Home Security System with Face Recognition based on Convolutional Neural Network

Nourman S. Irjanto[1], Nico Surantha[2]
Computer Science Department, BINUS Graduate Program - Master of Computer Science
Bina Nusantara University, Jakarta

***Abstract*—Security of house doors is very important and becomes the basis for the simplest and easiest security and sufficient to provide a sense of security to homeowners and along with technological developments, especially in the IoT field, which makes technological developments in locking house doors have developed a lot like locking house doors with faces and others. The development of facial recognition systems has also developed and has been implemented for home door locking systems and is an option that is quite simple and easy to use and is quite accurate in recognizing the face of homeowners. The development of the CNN method in facial recognition has become one of the face recognition systems that are easy to implement and have good accuracy in recognizing faces and has been used in object recognition systems and others. In this study, using the CNN Alexnet facial recognition system which is implemented in a door locking system, data collection is done by collecting 1048 facial data on the face of the homeowner using a system which is then used to train machine learning where the results are quite accurate where the accuracy is the result is 97.5% which is quite good compared to some other studies. The conclusion is the CNN Alexnet method can perform facial recognition which is quite accurate which can be implemented on the IoT device, namely, the Raspberry Pi.**

Keyword—Home door security; CNN Alexnet; facial recognition; Raspberry Pi

I. Introduction

Over the past few years, there have been quite a several choices in conventional technology and biometric technology to meet security needs for households or offices. Some conventional security systems, for example using keys, passcodes, ID cards, and/or RFID cards, can be unreliable if objects for access are stolen or lost [1]. Such security systems have disadvantages when access is stolen by people who do not have the authority to gain access and also daily activities sometimes force someone to leave the house empty, such as during work or school hours. This makes the house vulnerable to break into and theft, even when the house is locked or securely locked. The development of Information Technology and Communication currently offers convenience to users in various lines of life. One technology that is currently trending is the smart home or what is commonly known as the smart home. A smart home is a term used to define a residence that has the equipment, lighting, heating, air conditioning, TV, computer, audio system, video entertainment, security, and camera systems that can communicate with each other and can be controlled remotely with a timetable. through the internet or telephone [2]. Biometric systems are developing rapidly, especially for home security technology because they can fulfill two functions, namely identification, and verification, biometrics have characteristics that cannot be lost, cannot be forgotten, and cannot be faked where their inherent presence in humans will differ between humans and other humans so that their uniqueness is guaranteed [3]. In the journal [4] facial recognition as authentication is very good because the face is a physiological feature that is easiest to distinguish between individuals so face recognition is one of the biometrics technologies that are often studied and developed.

Convolutional Neural Networks combines three basic architectures, namely local receptive fields, shared weight in the form of filters, and spatial subsampling in the form of pooling. Convolution or what is commonly known as convolution is a matrix that functions to perform filters[5]. In the filtering process, there are two matrices, namely the input value matrix and the kernel matrix. In the Convolutional Neural Network, several layers function to carry out the filters that have been determined during the training process, namely Convolutional Layer, Pooling Layer, and Fully Connected Layer [6]. The architecture that is owned by the Convolutional Neural Network can be seen in Fig. 1.

The previous paper described a prototype of a safe room access control system based on facial recognition. This system consists of a webcam to detect faces and a solenoid door lock to access the room. Every user detected by the webcam will be checked for compatibility with the database on the system using the Haar cascade classifier method embedded in OpenCV. If the user has access rights, the solenoid door lock will open and the user can enter the room. In this paper, the Haar cascade classifier embedded in OpenCV can recognize multiple captured images [7]. Another project is designing facial recognition systems for smart home/office security applications. The design is implemented using a webcam and programmed using dlib and OpenCV. The connection between the cam and the computer can be made by cable and wireless. We'll be using a very simple approach to dealing with recognition using deep learning [8] and also in other research journals aimed at designing a door security system that uses Arduino as a microcontroller and utilizes open source OpenCV as a face reader where this research reads faces that have been entered into the database which will then match the images captured by the webcam. where the results of the accuracy measurement based on the test table carried out three times get a success rate of 71.40%, 85.71%, 71.42% [9] and In another study, a door security system was developed using facial recognition as a key to open doors. The method used in

this tool is the fisherface method. The main steps in facial recognition are face detection, PCA calculation, FLD calculation. where the measurement results of the accuracy of the system are 80% [10] and also in other research is an effort to develop assistance to maintain security in important places. We used the Viola-Jones algorithm to detect faces and the Eigenfaces algorithm to recognize people. The test results were recorded and we achieved 95% accuracy in recognition under fluorescent lighting conditions [11]. In this paper, we construct a face recognition system. In this work, we present the advantages and disadvantages of different techniques in a literature survey. It helps to choose a suitable technique among many as per our application requirements and solve current problems to some extent for real-time applications. We achieve 96.8% accuracy in real-time scenarios under many variations and seamless environments and also measure performance using the Multi-task Cascaded Convolutional Networks (MTCNN) method [12].

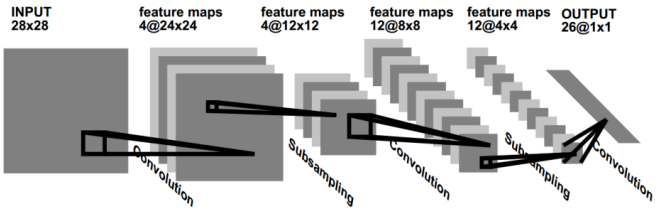


Fig. 1. Convolutional Neural Network Architecture.

Based on the existing cases, a new system must be devised to prevent house burglaries and thefts due to the weak security of the lock or padlock. So that the idea of facial recognition-based door security system innovation using the convolutional neural network (CNN)[13] method was created, of course, it has better security than locks or RFID. It can be said that this system is an automatic electronic lock. This system is expected to be able to tackle the occurrence of theft in houses that are often abandoned by the occupants.

This study expects a significant contribution to a new domain of knowledge regarding the application of accurate facial recognition technology to the home door locking systems. Therefore, this research is an attempt to build a facial recognition system that can work on house doors.

II. Method

In this study, we propose a facial recognition process for the process of opening the door of a house that can replace the process of home security using an electronic key or RFID, where the research stages are divided into 3 parts, namely the stages of collecting homeowner data, the data training process, and also the facial recognition process using Raspberry Pi. In this journal, we implement the facial recognition process with the CNN [14] method which will install it on a mini-computer, namely the raspberry pi which will serve as a microcontroller to lock and open the door automatically which is controlled by the face of the homeowner [15].

A. Homeowner Face Data Collection

The stages of data collection are carried out manually, namely by using a program designed to collect facial data from each homeowner consisting of 5 people where the total data is 1100 data which will then be divided 1040 for training data and 60 data is used for validation during training by doing the facial augmentation process starts from shifting 10-15 degrees with various expressions [16]. The results of data collection can be seen in Fig. 2 and 3.

B. Training Model

At this stage the training process is not carried out on the raspberry pi due to the small computation of the raspberry pi with that the training process is carried out on a separate computer with Intel Core i5 8500 Processor specifications and 8GB DDR4 RAM where this training process will also form a model that will be used to detect the face [17]. The stages of the training process use the CNN Alexnet method with two convolution processes and two pooling processes and softmax with several iterations of 20 times with the parameters shown in Fig. 4.

C. System Implementation

This prototype will be made by connecting the modified Pi Camera as a camera module to identify the face of the homeowner connected to the Raspberry Pi 3 Model B + where the Raspberry Pi will be connected via WLAN as a process of identifying the homeowner[18] as seen in Fig. 5.

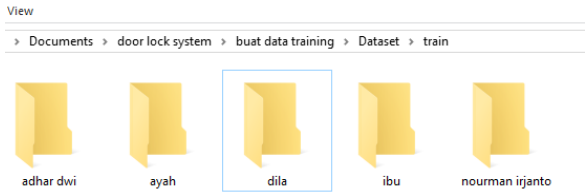


Fig. 2. Dataset of Homeowners Faces.

Fig. 3. Dataset of Face.

```
"""
Parameters
"""
img_width, img_height = 224, 224
batch_size = 32
samples_per_epoch = 1000
validation_steps = 300
nb_filters1 = 32
nb_filters2 = 64
conv1_size = 3
conv2_size = 2
pool_size = 2
classes_num = 5
lr = 0.0004
```

Fig. 4. Parameter Training Method.

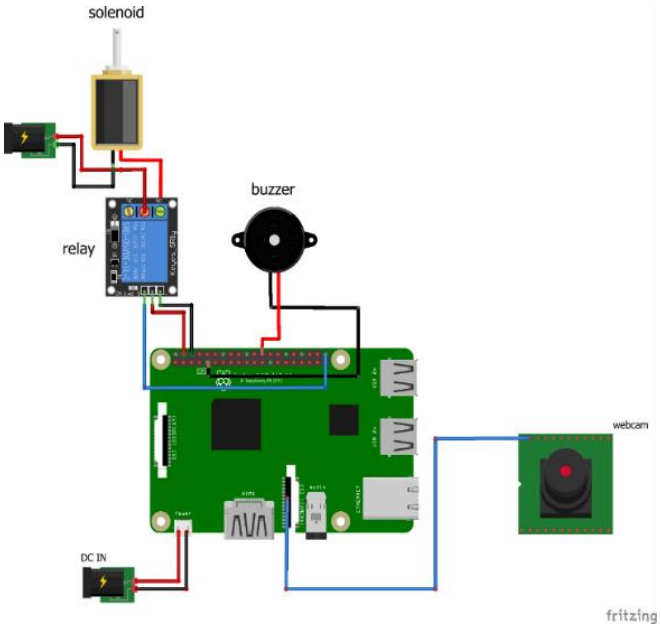


Fig. 5. System Design.

1) Flowchart system: The workflow of this system is divided into two parts, namely the registration stage where at this stage the data generated will be used as training data [19]. At this stage, there will be a registration process for the face data of the homeowner who will be trained on the computer to produce a training model which will be stored in the database on the Raspberry Pi and will be backed up and if it is already the device will be standby and ready to use as in Fig. 6.

The system installation process is carried out at the front door of the house which is the only entrance to the existing house as seen in Fig. 7 and Fig. 8.

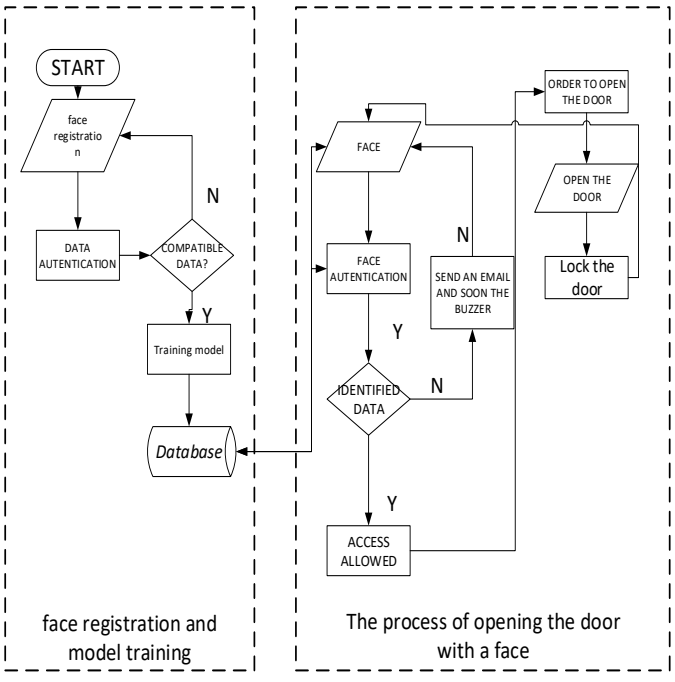


Fig. 6. Flowchart.

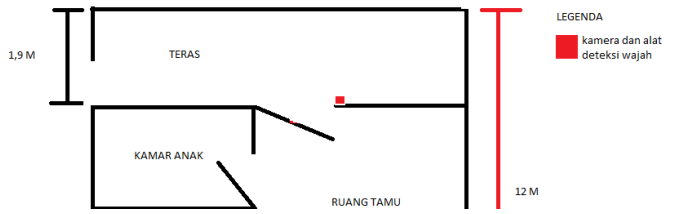


Fig. 7. Test Area.

Fig. 8. Device Placement.

III. Testing and Comparison

Testing is carried out by providing input in the form of five homeowners and also five faces of non-homeowners or neighbors who have been tested in morning conditions with a duration of 07.00 to 09.00, noon 12.00 to 14.00, noon 15.00 to 17.00, and night 19.00 to 22.00 with a distance 0.5 meters, 1 meter, and 1.5 meters, respectively and the distance from the front door [9].

A. Homeowner Testing

Testing of homeowners using the system built can be seen in Table I.

B. Testing is not a Homeowner or Neighbor

The non-homeowner test is carried out with the same conditions as the home owner's condition, namely in the morning, afternoon, evening, and night, which is shown in Table II.

C. Latency Testing

Latency testing is done by measuring the time it takes for the system to perform a face reading, the calculation process starts when the system is on standby until the solenoid functions and the door opens until the door closes again [20]. The test was conducted 20 times, 10 times for homeowners and 10 times for non-homeowners, where the time taken to take the average reading was 5.90 seconds, as shown in Fig. 9.

D. Comparison with other Studies

After being reviewed from previous journals, namely in research [11] using a dataset from AT&T Laboratories Cambridge face dataset, the training process using 400 negative images produces 95% accuracy and with the same dataset in this study, this study tests the accuracy of this method using this dataset with simulation results The same test produces better accuracy results where the accuracy value obtained is 97.83% which can be seen in Table III.

TABLE I. HOMEOWNER TESTING SAMPLES

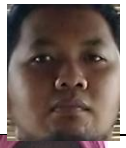
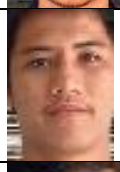
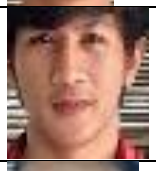
People	Face
	
	
	
	
	

TABLE II. NEIGHBOR'S FACE TESTING SAMPLE

People	Face
	
	
	
	
	

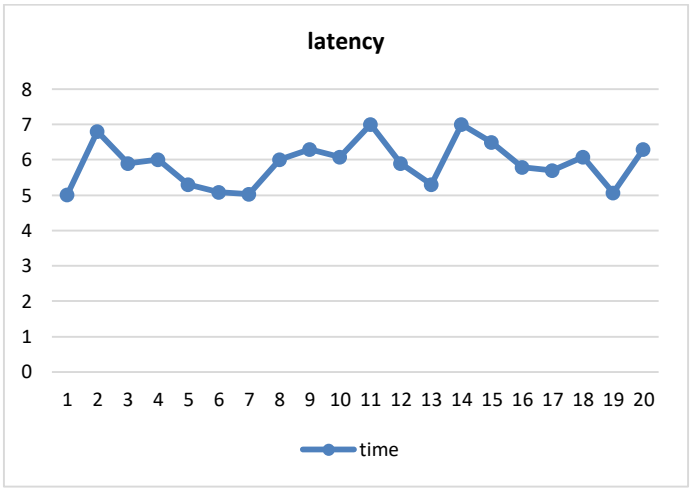


Fig. 9. Latency Testing.

TABLE III. COMPARISON WITH OTHER STUDIES

No	Paper	Method	Accuracy
1.	[11]	OpenCV	95%
2.	propose method	CNN	97.83%

E. Result

After carrying out the above tests, it resulted in a significant development both in terms of the accuracy of the image reading which has increased, and the processing is quite faster. Complete data can be seen in Table IV and Table V.

After testing four times at three different times and based on Table IV and Table V, it can be concluded that this system is running well which has test results in the morning, afternoon, evening, and night with three conditions and it can be concluded in Table VI.

TABLE IV. HOMEOWNER TEST RESULTS

Time	Face	Distance					
		1.5 m		1 m		0.5 m	
		Success	Fail	Success	Fail	Success	Fail
Morning	5	4	1	5	0	5	0
Afternoon	5	4	1	5	0	5	0
Evening	5	4	1	5	0	5	0
Night	5	5	0	5	0	5	0

TABLE V. TEST RESULTS ARE NOT HOMEOWNERS

Time	Face	Distance					
		1.5 m		1 m		0.5 m	
		Success	Fail	Success	Fail	Success	Fail
Morning	5	0	5	0	5	0	5
Afternoon	5	0	5	0	5	0	5
Evening	5	0	5	0	5	0	5
Night	5	0	5	0	5	0	5

TABLE VI. CALCULATION OF ACCURACY VALUE

Total sample: 120		Prediction	
		Negative	Positives
actual	Negative Positive	TN : 60 FN : 0	TP : 57 FP : 3
Akurasi: (TP+TN)/(TP+TN+FP+FN) = 0.975			

IV. CONCLUSION

The research was carried out in three distances, namely, 1.5 meters, 1 meter, and 0.5 meters, and carried out at four times, namely, morning, afternoon, evening, and night, where there was an error three times, namely, at a distance of 1.5 meters where there was excessive light on the background of the standing place. resulting in unclear images, and this research has used a method to increase the accuracy of facial recognition which can reach an accuracy of 97.5%. And also after comparisons with the proprietary OpenCV method [11] using the same dataset and testing stages, this research is a little better, producing an accuracy of 97.83% wherein in the previous research, 95% accuracy was obtained. Further research includes optimizing the facial data augmentation process used as a dataset, better camera resolution, and using the latest Raspberry Pi model to improve computing capabilities.

ACKNOWLEDGEMENT

The publication of this research is supported by Bina Nusantara University.

REFERENCES

[1] Y. D. S. V. D, A. Rakhmansyah, and N. A. Suwastika, "Implementasi Sistem Kunci Pintu Otomatis Untuk Smart Home Menggunakan SMS Gateway," e-Proceeding Eng., vol. 2, no. 2, pp. 6395–6407, 2015.

[2] A. Siswanto, A. Efendi, and A. Yulianti, "Alat Kontrol Akses Pintu Rumah Dengan Teknologi Sidik Jari Di Lingkungan Rumah Pintar Dengan Data Yang Di Enkripsi," J. Penelit. Pos dan Inform., vol. 8, no. 2, p. 97, 2019.

[3] A. Yudhana, "Perancangan pengaman pintu rumah berbasis sidik jari menggunakan metode uml," (Jurnal Teknol. Informasi) Sist. PENGGAJIAN KARYAWAN PADA LKP GRACE Educ. Cent., vol. Vol.1, No., no. 2, p. 12, 2018.

[4] B. Septian, A. Wijayanto, F. Utaminingrum, and I. Arwani, "Face Recognition Untuk Sistem Pengaman Rumah Menggunakan Metode HOG dan KNN Berbasis Embedded," Pengemb. Teknol. Inf. dan Ilmu Komput., vol. 3, no. 3, pp. 2774–2781, 2019.

[5] M. Yan, M. Zhao, Z. Xu, Q. Zhang, G. Wang, and Z. Su, "VarGFaceNet: An Efficient Variable Group Convolutional Neural Network for Lightweight Face Recognition," Iccvw 2019, pp. 2647–2654, 2019.

[6] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," Adv. Neural Inf. Process. Syst., vol. 2, pp. 1097–1105, 2012.

[7] A. Najmurrokhman, K. Kusnandar, A. B. Krama, E. C. Djamal, and R. Rahim, "Development of a secured room access system based on face recognition using Raspberry Pi and Android based smartphone," MATEC Web Conf., vol. 197, pp. 1–6, 2018.

[8] R. A. Isaac, A. Agarwal, and P. Singh, "Face Recognition Security Module using Deep Learning," J. Netw. Commun. Emerg. Technol., vol. 8, no. 10, pp. 10–13, 2018.

[9] J. Nasir and A. A. Ramli, "Design of Door Security System Based on Face Recognition with Arduino," vol. 3, no. 1, pp. 127–131, 2019.

[10] B. M. Susanto, F. E. Purnomo, and M. F. I. Fahmi, "Sistem Keamanan Pintu Berbasis Pengenalan Wajah Menggunakan Metode Fisherface Security System Based On Face Recognition Using Fisherface Method," J. Ilm. Inov., vol. 17, no. 1, p. 10, 2017.

[11] F. Faisal and S. A. Hossain, "Smart security system using face recognition on raspberry Pi," 2019 13th Int. Conf. Software, Knowledge, Inf. Manag. Appl. Ski. 2019, no. August, 2019.

[12] R. Singh, M. Singh, and L. Ragha, "Real-time Face Recognition Under Different Environment," SSRN Electron. J., 2019.

[13] M. F. A. Hassan, A. Hussain, M. H. Muhamad, and Y. Yusof, "Convolution neural network-based action recognition for fall event detection," Int. J. Adv. Trends Comput. Sci. Eng., vol. 8, no. 1.6 Special Issue, 2019.

[14] R. Ranjan, S. Sankaranarayanan, C. D. Castillo, and R. Chellappa, "An All-In-One Convolutional Neural Network for Face Analysis," Proc. - 12th IEEE Int. Conf. Autom. Face Gesture Recognition, FG 2017 - 1st Int. Work. Adapt. Shot Learn. Gesture Underst. Prod. ASL4GUP 2017, Biometrics Wild, Bwild 2017, Heteroge, pp. 17–24, 2017.

[15] Soe Sandar | Saw Aung Nyein Oo, "Development of a Secured Door Lock System Based on Face Recognition using Raspberry Pi and GSM Module," Int. J. Trend Sci. Res. Dev., vol. 3, no. 5, pp. 357–361, 2019.

[16] N. A. Al-Johania and L. A. Elrefaei, "Dorsal hand vein recognition by convolutional neural networks: Feature learning and transfer learning approaches," Int. J. Intell. Eng. Syst., vol. 12, no. 3, 2019.

[17] N. A. Muhammad, A. A. Nasir, Z. Ibrahim, and N. Sabri, "Evaluation of CNN, alexnet and GoogleNet for fruit recognition," Indones. J. Electr. Eng. Comput. Sci., vol. 12, no. 2, pp. 468–475, 2018.

[18] P. Barsocchi, A. Calabrò, E. Ferro, C. Gennaro, E. Marchetti, and C. Vairo, "Boosting a low-cost smart home environment with usage and access control rules," Sensors (Switzerland), vol. 18, no. 6, 2018.

[19] 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," Int. J. Power Electron. Drive Syst., vol. 11, no. 1, pp. 417–424, 2020.

[20] N. Surantha and W. R. Wicaksono, "An IoT based house intruder detection and alert system using histogram of oriented gradients," J. Comput. Sci., vol. 15, no. 8, pp. 1108–1122, 2019.