

# Development of a secured room access system based on face recognition using Raspberry Pi and Android based smartphone

Asep Najmurokhman<sup>1,\*</sup>, Kusnandar Kusnandar<sup>1</sup>, Arief Budiman Krama<sup>1</sup>, Esmeralda Contessa Djama<sup>2</sup>, and Robbi Rahim<sup>3</sup>

<sup>1</sup>Universitas Jenderal Achmad Yani, Dept. of Electrical Engineering, Jl. Terusan Jend. Sudirman PO Box 148 Cimahi 40533, Indonesia

<sup>2</sup>Universitas Jenderal Achmad Yani, Dept. of Informatics, Jl. Terusan Jend. Sudirman PO Box 148 Cimahi 40533, Indonesia

<sup>3</sup>Universiti Malaysia Perlis, School of Computer and Communication Engineering, Kubang Gajah, Malaysia

**Abstract.** Security issues are an important part of everyday life. A vital link in security chain is the identification of users who will enter the room. This paper describes the prototype of a secured room access control system based on face recognition. The system comprises a webcam to detect faces and a solenoid door lock for accessing the room. Every user detected by the webcam will be checked for compatibility with the database in the system. If the user has access rights then the solenoid door lock will open and the user can enter the room. Otherwise, the data will be sent to the master user via Android-based smartphone that installed certain applications. If the user is recognized by the master user, then the solenoid door lock will be opened through the signal sent from the smartphone. However, if the user is not recognized, then the buzzer will alert. The main control circuit on this system is Raspberry pi. The software used is OpenCV Library which is useful to display and process the image produced by webcam. In this paper, we employ Haar Cascade Classifier in an image processing of user face to render the face detection with high accuracy.

## 1 Introduction

The security aspect is needed in many areas of life today. The privacy factor also influences the importance of a security system. Advances in electronics technology helped to develop a reliable security system. A vital link in security chain is the identification of users who will enter the room. This paper describes the prototype of a secured room access control system based on face recognition. Face recognition has been one of the hot fields in computer vision and biometrics, since it is a challengeable work to identify a face image with varying expression, occlusion, disguise, and illumination [1]. Along with fingerprint match and eye retina match, they become a prominent method in biometric technology [2].

The task of face recognition is to compare a query face against multiple faces in the database in order to identify whether it belongs to a person in a database [3]. In some identification applications, one needs to find the most similar face. In a more advanced applications, the requirement is not only finding the most similar faces, but also the data associated with detected person as well as the notification system in terms of showing a suspicious person. In the face recognition systems, the facial detection is an initial step to capture an image of the user to be processed. The facial detection usually uses a light proximity sensor that consists of photodiode components. However, these sensors can only detect faces horizontally to the line. For a wider view of the face image, the use of webcam can provide more capability than the proximity sensor. The proposed

system employs the webcam to capture the facial image. Then, the image will be processed further by a certain algorithm to get the best results. In the security systems, that image will be compared to the user database in the system. If the user entered the room is recognized by the system, then the door lock will switch off the door and the user can enter the room. Otherwise, the door lock stays close unless the master user makes a decision to switch on the door lock due to a certain condition. Such mechanism was made to assure that only authorized user can access the room to improve the security aspect.

The proposed system employs Raspberry Pi as the main control unit and OpenCV as an open source library for processing the image produced by webcam. Raspberry Pi is a powerful credit-card sized single board computer that can be used for many applications due to functionality, small size, and its extension to support internet-of-things based systems. Pal *et al.* [4] employed Raspberry Pi to control a conformal beam-steering antenna for optimizing the throughput in a scattered and a poor Signal to Noise Ratio (SNR) environment. Filho *et al.* [5] utilized Raspberry Pi to realize the NPi-Cluster, a low-power consumption cluster architecture with energy proportionality, capable of automatically scaling the number of running machines according to the current processing demand. Pasolini *et al.* [6] developed a Raspberry Pi-based platform for signal processing education. In face recognition, Gupta *et al.* [7] explored a feasibility of implementing Raspberry Pi based face recognition system using conventional face detection and

\* Corresponding author: [asep.najmurokhman@lecture.unjani.ac.id](mailto:asep.najmurokhman@lecture.unjani.ac.id)

recognition techniques. The latter is in line with the proposed system described in our paper.

While OpenCV is a library of programming functions mainly aimed at real-time computer vision [8]. Initially developed by Intel, recently it becomes a platform library in image processing as it can be customized by the user. Some related works regarding the OpenCV application in image processing include Green [9], Shen *et al.* [10], Sharma and Shah [11], Mustafa and Khairul [12], and Emami and Suciu [13], for name a few. Green [9] enriched library in OpenCV to implement the median filtering for noise removal in images. Shen *et al.* [10] benchmarked the face recognition algorithm in OpenCV in order to realize the sparse representation classification for rendering face recognition accurately and efficiently on smartphones. Sharma and Shah [11] employed OpenCV library to implement a simple and a low-cost approach for automatic animal detection on highways for preventing animal-vehicle collision. Mustafa and Khairul [12] installed the OpenCV library into Raspberry Pi to identify color and size for accurate mature classification of fruits. While, Emami and Suciu [13] described facial recognition in OpenCV which uses a type of face detector called a Haar cascade classifier.

The rest of the paper is structured as follows. Section 2 describes a framework of the proposed system includes block diagram, flowchart, and schematic diagram respectively. Experimental results and discussion are given in Section 3. Finally, some concluding remarks and further recommendation for future research are summarized in Section 4.

## 2 System framework

A framework of a secured room access system is depicted in Fig. 1. When the user of the room wants to enter the room, webcam installed on the door of the room will take the user's face of the room. If the face is recognized, then Raspberry Pi will give the command via relay to open the solenoid door lock attached to the door of the room. However, if the face is not recognized, then the main controller will give the command to buzzer and make a notification and send the image of the face to Telegram installed on an android based smartphone. Telegram is a cloud-based mobile and desktop messaging application with a certain performance especially on security, speed, and connectedness to another interface. This application is very popular to enhance the communication between persons and recently between human and machine. If the face which sent to Telegram can be recognized by the master user of the room, then the door will open after the master user sent the command signal into the solenoid door lock. Once the room user enters, the solenoid door lock will automatically close the door again.

While, a flowchart adopted in the proposed system is shown in Fig.2. As shown in Fig. 2, user identification that will enter the room comprises two steps. If user is confirmed as authorized user, then solenoid door lock will switch on to let the user enters the room. Conversely, if someone is not confirmed as authorized

user then buzzer will alert. It might happen for authorized user due to lack of recognition by system in terms of incompleteness of facial detection, lesser intensity of light, and so forth. To overcome such situation, face image will be sent to master user via Telegram. Further, master user will decide to switch on or off the door lock based on recognition to face image. If it is recognized, then master user sends a signal to switch the buzzer off as well as open the door lock. Otherwise, buzzer remains alert for a while and the door lock stays in its initial state.

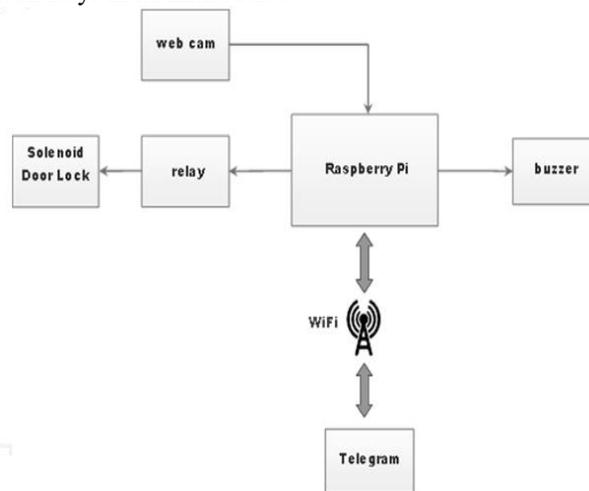


Fig. 1. System framework.

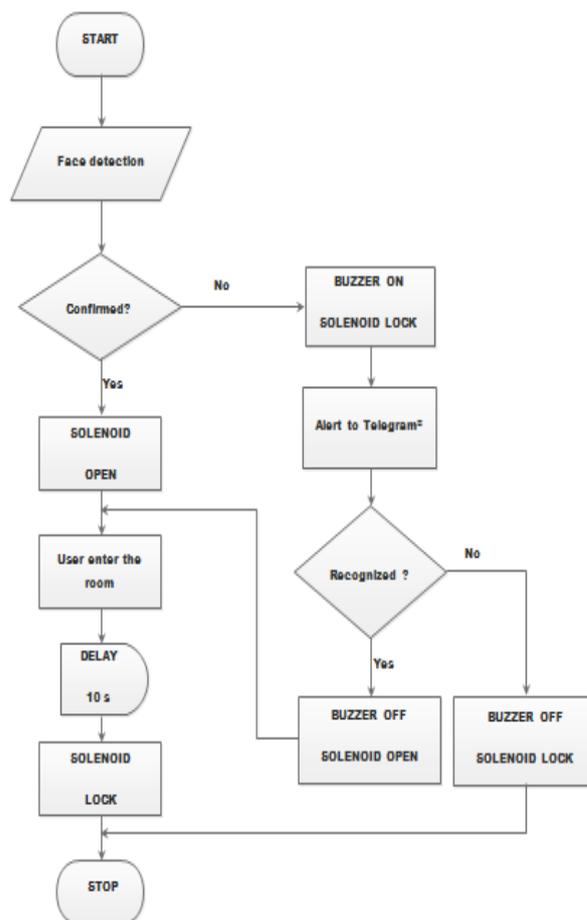
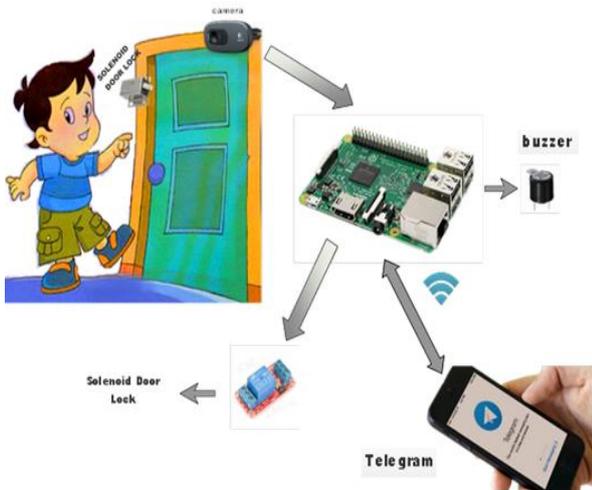


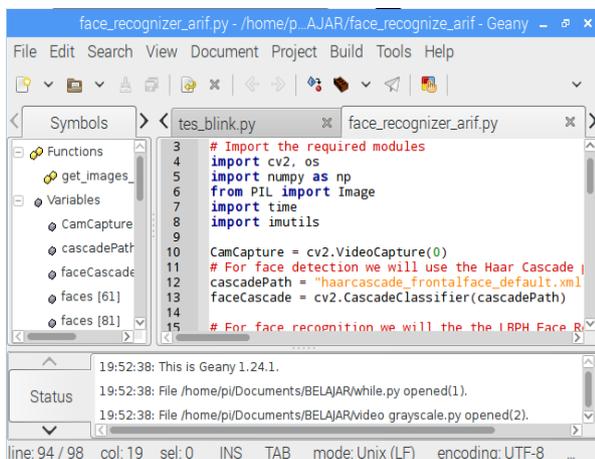
Fig. 2. Flowchart of the proposed system.

Schematic diagram of the proposed system is illustrated in Fig. 3. It comprises webcam, Raspberry Pi, solenoid door lock, and a smartphone installed Telegram application. A webcam is usually a video camera that can be used to capture, feed, and stream an image of the user entered the room. The captured facial image will be sent to Raspberry Pi to be compared with the facial image stored in the database. Raspberry Pi proceeds the facial data using algorithms that have been compiled in the OpenCV library. Facial detection method in OpenCV based on Haar cascade classifier proposed by Viola and Jones [14]. This approach extracts the image based on the features instead of pixels by pixels so that the image processing is very efficient and achieves the high detection rate.



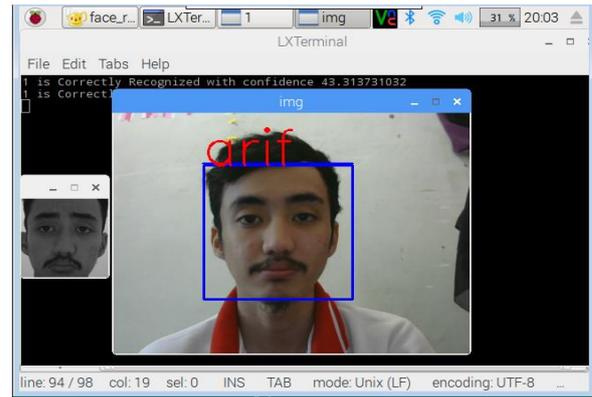
**Fig. 3.** Schematic diagram of the proposed system.

To implement the face recognition using OpenCV library installed in Raspberry Pi, the initial step is to collect and record all the image of user into a database. In this step, we capture 15 images and denote the identity of respective image. We use an editor what so called Geany Programmer's Editor to connect the recorded image with Raspberry Pi. This step is shown in Fig 4.



**Fig. 4.** Main view of Geany Programmer's Editor.

After compilation of previous step, we could get the result as shown in Fig 5.



**Fig. 5.** Captured image that was recorded and connected to Raspberry Pi.

For each user who stored in the database, we take 15 facial images respectively. Those images represent the facial expression, light condition around circumstance, larger part of facial, and so forth. Each image which related with the same user is stored in the database. It is also given an identity that will appear on the monitor along with the image.

Based on the flowchart depicted in Fig. 2, if the captured image which processed further by Raspberry Pi is conformed to the authorized user that is suitable within the database, then solenoid door lock will open the door. Otherwise, the captured image will be sent to the smartphone and verified by the master user via Telegram. Telegram is a cloud-based instant messaging and voice over IP service developed by the Russian entrepreneur Pavel Durov which has many advantages compared to other messenger services [15]. Nowadays, many applications have been developed to gain the advantages of Telegram including a monitoring of hydroponic smart farming system [16], digital forensic analysis [17], internet-of-things based application [18], and so forth. Integration between Telegram and the other hardware such as Raspberry Pi is possible due to Telegram provides bots: an automatic answering account that can respond to specific text command by giving preformatted answer [15, 19].

### 3 Results and discussion

In the experiments, we registered nine users as authorized user and their images are stored in the database. For respective users, we take 15 facial images with different pose and expression. The experiments are carried out by capturing the user with some conditions include normal, low light intensity, tilted face, and obstructed face. Normal condition means the face is straight to the camera so that the all parts of the face are captured by the camera clearly. At the second condition, the light intensity around user is less such that the image tends to be dark. Then, each user tilted their head around 15 degree to the Y-axis in the third pose. In last condition, an object was put in the front of user face and hence it causes the obstructed face. The authorized users include Arif, Jodi, Ahmad, Tiara, Tedi, Ninin, Ibu, Teh Nisa, and Teh Neng respectively.

The experimental results are tabulated in Table 1- Table 4. Table 1 shows the result of face recognition by the proposed system for normal condition. Due to clarity of the captured image, all authorized user are recognized by the proposed system as well as unauthorized user. Identity of the user can be classified exactly as it is stored in the database. When the authorized user is detected, the solenoid door lock will open. Such condition is displayed in Fig. 6.



**Fig. 6.** Solenoid door lock with open condition.

**Table 1.** The face recognition for normal condition.

No	User	Database	Captured image
1	Arif		
2	Jodi		
3	Ahmad		
4	Tiara		
5	Tedi		
6	Ninin		
7	Ibu		
8	Teh nisa		
9	Teh neng		
10	Mr X	Unauthorized user ( <i>tidak dikenal</i> )	

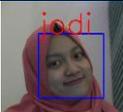
The results of second experiment are listed in Table 2. In this experiment, light intensity around the user is less. The captured images are darker than normal condition. In such cases, classifier in OpenCV is able to classify and recognize some the captured image. However, there is some false identification of the user. It could happen due to features of some captured image is no longer suitable with the related database. To alleviate the effect of illumination variation on face recognition, we could adopt a method of directional illumination estimation to extract directional illumination invariant sets from a facial image as proposed by Cheng *et al.* [20]. In that approach, the directional illumination invariant sets not only better preserve essential features of the face, but also largely reduce adverse effects of rapid light changes.

**Table 2.** The face recognition for lesser light intensity.

No	User	Database	Captured image
1	Arif		
2	Jodi		
3	Ahmad		
4	Tiara		
5	Tedi		
6	Ninin		
7	Ibu		
8	Teh nisa		
9	Teh neng		
10	Mr X	Unauthorized user ( <i>tidak dikenal</i> )	

Another experiment is undertaken by the tilted face and obstructed face. Some results are displayed in Table 3 and Table 4. Similar to previous results, Haar cascade classifier embedded in OpenCV can recognize some the captured image. The worse result is observed for obstructed face. It is quite straightforward due to incompleteness of part of user face. In that case, features of the captured images should be improved and enhanced via the advanced techniques to make the captured images such as local binary pattern described by Kasim *et al.* [21] or Fisher Liner Discriminant proposed by Rahim *et al.* [22].

**Table 3.** The face recognition for tilted face.

No	User	Database	Captured image
1	Arif		
2	Jodi		
3	Tedi		
4	Ibu		
5	Teh Nisa		

**Table 4.** The face recognition for obstructed face.

No	User	Database	Captured image
1	Arif		
2	Tiara		
3	Tedi		
4	Ibu		
5	Teh Nisa		

## 4 Concluding remarks

A secured room access system could be implemented from a combination of webcam, Raspberry Pi, relay, solenoid door lock, buzzer, and an android based smartphone installed Telegram. This system employed Haar cascade classifier method to detect and recognize a detected face from user. Experimental results show that face detection and recognition processing using Haar cascade classifier is said to be less sensitive, because it depends on the similarity, light intensity, facial angle, and completeness of the captured image. In some extent, we could conclude that Haar cascade classifier in an image processing of user face renders the face detection with high accuracy. However, we could apply some advanced techniques as described in [21-22] for further study to enhance the performance of Haar cascade classifier.

The first author thanks to LPPM Universitas Jenderal Achmad Yani who already partially supported this work in Competitive Research Scheme for fiscal year 2017. We would also like to thank all of volunteers who involve in this work.

## References

1. J. Gu, H. Hu, H. Li, *IEEE/CAA J. of Auto. Sinica* **5**, 2 (2018)
2. B. A. Patel, *R-EYE: An Image Processing-Based Embedded System for Face Detection and Tracking*, (Electrical Engineering, California State University, Long Beach, Master Thesis 2016)
3. S. Z. Li, A. K. Jain, *Handbook of Face Recognition 2nd*, (Springer Verlag, 2011)
4. A. Pal, A. Mehta, H. Goonesinghe, D. M. Syahkal, H. Nakano, *IEEE Trans. Antennas Propag.* **66**, 2 (2018)
5. S. E. A. Filho, A. M. F. Burlamaqui, R. V. Aroca, L. M. G. Gonçalves, *IEEE Access* **5**, 16297-16313 (2017)
6. G. Pasolini, A. Bazzi, F. Zabini, *IEEE Signal Process. Mag.* 151-157 (2017)
7. I. Gupta, V. Patil, C. Kadam, S. Dumbre, *Proc. WIECON-ECE*, 83-86 (2016)
8. K. Pulli, A. Baksheev, K. Korniyakov, V. Eruhimov, *Comm. of the ACM* **55**, 6 (2012)
9. O. Green, *IEEE Trans. Image Process.* **27**, 5 (2018)
10. Y. Shen, M. Yang, B. Wei, C. T. Chou, W. Hu, *IEEE Trans. Mobile Comput.* **16**, 6 (2017)
11. S. U. Sharma, D. J. Shah, *IEEE Access* **5**, 347-358 (2017)
12. I. B. Mustaffa, S. F. B M. Khairul, *Proc. ICORAS*, 1-3 (2017)
13. S. Emami, V. P. Suci, *J. of Mobile, Embed. and Distrib. Systems* **IV**, 1 (2012)
14. P. Viola, M. Jones, *Proc. of CVPR*, 511-518 (2001)
15. T. Sutikno, L. Handayani, D. Stiawan, M. A. Riyadi, I. M. I. Subroto, *IJECE* **6**, 3 (2016)

16. R. E. N. Sisyanto, Suhardi, N. B. Kurniawan, *Proc. ICITSI*, 239-245 (2017)
17. G. B. Satrya, P. T. Daely, M. A. Nugroho, *Proc. ICTS*, 1-7 (2016)
18. N. A. Othman, I. Aydin, *Proc. ICCICN*, 108-112 (2017)
19. J. C. de Oliveira, D. H. Santos, M. P. Neto, *Proc. ISCE*, 131-132 (2016)
20. Y. Cheng, L. Jiao, Y. Tong, Z. Li, Y. Hu, X. Cao, *IEEE Access* **5**, 25835-25845 (2017)
21. S. Kasim, R. Hassan, N. H. Zaini, A. S. Ahmad, A. A. Ramli, R. R. Saedudin, *IJASEIT* **7**, 5 (2017)
22. R. Rahim, T. Afriliansyah, H. Winata, D. Nofriansyah, Ratnadewi, S. Aryza, *Proc. InteriOR*, 300 (2018)