Face Recognition Enabled Door Access Control System

*Oluyemi E. Adetoyi and Boluwatife P. Awe
Department of Electrical and Electronics Engineering, University of Ibadan, Ibadan, Nigeria
oe.adetoyi@ui.edu.ng | awepius62@gmail.com

ORIGINAL RESEARCH ARTICLE
Received: 07-JUN-2021; Reviewed: 27-JUN-2021; Accepted: 19-JAN-2022
http://dx.doi.org/10.46792/fuoyejet.v7i1.656

Abstract- Face recognition has found usage in many applications from the simplest systems to the more complex systems. The years of researches in this field has witness improvements in detection accuracy. However, few studies that incorporate face recognition for access control are suitable for restricted areas. This work aims at using face recognition for access control systems using Haar cascade feature descriptor and LBPH as classifier algorithm. The system was implemented on raspberry pi 3- model B board, which consists of a solenoid lock that is activated to grant access to the user when a matching face is detected by the classifier algorithm. In the event when there is no match between the detected face and the database facial images, a red light comes on and the doorbell rang. The accuracy, sensitivity, specificity, and precision of the LBPH algorithm are respectively 96%, 97.5%, 90.5%, and 97.5%. The delay in the processing of signals to activate the door lock and doorbell is not more than 4 seconds. Thus, the system is effective as a real-time access control mechanism.

Keywords- Access control, Computer vision, Facial recognition, LBPH, OpenCV.

1 Introduction

With the advancement in biometrics technology and the rapid evolution in smart cities, there has been a corresponding need for efficient access control systems for homes and offices. In the office environment, it may be necessary to control which employee has access to which place or prevent non-employee from accessing a place due to operational demands. In the home situation, homeowners may want to admit visitors or domestic workers after being duly certified as the claimed person or identified as an authorized person as part of measures to curb rising insecurities.

Face recognition is an aspect of computer vision, which deals with the identification or verification of a face with an extensive study on improving its accuracy. A closely related field is facial emotion recognition, whereby the execution of a specific task is based on the detected emotion. Some of the studies on detection and recognition algorithm development can be found in (Viola & Jones, 2001; Chaaraoui, Climent-Perez & Florez-Revuelta, 2012; Padill-Lopez, Chaaraoui & Florez-Revuelta, 2015; Zhiguo & Cheng, 2020; Nuhu et al., 2021). Face recognition is also finding application in surveillance systems due to its efficiency. It can be implemented to alert in case of unauthorized access to a location or detection of wanted criminals or impersonation detection. This paper presents a low-computation and efficient face recognition access-controlled system, which is suitable for real-time operation.

*Corresponding Author

Section B- ELECTRICAL/ COMPUTER ENGINEERING & RELATED SCIENCES
Can be cited as:
Adetoyi O.E. and Awe B.P. (2022): Face Recognition Enabled Door Access Control System, FUOYE Journal of Engineering and Technology (FUOYEJET), 7(1), 28-31. http://dx.doi.org/10.46792/fuoyejet.v7i1.656

2 Related Works

A dash-bell system for home use was presented by Quadros et al. (2017). A WIFI-enabled Amazon dash button was connected to a network, to enable use of a smartphone to answer the bell triggered by a dash button. The feature of the dash button that allows customers to order frequently used daily items was explored to configure the doorbell. The dash-bell enables the homeowner to see the pictures of visitors and remotely ascertain their identity. It also offers the homeowner the ability to reject or accept a request anywhere when connected to the internet. The requirement of transmitting captured images to the cloud and notification of home users via mobile app will result in a long delay to the visitor. The proposed design eliminates the use of the Internet, which can pose a problem when there is poor Internet connectivity. It also circumvents the problem of unacceptable delay, since it is not required to transmit captured images before access is granted.

Sajjad et al., (2020) in their work, presented an assisted face recognition system for law enforcement services in smart cities. The system was implemented on Raspberry pi and Viola-Jones algorithm was used for face detection. A fast binary descriptor known as Binary Robust Independent Elementary Features (BRIEF), which is invariant with rotation was then used to extract points from the detected face. The design incorporates a Support Vector Machine (SVM) to train the recognizer in the cloud and categorize faces into their classes. The system provides saving in transmission energy and bandwidth since only the extracted features are transmitted as against the entire face. However, transmission to the cloud also creates a delay for the system. The use of ORB for feature selection, which is a combination of two algorithms can also increase the delay as compared to the use of Adaboost and cascade structure of Haar classifier that speed of selection of a small number of important features in the proposed design.

A smart home security system using face recognition was the subject of Pawar et al., (2018). The system makes use of Passive Infrared (PIR) to detect human presence and an ultrasonic sensor to estimate the human distance from the camera. If the distance is appropriate, the camera captures the image and compares it with the database, if a match is found, the door will be opened. If the image does not match database images, a red light comes on and the doorbell rang if the owner is at home; otherwise, SMS or Email will be sent to the owner. In case there is a break-in, an alarm will be generated. The Local Binary Pattern (LBP) algorithm was used for face match. The drawbacks of the system are that face detection is dependent on the subject's proper positioning. Also, a huge quantity of points is required to perform matching compared to a few important features obtained with the use of Adaboost.

Another facial recognition security system based on IoT was presented in Balla and Jadhao, (2018). The system captures the image of the visitor when the doorbell is pressed. The face feature is extracted and compared to the database, if there is a face match, the homeowner is notified via mail, if not the face is registered as an unknown face. A response is sent back from the homeowner to the system to grant access by opening the door or to decline the access. The major disadvantage is that the use of mail will introduce long delays, which will make real-time applications impossible. Thus, the decision is taken at the recognizer algorithm level in the proposed design, to prevent such delay.

Automated access control using face recognition was developed in Rameswari et al., (2020). An infrared sensor was used to detect motion, which activates the camera action for image capturing. Face encoding was then used to find distances between eyes, colour, edges, and background. The value of the encodings was assigned label and stored as an array. Features were extracted using Histogram Object Gradient (HOG). FaceNet algorithm, which maps each face image into Euclidean space such that distance in that space corresponds to face similarity was used for face verification. Support Vector Machine was further used to classify the face. Then the verified image is sent to a webpage where access can be granted or denied. The disadvantage of the system is that the computation overhead for feature selection is high as compared to Adaboost, which is being proposed. The use of SVM makes it complex and expensive to process large datasets on smart devices like Raspberry pi that was used in the proposed design.

3 Methodology

3.1 Design Concept

The goal is to develop a low computational yet efficient face recognition system for access control. The low computation requirement of the algorithm will facilitate facial recognition in real-time as needed by access control applications. The efficiency aspect will reduce to the barest minimum, the occurrence of missed detection or false detection, which is characteristic of biometrics. Based on these conditions, the Local Binary Pattern Histogram (LBPH) algorithm was used for facial recognition. This was implemented in the OpenCV environment. The system was designed in such a way that when an authorized face is detected, access was granted and the doorbell is rung, otherwise access was denied and the buzzer sounds. The system is divided into three major parts; the processing unit subsystem, face data acquisition, and recognition subsystem, and door activation subsystem. The schematic diagram and flowchart of the system are respectively shown in Figures 1 and 2.

3.2 The Processing Unit Subsystem

Raspberry pi 3- model B board serves as the central processing unit for the system. The Raspbian Buster operating system was used and was written on the SD card using the "balenaEtcher" application. The setting up of the Raspberry Pi for usage was done using the "puTTY" and "Angry IP Scanner" applications. Subsequent reconfiguration of the Raspberry Pi can be accomplished by wireless connection to Virtual Network Computing (VNC) interface that is residing on a laptop or a mobile device, thus making the system portable. The VNC is more user-friendly than puTTY.

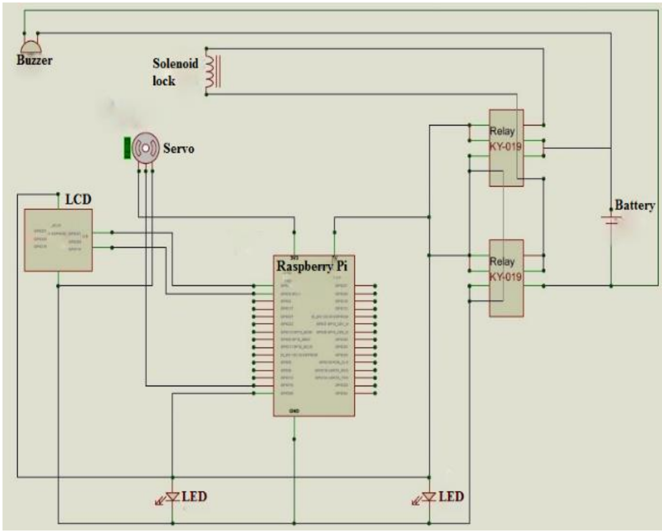

Fig. 1: The system circuit diagram

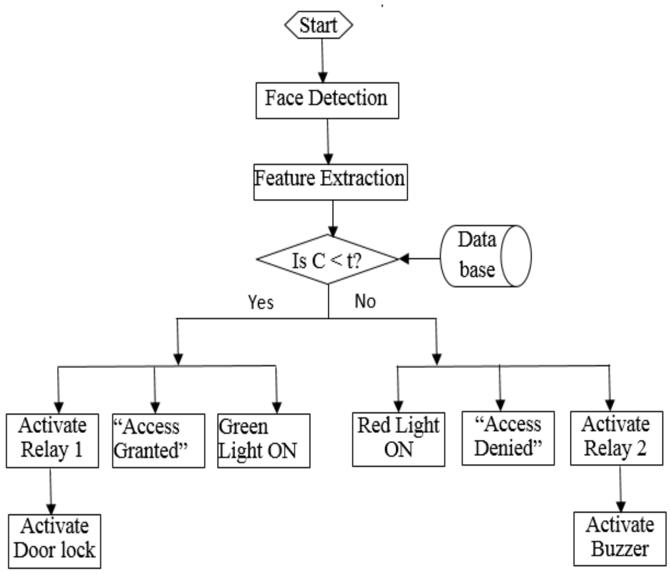

Fig. 2: Flowchart for the system

http://dx.doi.org/10.46792/fuoyejet.v7i1.656 http://journal.engineering.fuoye.edu.ng/

3.3 Face Image Acquisition

The data of authorized users' faces to access the system was acquired using Pi NOIR camera, whose precise angular position was achieved by the servomotor. Five sample faces of twenty users were collected and stored in the database for the face recognition process. The face data are acquired under different lighting conditions, moods, with or without glasses, such that the algorithm's recognition accuracy can be improved. The choice of the camera is influenced by its ability to compensate for illumination problems in a low illumination environment. The camera object of the Raspberry Pi was initialized to allow access to the camera, the resolution was set at (480, 320) and the frame rate at 30fps.

3.4 Facial Features Extraction

The Haar-cascade classifier algorithm was employed to detect the face in the captured image and store it in a database during the enrolment phase or perform a 1 x M comparison of the image with the M-images in the database during the recognition phase. Object detection using Haar feature-based cascade classifiers is a visual object detection framework proposed by Paul Viola and Michael Jones (Jones and Viola, 2001; Viola and Jones, 2001). It is capable of processing images rapidly to achieve high detection rates. The quick computation of the features required by the detector is made possible by integral representation of the images. While the use of AdaBoost based algorithm ensures a selection of a small number of important visual features that yield efficient classifiers. The method of combining classifiers in a cascade allows for quick discard of the image background and concentrating computation on object regions. The OpenCV implementation of Haar-cascade feature descriptor for the frontal face was used.

Fig. 3: Pre-processed face images of four subject

3.5 Recognition Subsystem

After the faces have been enrolled, the next step carried out is the training of the LBPH recognizer algorithm with 70% of the faces to be recognized. The LBPH is a texture-based classifier, which find local features of an image by comparing the intensities of the centre pixel with its neighbouring pixels of usually not more than eight. Each neighbour with an intensity value greater than the centre pixel is assigned one, otherwise zero will be assigned. The obtained binary code is converted into decimal, and the process is repeated for each pixel. A local histogram of the binary patterns was thus obtained to perform face recognition. The LBPH classifier was implemented in the OpenCV environment using Python language.

In the final process, the recognition of pre-trained and non-trained faces was carried out. The remaining 30% of test data was run on the algorithm. This is done to determine who should be granted access to the system when the subject is in the camera view field. The recognition aspect is a very important aspect of the system and it has to be done with a high level of precision. Hence, sufficient data was used to train the algorithm to prevent false negatives, which can lead to denial of an authorized user in the facial recognition process or false positives that will permit entry of unauthorized users. Subsequent faces positioned in the view area of the camera will be captured and the recognizer algorithm will compare the new face features with that in the database and decide whether the face has authorized access or not. The LBPH recognizer algorithm will then make a prediction returning subject id and an index showing the confidence level as well.

3.6 Door and Buzzer Activation Subsystem

This aspect consists of the sending of signals by the processor and the door opening mechanism. The sending of signals is done via the GPIO pins of the processor. The used GPIO pins are 19, 26, 5V, 3V, SDA, SLC, and ground. The 5V, SDA, SLC, and ground pins are used for the LCD. The 3V, 19, and ground pins are used for the servomotor. The 5V, 19, and ground are used for relay 1 while the 5V, 26, and ground are used for relay 2.

In the instance of a match between an input face image and a database image, the GPIO 19 pin will be set HIGH, thereby energizing relay 1 that operates the solenoid to unlock the door. In addition, the message "Welcome <user_id>" was displayed on the screen, as the green light indicator turns on. If the image comparison is false, which means the detected face in the view area does not match any image in the database; then the GPIO 26 is set to HIGH to activate LCD to display an "Unknown user" message, while relay 2 is energized to turn on the buzzer and the red-light indicator.

4 Results and Discussion

The access control system of Figure 1 was implemented on a PCB board and the confidence level of the LBPH algorithm was set at 90 because an accurate facial match is important. The confusion matrix of the algorithm thus obtained, is presented in Table 1. The confusion matrix describes the performance of the classifier on the test set of 100 faces whose true values are known are compared to the database. From the confusion matrix, the performance metrics of the LBPH are measured. The accuracy of making correct predictions by the LBPH algorithm was obtained thus:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} = 96\% \quad (1)$$

http://dx.doi.org/10.46792/fuoyejet.v7i1.656 http://journal.engineering.fuoye.edu.ng/

where TP is a true positive, TN is a true negative, FP is a false positive and FN is a false negative. The sensitivity measure of how good the classifier is, in detecting positive events was measured as:

$$Sensistivity = \frac{TP}{TP+FN} = 97.5\% \quad (2)$$

While the specificity measure of detecting unauthorized users was obtained as follows:

$$Specificity = \frac{TN}{TN+FP} = 90.5\% \quad (3)$$

and the precision of the algorithms at recognizing authorized users was measured as:

$$Precision = \frac{TP}{TP+FP} = 97.5\% \quad (4)$$

The average delay in activating the devices is shown in Table 2.

Table 1. Confusion Matrix of 100 faces recognition

		ACTUAL TRAINED FACES	
		True	False
PREDICTED FACES	Positive	77	2
	Negative	19	2

Table 2. Average time delay of devices' operation

Components	Time delay(s)
Servomotor	3
Light indicator	4
LCD	2
Solenoid	4
Doorbell	4

5 Conclusion

The proposed solution for access control based on facial recognition yields a good result. However. the distance of the face from the camera has a great effect on the performance of the system. The farther the distance, the less accurate the system is, if the face is also too close, the less accurate the system becomes. An approximate face to camera distance of 15cm was used. The number of datasets used for training influences the performance of the system as well. It is recommended that the number of datasets for face training should be large to improve system performance. Furthermore, the negative dataset should be made much larger than the positive dataset.

References

Balla, P. B., & Jadhao, K. T. (2018). IoT Based Facial Recognition Security System. International Conference on Smart City and Emerging Technology (ICSCET), 1–4. https://doi.org/10.1109/ICSCET.2018.8537344

Chaaraoui, A. A., Climent-Perez, P., & Florez-Revuelta, F. (2012). A Review on Vision Techniques Applied to Human Behaviour Analysis for Ambient-Assisted Living. Expert Systems with Applications, 39, 10873–10888.

Nuhu, A. S., Akut, E. K., Cinfwat, K. Z., Julius, P. N., Imam, M. L., Momoh, S. I., Felix, E. I., & Dajab, D. D. (2021). Facial Emotion Recognition with Sparse Coding Descriptor. FUOYE Journal of Engineering and Technology, 6(2), 53–57. https://doi.org/10.46792/fuoyejet.v6i2.642

Padill-Lopez, J. R., Chaaraoui, A. A., & Florez-Revuelta. (2015). Visual Privacy Protection Methods: A Survey. Expert Systems with Applications, 42(9), 4177–4195.

Pawar, S., Kithani, V., Ahuja, S., & Sahu, S. (2018). Smart Home Security Using IoT and Face Recognition. International Conference on Computing, Communication Control and Automation, ICCUBEA Proceedings, 1–6. https://doi.org/10.1109/ICCUBEA.2018.8697695

Quadros, B., Kadam, R., Saxena, K., Shen, W., & Kobsa, A. (2017). Dashbell: A Low-cost Smart Doorbell System for Home Use. Arxiv, abs/1706.0, 1–4.

Rameswari, R., Naveen Kumar, S., Abishek Aananth, M., & Deepak, C. (2021). Automated Access Control System Using Face Recognition. Materials Today: Proceedings, 45(2), 1251–1256. https://doi.org/10.1016/j.matpr.2020.04.664

Sajjad, M., Nasir, M., Muhammad, K., Khan, S., Jan, Z., Sangaiah, A. K., Elhoseny, M., & Baik, S. W. (2020). Raspberry Pi Assisted Face Recognition Framework for Enhanced Law-Enforcement Services in Smart Cities. Future Generation Computer Science, 108, 995–1007.

Viola, P., & Jones, M. (2004). Robust Real-time Face Detection. International Journal of Computer Vision, 57(2), 137–154. https://doi.org/10.1023/B:VISI.0000013087.49260.fb

Viola, P., & Jones, M. (2001). Rapid Object Detection Using a Boosted Cascade of Simple Features. Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. CVPR 2001, 1–9. https://doi.org/10.1109/CVPR.2001.990517

Zhiguo, Z., & Cheng, Y. (2020). Application of Attitude Tracking Algorithm for Face Recognition Based on OpenCV in the Intelligent Door Lock. Computer Communications, 154, 390–397.