International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 05 | May 2023 www.irjet.net p-ISSN: 2395-0072

AUTOMATIC DOOR UNLOCK WITH FACIAL RECOGNITION USING IoT

Birali Prasanthi[1], Kakumani Sravya[2], Komirishetty Saiteja[3]

[1]*Senior Assistant Professor, Dept. of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Hyderabad, Telangana, India*
[2]*Student, Bachelors in Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Hyderabad, Telangana, India*
[3]*Student, Bachelors in Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Hyderabad, Telangana, India*

Abstract - *Security is the primary problem that must be dealt with in the current society. With the recent progress in emerging technologies, IoT stands out as a cutting-edge technology capable of resolving a wide range of security-related issues. This paper deals with the proposed system for a sophisticated and knowledgeable door that unlocks automatically when a registered face is recognized. The faces in the dataset are first detected using the hog model and then the detected faces are encoded using OpenCV libraries. Whereas, the Haar Cascade classifier is used for real-time facial detection. The objective of this project is to replace traditional passwords and patterns and add more security to the lives of people. This process is carried out by the raspberry pi3B because it has low processing time.*

Key Words: OpenCv, Haar Cascade classifier, hog model, Raspberry pi 3B.

1. INTRODUCTION

Faster and accurate identification and authentication methods are necessary in this modern era. Facial recognition is one such method, but the problem is that the software should be able to able to distinguish spoofing and should be highly accurate. It is thus necessary to use appropriate algorithm. The system collects the images of registered users in the database. The faces in these images are detected and then encoded. The encodings of detected faces during the livestream are then compared with the encodings in the database. If they match then the door will be unlocked. To achieve this Raspberry pi, solenoid lock, relay module and raspberry pi camera are used .Facial recognition is preferred over other biometrics because they can be taken without owner's consent and thus useful for various security related applications. Furthermore, images can also be taken from distance which is unique compared to other approaches.

1.1 Proposed System

The proposed system unlocks the door if a registered face is recognized and sends a telegram message with the picture of the unknown face and an OTP. The intruder can unlock the door if and only if he enters correct OTP through Bluetooth. In this system an interface is created to collect images of registered users comfortably. Here, the faces in dataset are first detected using hog model and these detected faces are encoded. Haar cascade classifier is used for real-time face detection for more accuracy.

1.2 Hardware requirements

Raspberry Pi 3 B: It is a third-generation Raspberry Pi. This powerful credit-card-sized single board computer outperforms the previous models. Its processor is ten times faster than that of the original Raspberry Pi. It also supports wireless LAN and Bluetooth connectivity.

Raspberry Pi camera module v1.3: It receives software and hardware support from the developers as it is an official product of the foundation. It has a 5-megapixel OV5647 sensor. It supports video modes of 1080p30, 720p60 and 640X480p60/90 video record. It can be connected to the Raspberry Pi at the CSI port using a flex cable. It provides 2592 X 1944 still picture resolution. It is compatible with both model A and model B and weighs about 3 grams.

HC-05 - Bluetooth Module: It is a popular Bluetooth module that can add full-duplex wireless functionality. It has a range of up to <100m which depends upon transmitter and receiver, atmosphere and geographic conditions. Serial communication is used between two devices.

Relay module: A relay is electromechanical device that uses an electric current to open or close switch contacts.

Solenoid lock: Solenoids are primarily electromagnets made up of an enormous coil of copper wire with a metal in the centre. When the current flows through the coil, the slug is drawn into the coil's centre. This allows the solenoid to pull from only one end. It's basically an electronic lock, used for a basic cabinet, safe or door.

1.3 Software requirements

Raspberry Pi OS: It is previously known as Raspbian and is officially supported OS. It's based on Debian and is built on

the same philosophy that is stability and performance. Many Debian packages are available on Raspberry Pi OS.

OpenCV: OpenCV can be used to develop real-time computer vision applications. It is a cross-platform library. It can be used for image processing, video capture and analysis including various functions like face object detection. It has more than 2500 algorithms, extensive documentation and sample code for real-time computer vision.

Telegram Bot: Telegram Bot is a good way to deliver information whenever it is needed. It behaves like a normal chat partner but with extra features. It has an ability to execute commands which can request information or trigger an action.

2. LITERATURE SURVEY

A study on Development of Intelligent Door Locking System based on Face Recognition Technology [1] presents an affordable smart door locking systems based on facial recognition using Arduino and Android phone. The system can perform all the stages on its own. This system is easy to tune and allows to update the database for face recognition easily. But this does not detect spoofing accurately and it is difficult to add OpenCV directories to the phone.

Another study on Remotely Accessible Smart Lock Security System with Essential Features [2] presents a smart locking system without face recognition. The stream begins when the visitor presses the calling bell. The owner can monitor the live stream using Raspberry Pi's IP and decide whether to unlock the doors. This system provides remote access but does not provide automation.

Secure Home Entry Using Raspberry Pi with Notification via Telegram [3] presents an automatic door unlocking system where IR sensor is used for object detection. When an object is detected, camera gets triggered. It also uses various sensors like temperature sensor and gas sensor which can be used for fire detection for sensing the gas leakage respectively. This system is of low cost and consumes low energy. It uses telegram notification which can be easily used even by older generation. The disadvantage of this system is that it requires high processing time.

Face Recognition for Smart Door Lock System using Hierarchical Network [4] uses a hierarchical classification network based on two-tier recognition systems. It used ResNet101 for recognition and FaceNet for authentication. It recognizes registered faces with an accuracy of 87.36 percent and it also provides a user interface for altering registered faces. However, it does not provide a way for the owner to open the door if an unregistered user is detected. It also does not detect spoofing accurately due to which an intruder can open the door with the image of the registered user.

3. METHODOLOGY

3.1 System Architecture

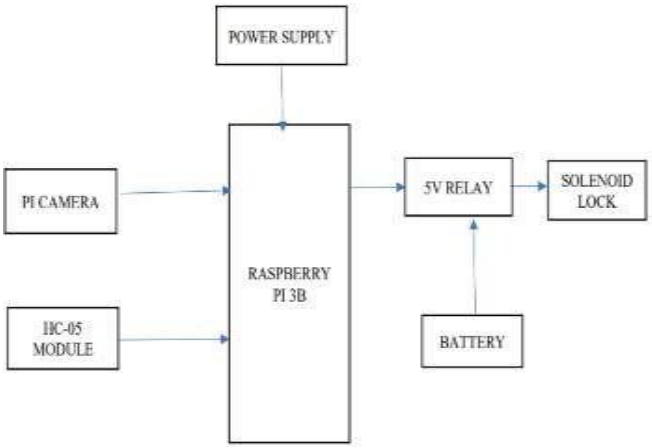

Fig -1: Architecture for automatic door unlock system

Raspberry Pi controls the overall functioning of the system. Picamera which is used to take pictures and video is attached to the camera slot of the Raspberry Pi using a flex cable. The HC- 05 module is connected to RX pin of Raspberry Pi so that the Raspberry Pi can receive the OTP entered. Relay helps in locking and unlocking the solenoid lock and is controlled by Raspberry Pi. Raspbian is used to program Raspberry Pi and Open CV libraries are used for image processing. The architecture of the system is shown in Fig1.

3.2 Methodology for face recognition

First, the photos of authorized users are collected along with their names through a GUI upon running "facedataset.py". Then the faces in the dataset are detected using a Histogram of Oriented Gradients (HOG). These detected faces are then encoded and dumped into a pickle module along with their names. Upon processing all the images in the dataset the video stream will turn on and Haar Cascade Classifier will detect the face in the live stream. The detected faces are then encoded and compared with the previously encoded data. If it matches with any of them, then the person is considered authorized and the door opens automatically

3.3 Implementation Steps

i. Creating a Telegram Bot:

BotFather which is a Telegram Bot is used to create a new bot and the command "/newbot" is used to create it. Upon creating a new bot with a valid username, a token is generated. This token can be used while programming, to allow communication between the microcontroller and the owner. Creation of bot is illustrated in Fig2.

Fig -2: Illustration of creating a new bot

ii. Data Gathering and training:

Here the pictures of authorized users are collected through a GUI. Upon successfully running "faceDataset.py" in the source code. An interface named "Database creation" will pop up with a blank to enter the name as shown in Fig3 and the video capture will not start until the folder is created. Upon entering the name and clicking on the button "create", a folder with the given name will be created in "dataset" directory.

Fig -3: Interface for database creation

When "start Capture" button as in Fig3 is clicked, a small application as shown in the Fig 4 will pop up. This application will help us to click the picture and it will save the pictures in the picture automatically in directory "sravya" which is the secondary directory. Here, required number of pictures can be taken by simply pressing the button "Snapshot!", and all these pictures will be saved automatically to the directory "sravya" which is the secondary directory here.

Fig -4: Application for image capturing

After creating the dataset of all the authorized users along with their names, the faces of the images in the dataset need to be detected and the encoded, which is together termed as processing here. Upon running "facerecognition.py" the processing of the images in dataset occurs and after successfully completing the processing of all the images in the data set all the encodings are serialized and video stream will start as in Fig5. Real-time detection is done during the stream. The faces of the objects in this stream are first detected and then compared with the dataset of registered faces to identify if they are registered user.

Fig -5: Starting of Video stream

4. RESULT

Side view of the initial hardware setup is shown in Fig 6.

Fig -6 : Side view of the automatic door setup

When a face is detected, the device will encode the detected face and compare it with the encodings of faces in the dataset. When the encodings are matched then the device will recognize the detected face as a registered user. When detected face is recognized as the authorized, the door opens as shown in Fig 7..

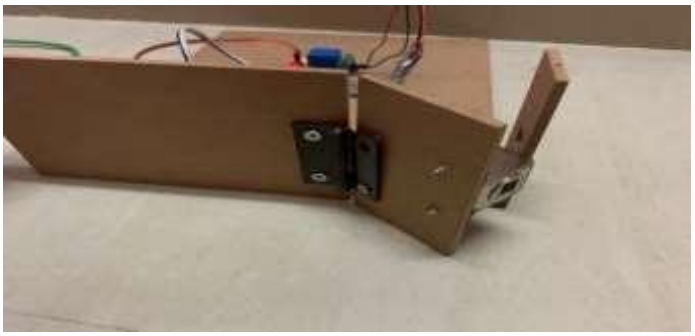

Fig -7: Opening of door when an authorized user is detected

When an unregistered user is detected a telegram notification is sent to the owner along with an OTP as in Fig 8.

Fig -8: Message sent to the owner's telegram

Fig -9: Bluetooth terminal HC-05

The guest needs to connect to the Bluetooth terminal HC-05, where he can enter the OTP as in Fig 9. The door unlocks only if he enters the correct OTP.

5. CONCLUSION

This system detects faces faster and with high accuracy. When a registered face is recognised, the door unlocks successfully and when an unregistered face is recognized, message will be sent to owner's telegram. The door opens successfully if correct OTP is entered. But the problem arises when multiple faces is detected at a time and when the intruder tries to unlock the door by spoofing registered user's face. The result is unpredictable in both these cases. When multiple faces are recognised, the door should be unlocked even if there is one registered user among them, but here the result depends upon whose face is detected first and the result of spoofing depends upon the quality of the imaged used by the intruder.

REFERENCES

[1] Khalimov, R., Rakhimbayeva, Z., Shokayev, A., Kamalov, B., & Ali, M. H. (2020) "Development of Intelligent Door Locking System Based on Face Recognition Technology" 2020 11th International Conference on Mechanical and aerospace engineering (ICMAE).

[2] Pinjala, S. R., & Gupta, S. (2019). Remotely Accessible Smart Lock Security System with Essential Features. 2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET).

[3] N., H., & Yadav, J. (2020). Secure Home Entry Using Raspberry Pi with Notification via Telegram. 2020 6th International Conference on Signal Processing and Communication (ICSC).

[4] Waseem M., Khowaja S. A., Ayyasamy, R. K., & Bashir, F. (2020) "Face Recognition for Smart Door Lock System using Hierarchical Network". 2020 International Conference on Computational Intelligence (ICCI).