ISSN 2278-3091

Volume 9, No.5, September - October 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse104952020.pdf

https://doi.org/10.30534/ijatcse/2020/104952020

Multi-Way Door Unlocking Using Raspberry Pi

T.Jalaja[1], Dr. T. Adilakshmi[2], Aditya Abhiram A [3]

[1] Vasavi College of Engineering (A), India, jalaja.t@staff.vce.ac.in

[2] Vasavi College of Engineering (A), India, t_adilakshmi@staff.vce.ac.in

[3] Vasavi College of Engineering (A), India, aditya.abhi123@gmail.com

ABSTRACT

Security is the main problem in our daily life. Each and every individual person needs to be secure. An access control for the doors of the home or office is very essential in our security pattern. Doors which are locked/unlocked using the traditional locks are not safe as they can be easily broken. Therefore we provide a different way of solution to this problem which could serve full security to our home and other commercial places. Door Locking and Unlocking using Raspberry Pi is one such trial made where we could safe guard the home or any other lock. This system makes use of fingerprint and face detection to unlock doors. The system allows only authorized persons to access the room by unlocking the lock. It makes use of Raspberry Pi which can store the images or fingerprints of persons to authorize. Fingerprints are stored as images. It comprises of webcam which can take photos and fingerprint sensor which is matched with stored data to unlock. The most important and unique part of this model is recognizing an unauthorized user or thief by taking the image and sending it through mail to the admin. If the person is unknown, admin can be able to report it to police in the mean time. Therefore it plays a vital role in reducing the thefts across the country. This programmed multi-way unlocking system will provides users more secure system with minimal effort. The security door lock/unlock automation is an efficient mechanism for the future. The current mechanical door locking system can be replaced by this smart door lock with uses electronics.

Key words: Door Unlocking system, Raspberry Pi3, microcontroller, face detection, figure print recognition, camera.

1. INTRODUCTION

The problem of not having proper and efficient security at commercial and household places for keeping the secret rooms locked is one of the main problems in security sector. There have been many identification methods like password, drawing patterns which were not as efficient as this method of face and finger identification. Decoding the passwords and drawing patterns have become very easy for professional hackers which would increase the problem of security. Face detection plays an important and powerful role in designing the smart door unlocking security system for the modern era. It is being implemented in many other platforms like Attendance system in school/ colleges, door. Hence, this inexpensive model can make our life safe and secure. In addition to these this model can solve the problem of unlocking doors of the cars too by face detection which would be a boon in this developing world. OpenCV supports a wide variety of programming languages such as C++, Java, python etc. It is available on different platforms/ operating systems like Windows, Linux, OS X, Android, and iOS. OpenCV-Python is a library of Python bindings designed to solve many of the computer vision problems. The main purpose of this system is to provide high and reliable security at both commercial and household places by unlocking door only for specific authorized users using the efficient face and fingerprint detection. This can be implemented to attain better security for the country. The system also mapped to an application named ‘Pushbullet’ can be installed in admin mobile and is used to monitor the security of the home. If the user/person face does not match with the face stored in the module an email will be sent to the authorized user /owner with the attachment of the image/face of the thief. The application reads the images in real-time which provide much secure and easy way for monitoring**.**

2. LITERATURE SURVEY

2.1 Facial detection and recognition

Currently we can notice many robberies reported and it has become the major issue now-a -days. Typical ways of detection and recognition requires external elements such as keys, passwords, RFID tags in order to enter into any public space or private space. There are various drawbacks of these typical methods such as loss in keys, forgetting passwords, losing RFID tags may lead to loss in recognition of the person itself. This leads to a hassle situation to recover back. These methods are slowly getting replaced by biometric methods as it is one of the most efficient ways to solve the above mentioned drawbacks. These techniques involve usage of modern equipment such as finger print scanner, DNA analyzer, IR camera, palm scanner and other equipment in order to recognize and identify people. Biometric is a technique which is used to identify the physical features of any human being [1]. Biometric is one of the widely used trusted method/ technique for security purposes at office places. They are two types of biometrics - physical biometrics and behavioral biometrics. The face recognition and face detection technology has become one of the most significant areas for researchers and it is the most commonly used method now-a-days compared to older biometric methods. Face recognition is a process for image/face matching with the stored data. It is an emerging field which replaces the traditional method. It is the most stable method compared to the other methods of biometric because it uses the human faces (that does not change in people's life) with high accuracy and lowest false recognition.

2.2 Different methods of facial recognition

In the current situation, facial detection and recognition plays an important role in the security applications. It is used to develop the system which is cost-effective and secure. Face recognition has become an important technique which is used to use to identify the correct person/owner face and authorize them. Face recognition is used to identify the correct person or reject the wrong person. The input face is processed and later compared with the images/ faces that are stored in the database/library to verify whether the person is the authorized person or not.

Thus it is the prominent technique/method for identifying the user. The other techniques that support face recognition are Haar cascades, HOG + Linear SVM, Principle Component Analysis (PCA), OpenCV, or CNNs.

2.3 Facial Recognition using Raspberry Pi

Raspberry Pi 3 is a microprocessor which runs on Raspbian OS. It has got 1 GB of RAM. It is a mini-CPU which can perform less intense tasks. So methods such as CNN cannot be implemented in Raspberry Pi for facial recognition. Hence Histogram of Oriented Gradients (HOG) is used to perform the task [1]. Raspberry Pi is preferred for facial recognition instead of PC or laptop because of various factors such as its portability, power efficient, low cost, less weight, and many other factors. It divides the task into 3 parts- recording images, training and finally detection and recognition.

2.4 Finger Print Recognition using FingePrint Module

In this proposed work an optical biometric fingerprint reader/ sensor (R305) module is used for recognizing the fingerprint. The module is used with TTL UART interface for connecting to a UART microcontroller. The user should store the finger print data of the person (owner) in the module and later should configure it in 1:1 or 1: N mode in order to identify the person/owner. This module has capability to connect with either 3.3V microcontroller or 5V microcontroller. For this purpose a suitable converter or serial adapter is required for interfacing the module with the serial port of a PC.

3. PROPOSED MODEL

This paper has implemented the facial recognition technique which is used for the security purpose in real-time. Facial recognition technology is integrated with raspberry pi along with Internet of Things to design a home security smart system. A deep learning technique is used in identifying the faces in this paper. In this paper the data is collected first to train the system, later the algorithm is implemented to detect and recognize the face/ fingerprint and tested to identify the given image.

3.1 Data Collection and Training Phase

This phase deals with the training of the machine with a dataset consisting of the images of the authorized users. The images are captured using Pi Camera or a normal USB camera. These images are stored in the database and are used to train the model. Multiple images of each user are stored in a directory named with user's name in order to get the higher accuracy. These images are subjected to HOG, Haar Cascade and linear SVM models for facial detection. A Haar classifier is designed on an object detection framework. A single classifier is trained using each feature as shown in Figure 1. Multiple such classifiers are cascaded to get high accuracy as a single classifier does not give good accuracy. The final classifier is a weighted sum of previous classifiers. Using this method, the classifier provides classification with an accuracy greater than 95% [2].Then these images with faces detected are converted to 128-d vector embeddings using deep metric network. Along with facial data, fingerprints of the users are also captured using a fingerprint sensor which can be used for multi-factor authentication or night-time authentication where there is no sufficient light to capture an image. LDR (light dependent resistor) can be used to automatically detect the light intensity and switch between various methods for unlocking the door either by face or fingerprint. Figure1 shows the block diagram for training the face.

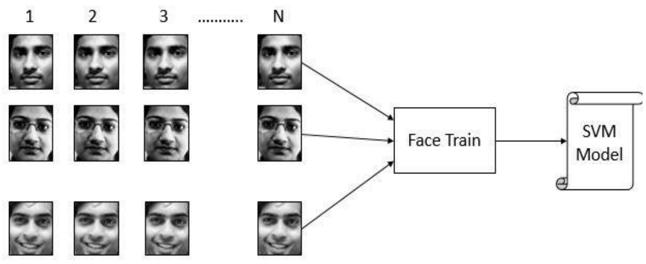

Figure 1: Block diagram of face training

3.2 Implementation Phase

This phase deals with implementation of the facial, fingerprint detection and recognition of the users for door unlocking.

The Raspberry Pi is setup by connecting the camera and other sensors in the correct position so that face of the person (owner) can be easily identified. Whenever any person comes in-front of the camera, his/her distance from the camera is measured continuously using a Ultrasonic sensor. Whenever the person in within a threshold distance value, the facial detection algorithm gets activated and images of the person are captured. These images are converted to 128-d vector embeddings and are compared with the embeddings that are stored in the database [3]. A match between them leads to successful authentication and a mismatch will indicate the presence of thief or un-authorized person. During night time or when there is no sufficient light, camera fails to capture the clear picture of the person which may lead to failure in accurate facial recognition. In such cases users can chose the option to unlock the door with their fingerprint which works based on optical patterns of the users that are stored in database. Raspberry Pi is used in applications which were successful in its performance [8].

Fingerprint processing requires two parts, one is the fingerprint enrollment and the other is fingerprint matching (the matching can be either 1:1or 1:N) [7]. At the time of enrolling the user/person has to enter the finger prints two times. The system will process the two given finger print images and generates a template based in the processed result of the finger prints and stores the template. In the matching phase the user/person enters the finger print through the optical sensor and the system will generate a template of the finger print and compares it with templates of the finger print present in the library. For 1:1 matching, system will compare the live finger with specific template designated in the Module; for 1:N matching, or searching, system will search the whole finger library for the matching finger. In both situations the system will return whether the matching result was success or failure. Figure 2 below shows the steps followed to register and recognize a fingerprint. Figure 3 shows the complete process for multi-way door unlocking.

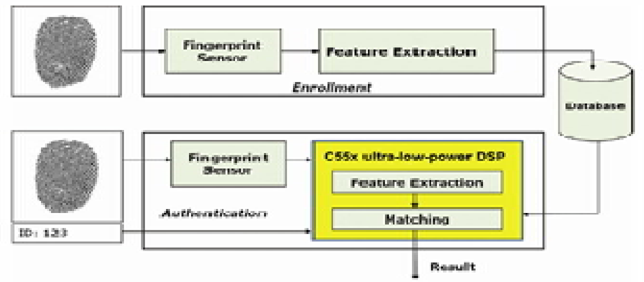

Figure 2: Series of steps which are followed to register and recognize a fingerprint.

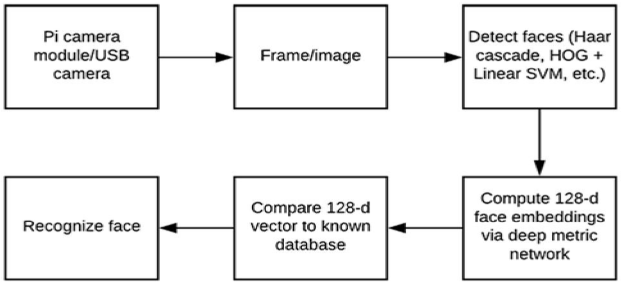
Pi camera module/USB camera
Frame/image
Detect faces (Haar cascade, HOG + Linear SVM, etc.)
Compute 128-d face embeddings via deep metric network
Compare 128-d vector to known database
Recognize face

Figure 3: Process for multi_way door unlocking

Figure 3. shows the detailed process starting from accepting/ capturing the input frames from Raspberry Pi. The workflow first detects the faces and then computes face embeddings, later compares it to the images in database through a voting mechanism. dlib and OpenCV are used for the recognition of the face.

3.3 Testing Phase

This phase involves testing of the application in various ways. Two main ways are used-

3.3.1. Testing the application with the images of the users. The system is tested with images of both authorized and unauthorized users.

3.3.2. Testing the system with real-time data of the users, i.e. a live video stream. In both the cases the application was successfully able to authenticate the authorized and trusted user with 90% accuracy and open the door for them. Fingerprint feature is tested using the fingerprints of various users who are successfully authenticated.

4. METHODOLOGY AND SECURITY

Here we explain the whole process of the paper. It can be segmented into two steps, algorithm that runs the facial recognition mechanism and the algorithm which ensures security by sending emails and notifications to users whenever any intruder tries to enter the house.

4.1 Facial Recognition Process

In general images are processed and identified in different applications [9]. In this paper Facial recognition process starts with a raspberry pi loaded with the images of the trusted users, arranged on the house door with an ultrasonic sensor, camera along with a finger- print sensor. The power to the system is supplied by a 12 re-chargeable battery. Ultrasonic sensor detects the presence of a person in front of the door and triggers the algorithm which starts capturing the images of the person [5]. User can choose either to unlock the door using his face or his fingerprint. The algorithm, using Deep learning and HOG methods, compare the images with the images stored in database. On successful authentication, it will unlock the door.

4.2 Security Provided by the System

The main purpose of the system is to provide a high level of security to the user. It should be reliable and robust. The system provides security in multiple ways. A threshold value is set which represents the number of un-successful attempts a person can make to unlock the door. On exceeding the threshold, algorithm that provides security will be trigged. It uses SMTP (Simple Mail Transfer protocol) to send an email to the user with images of the intruder attached with it[6]. It shares the time of intrusion along with images. The system also uses an application namely 'Pushbullet' which provides cloud functionality [4]. It sends the images to the mobile phone of the user using the app which stores them in the cloud account of the user. Figure 4 shows the process of facial recognition and the security implementation of the system.

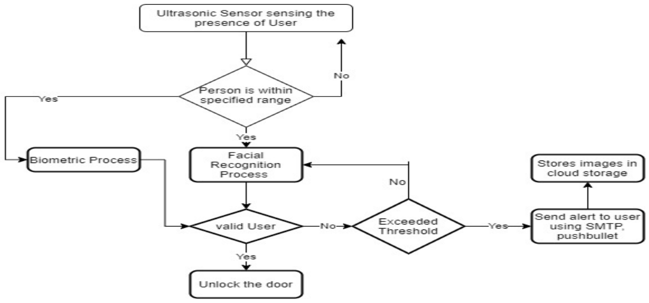
Ultrasonic Sensor sensing the presence of User
Person is within specified range
No
Yes
Yes
Biometric Process
Facial Recognition Process
valid User
No
Exceeded Threshold
No
Yes
Stores images in cloud storage
Send alert to user using SMTP, pushbullet
Yes
Unlock the door

Figure 4. Flowchart showing the process of facial recognition and security implementation of the system

5. RESULTS

Figure 5 shows the connections made using the raspberry pi. Figure 6(a) shows the identification of the valid face. Figure 6(b) shows the output after removing the face/invalid face.

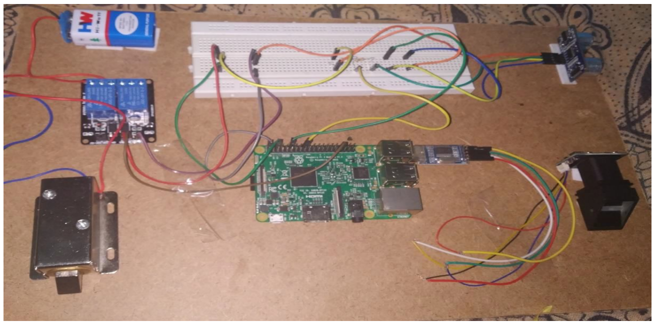

Figure 5: Connections diagram

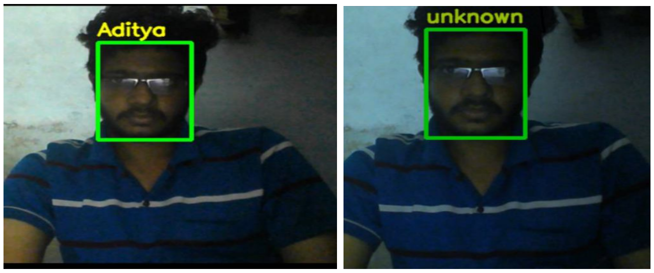

Figure 6(a) : Valid User, **Figure 6(b):** Invalid User (removed face data for demonstration purpose

6. CONCLUSION & FUTURE WORK

In this paper, we developed a robust, reliable, power, space efficient system that can be used to unlock the door using modern technologies. Users can use either their face or fingerprint to unlock the door just as they unlock their mobile. They can get alerts in the form of email, or through the 'Pushbullet' application whenever there is a possibly of intrusion into the house. They can train the model with the images of all the trusted users and add their names to the directory where their images are stored. Using the images of the intruders or thieves stored in the cloud, they can report to police. They can also register their fingerprints and can unlock the door using it whenever there is no sufficient light to unlock the door using their face. Therefore, users can use the system to get an efficient, seamless way of unlocking their house door.

The current system is developed using raspberry pi which has its own computation limitations. It currently supports only 1-2 FPS of video processing. Using more powerful algorithms can increase it to 24-30 FPS. A mobile application can be developed through which users can directly register their faces into the system. They can ever unlock the door using the mobile camera instead of USB camera. The user can remotely send the command to the system through a mobile application to unlock the door for a trusted user whose face is not registered in the system. The device can be paired with a CCTV module to enhance the security.

ACKNOWLEDGEMENT

We would like to express our gratitude towards Vasavi college of Engineering (A), Hyderabad for their guidance, constant supervision and support in completing this endeavor. We also thank the management of Vasavi College of Engineering (Autonomous), Hyderabad, India, for funding for the publication of this paper.

REFERENCES

1. Rajeev Thaware (2018), Real-Time Face Detection and Recognition with SVM and HOG Features.
2. Kushwanth Sehra, Ankit Rajpal, Anurag Mishra (2019), HOG Based Facial Recognition Approach Using Viola Jones Algorithm and Extreme Learning Machine.
3. Adrian Rosebrock (2018), Raspberry Pi Face Recognition- pyimagesearch.
4. Pavan Deligence (2017), https://github.com/dcconn/Intruder-detector-with-Raspberry-Pi-and-Pushbullet.
5. Ravi (2018), Raspberry Pi Ultrasonic Sensor HC-SR04 Interface Tutorial.
6. Pradeep Singh (2017), Send Email from Raspberry Pi using Python Script and Gmail SMTP.
7. Janina Ander (2017), RaspiReader: build your own fingerprint reader.

8. Engineering and Deploying a Cheap Recognition Security System on a Raspberry Pi Platform for a rural Settlement, Volume 8, No.6, IJATCSE November – December 2019, http://www.warse.org/IJATCSE/static/pdf/file/ijatcse36862019.pdf
9. A New Frame Work for Content Based Image Retrieval Based on Rule Based Motifs on Full Texton Images, IJATCSE, Volume 8, No.4, July- August 2019. https://doi.org/10.30534/ijatcse/2019/15842019