Accredited Ranking SINTA 2
Decree of the Director General of Higher Education, Research, and Technology, No. 158/E/KPT/2021
Validity period from Volume 5 Number 2 of 2021 to Volume 10 Number 1 of 2026

Published online on: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 7 No. 6 (2022) 1387 - 1393 ISSN Media Electronic: 2580-0760

Face Recognition-Based Room Access Security System Prototype using A Deep Learning Algorithm

Immanuel Morries Pohan[1], Suci Dwijayanti[2*], Bhakti Yudho Suprapto[3], Hera Hikmarika[4], Hermawati[5]
[1,2,3,4,5]Department of Electrical Engineering, Universitas Sriwijaya, Palembang, Indonesia
[1,2]Control and Computational Intelligent System (CoCIS) Research Group, Universitas Sriwijaya, Palembang, Indonesia
[1]morispohan740@gmail.com, [2]sucidwijayanti@ft.unsri.ac.id, [3]bhakti@ft.unsri.ac.id, [4]herahikmarika@ft.unsri.ac.id,
[5]hermawati@ft.unsri.ac.id

Abstract

Currently, security systems use conventional security methods, which provide low levels of security. Therefore, some organizations now use biometric-based security systems, which include facial recognition-based systems. However, processing facial data requires computationally intensive feature extraction, making real-time implementation difficult. Additionally, most data used are from public datasets. In this study, we developed a facial recognition-based security system for door access using a convolutional neural network (CNN) for real-time face recognition. We used the primary data of 102 students. The datasets include two settings (i.e., outdoor and indoor) and three facial expressions (i.e., normal, smiley, and sleepy), amounting to 3060 samples. The training was performed using three deep-learning CNN architectures: Xception (model X), VGG16 (model Y), and modified VGG16 (model Z). The best accuracy results of the three training architectures of model X, model Y, and model Z for 100 epochs are 0.9469, 0.9971, and 1, respectively. In tests conducted on the 102 test data points, models X, Y, and Z achieved accuracies of 50%, 97.05%, and 97.05%, respectively. These results indicate that the modified VGG16 (model Z) is the best for real-time testing. In real-time tests conducted on the security system prototype with 15 respondents, the resulting accuracy of model Z is 86.6%. This demonstrates that the modified VGG16 model has excellent recognition capabilities and can be implemented as a room access security system.

Keywords: *security system; convolutional neural network (CNN;, face recognition; biometric; VGG16*

1. Introduction

Computer technologies, which are rapidly and continuously developing, are very important in various applications, including room access [1]. Security is an important aspect that must be considered by a company, especially for rooms where important files are stored.

However, companies employ security systems that are conventionally designed and based on mechanical principles. Conventional security systems have many weaknesses, such as low levels of security, that allow doors to be easily breached. For example, the use of a manipulated paper clip, the duplication of keys, and the loss of keys, which can be misused if they fall into the wrong hands, are all instances of security risks. In addition to their low level of security, conventional door security systems are considered less effective and efficient. This is because opening a lock requires two steps: inserting the key into the keyhole and turning it in a certain direction, making the process of opening a conventional door slow. Another factor that makes conventional door security systems inefficient is the use of the lock-and-hole system, which can be damaged in regular use.

The security system required for a room to be secure should be effective, efficient, and provide a high level of security. With the advent of the modernization of security systems, modern security systems combine several components of conventional and current electronic technologies. There are three types of modern security systems: radio frequency identification (RFID), password identification numbers (PIN), and biometrics. RFID is a security system that uses small electronic devices consisting of chips and antennas. The working principle of RFID is to transmit data using radio waves to allow transmission without touching. However, RFID has a weakness: if the identification card is lost, the door cannot be accessed and opened. On the other hand, PIN is a security system that uses a combination of numbers or letters that are verified by a data validation machine; however, the combination of numbers or characters can be forgotten. Therefore, to

Accepted: 21-08-2023 | Received in revised: 21-12-2023 | Published: 26-12-2023

avoid these disadvantages, a biometric approach is needed to replace conventional methods of security.

The biometric approach involves the use of biometric features to identify, measure, and validate individuals [2]. They are permanent, unique, and can be used to distinguish one person from another. Biometric systems can be implemented in two distinct modes: authentication and enrollment [3]. Therefore, biometrics are presently the best option for security systems. There are several types of biometrics, such as human physical identification and fingerprint, retina, iris, face, signature, and keystroke recognition [4].

Some of the methods that have been frequently proposed for system security are RFID-based systems and fingerprint scanners. However, although they are accurate, these systems are unhygienic, and RFID systems cannot avoid proxies [5]. On the other hand, with the rapid development of technology, facial recognition has become easier compared to the other forms of human body recognition, such as those based on fingerprint, iris, and DNA. This is because facial recognition does not require mandatory participation and can solve security problems without affecting the normal lives of people. It has advantages in terms of low cost, high user acceptance, and high reliability, and has broad applications in identification, security monitoring, human–computer interaction, and other fields [6]. By using an actual face, the process of opening a door becomes more efficient and optimized because the person only needs to look at a camera for the system to determine if they are permitted to enter [7]. Furthermore, although other biometric techniques, such as fingerprint reading, are more accurate than facial recognition, facial recognition methods are more advantageous because there are numerous techniques available in the literature that can be used to identify the shapes of faces [8], [9]. In the realm of artificial intelligence (AI), computer vision is generally used in face recognition. Vision is a fundamental element of intelligence and includes coordination, memory, retrieval, reasoning, estimation, and recognition, among others [10]. The conventional face recognition process involves four steps: face detection, face alignment, feature extraction, and face classification. The most important step is feature extraction, which directly affects recognition accuracy [6]. Face recognition technology simulates the ability of the human eye to identify facial expressions. This is achieved through the use of computer intelligence to generate a collection of faces. Features are extracted from the collected faces and then stored as templates.

In the previous work of Ku and Dong [6], a multi-task cascaded convolutional neural network (MTCNN) was used for face detection, and a convolutional neural network (CNN) was used for face recognition learning. The accuracy reached 98.53% with a computation time of 6 m/s. However, the method was not implemented in real time and still used secondary datasets, such as the CASIA-WebFace dataset, which has 50000 images, and labeled faces in the wild (LFW) dataset, which has 13233 images. Another study used an MTCNN for face recognition with multiple cameras [11].

Meanwhile, Dwijayanti et al. [12] used the dataset obtained via the capture of 52 facial patterns with four different facial expressions and different light intensities in outdoor conditions using a camera. Their results showed that the CNN can recognize both faces and facial expressions. However, this study focused on simulation cases that were not implemented in real applications.

Gupta et al. [13] conducted an additional study on face recognition using speeded up robust features (SURF) and scale-invariant feature transform (SIFT) for feature extraction. Their study demonstrated that through the integration of a decision tree and random forest classifier features, accuracy can be enhanced compared to when using only one feature. However, the system developed in their study had several flaws, such as the computations in the image management process were more expensive because of feature extraction and were not applied to room security. Additionally, their system was implemented on a secondary dataset. In another study by Ahmed and Rasheed [14], attendance was implemented in real-time based on facial recognition. Principal component analysis (PCA) was used for feature extraction. Meanwhile, [15] used back propagation neural network and [16] utilized a genetic algorithm for face recognition.

Unfortunately, feature extraction, which was the focus of these studies [7], [13], [17], requires complex computations and has a high probability of data loss during transformation. Therefore, in this study, we developed a facial recognition security system based on the CNN algorithm as it achieves very good results [18], is efficient and reliable, and can be implemented in real time for face recognition. In addition, except for Gupta et al. [13], few studies have investigated deep-learning models for the Raspberry Pi implementation of door security systems. Most of the data used in related research were from either public source, such as Kaggle, or private sources.

Consequently, this study aims to develop a facial recognition-based door security system using a CNN algorithm implemented under real-time conditions. The contributions of this study are: Implementation of a facial recognition system for room access based on deep learning; Acquisition of an Indonesian dataset; Comparative study of three architectures for the implementation of a security system using deep learning.

DOI: https://doi.org/10.29207/resti.v7i6.5376

This paper is organized as: Section 1 presents the introduction of the study. Section 2 describes the methodology, including the process for obtaining the data. Section 3 provides the results and discussions. Finally, Section 4 presents the conclusions of this study.

2. Research Methods

2.1 System Design

This study was conducted to increase security at the Control and Robotics Laboratory of the Electrical Engineering Department, Faculty of Engineering, Universitas Sriwijaya, Indonesia. The workflow of the system built in this study was in accordance with its functions and objectives. Figure 1 shows a flowchart of the system.

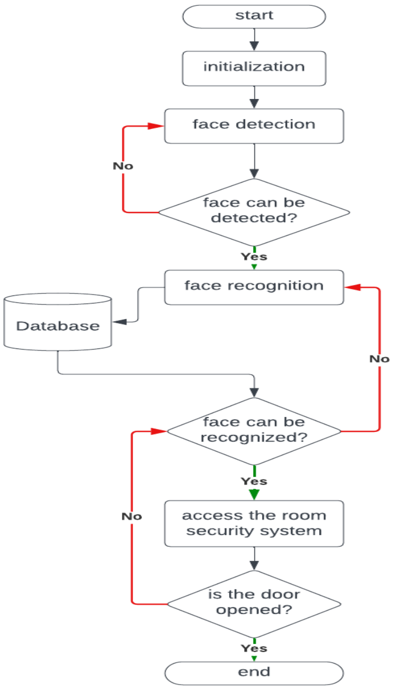


Figure 1. System Flowchart

Herein, a deep learning algorithm based on a convolutional neural network (CNN) with three architectures, i.e., Xception, VGG16, and Modified VGG16, was employed. Several data collection and processing steps were performed before the training process. Data processing included face augmenting, cropping, and resizing. Subsequently, the data or face images were used to train the aforementioned three architectures, which were then tested using test data and in real time using a webcam.

2.2 Data Collection

The primary data for this study were used as input for CNN training. These data included the faces of 102 individuals, comprising Sriwijaya University students, laboratory employees, and laboratory lecturers. Each class consisted of 24 face samples for the training; three validation data points; and three test data points. The primary data were collected offline using a Logitech C992 webcam at a 1080p/30–720p/60 fps resolution. The images were captured manually using a camera application in a basic laboratory of electrical engineering control systems. Facial images were captured under two distinct settings, i.e., indoor and outdoor environments. Participants were instructed to obtain images exhibiting three different facial expressions: flat, smiling, and sleepy.

2.3 Data Processing

The collected image data were then preprocessed. The first step was to crop the faces using the Python programming language. An example of face cropping is shown in Figure 2. The preprocessed image was then saved in JPEG format.

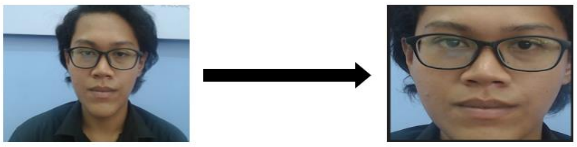


Figure 2. Face Crop Preprocessing

After cropping was applied to all the data, the next step was to resize the images from their original dimensions of 555 × 554 pixels to the desired dimensions of 224 × 224 pixels. This step was performed to reduce the amount of data that entered the CNN architecture during the training process. Subsequently, data augmentations were applied to obtain variations in the images. These augmentations included rescale=1/255, shear_range=0.2, zoom_range=0.2, and horizontal_flip=True. Examples of the results of the augmentation process are shown in Figure 3.

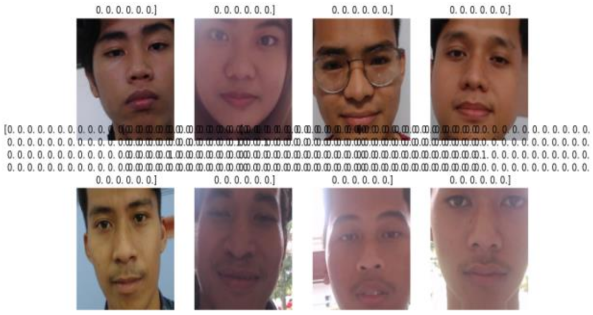


Figure 3. Face Image Augmentation Results

2.4 Convolutional Neural Network (CNN)

A CNN is a popular algorithm for image classification and recognition. It is a derivative algorithm of deep learning developed from a multilayer perceptron (MLP) that is designed to process data in two-dimensional form, such as images or sounds. A CNN takes the values of image pixels in vector/matrix form as input, passes them through a sequence of layers, and outputs a classification for the image [19].

DOI: https://doi.org/10.29207/resti.v7i6.5376

Layers of a CNN model include convolutional, fully connected, and pooling layers. The convolutional layers comprise the first two layers, which are followed by a normalization layer and maximum pooling layer. The subsequent layer is the fully connected layer, which is then followed by the output layer [16].

2.5 Comparison of Three CNN Architectures

In this study, three CNN architecture models were developed to determine which architecture had the most accurate performance in face recognition. These architectures included Xception, VGG16, and a self-modified model, referred to as models X, Y, and Z, respectively.

Xception (Model X), which was developed in 2017 by the Google research team using a CNN model, is an inception model that uses deeply separated convolutional layers to improve network efficiency and accuracy. The Xception architecture consists of 36 convolutional layers [20]. Its architecture is illustrated in Figure 4.

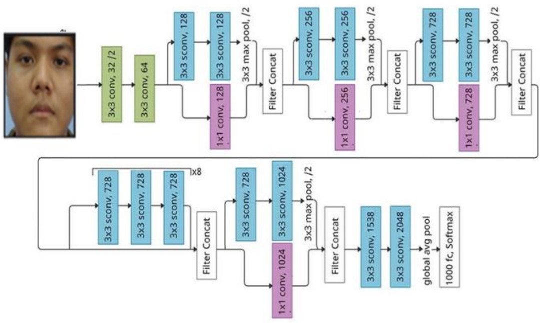


Figure 4. Xception Architecture

VGG16 (Model Y), which was developed by the Visual Geometry Group at Oxford University in 2014 [21] , consists of 16 layers, 13 convolutional layers, and three fully connected layers. Each convolutional layer consists of 3 × 3 filters with a different number of filters in each layer. The max pooling layer follows after two convolutional layers and consists of three fully connected layers at the end of the architecture, of which the first two layers each consist of 4096 neurons. The last layer contains the number of neurons corresponding to the number of classes in the dataset. The VGG16 architecture is visualized in Figure 5.

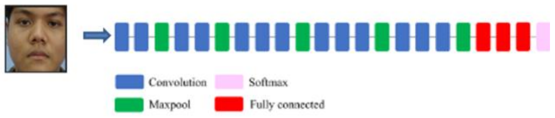


Figure 5. VGG16 Architecture

In this study, a new CNN model was developed as a modification of the VGG16 architecture. The modifications included pruning the last four layers, learning rate, batch size, dense layer, drop out after the dense layer, 3 × 3 convolutional layer, and batch normalization, as shown in Figure 6. Modified VGG16 (Model Z) was modified by the addition of one convolutional layer, one dropout layer following a dense layer with 256 neurons, and batch normalization.

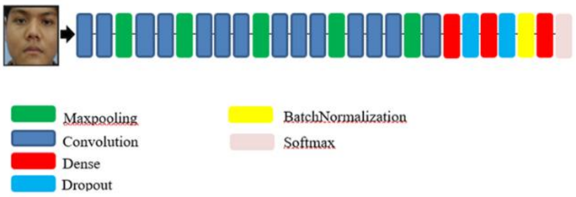


Figure 6. Modified VGG16 Architecture

3. Results and Discussions

3.1 Training Results for Three CNN Architectures

The training in this study was performed using the transfer learning method, adapting the existing architecture known as the Keras library to the needs of the existing 102 classes and retraining it with ImageNet weights to obtain visual knowledge trained and implemented on existing datasets.

The three different architectures, namely models X, Y, and Z, were trained such that each architecture had the same hyperparameters, with a learning rate value of 0.0001, batch size of 32, Adam optimizer, and the same numbers of epochs of 50 and 100. The accuracy results for the three architectures after 50 epochs are shown in Figure 7. From the graph, we can observe that with training, model X obtained an initial accuracy of 0.02 and, when trained for 50 epochs, ended at 0.82. By comparison, model Y achieved an initial accuracy of 0.0849 and ended with an accuracy of 0.9857, whereas model Z achieved an initial accuracy of 0.1221 and ended at 0.9967.

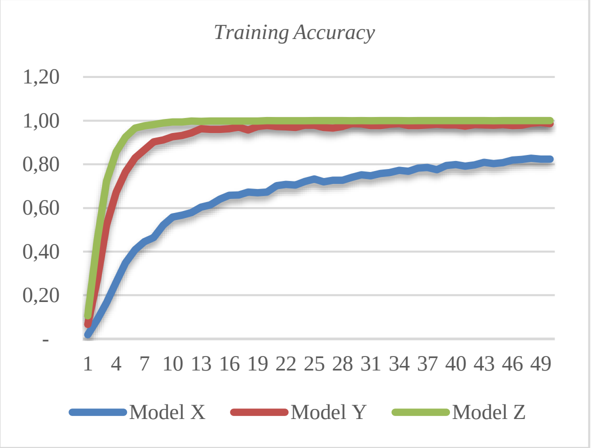


Figure 7. Face Recognition Training Accuracy for 50 Epochs

Training was then continued with the number of epochs increased to 100 to obtain a comparison and determine if the accuracy could be increased. A graph for 100 epochs is shown in Figure 8. Model X achieved an

DOI: https://doi.org/10.29207/resti.v7i6.5376

initial accuracy of 0.027 and ended at 0.9469; model Y achieved an initial accuracy of 0.0906 and ended at 0.9935; and model Z achieved an initial accuracy of 0.1213 and ended at 0.9980.

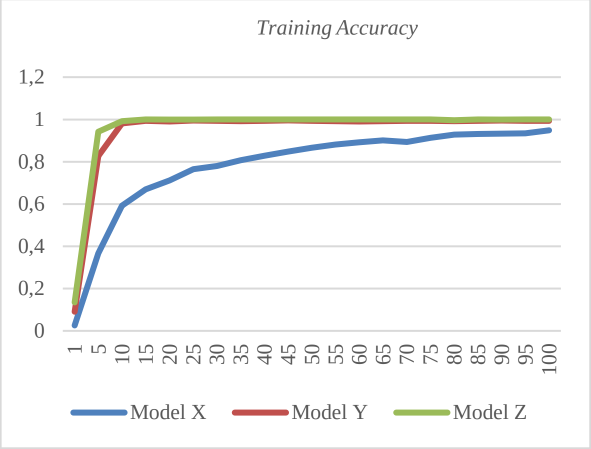


Figure 8. Face Recognition Training Accuracy for 100 Epochs

From Figures 7 and 8, it can be concluded that as the number of epochs used in the training process increases, the accuracy moves closer to one. Furthermore, based on the obtained data, the increase in the accuracy value becomes smaller or insignificant as the accuracy approaches one.

A comparison of the best training accuracies of models X, Y, and Z with epoch variations of 50 and 100 is shown in Table 1. From these data, it can be concluded that for all three architectures, the best accuracies were obtained at 100 epochs. It can also be observed that the Z model attained the best accuracy over all epochs, with a value of 1, compared to those of the two other architectures. By comparison, models X and Y attained accuracy values of 0.9469 and 0.9971, respectively.

Table 1. Comparison of Training Accuracies of Three Architectures in Face Recognition

Epoch	Best Training Accuracy		
	Model X	Model Y	Model Z
50	0.8276	0.9918	0.9996
100	0.9469	0.9971	1

3.2 Testing Using Test Data

The model resulting from the training process was then evaluated for its performance. Given that each architecture was trained to recognize the face dataset used in the training process, the tests were performed using face data not used in the training process. The results of these tests, performed on 102 samples from 102 classes, were: The accuracies of the Xception architecture trained for 50 and 100 epochs were 18.62% and 50%, respectively; The accuracies of the VGG16 architecture trained for 50 and 100 epochs were 97.05% and 97.05%, respectively; The accuracies of the modified VGG16 architecture trained for 50 and 100 epochs were 99.01% and 97.05%, respectively.

3.3 Prototype of Biometric Security System Box

To function as a room security system, the prototype requires the integration of coding, components, and a microcontroller (Arduino) connected to a laptop via serial communication. This enables the prototype to function as the driver of a door lock solenoid connected to the relay module of a 12V adapter, allowing the door to be opened and closed. The prototype also requires a 16 × 2 LCD equipped with an I2C module for feedback from the system in the form of predicted information about the face name and status of the solenoid. All the aforementioned components are connected through a breadboard as a terminal to facilitate wiring. The prototype and its wiring circuit are shown in Figure 9.

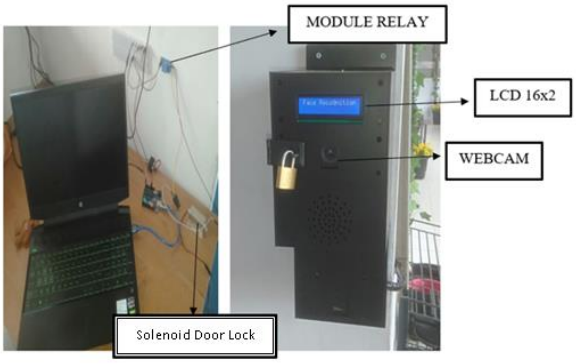


Figure 9. Prototype Face Recognition-Based Security System

3.4 Real-Time Online Testing

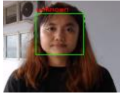
The offline face recognition tests were conducted on test data that included 13 classes with a 70% confidence threshold. For each class, the X, Y, and Z architectures were subjected to a training process for 50 and 100 epochs, as listed in Table 1. During offline testing, model Z trained for 50 epochs achieved the highest accuracy of 99.01%. Model Z trained for 100 epochs then followed. The worst accuracy, which was 18.62%, was exhibited by model X trained for 50 epochs. By comparison, model Y, trained for 50 and 100 epochs, achieved an accuracy of 97.05%. However, although the accuracy of model X was the lowest, the length of its training time was the fastest compared to those of the other two models at their highest numbers of layers. By contrast, model Y required the longest training time. Thus, model Z was chosen for the real-time online testing.

The real-time online testing was performed using samples that were in the dataset and samples that were not in the dataset, classified as unknown. The samples were positioned in front of the camera, which had been embedded in the prototype of the room security system. The door lock was opened if the face was recognized as one of the persons in the dataset. On the other hand, the door lock remained closed if the person was not recognized or was recognized as unknown.

DOI: https://doi.org/10.29207/resti.v7i6.5376

As shown in Table 2, the security system based on model Z was able to recognize the faces of people that were included in the dataset. The system was also capable of recognizing “unknown” persons who were not included in the dataset. However, errors still occurred in recognizing some of the samples, as shown with samples 8 and 10. Specifically, each person was recognized as someone else. This could have been due to the similarity of features carried by the person with those of other individuals.

Table 2. Tests on 13 Face Samples

No	Sample	Face image	Model Z 100 Epochs
1	Sample 1		Recognized
2	Sample 2		Recognized
3	Sample 3 (out of the dataset)		Recognized as unknown
4	Sample 4		Recognized
5	Sample 5 (out of the dataset)		Recognized as unknown
6	Sample 6		Recognized
7	Sample 7		Recognized
8	Sample 8		Unrecognized
9	Sample 9 (out of the dataset)		Recognized as unknown
10	Sample 10		Recognized
11	Sample 11		Recognized
12	Sample 12 (out of the dataset)		Recognized as unknown
13	Sample 13 (out of the dataset)		Recognized as unknown
14	Sample 14		Unrecognized
15	Sample 15 (out of the dataset)		Recognized as unknown
Accuracy	86.6 %		

The performance exhibited by model Z, when tested with a real-time webcam in a basic laboratory for electrical engineering control systems, revealed weaknesses and failures in predicting the faces of several respondents. This is because the performance loss of the model remained high, as depicted in Figure 10, and thus the model was prone to overfitting. Overfitting is a condition wherein the model is unable to generalize for datasets on which it has never been trained, consequently performing inadequately in real-time image prediction testing. With 50 epochs of training, the test loss value in the model evaluation was 1.1860. With 100 epochs of training, the test loss in the model evaluation was 1.2945.

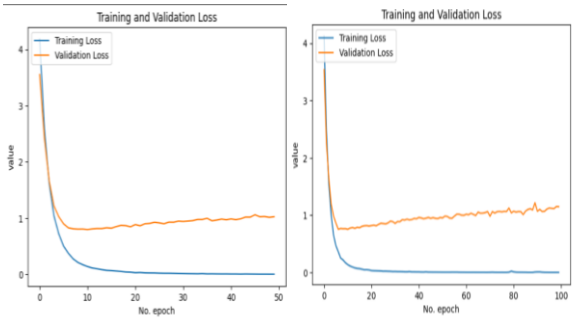


Figure 10. Loss Graph of Z Model for 50 and 100 Epochs

Several attempts were made to reduce overfitting, including the addition of L2 regularization, early stopping to prevent the model from being overtrained, and the addition of the learning reduction parameter. The results are shown in Figure 11. According to this graph, the results did not deteriorate substantially, as indicated by a test loss value of 1.0791, and training was terminated at epoch five.

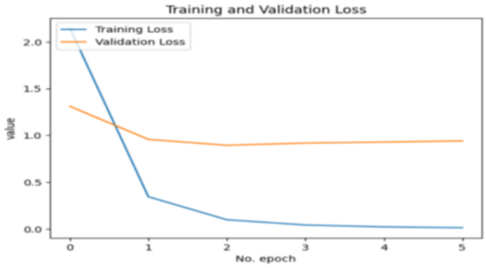


Figure 11. Loss Graph of Z Model After Regularization

4. Conclusion

The implementation of a convolutional neural network with VGG16 architecture (model Y) and modification of VGG16 architecture (model Z) to recognize faces and open a door has been successful, as evidenced by accuracy graphs and test tables, which reveal an accuracy of 86.6% (model Z). However, further development is needed to obtain more optimal and robust models. The best model among the three CNN architectures used in the prototype of the facial recognition-based security system was the Z model. Its accuracy rates in tests on 102 test data points as input were 99.01% (50 epochs) and 97.05% (100 epochs). Furthermore, its accuracy rate in real-time tests with a webcam as the input was 86.6% (100 epochs) for nine database-registered participants and six unregistered

DOI: https://doi.org/10.29207/resti.v7i6.5376

participants. However, the fastest time for the training process was demonstrated by model X, followed by models Z and Y. After a second modification to reduce the overfitting of the training process, no significant reduction in the loss value was observed.

Acknowledgments

This study was funded by DIPA of the Public Service Agency of Universitas Sriwijaya, 2023. No SP DIPA-023.17.2.677515/2023, on November 30, 2022. In accordance with the rector's Decree Number 0118/UN9.3.1/SK/2023, dated April 18, 2023.

References

[1] Andreas, C. R. Aldawira, H. W. Putra, N. Hanafiah, S. Surjarwo, and A. Wibisurya, "Door security system for home monitoring based on ESp32," *Procedia Comput. Sci.*, vol. 157, pp. 673–682, 2019, doi: 10.1016/j.procs.2019.08.218.

[2] S. Dargan and M. Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities," *Expert Syst. Appl.*, vol. 143, p. 113114, 2020, doi: 10.1016/j.eswa.2019.113114.

[3] S. A. Abdulrahman and B. Alhayani, "A comprehensive survey on the biometric systems based on physiological and behavioural characteristics," *Mater. Today Proc.*, vol. 80, no. July, pp. 2642–2646, 2023, doi: 10.1016/j.matpr.2021.07.005.

[4] Z. Rui and Z. Yan, "A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification," *IEEE Access*, vol. 7, pp. 5994–6009, 2019, doi: 10.1109/ACCESS.2018.2889996.

[5] V. Seelam, A. K. Penugonda, B. Pavan Kalyan, M. Bindu Priya, and M. Durga Prakash, "Smart attendance using deep learning and computer vision," *Mater. Today Proc.*, vol. 46, pp. 4091–4094, 2020, doi: 10.1016/j.matpr.2021.02.625.

[6] H. Ku and W. Dong, "Face Recognition Based on MTCNN and Convolutional Neural Network," *Front. Signal Process.*, vol. 4, no. 1, pp. 37–42, 2020, doi: 10.22606/fsp.2020.41006.

[7] D. A. R. Wati and D. Abadianto, "Design of face detection and recognition system for smart home security application," *Proc. - 2017 2nd Int. Conf. Inf. Technol. Inf. Syst. Electr. Eng. ICITISEE 2017*, vol. 2018-Janua, pp. 342–347, 2018, doi: 10.1109/ICITISEE.2017.8285524.

[8] M. Sajjad *et al.*, "Raspberry Pi assisted face recognition framework for enhanced law-enforcement services in smart cities," *Futur. Gener. Comput. Syst.*, vol. 108, pp. 995–1007, 2020, doi: 10.1016/j.future.2017.11.013.

[9] A. A. Sukmandhani and I. Sutedja, "Face Recognition Method for Online Exams," *Proc. 2019 Int. Conf. Inf. Manag. Technol. ICIMTech 2019*, vol. 1, no. August, pp. 175–179, 2019, doi: 10.1109/ICIMTech.2019.8843831.

[10] K. H. Teoh, R. C. Ismail, S. Z. M. Naziri, R. Hussin, M. N. M. Isa, and M. S. S. M. Basir, "Face Recognition and Identification using Deep Learning Approach," *J. Phys. Conf. Ser.*, vol. 1755, no. 1, 2021, doi: 10.1088/1742-6596/1755/1/012006.

[11] E. Jose, M. Greeshma, T. P. Mithun Haridas, and M. H. Supriya, "Face Recognition based Surveillance System Using FaceNet and MTCNN on Jetson TX2," *2019 5th Int. Conf. Adv. Comput. Commun. Syst. ICACCS 2019*, no. March, pp. 608–613, 2019, doi 10.1109/ICACCS.2019.8728466.

[12] S. Dwijayanti, R. R. Abdillah, H. Hikmarika, Hermawati, Z. Husin, and B. Y. Suprapto, "Facial Expression Recognition and Face Recognition Using a Convolutional Neural Network," in *2020 3rd International Seminar on Research of Information Technology and Intelligent Systems, ISRITI 2020*, Dec. 2020, pp. 621–626. doi: 10.1109/ISRITI51436.2020.9315513.

[13] S. Gupta, K. Thakur, and M. Kumar, "2D-human face recognition using SIFT and SURF descriptors of face's feature regions," *Vis. Comput.*, vol. 37, no. 3, pp. 447–456, 2021, doi: 10.1007/s00371-020-01814-8.

[14] H. M. Ahmed and R. T. Rasheed, "A Raspberry PI Real-Time Identification System on Face Recognition," *Proc. 2020 1st Inf. Technol. to Enhanc. E-Learning other Appl. Conf. IT-ELA 2020*, pp. 89–93, 2020, doi: 10.1109/IT-ELA50150.2020.9253107.

[15] Z. Yu, F. Liu, R. Liao, Y. Wang, H. Feng, and X. Zhu, "Improvement of Face Recognition Algorithm Based on Neural Network," *Proc. - 10th Int. Conf. Meas. Technol. Mechatronics Autom. ICMTMA 2018*, vol. 2018-January, pp. 229–234, 2018, doi: 10.1109/ICMTMA.2018.00062.

[16] H. Zhi and S. Liu, "Face recognition based on genetic algorithm," *J. Vis. Commun. Image Represent.*, vol. 58, pp. 495–502, 2019, doi: 10.1016/j.jvcir.2018.12.012.

[17] M. H. Wan and Z. H. Lai, "Generalized Discriminant Local Median Preserving Projections (GDLMPP) for Face Recognition," *Neural Process. Lett.*, vol. 49, no. 3, pp. 951–963, 2019, doi: 10.1007/s11063-018-9840-6.

[18] M. Owais, A. A. Jalal, M. M. Hassan, and A. Shaikh, "Facial Recognition based Attendance System Using CNN and Raspberry Pi," *4th Int. Symp. Multidiscip. Stud. Innov. Technol. ISMSIT 2020 - Proc.*, 2020, doi: 10.1109/ISMSIT50672.2020.9254300.

[19] S. A. Dar and S. Palanivel, "Neural Networks (CNNs) and Vgg on Real Time Face Recognition System," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 9, pp. 1809–1822, 2021.

[20] K. R. Avery *et al.*, "Fatigue Behavior of Stainless Steel Sheet Specimens at Extremely High Temperatures," *SAE Int. J. Mater. Manuf.*, vol. 7, no. 3, pp. 560–566, 2014, doi: 10.4271/2014-01-0975.

[21] K. Simonyan and A. Zisserman, "Very Deep Convolutional Networks for Large-Scale Image Recognition," Sep. 2014, [Online]. Available: http://arxiv.org/abs/1409.1556

DOI: https://doi.org/10.29207/resti.v7i6.5376