Prevention of unauthorized door access using face recognition built with Haar Cascade Classifier and Histogram of Oriented Gradients

ARUNKUMAR N[1], KUNDHAN P[2], JOHN SHAHID SK[3], SUNITA PANDA[4],
KAMALANATHAN CHANDRAN[5]

[1,2,3]UG Student, Department of Electrical, Electronics and Communication Engineering,

[4]Assistant Professor, Department of Electrical, Electronics and Communication Engineering,

[5]Associate Professor, Department of Electrical, Electronics and Communication Engineering,

GITAM School of Technology, GITAM Deemed to be University, Bengaluru.

.

Abstract:

With the emergence of Internet of Things (IoT) along with its development of advanced authentication, both security and remote monitoring have become imperative as well as essential, and the need for smarter security systems has only been growing. The traditional system needs an individual to use a key or an identification (ID) card or a password to access the security doors. However, they have many limitations such as keys can be forged, recreation of ID cards and passwords can be stolen. To overcome, the existing system issues, a novel approach is proposed with the design and development of face authenticated web-based smart door lock control system using facial recognition and remotely monitoring the door. In this proposed system OpenCV's self-trained Haar Cascade Classifier along with Histogram of Gradient is used for face Recognition. Door will be unlocked when user's face is recognised else will remain closed. In case an unauthorised person is found, the time of intrusion and the intruders' image will be captured and sent to a separate server on discord, so that the user or the admin can view them at their convenience. The main usage of this system is to assist users for improvement of the door security of sensitive locations by using face recognition and is also designed by considering the physically challenged persons also.

Keywords: Raspberry Pi, Discord, Face recognition, IoT, Haar Cascade Classifier.

1. INTRODUCTION

In modern world of connectivity and smart devices, security is a crucial role in various places, so there is an urgent need to modify our existing day to day objects and make them smart and more secure, also it is not the era where one can blindly trust the old and conventional security measures, specifically door locks. The drawbacks in a traditional door lock system is that anyone can open the lock by duplicating or stealing the key and it is impossible for relatives and friends to enter the house, without us physically present over there. To overcome the existing issues, a novel approach is proposed. In this proposed system, a normal door system can be replaced by a smart door system to provide security for residence, which can open the door whenever the user stand in front or open up for someone else without being physically present.

Face recognition is the technology which is used to find access through the secured system. But there might be a risk of entering an unauthorized person into a restricted area. So, there is a requirement of upgradation from face detection to face recognition helps to achieve good security level compared to existing methodology. Instead of detecting the face recognition plays an important aspect in security system. With this proposed approach, to identify a person, the captured face is compared with the faces in the bundled dataset. The aim is to search a face in the dataset, which has the highest similarity with the given face. The need of face recognition in security systems is attributed to the rise of commercial interest and therefore the development of feasible technologies to support the development of face recognition. IoT enables things to be sensed or controlled remotely via established network infrastructure, making motivators for additional dynamic joining of the physical world into PC based frameworks and the subsequent in improved profitability, exactness and financial addition close by diminished human obstruction.

The face recognition system with IoT technology is proposed to access the door. The proposed system helps for the physically handicapped people. On the off chance that the framework neglects to perceive the individual, the intruders' image is sent over web to the proprietor. This system utilises Raspberry Pi with OpenCV installed and programmed such that it can recognise only authorised users and controls the door locking mechanism. The real-time data will be sent over internet to discord server, so that the admin will be notified where ever possible. The first task is to detect the face using Haar Cascade Classifier and search them in the dataset, which were trained using HOG feature descriptor.

2. LITERATURE REVIEW

Over last few decades, the security systems have been configured to recognize the intruder’s face and thus some of the face images at various angles and light conditions are added to the database. Use of technology within the field of security plays a vital role in increasing the protection yet as reducing the man power efforts.

Nooman S et al. [1] had executed security framework where if any individual came before the entry way it was informed to the property holder by means of email and twitter then the client could see the individual remaining at the entry way utilizing camera from remote area. The confinement of this work happens if the client didn't have web association.

Ramaj V. et al. [2] proposed continuous access control for face acknowledgment using Raspberry pi rather than GSM administrations and transfer. The restriction of the work was it couldn't control the foundation light circumstance and encompassing light conditions.

Lwin H.et al.[3] has proposed an entry way lock get to framework which comprises of three sub systems to be explicit face acknowledgment, face identification, and computerized entry way get to control. PC is related with the microcontroller. The whole framework won't work if PC is smashed or when Non-Functioning.

M. Carikci et al. [4] proposed a work on A Face Recognition System dependent on Eigen face technique in which they utilized Eigen strategy for face acknowledgment and Euclidean separation technique to think about the picture of the individual worried about the pictures in the database. It was extremely proficient and quick strategy and furthermore gave high precision.

3 METHODOLOGY

Existing Methods

In the existing systems, Local Binary Pattern (LBP) and along with Support Vector Machines has been used. Both LBP and SVM methods are inefficient with respect to accuracy and performance. So, using Haar cascade classifier, truly created for object and face recognition, contains a collection of most complex classifier in cascade form to increase the speed of detection. This method utilizes integral images to increase the computation sum of pixels. This selection algorithm is based on the computation of difference in sum of black pixels and the sum of white pixels. Use of Passive Infrared (PIR) sensor comes with its drawbacks, that it captures intruder data even if the person is standing in front of door, who doesn't need access to it. Also, in the existing systems, a database or a message sending service is used, where they might not be capable of either handling the usage data or the high database storage costs or the intruder's images is not sent to the user. To overcome the above issues, we can use of discord messenger, to post images and messages using webhooks.

Proposed Method

Training a cascade classifier: OpenCV provides some useful applications to self-train cascade classifier, that are: *opencv_createsamples* and *opencv_haartraining.* Training the classifier, requires positive images (images with faces) and negative images (images without faces). In this proposed system, 1000 positive images and 10000+ negative images are used for classifier. It is always suggested to maintain at least 1:10 ratio of positive and negative images. The steps involved areas follows:

Step 1: Create positive and negative datafiles from the images.

Step 2: Create Samples data file using *opencv_createsamples*.

Step 3: Convert Samples data file to vector format using *mergevec*.

Step 4: Generate temporary *haarcasade* file using *opencv_haartraining*.

Step 5: Convert *haarcascade* file to .xml (Extensible Mark-up Language) file

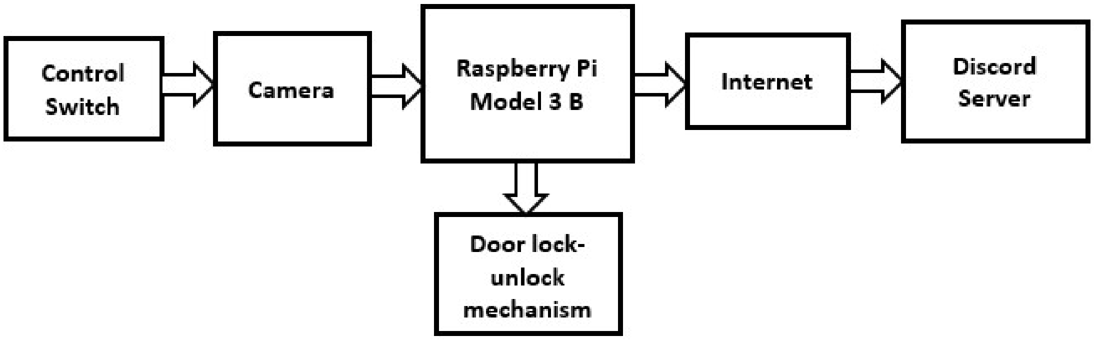


Fig 1: Block Diagram

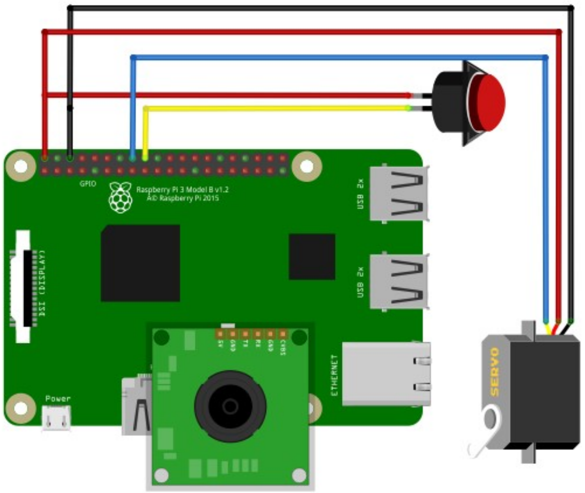


Fig. 2: Circuit Arrangement

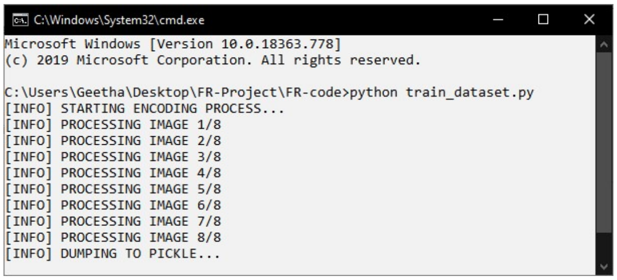
To implement smart door model, components such asRaspberry Pi 3 Model B with OpenCV installed, Camera, Servo motors for door mechanism, control switch and internet are required. Camera is attached to Raspberry Pi and it is connected to internet for face recognition, and a servo motor is attached to the door for closing and opening. The proposed system is designed on the basis of Haar cascade detection. Initially the owner’s image is captured in different angles and is stored in dataset folder. The facial vectors encodings of the images are stored so that it helps in fast comparison and recognition. Servo motors are used for door mechanism, which is connected with raspberry pi for controlling the moment or the rotation, the size and operations can be varied depending on the usage. If the face is recognized it implies that an authorized person is trying for the door access and hence the door lock is opened, but if the face is not recognized, then the remote user gets a notification along with the image of the intruder in discord server using webhooks, which in turn creates a bot for posting messages. This reduces the cost of database and their complex setup.

4. Experimental Setup

Hardware tools used: Raspberry Pi, Pi camera, Push Button, Servo Motor, Connecting wires. Software used: OpenCV, Python, Discord, Raspbian OS.

5. Result

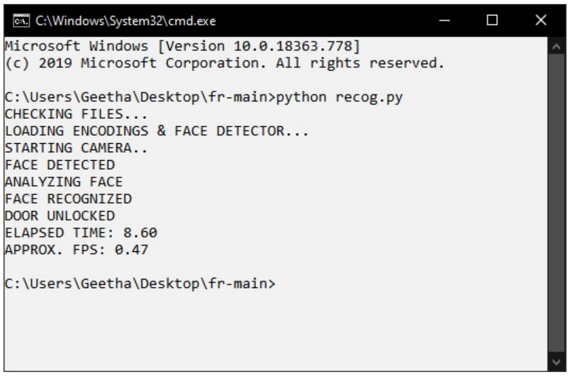
When the user pushes the button, the camera will capture the face. The image vector readings are compared to the face encodings in the dataset, which was initially trained using multiple user faces. If the data is matched, the door will be opened, if not matched the captured image will be sent as a notification along with warning message to user's discord account.



```
Microsoft Windows [Version 10.0.18363.778]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Geetha\Desktop\FR-Project\FR-code>python train_dataset.py
[INFO] STARTING ENCODING PROCESS...
[INFO] PROCESSING IMAGE 1/8
[INFO] PROCESSING IMAGE 2/8
[INFO] PROCESSING IMAGE 3/8
[INFO] PROCESSING IMAGE 4/8
[INFO] PROCESSING IMAGE 5/8
[INFO] PROCESSING IMAGE 6/8
[INFO] PROCESSING IMAGE 7/8
[INFO] PROCESSING IMAGE 8/8
[INFO] DUMPING TO PICKLE...
```

Fig. 3 Training the dataset

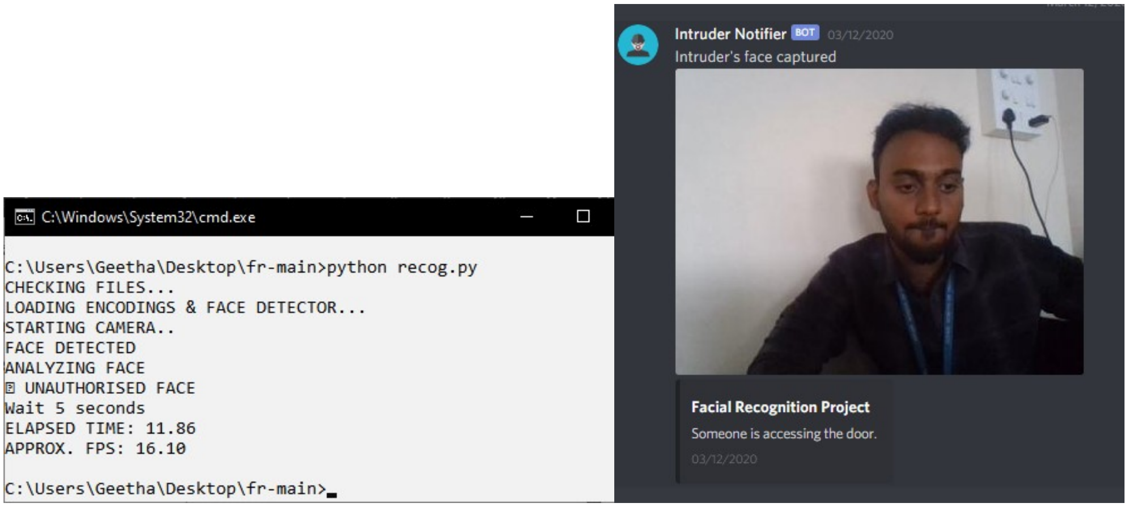


```
Microsoft Windows [Version 10.0.18363.778]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Geetha\Desktop\fr-main>python recog.py
CHECKING FILES...
LOADING ENCODINGS & FACE DETECTOR...
STARTING CAMERA..
FACE DETECTED
ANALYZING FACE
FACE RECOGNIZED
DOOR UNLOCKED
ELAPSED TIME: 8.60
APPROX. FPS: 0.47

C:\Users\Geetha\Desktop\fr-main>
```

Fig. 3: Result when face is recognised



```
C:\Users\Geetha\Desktop\fr-main>python recog.py
CHECKING FILES...
LOADING ENCODINGS & FACE DETECTOR...
STARTING CAMERA..
FACE DETECTED
ANALYZING FACE
□ UNAUTHORISED FACE
Wait 5 seconds
ELAPSED TIME: 11.86
APPROX. FPS: 16.10

C:\Users\Geetha\Desktop\fr-main>
```

Intruder Notifier BOT 03/12/2020
Intruder's face captured

Facial Recognition Project
Someone is accessing the door.
03/12/2020

Fig. 4: Result when face is not recognised

6. Conclusion

This proposed system mainly focuses on security by utilizing Raspberry Pi, OpenCV, Python, Machine Learning, IoT to a great extent. With the implementation of face recognition and remote accessibility, the user can have a freedom if the door should open or keep it locked. The system also keeps track of the visitors by storing the date and time of the visit along with their name in the database. The end goal is to improve home security, providing better resource management and physically challenged people. This implementation of project is cheap, fast, and highly reliable as Raspberry pi takes less power with enough flexibility and also reduces the database and maintenance costs, giving more control to the user.

Future work

[1] In case of power failures, the door may not be used so necessary power backup can be provided.
[2] A voice assistant with a speaker can be deployed, which would be helpful for people who are not good at using technology.
[3] Highly secure protocols such as TLS can be used to ensure there is no security breach.
[4] Certain motion sensors can be attached to door, so that it can warn user/owner when someone tries to break the door.
[5] Wider angle cameras and cameras with more pixel resolution can be used to improve the overall efficiency.
[6] Real-time or live video streaming can be provided to user/owner, so that the door can also be used as a surveillance camera.

REFERENCE:

[1] Nooman S, Chowdhury M,2013. Access Control of Door and Home Security by Raspberry Pi through Internet.
[2] Ramaj V. JanuzajY, Luna A, 2015 Real time access control based on Facial Recognition.
[3] H Lwin, Aung SoeKhaing, HlaMyo Tun, “Automatic Door Access System Using Face Recognition”, International Journal of Scientific & Technology Research, June2015.
[4] ÇarıkçıM, Özen F, 2012. A Face Recognition System Based on Eigen faces Method.
[5] Discord Documentation https://discordapp.com/developers/docs/intro
[6] Haar Training http://note.sonots.com/SciSoftware/haartraining.html
[7] Raspberry Pi Foundation [Online] http://www.raspberrypi.org/downloads/.