International Journal of Trend in Research and Development, Volume 5(3), ISSN: 2394-9333
www.ijtrd.com

IoT Based Automatic Humanoid Detective System Using Modified HAAR Classifier

[1]Dr. Shaik Akbar, [2]N. Jhansi Rani, [3]S. Divya, [4]P.D.S.L.Pravallika and [5]P. Sravya,
[1]Professor, [2,3,4,5]Student,
[1,2,3,4,5]Department of CSE, Potti Sriramulu Chalavadi Mallikarjunarao College of Engineering and Technology, Vijayawada, Andhra Pradesh, India

Abstract- Nowadays, the number of thefts and identity fraud has become a major problem. To simply convert this normal door lock into a smart lock system, by connecting the normal door to a face recognition system. Mainly, it is useful to detect whether the person is belong to the same organization or not. If any new people came to the door to enter inside into it, then the doors will not be opened for them. Most doors are controlled by persons with the utilization of keys, security cards, password or pattern to open the door. The aim of this project is to avail users for enhancement of the door security of sensitive locations by utilizing face detection and identification.

Keywords- *Face recognition, smart lock, and utilization of keys, security cards, password or pattern, enhancement of the door security, sensitive locations.*

I. INTRODUCTION

In 1960,'s the semi-automated system for facial recognition to locate the features such as face, eyes, nose, mouth on the photographs. In 1970's, Goldstein and Harmon used 21 specific subjective markers such as hair color and lip thickness to automate the recognition. In 1988, Kirby and Sirovich used standard linear algebra technique, to the face recognition. Nowadays, automatic personal identification in access control has propagate by utilizing biometrics data instead of utilizing cards, passwords or pattern. Most of the biometrics data have to be collected by utilizing special hardware such as palm print scanner, DNA analyzer. Enhancement of security by using surveillance cameras in association with face recognition system. The main aim of the project is to provide security in the where it security problems arise.

This paper describes about the implementation and deployment of face recognition system. By using this safe &secure face recognition automatic door system, we restrict people who are unauthorized and allow people who are authorized means i.e, whitelisted there image is in the database. The whole control is in the hand of admin and the admin remotely monitor the visitors. If the image is not in database their image is send to the controller through email attachment and the admin see the image later he wants to allow the person through IOT he will allow the person. By using the App he will allow the person by clicking allow button. After allowing within specified time the door automatically locked again the whole process continues. The technique for detection is HAAR classifier and recognition is LBPH.

II. EXISTING SYSTEM

Facial recognition technology is a fairly new way of identify people who could be dangerous or need to be located. It works by picking faces obtaining the measurements necessary and comparing it to the images already in its database. The latest facial recognition systems are self-contained units that attach directly to the network. These IP Facial readers are very easy to install. Facial recognition readers connect to the network and identify a person's face from a template that has previously been recorded. These integrated units contain all the intelligence, allowing enrolment as well as door control.

"It's a prototype that identifies the visitor." If the door recognizes the visitor, and the door will be unlocked and opened.

"If it doesn't recognize the visitor", it notifies the person that they are not recognized and keeps the door locked.

III. PROPOSED SYSTEM

It almost work like existing system, it has some limitations. It will overcome those limitations.

- When any new people came to the door, their image will be automatically captured and then send to the administrator through IOT and save the image in file.
- Another authenticate system is there, if any authenticated person, who are wearing a mask or their face is covered with hair for those people login id and password is there.
- If two or more people came to the door for them only authenticated person will be allowed, others are not allowed (the door will be locked automatically).

IV. IMPLEMENTATION

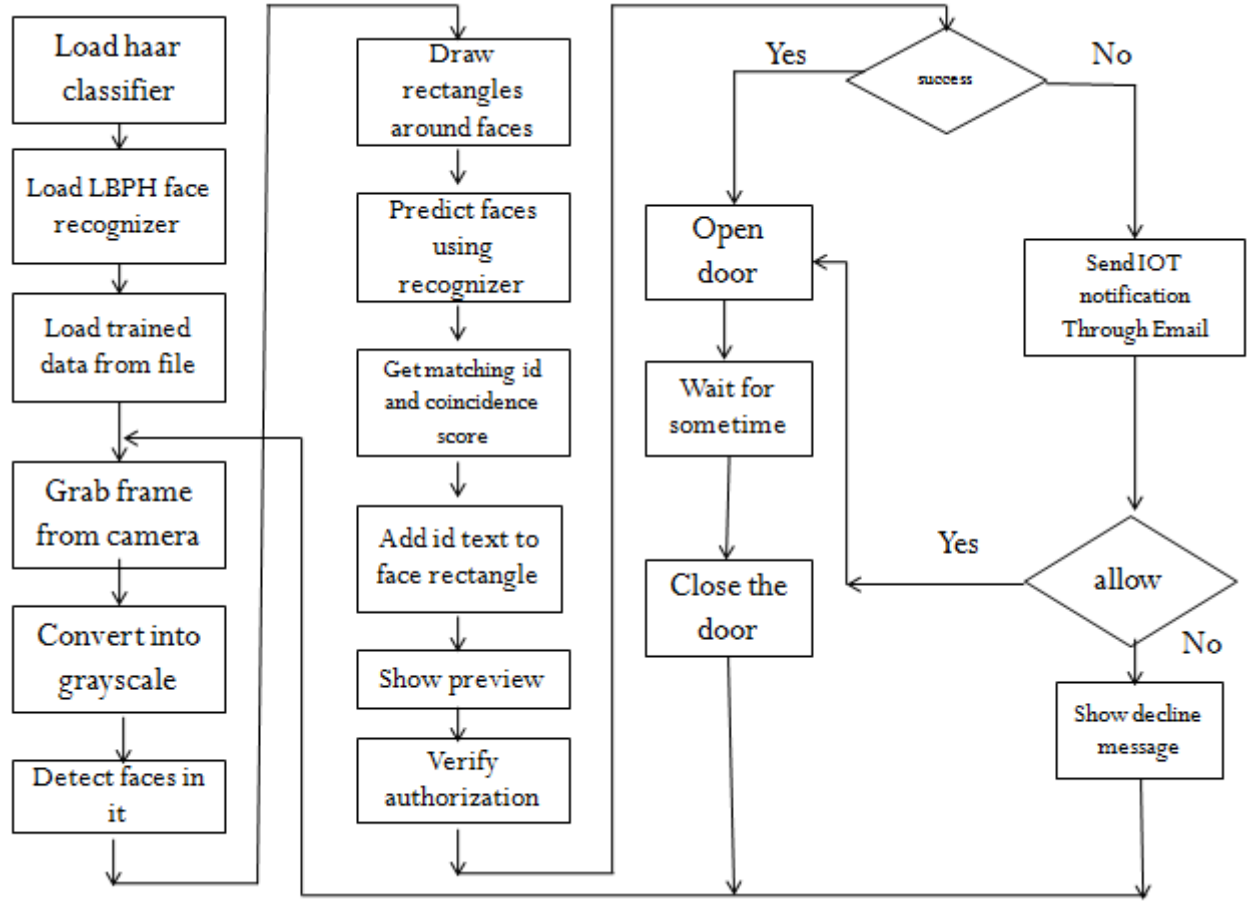
The flowchart of face captures and recognition process, at initial stage the authorized person comes in front of camera. The camera module will capture the face image with current poses. The captured face of current poses creates a data base of the authorized person and stores this. At the next time camera module will capture the current live face of the person. All this process is done in Raspberry pi module. When comparison done successfully the Relay switch is ON to unlock the door otherwise Raspberry pi module will capture an image once again through the camera and process is repeat Raspberry pi will send a command to the Mobile device send a message to the Authorized person is "FACE MATCHED" when comparison is done successfully otherwise send security alert "Unknown person will try to unlock the door".

IV. METHODOLOGY

A. Face Detection

HAAR Classifier:

This protest location system is to give focused question identification rates progressively like discovery of appearances in a picture. A human can do this effectively, however a PC needs exact guidelines and imperatives. To make the errand more reasonable, Viola– Jones requires full view frontal upright appearances. In this way with a specific end goal to be recognized, the whole face must point towards the camera and



cought not be tilted to either side. While it appears these limitations could reduce the calculation's utility to some degree, in light of the fact that the discovery step is regularly trailed by an acknowledgment venture, practically speaking these cutoff points on posture are very adequate. The qualities of Viola– Jones calculation which make it a decent recognition calculation are:

a) Robust – high identification rate (genuine positive rate) and low false-positive rate dependably.

b) Real time – For useful applications no less than 2 outlines for each second should be handled.

c) Face location just (not acknowledgment) - The objective is to recognize faces from non-faces (discovery is the initial phase in the acknowledgment procedure).

This calculation incorporates HAAR include choice process. Every human face share some comparative properties. These regularities might be coordinated utilizing HAAR Features. A couple of properties basic to human appearances:

a) The eye district is darker than the upper-cheeks.

b) The nose connect district is brighter than the eyes.

Synthesis of properties framing matchable facial highlights:

A) Location and size: eyes, mouth, extension of nose

B) Value: arranged inclinations of pixel forces

B. Face Recognition

Local Binary Patterns (LBP) is a type of visual descriptor used for classification in computer vision. LBP was first described in 1994 and has since been found to be a powerful feature for texture classification. It has further been determined that when LBP is combined with the Histogram of oriented gradients (HOG) descriptor, it improves the detection performance considerably on some datasets.

As LBP is a visual descriptor it can also be used for face recognition tasks, as can be seen in the following Step-by-Step explanation.

Step-by-Step

In this section, it is shown a step-by-step explanation of the LBPH algorithm:

1. First of all, we need to define the parameters (radius, neighbours, grid x and grid y) using the Parameters structure from the LBPH package. Then we need to call the Init function passing the structure with the parameters. If we not set the parameters, it will use the default parameters as explained in the Parameters section.

2. Secondly, we need to train the algorithm. To do that we just need to call the Train function passing a slice of images and a slice of labels by parameter. All images must have the same size. The labels are used as IDs for the images, so if you have more than one image of the same texture/subject, the labels should be the same.

3. The Train function will first check if all images have the same size. If at least one image has not the same size, the Train function will return an error and the algorithm will not be trained.

4. Then, the Train function will apply the basic LBP operation by changing each pixel based on its neighbors using a default radius defined by the user. The basic LBP operation can be seen in the following image (using 8 neighbors and radius equal to.

5. After applying the LBP operation we extract the histograms of each image based on the number of grids (X and Y) passed by parameter. After extracting the histogram of each region, we concatenate all histograms and create a new one which will be used to represent the image.

6. The images, labels, and histograms are stored in a data structure so we can compare all of it to a new image in the Predict function.

7. Now, the algorithm is already trained and we can predict a new image.

8. To predict a new image we just need to call the Predict function passing the image as parameter. The Predict function will extract the histogram from the new image, compare it to the histograms stored in the data structure and return the label and distance corresponding to the closest histogram if no error has occurred. Note: It uses the euclidean distance metric as the default metric to compare the histograms. The closer to zero is the distance, the greater is the confidence.

VI. ALGORITHM

Step-1: Initialize camera to discard empty frames camini() database creation and training using train().
Step-2: Take frames from the camera cam.read()
Step-3: Convert color frame to grayscale gray=cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
Step-4: Detect faces in it using HAAR classifier (object detection) or detect objects in video stream
cascadeClassifier()
detectMultiscale();
Step-5: Draw rectangles around faces.
rectangle()
Step-6: Predict faces using recognizer.
predict()
createLBPHFaceRecognizer()
Step-7: Get matching id and confidence score.
Step-8: Add id text to face rectangle.
Step-9: Show preview or display on image.
imshow()
Step-10: Based on confidence score the lock is opened to authenticated persons.
Step-11: If authentication is failed or confidence score is not matched it sends alert to email of the admin through IoT.
IoT.connect()
Iot.addAsset()
IoT.Subscibe()
Sendmail() using SMTP Protocol

VII. RESULTS

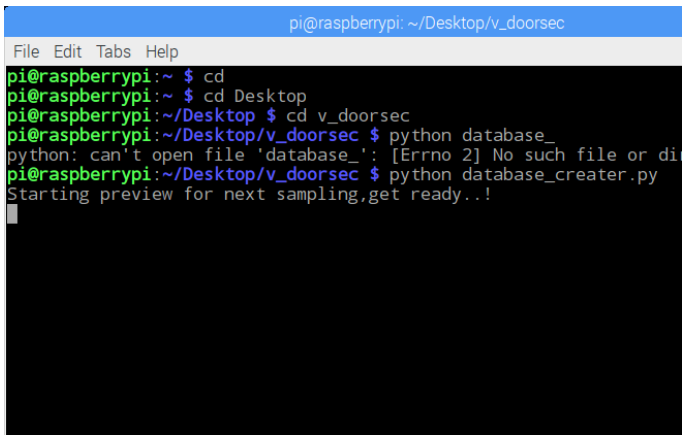


Fig.1: Storing the images into the database

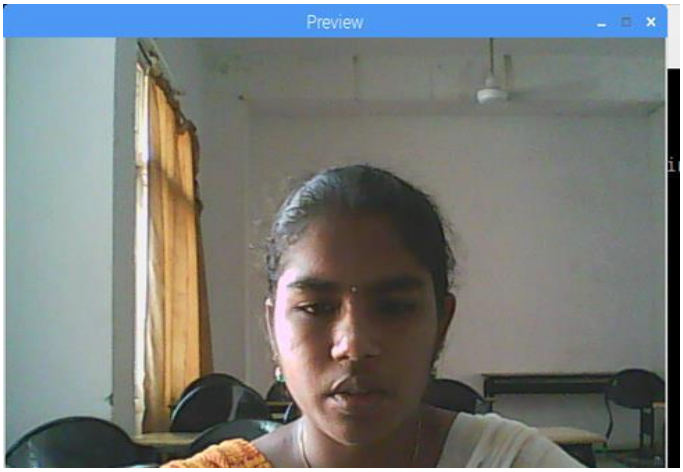


Fig.2: Get ready for capturing the image into database (preview)

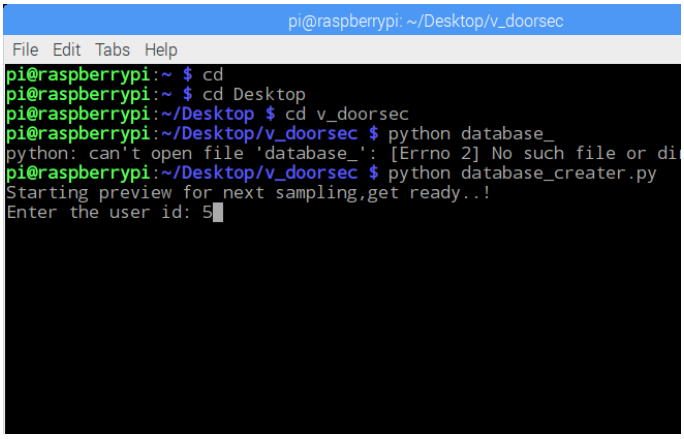


Fig.3: Giving id for image

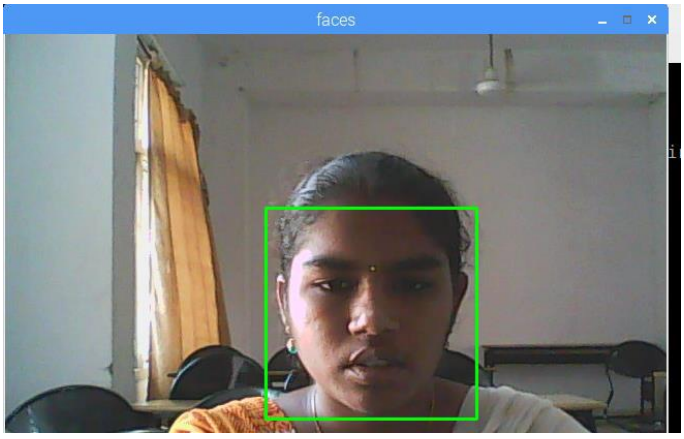


Fig.4: Sampling faces

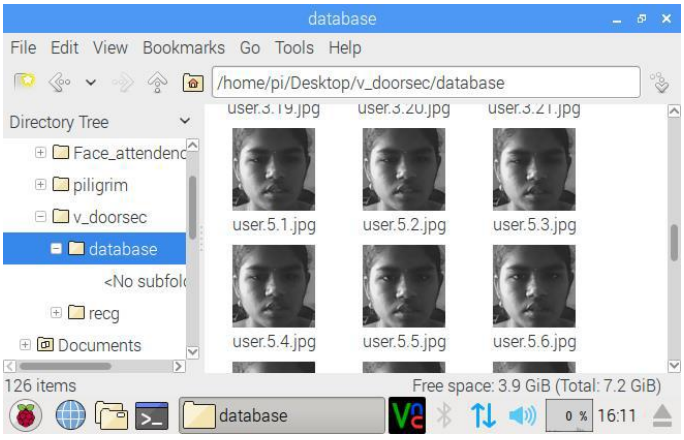


Fig.5: Sample images in database

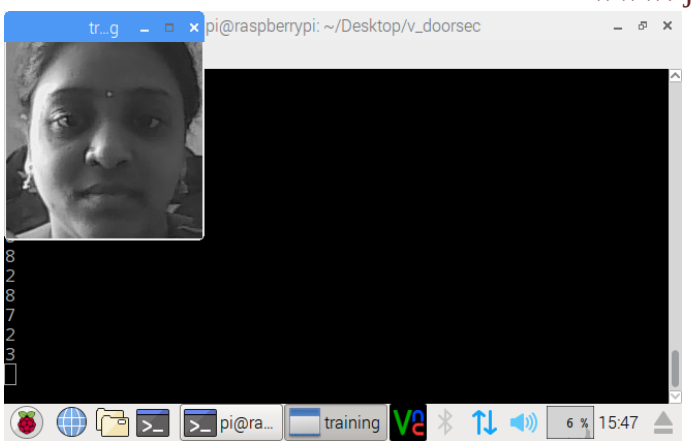


Fig.6: Training images in database

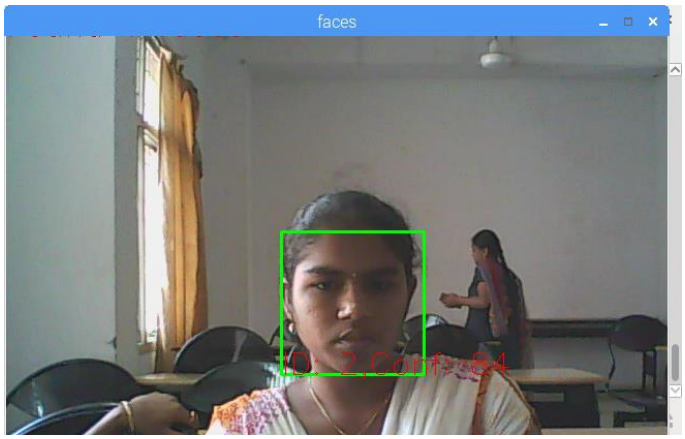


Fig.7: Testing the image in database

Fig.8: Image is in database the door is opened

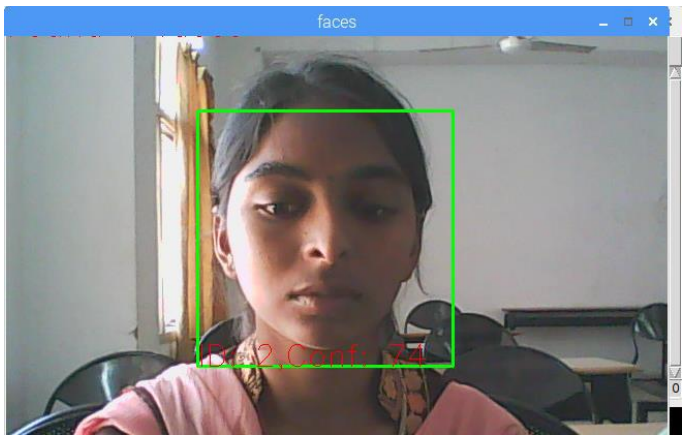


Fig.9: New person try to enter into the door

Fig.10: Door was closed

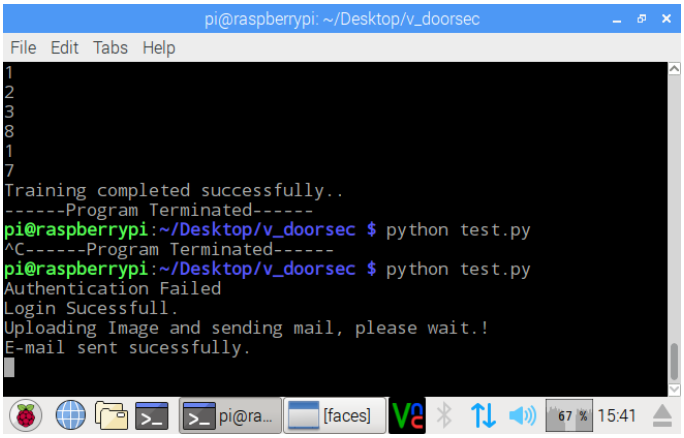


Fig.11: Image was not found in database so Image is sent to email.

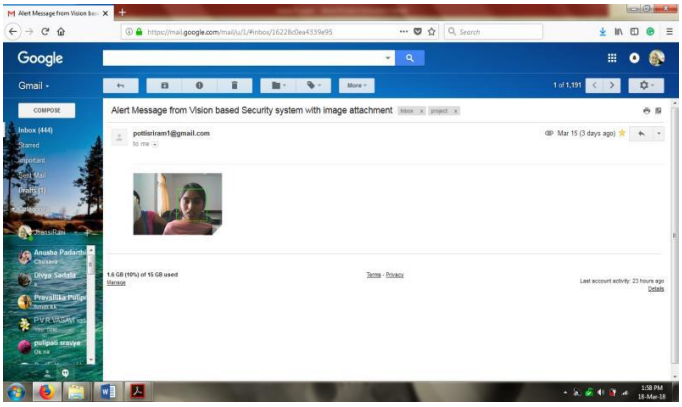


Fig.12: Alert message to mail

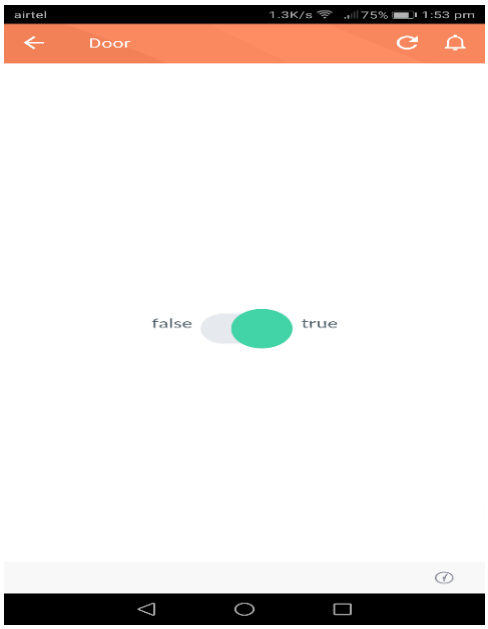


Fig.13: Closing the door using IoT

CONCLUSION

The outline of the face acknowledgment framework utilizing Raspberry pi can make the littler, lighter and with bring down power utilization, so it is more helpful than the PC-based face acknowledgment framework. As a result of the open source code, it is more liberated to do programming advancement on Windows.

We utilize LBPH+HAAR calculation for the face recognition and face detection. Additionally send a security ready message to the approved individual. A face location framework utilizing Raspberry Pi was created. The framework was customized utilizing Python programming dialect. Both Real time confront identification and face recognition from particular pictures, i.e. question acknowledgment, was completed. The proficiency of the framework was broke down as far as face recognition rate. The investigation uncovered that the present framework indicates brilliant execution productivity and can be utilized for confront recognition even from low quality pictures.

FUTURE SCOPE

Utilizing raspberry pi the present undertaking can be adjusted by an Infrared camera interfacing it can be utilized as a part of Smart Surveillance Monitoring security framework which any kind of open security is utilizing Living body location or spying, Also it can be utilized as a part of Attendance arrangement of the class, Also some significant applications can be executed utilizing interfacing of Raspberry pi and Arduino UNO board like sensor use of smartcard swapping, finger recognition, liquor identification, agribusiness stickiness detecting, Temperature detecting utilizing web server, and some more. New investigations are being made to enable pictures to be prepared on the GPU of the Raspberry Pi, accomplishing better outcomes with the utilization of particular libraries.

References

[1] Hteik Htar Lwin, Aung Soe Khaing, Hla Myo Tun, “Automatic Door Access System Using Face Recognition”, International Journal of Scientific & Technology Research Volume 4, Issue 06, June 2015.

[2] F. Zuo, and P. H. N. de With, Real-time embedded face recognition for smart home, IEEE Trans. Consumer Electron., vol. 51, no. 1, pp.183-190, Feb. 2005.

[3] Jie-Ci Yang et. all An Intelligent Automated Door Control System Based on a Smart Camera.

[4] S. Nazem Basha et all An Intelligent Door System using Raspberry Pi and Amazon Web Services IoT