Face recognition for smart door security access with convolutional neural network method

Dhimas Tribuana, Hazriani, Abdul Latief Arda

Department of Computer System, Faculty of Computer Science, Handayani University Makassar, Makassar, Indonesia

Article Info	ABSTRACT
	This study focuses on enhancing office security through a smart door system, designed to protect sensitive documents and critical data. Emphasizing exclusive access for authorized personnel, the system integrates advanced biometric authentication, predominantly facial recognition. The project's aim is to optimize face recognition using convolutional neural network (CNN) techniques, identifying the best preprocessing methods and hyperparameter settings. A significant aspect of the research involves developing a smart door system with remote authentication and control capabilities via internet connectivity. Employing transfer learning with MobileNet V2, the study presents a compact model tailored for the Raspberry Pi platform. The model utilizes a dataset with five facial recognition classes and an additional class for unknown faces, ensuring a diverse representation. The trained model achieved a high accuracy (0.9729) and low loss (0.09). System evaluation revealed an overall accuracy of 0.96, perfect recall (1.00), and a precision of 0.897. These results demonstrate the system's efficacy in secure access control, making it a viable solution for contemporary office environments.

Corresponding Author:

Abdul Latief Arda
Department of Computer System, Handayani University Makassar
90231, Makassar, South Sulawesi, Indonesia
Email: abdullatief@handayani.ac.id

1. INTRODUCTION

The topic of security is frequently overlooked by the majority of individuals, despite the potential risk of losing important possessions. The door holds significant importance within a building, as it serves a crucial function in facilitating access to various areas or confidential components of the structure. It is imperative that the door be equipped with a dependable security system. In a broad sense, the process of manually operating doors can be mechanized to enhance a range of human endeavors while also incorporating a built-in security mechanism. The primary objective of an office security system incorporating a smart door is to mitigate potential losses, namely those pertaining to the misplacement or compromise of critical papers and valuable data. In addition to this, the advantages of employing a smart door system for organizations that encompass a diverse workforce with varying roles would manifest in its exclusive accessibility to authorized individuals. Contemporary technology continues to rely on fingerprint authentication, a method that presents several challenges. Notably, its applicability is compromised during a pandemic due to the potential for hands to serve as vectors for viral transmission. Moreover, the prevalence of reading failures is a common occurrence due to unclean finger scanning surfaces. Additionally, fingerprint-based systems are susceptible to duplication, necessitate data input on individual machines, and lack remote monitoring and control capabilities [1], [2].

In office settings, particularly within the banking sector, the consequences resulting from inadequate physical access security, such as the door mentioned, encompass significant financial losses stemming from the theft of assets or currency, as well as losses arising from unauthorized access to sensitive data or information. In the banking sector, it is imperative to exercise caution when handling data, ensuring that only authorized staff are granted access and use privileges [3], [4]. The local government of Odo-Otin in Osun State reported an incident involving the perpetration of armed robbery by a group of individuals donning hooded robes, targeting two banks. The attempted intrusion into the bank by the robbers was thwarted due to the presence of a security door at the entry. However, it is worth noting that the criminals successfully managed to extract the funds from the ATM machine situated outside the bank premises [5].

Previous studies have demonstrated the successful performance of a smart door system including facial recognition technology, with an accuracy rate of 94% [6]. The current stage of development for the smart door system outlined in this research involves a prototype that utilizes a solenoid lock mechanism. However, a limitation of this implementation is the inability to integrate a buzzer that would provide an indication in the event of an imperfect lock. The algorithm employed in this work does not incorporate deep learning techniques, and the research conducted does not make use of the internet of things (IoT).

Additionally, there exists an academic study that has developed a sophisticated door system incorporating an alarm and an automated locking mechanism that can be conveniently activated using an android application. The alarm function will be triggered at the opening of the door, whereas the automatic locking mechanism will be engaged after a few minutes of the door being closed. The android application does not display the current status of the door, indicating that it is either locked or inaccessible. Additionally, the program allows for remote locking of the door [7]. This study uses a solenoid key as a prototype and does not incorporate face recognition. It utilizes IoT technology to facilitate the control of door opening and closing exclusively through an android application. The authors aim to develop a smart door system for access security doors by using the convolutional neural network (CNN) approach, as shown by the provided background information. The primary contributions of our proposed approach can be outlined as follows: firstly, the development of a method for processing image datasets in small quantities; secondly, the applicability of this approach in the domain of building security systems, as it effectively reduces facial recognition errors when identifying unfamiliar individuals; and finally, the adaptability of the approach to devices with constrained computational capabilities, such as the Raspberry Pi.

2. RELATED EXISTING REVIEW

The significance of single-board computers, such as the Raspberry Pi, has been amplified with the advancement of technology in the realm of the IoT. Previous research has demonstrated successful utilization of the Raspberry Pi in many applications, such as the development of smart door systems, including facial recognition technology. These studies have achieved commendable results, with a minimum accuracy rate of 94% being attained. Facial biometrics are effectively employed in smart door systems to restrict unauthorized access, enhancing security measures and mitigating the risk of intrusion or tampering [8]-[14]. The door unlocking system's design incorporates face recognition technology through the utilization of the "Doorlock" application loaded on a smartphone, GSM module functionality on the smartphone, and an active raspberry device. The "Doorlock" program is designed to establish an automatic connection with the system and is capable of receiving commands from the user [15]-[17].

Data preprocessing is the process of preparing data for processing using machine learning or deep learning. Before heading to the processing stage, the raw data will be processed first. Some common preprocessing techniques are as follows: grayscale conversion, edge detection, gaussian smoothing, contrast enhancement, binarization, facial cropping, image resizing, and face alignment [18]-[21]. Image preprocessing shortens the processing time and increases the likelihood of a perfect match. Face images are preprocessed to meet feature extraction requirements [22]-[25].

The MobileNet V2 architecture is designed for use in mobile applications as well as computer devices by utilizing the Tensorflow library. MobileNet V2 is a development of the previous version, which also used depthwise separable convolution (DSP) techniques, namely depthwise convolution (DW) and pointwise convolution (PW). The difference in MobileNet V2 compared to the previous version is the addition of bottleneck and shortcut connection features [26], [27]. Currently, there are many studies using MobileNet V2, because this model gives better results with smaller parameters when using transfer learning from MobileNet V2 when compared to regular CNN [28]-[30]. In several studies also compared the VGG16 and MobileNet V2, and MobileNet V2 transfer learning methods had better accuracy [31].

The classic classification paradigm has a closed set configuration, with training and testing classes drawn from the same set (objects to be recognized). This can result in overly confident predictions of a known class, so if the model comes across data from an unknown category, it will recognize it as a known category. The use of an open set is advocated in order to retain classification performance on known classes

while rejecting new ones [32]. Deep neural networks meet object classes that were unknown during training when doing open-set recognition. Existing open-set classifiers differentiate between known and unknown classes by measuring distance in the logit space of a network, assuming that known classes cluster closer to the training data than unknown classes [33].

3. METHOD

The system architecture incorporates Raspberry Pi hardware and the Raspbian operating system, along with several peripheral devices. Notably, a web camera is employed to execute facial recognition tasks, leveraging a Python script developed with the utilization of the OpenCV library. When the Raspberry Pi detects a recognized face, it utilizes the general purpose input output (GPIO) to transmit a signal to the relay, resulting in the activation of the magnetic lock door after a 2-second delay. In order to facilitate manual unlocking from within the room, the installation of a button door release and an emergency break glass mechanism has been implemented to cater to emergency situations. The utilization of the Thingsboard community edition enables the logging of facial recognition activity in real time to the cloud. This functionality further facilitates the online monitoring of devices and the execution of remote-control operations by users. We can see the design of the hardware in Figure 1, wairing from Raspberry Pi connected to relay (ground, electrical voltage 5 volt, and data) and from relay (normaly closed (NC) port in relay) is connected to door EM lock and from relay (COM port) is connected to ground om power supply 12 volt. All of IP camera is connected to Raspberry Pi to capture face image and Raspberry Pi connected to Thingsboard server via WiFi router.
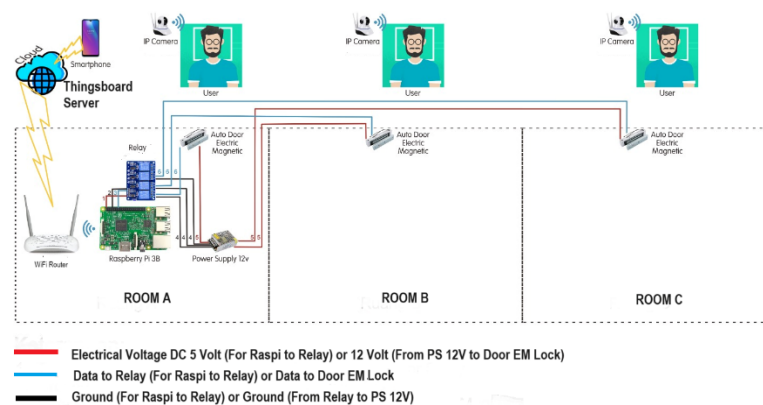

Figure 1. Hardware design

We can see the design of the software in the Figure 2. Access logs record the user and confidence level of facial recognition, as well as the time stamp of entering the room and the length of time activity in the room. The condition of the door lock is visible in a green light, if the green light is lit marks the doorlock in the locking position. There are two buttons respectively functioning "*Buka Pintu*" to open the lock while "*Kunci Pintu*" to lock the door of the room. Communication between the GPIO Raspberry Pi and the Thingsboard Server using the message queuing telemetry transport (MQTT) protocol.

The dataset utilized in this study comprises three distinct types of data. The initial dataset comprises five distinct classes, with each class representing a face to be recognized. The subsequent dataset consists of six classes, encompassing five classes representing recognized faces and one class representing an unidentified face. The objective of this dataset is to facilitate the training of the model to generalize facial recognition beyond the specific five faces of interest. The third dataset employs the same data as the second dataset, but with the additional step of background image removal. This modification aims to direct the model's attention towards learning patterns from the crucial facial components.

The amount of data used will be made in 2 (two) variations, namely 500 and 800 class images, while for unrecognized face classes a 1:6 ratio will be used. For comparison of training (Train) data and test (Val) data, 2 (two) variations will be made, namely 80:20 and 90:10. The hyperparameter tuning that is carried out is on the number of epochs. While the learning rate (LR) used is 0.0001, the batch size (BS) is 32, random state RS) is 42, and the number of epochs to be used is 30, 40, and 50. To choose the best model will be seen from the accuracy and also the loss. The deep learning method used in this study is CNN, which utilizes transfer learning from MobileNet V2.
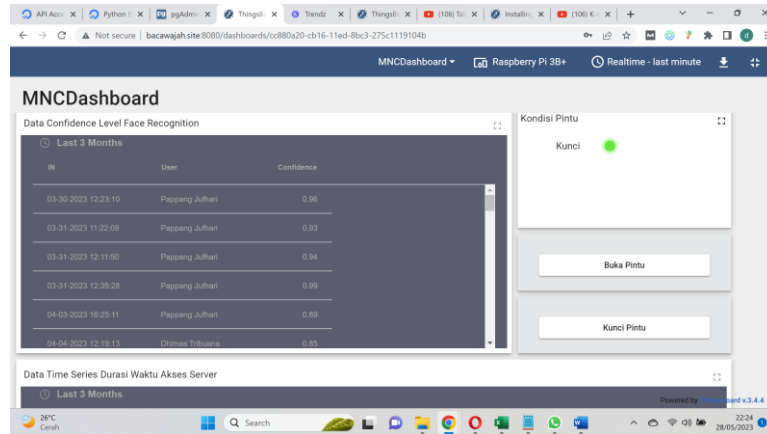
Figure 2. Software design

4. RESULTS AND DISCUSSION

In our study, we explored the impact of various hyperparameters on the model's performance. Table 1 presents the results of this exploration, where we trained the model with five distinct classes. These findings are crucial in understanding how different settings influence accuracy and loss, offering insights into optimal model configuration.

Table 1. Results of training with five classes

Dataset	Train	Val	LR	Epoch	BS	RS	Accuracy	Loss
500	80	20	0.0001	30	32	42	0.9010	0.2911
	80	20	0.0001	40	32	42	0.9340	0.2239
	80	20	0.0001	50	32	42	0.9185	0.2564
	90	10	0.0001	30	32	42	0.9102	0.2806
	90	10	0.0001	40	32	42	0.9471	0.1748
	90	10	0.0001	50	32	42	0.9262	0.2274
800	80	20	0.0001	30	32	42	0.9241	0.2408
	80	20	0.0001	40	32	42	0.9606	0.1470
	80	20	0.0001	50	32	42	0.9722	0.0977
	90	10	0.0001	30	32	42	0.9650	0.1173
	90	10	0.0001	40	32	42	0.9231	0.2460
	90	10	0.0001	50	32	42	0.9361	0.1976

Our research extended to evaluating the model with an additional class, making it six in total. Table 2 illustrates the outcomes of this extended training. This table helps in comparing the model's performance under different class configurations and provides a clear view of scalability and adaptability of our approach.

Table 2. Results of training with six classes

Known	Unknown	Train	Val	LR	Epoch	BS	RS	Accuracy	Loss
5 Class,	3,000	80	20	0.0001	30	32	42	0.9407	0.1793
500/Class		80	20	0.0001	40	32	42	0.9482	0.1649
2500		80	20	0.0001	50	32	42	0.9555	0.1396
Total		90	10	0.0001	30	32	42	0.9343	0.1968
		90	10	0.0001	40	32	42	0.9465	0.1713
		90	10	0.0001	50	32	42	0.9560	0.1341
5 Class,	4,800	80	20	0.0001	30	32	42	0.9491	0.1610
800/Class		80	20	0.0001	40	32	42	0.9568	0.1258
4000		80	20	0.0001	50	32	42	0.9680	0.1005
Total		90	10	0.0001	30	32	42	0.9564	0.1372
		90	10	0.0001	40	32	42	0.9644	0.1115
		90	10	0.0001	50	32	42	0.9693	0.0951

An important aspect of our research was to assess the effect of background noise on model accuracy. In Table 3, we present the results obtained from training the model with six classes, but without

any background. These results underscore the importance of background in model training and its impact on the effectiveness of face recognition.

Table 3. Results of training with six classes and without background

Known	Unknown	Train	Val	LR	Epoch	BS	RS	Accuracy	Loss
5 Class,	3,000	80	20	0.0001	30	32	42	0.9411	0.1872
500 per		80	20	0.0001	40	32	42	0.9441	0.1732
Class 2500		80	20	0.0001	50	32	42	0.9636	0.1160
Total		90	10	0.0001	30	32	42	0.9487	0.1786
		90	10	0.0001	40	32	42	0.9535	0.1513
		90	10	0.0001	50	32	42	0.9606	0.1387
5 Class,	4,800	80	20	0.0001	30	32	42	0.9615	0.1301
800 per		80	20	0.0001	40	32	42	0.9652	0.1121
Class 4000		80	20	0.0001	50	32	42	0.9729	0.0900
Total		90	10	0.0001	30	32	42	0.9601	0.1241
		90	10	0.0001	40	32	42	0.9697	0.0996
		90	10	0.0001	50	32	42	0.9675	0.1027

It can be seen from the Tables 1-3 that the results of the highest accuracy and the smallest loss are in the model with six classes and without background with 80% training data and 20% testing with epoch 50, batch size 32, and a learning rate of 0.0001 in Table 3. In Figure 3, which is shown the accuracy and loss metrics for training outcomes are shown graphically for three different cases: 5 classes, 6 classes, and 6 classes without background. The evaluation of the system as a whole was conducted in three distinct stages. In the initial phase, a sample size of 20 individuals was used to evaluate the performance of facial recognition technology. This sample consisted of 5 individuals who were registered in the system with recognizable labels, 5 individuals who were registered in the system with unknown labels, and 10 individuals whose facial data had not been previously included in the dataset. Among the sample of ten individuals, it was observed that two individuals exhibited facial similarities, which can be attributed to their close familial relationship as siblings. This observation was made in order to evaluate the efficacy of the implemented method. Table 4 is pivotal in showcasing the practical application of our system. It provides the results of the face recognition system in real-world scenarios, emphasizing the system's ability to distinguish between registered and unregistered faces, which is vital for security applications.

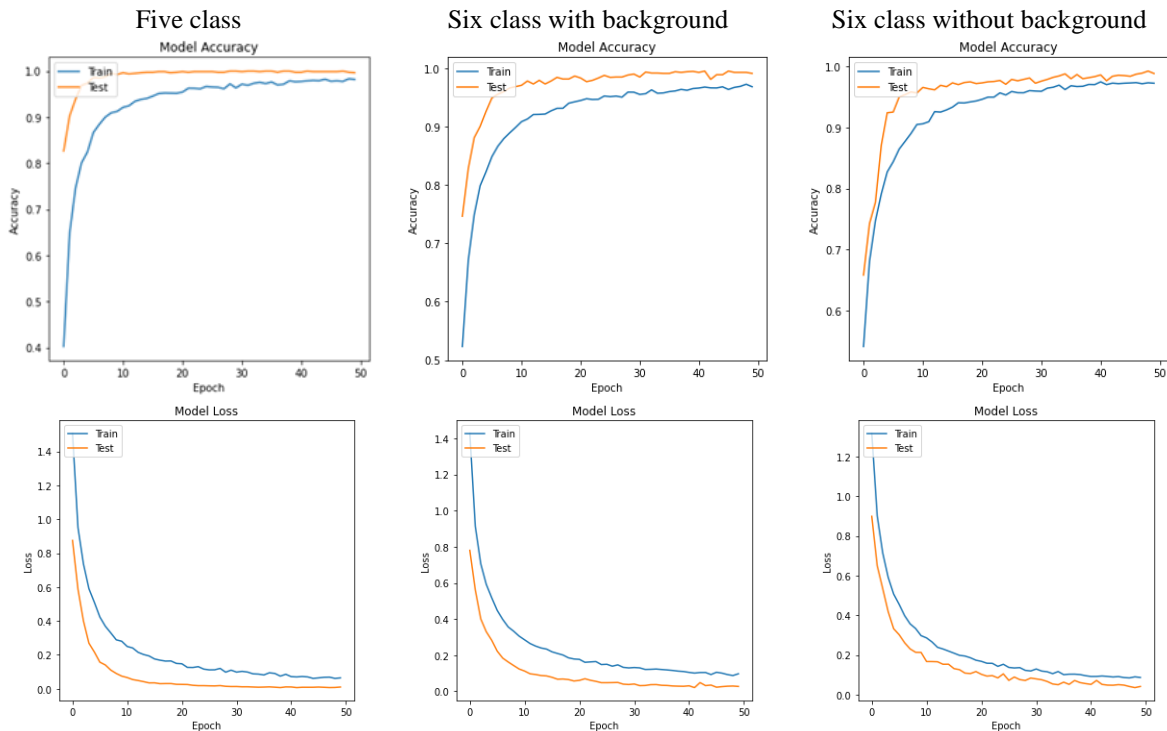| Five class	Six class with background	Six class without background

Figure 3. Accuracy dan loss dataset graphics 800 80:20 50 epoch

The evaluation of real-time face recognition involves the implementation of direct recognition for a duration of three minutes. Subsequently, the system classifies the recognition outcome by calculating the average of the most recent 20 frames of facial images belonging to the same class. This process applies to recognized classes ranging from class 0 to class 4. If the mean value is equal to or more than 0.90, or if the mean value is less than 0.90, it will be classified as unrecognized.

The previously mentioned test reveals the occurrence of a single failure in the process of facial recognition. The classification of this event as a failure stems from the examination of the facial recognition logs, which revealed that out of a total of 150 records pertaining to sample number 2, 74 records (equivalent to 49% of the total) were classified as recognized, while 76 records (equivalent to 51% of the total) were classified as unrecognized. In the case of sample number 3, the system successfully identified it. However, upon analyzing the log data of facial recognition results, it was observed that out of a total of 143 records for sample number 3, 87 records (61% of the total) were classified as recognized, while 56 records (39% of the total) fell into the unrecognized category. To demonstrate the system's responsiveness, we conducted a no-touch push button test. The results, as shown in Table 5, indicate the system's reliability in responding to automated triggers, a feature essential for touchless security systems.

Table 4. Face recognition system result

No	Recorded in dataset	Face recognized		Door lock opened		Access recorded in clouds		Explanation
		Test result	Expected result	Test result	Expected result	Test result	Expected result	
1	Yes	Recognized	Recognized	Opened	Opened	Recorded	Recorded	Class 0
2	Yes	Not recognized	Recognized	Not opened	Opened	Not recorded	Recorded	Class 1
3	Yes	Recognized	Recognized	Opened	Opened	Recorded	Recorded	Class 2
4	Yes	Recognized	Recognized	Opened	Opened	Recorded	Recorded	Class 3
5	Yes	Recognized	Recognized	Opened	Opened	Recorded	Recorded	Class 4
6	Yes	Not recognized	Not recognized	Not opened	Not opened	Not recognized	Not recognized	Class 5 unknown
7	Yes	Not recognized	Not recognized	Not opened	Not opened	Not recognized	Not recognized	Class 5 unknown
8	Yes	Not recognized	Not recognized	Not opened	Not opened	Not recognized	Not recognized	Class 5 unknown
9	Yes	Not recognized	Not recognized	Not opened	Not opened	Not recognized	Not recognized	Class 5 unknown
10	Yes	Not recognized	Not recognized	Not opened	Not opened	Not recognized	Not recognized	Class 5 unknown
11	No	Not recognized	Not recognized	Not opened	Not opened	Not recognized	Not recognized	Not in dataset
12	No	Not recognized	Not recognized	Not Opened	Not opened	Not recognized	Not recognized	Not in dataset
13	No	Not recognized	Not recognized	Not opened	Not opened	Not recognized	Not recognized	Not in dataset
14	No	Not recognized	Not recognized	Not opened	Not opened	Not recognized	Not recognized	Not in dataset
15	No	Not recognized	Not recognized	Not opened	Not opened	Not recognized	Not recognized	Not in dataset
16	No	Not recognized	Not recognized	Not opened	Not opened	Not recognized	Not recorded	Not in dataset
17	No	Not recognized	Not recognized	Not opened	Not opened	Not recognized	Not recognized	Not in dataset
18	No	Not recognized	Not recognized	Not opened	Not opened	Not recognized	Not recognized	Not in dataset
19	No	Not recognized	Not recognized	Not opened	Not opened	Not recorded	Not recognized	Siblings of rec number 3
20	No	Not recognized	Not recognized	Not opened	Not opened	Not recorded	Not recognized	Siblings of rec number 4

Table 5. No-touch push button test result

No	No push button		Access recorded in clouds	
	Test result	Expected result	Test result	Expected result
1	Opened	Opened	Recorded	Recorded
2	Opened	Opened	Recorded	Recorded
3	Opened	Opened	Recorded	Recorded
4	Opened	Opened	Recorded	Recorded
5	Opened	Opened	Recorded	Recorded

Testing in stage 3 tests the platform on the cloud server with one try to see the performance of the platform used. Cloud-based operations of our system were also rigorously tested. In Table 6, we present the results from these platform tests. This table highlights the system's efficiency and reliability when operating in a cloud-based environment, which is critical for scalability and remote access.

Table 6. Platform test result

No	Registered in system	System proccess							
		Login to *Clouds*		Monitoring door condition		Open door lock from *Clouds*		Lock door from *Clouds*	
		Test result	Expected result	Test result	Expected result	Test result	Expected result	Test result	Expected result
1	Yes	Success	Success	Success	Success	Success	Success	Success	Success

To analyze the test results, the confusion matrix is used so that the accuracy of the system can be known. Assessing the accuracy of our facial recognition system is crucial. Table 7 features the confusion matrix, a standard tool in machine learning for evaluating classification models. This table offers an in-depth look at the precision and recall rates of our system, vital for understanding its practical effectiveness.

Table 7. Confusion matrix

		Test result	
		TRUE	FALSE
Prediction	TRUE	26	3
	FALSE	0	45

$$Recall = \frac{TP}{(TP+FN)} = \frac{26}{(26+0)} = \frac{26}{26} = 1 \tag{1}$$

$$Precision = \frac{TP}{(TP+FP)} = \frac{26}{(26+3)} = \frac{26}{29} = 0.897 \tag{2}$$

$$Accuracy = \frac{(TP+TN)}{(TP+TN+FP+FN)} = \frac{(26+45)}{(26+45+3+0)} = \frac{71}{74} = 0.96 \tag{3}$$

Where TP is true positive, TN is true negative, FP is false positive, and FN is false negative. Considering the system's primary objective of functioning as a security system, it is imperative to minimize instances of false negatives. Hence, recollection serves as the primary metric employed for assessment. The results of the confusion matrix computation indicate that the current system has a high level of accuracy and successfully reduces the occurrence of false negatives because of its excellent recall values. Compared to the accuracy obtained in the study entitled "smart door system using face recognition based on Raspberry Pi" by Azmi *et al*. [6], our study yielded better results than the accuracy and recall that were more suitable for security doors.

Comparing the results of "Face Recognition-based Door Unlocking System using Raspberry Pi" by Vamsi and Sai [11]. Our research can be implemented on more than one door in a building and also provide a more complete and user-friendly report using the Thingsboard IoT platform. Comparing the results of real-time face mask detection using the same algorithm as MobilenetV2 in the study "Real-Time Face Mask Detection Using Mobilenetv2 Algorithm" by Kanna and Kumar [27]. Our research provides better accuracy, precision, and recall.

5.   CONCLUSION

The study determined that among the various models examined, MobileNet V2 with an input image size of 128 pixels, a pool size of 4,4, a density of 256, a dropout of 0.5, a learning rate of 0.0001, a batch size of 32, 800 images per class for the datasets, 4800 images for the unknown class, and an 80:20 split for training and testing datasets exhibited the highest level of optimality with respect to the dataset used in the study. This model achieved an accuracy of 0.9729 and a loss of 0.09. The present study has successfully developed a smart door system that uses the CNN technique for face recognition in order to enhance the security of access doors.

This system is capable of automatically locking and unlocking doors upon successful face recognition and can also transmit access logs and door lock status to a cloud server. Based on the comprehensive system testing conducted across three distinct stages, namely face recognition testing, no touch button testing, and cloud server testing, it can be deduced that the system exhibits satisfactory performance. The system demonstrates a commendable accuracy level of 0.96, ensuring a high degree of precision in its operations. Additionally, the system achieves a recall rate of 1.00, indicating its ability to accurately identify and retrieve relevant information. Moreover, the system exhibits a precision value of 0.897, further affirming its capability to effectively discern and deliver accurate results.

REFERENCES

[1]   R. Ullah *et al.*, "A Real-Time Framework for Human Face Detection and Recognition in CCTV Images," *Mathematical Problems in Engineering*, vol. 2022, pp. 1–12, 2022, doi: 10.1155/2022/3276704.

[2]   L. Alzubaidi *et al.*, "Review of deep learning: concepts, CNN architectures, challenges, applications, future directions," *Journal of Big Data*, vol. 8, no. 1, Dec. 2021, doi: 10.1186/s40537-021-00444-8.

[3]   S. Yedulapuram, R. Arabelli, K. Mahender, and C. Sidhardha, "Automatic Door Lock System by Face Recognition," in *IOP Conference Series: Materials Science and Engineering 981, IOP Publishing Ltd*, Dec. 2020, pp. 1–6, doi: 10.1088/1757-899X/981/3/032036.

[4]   J. Zeng, X. Qiu, and S. Shi, "Image processing effects on the deep face recognition system," *Mathematical Biosciences and Engineering*, vol. 18, no. 2, pp. 1187–1200, 2021, doi: 10.3934/MBE.2021064.

[5]   S. Obarayese, "Osun robbery: Security door saves bank as robbers break ATM [VIDEO]," *dailypost.ng, Odo-Otin*, Mar. 2021. [Online]. Available: https://dailypost.ng/2021/03/11/breaking-armed-robbers-attack-bank-in-osun/. (accessed: Feb. 26, 2023).

[6]   F. Azmi, I. Fawwaz, and R. Anugrahwaty, "Smart Door System using Face Recognition Based on Raspberry Pi," *JURNAL INFOKUM*, vol. 10, no. 1, pp. 360–369, 2021.

[7]   L. Rai, Z. Wang, A. Rodrigo, Z. Deng, and H. Liu, "Software development framework for real-time face detection and recognition in mobile devices," *International Journal of Interactive Mobile Technologies*, vol. 14, no. 4, pp. 103–120, 2020, doi: 10.3991/IJIM.V14I04.12077.

[8]   S. Roy, M. N. Uddin, M. J. Kabir, and M. Z. Haque, "Design and Implementation of the Smart Door Lock System with Face Recognition Method using the Linux Platform Raspberry Pi," *IJCSN-International Journal of Computer Science and Network*, vol. 7, no. 6, pp. 382–388, 2018.

[9]   A. D. Deshmukh, M. G. Nakrani, D. L. Bhuyar, and U. B. Shinde, "Face Recognition Using OpenCv Based on IoT for Smart Door," *Sustainable Computing in Science, Technology & Management*, pp. 1066–1073, 2019, doi: 10.2139/ssrn.3356332.

[10]   J. Linggarjati, "Raspberry Pi Zero Door Locking System with Face Recognition using CNN (Convolutional Neural Network) and Fingerprint Sensor," in *Proceedings of the 3rd South American International Industrial Engineering and Operations Management Conference*, 2022, pp. 1147–1152.

[11]   T. K. Vamsi and K. C. Sai, "Face recognition based door unlocking system using Raspberry Pi," *International Journal of Advance Research, Ideas and Innovations in Technology (IJARIIT)*, vol. 5, no. 2, pp. 1320–1324, 2019.

[12]   S. Patankar, V. Dubey, R. Bishnoi, R. Porwal, U. Tomar, and R. Jain, "Mask Detection and Face Recognition System Using Tensor Flow, Keras and Mobile Net," *International Journal of Scientific Research & Engineering Trends*, vol. 7, no. 3, pp. 1753–1758, 2021.

[13]   R. Iyer, P. S. Ringe, R. V. Iyer, and K. P. Bhensdadiya, "Comparison of YOLOv3, YOLOv5s and MobileNet-SSD V2 for Real-Time Mask Detection," *International Journal of Research in Engineering and Technology (IRJET)*, vol. 8, no. 7, pp. 1156–1160, 2021.

[14]   B. Nethravathi, S. S. Sinchana, and H. N. P. Kumar, "Advanced Face Recognition Based Door Unlock System Using Arduino & MATLAB," *International Journal of Internet of Things and Web Services*, vol. 5, pp. 1–6, 2020.

[15]   C. K. Gomathy, K. Keerthi, and N. Pavithra, "Smart Door with Facial Recognition," *International Research Journal of Engineering and Technology (IRJET)*, vol. 8, no. 10, pp. 471–474, 2021.

[16]   D. Kurnia, I. H. Muis, S. Riyadi, A. A. Supriyanto, and F. S. Hadisantoso, "AI-based face recognition system with telegram notification for room security on raspberry PI," *Jurnal Polimesin*, vol. 21, no. 3, pp. 297–303, 2023, doi: 10.30811/jpl.v21i3.3534.

[17]   S. Sandar, S. Aung, and N. Oo, "Development of a Secured Door Lock System Based on Face Recognition using Raspberry Pi and GSM Module," *International Journal of Trend in Scientific Research and Development (IJTSRD)*, vol. 3, no. 5, pp. 357–361, 2019, doi: 10.31142/ijtsrd25280.

[18]   B. Qin, L. Liang, J. Wu, Q. Quan, Z. Wang, and D. Li, "Automatic identification of down syndrome using facial images with deep convolutional neural network," *Diagnostics*, vol. 10, no. 7, Jul. 2020, doi: 10.3390/diagnostics10070487.

[19]   I. Ahmad, I. Moon, and S. J. Shin, "Color-to-grayscale algorithms effect on edge detection — A comparative study," in *2018 International Conference on Electronics, Information, and Communication (ICEIC)*, 2018, pp. 1–4, doi: 10.23919/ELINFOCOM.2018.8330719.

[20]   T. Ayyavoo and J. J. Suseela, "Illumination pre-processing method for face recognition using 2D DWT and CLAHE," in *IET Biometrics, Institution of Engineering and Technology*, Jul. 2018, pp. 380–390, doi: 10.1049/iet-bmt.2016.0092.

[21]   M. Heidari, S. Mirniaharikandehei, A. Z. Khuzani, G. Danala, Y. Qiu, and B. Zheng, "Improving the performance of CNN to predict the likelihood of COVID-19 using chest X-ray images with preprocessing algorithms," *International Journal of Medical Informatics*, vol. 144, Dec. 2020, doi: 10.1016/j.ijmedinf.2020.104284.

[22]   T. Hussain *et al.*, "Internet of Things with Deep Learning-Based Face Recognition Approach for Authentication in Control Medical Systems," *Computational and Mathematical Methods in Medicine*, vol. 2022, 2022, doi: 10.1155/2022/5137513.

[23]   D. S. AbdELminaam, A. M. Almansori, M. Taha, and E. Badr, "A deep facial recognition system using computational intelligent algorithms," *PLoS One*, vol. 15, no. 12 December, Dec. 2020, doi: 10.1371/journal.pone.0242269.

[24]   X. Liu, Y. Zou, H. Kuang, and X. Ma, "Face image age estimation based on data augmentation and lightweight convolutional neural network," *Symmetry (Basel)*, vol. 12, no. 1, 2020, doi: 10.3390/SYM12010146.

[25]   D. Tribuana, Hazriani, and A. L. Arda, "Image Preprocessing Approaches Toward Better Learning Performance with CNN," *JOURNAL RESTI (Rekayasa Sistem Teknologi Informasi)*, vol. 8, no. 1, pp. 1–9, 2024, doi: 10.29207/resti.v8i1.5417.

[26]   F. M. Javed *et al.*, "A Transfer Learning Approach for Face Recognition using Average Pooling and MobileNetV2," in *Congress on Intelligent Systems: Proceedings of CIS 202*, vol. 114, pp. 531–541, 2022, doi: 10.1007/978-981-16-9416-5_38.

[27] R. R. Kanna and M. P. Kumar, "Real-time face mask detection using mobilenetv2 algorithm," *Recent Trends in Computational Intelligence and Its Application*, 2023, pp. 215–221.

[28] A. H. I. Al-Rammahi, "Face mask recognition system using MobileNetV2 with optimization function," *Applied Artificial Intelligence*, vol. 36, no. 1, 2022, doi: 10.1080/08839514.2022.2145638.

[29] B. A. Kumar and M. Bansal, "Face Mask Detection on Photo and Real-Time Video Images Using Caffe-MobileNetV2 Transfer Learning," *Applied Sciences (Switzerland)*, vol. 13, no. 2, Jan. 2023, doi: 10.3390/app13020935.

[30] L. Hu and Q. Ge, "Automatic facial expression recognition based on MobileNetV2 in Real-time," in *Journal of Physics: Conference Series, Institute of Physics Publishing*, Jun. 2020, doi: 10.1088/1742-6596/1549/2/022136.

[31] F. D. Adhinata, N. A. F. Tanjung, W. Widayat, G. R. Pasfica, and F. R. Satura, "Comparative Study of VGG16 and MobileNetV2 for Masked Face Recognition," *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika*, vol. 7, no. 2, p. 230, Jul. 2021, doi: 10.26555/jiteki.v7i2.20758.

[32] D.-W. Zhou, H.-J. Ye, and D.-C. Zhan, "Learning Placeholders for Open-Set Recognition," in *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Mar. 2021, pp. 4399–4408.

[33] D. Miller, N. Sünderhauf, M. Milford, and F. Dayoub, "Class Anchor Clustering: A Loss for Distance-based Open Set Recognition," in *IEEE Winter Conference on Applications of Computer Vision (WACV)*, 2021, pp. 3569–3577.

BIOGRAPHIES OF AUTHORS

Dhimas Tribuana received a Bachelor's degree at Hasanuddin University in 2002, a master's degree in Magister Management at STIE Artha Bodhi Iswara Surabaya in 2023 and a master's degree in Computer System at Handayani University Makassar in 2023. Currently, he is working in the private sector. His research interests include machine learning, applied networks, the internet of things, and embedded systems. He can be contacted at email: d.tribuana@gmail.com.

Hazriani obtained a Bachelor of Computer Systems from STMIK Handayani in 2001, a Master of Informatics Engineering at Hasanuddin University in 2007, and a Doctor of Advanced Information Technology at Kyushu University in 2018. Since 2005 until now, her status has been that of a permanent lecturer at LLDIKTI Wil IX. She also worked at Handayani University in Makassar. She can be contacted at email: hazriani@handayani.ac.id.

Abdul Latief Arda received a Bachelor in Computer Science at STMIK Handayani in 2000, a Master's degree at the University Hasanuddin in 2008, a Master's degree in Computer System at Handayani University Makassar in 2015, and the Doctoral Degrees at Universitas Negeri Makassar in 2017. Since 2005 until now, the status concerned is that of a permanent lecturer at LLDIKTI WIL. IX, employed at Handayani University Makassar. He can be contacted at email: abdullatief@handayani.ac.id.