Design and Build a Door Security System Using a Raspberry-Pi based Liveness Detection

Reinaldo Riswanto Saputra[1], Abdul Rasyid[2], Mohammad Abdullah Anshori[3*], Adzikirani Adzikirani[4]

1,4 Digital Telecommunication Network Study Program,
Electrical Engineering Departement, State Polytechnic of Malang, Malang City, 65141, Indonesia
2,3 Telecommunication Engineering Network Study Program,
Electrical Engineering Departement, State Polytechnic of Malang, Malang City, 65141, Indonesia

[1]aldoaxel88@gmail.com, [2]abdul.rasyid@polinema.ac.id, [3]moh.abdullah@polinema.ac.id, [4]adzikirani@polinema.ac.id

***Abstract*— Various problems with the door threaten the security of the room owner such as theft. Many are done by thieves to carry out their actions. In the data from the National Police Center, there are 158,267 cases of theft with aggravation, the act of theft with aggravation is included in the theft at home or in a boarding room. This causes the need for a door security system. The purpose of this research is to make door security using Convolutional Neural Network (CNN) as accuracy detection and face prediction with Liveness Detection as real face detection or not. The overall test results of facial accuracy obtained based on epoch 25, epoch 50, epoch 100, epoch 150, epoch 200, and epoch 250. With average accuracy test results of 95.1% at epoch 25, 98.2% at epoch 50, 97.9% at epoch 100, 98.6% at epoch 150, 96.3% at epoch 200, and 95.7% at epoch 250. Prediction results were 95.3% at epoch 25, 98.1% at epoch 50, 97.7% at epoch 100, 98.6% at epoch 150, 96.3% at epoch 200, and 95.7% at epoch 250. Overall, the use of Liveness Detection and Convolutional Neural Network (CNN) technology in the door security system can improve security with more than 95% accuracy. This system also provides convenience for users to monitor the state of the door remotely through Android applications, so that it can be relied upon to improve room efficiency and security.**

Keywords*— *Android, Convolutional Neural Network, Face Recognition, Firebase, Security.

I. INTRODUCTION

Room security is a crucial concern due to the high incidence of theft occurring in private spaces such as boarding houses, rented rooms, and residential buildings. Weak door security systems are often exploited by criminals to gain unauthorized access and steal valuables, particularly when occupants are absent. This condition highlights the urgent need for more reliable and intelligent door security systems [1].

Conventional security methods, such as mechanical door locks and door bars, are still widely used because of their simplicity and affordability. However, these methods have major weaknesses, including susceptibility to key duplication, forced entry, and the absence of monitoring capabilities. As a result, traditional mechanical security systems are no longer sufficient to address modern security challenges [2], [3].

Electronic access control systems were developed to improve security reliability, including password-based authentication using numeric or alphanumeric inputs. Nevertheless, such systems are prone to input errors, password leakage, and brute-force attacks, making them vulnerable in real-world applications [4]. To overcome these limitations, biometric-based authentication systems have been introduced, utilizing unique physiological characteristics such as fingerprints, iris patterns, and facial features [5].

Among various biometric modalities, face recognition has gained significant attention due to its non-contact nature, ease of use, and suitability for real-time implementation. Facial features are difficult to replicate compared to conventional credentials, making face recognition an effective solution for access control and security systems [6], [7]. Face recognition has been widely applied in surveillance systems, identity verification, smart homes, and human–computer interaction applications [8].

Despite its advantages, conventional face recognition systems are vulnerable to spoofing attacks, such as the use of printed photos, video replays, or images displayed on digital screens. These attacks can deceive systems that rely solely on facial appearance, leading to unauthorized access [9]. To address this vulnerability, liveness detection techniques have been developed to distinguish real human faces from fake representations by analyzing facial texture, motion, and depth information [10], [11].

Recent advancements in deep learning, particularly Convolutional Neural Networks (CNNs), have significantly improved the performance of face recognition and liveness detection systems. CNNs are capable of automatically extracting discriminative facial features and have demonstrated superior accuracy compared to traditional methods such as Eigenface, Fisherface, and Local Binary Patterns (LBP) [12]–[14]. Deep learning frameworks such as TensorFlow provide efficient tools for implementing and training CNN-based models [15].

In embedded system applications, Raspberry Pi has become a popular platform for implementing intelligent security systems due to its compact size, low power consumption, and support for various peripherals such as webcams, RFID modules, and wireless communication interfaces [16], [17]. Several studies have successfully implemented Raspberry Pi-based face recognition systems for door security applications,

*Corresponding author

demonstrating promising results in controlled environments [18], [19].

However, many existing Raspberry Pi-based door security systems still rely solely on face recognition without integrating liveness detection, which leaves them vulnerable to spoofing attacks. Therefore, this research proposes a Door Security System Design Using Raspberry Pi Based Liveness Detection, which integrates CNN-based face recognition with liveness detection to enhance authentication reliability. The proposed system combines a webcam for facial acquisition, RFID as secondary authentication, and an Android application for monitoring and data management, aiming to provide a more robust and practical door security solution [20]. Although numerous studies have implemented face recognition for door security systems, many of them rely solely on facial appearance without considering liveness detection, making them vulnerable to spoofing attacks. In addition, several existing systems focus only on desktop-based processing or lack real-time monitoring capabilities. This research addresses these limitations by integrating CNN-based face recognition with liveness detection on a Raspberry Pi platform, combined with RFID authentication and Android-based monitoring. This integration provides a more secure, practical, and deployable solution for real-world room security applications

II. METHOD

The method section provides detail of research conducted.

A. System Design

The proposed door security system is designed by integrating hardware, software, and application components to perform face recognition with liveness detection as the primary authentication method, as shown in Fig. 1. The system architecture consists of a Raspberry Pi as the main controller, a webcam for facial image acquisition, an RFID module as secondary authentication, and an Android application for monitoring and data management.

The overall system workflow begins with face detection using a webcam connected to the Raspberry Pi. The captured facial image is processed using a Convolutional Neural Network (CNN) model to perform face recognition and liveness detection. If the detected face is classified as a live and authorized user, the system proceeds to the RFID authentication stage. When both authentication stages are successfully verified, the Raspberry Pi activates a relay to unlock the solenoid door lock automatically. If authentication fails, the system records the facial image and sends the data to Firebase for monitoring through the Android application.

B. Hardware Design

The hardware design consists of several interconnected components installed in a protective enclosure. Raspberry Pi 4 Model B is used as the main processing unit due to its capability to handle image processing and deep learning inference. A USB webcam is utilized to capture real-time facial images of users standing in front of the door.

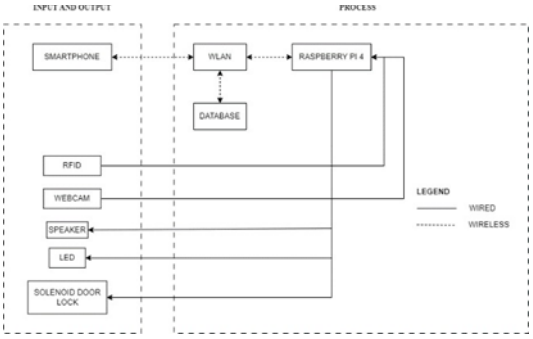

Figure 1. Block Diagram of the Proposed Door Security System

An RFID reader module functions as a secondary layer of security after successful face recognition and liveness detection. Visual and audio feedback is provided through LED indicators and a speaker to notify users whether access is accepted or rejected. A relay module is used to control the solenoid door lock, allowing the door to open automatically when authentication is successful, as shown in Fig. 2.

All hardware components are powered through a regulated power supply to ensure stable operation during continuous use.

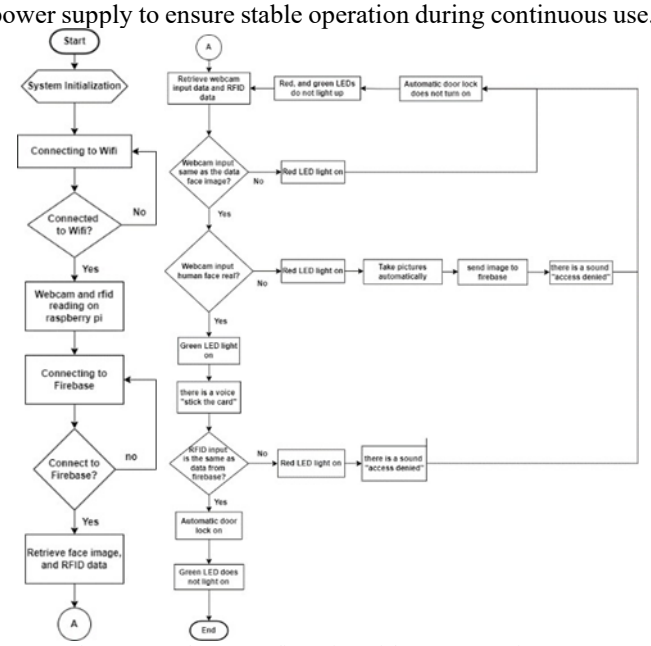

Figure 2. Hardware Configuration of the Door Security System

C. Software Design

The software system is developed using Python programming language on the Raspberry Pi platform. OpenCV is used for real-time image acquisition and face detection, while TensorFlow is employed to implement the CNN-based face recognition and liveness detection model. The trained model is loaded into the Raspberry Pi to perform inference on incoming facial images captured by the webcam.

The software workflow includes image preprocessing, face detection, liveness detection, and face recognition. If the system detects a fake face or an unregistered user, the access request is rejected, and the facial image is automatically stored in Firebase for further monitoring. Authorized access triggers

the relay to unlock the door and provides audio and visual feedback

The dataset used in this research consists of facial images collected from ten individuals. Each subject was captured using a webcam under indoor lighting conditions with variations in facial pose and expression. The collected images were divided into training and validation datasets to ensure reliable model evaluation. Image preprocessing was applied before training to normalize input size and improve model performance. The CNN model used in this research consists of convolutional layers followed by pooling layers and fully connected layers for classification. The ReLU activation function is applied in convolutional layers, while Softmax is used in the output layer. The model is trained using the Adam optimizer with categorical cross-entropy loss. Training was conducted using multiple epoch values (25, 50, 100, 150, 200, and 250) to analyze the effect of training duration on model performance, as shown in Fig. 3.

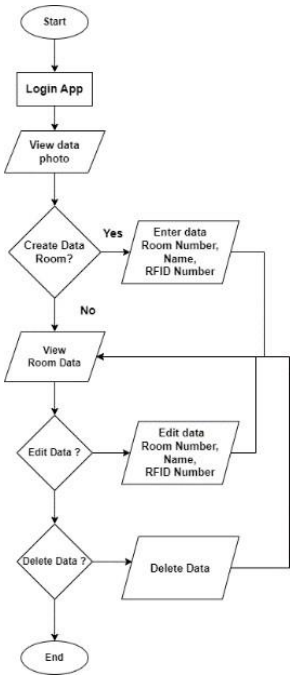

Figure 3. Flowchart of the Android Application System

D. Liveness Detection and Face Recognition Process

Liveness detection is applied to distinguish between real human faces and spoofing attempts such as printed images or digital displays. The CNN model is trained using facial image datasets containing both live and spoof samples. Feature extraction is automatically performed by convolutional layers, followed by classification layers to determine whether the detected face is live or fake.

Face recognition is performed after liveness verification by comparing the extracted facial features with stored facial data. Only faces that pass both liveness detection and recognition stages are allowed to proceed to RFID authentication.

E. Application Design

The Android application is designed to provide a user interface for monitoring system activity and managing user data. The application retrieves data from Firebase, including captured facial images, user identity information, and access logs.

The application provides features such as viewing image data lists, adding new user data, updating room information, and deleting user records. This allows room owners or administrators to manage access permissions efficiently and monitor security events remotely.

F. System Flowchart

The system flowchart describes the operational sequence of the door security system. The process starts when a user stands in front of the webcam. The system captures the facial image and performs face detection. If a face is detected, liveness detection and face recognition are executed. If the authentication result is valid, the system proceeds to RFID verification. Successful verification unlocks the door automatically, while failure at any stage results in access rejection and data recording, as shown in Fig. 4.

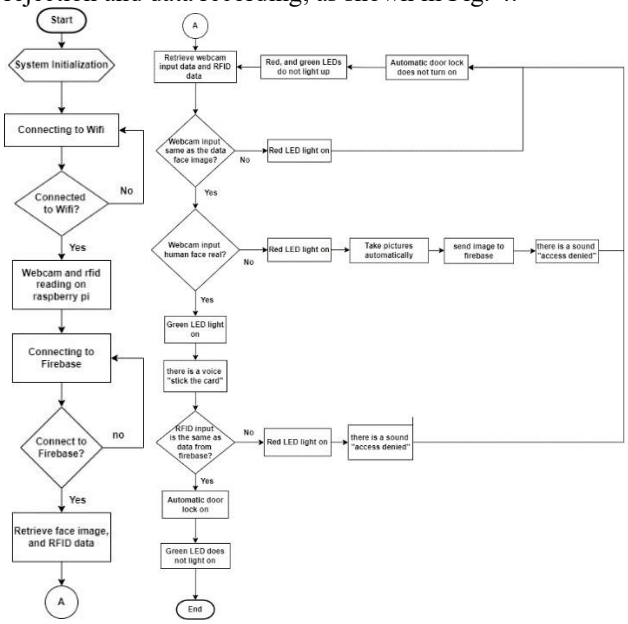

Figure 4. Flowchart of the Door Security System Operation

G. CNN Architecture and Training Parameters

The face recognition and liveness detection model in this research is implemented using a Convolutional Neural Network (CNN) architecture due to its ability to automatically extract discriminative features from facial images. The CNN model consists of several convolutional layers for feature extraction, followed by pooling layers to reduce spatial dimensions and fully connected layers for classification. Rectified Linear Unit (ReLU) is used as the activation function in the convolutional layers to improve non-linearity, while the Softmax function is applied in the output layer to classify facial identities.

Before training, all facial images are resized and normalized to ensure uniform input dimensions and stable training

performance. The training process uses the Adam optimizer with categorical cross-entropy as the loss function. To evaluate the effect of training duration on model performance, multiple epoch values are applied, namely 25, 50, 100, 150, 200, and 250 epochs. This variation allows analysis of accuracy trends and identification of the optimal training configuration.

The trained CNN model is then deployed on the Raspberry Pi for real-time inference. By evaluating multiple epoch settings, this research ensures that the selected model achieves high accuracy while avoiding overfitting, making it suitable for practical implementation in a real-time door security system.

H. Performance Evaluation Metrics

The performance of the proposed door security system is evaluated using several classification metrics, namely accuracy, precision, recall, and F1-score. These metrics are derived from the confusion matrix to provide a comprehensive evaluation of the CNN-based face recognition and liveness detection model.

Accuracy is used to measure the overall correctness of the classification results by comparing the number of correctly classified samples with the total number of samples. Precision represents the ratio of correctly predicted positive samples to all predicted positive samples, indicating the system's ability to minimize false acceptance. Recall measures the ratio of correctly predicted positive samples to all actual positive samples, reflecting the system's capability to recognize authorized users. The F1-score is calculated as the harmonic mean of precision and recall to provide a balanced evaluation of the classification performance.

By using these metrics, the evaluation does not rely solely on accuracy but also considers the reliability and robustness of the system in real-world security scenarios. This approach ensures that the proposed system achieves high recognition performance while minimizing both false acceptance and false rejection rates.

III. RESULTS AND DISCUSSION

This section presents the results of the proposed door security system implementation and discusses the performance of the hardware, software, and face recognition with liveness detection.

A. Hardware Implementation Results

The hardware implementation of the door security system was successfully assembled and operated according to the system design. All components, including the Raspberry Pi 4 Model B, webcam, RFID reader, relay module, solenoid door lock, LED indicators, and speaker, functioned properly during testing.

The webcam was able to capture facial images clearly under normal indoor lighting conditions. The relay module successfully controlled the solenoid door lock based on authentication results. When access was accepted, the solenoid door lock opened automatically, and when access was rejected, the door remained locked. LED indicators and audio notifications from the speaker provided clear feedback to users regarding access status, as shown in Fig. 5.

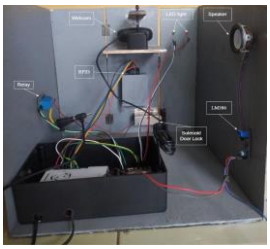

Figure 5. Hardware Implementation of the Door Security System

B. Application Interface Results

The Android application was tested to ensure that all features functioned as expected. The onboarding page was displayed correctly when the application was opened, directing users to the image data list page. The image data list page successfully displayed facial images captured by the system and stored in Firebase.

The create data page allowed users to input and store new room data, including name, room number, and RFID information. The room data list page displayed stored room data accurately, and the detail page enabled users to update or delete room data without errors.

Based on functional testing results, all application features operated correctly, including navigation, data input, data display, update, and deletion processes. This confirms that the application is reliable for monitoring and managing the door security system remotely, as shown in Fig. 6.

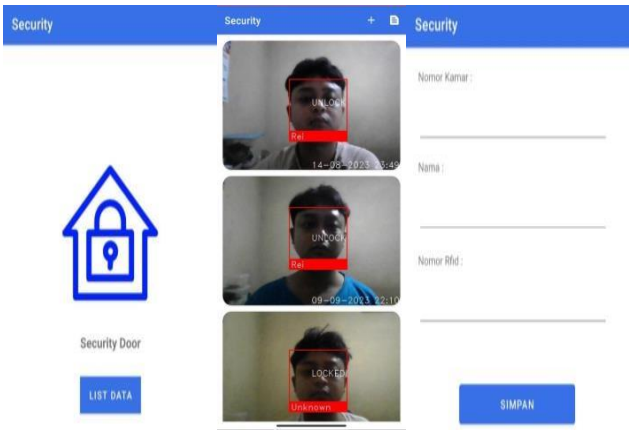

Figure 6. Android Application Interface Display

C. Face Recognition and Liveness Detection Performance

The performance of the face recognition and liveness detection system was evaluated using CNN training and validation at different epoch values, namely 25, 50, 100, 150, 200, and 250 epochs. The evaluation metrics used include accuracy, precision, recall, and F1-score, calculated based on the confusion matrix results.

The experimental results show that the CNN model achieved high recognition accuracy across all tested epochs. The average accuracy reached 95.1% at epoch 25 and increased to 98.2% at epoch 50. The highest average accuracy of 98.6% was achieved at epoch 150. However, a slight decrease in accuracy was

observed at epochs 200 and 250, indicating the possibility of overfitting when excessive training was applied.

This trend demonstrates that increasing the number of epochs improves model performance up to an optimal point, after which performance begins to decline. Therefore, epoch values between 50 and 150 provide the most stable and optimal performance for face recognition and liveness detection in this system.

D. Confusion Matrix Analysis

The confusion matrix analysis shows that most facial images were correctly classified, as indicated by the dominant values along the main diagonal of the confusion matrix. This confirms that the CNN model has a strong capability to distinguish between authorized and unauthorized users.

Misclassification cases occurred in a small number of samples, where some faces were incorrectly predicted as other registered individuals. These errors were primarily caused by similarities in facial features and variations in facial pose and lighting conditions. Despite these minor errors, the overall classification performance remained high, with precision and recall values exceeding 95% for most users, as shown in Table I.

TABLE I
. CONFUSION MATRIX OF FACE RECOGNITION RESULTS

True Label \ Predicted Label	Agung Tri	Erlangga Putra	Faris Hermawan	Hasbullah Putra	Ichsan Malik	Ilham Santosa	Raffi Aditya	Rama Wijaya	Refangga Indraprastha	Reinaldo Riswanto	Result
Agung Tri	155	1	3	2	0	0	0	0	0	0	161
Erlangga Putra	0	147	0	1	0	0	0	3	0	0	151
Faris Hermawan	1	0	136	0	2	0	0	1	0	0	140
Hasbullah Putra	0	0	0	145	1	2	0	0	1	0	149
Ichsan Malik	0	1	0	2	152	0	0	1	0	0	159
Ilham Santosa	0	0	0	1	0	136	0	0	0	2	139
Raffi Aditya	0	0	0	0	0	0	153	0	0	0	153
Rama Wijaya	0	0	0	0	2	0	0	153	0	0	155
Refangga Indraprastha	0	2	1	0	0	0	0	0	160	0	167
Reinaldo Riswanto	0	0	0	0	0	0	0	0	0	129	129

E. Precision, Recall, and F1-Score Evaluation

Precision, recall, and F1-score values were calculated to evaluate the reliability of the face recognition system in more detail. The results show that the model consistently achieved high precision and recall values across different epochs. The F1-score results further confirm the balance between precision and recall, indicating that the model performs well in recognizing authorized faces while minimizing false acceptance and false rejection rates.

The highest F1-score values were achieved at epoch 150, which aligns with the highest accuracy results. This confirms that the CNN model performs optimally when trained within an appropriate epoch range, as shown in Table II.

TABLE II
. PRECISION, RECALL, AND F1-SCORE RESULTS AT EPOCH 100

Class	Precision	Recall	F1-Score	Support
Agung Tri	0.99	0.96	0.98	161
Erlangga Putra	0.96	0.97	0.97	151
Faris Hermawan	0.97	0.97	0.97	140
Hasbullah Putra	0.96	0.97	0.97	149
Ichsan Malik	0.96	0.97	0.97	156
Ilham Santosa	0.99	0.98	0.98	139
Raffi Aditya	0.99	1.00	1.00	153
Rama Wijaya	0.99	0.99	0.99	155
Refangga Indraprastha	0.96	0.96	0.96	167
Reinaldo Riswanto	1.00	1.00	1.00	129

F. Discussion

The experimental results demonstrate that the proposed door security system based on Convolutional Neural Network (CNN) and liveness detection achieves high reliability and robustness. The confusion matrix results show that most predictions are located along the main diagonal, indicating that the system is able to correctly classify authorized users with minimal misclassification. This confirms that the CNN model successfully learns discriminative facial features for each registered individual.

The performance evaluation using precision, recall, and F1-score at epoch 100 further supports this finding. All classes achieved precision and recall values above 0.96, indicating that the system performs well in minimizing both false acceptance and false rejection. Several classes, such as Raffi Aditya and Reinaldo Riswanto, achieved near-perfect or perfect F1-score values, demonstrating high model stability when sufficient and consistent facial data are available. Minor misclassification observed in some classes can be attributed to similarities in facial characteristics, variations in lighting conditions, and differences in facial pose during image acquisition. However, these errors remain within an acceptable range and do not significantly affect overall system performance.

In addition to the classification performance, the effect of training epochs on system accuracy is presented in Table III. The accuracy results show that the face recognition system consistently achieves high performance across all tested epochs, with average accuracy values exceeding 95%. At epoch 25, the model already demonstrates strong initial learning capability with an average accuracy of 95.1%. As the number of epochs increases, accuracy improves significantly, reaching 98.2% at epoch 50 and achieving the highest average accuracy of 98.6% at epoch 150.

After epoch 150, a gradual decrease in accuracy is observed at epochs 200 and 250, where the average accuracy drops to

96.3% and 95.7%, respectively. This trend indicates that excessive training may lead to overfitting, causing the model to lose generalization capability on unseen data. Therefore, the results in Table V suggest that training epochs between 50 and 150 provide the most optimal balance between learning performance and generalization ability for the proposed system. The small differences between Training Result (TR) and Theoretical Calculation (TC) values further confirm the consistency and reliability of the evaluation process (Table III).

From a system perspective, the integration of liveness detection significantly enhances security by reducing the risk of spoofing attacks using printed images or digital displays. When combined with RFID authentication as a secondary security layer, the proposed system implements a multi-factor authentication mechanism that improves access control reliability. Overall, the discussion confirms that the proposed Raspberry Pi-based door security system is capable of delivering high accuracy, stable performance, and practical usability for real-world room security applications.

From a practical perspective, the high accuracy achieved by the proposed system indicates its suitability for real-time door security applications. The system is able to perform face recognition and liveness detection with minimal delay, making it convenient for daily use. The combination of biometric authentication and RFID enhances security while maintaining usability for users.

TABLE III
ACCURACY REPORT

No.	Wajah	Epoch (Accuracy)											
		25		50		100		150		200		250	
		TR	TC	TC	PT	TR	TC	TR	TC	TR	TC	TR	TC
1	Agung Tri	96%	96,49%	99%	98,98%	98%	97,47%	99%	99,49%	97%	97,49%	96%	96%
2	Erlangga Putra	97%	96,98%	99%	99,49%	97%	96,49%	98%	98,49%	95%	95,49%	95%	95%
3	Faris Hermawan	97%	96,95%	98%	98%	97%	97%	100%	99,49%	96%	96%	96%	95,95%
4	Hasbullah Putra	89%	89,16%	97%	97%	97%	96,49%	97%	96,49%	95%	94,47%	93%	92,98%
5	Ichsan Malik	93%	92,98%	97%	96,49%	97%	96,49%	97%	97%	95%	94,49%	95%	94,49%
6	Ilham Santosa	97%	97%	98%	97,47%	98%	98,49%	99%	99%	95%	95,47%	95%	95,49%
7	Raffi Aditya	96%	95,47%	98%	97,98%	100%	99,49%	99%	99,49%	97%	96,95%	95%	94,47%
8	Rama Wijaya	94%	93,9%	99%	99%	99%	99%	99%	98,98%	99%	98,49%	97%	96,95%
9	Refangga Indraprastha	92%	92,27%	97%	96,95%	96%	96%	98%	98%	95%	94,49%	94%	94,49%
10	Reinaldo Riswanto	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	99,49%
	Rata-rata	95,1%	95,12%	98,2%	98,13%	97,9%	97,69%	98,6%	98,64%	96,3%	96,33%	95,7%	95,53%

G. *Real-Time System Performance Discussion*

In addition to classification accuracy, system performance in real-time operation is an important aspect of door security applications. The proposed system demonstrates stable operation when deployed on Raspberry Pi, with face recognition and liveness detection executed in real time using a webcam. The processing time remains acceptable for practical use, allowing users to access the room without noticeable delay.

The integration of RFID authentication further enhances system reliability by providing an additional verification layer. Even if facial recognition errors occur, unauthorized access can still be prevented through RFID validation. This multi-factor authentication approach improves overall security without significantly increasing system complexity.

From an implementation perspective, the use of Raspberry Pi allows the system to operate with low power consumption and minimal hardware cost. Combined with Android-based monitoring via Firebase, the system enables users to observe access activity remotely, increasing practicality and security awareness. These characteristics indicate that the proposed system is suitable for real-world deployment in residential and boarding room environments, as shown in Fig. 7.

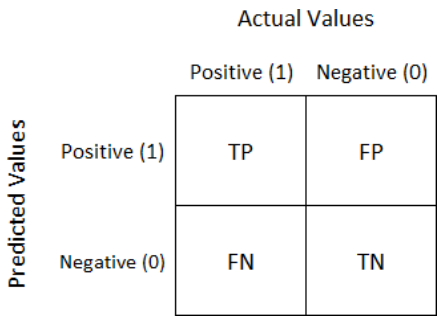

Figure 7. Image Confusion Matrix

The average prediction result is obtained from each epoch, summed from each epoch, and divided by the number of faces that do the training.

Epoch150=(100+98,01+99,29+97,27+97,41+99,28+98,1+98,2+98,2+100):10=98.57%

The results of testing people's faces, Reinaldo Riswanto Saputra with epoch 100 produces the highest accuracy value of 100%, while Hasbullah Putra at epoch 25 produces the lowest

accuracy value, which is 84%, the use of epoch affects the resulting accuracy value. face recognition accuracy prediction results of ten individuals at various epochs. In this table, two evaluation methods are used: Training Result (HT) and Theoretical Calculation (PT).

Overall, the proposed system successfully achieves high accuracy, reliable authentication, and effective access control, making it suitable for room security applications in residential and boarding environments.

H. System Limitations and Future Work

Although the proposed door security system demonstrates high accuracy and reliable performance, several limitations should be considered. First, the facial image dataset used in this research is limited to ten individuals and is collected under controlled indoor lighting conditions. Variations in extreme lighting, occlusion, or camera angles may affect recognition performance in real-world environments. Expanding the dataset with more subjects and diverse acquisition conditions could further improve model robustness.

Second, the system relies on a single webcam for facial acquisition. While this configuration is sufficient for basic room security applications, the use of multiple cameras or depth sensors could enhance face detection accuracy and improve liveness detection performance, especially in challenging lighting conditions. Additionally, the current liveness detection approach focuses on visual features and may be further strengthened by incorporating temporal or motion-based analysis.

From a computational perspective, deploying the CNN model on Raspberry Pi introduces hardware constraints related to processing power and memory. Although real-time performance is achieved, more complex deep learning architectures may require optimization techniques such as model pruning or quantization to maintain efficiency on embedded platforms.

Future work may focus on improving system scalability by integrating cloud-based processing or hybrid edge–cloud architectures. The implementation of adaptive thresholding and continuous learning mechanisms could also enhance system flexibility and long-term performance. Furthermore, integrating additional security features such as mobile notifications, access history analytics, or integration with smart home systems would increase system functionality and usability.

Overall, addressing these limitations in future research is expected to enhance the reliability, scalability, and applicability of the proposed door security system for broader real-world deployments.

IV. CONCLUSION

This research successfully developed a Raspberry Pi–based door security system that integrates Convolutional Neural Network (CNN) face recognition, liveness detection, and RFID authentication to enhance access control reliability. The experimental results demonstrate that the proposed system achieves consistently high performance, with average accuracy values exceeding 95% across all tested epochs and optimal results obtained at epoch 150, indicating a good balance between learning and generalization. The incorporation of liveness detection effectively reduces spoofing risks, while the Android application and Firebase integration enable practical monitoring and user management. Overall, the system provides an effective, affordable, and robust solution for room security applications in residential and boarding environments.

REFERENCES

[1] E. Fadly, S. A. Wibowo, and A. P. Sasmito, “Sistem Keamanan Pintu Kamar Kos Menggunakan Face Recognition,” JATI, vol. 5, no. 2, 2021.

[2] R. Kurniawan and A. Zulius, “Smart Home Security Menggunakan Face Recognition Berbasis Raspberry Pi,” Jurnal Sustainable, vol. 8, no. 2, 2019.

[3] C. Lesmana, R. Lim, and L. W. Santoso, “Implementasi Face Recognition untuk Akses Ruangan Pribadi,” Jurnal Infra, vol. 7, no. 1, 2019.

[4] B. Wijayanto, F. Utaminingrum, and I. Arwani, “Face Recognition untuk Sistem Pengaman Rumah,” Jurnal Pengembangan TI, vol. 3, no. 3, 2019.

[5] K. Jain, A. Ross, and S. Prabhakar, “An Introduction to Biometric Recognition,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, 2004.

[6] W. Zhao, R. Chellappa, A. Rosenfeld, and P. J. Phillips, “Face Recognition: A Literature Survey,” ACM Computing Surveys, vol. 35, no. 4, 2003.

[7] S. Z. Li and A. K. Jain, Handbook of Face Recognition, Springer, 2011.

[8] R. Chellappa, C. L. Wilson, and S. Sirohey, “Human and Machine Recognition of Faces: A Survey,” Proceedings of the IEEE, vol. 83, no. 5, 1995.

[9] Hadid, M. Pietikäinen, and T. Ahonen, “Face Spoofing Detection,” IEEE Transactions on Information Forensics and Security, vol. 7, no. 3, 2012.

[10] Chingovska, A. Anjos, and S. Marcel, “On the Effectiveness of Local Binary Patterns in Face Anti-Spoofing,” in Proceedings of BIOSIG, 2012.

[11] Z. Boulkenafet, J. Komulainen, and A. Hadid, “Face Anti-Spoofing Using Color Texture Analysis,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 8, 2016.

[12] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, “DeepFace: Closing the Gap to Human-Level Performance in Face Verification,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2014.

[13] Schroff, D. Kalenichenko, and J. Philbin, “FaceNet: A Unified Embedding for Face Recognition and Clustering,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2015.

[14] O. M. Parkhi, A. Vedaldi, and A. Zisserman, “Deep Face Recognition,” in Proceedings of the British Machine Vision Conference (BMVC), 2015.

[15] M. Abadi et al., "TensorFlow: A System for Large-Scale Machine Learning," in Proceedings of the 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI), 2016.
[16] E. Upton and G. Halfacree, Raspberry Pi User Guide, Wiley, 2016.
[17] I. Setiawan, A. Jaenul, and D. Priyokusumo, "Prototype Sistem Keamanan Rumah Menggunakan Face Recognition Berbasis Raspberry Pi 4," Jurnal Poltekba, vol. 4, no. 1, 2020.
[18] R. Muwardi and R. R. Adisaputro, "Design Sistem Keamanan Pintu Menggunakan Face Detection," Jurnal Teknologi Elektro, vol. 12, no. 3, 2021.
[19] P. Jutika, "Implementasi Face Recognition Berbasis Haar-Cascade Classifier pada Sistem Keamanan Rumah," INFOTECH Journal, 2022.
[20] M. Susanto, F. E. Purnomo, and M. F. I. Fahmi, "Sistem Keamanan Pintu Menggunakan Metode Fisherface," Jurnal Ilmiah Inovasi, vol. 17, no. 1, 2017.