e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:02/Issue:06/June-2020 www.irjmets.com

REAL TIME SMART DOOR LOCK SYSTEM USING IMAGE DETECTION AND VOICE RECOGNITION

Aiswarya I P
M. Tech, Department Of Computer Science and Engineering
Mar Baselios College of Engineering & Technology
Thiruvananthapuram, Kerala, India.

ABSTRACT

A smart door lock system which can be controlled by an Android application installed on smartphone has been proposed. IOT concepts and Android OS were used to enhance the security of smart lock. Motion sensors are used to detect any movement in front of the door. If a person comes in front of the door, the image of the person is captured and notified to the owner of the house. Motion sensing in the front of the door in real time even if there is no one at home and controlling the movement of the door by the smart phone are the main features of this project. The proposed approach is to notify the owner about the visitors present at the door step by a phone message. The Android application will implement a message to speech conversion via synthesized speech which has a much greater chance of catching the owner's attention. The visitor's access to door is authorized through a voice command issued from the owner's phone. Authorization is done by matching the input voice to a list of authorized voices, and also verifies if it is done through an authorized phone.

KEYWORDS: IoT, Image Detection, Voice Recognition, Door lock system.

I. INTRODUCTION

1.1 General Background

Security plays an important role in our life. Home security is essential, as it protects our home and valuables, and keeps our family safe from intruders. With increasing safety and security issues, the use of smart door system increased consistently with the advent of security-related electronics. As security issues increase, it is necessary to use new technologies to strengthen home security. Various security measures used in networks include access control and intrusion control methods in the system. This project i.e. smart door lock system uses image detection and voice recognition to prevent intruders from trespassing into a home. The application is mainly for home security, and deals with the smart door lock systems. In earlier days home security was enforced by using mechanical locks, latches, and combination locks etc. but some burglars attempt to sabotage or pick the lock. As Technology improves, more sophisticated security measures are required in a home. Various methods available for secure access include password authentication, iris recognition, Radio Frequency Identification (RFID) etc. The each system is applicable for different purposes, but each one having some drawbacks so the burglars are breaching the security aspects. There for improving more security three way authentication mechanism are introducing for saving our valuable life and belongs, and improving the existing systems.

1.2 Objectives

This project aims at:
1. Implementing a smart door lock control system.
2. Using image detection and voice recognition technologies to strengthen the security aspects.

1.3 Scope

The scope of this project is for providing a two way security in user authentication that ensures:

- Home security to protect your home and family from Intruders by sending an alarm to all authorized users.
- Critical Zone Access Control that keeps the data confidential from unauthorized access.

II. METHODOLOGY

IoT is used as the backbone technology for home security system. IoT is a combination of network and devices connected to the network that autonomously communicate with each other and coordinate among themselves. In the proposed system a smart phone is used as the interface between the user and the door lock system. It's a keyless system, so burglars cannot physically gain entry or sabotage the lock system. If the door security is breached, a notification is send as alert to the owner of the house.

The proposed door lock system uses image detection and voice recognition methods based on Android OS for security, and are efficient and reliable. The system offers security in homes, shops, institutions, critical zones etc. The main component of this system includes hardware module for door lock, image detection and voice recognition modules.

The motion sensing module includes a motion sensor which is placed in front of the door. Motion can be detected via sound or vibration and is utilized for distinguishing moving object. If any motion is triggered, there is a camera which captures the image of the person detected by the motion sensor. The captured image is stored in the central server database. The central server consists of some data which is already stored in the system. The server verifies the captured image with the data present in the server database. If it is a new person or a match occurs with data stored in the database, the server sends a notification to a registered mobile phone.

A secure Android app, which allows users to manage passwords in the system when he/she logs into the application is also included in the project. In this app, users can login to the system using User ID and Password. Encryption keys are uploaded to the database for the first time. After that, a user can view the encryption keys whenever they login to the system and also update the keys. An OTP is generated for each registration process; if it successfully registers, an OTP is sent to the registered mobile number for verifying the registration process. The authorised owner will get a notification and checks the message. The authorized person allows the entry using his/her voice command. The system verifies whether the command is valid or invalid. If it is a valid command and the person is known, he/she may unlock the door. Otherwise, the door remains locked and an alert message is sent.

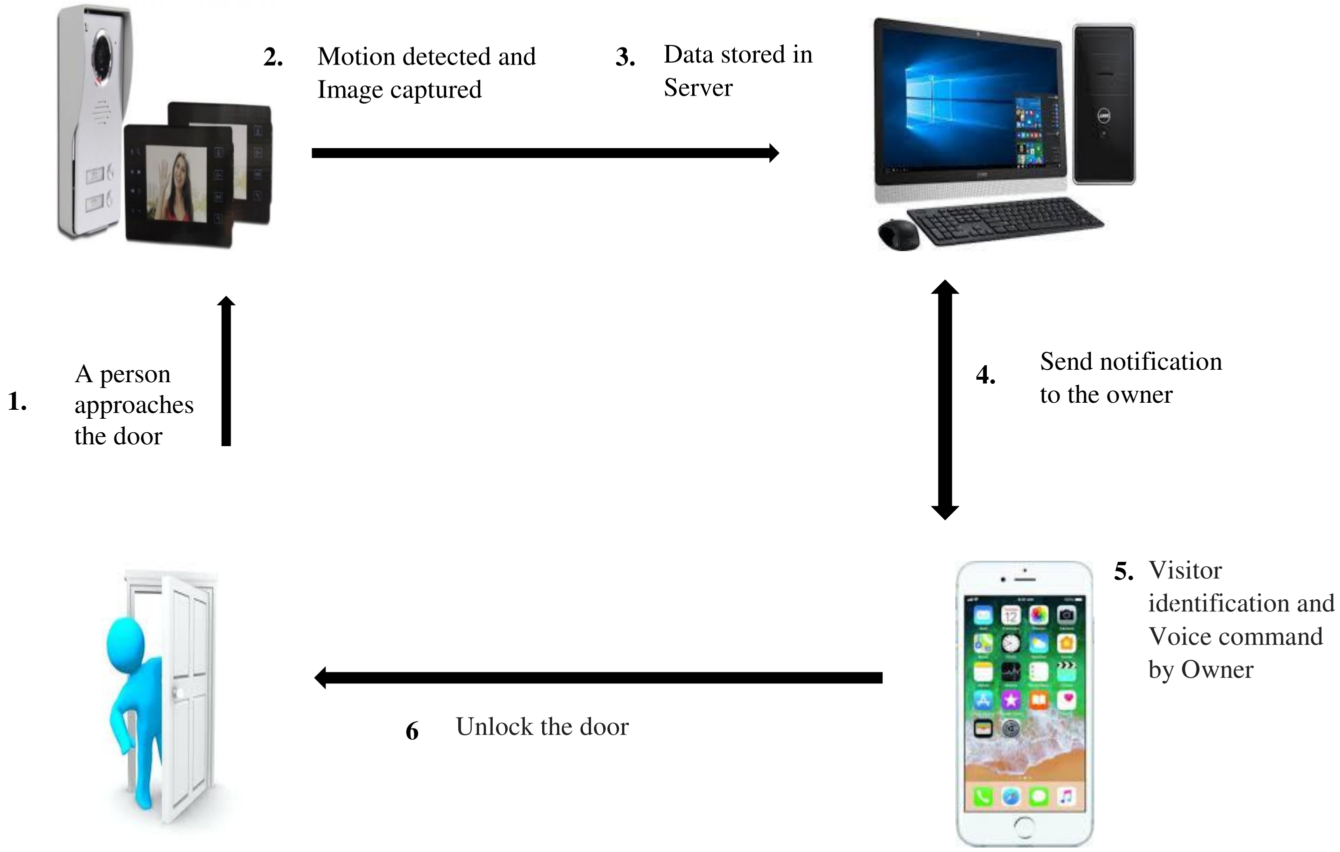

2. Motion detected and Image captured
3. Data stored in Server
1. A person approaches the door
4. Send notification to the owner
5. Visitor identification and Voice command by Owner
6 Unlock the door

Fig-1: Sequence for unlocking the door

III. DESIGN AND IMPLEMENTATION

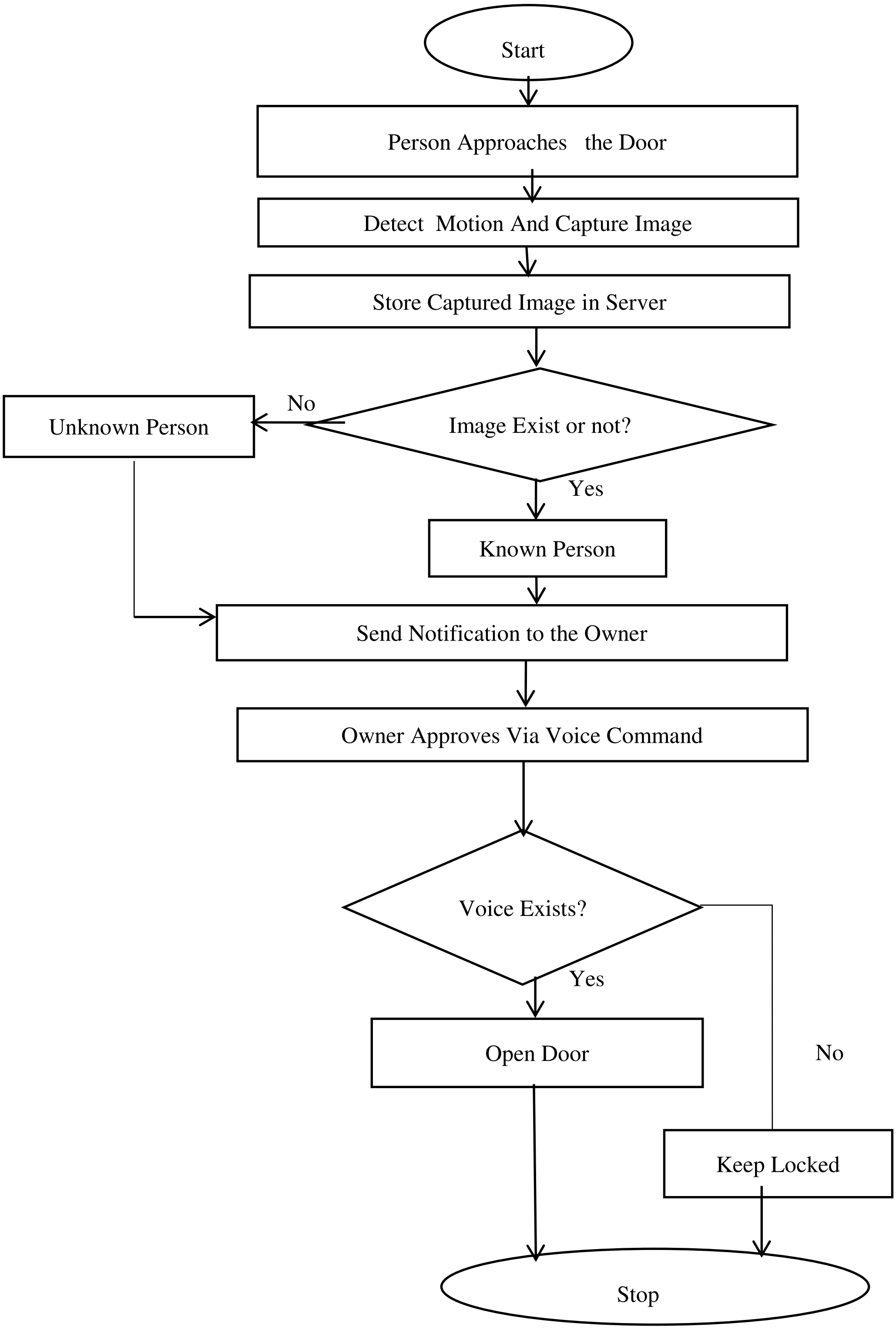

Start
Person Approaches the Door
Detect Motion And Capture Image
Store Captured Image in Server
Image Exist or not?
No
Unknown Person
Yes
Known Person
Send Notification to the Owner
Owner Approves Via Voice Command
Voice Exists?
Yes
Open Door
No
Keep Locked
Stop

Fig-2: Overall data/ logic flow of door lock system

This paper deals with a smart door lock system. The motion sensor and camera is attached to the door. If a person approaches the door, the motion sensor detects his/her presence and the buzzer makes a sound. The camera switches on when the motion detector detects movement, and it captures the image of the person standing in front of the door. The captured image is stored in the server. The server contains a database of labelled human faces, and it compares the captured images with stored images. The image detection is powered by a deep learning network called CNN (Convolutional Neural Network), which is used for image recognition. The detected image is sent to the authorized phone. An android application named ‘Door Lock System’ is installed on the authorized phone, which controls the entire door lock system. The application can be accessed only by the registered user. If a person registers himself/herself in the application, that person receives an OTP on their registered mobile number and he/she will be granted full access to the application. Whenever a person approaches the door, their face is captured and sent to the phone as a notification. The authorized user visually verifies if the person is known. If it is a known person, the authorized user unlocks the door via a voice command. This voice is compared with multiple voices stored in the database. If a match exists, the door is unlocked. Otherwise, it remains locked.

3.1 Hardware Implementation

In hardware module, ARM microcontroller is the core component of the door lock system. The IR sensor is a motion sensor used for detecting the object. A camera is used for capturing the detected object i.e. human face. The captured image is stored in the server and comparison operations are performed in software. The Wi-Fi module is used for network connectivity, which is used for fast data transfer compared to other wireless networks. This module transmits and receives data from the server. A power supply unit is used for regulating input voltage. The controller’s operating voltage is 3.3v. The LCD display is used for displaying messages from the working system.

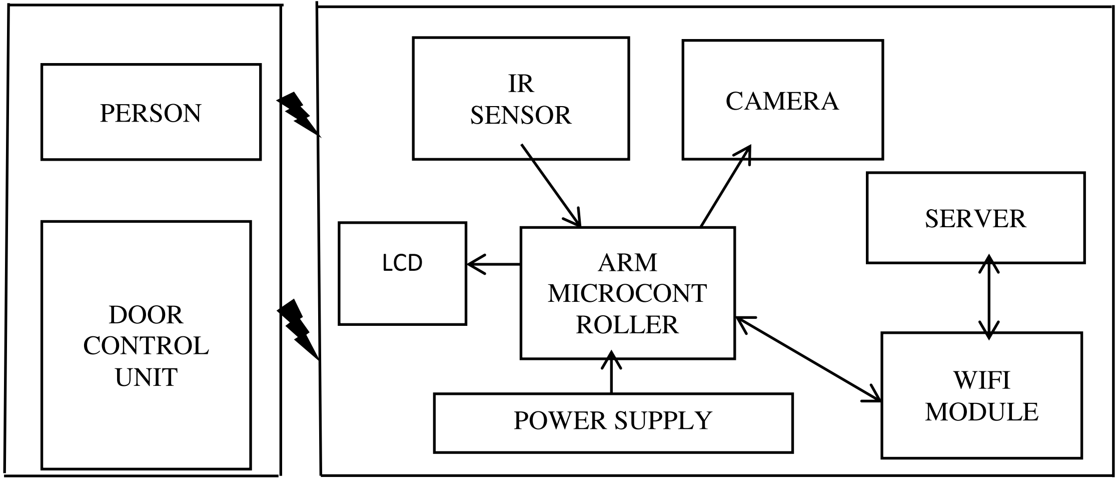


Fig-3: Door Lock Hardware Modules

3.2 Software Implementation

The software module consists of 3 parts for access control of door lock system.

1. Image detection

2. Voice recognition

3. Door lock application module

3.2.1 Image Detection Using Deep Learning

It is process of identifying the input images. This is a classification method, that uses pattern matching on the input data and image recognition classifies data into one category out of many. The input images are different human faces and image data is in the form of 2-dimensional matrices.

The major steps in image recognition process are gathering and organizing data, building a predictive model and using it to recognize images.

3.2.1.1 Gather and Organize Data

Operating systems recognize images as bitmaps. Bitmap images are collection of pixels each having a Red, Green, Blue values (in some cases alpha values). These values are decoded by image viewers and displayed on screen. Input images were analysed by performing geometric encoding such as brightness of RGB colour images, geometrically positioning the RGB image for cropping and resizing the image and transformation into constructs rendering physical features and objects. These were assembled and logically analysed by the computer. Organizing data involved classification and feature extraction. The first step in image classification was to simplify the image by extracting important facial information and leaving out the rest of background information as it would have caused significant variation in RGB pixel values.

The input image of a human face undergoes pre-processing i.e. image was cropped and resized and the essential information was obtained from the images while avoiding the non-essential features of that image. The pre-processed image was used for the feature descriptor; Histogram of Oriented Gradients (HOG) was used for feature descriptor. It extracted HOG features from a coloured or grey scale input image. The features were returned in a 1 by N vector; where N was the HOG feature length. Features were encoded into local shape information from regions within an image and Local Binary Pattern (LBP) was used for extracting the features of local texture information. The feature of HOG and LBP were concatenated with each other for image recognition and resulted in HOG visualizations.

3.2.1.2 Build a Predictive Model

In first step, the network learns to convert an input image to a feature vector. Then it built a predictive model for classification of the obtained feature vectors as input and a class label was provided as output. A large amount of input images i.e. human faces were obtained to train the system. A Neural Network was used to predict the output from the given input.

To build a predictive model, a deep neural network i.e. Convolutional Neural Network (CNN), was used for image detection. The advantage of CNN is that it requires minimal pre-processing and it did not require prior knowledge. The proposed CNN consisted of an input layer, output layer and multiple hidden layers. In this model, 7Convolution layers were used. Input layer obtained the input images in a grey scale format and this layer’s output was passed to the Convolution layer, which detected the edges of the images, and max pooled them i.e. a filter was used for reducing spatial size of the image. It also prevented overfitting. A second Convolution layer and pooling were used for detecting the shape of the image and other Convolution layers were used for detecting the special features of the images. This convolution network is used for performing feature extraction. The output of feature extraction was given for classification purposes. The fully connected layer was used for connecting the convolution layers and the neural network. The neural network learned the classification and the probability was output in ‘Softmax’ layer.

3.2.1.3 Recognize Images

Both training and testing images were organized and duplicates were removed. This data was fed into the model for image recognition. The image of a human face was recognized in the database of known images, which were nearly closer to the test image. The CNN classifier was trained to take the closest values from the test image and recognize a similar face image from the database.

CNN classifier is used to classify the facial images and to identify known and unknown persons.

3.2.1.4 Creating Database

The database consisting of different people was created.50 images of a person with different poses were taken using a webcam. These were stored into different folders, each with a unique name.

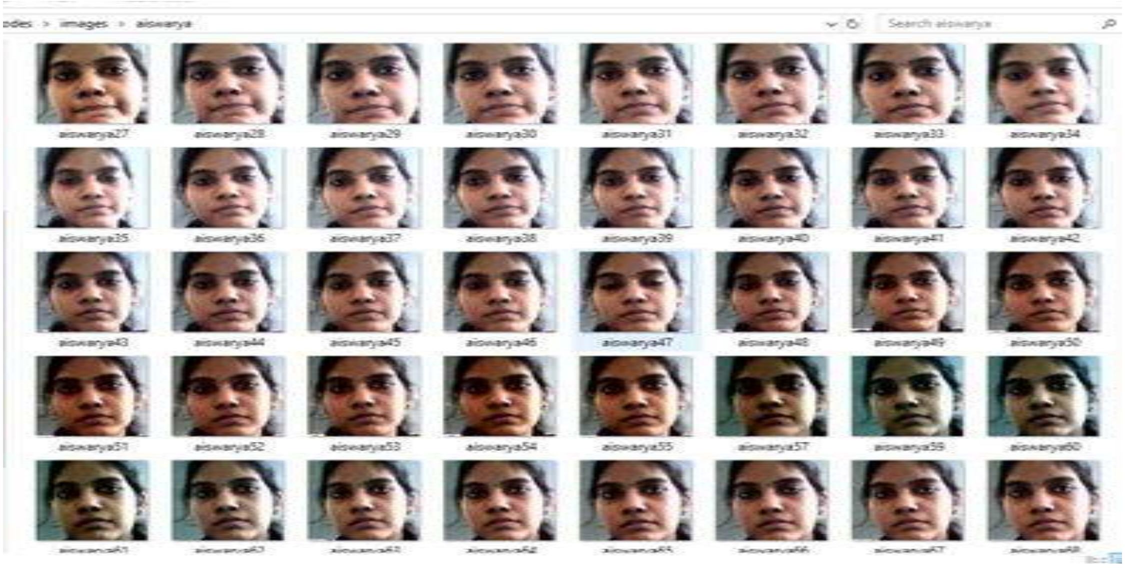


Fig-4: Database of a person

3.2.1.5 Training the Network

The stored images were used for training. For each facial expression, training was done using the detected face from the image, and feature extraction was performed. HOG feature extraction was used for calculating the pixel values for each image. Pre-processing of images ensures that only the relevant part of the images is obtained and all other irrelevant data are removed.

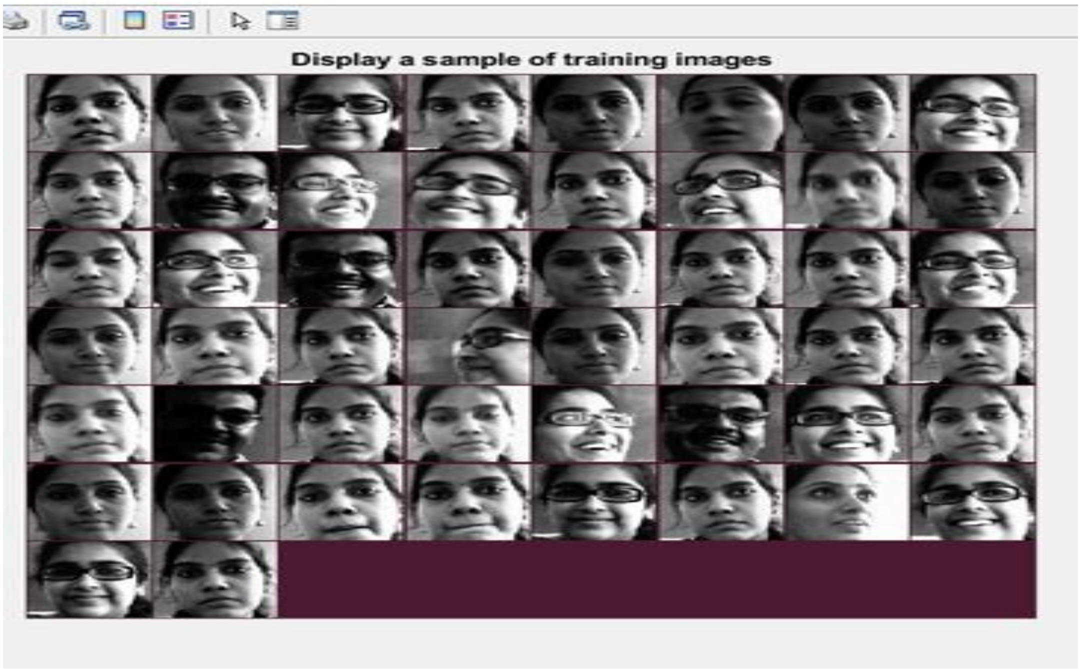


Fig-5: Training image samples

3.2.1.6 Testing the Network

A database was used to store the classified features. After data collection, the whole dataset was divided into two, training (80%) and testing (20%), for the purpose of feature level classification. Total input was 600 images i.e. 400 images for training and 200 images for testing.

3.2.2 Speech Recognition Using Deep Learning

Speech recognition is the method of recognizing the voice command of an authorized user. The deep learning model was trained on voice commands using a Convolutional Neural Network.

The model was trained on several voice samples and therefore is suited for the proposed system.

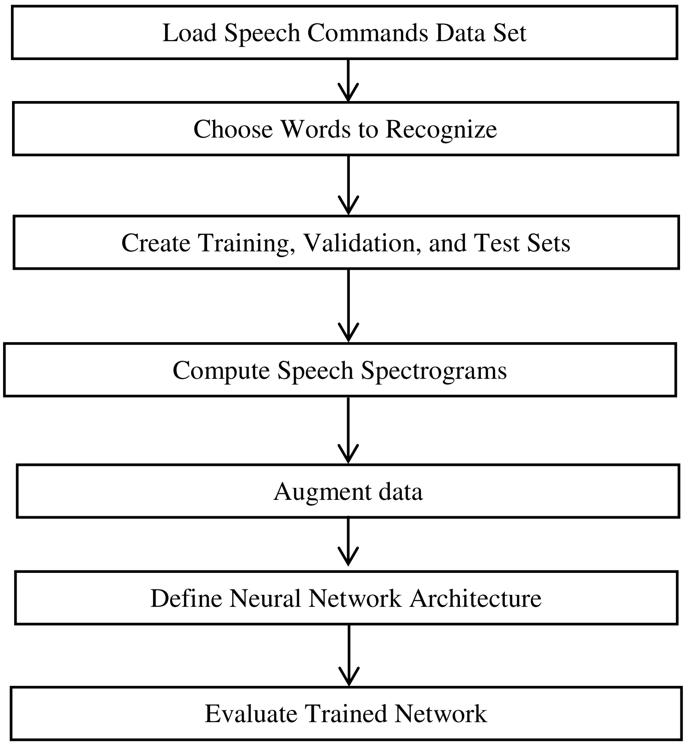

Load Speech Commands Data Set
Choose Words to Recognize
Create Training, Validation, and Test Sets
Compute Speech Spectrograms
Augment data
Define Neural Network Architecture
Evaluate Trained Network

Fig-6: Flow diagram of voice recognition

3.2.2.1 Data Set for Speech Commands

The audio commands are stored in the ‘audio Data store’. These commands are used for creating a voice data file with users’ name. The folder names are used as the label source.

3.2.2.2 Selection of Words for Recognition

Recognition words for the model to use as commands were chosen, such that it learned the difference between commands and all other words.

To create a balance between known and unknown words and also to speed up recognition, only a part of the unknown words ‘include Fraction’ was included in the training set. Background noise is added later, to improve robustness.

A data store was created to hold files and labels that were indexed. The data store was reduced to contain only commands and subset of unknown words.

3.2.2.3 Training, Validation, and Test Set Creation

The dataset folder contained text files that stored a list of names of audio files that were to be used for creation of testing and validation sets. These sets contained utterances of different words by different people. ‘split Data’ function was used for the data store split into training, validation, and test sets, based on the list of validation and test files present in the data set folder.

As only a single network being trained, only validation set was used to evaluate the trained model, excluding the test set from this process. However, if multiple networks were used for training, and the one containing the highest validation accuracy was chosen, then the test set could be used for final network evaluation.

The input dataset contains 45 voice commands and it labelled as 3 batches and each batch contains 15 voice commands. After collection of input voice data, the whole dataset was divided into two, training (80%) and testing (20%), for the purpose of voice recognition.

3.2.2.4 Speech Spectrogram Computation

Speech waveforms were converted to log-mel spectrograms for efficient CNN training.

Spectrogram calculation parameters were defined. ‘segment Duration’ was the length of each speech clip in seconds. ‘frame Duration’ was the length of each frame in seconds, for spectrogram calculation. ‘hopDuration’ was the time step between each spectrogram column. ‘numBands’ was the quantity of log-mel filters used, and equalled to the height of each spectrogram.

‘speech Spectrograms’ function was used for spectrogram computation for each of the training, validation, and test sets. ‘melSpectrogram’ was used for log-mel spectrogram calculations. Data with a smoother distribution was obtained by taking the log of the calculated spectrograms using a small offset ‘epsil’.

25

3.2.2.5 Data Augmentation

Automatic augmentation and resizing of spectrograms was performed for an augmented data store creation. The spectrogram was randomly translated up to 10 frames (100 ms) forwards or backwards in time, and scaled by 20 per cent up or down along the time Data augmentation increased the effective training set size and also helped to prevent the neural network from overfitting. The augmented image data store was created in real time during the training process and then passed as inputs to the network. Augmented spectrograms were not saved in memory.

3.2.2.6 Neural Network Architecture Definition

Simple multi-layered network architecture was created. Convolutional and Batch Normalization layers were used. Feature maps were spatially down sampled via use of Max Pooling layers. A final Max Pooling layer that pooled the input feature map globally over time was added. This enforced approximate time-translation invariance in the input spectrograms, that allowed the same classification to be performed in the network regardless of the exact speech position in time. Parameter reduction due to global pooling was also performed in the final Fully Connected Layer. A small amount of dropout was added to the input in the last fully connected layer, to prevent overfitting.

The network has 5 convolutional layers with few filters. The number of filters in the convolutional layers was controlled using ‘numF’. To increase the accuracy of the network, the network depth was increased by adding identical blocks of convolutional, batch normalization, and ReLU layers. Weighted cross entropy was used asclassificationlossmetric.WeightedClassificationLayer(classWeights) created a custom classification layer that calculated the cross entropy loss with observations weighted by class Weights. The class weights were specified in the same order as their appearance in categories(YTrain). To give each class equal total weight in the loss, class weights that were inversely proportional to the number of training examples in each class were used. When the Adam optimizer was used to train the network, the training algorithm was independent of the overall normalization of the class weights.

3.2.2.7 Evaluate Trained Network

The final network accuracy was calculated, based on training set (excluding data augmentation) and a validation set. The network is highly accurate on this data set. However, training, validation, and test data sets have similar distributions that do not often realistically reflect real-world environments. This limitation particularly applies to the unknown category, which consists of utterances of only a small number of words.

3.2.3 Door Lock Application Modules

This paper performs the following steps enforce door lock security.

i. User Authentication

ii. Registration

iii. Image Notification

iv. Voice authentication

MODULE	INPUT	PROCESS	OUTPUT
User authentication	Username Password	Login Process	Application home page
Registration	Username Password Phone Number PIN	Adding user details OTP verification	Application home page
Image Notification	Captured image camera	Image verification	Image displayed in notification window
Voice authentication	Voice command	Voice verification for door locks access.	Unlock door

Table-1: Door lock application module

The user logs in with his/her username and password. The user enters the details for registration in the application. If successfully registered, the user receives an OTP in their registered mobile number. This OTP is entered into the OTP field. Then user is successfully registered in the system. OTP is used for security authentication. This is valid only for one interaction. OTP works using randomizer algorithms that generate a new and random password each time the algorithm is called. Since the algorithm always randomizes characters and symbols, a hacker/cracker cannot guess the correct password. After a successful registration, the user will be the authenticated person in the application. If any object is detected by the motion sensor, the security camera is switched on and the image is captured and the image is compared in the server. Regardless of whether it is a known or unknown person, the server sends an image notification to the ‘Door Lock System’ user application for image verification. When the image notification is obtained, the user identifies the person and allows door access by using authorized voice command. Voice command is checked. If it is a valid voice the door opens automatically. Otherwise door remains locked.

IV. RESULTS AND DISCUSSION

The door lock systemwasdeveloped for home security, and it is also applicable to office, apartments and other locations. The door does not open into two cases:

1. The detected face is not authorized.
2. Unrecognized voice or unauthorized voicecommand was given as input to the mobile application.

4.1 Door Lock System

The door lock system connects with wifi network for accessing the system. If the sensor activate and any object is detected by the sensor, it initiates a beep sound. Tranfering detection data to the server system.

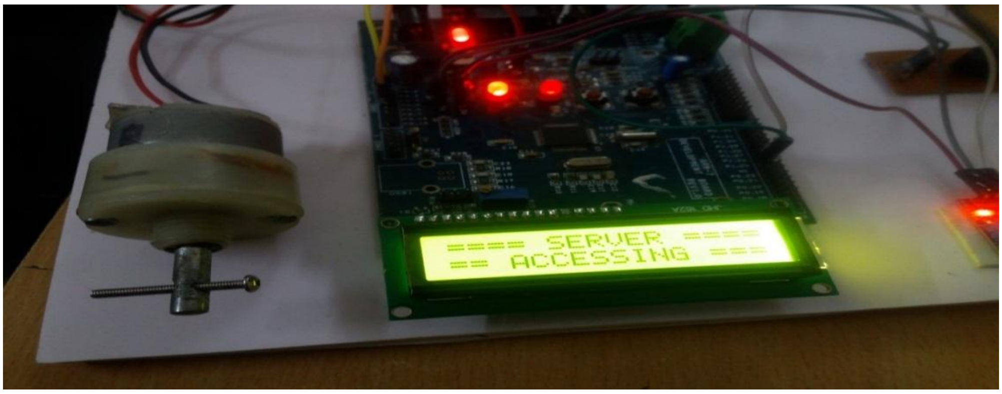


Fig-7: Door lock system acessing server

Door lock system activates after successful image detection and voice recognition.

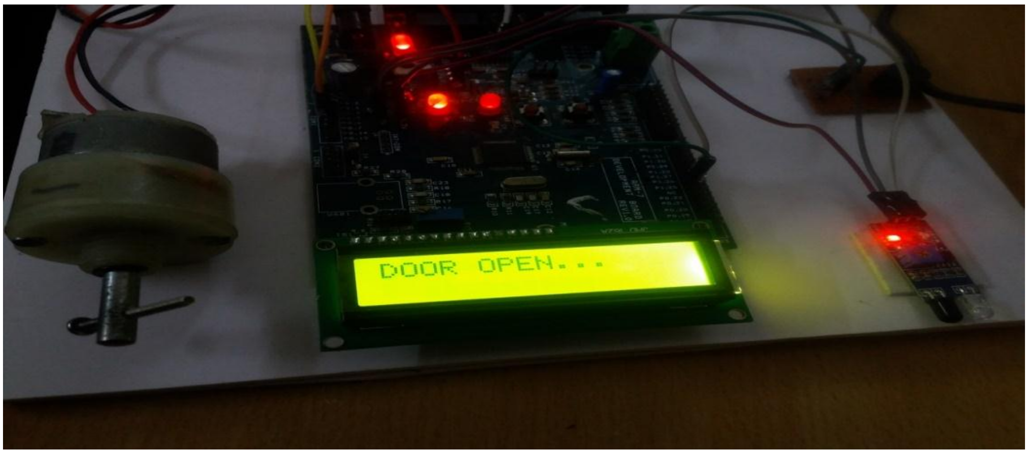
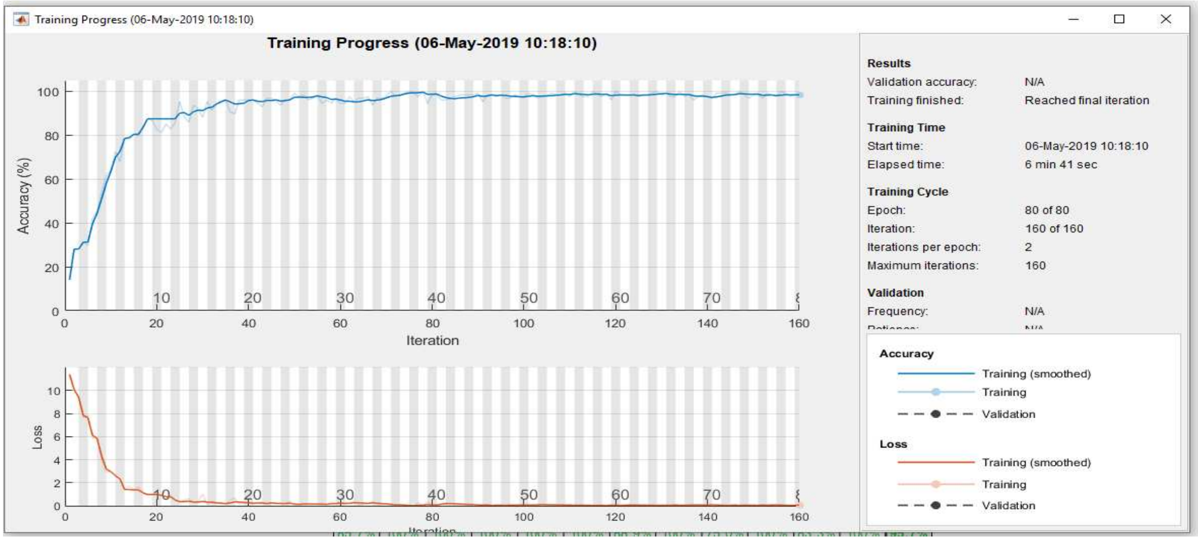


Fig-8: Door opening on sucessful image and voice recognition

Door lock automatically engaging lock system after a certain timeout.

Fig-9: Door being locked due to a timeout

4.2 Image Detection



Results
Validation accuracy: N/A
Training finished: Reached final iteration

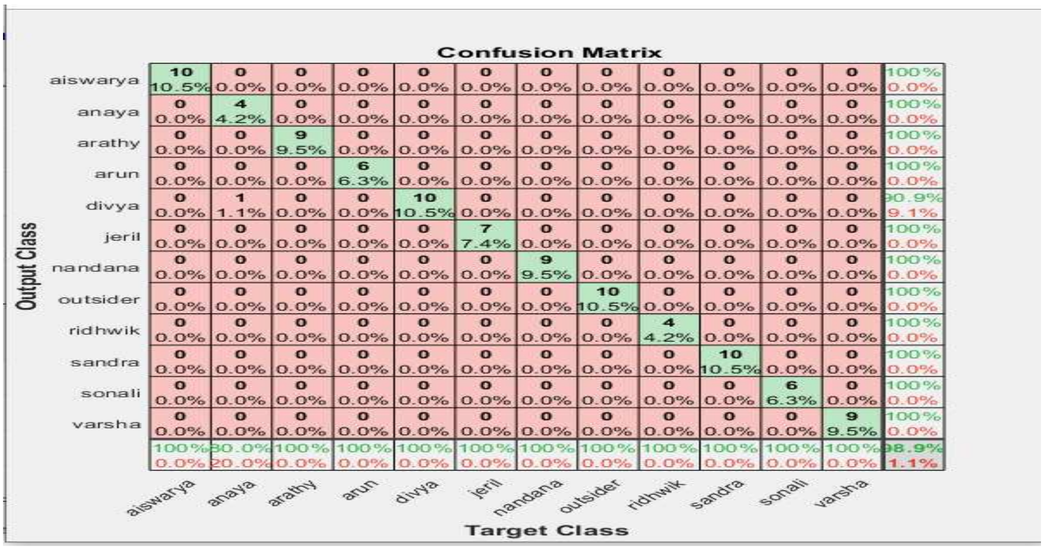
Training Time
Start time: 06-May-2019 10:18:10
Elapsed time: 6 min 41 sec

Training Cycle
Epoch: 80 of 80
Iteration: 160 of 160
Iterations per epoch: 2
Maximum iterations: 160

Validation
Frequency: N/A

Fig-10: Graph showing training process

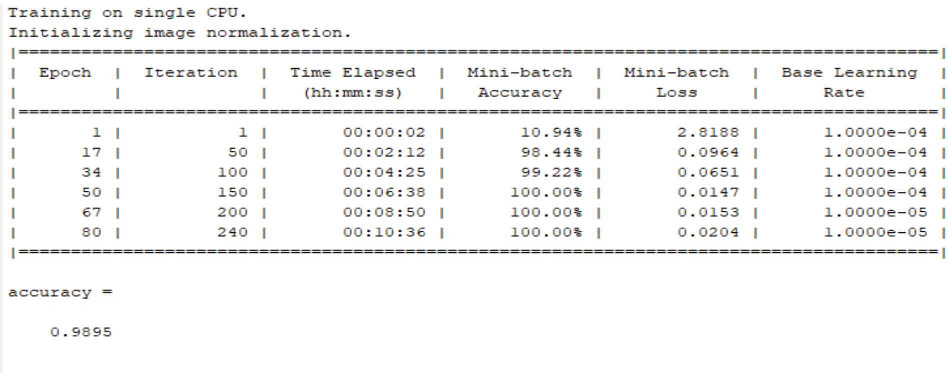
The image detection performs a major role in home security. The detected face is compared with a created database. If any match has occurred, the person is a known one.Otherwise, the person is unknown. In the classification phase, the database is split into two, training and testing phases. In training phase, 80 epoch were carried out, and an accuracy of 98.9% was obtained, while the loss rate was 0.001.



Confusion Matrix

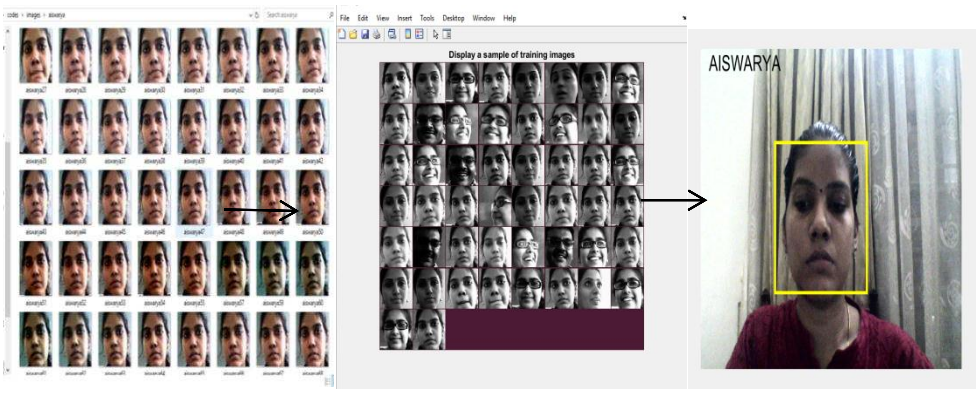
Output Class \ Target Class	aiswarya	anaya	arathy	arun	divya	jeril	nandana	outsider	ridhwik	sandra	sonali	varsha	
aiswarya	10 10.5%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	100% 0.0%
anaya	0 0.0%	4 4.2%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	100% 0.0%
arathy	0 0.0%	0 0.0%	9 9.5%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	100% 0.0%
arun	0 0.0%	0 0.0%	0 0.0%	6 6.3%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	100% 0.0%
divya	0 0.0%	1 1.1%	0 0.0%	0 0.0%	10 10.5%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	90.9% 9.1%
jeril	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	7 7.4%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	100% 0.0%
nandana	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	9 9.5%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	100% 0.0%
outsider	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	10 10.5%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	100% 0.0%
ridhwik	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	4 4.2%	0 0.0%	0 0.0%	0 0.0%	100% 0.0%
sandra	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	10 10.5%	0 0.0%	0 0.0%	100% 0.0%
sonali	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	6 6.3%	0 0.0%	100% 0.0%
varsha	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	9 9.5%	100% 0.0%
	100% 0.0%	80.0% 20.0%	100% 0.0%	100% 0.0%	100% 0.0%	100% 0.0%	100% 0.0%	100% 0.0%	100% 0.0%	100% 0.0%	100% 0.0%	100% 0.0%	98.9% 1.1%

Fig-11: Confusion matrix for image classification



```
Training on single CPU.
Initializing image normalization.
|=========================================================================================|
|  Epoch  |  Iteration  |  Time Elapsed  |  Mini-batch  |  Mini-batch  |  Base Learning  |
|         |             |   (hh:mm:ss)   |   Accuracy   |     Loss     |      Rate       |
|=========================================================================================|
|       1 |           1 |       00:00:02 |       10.94% |       2.8188 |      1.0000e-04 |
|      17 |          50 |       00:02:12 |       98.44% |       0.0964 |      1.0000e-04 |
|      34 |         100 |       00:04:25 |       99.22% |       0.0651 |      1.0000e-04 |
|      50 |         150 |       00:06:38 |      100.00% |       0.0147 |      1.0000e-04 |
|      67 |         200 |       00:08:50 |      100.00% |       0.0153 |      1.0000e-05 |
|      80 |         240 |       00:10:36 |      100.00% |       0.0204 |      1.0000e-05 |
|=========================================================================================|

accuracy =

    0.9895
```

Fig-12: Training process for image classification

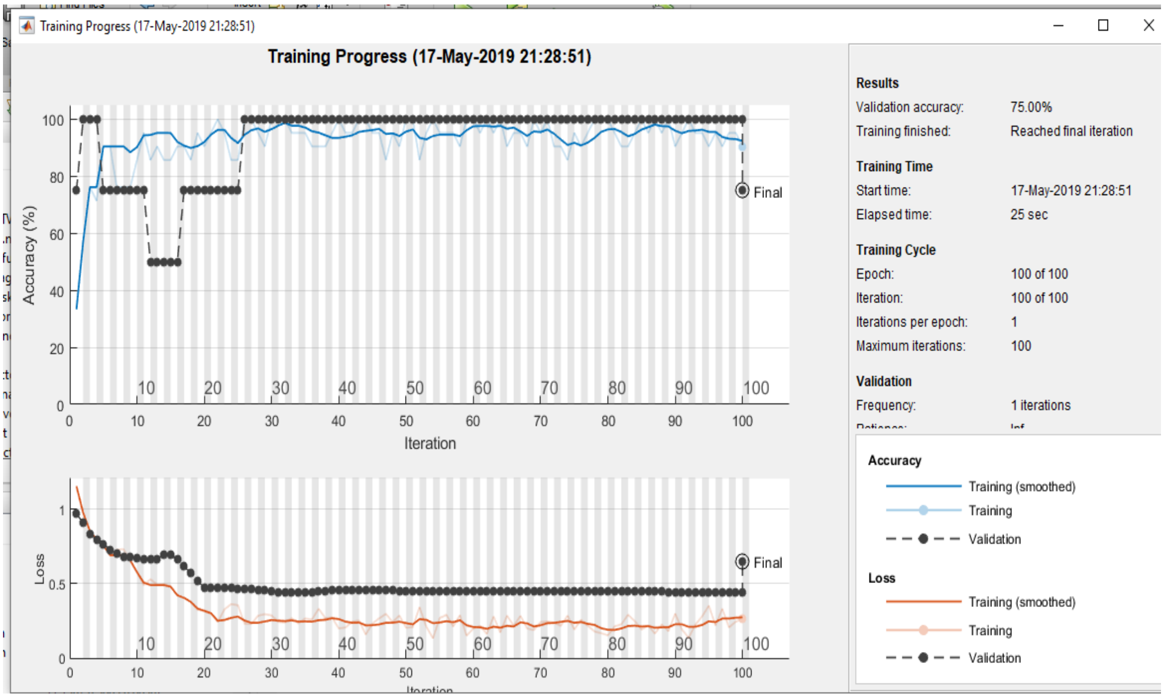


Input images **Training images** **Recognize image**

Fig-13: Output for image detection

4.3 Voice Recognition

Voice recognition uses CNN (Convolutional Neural Network). It is a deep learning technique. This phase uses a trained network. Training the 80% of stored voices and remaining 20% of the voices for testing. This system recognizes the voice command from the given input and approves door access. This system trained with accuracy of 95.2% and the error rate of 4.8%.



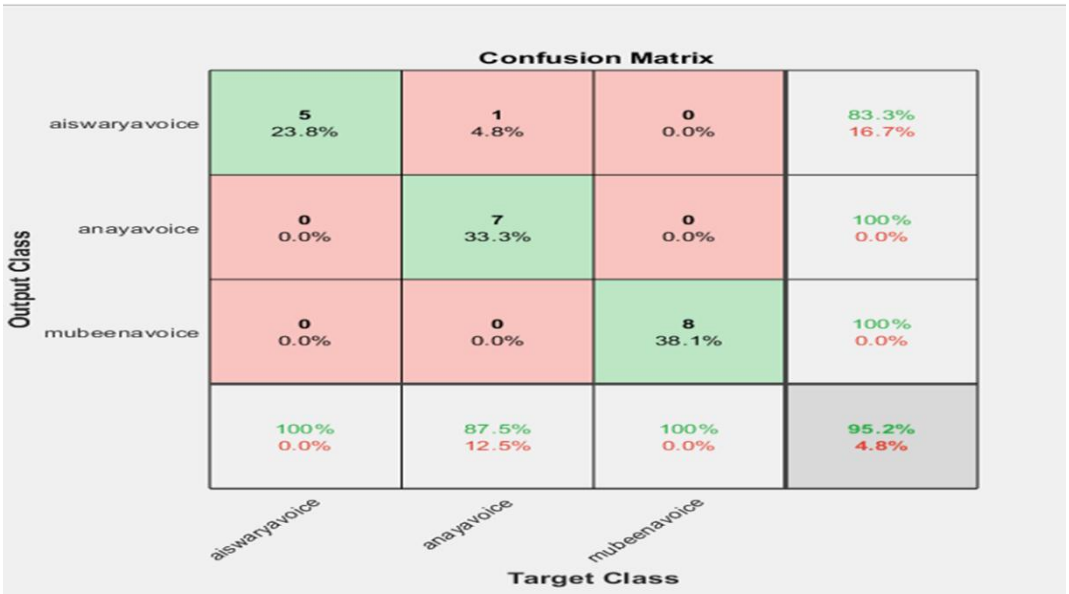
Results
Validation accuracy: 75.00%
Training finished: Reached final iteration

Training Time
Start time: 17-May-2019 21:28:51
Elapsed time: 25 sec

Training Cycle
Epoch: 100 of 100
Iteration: 100 of 100
Iterations per epoch: 1
Maximum iterations: 100

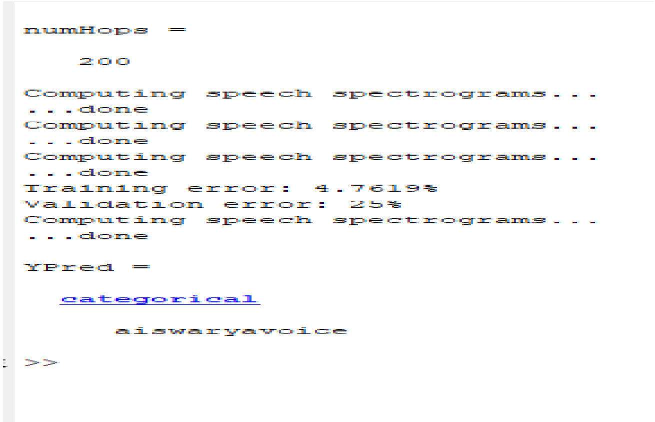
Validation
Frequency: 1 iterations

Fig-14: Graph showing training process of voice recognition



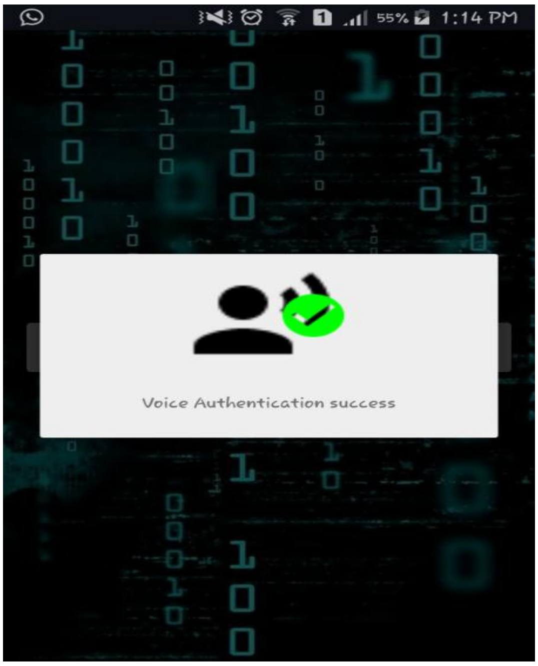
	aiswaryavoice	anayavoice	mubeenavoice	
aiswaryavoice	5 23.8%	1 4.8%	0 0.0%	83.3% 16.7%
anayavoice	0 0.0%	7 33.3%	0 0.0%	100% 0.0%
mubeenavoice	0 0.0%	0 0.0%	8 38.1%	100% 0.0%
	100% 0.0%	87.5% 12.5%	100% 0.0%	95.2% 4.8%

Fig-15: Confusion matrix for voice recognition



```
numHops =

   200

Computing speech spectrograms...
...done
Computing speech spectrograms...
...done
Computing speech spectrograms...
...done
Training error: 4.7619%
Validation error: 25%
Computing speech spectrograms...
...done

YPred =

  categorical

     aiswaryavoice

>>
```

Fig-16: Predicted the authenticate voice command



Voice Authentication success

Fig-17: Voice Authentication Page

V. CONCLUSION

Different types of door lock security methods and different security technologies were studied. The paper is basically a door lock system using image detection and voice recognition methods.

An ARM microcontroller was used for controlling the entire door lock system. The microcontroller was connected with a motor, motion sensor, LCD display, buzzer and a Wi-Fi module. The Wi-Fi module was paired with user registered mobile phone and server system, the entire system was interacting with an android application called ‘Door Lock System’. The Wi-Fi module was always connected with server system, if any person approaches the door the motion detected by the motion sensor and the buzzer produces an alarm sound, the microcontroller enabled the camera and it captured the detected person’s image. The image stored into the server and the server system contains the database, it compared with new captured image if any match was occurred it was a known person otherwise an unknown person regardless send a notification to the registered mobile. The authorized user verified the image and allows entry by using his/her voice command, the voice command was verified with server and their already having a database of authorized users, and checking that it was valid or invalid. If it was valid door open otherwise door remains locked.

The image detection module was detecting the person by compared with stored database images, the method used for image detection was Convolutional Neural Network (CNN) it is a deep learning technique. This recognized the human face with labelled name and sends it as a notification to user application. This image detection achieved an accuracy of 98.9%.

The voice recognition module was controlled by the authorized users, the method used for voice recognition was Convolutional Neural Network (CNN) it is a deep learning technique. The detected face sends a notification to the user application the authorized user allows entry by used his/her voice command. This command checked in server it was a valid unlock the door otherwise the door remains locked. Voice recognition method recognizes the voice and detecting the authorizing voice and achieved an accuracy of 95.5%.

An Android application for login, registration of user details, and transmission of an OTP to a registered mobile phone for improved lock security, was implemented. A random number was created as an OTP and user details were stored in the server system. 'Image Detection System 'was successfully implemented and the output was obtained.

This proposed system overcomes the problems behind the existing systems. This system provides a two way security mechanism-image detection module detecting the person after that it will send a notification to the user application and the voice command is used for authorizing entry. The system sends an alert message to all the authorized users, if any intrusion occurs. This door locks system secure and can used in home security and office.

VI. REFERENCES

[1] Muhammad Sabirin Hadis, Amil Ahmad Ilham, Akbar Hendra and Elyas Palantei, "Design of Smart Lock System for Doors with Special Features using Bluetooth Technology", 2018 International Conference on Information and Communications Technology (ICOIACT).

[2] Faizaman, AnithaC, "Motion Sensing and Image Capturing based Smart Door System on Android Platform", International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017).

[3] Meera Mathew, Divya R S, "Super Secure Door Lock System For Critical Zones", 2017 International Conference on Networks & Advances in Computational Technologies (NetACT) |20-22 July 2017.

[4] Arun Cyril Jose, Reza Malekian "Improving Smart Home Security: Integrating Logical Sensing Into Smart Home", Journals& Magazines , IEEE Sensors Journal Volume: 17 Issue: 13.

[5] Ravi Kishore Kodali, Vishal Jain, Suvadeep Bose and Lakshmi Boppana,"IoT Based Smart Security and Home Automation System", International Conference on Computing, Communication and Automation (ICCCA2016).

[6] Freddy K Santoso , Nicholas C H Vun "Securing IoT for smart home system", 2015 International Symposium on Consumer Electronics (ISCE).

[7] Gyanendra K Verma and PawanTripathi, "A Digital Security System with Door Lock System Using RFID Technology", International Journal of Computer Applications (0975 – 8887) Volume 5– No.11, August 2010.

[8] Mohan M, Vishal Kannan, M Keshav," Phone Controlled Security Lock Systems ",International journal of Advanced ResearchVol. 6, Issue 4, April 2017.

[9] Yong Tae Park,Pranesh SthapitandJae-Young Pyun,"Smart Digital Door Lock for the Home Automation",TENCON 2009 - 2009 IEEE Region 10 Conference.

[10] JayantDabhade, AmirushJavare, TusharGhayal, AnkurShelar and Ankita Gupta," Smart Door Lock System: Improving Home Security using Bluetooth Technology", International Journal of Computer Applications (0975 – 8887) Volume 160 – No 8, February 2017.

[11] Esenogho Ebenezer, Idiagi Neville S. and Igimoh John A. “Development and Implementation of a Biometric Security Lock System”,Reserchgate March 2013.

[12] Meera Mathew, Divya R S “Survey on Various Door Lock Access Control Mechanisms”, 2017 International Conference on circuits Power and Computing Technologies [ICCPCT].