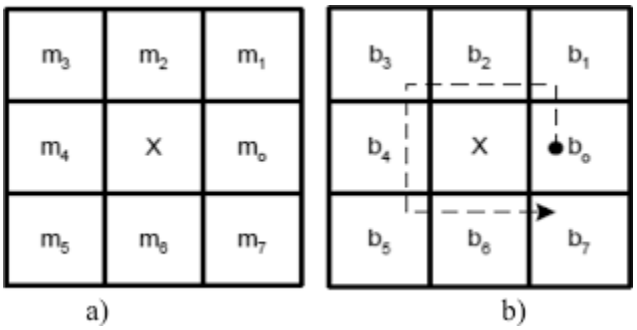

Fig.3.7: Mask Response and LDP Bit Positions

Here, the top k directional bit responses i b are set to 1.The remaining (8-k) bits of the 8-bit LDP pattern are set to 0. Finally, the LDP code is derived using equation 1. Figure3.6 shows the mask response and LDP bit positions, and Figure3.6 shows an exemplary LDP code with k=3. Local Directional Pattern (LDP) is a descriptor used for face recognition. It assigns a code for each pixel in the image, and the resultant LDP-encoded image is divided into regions for which each a histogram is generated. The significance of DR-LDP is the compact code generation for efficient face recognition.

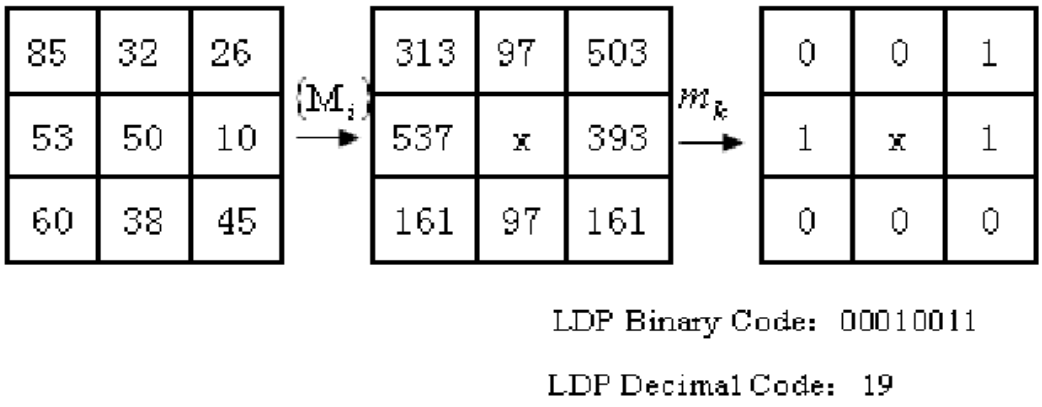

Fig. 3.8.LDP Code with K=3

$$LDP_k = \sum_{i=0}^{7} b_i(m_i - m_k) \times 2^i$$

$$b_i(a) = \begin{cases} 1 & a \geq 0 \\ 0 & a < 0 \end{cases}$$

Where, mk is the k-th most significant directional response. Since edge responses are more stable than intensity values, LDP pattern provides the same pattern value even presence of noise and non-monotonic illumination changes. After computing the LDP code for each pixel (r , c) ,the input image I of size M × N is represented by a LDP histogram H using equation 3. The resultant histogram H is the LDP descriptor of that image.

The LBP operator labels the pixels of an image by thresholding a 3x3 neighborhood of each pixel with the center value and considering the results as a binary number, of which the corresponding decimal number is used for labeling. The derived binary numbers are called local binary patterns or LBP codes. While the LBP operator uses the information of intensity changes around pixels, LDP operator use the edge response values of neighborhood pixels and encode the image texture. The LDP is computed as follow [24, 25]. The LDP assigns an 8 bit binary code to each pixel of an input image. This pattern is then calculated by comparing the relative edge response values of a pixel by using Kirsch edge detector. Given a central pixel in the image, the eight-directional edge response values are computed by Kirsch masks as shown in Figure 1. Since the presence of a corner or an edge shows high response values in some particular directions, thus, most prominent directions of number with high response values are selected to generate the LDP code. In other words, directional bit responses are set to 1, and the remaining bits are set to0.

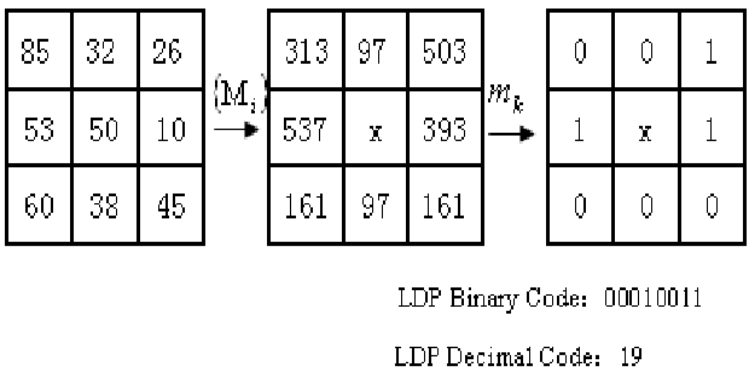

Fig.3.9. Edge Response and LDP Binary Bit Positions

3.7.4. Histogram:

Histogram Equalization is a computer image processing technique used to improve contrast in images. It accomplishes this by effectively spreading out the most frequent intensity values, i.e. stretching out the intensity range of the image. An image histogram is a type of histogram that acts as a graphical representation of the tonal distribution in a digital image. It plots the number of pixels for each tonal value. By looking at the histogram for a specific image a viewer will be able to judge the entire tonal distribution at a glance. In digital image processing, histograms are used for simple calculations in software. It is used for image equalization. Gray level intensities are expanded along the x-axis to produce a high contrast image.Histograms are used in thresholding as it improves the appearance of the image. The purpose of a histogram (Chambers) is to graphically summarize the distribution of a univariate data set. The histogram graphically shows the following: skewness of the data; presence of outliers. A histogram is a chart that plots the distribution of a numeric variable's values as a series of bars. Each bar typically covers a range of numeric values called a bin or class; a bar's height indicates the frequency of data points with a value within the corresponding bin. It helps to visualize the distribution of the data. Demerits are:1) Cannot read exact values because data is grouped into categories. 2) More difficult to compare two data sets. 3) Use only with continuous data. A histogram is an approximate representation of the distribution of numerical data. To construct a histogram, the first step is to "bin" (or "bucket") the range of values—that is, divide the entire range of values into a series of intervals

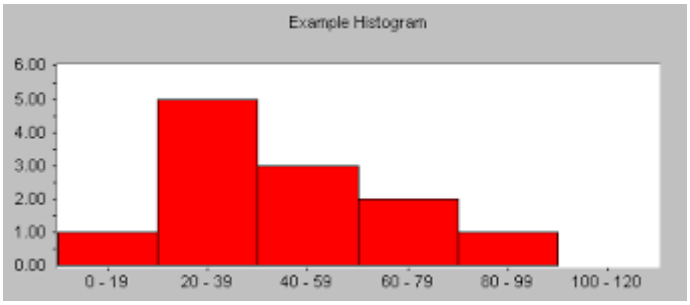

Fig.3.10.Histogram Representation

3.7.5. Local Binary Pattern Histogram(LBPH):

LBPH (Local Binary Pattern Histogram) is a Face-Recognition algorithm it is used to recognize the face of a person. It is known for its performance and how it is able to recognize the face of a person from both front face and side face. Local Binary Pattern (LBP) is an effective texture descriptor for images which thresholds the neighboring

pixels based on the value of the current pixel. LBP descriptors efficiently capture the local spatial patterns and the gray scale contrast in an image. For calculating the LBP, the LBP code for each pixel is calculated and the histogram of LBP codes is constructed as the LBP feature.

To calculate the lbp code, for each pixel p, the 8 neighbors of the center pixel are compared with the pixel p and the neighbor's x are assigned a value 1 if $x \geq p$. LBP feature vector, returned as a 1-by-N vector of length N representing the number of features. LBP features encode local texture information, which you can use for tasks such as classification, detection, and recognition. The function partitions the input image into non-overlapping cells. In addition to face and facial expression recognition, the LBP has also been used in many other applications of biometrics, including eye localization, iris recognition, fingerprint recognition, palmprint recognition, gait recognition and facial age classification. So to find the image that matches the input image we just need to compare two histograms and return the image with the closest histogram.

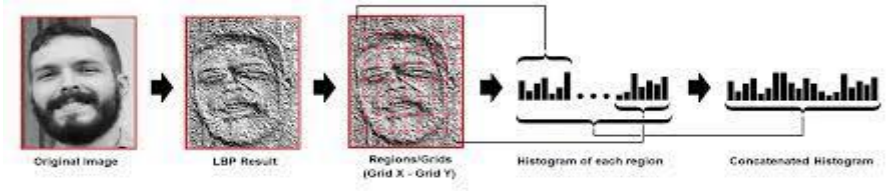

Fig.3.1.1.LBPH Representation of Image

So the algorithm output is the ID from the image with the closest histogram. The algorithm should also return the calculated distance, which can be used as a 'confidence' measurement. Note: don't be fooled about the 'confidence' name, as lower confidences are better because it means the distance between the two histograms is closer.

Eigenfaces and Fisherfaces take a somewhat holistic approach to face recognition. You treat your data as a vector somewhere in a high-dimensional image space. We all know high-dimensionality is bad, so a lower-dimensional subspace is identified, where (probably) useful information is preserved. The Eigenfaces approach maximizes the total scatter, which can lead to problems if the variance is generated by an external source, because components with a maximum variance over all classes aren't necessarily useful for classification. So to preserve some discriminative information we applied a Linear Discriminant Analysis and optimized as described in the Fisherfaces method. The Fisherfaces method worked great at least for the constrained scenario we've assumed in our model.

Now real life isn't perfect. You simply can't guarantee perfect light settings in your images or 10 different images of a person. So what if there's only one image for each person? Our covariance estimates for the subspace *may* be horribly wrong, so will the recognition. Remember the Eigenfaces method had a 96% recognition rate on the AT&T Face database? . How many images do we actually need to get such useful estimates? Here are the Rank-1 recognition rates of the Eigenfaces and Fisherfaces method on the AT&T Facedatabase, which is a fairly easy image database.

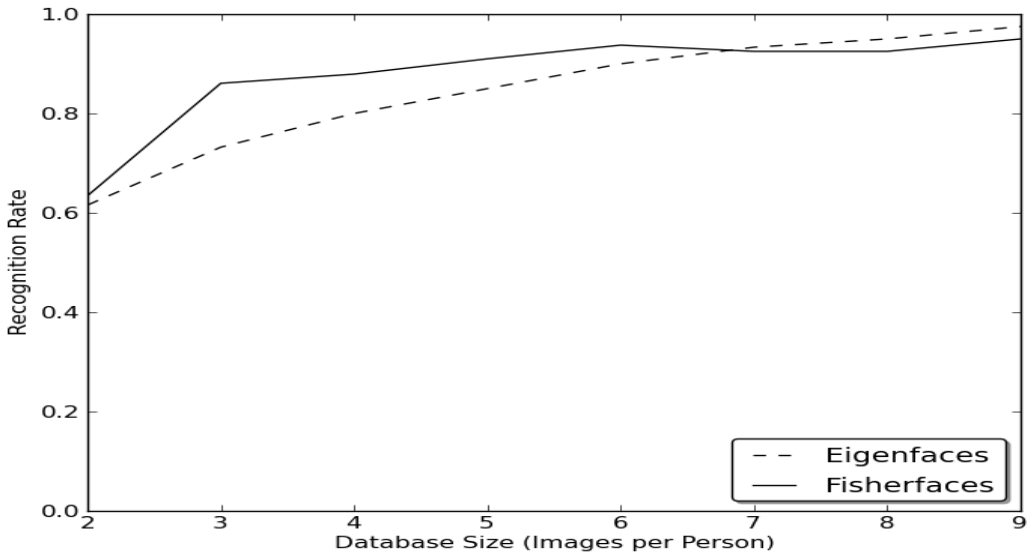

Fig.3.1.2.LBPH Pattern in Graphical form

3.7.6. Gray Scaling:

Gray scaling is the process of converting an image from other color spaces e.g. RGB, CMYK, HSV, etc. to shades of gray. It varies between complete black and complete white a series of regularly spaced tones ranging from black to white through intermediate shades of gray also an image composed solely of gray scale tones. The main reason why grayscale representations are often used for extracting descriptors instead of operating on color images directly is that grayscale simplifies the algorithm and reduces computational requirements. Grayscale images are distinct from one-bit bi-tonal black-and-white images, which, in the context of computer imaging, are images with only two colors: black and white (also called bilevel or binary images). Grayscale images have many shades of gray in between. Grayscale images can be the result of measuring the intensity of light at each pixel according to a particular weighted combination of frequencies (or wavelengths), and in such cases they are monochromatic proper when only a single frequency (in practice, a narrow band of

frequencies) is captured. The frequencies can in principle be from anywhere in the electromagnetic spectrum.

3.7.7. Image Enhancement:

Image enhancement is the procedure of improving the quality and information content of original data before processing. Common practices include contrast enhancement, spatial filtering, density slicing, and FCC. Image enhancement is the process of adjusting digital images so that the results are more suitable for display or further image analysis. For example, you can remove noise, sharpen, or brighten an image, making it easier to identify key features. The aim of image enhancement is to improve the interpretability or perception of information in images for human viewers, or to provide `better' input for other automated image processing techniques. Principle objective of Image enhancement is to process an image so that result is more suitable than original image for specific application. Digital image enhancement techniques provide a multitude of choices for improving the visual quality of images.

3.8. PRELIMINARIES:

Face Recognition: Face recognition is a method of identifying an individual identity utilizing their face. This technology can match a human individual face from a computerized image or a video frame against a database or in real-time. OpenCV: OpenCV is a very large open source library use for computer vision, machine learning, and image processing it also plays a major role in real-time operation. This library provides us tools for processing and analysing the content of a computerized picture. Dlib in Python: Dlib in python is used for facial mapping, it uses the pre-trained models to identify the different facial landmarks. It calculates the location of 68 coordinates (x, y) which maps the facial points on an individual face.

4.SYSTEM REQUIREMENTS

4.1. HARDWARE TOOLS REQUIRED:

4.1.1 Raspberry Pi:

Raspberry Pi (RP) is an ARM-based single board computer. The Raspberry Pi 3 Model B is the third generation Raspberry Pi [3].It has Broadcom BCM2837 64bit ARM Cortex-A53 Quad Core Processor SoC running at 1.2GHz and 1GB RAM. The operating system used for Raspberry Pi is Raspbian as it is open source anyone can use. Raspbian is a Linux-based computer operating system. It has 40 pins in which 24 are GPIO pins these pins are used for general purpose, 8 ground pins, two of each 5V and 3V power pin. It has four USB-2 ports and a Micro USB power source. It runs on the 5V power supply. Additionally, it adds wireless LAN (BCM43143 WiFi on board (802.11 a/b/g/n)) and Bluetooth connectivity making it the ideal solution for powerfully connected designs.

Family	**Model**	**Form**	**Ethernet**	**Wireless**	**GPIO**	**Released**	**Discontinued**
Raspberry Pi 1	A+	Compact (65 × 56.5 mm)	No	No	40-pin	2014	
Raspberry Pi 1	A	Standard (85.60 × 56.5 mm)	No	No	26-pin	2013	Yes
Raspberry Pi 1	B+	Standard (85.60 × 56.5 mm)	Yes	No	40-pin	2014	

Raspberry Pi 1	B	Standard (85.60 × 56.5 mm)	Yes	No	26-pin	2012	Yes
Raspberry Pi 2	B	Standard	Yes	No	40-pin	2015	
Raspberry Pi 3	A+	Compact	No	Yes	40-pin	2018	
Raspberry Pi 3	B+	Standard	Yes	Yes	40-pin	2018	
Raspberry Pi 3	B	Standard	Yes	Yes	40-pin	2016	
Raspberry Pi 4	B (4 GB)	Standard	Yes	Yes	40-pin	2019	
Raspberry Pi 4	B (2 GB)	Standard	Yes	Yes	40-pin	2019	
Raspberry Pi 4	B (1 GB)	Standard	Yes	Yes	40-pin	2019	
Raspberry Pi Zero	Zero	Zero (65 × 30 mm)	No	No	40-pin	2015	
Raspberry Pi Zero	W/WH	Zero (65 × 30 mm)	No	Yes	40-pin	2017	

Table 1.Raspberry pi Models

How Raspberry Pi Works?

An SD card read by USB and the video output can be hooked up to a traditional RCA TV set, a inserted into the slot on the board acts as the hard drive for the Raspberry Pi, it is pow more modern monitor, or even a TV using the HDMI port. This gives you all of the

basic abilities of a normal computer. It also has an extremely low power consumption of about 3 watts.

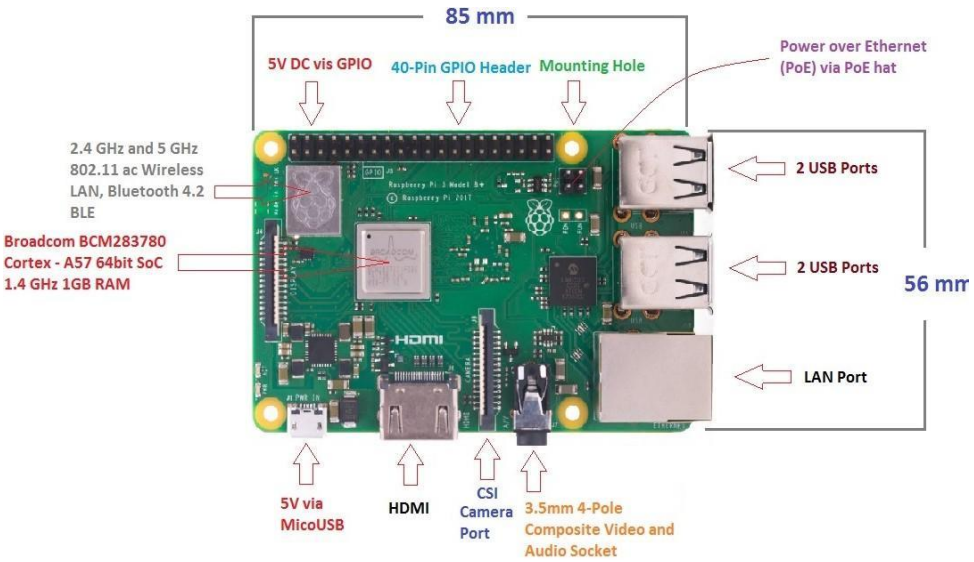

Fig.4.1.1 An Image of Raspberry Pi

Here we are using Raspberry Pi 3B+ board. Firstly, get your Raspberry Pi board and lay it on the table in front of you. And install the Raspbian OS into the Raspberry pi 3b+ through the following steps.

4.1.1.1. installation of Raspbian OS in Raspberry Pi:

Step1: Download the required Software and Files

You need to download 2 software's and 1 OS i. e. Raspbian for this complete process.

1st Software : The first software is Win32 Disk Imager.

https://sourceforge.net/projects/Win32diskimager/

Fig.4.1.2. Downloading Image of Raspbian OS

2nd Software : Second software is SD Card Formatter.

https://www.sdcard.org/downloads/formatter_4/

Raspbian OS : This is the Main operating system of the Pi.

https://www.rasberrypi.org/downlods/raspbian/

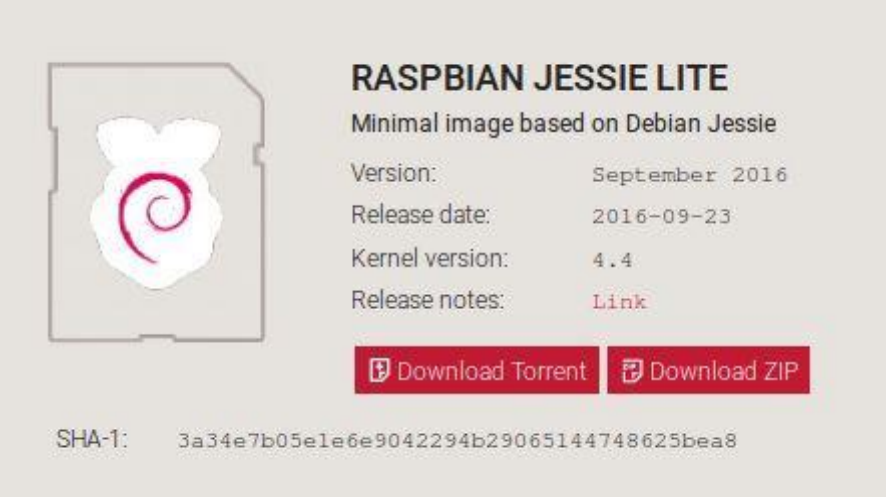

Fig.4.1.3. Extracting Files of OS

Step 2 : Get the SD card and the Card Reader

Get a minimum 8GB class 10 SD card with a card reader.

Insert that card into the card reader and plug that to the USB port.

Step 3 : Check the Drive in which SD Card is Mounted

Go to my computer or MY PC and find the drive name where the SD card is mounted.

Step 4 : Format the SD Card

Open SD Card Formatter and select the drive the drive you noticed in the previous step.

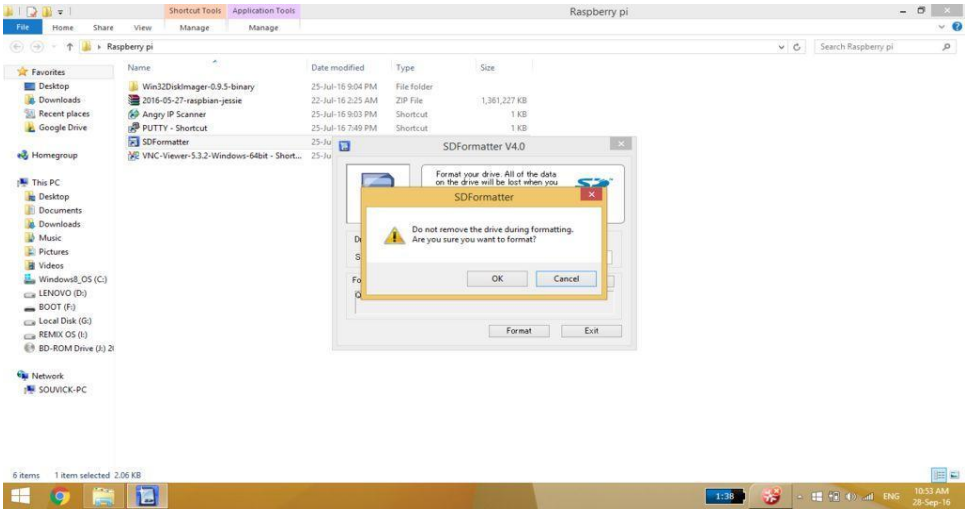

Fig.4.1.4. Formatting SD Card

Step 5 : Write the OS on the SD Card

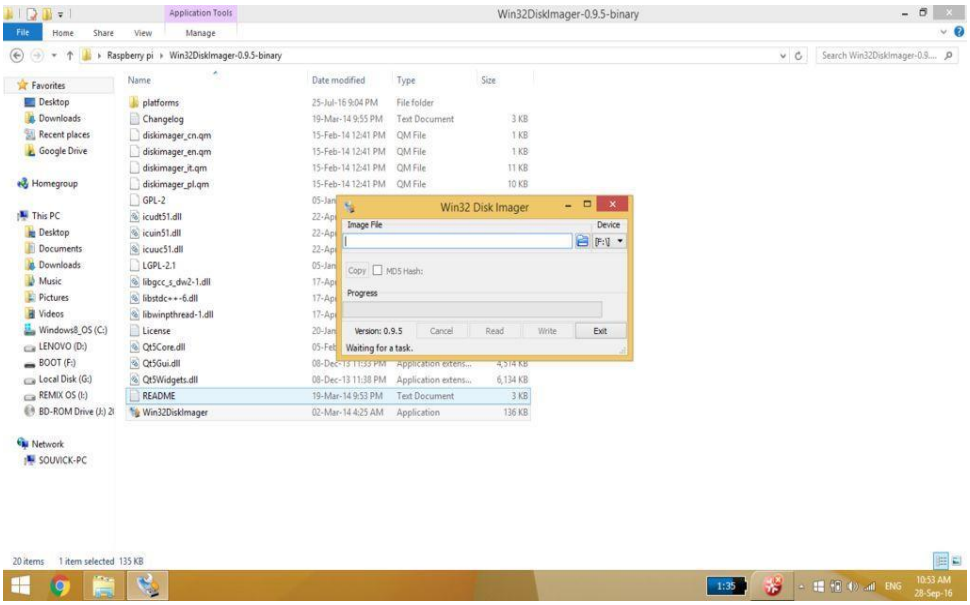

Fig.4.1.5. OS on the SD Card

Open **Win32 Disk Imager**

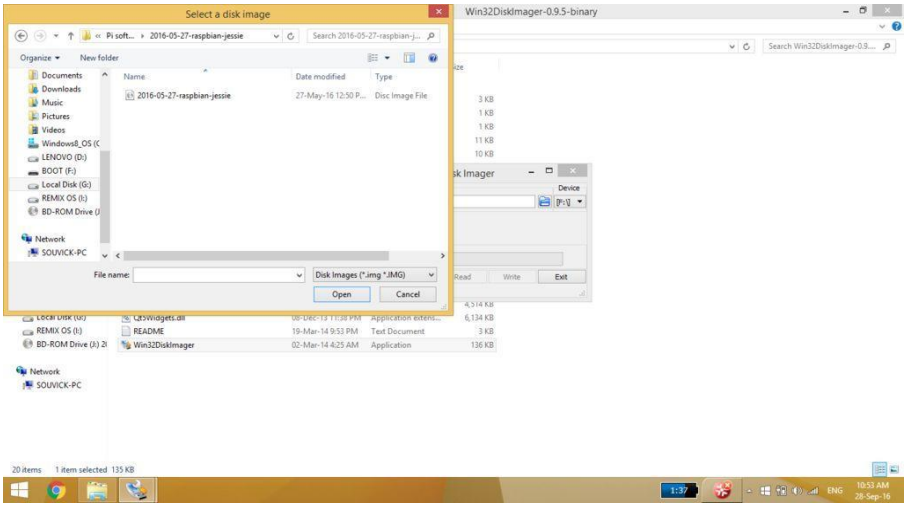

***Fig.4.1.6.* Disk Imager**

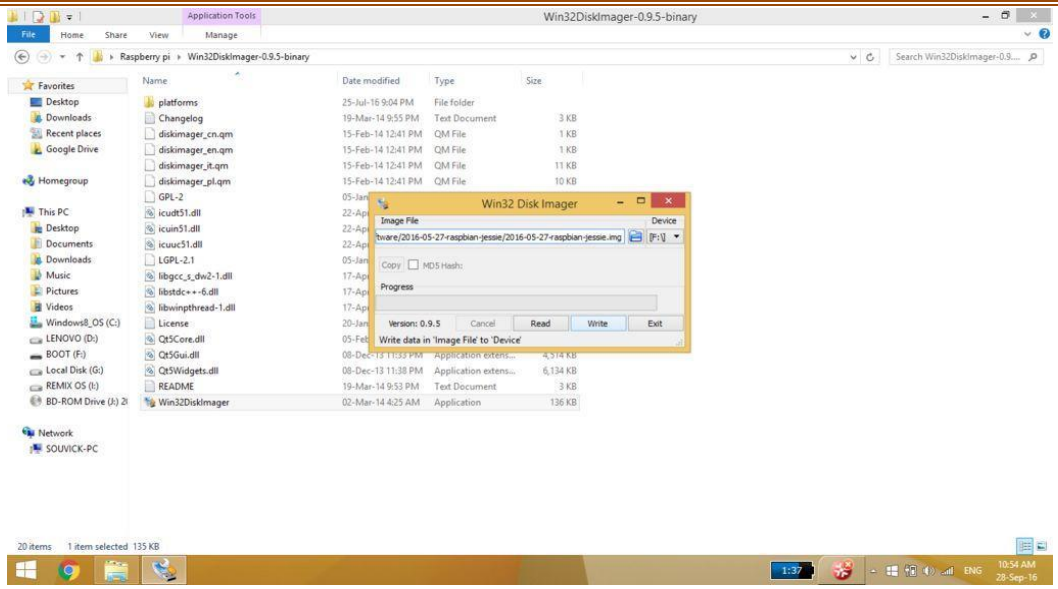

Fig.4.1.7.Browse the .img file of Raspbian OS that was extracted from the file

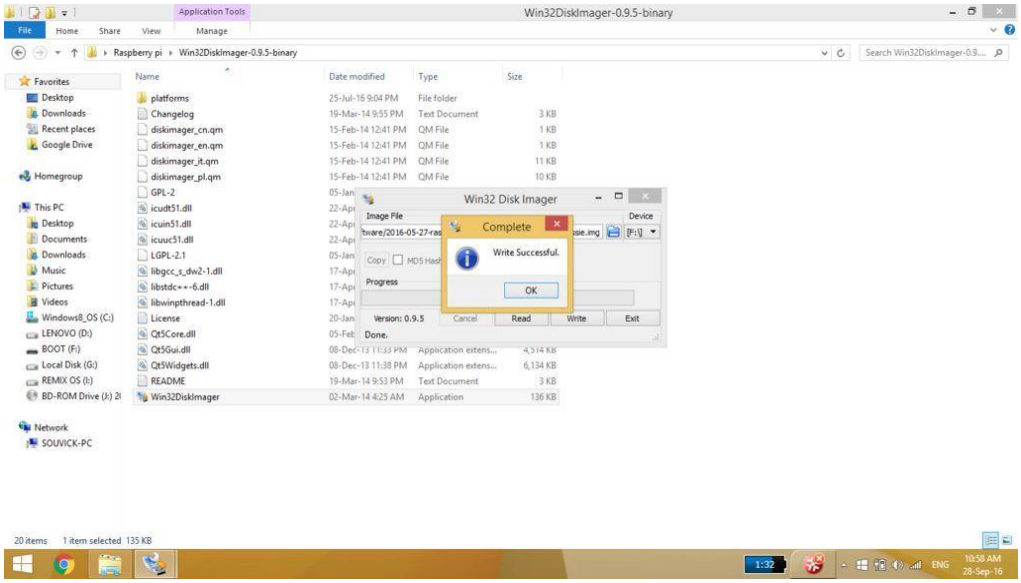

Fig: 4.1.8. Click on open and then write. If any warning pops up then ignore it

Step 6 : Eject the SD Card

Now OS is installed in Raspberry Pi

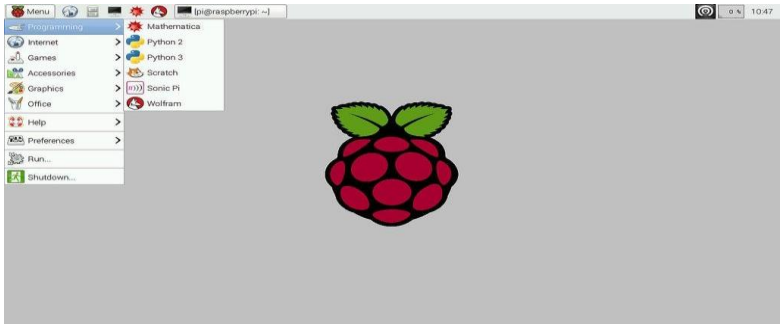

Fig.4.2.0.Raspbian OS Installed in the System

4.1.2 Pi Camera:

Pi Camera Module is a custom designed add-on for Raspberry Pi. This interface uses the dedicated CSI interface, which was designed especially for interfacing to cameras [4] The CSI bus is capable of extremely high data rates, and it exclusively carries pixel data. The sensor itself has a native resolution of 5 megapixels and has a fixed focus lens on board. In terms of still images, the camera is capable of 2592 x 1944- pixel static images, and supports 1080p30, 720p60 and 640x480p60/90 video.

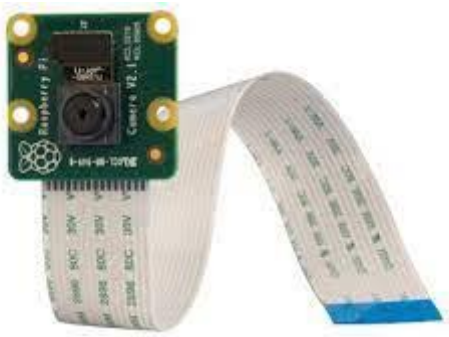

Fig.4.2.1 Raspberry Pi Camera Module

4.1.3 Keypad:

A 3X4 keypad has 4 rows and 3 columns, and a 4X4 keypad has 4 rows and 4 columns: Beneath each key is a membrane switch. Each switch in a row is connected to the other switches in the row by a conductive trace underneath the pad.

The Raspberry Pi keyboard has three lock keys: Num Lock, Scroll Lock, and Caps Lock. Scroll Lock (ScrLk) – Allows use of the cursor keys for browsing web pages and spreadsheets without the mouse. This mode is enabled and disabled by pressing the ScrLk key while holding the Fn key.

Fig.4.2.2. Raspberry Pi keypad

4.1.4 Servo Motor:

A type of servomotor that uses DC electrical input to generate mechanical output like velocity, acceleration or position is known as DC servomotor. It is somewhat similar to a normal DC motor. Basically, DC servomotors of all types are required to be excited individually.

Attach the servo to a GPIO (we selected GPIO 17 here) of the Raspberry pi A and control its rotation utilizing pulse-width modulation. The servo is powered by a 6V-battery pack.

Dc servo motor characteristics include inertia, physical shape, costs, shaft resonance, shaft configuration, speed, and weight. Although these dc servo motors have similar torque ratings, their physical and electrical constants vary.

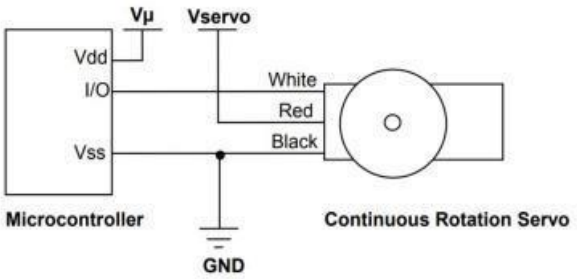

Figure 2: Servo

Fig.4.2.3. Phase DC Servo Motor

4.2. SOFTWARE REQUIREMENTS:

4.2.1 Proteus:

The Proteus Design Suite is a proprietary software tool suite used primarily for electronic design automation. The software is used mainly by electronic design engineers and technicians to create schematics and electronic prints for manufacturing printed circuit boards. The Proteus Design Suite is a Windows application for schematic capture, simulation, and PCB (Printed Circuit Board) layout design. It can be purchased in many configurations, depending on the size of designs being produced and the requirements for microcontroller simulation. All PCB Design products include an autorouter and basic mixed mode SPICE simulation capabilities.

Proteus is a complete development platform from product concept to design completion. Its advantages are intelligent principle layout, hybrid circuit simulation and accurate analysis, single-chip software debugging, single-chip and peripheral circuit co-

simulation, PCB automatic layout and wiring. The Proteus Design Suite is a proprietary software tool suite used primarily for electronic design automation. The software is used mainly by electronic design engineers and technicians to create schematics and electronic prints for manufacturing printed circuit boards.

Proteus is a simulation software used to simulate components and is capable of drawing desired circuit. It is being used for fast checkup of code you have written for microcontrollers.

4.2.2 Proteus Function Library:

SnapEDA is a free online Proteus CAD library of symbols, decals (footprints), and 3D models for millions of electronic components.

Arduino Library for Proteus. Using this Library you can easily simulate Arduino boards in Proteus and can design any kind of circuit. This Arduino Library is the first one in this Proteus Libraries list. Once you install this Arduino Library for Proteus, you will be able to easily simulate Arduino boards in Proteus.

GPS is a very useful module which is used in almost every navigation project. GPS is used for detection of user location. It works in NMEA coding and gives longitude and latitude. Most of the GPS modules are operated through Serial Port i.e. they give data via serial ports. We have designed this GPS module for Proteus using which you can easily simulate this GPS module. I have skm53 in mind while designing this GPS Library for Proteus but still you can use it for any kind of GPS modules because most of them works on NMEA coding so all NMEA coded modules follow this GPS module.

4.2.3 Proteus Application Program Interface(API):

When you use an application on your mobile phone, the application connects to the Internet and sends data to a server. It enables you to write and apply your firmware to a microcontroller component on the schematic and then co-simulate the program within a mixed-mode SPICE circuit simulation. It is used both to design 'virtual hardware' for Proteus VSM simulation and then also for PCB design using our PCB Layout module. Proteus is a complete development platform from product concept to design completion. Its advantages are intelligent principle layout, hybrid circuit simulation and accurate analysis, single-chip software debugging, single-chip and peripheral circuit co-simulation, PCB automatic layout and wiring.

4.2.4 Python 3.8:

Python is an interpreted, object-oriented, high-level programming language with dynamic semantics. Python supports modules and packages, which encourages program modularity and code reuse. Besides web and software development, Python is used for data analytics, machine learning, and even design. We take a closer look at some of the uses of Python, as well as why it's such a popular and versatile programming language. The programming language is used globally to design and build 2D imaging software like Inkscape, GIMP, Paint Shop Pro, and Scribus.

4.2.5 Python In Image Processing:

PIL (Python Imaging Library) is an open-source library for image processing tasks that requires python programming language. PIL can perform tasks on an image such as reading, rescaling, saving in different image formats. PIL can be used for Image archives, Image processing, Image display.

Numpy it is an open-source python library that is used for numerical analysis. It contains a matrix and multi-dimensional arrays as data structures. But NumPy can also use for image processing tasks such as image cropping, manipulating pixels, and masking of pixel values.

4.2.6 Opencv:

OpenCV-Python is a library of Python bindings designed to solve computer vision problems. OpenCV is a great tool for image processing and performing computer vision tasks. It is an open-source library that can be used to perform tasks like face detection, objection tracking, landmark detection, and much more. It supports multiple languages including python, java C++.

OpenCV is used as an image processing library in many computer vision real-time applications. As we know an image is a combination of pixels, for a color image we have three channels with pixels ranging from 0 to 225, and for black & white-colored images has only one change ranging from 0 to 1. OpenCV is a video and image processing library and it is used for image and video analysis, like facial detection, license plate reading, photo editing, advanced robotic vision, and many more. This project utilizes OpenCV Library to make a Real-Time Face Detection using your webcam as a primary camera. Approach/Algorithms used: This project uses LBPH (Local Binary Patterns Histograms) Algorithm to detect faces.

4.2.7 Virtual Serial Port Emulator(Vspe) :

Virtual Serial Port Emulator. Virtual Serial Port Emulator allows you to create an unlimited number of virtual COM ports. The software emulates serial port functionality connected by virtual null modem cable in such a way that the system does not see the difference between virtual and real hardware ports. It is a software application that replicates physical COM ports. The virtual serial ports that are created are fully compatible with operating systems and applications and are treated in the same way as a real port. A software-based virtual serial port presents one or more virtual serial port identifiers on a PC which other applications can see and interact with as if they were real hardware ports, but the data sent and received to these virtual devices is handled by software that manipulates the transmitted and received data to grant greater functionality.

Operating systems usually do not provide virtual serial port capability. Third-party ;applications can add this ability, such as the open-source com0com, freeware HW VSP3, or the commercial Virtual Serial Port Driver.

Some virtual serial ports emulate all hardware serial port functionality, including all signal pin states, and permit a large number of virtual ports in any desired configuration. Others provide a limited set of capabilities and do not fully emulate the hardware.

This technique can be used either to extend the capabilities of software that cannot be updated to use newer communication technologies, such as by transmitting serial data over modern networks, or to achieve data flows that are not normally possible due to software limitations, such as splitting serial port output.

A serial port typically can only be monitored or transmitted to by one device at a time under the constraints of most operating systems, but a virtual serial port program can create two virtual ports, allowing two separate applications to monitor the same data. For instance, a GPS device which outputs location data to a PCs serial port may be of interest to multiple applications at once. It allows two computers to send and receive data. This library has the flexibility to communicate with custom microcontroller devices and to use them as the input or output to Processing programs. The serial port is a nine pin I/O port that exists on many PCs and can be emulated through USB.

4.3.FEASIBILITY STUDY:

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis

the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are:

- Economical Feasibility
- Technical Feasibility
- Social Feasibility

4.3.1.Economical Feasibility:

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus, the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

4.3.2.Technical Feasibility:

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

4.3.3.Social Feasibility:

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His/ Her level of confidence must be raised so that he/she is also able to make some constructive criticism, which is welcomed, as he/she is the final user of the system.

5.SYSTEM DESIGN

5.1.SYSTEM ARCHITECTURE:

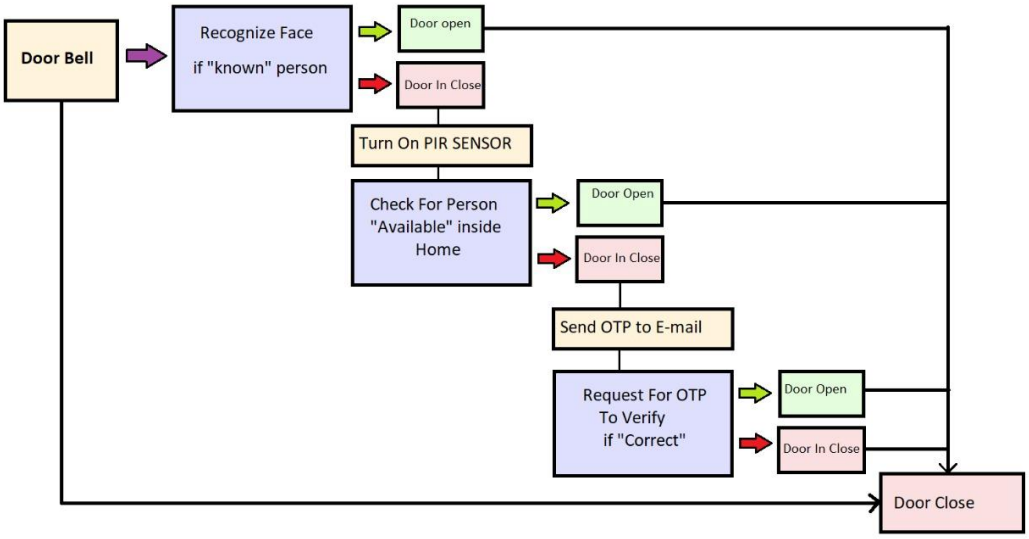

Fig:5.1.System Architecture

The Raspberry Pi board consists of ports to connect the required components. We connect all the required hardware components as shown in figure 5.1.

The Raspberry Pi board is connected to a monitor using a HDMI to VGA converter cable along with a web camera which is used to capture the video and the buzzer is also used which alerts the driver when the drowsiness is detected.

The Raspberry Pi contains Raspbian OS in which the python is pre-installed by default. We use the python library called Open CV (Open Source Computer Vision) which contains the default functions for detecting eyes from face. The algorithm called Eye Aspect Ratio (EAR) is used for blink detection. After detecting drowsiness, the information like date and time of the drowsiness are stored automatically into a cloud database.

5.2. MODULES:

5.2.1. Video Capturing Module:

When the system is turned on, the power supply is provided to the system. The Camera starts to capture the video of the driver. After that, the system takes input frames from the camera. We have to connect this camera to the Raspberry Pi board and this takes the power from the board.

The capturing frames can be seen in the monitor which also shows the detection of eyes by drawing boundaries across the eyes. The calculated eye aspect ratio is also displayed

in the monitor. When the drowsiness is detected a warning “drowsiness alert” is also displayed in the frame. The method videostream( ) is used to start the camera and capture the video.

5.2.2. Image Processing Module:

OpenCV (Open Source Computer Vision) is a library of programming functions mainly aimed at real-time computer vision. It is also a library which is used for image processing. It is mainly used to do all the operation related to images. It uses the predefined functions like dlib, which is used in image processing like detecting and extracting facial landmarks. A night vision camera is used to handle different light conditions.

The libraries like cv2 and dlib are used to perform image processing and the make use of methods like get_frontal_face_detector and shape_predictor , which are used to detect the face of the driver and also to detect eyes from the face. The algorithm Eye Aspect Ratio (EAR) will be used for eye blink detection. This module is processed after the input is taken from the camera.

5.2.3. Alert Module:

A buzzer is an audio signaling device, which may be mechanical, electromechanical or piezoelectric. Typical users of buzzers and beepers include alarm devices, timers and confirmation of user input such as mouse click or keystroke.

A buzzer or an alarm is connected to the raspberry pi board in the (21,1) pins. When the eye closure period is greater than the normal blinking period then this buzzer is activated and it stops as soon as the driver open his eyes. To recognize the buzzer rpi.gpio method is used in the system.

5.2.4. Database Module:

After the alerting is provided the information like the date, time and the number of times the driver got drowsy is stored in the cloud database. The driver can login to the system and check these details.

For this to happen, the hyperlink of the cloud database is included in the code. This module is optional. If we don’t want to store this data we can remove the hyperlink.

5.3. Image Encoding:

A face encoding is basically a way to represent the face using a set of 128 computer-generated measurements. Two different pictures of the same person would have similar

encoding and two different people would have totally different encoding. 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.

Face encoder is used to get the (128,1) dimension encoding of the image which is passed to it. It is a pretrained ResNet network model with 29 conv layers. The model is trained on a dataset of about 3 million faces modelFile, configFile are the files for the dnn based cv2 face detection model.

5.4 UML DIAGRAMS:

5.4.1 Introduction To UML:

UML (Unified Modeling Language)

UML is a language for visualizing, specifying, constructing and documenting the artifacts of a software intensive system. UML is simply another graphical representation of a common semantic model. UML diagrams are the ultimate output of the entire discussion. All the elements, relationships are used to make a complete UML diagram and the diagram represents a system.

The visual effect of the UML diagram is the most important part of the entire process. All the other elements are used to make it a complete one.UML includes the following nine diagrams and the details are described in the following chapters.

- Class diagram
- Object diagram
- Use case diagram
- Sequence diagram
- Collaboration diagram
- Activity diagram
- State chart diagram
- Deployment diagram
- Component diagram

UML defines several models for representing systems

1. **Use case diagram :** represents the functions of a system from the user's point of view.
2. **Class diagram :** represents the static structure in terms of classes and relationships

3. **Object diagram :** represents objects and their relationships and correspond to simplified collaboration diagrams that do not represent message broadcasts.
4. **Sequence diagram :** Temporal representation of objects and their interactions.
5. C**ollaboration diagram :** Spatial representation of objects, links, and interactions.
6. **State chart diagram :** represents the behavior of a class in terms of states at run time.
7. **Activity diagram :** represents the behavior of an operation as a set of actions.
8. **Component diagram :** represents the physical components of an application.
9. **Deployment diagram :** represents the deployment of components on particular pieces of hardware.

Advantages

- To represent complete systems (instead of only the software portion) using object-oriented concepts.
- To establish an explicit coupling between concepts and executable code.
- To take into account the scaling factors that are inherent to complex and critical systems.
- To create a modeling language usable by both humans and machines.

Conceptual model of UML can be mastered by learning the following three major elements:

- UML building blocks.
- Rules to connect the building blocks.
- Common mechanisms of UML.

5.4.2 Class Diagram:

AIM: To implement class diagram for Face Recognition System Using Opencv.

DESCRIPTION: A class diagram shows a set of classes, interfaces and collaborations and their relationships.

OBJECTIVE : The main objective of the class diagram to illustrate the static design of a view system.

THINGS : class, interfaces, collaboration, active class.

RELATIONSHIPS : Dependency, generalization and association

5.4.3 Use Case Diagram:

AIM : To implement use case diagram for Face Recognition System Using Opencv.

DESCRIPTION : Use case diagrams are central to modeling the behavior of the system or a class. Use case diagrams are important for testing executable systems through reverse engineering.

OBJECTIVE : Use case diagram organizes the behavior of the system.

THINGS : Use cases, Actors.

RELATIONSHIPS : Dependency, generalization and Association.

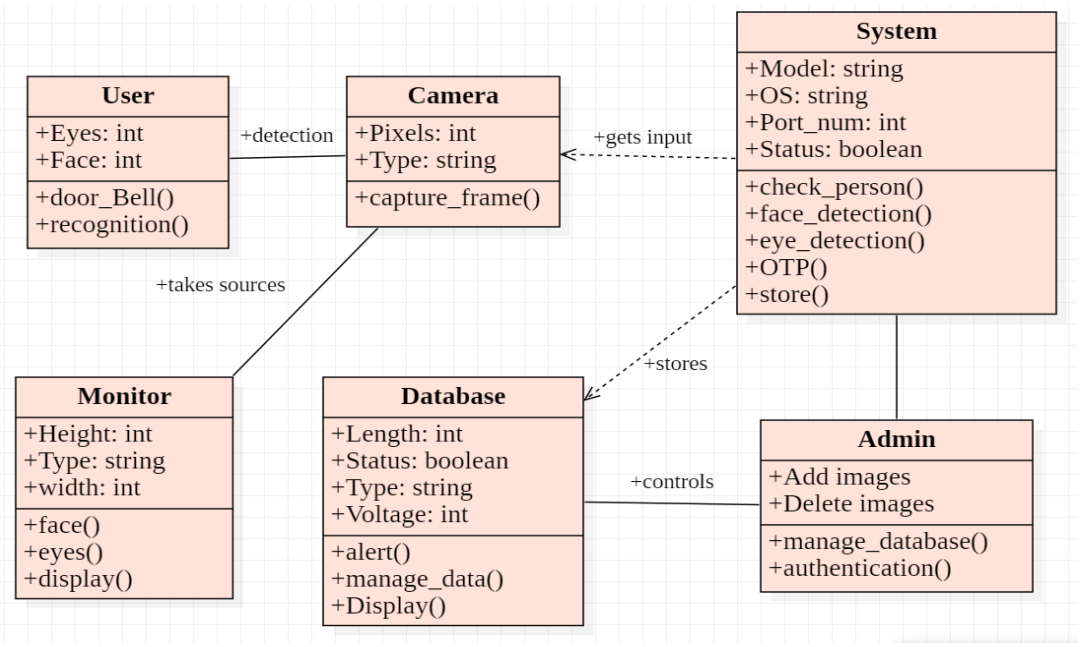

Fig.5.2.Class Diagram

5.4.3 Use Case Diagram:

AIM : To implement use case diagram for Face Recognition System Using Opencv.

DESCRIPTION : Use case diagrams are central to modeling the behavior of the system or a class. Use case diagrams are important for testing executable systems through reverse engineering.

OBJECTIVE : Use case diagram organizes the behavior of the system.

THINGS : Use cases, Actors.

RELATIONSHIPS : Dependency, generalization and Association.

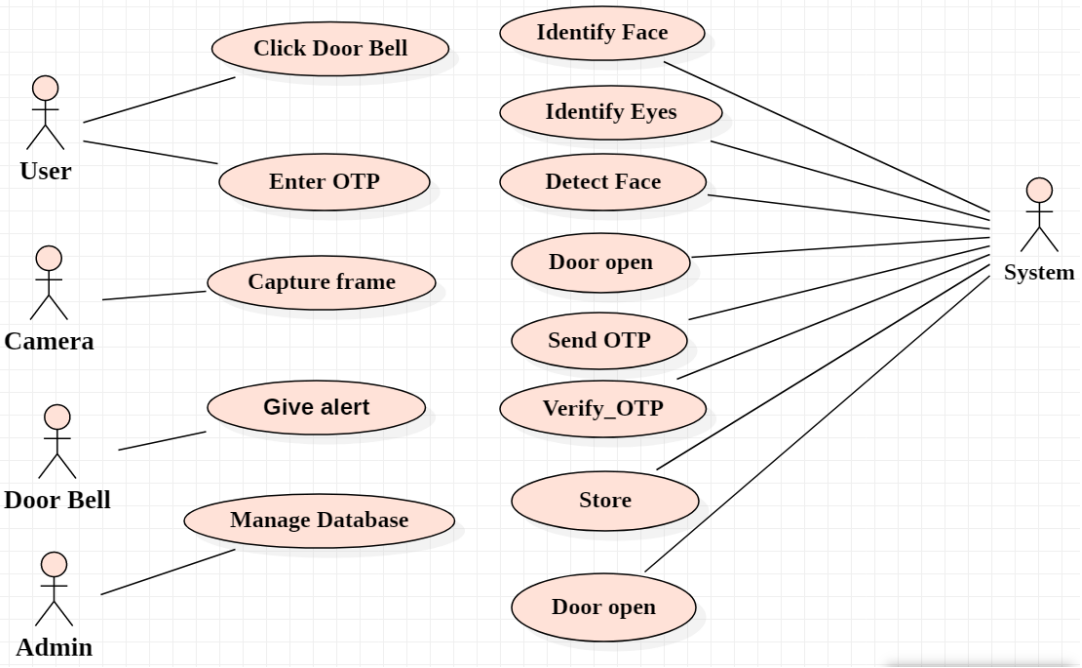

Fig.5.3.Use Case Diagram

5.4.4 Sequence Diagram:

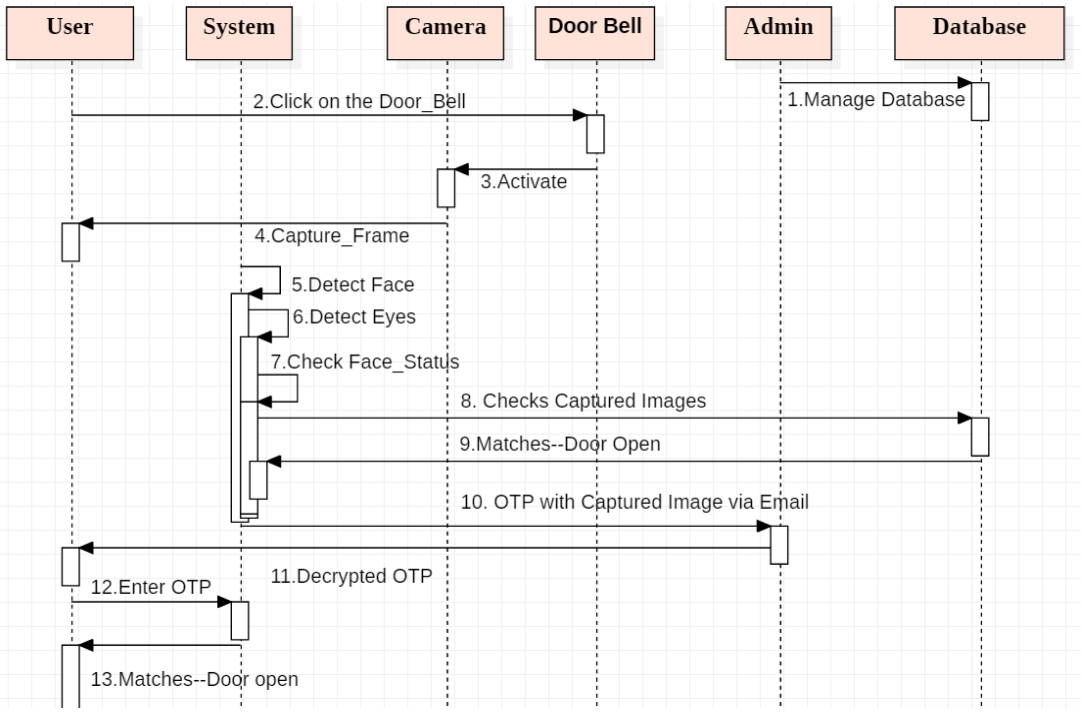

Fig.5.4.Sequence Diagram

AIM : To implement sequence diagram for Face Recognition System Using Opencv.

DESCRIPTION :A Sequence diagram is an interaction diagram that emphasizes the time ordering messages. It shows a set of objects and messages sent and received by the by those objects.

OBJECTIVE : To illustrate the dynamic view of system

THINGS : Objects and Messages

RELATIONSHIP : Time and life line, Links

5.4.5 Activity Diagram:

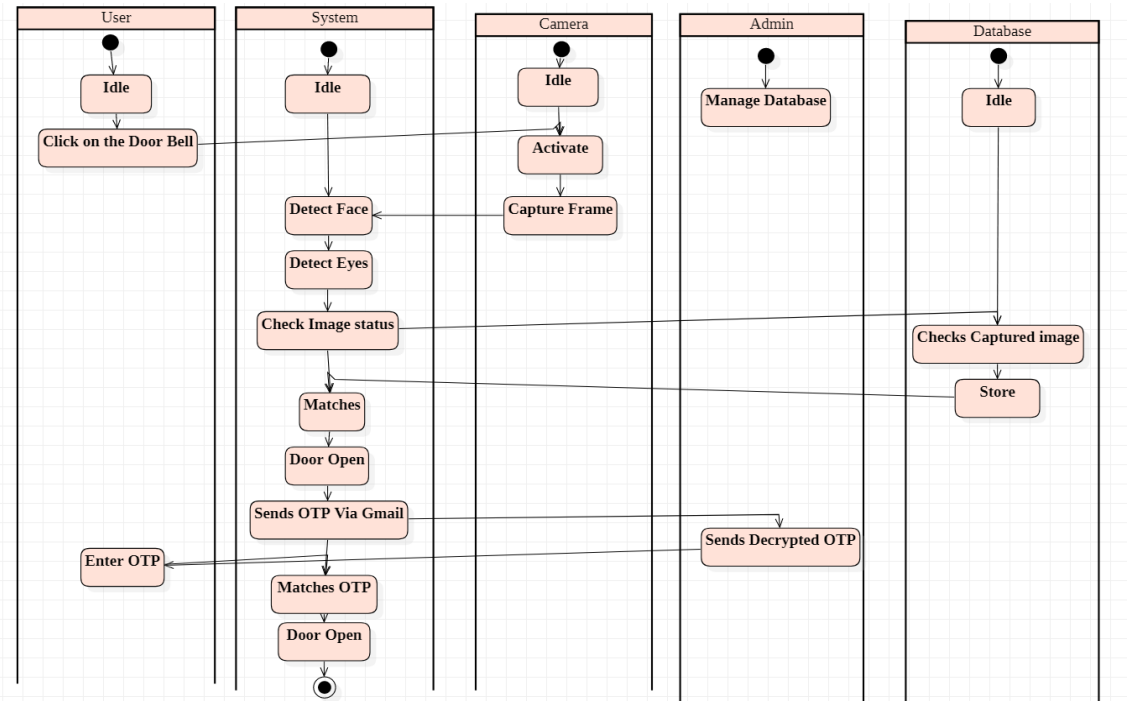

Fig.5.5.Activity Diagram

AIM : To implement activity diagram for Face Recognition System Using Opencv.

DESCRIPTION : An activity diagram is essentially a flow chart, showing flow of control from activity to activity. It involves modeling the sequential steps in computational process. Activity diagram not only important for modeling dynamic aspects of a system, but also for constructing executable system through forward and reverse engineering.

OBJECTIVE : Focused on flow of control from activity to activity

THINGS : State and object

RELATIONSHIPS : Transitions

5.4.6 Deployment Diagram:

AIM : To implement deployment diagram for Face Recognition System Using Opencv.

DESCRIPTION :A deployment diagram is a type of diagram that specifies the physical hardware on which the software system will execute. The software system is manifested using various artifacts, and they are mapped to an execution environment that is going to execute software such as nodes.

OBJECTIVE : Used with the sole purpose of describing how software is deployed into the hardware system.

THINGS : Node, Component, Artifact and Interface.

RELATIONSHIP : Nodes.

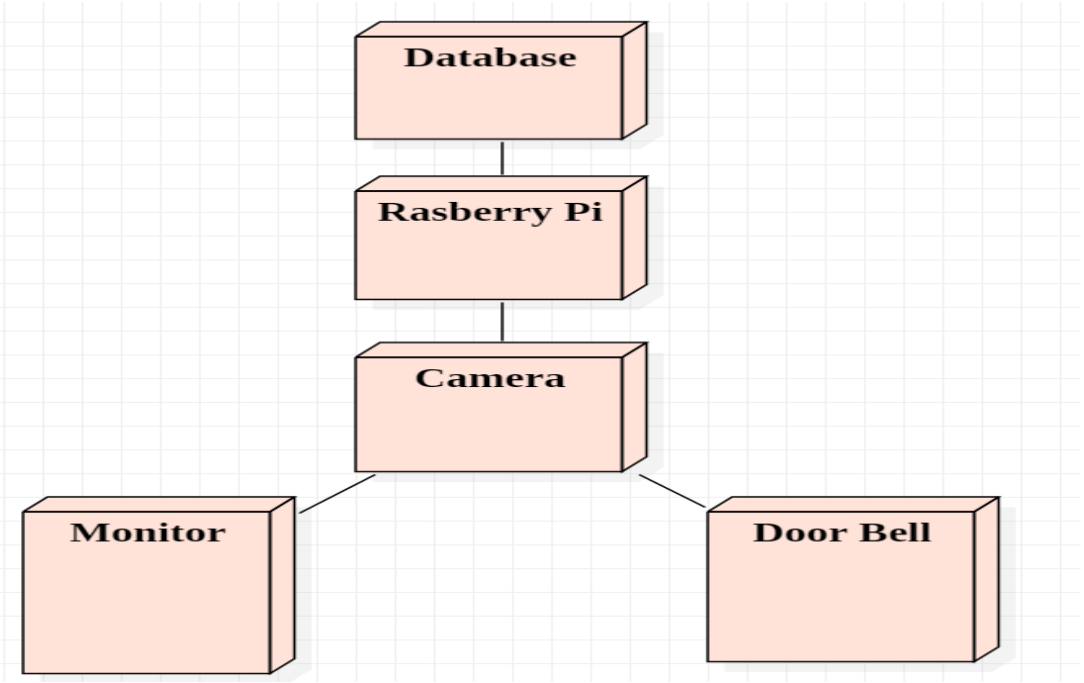

Fig.5.6.Deployment Diagram

6.SYSTEM IMPLEMENTATION

6.1 SOFTWARE DESCRIPTION:

6.1.1Python Introduction:

- Python laid its foundation in the late 1980s.
- The implementation of Python was started in the December 1989 by **Guido Van Rossum** at CWI in Netherland.
- In February 1991, van Rossum published the code (labeled version 0.9.0)
- In 1994, Python 1.0 was released with new features like: lambda, map, filter, and reduce.
- Python 2.0 added new features like: list comprehensions, garbage collection system.
- On December 3, 2008, Python 3.0 (also called "Py3K") was released. It was designed to rectify fundamental flaw of the language.
- ABC programming language is said to be the predecessor of Python language which was capable of Exception Handling and interfacing with Amoeba Operating System.
- Python is influenced by following programming languages:
- ABC language.
- Modula-3

6.1.2.Raspbian OS:

Raspian OS is one of the official Operating systems available for free to download and use. The system is based on Debian Linux and is optimized to work efficiently with the Raspberry Pi computer. As we already know an OS is a set of basic programs and utilities that runs on a specified hardware, in this case the Pi.

Debian is very lightweight and makes a great choice for the Pi. The Raspbian includes tools for browsing, python programming and a GUI desktop.

The Raspian desktop environment is known as the “Lightweight X11 Desktop Environment” or in short LXDE. This has a fairly attractive user interface that is built using the X Window System software and is a familiar point and click interface. We shall look more into how to install and use this OS in the next section.

Setting Up Raspian OS:

Step 1: Take the Pi out of its anti static cover and place it on the non-metal table.

Step 2: Connect the display – Connect the HDMI cable to the HDMI port on the Pi and the other end of the cable to the HDMI port of the TV.
Step 3: Connect your Ethernet cable from the Router to the Ethernet port on the Pi
Step 4: Connect your USB mouse to one of the USB ports on the Pi
Step 5: Connect your USB Keyboard to the other USB port on the Pi
Step 6: Connect the micro USB charger to the Pi but don't connect it to the power supply yet
Step 7: Flash the SD Card with the Raspian OS.

1. The card for use with the Pi we will need to put a OS on the card. We certainly cannot drag and drop the OS files in to the card but flashing the card is not too difficult either.
2. Since we have already decided to install Raspbian, download the RASPBIAN image from the following link. http://www.raspberrypi.org/downloads/.
3. Unzip the contents of the Zip file into a folder on your machine, one of the unzipped files would be a .img file which is what needs to be flashed on to
   the SD card.[In case there are more than one file, then prepare current version of the zip has only this file and none other]
4. Flashing from Linux instructions.
    1. Start the terminal on your Linux OS
    2. Insert the empty SD Card into the card reader of your machine.
    3. Type sudo fdisk -l to see all the disks listed. Find the SD card by its size, and note the device address (/dev/sdX, where X is a letter identifying the storage device. Some systems with integrated SD card readers may use /dev/mmcblkX— format, just change the target in the following instructions accordingly).
    4. Use cd to change to the directory with the .img file you extracted from the Zip archive.
    5. Type sudo dd if=imagefilename.img of=/dev/sdX bs=2M to write the fileimagefilename.img to the SDcard connected to the device address. Replace imagefilename.img with the actual name of the file extracted from the Zip archive. This step takes a while.During flashing, nothing will be shown on the screen until the process is fully complete.

6.1.3.OpenCV:

OpenCV (Open Source Computer Vision Library) is an open source computer vision and machine learning software library. OpenCV was built to provide a common infrastructure for computer vision applications and to accelerate the use of machine

perception in the commercial products. Being a BSD-licensed product, OpenCV makes it easy for businesses to utilize and modify the code. The library has more than 2500 optimized algorithms, which includes a comprehensive set of both classic and state-of-the-art computer vision and machine learning algorithms.

These algorithms can be used to detect and recognize faces, identify objects, classify human actions in videos, track camera movements, track moving objects, extract 3D models of objects, produce 3D point clouds from stereo cameras, stitch images together to produce a high resolution image of an entire scene, find similar images from an image database, remove red eyes from images taken using flash, follow eye movements, recognize scenery and establish markers to overlay it with augmented reality, etc

6.1.4.Package:

A package is basically a directory with Python files and a file with the name __init__.py. This means that every directory inside of the Python path, which contains a file named __init__.py, will be treated as a package by Python. It's possible to put several modules in to a package.

Examples : Pillow, Matplotlib, Keras, Tensorflow, OpenCV, etc

Importing Packages

We will need to import the module with an import statement. An import statement is made up of the import keyword along with the name of the module. In a Python file, this will be declared at the top of the code.

Example : import keras

The packages used in this software are :

6.1.4.1cv2:

cv2 (old interface in old OpenCV versions was named as cv) is the name that OpenCV developers chose when they created the binding generators. OpenCV-Python makes use of Numpy, which is a highly optimized library for numerical operations with a MATLAB-style syntax. All the OpenCV array structures are converted to and from Numpy arrays. This also makes it easier to integrate with other libraries that use Numpy such as SciPy and Matplotlib.

6.1.4.2.scipy:

SciPy is a library that uses NumPy for more mathematical functions. SciPy uses NumPy arrays as the basic data structure, and comes with modules for various commonly used tasks in scientific programming, including linear algebra, integration (calculus), ordinary differential equation solving, and signal processing. SciPy is a collection of mathematical algorithms and convenience functions built on the NumPy extension of Python. It adds significant power to the interactive Python session by providing the user with high-level commands and classes for manipulating and visualizing data. With SciPy, an interactive Python session becomes a data-processing and system-prototyping environment rivaling systems, such as MATLAB, IDL, Octave, R-Lab, and SciLab.

The additional benefit of basing SciPy on Python is that this also makes a powerful programming language available for use in developing sophisticated programs and specialized applications. Scientific applications using SciPy benefit from the development of additional modules in numerous niches of the software landscape by developers across the world. Everything from parallel programming to web and data-base subroutines and classes have been made available to the Python programmer. All of this power is available in addition to the mathematical libraries in SciPy.

6.1.4.3. imutils:

imutils are a series of convenience functions to make basic image processing functions such as translation, rotation, resizing, skeletonization, and displaying images easier with OpenCV and both Python 2.7 and Python 3.imutils A series of convenience functions to make basic image processing functions such as translation, rotation, resizing, skeletonization, and displaying Matplotlib images easier with OpenCV.

6.1.4.4. threading:

The threading module provided with Python includes a simple-to-implement locking mechanism that allows you to synchronize threads. A new lock is created by calling the Lock() method, which returns the new lock. The acquire(blocking) method of the new lock object is used to force threads to run synchronously. A thread is a separate flow of execution. This means that your program will have two things happening at once. But for most Python 3 implementations the different threads do not actually execute at the same time: they merely appear to.

Threading can be explained as having two (or more) different processors running on your program, each one doing an independent task at the same time. The threads may be running on different processors, but they will only be running one at a time. Getting multiple tasks running simultaneously requires a non-standard implementation of Python, writing some of your code in a different language, or using multiprocessing which comes with some extra overhead.

Because of the way CPython implementation of Python works, threading may not speed up all tasks. This is due to interactions with the GIL that essentially limit one Python thread to run at a time. Tasks that spend much of their time waiting for external events are generally good candidates for threading. Problems that require heavy CPU computation and spend little time waiting for external events might not run faster at all.

This is true for code written in Python and running on the standard CPython implementation. If your threads are written in C they have the ability to release the GIL and run concurrently. If you are running a standard Python implementation, writing in only Python, and have a CPU-bound problem, you should check out the multiprocessing module instead. Architecting your program to use threading can also provide gains in design clarity.

6.1.4.5numpy:

NumPy is a general-purpose array-processing package. It provides a high-performance multidimensional array object, and tools for working with these arrays. It is the fundamental package for scientific computing with Python.

6.1.4.6. Rpi GPIO :

This package provides a class to control the GPIO on a Raspberry Pi. A powerful feature of the Raspberry Pi is the row of GPIO (general-purpose input/output) pins along the top edge of the board. Any of the GPIO pins can be designated (in software) as an input or output pin and used for a wide range of purposes.

6.1.4.7time :

There is a popular time module available in Python which provides functions for working with times, and for converting between representations. The function time. time() returns the current system time in ticks since 12:00am, January 1, 1970(epoch).The Python time module provides many ways of representing time in code, such as objects, numbers, and strings. It also provides functionality other than representing time, like waiting during code execution and measuring the efficiency of your code.

- One of the ways you can manage the concept of Python time in your application is by using a floating point number that represents the number of seconds that have passed since the beginning of an era—that is, since a certain starting point.
- Let's dive deeper into what that means, why it's useful, and how you can use it to implement logic, based on Python time, in your application.
- understand core concepts at the heart of working with dates and times, such as epochs, time zones, and daylight savings time
- Represent time in code using floats, tuples, and struct_time
- Convert between different time representations
- Suspend thread execution
- Measure code performance using perf_counter().

6.1.4.8.argparse:

The argparse module makes it easy to write user-friendly command-line interfaces. It parses the defined arguments from the sys. argv . The argparse module also automatically generates help and usage messages, and issues errors when users give the program invalid arguments. Python argparse is the recommended command-line argument parsing module in Python. It is very common to the getopt module but that is a little complicated and usually need more code for the same task.

6.1.4.9. Requests :

This module allows you to send HTTP requests using Python. The HTTP request returns a Response Object with all the response data (content, encoding, status, etc).Requests is an Apache2 Licensed HTTP library, written in Python. It is designed to be used by humans to interact with the language. With it, you can add content like headers, form data, multipart files, and parameters via simple Python libraries. It also allows you to access the response data of Python in the same way.

6.1.4.10. dlib:

Dlib is a general purpose cross-platform software library written in the programming language C++. It contains software components for dealing with networking, threads, graphical user interfaces, data structures, linear algebra, machine learning, image processing, data mining, XML and text parsing, numerical

optimization, Bayesian networks, and many other tasks. Its design is heavily influenced by ideas from design by contract and component-based software engineering. This means it is,first and foremost, a collection of independent software components, each accompanied by extensive documentation and thorough debugging modes.

6.1.5.Methods:

A method in python is somewhat similar to a function, except it is associated with object/classes. Methods in python are very similar to functions except for two major differences. The method is implicitly used for an object for which it is called. The method is accessible to data that is contained within the class.

The simplest way to get list of methods of any object is to use help() command. It will list out all the available/important methods associated with that object. There is no reliable way to list all object's methods. dir(object) is usually useful, but in some cases it may not list all methods.

The methods used in this software are :

6.2 Hardware Description:

6.2.1.Raspberry pi 3B+:

The Raspberry Pi is a low cost, credit-card sized computer that plugs into a computer monitor or TV, and uses a standard keyboard and mouse. It is a capable little device that enables people of all ages to explore computing, and to learn how to program in languages like Scratch and Python. It is capable of doing everything you'd expect a desktop computer to do, from browsing the internet and playing high-definition video, to making spreadsheets, word-processing, and playing games.

Raspberry Pi 3 Model B was released in February 2016 with a 1.2 GHz 64-bit quad core processor, on-board 802.11n Wi-Fi, Bluetooth and USB boot capabilities. On Pi Day 2018 the Raspberry Pi 3 Model B+ was launched with a faster 1.4 GHz processor and a three-times faster gigabit Ethernet (throughput limited to ca. 300 Mbit/s by the internal USB 2.0 connection) or 2.4 / 5 GHz dual-band 802.11ac Wi-Fi (100 Mbit/s). Other features are Power over Ethernet (PoE) (with the add-on PoE HAT), USB boot and network boot (an SD card is no longer required).

Fig.6.1. Raspberry Pi 3B+

6.2.2.Camera:

A webcam is a camera that connects to a computer. It captures either still pictures or motion video, and with the aid of software, can transmit its video on the Internet in real-time. We use the camera to shoot the video of the driver . This camera is used to give input to the system. We have to connect this camera to the raspberry pi board and this takes the power from the board.

Fig.6.2.Camera

6.2.3.HDMI to VGA Converter :

HDMI, which stands for high-definition multimedia interface, supports the connection Fubetween a device such as a Blue-ray player or cable box and a flat-screen HDTV or projector. HDMI combines video and audio interfaces into one connection, which simplifies the installation process of a home-entertainment system.

Fig.6.3.HDMI to VGA Converter

6.2.4.Monitor:

A monitor is an electronic visual computer display that includes a screen, circuitry and the case in which that circuitry is enclosed. Older computer monitors made use of cathode ray tubes (CRT), which made them large, heavy and inefficient. Nowadays, flat-screen LCD monitors are used in devices like laptops, PDAs and desktop computers because they are lighter and more energy efficient. A monitor is also known as a screen or a visual display unit (VDU).

Fig.6.4* : *Monitor

6.3 Database Description:

A database is an organized collection of data, generally stored and accessed electronically from a computer system. In this system, we use a cloud database for storing the date and time of driver drowsiness detection. We can use any free cloud to store this data and can include the hyperlink in the program. The user can check the details by logging into the cloud. The data is stored in the cloud once the alarm is activated.

6.4 Flow Chart:

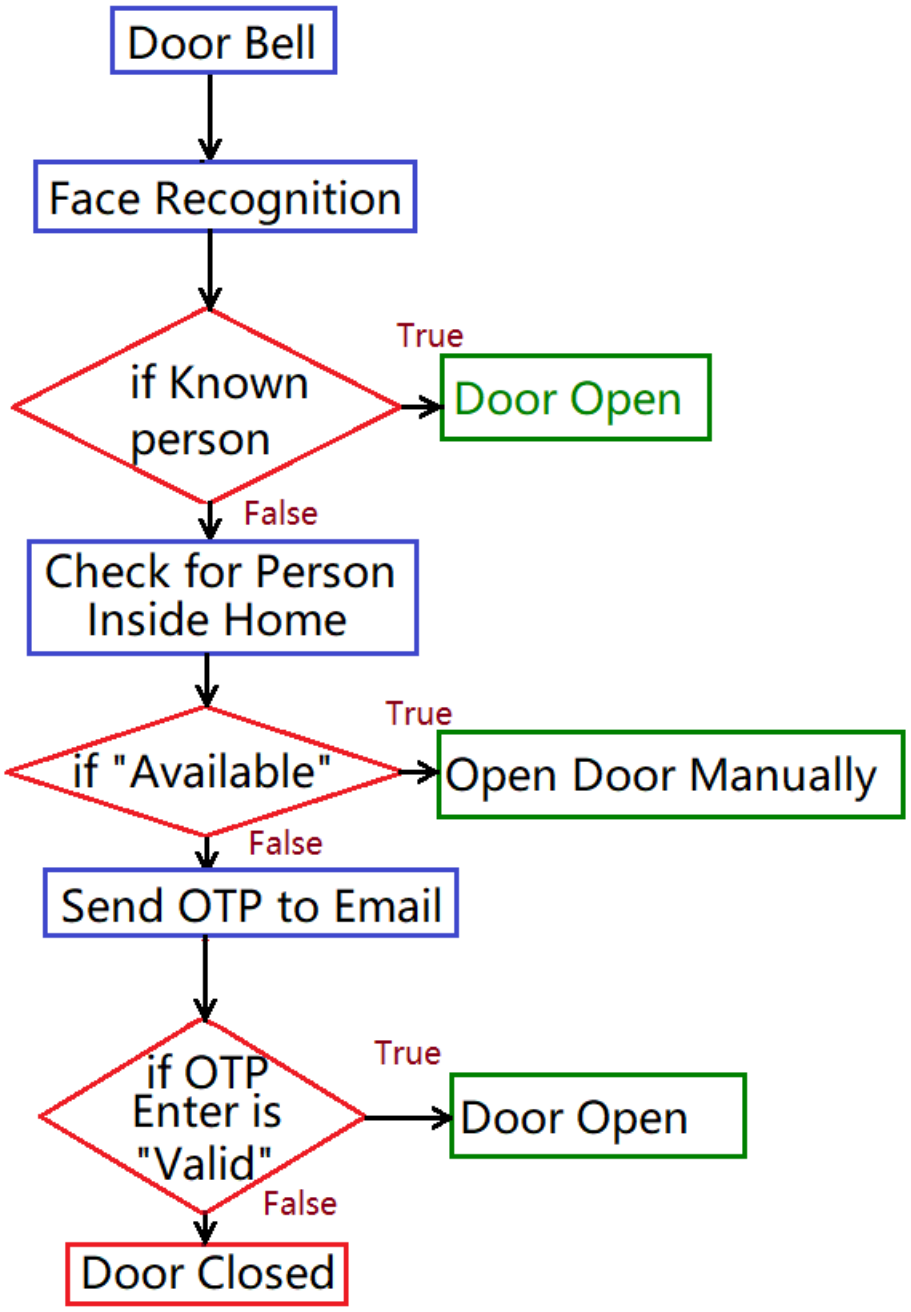

Fig 6.4 Flow Chart of Door Lock System

7.SYSTEM TESTING

7.1.SOFTWARE TESTING:

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product. It is the process of exercising software with the intent of ensuring that the software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

7.2.TYPES OF TESTING:

7.2.1 Unit Testing :

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .It is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Test strategy and approach:

Field testing will be performed manually and functional tests will be written in detail.

Test objectives

- All field entries must work properly.
- Pages must be activated from the identified link.
- The entry screen, messages and responses must not be delayed.

Features to be tested

- Verify that the entries are of the correct format
- No duplicate entries should be allowed
- All links should take the user to the correct page.

7.2.2 Integration Testing:

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent.

Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects.

The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

Test Results : All the test cases mentioned above passed successfully. No defects encountered.

7.2.3 Acceptance Testing:

User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

Test Results : All the test cases mentioned above passed successfully. No defects encountered.

7.2.4.Functional Testing:

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted.

Invalid Input : identified classes of invalid input must be rejected.

Functions : identified functions must be exercised.

Output : identified classes of application outputs must be exercised.

Systems/Procedures : interfacing systems or procedures must be invoked.

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

7.3.TEST CASES:

7.3.1.Test Case 1:

SNO	Test Case ID	Face Detection
1	**Precondition**	Known user Rings the Door Bell
2	**Description**	Recognition of face using camera
3	**Test Steps**	1. Place camera in front of Door 2. Ring the Door Bell
4	**Expected Output**	Know user Recognized Door Opened
5	**Actual Output**	Know user Recognized Door Opened
6	**Status**	PASS
7	**Remarks**	-

Table7.1.Test Case1

7.3.2.Test Case 2:

SNO	Test case ID	Alarm activation through Unknown detection
1	**Precondition**	Unknown user Rings the Door Bell
2	**Description**	Recognition of face using camera
3	**Test Steps**	1. Place camera in front of Door 2. Ring the Door Bell
4	**Expected Output**	Unknown User Recognized Door Close
5	**Actual Output**	Unknown User Recognized Door Close
6	**Status**	PASS
7	**Remarks**	-

Table.7.2.Test Case2

7.3.3.Test Case 3:

SNO	Test case ID	Storage of values in database
1	**Precondition**	Unknown user Rings the Door Bell
2	**Description**	Recognition of face using camera
3	**Test Steps**	1. Verify for the OTP from Admin. 2. Enter correct OTP
4	**Expected Output**	Unknown User Recognized and entered correct OTP
5	**Actual Output**	Unknown User Recognized and entered correct OTP
6	**Status**	PASS
7	**Remarks**	-

Table.7.3.Test case 3

8.RESULTS

8.1. EXECUTION PROCEDURE:

Step 1. Initially the execution of main program started by Admin.

Step 2. Program will wait for input of doorbell.

Step 3. Raspberry is activated to detect and recognize the Video frame of user by comparing with database.

Step 4. If user image is existing in database then automatically door lock will open.

Step 5. If user image is not matched with any of image in database then it will check for the persons available inside the home by using PIR sensor.

Step 6. If anybody present inside home then it will not send any email to admin and door lock will be open by the person inside home.

Step 7. If no one present inside the home the email is sent to admin with image of unknown person and OTP for verification.

Step 8. If unknown user enter correct OTP then door will be open.

Step 9. If entered OTP wrong then door will not open again it will be started from the Step 2.

Step 10. Finally, the door will close and again start from Step 2.

8.2.SCREENSHOTS:

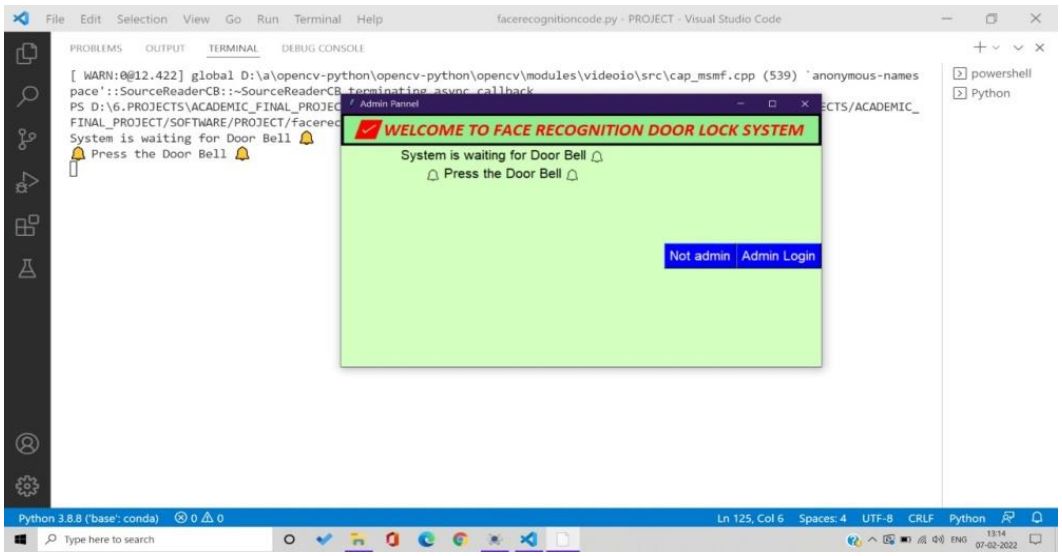

Fig.8.1.Admin Interface, Initially the execution of main program started by Admin

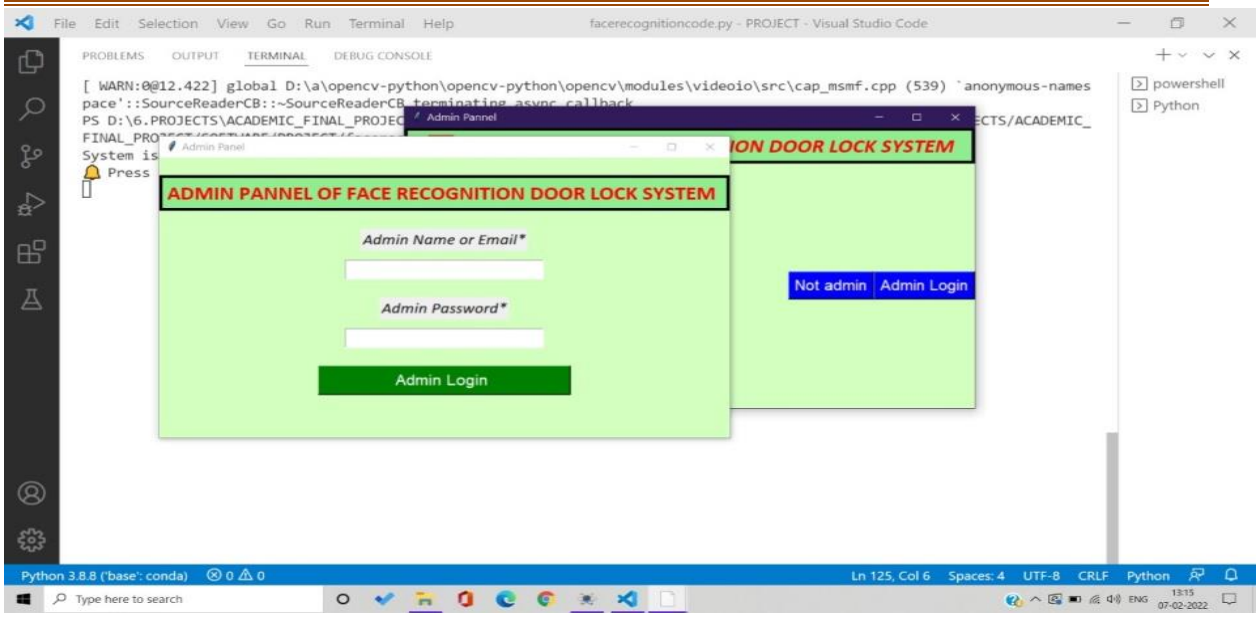

Fig.8.2.Admin Login to Account by entering the valid name and password.

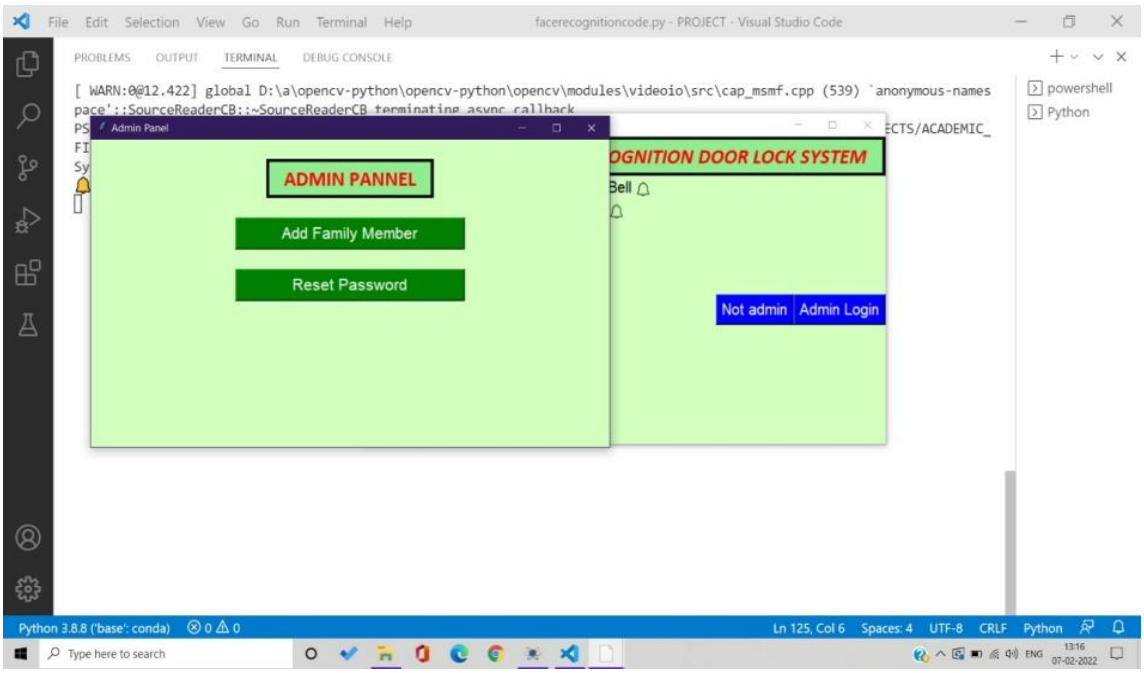

Fig.8.3.Operations for Admin to add data of new user in to database in secured way.

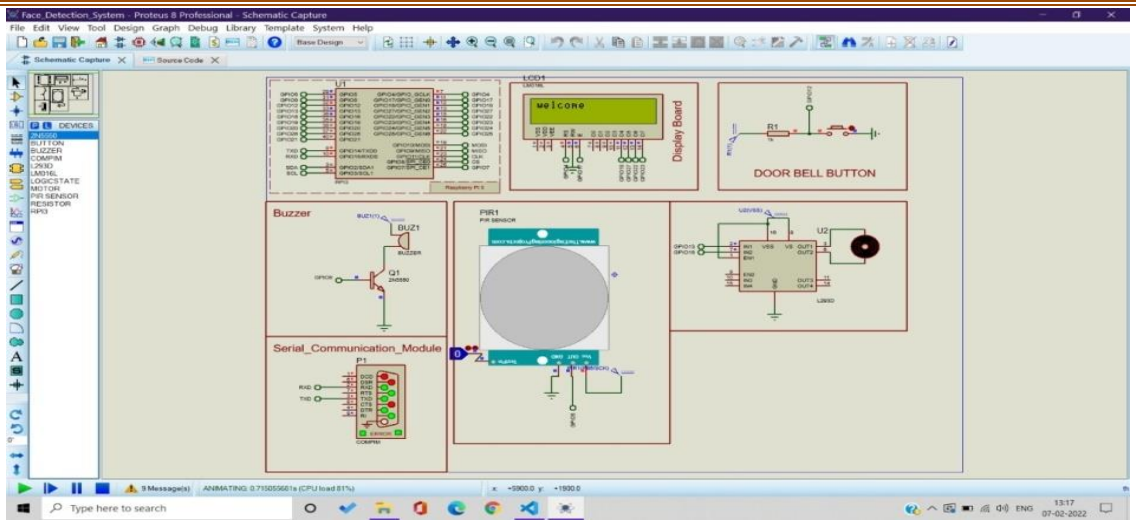

Fig.8.4.Simulation of Raspberry Pi door lock security Circuit in Proteus.

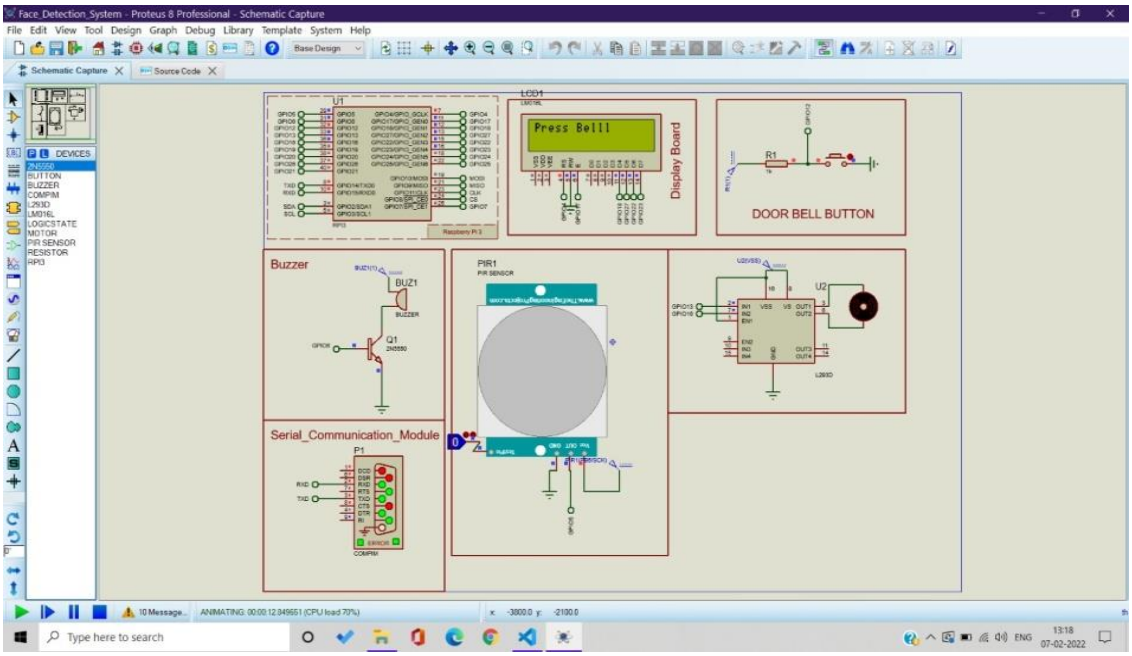

Fig.8.5.Waiting for the Door Bell for activation of raspberry pi to detect and recognize the Video frame of user by comparing with database.

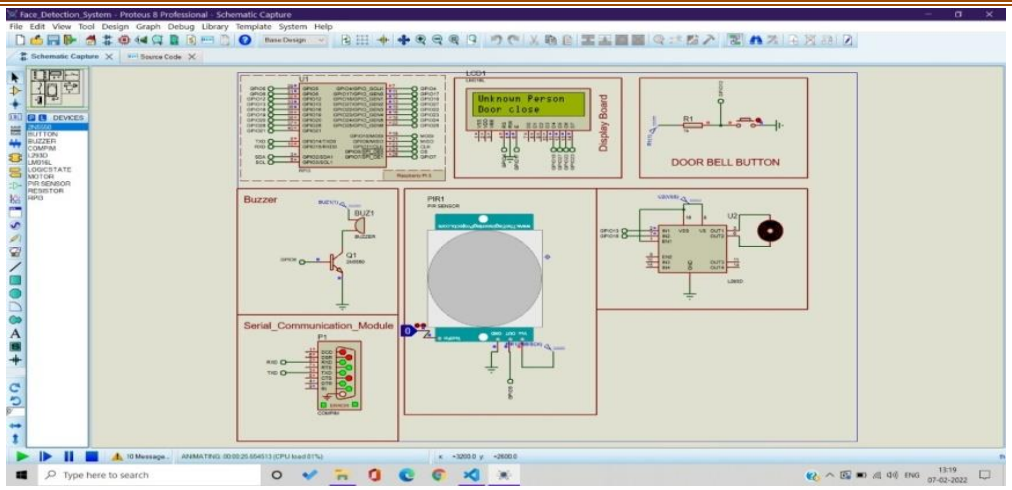

Fig.8.6. Recognition of Unknown Person,If user image is not matched with any of image in database then it will check for the persons available inside the home by using PIR sensor.

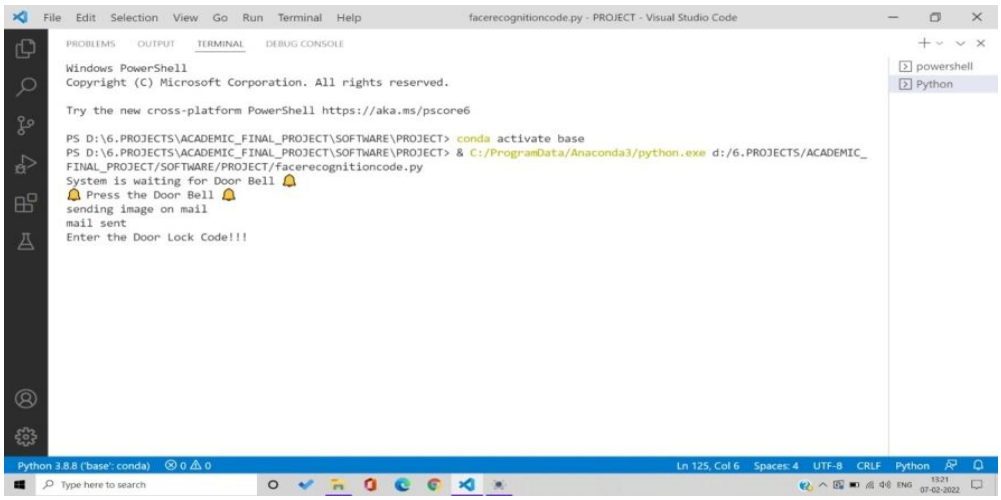

Fig.8.7. Sending Image and OTP to Admin through Email with image of unknown person and OTP for verification.

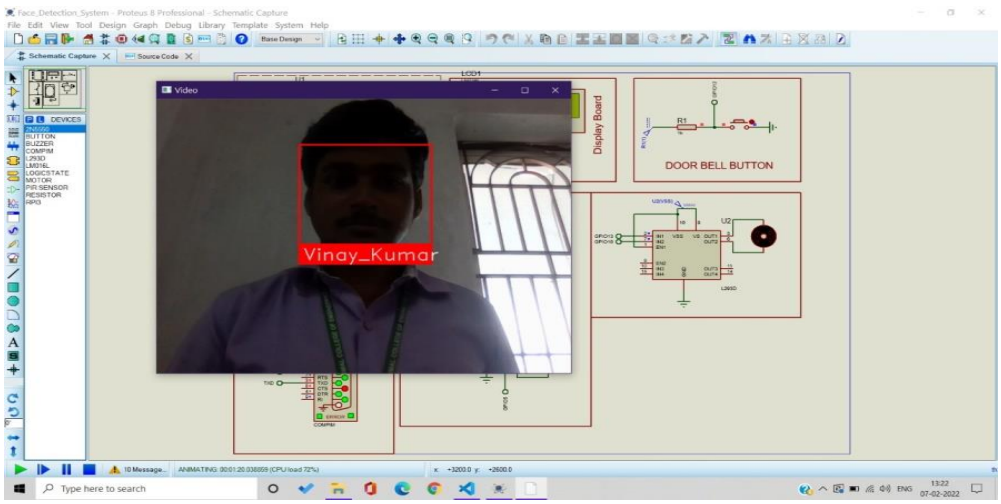

Fig.8.8. Image of known person is Detected and Displays name

9.CONCLUSIONS

9.1. Conclusion:

Face Recognition door locking/unlocking system will help in developing keyless door locking/unlocking and alaso Password based locking/unlocking. This Raspberry based face recognition device will remove the need of manually locking/unlocking the door for the known user.

Also for an unknown user, this device will provide an extra layer of security for the residents of the house. An alertmessage will be sent through email with image of unknown person and OTP immediately to the registered user when unknown face is detected. This will help in user to decidewhether or not to allow a particular person by verifying password.

9.2. Future Enhancement:

Future Enhancements are always meant to be items that require more planning, budget and staffing to have them implemented. The recommended area for future enhancements is a Standalone Product. It can be implemented as a standalone product, which can be installed in a type of Door Security systems. Along with the external added features of emotion recognition.

10.BIBLIOGRAPHY

10.1.References:

1.Sandesh Kulkarni, Minakshee Bagul,Akansha Dukare ,"Face recognition system using IoT" , IJARCET Publications, 2017

2.Thulluri Krishna Vamsi, Kanchana Charan Sai, Vijayalakshmi M, "Face recognition based door unlocking using raspberry pi" IJARIIT Publications, Feb 2019

3.David Gsponer, "Building a raspberry pi security system using facial recognition", Haaga-Helie publications,2018.

4. A.D.Deshmukh, M.G.Nakrani, D.L.Bhuyar, U.B.Shinde, "Face recognition using OpenCV on IoT for smart door ",Elsevier SSN publications, February 2019

5. Muhammad Arif Azhari Halim, Mohd. Fairuz Iskandar Othman, Aa Zezen Zaenal Abidin, Erman Hamid, Norharyati Harum, Wahidah Md Shah " Face Recognition-based Door Locking System with Two-Factor Authentication Using OpenCV**"** IEEE Publications December 2021

6.H. Raddum, L.H. Nestas, K.J. Hole, Security analysis of mobile phones used as OTP generators, Int. Federation Inf. Process. (2010) 324–331.

7.Sania Bhatti, Pirah Memon, Veena Kumari, Anum Arain, Ayaz Jiskani, Keyless Smart home: an application of home security and automation, Oriental J. Computer Sci. Technol., 2018.

8.Malabika Sarma, Amlanjyoti Gogoi,Rahul Saikia, Dibya Jyoti Bora, Fingerprint based door access system using arduino, Int. J. Sci. Res. Eng. Management (IJSREM), 04(08), 2020.

9.Aditya Shankar, P.R.K. Sastry, A.L. Vishnu Ram, A. Vamsidhar, Fingerprint

10.based door locking system, Int. J. Eng. Computer Sci., 04(03), 2015, 10810-10814.

11.Hashem Alnabhi, Yahya Al-naamani, Mohammed Al-madhehagi, Mohammed Alhamzi, Enhanced security methods of door locking based fingerprint, Int. J. Innovat. Technol. Explor. Eng. (IJITEE), 09(03), 2020.

12.Tertsegha Daniel Ipilakyaa, Victor Oji, Vincent Okeke, Design, construction and performance evaluation of an automated door lock System using Biometric Security System with Phone Text Alert Notification, Federal University of Agriculture, 2020.

13.R. Nayana, R. Shashidhar, Smart door lock system, J. Int. Modern Trends Sci. Technol. 05 (02) (2019) 36–38.

14.Piash Paul, Md. Abdullah Al Achib, Hazrat Sauda Hossain, Md. Kaviul Hossain, Smart Door Lock Using Fingerprint Sensor, BRAC University, 2019.

15.S. Umbarkar, G. Rajput, S. Halder, P. Harname and S. Mendgudle, Keypad/ bluetooth/GSM based digital door lock security system, Int. Conference on Communication and Signal Processing 2016 (ICCASP 2016), December 2016.

16.K.A. Patil, N. Vittalkar, P. Hiremath, M.A. Murthy, Smart door locking system using IoT, Int. J. Eng. Technol. 07 (05) (2020) 90–94.

17.Aleksander Ibro, Augusto Rolando Wong, Mario A. Zyla, Face Recognition Door Lock, Worcester Polytechnic Institute, April 2019, pp.15-20.

18.S. Mishra, V.K. Soni, Smart door system for home security using raspberry pi3, Int. J. Innovat. Res. Technol. 04 (11) (2018) 82–86.

19.K.h. Smaranika Subhasini, M. Singh, Color image edge detection: a survey, Int. J. Innovat. Eng. Technol. (IJIET) 8 (1) (2017) 239–243.

20.Gregor Alexander Aramice, Smart house two level security system, World J. Adv. Eng. Technol. Sci., 2017, pp. 44-50.

21.M. Irfan, (2019) CNN Image classifier on Raspberry pi 3B using pre trained data, Student of Electronics and Communication, Christu Jyoti Institute of Technology & Science, Volume 08, Issue 06, June 2019, pp.14-17.

22.R. Dhana Lakshmi, P. Leeela Priya , G. Lokanyaa , J. Sharmila, (2017) Security system using raspberry pi with door lock controller, Int. J. Eng. Sci.Comput.,07 (04), 2017,pp. 90-93.

23.Yugashini,S.Vidhyasri,K.Gayathri Devi,Design and implementation of automated door accessing system with face recognition,Int.J. Sci. Modern Eng. (IJISME) 01(12) (2013).

24.S. Priyadharshini, D. Nivetha, T. Anjalikumari, P.Prakash, Mobile controlled door locking system with two-factor authentication, Int. J. Adv. Eng. Technol. 04 (02) (2020) 08–13.

25.A.Z.M. Tahmidul Kabir, Nirmol Deb Nath, Utshaw Rafin Akther, Fukrul Hasan, Tawsif Ibne Alam, Six tier multipurpose security locker system based on arduino, World J. Adv. Eng. Technol. Sci., 2020, pp.44-50.

10.2. Websites:

[1] www.python.org

[2] wiki.python.org

10.3. Textbooks:

[1] Computer Vision: Algorithms and Applications

[2] Learning with Python - How to Think Like a Computer Scientist