Turnitin Fakultas Teknik

Jurnal Sinta 2 Polimesin Aceh-Deni K dkk

Face_recognition_Deni

Document Details

Submission ID
trn:oid:::3618:125440468

Submission Date
Dec 31, 2025, 9:30 PM GMT+7

Download Date
Dec 31, 2025, 10:12 PM GMT+7

File Name
Jurnal Sinta 2 Polimesin Aceh-Deni K dkk.pdf

File Size
665.5 KB

7 Pages

4,805 Words

23,768 Characters

5% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text
- Small Matches (less than 8 words)

Exclusions

- 28 Excluded Matches

Match Groups

2 Not Cited or Quoted 5%
Matches with neither in-text citation nor quotation marks

0 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

5% Internet sources
0% Publications
5% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- **2** Not Cited or Quoted 5%
  Matches with neither in-text citation nor quotation marks
- **0** Missing Quotations 0%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

5% Internet sources
0% Publications
5% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1 Student papers

Syiah Kuala University on 2023-07-21 **5%**

Jurnal Polimesin
Department of Mechanical Engineering
State Polytechnic of Lhokseumawe
http://e-jurnal.pnl.ac.id/polimesin
e-ISSN : 2549-1999 No. : 3 Month : June
p-ISSN : 1693-5462 Volume : 21 Year : 2023

Article Processing Dates: Received on 2022-12-28, Reviewed on 2023-03-25, Revised on 2023-04-28, Accepted on 2023-05-02, and Available online on 2023-06-30

AI-based face recognition system with telegram notification for room security on raspberry PI

Deni Kurnia[1*], Afzeri[1], Imam Muis H[1], Slamet Riyadi[1], Adolf Asih Supriyanto[1], Feri Siswoyo Hadisantoso[2]
[1]Mechatronics Engineering Department, Politeknik Enjinering Indorama, Purwakarta, 41152, Indonesia.
[2]Electrical Engineering Department, Politeknik Enjinering Indorama, Purwakarta, 41152, Indonesia.
[*]Corresponding author**:** deni.kurnia@pei.ac.id

Abstract

This research is based on the importance of a security system in a room by implementing AI combined with the telegram notification system. The goal is that security information can be obtained quickly and in real-time. The methodology used is to design a hardware system consisting of input, process and output devices. The input device consists of a Logitech C270 camera mounted on 2 MG966R type servo motors so that the camera can rotate on the X and Y axes, then the results of the camera captures are processed using the Haar Cascade Classifier and Local Binary Pattern Histogram (LBPH) algorithms. Raspberry Pi 4 is used as a data processing center and push notification to telegrams in the form of images when faces are detected by a web camera. Only registered users may enter the room, by opening the door when a face is recognized. Our findings show that a room security system with an AI-based facial recognition application can be implemented, according to the planning and design results in this study. The door opening process produces an average result of 4.586 seconds, with the longest time being 4.981 seconds and the fastest time being 4.116 seconds. The door closing process produces an average result of 4.496 seconds, with the longest time being 4.966 seconds and the fastest time being 4.106 seconds. The average time of opening and closing the door is ideal and safe. From the results of the research that has been done, it can be concluded that the use of AI in this study aims to make decisions that only registered users can enter a room. In addition, the ability of the camera to move dynamically on the x and y axes is one of the system developments that did not exist before, so that the ability to take pictures besides being more accurate also becomes wider dynamic.

Keywords: face recognition, telegram notification, raspberry pi, security system

1 Introduction

The security system of a room is one of the needs that must be met by a public or private organization. This security system was constructed utilizing classic models, such as keys in general, to construct it using the most recent research. One application of the security system makes use of a fingerprint and facial recognition system[1], [2].

Face identification via digital image processing is a technique used by face recognition technologies [3]–[6]. This facial recognition technique is being used more and more in biometric recognition systems, digital video, security systems, search, indexing picture datasets, video conferencing, and human-computer interaction [7]–[9].

Face detection is the initial stage before the face recognition process is carried out. With the increasing use of facial recognition technology, an accurate image processing system is needed to be able to identify a person by analyzing patterns based on the texture and shape of a person's face which has previously been stored in a dataset and has been previously trained. In previous research, the role of raspberry pi is important in data processing [10] combined with an IoT monitoring system [11], [12]. In addition, other researchers also use MATLAB [13], [14] and the K-Nearest Neighbor algorithm[15].

There were two things that became the basis for the emergence of this research from previous research. First, creating a system using IoT but not using face recognition[16]. Second, creating face recognition but data is only stored locally, not transmitted[17]. This research fills in the research gap, namely AI face recognition [18]–[20] transmission via telegram notification [21]–[23] with IoT system, thereby making the monitoring process more effective because it can be accessed remotely in real time.

2 Research methods

The research methodology is to develop hardware and software systems. On the hardware side of development, the system is divided into system design and testing design.

2.1 System design

The prototype room security system with face recognition is designed to fulfill the security of the room when occupied or unoccupied. The system works using a raspberry pi 4 which has 40 pins which are divided, namely 26 pins for GPIO, 8 pins for GND, 2 pins for 5 V voltage, 2 pins for 3.3 V voltage, and 2 pins for I2C communication backup.

A web camera on the raspberry pi 4 is used to take digital pictures in addition to acting as a data processing hub. The type of web camera used is Logitech C270. This webcam has an image resolution of about 1280 x 720 pixels and a video frame rate of 1080p at 30fps.

To locate the discovered users, the system makes use of the telegram bot. The image is captured by the webcam and shown on the monitor. If the user's face is recognized, the door will automatically open and close with a limit switch sensor, and if they don't enter for more than five seconds, the door will close again and they will be asked to re-enter. Three actuators are employed in the system: a servo motor to move the webcam, a DC motor with a gearbox to automatically open and close the door, and a solenoid door lock to lock the door. The input block, process block, and output block are the three sections of the block diagram in Fig. 1.

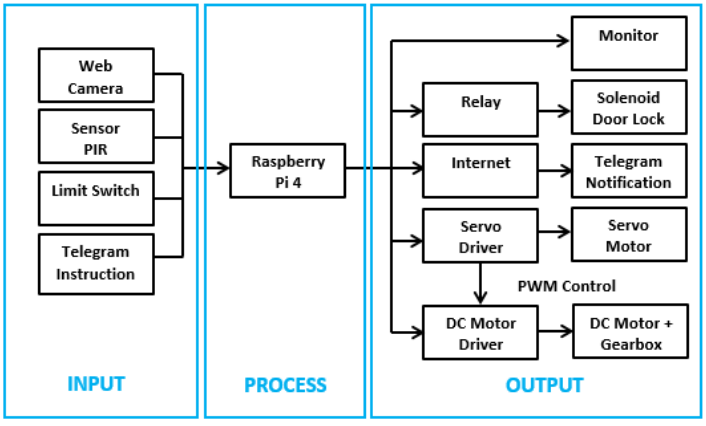


Fig. 1. Block diagram for a room security

Figure 1 shows the hardware system is divided into three main blocks, namely: input, process and output.

2.1.1 Input Block

Web cameras Logitech C270 are used to take pictures. PIR Sensors work to identify people who have entered, limit switches work to locate open and closed doors, send commands to the system using the telegram commands feature to stop it by entering a password, retrieve the image of the most recent user who entered, set the direction of servo movement, and take the most recent photos from web camera captures.

2.1.2 Process Block

The raspberry pi's primary purpose is to process input data so that it can be routed to output data via GPIO pins. Python programming is used to control the process between input and output data.

RPi.GPIO, busio, board, CV2, numpy, socket, telepot, datetime, openpyxl, adafruit servokit, and adafruit PCA9685 are all included in version 3. It should be further explained that as the main controller, so that this Raspberry pi can be used to implement an artificial intelligence system for a room security system, several libraries are required to be installed.

There are 13 libraries are needed for the system design in the final project, but 5 of them must be installed on the raspberry pi because they are not yet there. These are the libraries that were used in Table 1 and the raspberry pi image is shown in Fig. 2.

Table 1. Library needs for raspberry pi system design

Library type	Usability
Telepot	Accessing Telegram bots
Datetime	Know the current time, day, and date
Openpyxl	Manage Microsoft Office Excel files
RPi.GPIO	Accessing Raspberry Pi GPIO pins
Busio & board	I2C communication with servo driver
Adafruit_servokit	Setting the servo motor
Adafruit_pca9685	Set the PWM signal of the DC motor
OS	Managing files in Raspberry Pi storage
CV2	Face detection and recognition
Time	Delay to hold the door open
PIL	Image processing
Numpy	Training data of face sample array
Socket	Check internet connectivity

Fig. 2. Raspberry Pi 4 as the main controller

2.1.3 Output Block

The relay functions as a switch for the door lock solenoid, while the internet functions as a channel for telegram notifications. Solenoid door lock functions to lock the door, monitor functions to display web camera captures, Servo motor functions to direct the camera if the user's face is not right in the middle of the webcam shooting area, DC Motor + gearbox functions to open and close doors, and telegram notifications functions as a notification of detected users.

Overall how the security system works can be explained in the flowchart of Fig. 3.

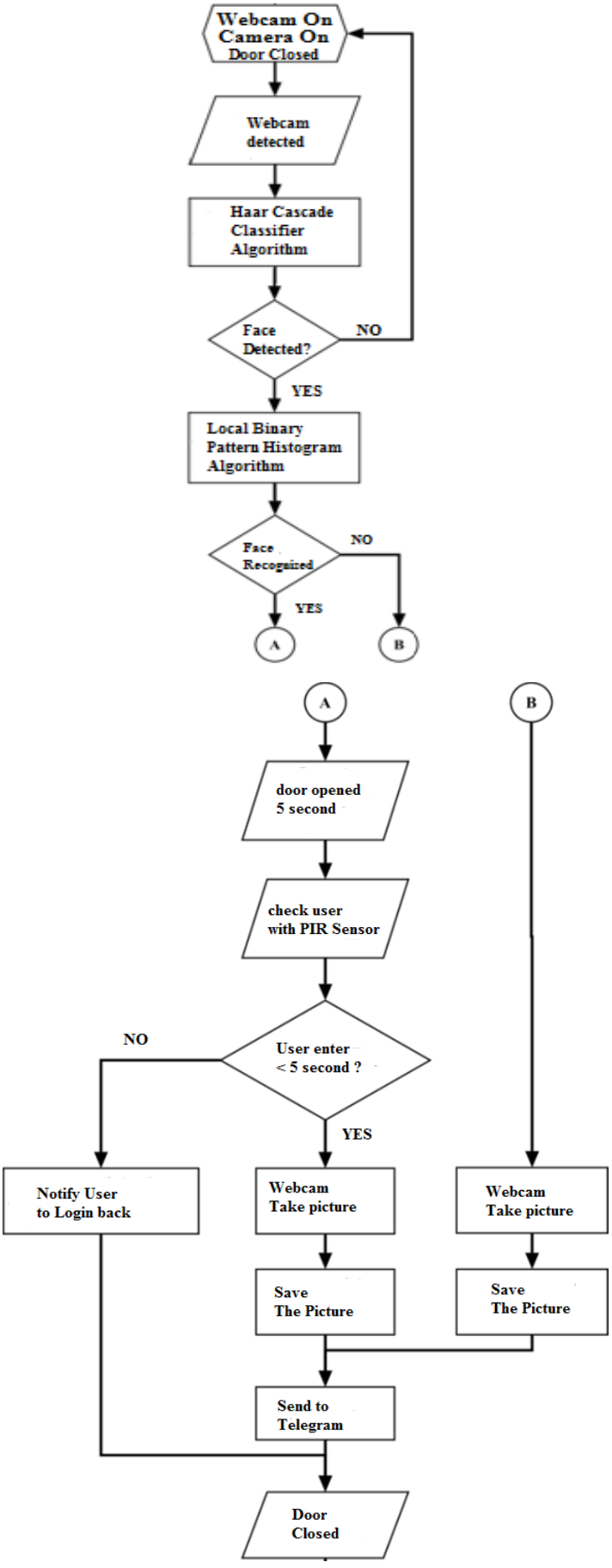


Fig. 3. Flowchart of how the security system works

Fig. 4 shows it can be explained that the Haar cascade classifier algorithm is used to process facial data when the camera detects people entering the room. The Haar Cascade Classifier Algorithm is one of the algorithms used to detect a face. The algorithm is able to detect objects quickly and in real time, including human faces[24], [25].

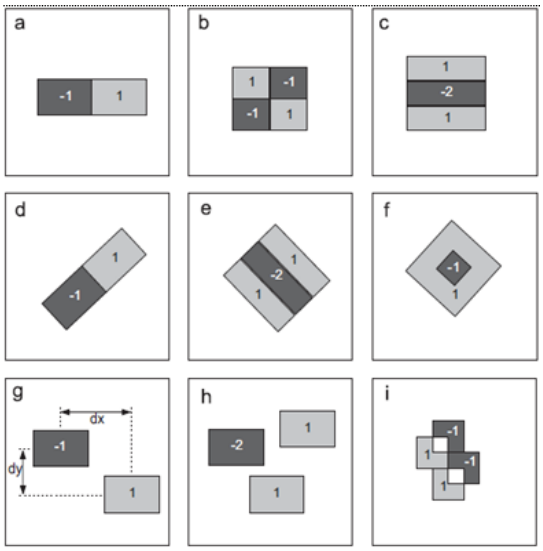


Fig. 4. The Haar Cascade Classifier Algorithm

Furthermore, the Local Binary Pattern Histogram (LBPH) is used to check whether the detected face is known or not as shown in fig. 5. Because this algorithm is a face recognition algorithm based on a local binary operator, designed to recognize both the side and front face of a human. However, the recognition rate of the LBPH algorithm is limited, if the conditions, such as in the expression diversification, disorientation, and a change in the lighting performance manifest[26].

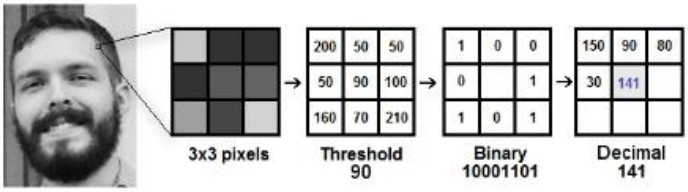


Fig. 5. Local Binary Pattern Histogram (LBPH)

The next process is when the camera detects a person. If the face is recognized (YES) it will proceed to the following process: open the door for 5 minutes, the active PIR sensor detects whether the person has entered or not. If the person has entered the room through the door, then proceed with the process of taking pictures, saving the picture to the database on Raspberry and sending notifications to Telegram. Still in this process, if the person has not been detected entering, the door will reopen for 5 minutes.

Conversely, if the system detects an unknown face (NO), then the door will not open and proceed by taking a photo of the person's face which is then stored in the database and sent via telegram.

2.2 Testing Design

2.2.1 System evaluation with confusion matrix

The facial recognition system will be tested to determine whether the face belongs to a registered or unregistered user. 100 tests are performed by registered users, and 50 tests are performed by unregistered users, for a total of 150 tests. In comparison to the 50 tests taken by unregistered users, 93 of the 100 tests taken by registered users yielded right results, while 7 of the 100 tests taken by registered users yielded wrong results. The confusion matrix that was used to test the facial recognition system for the final project is shown in fig. 6.

	Actually Positive	*Actually Negative*
Predicted Positive	93	5
Predicted Negative	7	45

Fig. 6. Confusion matrix table

a. Accuracy value

Accuracy describes how accurately the model can classify correctly. Therefore, accuracy is the ratio of correct predictions (positive and negative) to the overall data. In other words, accuracy is the closeness of the predicted value to the actual value.

The accuracy value can be calculated (Eq. 1) using the binary classification confusion matrix shown above to provide an answer to the question of "What proportion of faces are properly predicted as registered or unregistered users from all faces".

$$accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad \text{.....(1)}$$

$$accuracy = \frac{93 + 45}{93 + 45 + 5 + 7}$$

$$accuracy = 0.92 \times 100\%$$

$$accuracy = 92\%$$

b. Precision value

The degree of accuracy between the requested data and the model's expected output is referred to as precision. The proportion of accurate positive forecasts to all positive expected results is hence known as precision. “How many of the correctly anticipated positive classes actually have positive data”.

The precision value can be calculated (Eq. 2)using the aforementioned binary classification confusion matrix to provide the response to the question of "What proportion of faces are successfully registered users out of all faces predicted as registered users".

$$precision = \frac{TP}{TP + FP} \quad \text{.....(2)}$$

$$precision = \frac{93}{93 + 5}$$

$$precision = 0.949 \times 100\%$$

$$precision = 94.9\%$$

c. Recall value

The success of the model in information retrieval is indicated by recall. Recall is the proportion of correctly predicted positive outcomes to all true positive data. By such equation below, one may determine the recall value.

The recall value can be calculated using the aforementioned binary classification confusion matrix to provide the answer to the query of "What proportion of faces are anticipated as registered users related to all faces that are really registered”.

$$recall = \frac{TP}{TP + FN} \quad \text{.....(1)}$$

$$recall = \frac{93}{93 + 7}$$

$$recall = 0.93 \times 100\%$$

$$recall = 93\%$$

The following Fig. 7 shows the overall face recognition system performance.

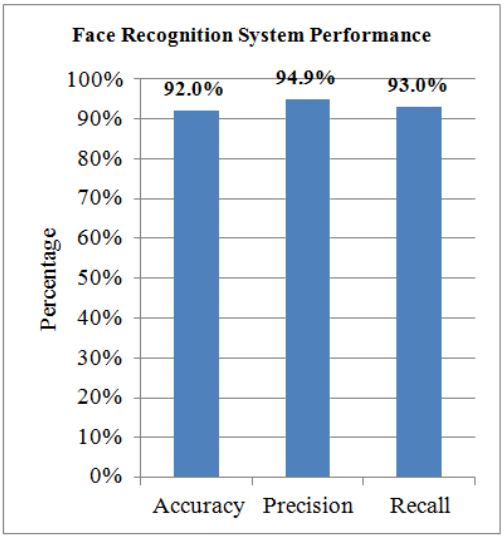


Fig. 7. Face recognition system performance

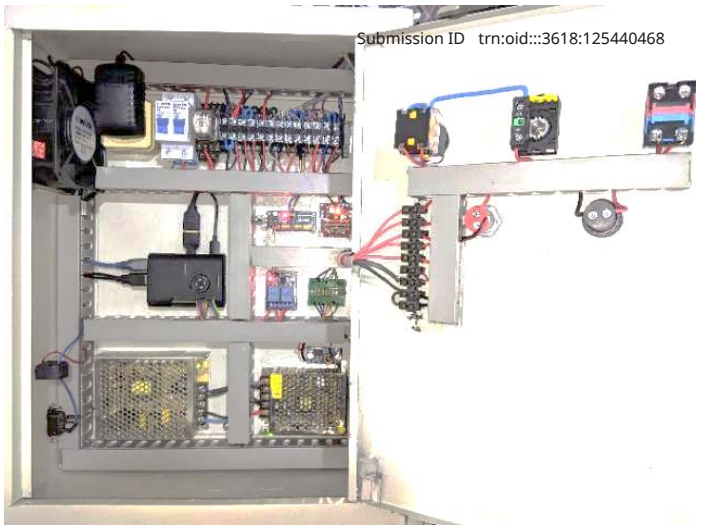
Fig. 7 explains that in system testing, the percentages for three important values are obtained, namely accuracy with a value of 92.0%, precision with a value 94.9% and recall with a value 93.0%.

3 Result and Discussion

The outcomes of the entire system design can be showed in Fig. 8a. All the steps of the above method are applied to the hardware design result with inside panel view that is shown in Fig. 8b.

Fig. 8 is a panel that is designed in a compact and portable manner, this panel consists of a camera, LCD screen and control panel. Inside the control panel there is the following equipment: Raspberry pi 4, power supply unit, relay connected to the output block device as described in the block diagram in Fig. 1.

(a)



(b)

Fig. 8a. The system's panel view (1. Camera, 2. LCD Screen, 3. Panel Control). 8b. looks inside the panel control.

3.1 Performance evaluation of webcam image processing

The average picture processing result from testing webcam Logitech C270 image processing speed is 26.74 FPS, with the lowest image processing result being 23 FPS and the best being 30 FPS. A graph of webcam performance testing for image processing is shown in Fig. 9.

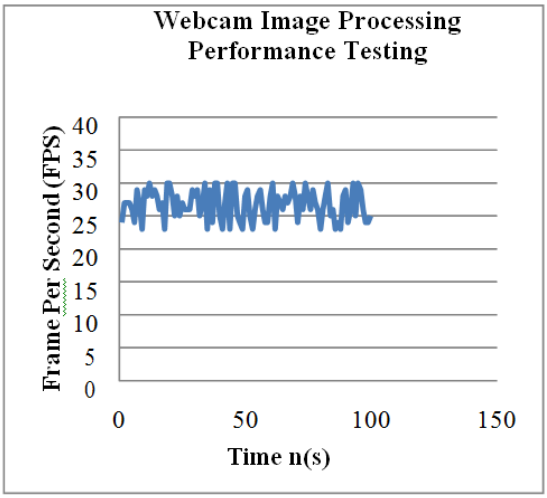


Fig. 9. Performance testing for image processing.

From the graph in Fig. 9 it can be explained that this web camera has a range between 23-30 fps when performing image processing speed.

3.1.1 Door access system testing and first user photo delivery

The initial user test consisted of 50 trials, with an average facial accuracy of 93.90%, the lowest accuracy being 89%, and the greatest accuracy being 99%. The average time for opening a door is 4.639 seconds, with the longest time being 4.976 seconds and the quickest being 4.124 seconds. The average time for closing a door is 4.493 seconds, with the longest time being 4.987 seconds and the quickest being 4.100 seconds. The average time for sending photos of incoming users is 2.327 seconds, with the longest time being 4.599 seconds and the quickest being 2.009 seconds. The test results for the first user are shown in table 2 and Fig. 10.

Table 2. First user testing data

Value	Accuration (%)	Door Opened(s)	Door Closed(s)	Sending Image(s)
Lowest	89	4.124	4.100	2.009
Highest	99	4.976	4.987	2.599
Average	93.9	4.639	4.493	2.327

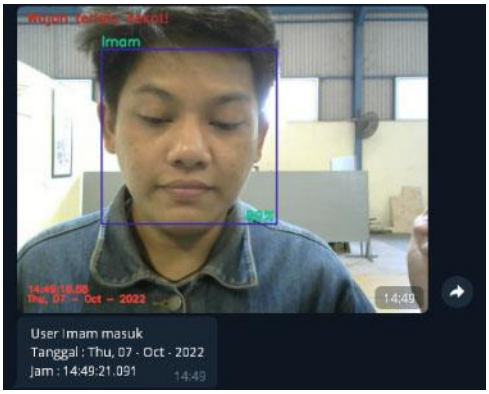


Fig. 10. Test the first user taking a photo

3.1.2 Testing the door access system and delivering the second user's photos

In the second user test, 50 trials were conducted where the average facial accuracy was 92.98% with the lowest accuracy of 87% and the highest of 99%. In the door opening process, the average result is 4.532 seconds with the longest time of 4.986 seconds and the fastest time of 4.107 seconds. The average time for closing a door is 4.500 seconds, with the longest time being 4.944 seconds and the quickest being 4.111 seconds. The average time for sending images of approaching people is 2.269 seconds, with the longest time being 4.572 seconds and the quickest being 2.004 seconds (table 3)

Table 3. Second User Testing Data

Value	Accuration (%)	Door Opened(s)	Door Closed(s)	Sending Image(s)
Lowest	87	4.107	4.111	2.004
Highest	99	4.986	4.944	2.572
Average	92.98	4.532	4.500	2.269

3.1.3 Command testing: take photos via telegram and send photos unrecognized face

In testing take photos via telegram and send unrecognized faces, testing was carried out 50 times. In testing send photos from the take photos command, it was obtained the average results of 2.807 seconds with the longest time of 3.098 seconds and the fastest time of 2.528 seconds. While in testing send unrecognized faces, it was obtained average results for 2.310 seconds with the longest time of 2.593 seconds and the fastest time of 2.009 seconds. The following Table 4 and Fig. 11 are the results of testing photo delivery on the take photos command and unrecognized faces.

Fig. 11. Take a photo via telegram and send unrecognize face

Table 4. Send photos via telegram

Value	Take Photo (s)	Unrecognized face
Lowest	2.528	2.009
Highest	3.098	2.593
Average	2.807	2.310

On telegram, a menu is available for taking photos as shown in Fig. 12. Meanwhile, the captured photos shown in Fig. 13.

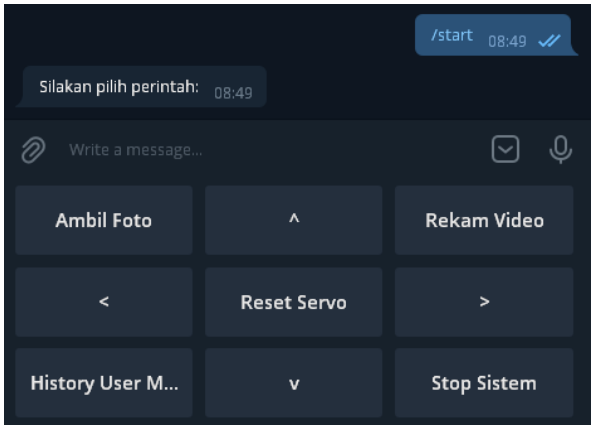


Fig. 12. Telegram menu user interface

Fig. 13. The results of the photos obtained and appear on telegram

3.1.4 Video recording test for monitoring

In the video recording test, the average recording time is 15.761 seconds with the longest time of 23.754 seconds and the fastest time of 12.854 seconds. While for video delivery time, the average recording time is 3.292 seconds with the longest time of 4.355 seconds and the fastest time of 2.886 seconds. The following Table 5 shows video recording during monitoring.

Table 5. Test video recording during monitoring

Value	Recording time(s)	Video Delivery Time (s)	File Size (MB)
Lowest	12.854	2.886	2.540
Highest	23.754	4.355	4.020
Average	15.761	3.295	2.953

Fig. 14 shows that the length of video transmission is virtually directly inversely correlated with the size of the video file, leading to the conclusion that the longer it takes to send the environment monitoring video file to telegram, the larger the video file size. Fig. 15 shows the results of the capture of the video monitoring camera.

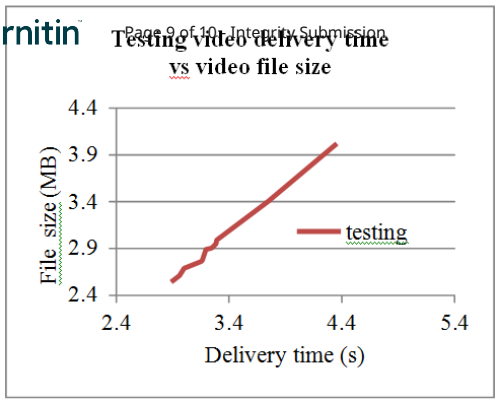


Fig. 14. Testing video delivery time vs video file size

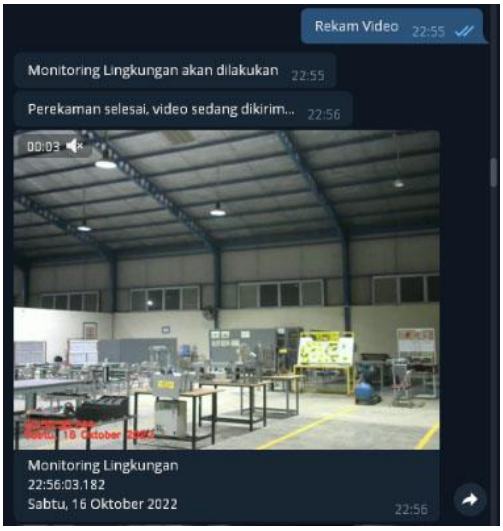


Fig. 15. Video Monitoring

The findings show that a room security system with an AI-based facial recognition application can be implemented, according to the planning and design results in this study. The door opening process produces an average result of 4.586 seconds, with the longest time being 4.981 seconds and the fastest time being 4.116 seconds. The door closing process produces an average result of 4.496 seconds, with the longest time being 4.966 seconds and the fastest time being 4.106 seconds. The average time of opening and closing the door is ideal and safe.

Furthermore, average image processing results using facial recognition application is 26.74 FPS, with the lowest image processing is 23 FPS and the best is 30 FPS. While the video recording test resulted in an average recording time is 15.761 seconds with the longest time being 23.754 seconds and the fastest time being 12.854 seconds. The video sending time resulted in an average recording time is 3.292 seconds with the longest time being 4.355 seconds and the fastest time being 2.886 seconds. The results of the photo sending process show that the sending time ranges from 2.004 to 3.098 seconds with an average of 2.428 seconds. This Fig. is not the best Fig., but the performance of the AI system can be processed quite well.

In the system testing section, out of a total of 150 tests, where 100 tests were carried out on registered users and 50 tests on unregistered users, the face recognition application that uses the Raspberry Pi 4 achieves an accuracy value of 92%, a precision value of 94.9%, and a recall value of 93. %. Compared to 50 tests performed by unregistered users, 93 out of 100 tests performed by registered users returned correct results, while 7 out of 100 tests performed by registered users returned incorrect results. This means that the percentage of failure for unknown faces is still below 0.07%.

4 Conclusion

The use of AI in this study aims to make decisions that only registered users can enter a room. In addition, the ability of the camera to move dynamically on the x and y axes is one of the system developments that did not exist before so that the ability to take pictures besides being more accurate also becomes wider dynamic. The use of the Haar Cascade Classifier Algorithm and the Local Binary Pattern Histogram (LBPH) Algorithm is a combination that is quite effective as a tool in this AI-based room security system. One of the contributions of this research is the existence of a real time notification system via Telegram with a user interface that is easy to develop on the Telegram menu. So besides being able to receive notifications in the form of pictures from known and unknown users, the system can intelligently make decisions about who is allowed to enter and not by giving instructions whether the room door is open or not. The use of a camera with a higher resolution is a future suggestion so that the accuracy of sampling user data is faster and more accurate. This research may be further developed towards machine learning and deep learning in the future.

Reference

[1] N. Kar, M. K. Debbarma, A. Saha, and D. R. Pal, “Study of Implementing Automated Attendance System Using Face Recognition Technique,” *International Journal of Computer and Communication Engineering*, vol. 1, no. 2, pp. 100–103, 2012, doi: 10.7763/ijcce.2012.v1.28.

[2] A. Trisnani, B. F. Barry, H. Santoso, I. M. Putra, and F. A. Saputra, “‘ SMART DOOR LOCK ’ : Anti-Sabotage Door Security System for Restricted Room,” *Proceedings on Science and Technology*, vol. 1, pp. 2–6, 2017, [Online]. Available: http://proceedings.ui.ac.id/index.php/uipst/article/download/109/153

[3] S. J. Lee, S. B. Jung, J. W. Kwon, and S. H. Hong, “Face detection and recognition using PCA,” *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, vol. 1, no. December, pp. 84–87, 1999, doi: 10.1109/TENCON.1999.818355.

[4] T. Menezes, “Face Recognition Attendance System using Raspberry Pi,” *Int J Res Appl Sci Eng Technol*, vol. 9, no. 8, pp. 1145–1149, 2021, doi: 10.22214/ijraset.2021.37499.

[5] R. Purwati and G. Ariyanto, “Pengenalan Wajah Manusia berbasis Algoritma Local Binary Pattern,” *Emitor: Jurnal Teknik Elektro*, vol. 17, no. 2, pp. 29–38, 2017, doi: 10.23917/emitor.v17i2.6232.

[6] T. K. Vamsi, “Face recognition based door unlocking syVamsi, T. K. (2019) ‘Face recognition based door unlocking system using Raspberry Pi’, Academia.Edu.stem using Raspberry Pi,” *Academia.Edu*, vol. 5, no. 2, pp. 1320–1324, 2019.

[7] Z. QasemJaber and M. Issam Younis, “Design and Implementation of Real Time Face Recognition System (RTFRS),” *Int J Comput Appl*, vol. 94, no. 12, pp. 15–22, 2014, doi: 10.5120/16395-6014.

[8] A. Santos-Olmo, L. E. Sánchez, I. Caballero, S. Camacho, and E. Fernandez-Medina, “The importance of the security culture in SMEs as regards the correct management of the security of their assets,” *Future Internet*, vol. 8, no. 3, 2016, doi: 10.3390/fi8030030.

[9] B. A. Sujatmoko and A. Sujarwo, "Dual Security System for Room Access Control Using RFID at Islamic University of Indonesia (UII)," *IOP Conf Ser Mater Sci Eng*, vol. 803, no. 1, 2020, doi: 10.1088/1757-899X/803/1/012029.

[10] Gaurav Dhiman, Srihari. K, Ramesh. R, and Udayakumar. E, "An Innovative Approach for Face Recognition Using Raspberry Pi," *Artificial Intelligence Evolution*, pp. 102–107, 2020, doi: 10.37256/aie.12202062.

[11] I. G. M. Ngurah Desnanjaya and I. N. A. Arsana, "Home security monitoring system with IoT-based Raspberry Pi," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 3, pp. 1295–1302, 2021, doi: 10.11591/ijeecs.v22.i3.pp1295-1302.

[12] A. R. Syafeeza, M. K. Mohd Fitri Alif, Y. Nursyifaa Athirah, A. S. Jaafar, A. H. Norihan, and M. S. Saleha, "IoT based facial recognition door access control home security system using raspberry pi," *International Journal of Power Electronics and Drive Systems*, vol. 11, no. 1, pp. 417–424, 2020, doi: 10.11591/ijpeds.v11.i1.pp417-424.

[13] A. A. Shah, Z. A. Zaidi, B. S. Chowdhry, and J. Daudpoto, "Real time face detection/monitor using raspberry pi and MATLAB," *Application of Information and Communication Technologies, AICT 2016 - Conference Proceedings*, pp. 2–5, 2017, doi: 10.1109/ICAICT.2016.7991743.

[14] S. Gurumurthy and B. K. Tripathy, "Design and Implementation of Face Recognition System in Matlab Using the Features of Lips," *International Journal of Intelligent Systems and Applications*, vol. 4, no. 8, pp. 30–36, 2012, doi: 10.5815/ijisa.2012.08.04.

[15] E. Setiawan and A. Muttaqin, "Implementation of K-Nearest Neightbors Face Recognition on Low-power Processor," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 13, no. 3, p. 949, 2015, doi: 10.12928/telkomnika.v13i3.713.

[16] Juman Kundang K, Tjahjono B, Yulhendri, and Apresia Kadek, "Design And Build A Room Security System Based On Internet Of Things (IOT)," *International Journal of Science, Technology & Management*, vol. 2, no. 3, pp. 710–717, 2021, doi: 10.46729/ijstm.v2i3.186.

[17] A. A. Wazwaz, A. O. Herbawi, M. J. Teeti, and S. Y. Hmeed, "Raspberry Pi and computers-based face detection and recognition system," *2018 4th International Conference on Computer and Technology Applications, ICCTA 2018*, pp. 171–174, 2018, doi: 10.1109/CATA.2018.8398677.

[18] L. Li, X. Mu, S. Li, and H. Peng, "A Review of Face Recognition Technology," *IEEE Access*, vol. 8, pp. 139110–139120, 2020, doi: 10.1109/ACCESS.2020.3011028.

[19] T. Bucher, "Facing AI: conceptualizing 'fAIce communication' as the modus operandi of facial recognition systems," *Media Cult Soc*, vol. 44, no. 4, pp. 638–654, May 2022, doi: 10.1177/01634437211036975.

[20] I. Chatisa, Y. A. Syahbana, and A. U. A. Wibowo, "Object Detection and Monitor System for Building Security Based on Internet of Things (IoT) Using Illumination Invariant Face Recognition," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, Feb. 2023, doi: 10.22219/kinetik.v8i1.1622.

[21] R. Wahyuni, A. Rickyta, U. Rahmalisa, and Y. Irawan, "Home security alarm using wemos D1 and HC-SR501 sensor based telegram notification," *Journal of Robotics and Control (JRC)*, vol. 2, no. 3, pp. 200–204, May 2021, doi: 10.18196/jrc.2378.

[22] U. Rahmalisa, A. Febriani, and Y. Irawan, "Detector leakage gas LPG based on telegram notification using wemos D1 and MQ-6 sensor," *Journal of Robotics and Control (JRC)*, vol. 2, no. 4, pp. 287–290, Jul. 2021, doi: 10.18196/jrc.2493.

[23] M. Zuma, P. A. Owolawi, V. Malele, K. Odeyemi, G. Aiyetoro, and J. S. Ojo, "Intrusion Detection System using Raspberry Pi and Telegram Integration," Association for Computing Machinery (ACM), Dec. 2021, pp. 1–7. doi: 10.1145/3487923.3487928.

[24] I. Muhammad Hakim, D. Christover, and A. M. Jaya Marindra, "Implementation of an Image Processing based Smart Parking System using Haar-Cascade Method," *ISCAIE 2019 : 2019 IEEE Symposium on Computer Applications & Industrial Electronics*, Apr. 2019.

[25] N. Kamarudin *et al.*, "Implementation of haar cascade classifier and eye aspect ratio for driver drowsiness detection using raspberry Pi," *Universal Journal of Electrical and Electronic Engineering*, vol. 6, no. 5, pp. 67–75, Dec. 2019, doi: 10.13189/ujeee.2019.061609.

[26] R. Kosasih and C. Daomara, "Pengenalan Wajah dengan Menggunakan Metode Local Binary Patterns Histograms (LBPH)," *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 5, no. 4, p. 1258, Oct. 2021, doi: 10.30865/mib.v5i4.3171.