DOI: https://doi.org/10.61762/pjstvol7iss1art27053

PLATFORM - A Journal of Science & Technology

Received: 29 April 2024, Accepted: 24 June 2024, Published: 28 June 2024, Publisher: UTP Press, Creative Commons: CC BY 4.0

MOBILEFACENET-BASED FACIAL RECOGNITION SYSTEM FOR CONTACTLESS ACCESS CONTROL

Zubairu Muhammad Ahmad[1,2], Abdullateef Oluwagbemiga Balogun[1*], Aminu Aminu Muazu[1,3], Hussain Mamman[1,4], Rafiat Ajibade Oyekunle[5]

[1]Department of Computer & Information Science, Universiti Teknologi PETRONAS, Malaysia
[2]Department of Computer Science, Gombe State University, Nigeria
[3]Department of Computer Science, Umaru Musa Yar'adua University, Nigeria
[4]Department of Management and Information Technology, Abubakar Tafawa Balewa University, Nigeria
[5]Department of Information Technology, University of Ilorin, Nigeria

*E-mail: abdullateef.ob@utp.edu.my

ABSTRACT

Conventional access control systems require physical contact, such as pressing buttons, using fingerprints, or employing radio-frequency identification (RFID). These interactions increase the risk of transmitting diseases like COVID-19 through surface contact. To mitigate this risk, a contactless identification method becomes imperative. Hence, this study proposes an adaptive and seamless dual-mode mobile facial recognition-based access control system. Specifically, the proposed system uses a convolutional neural network (CNN) algorithm (MobileFaceNet) to develop high-precision facial verification on mobile devices with a dual-mode (real-time and offline) facial recognition system. The system is implemented on Raspberry Pi, running an Android Operating System equipped with camera functionality. The system instantaneously operates by detecting human faces, compares the faces with a pre-existing database, and grants access to successful matches. The system underwent preliminary testing on an Android 9 device with an 8-megapixel camera. Faces were detected and recognised in a record time (within seconds), showcasing commendable accuracy. The system achieved a recognition accuracy of 95% under varied lighting conditions and distances. The proposed system can be seamlessly integrated with electronic doors, ensuring optimal access control for smart homes and restricted facilities.

Keywords: *access control, convolutional neural network, face recognition, firebase, mobilefacenet*

INTRODUCTION

Access control refers to the techniques employed to regulate entry into or exit from a designated space. In its simplest form, this can involve the use of a traditional mechanical lock requiring a physical key for authorisation. However, as security measures have evolved over time, access control systems have become increasingly complex and sophisticated. Modern implementations typically involve computerised or electronic card-based systems [1]. These advanced systems leverage cutting-edge technologies such as biometrics (e.g., facial recognition, iris scanning, or fingerprint identification) to grant secure access to authorised individuals while restricting unauthorised entrance. The primary goal of these access control systems is to facilitate expedient and seamless entry for legitimate parties while maintaining a robust barrier against unwanted intrusion [2].

Facial recognition systems, also known as face recognition systems, constitute a type of computer application that leverages complex mathematical computations to enable computers to identify and recognise human faces based on specific features of the face [3]. These systems fall under the broader category of biometrics, which involves the use of physical or behavioural characteristics to authenticate an individual's identity. While the accuracy of facial recognition systems may be lower compared to other biometric modalities, such as iris recognition and fingerprint recognition, their non-invasive nature has contributed to their widespread adoption, particularly in applications where contactless authentication is desired [4].

Facial recognition systems are primarily used for access control. They are increasingly employed alongside computer-based or electronic card systems [5]. Using biometric technologies like facial recognition, these systems provide rapid and seamless entry to authorised individuals. They also restrict access to unauthorised parties. Moreover, access control systems can refer to any methodology designed to regulate movement within or outside a particular area [5]. In recent times, access control systems have evolved significantly, becoming more sophisticated and advanced [6]. In many cases, these systems now rely on biometric technology, including facial recognition, iris recognition, or fingerprint recognition, instead of traditional keys or cards. This shift towards biometric authentication has enhanced security and convenience, making it easier for authorised personnel to gain access to secure areas without the need for bulky keys or cumbersome identification documents.

Traditionally, access control systems require physical contact. This increases the risk of contracting viruses such as COVID-19 by touching contaminated surfaces and facial areas. Therefore, a contactless access control solution is needed to minimise infection risk. Additionally, network connectivity issues in remote areas necessitate a solution that ensures reliable access control even with unreliable network connectivity. This study aims to develop an adaptive and seamless dual-mode mobile facial recognition-based access control system. The specific objectives are:

1. Adaptive Solution: To create a system that operates efficiently in both real-time and offline modes, ensuring reliable performance even in areas with inconsistent network access.
2. Seamless Integration: To provide a facial recognition system that integrates effortlessly with existing access control mechanisms, enhancing security and user convenience without requiring significant infrastructure changes.

The implementation leverages state-of-the-art convolutional neural networks, specifically the MobileFaceNet algorithm, designed for high-precision real-time face verification on mobile devices. This study significantly advances access control and facial recognition technology through several key contributions. Firstly, it introduces a pioneering dual-mode mobile facial recognition-based system that operates in both real-time and offline modes, effectively overcoming the limitations associated with traditional access control systems. Integrating the MobileFaceNet convolutional neural network algorithm enhances the accuracy of facial recognition on mobile devices, ensuring precise verification. When deployed on Raspberry Pi, the system provides a cost-effective and accessible platform for seamless integration with electronic doors, particularly suitable for smart homes and restricted facilities.

LITERATURE REVIEW

Managing access control by simplifying the traditional way was proposed using different approaches. This section attempts to highlight previous work's approaches to the access control system. During this section, we reviewed research works and projects like this study and selected the top three that offer the best functionality or that have a reasonable amount of accuracy with a consistent solution. Below is a review of the selected works, some of which have some limitations highlighted.

A study by Gunawan et al. [4] proposed a face recognition security system using Raspberry Pi, which can be connected to the smart home system. Eigenface was used as the feature extraction, while Principal Component Analysis (PCA) was used as the classifier. The output of the face recognition algorithm is then connected to the relay circuit, in which it will lock or unlock the magnetic lock placed at the door. Results showed the effectiveness of our proposed system, in which we obtained around 90% face recognition accuracy. However, their system uses memory to store data; therefore, if the system fails, the data may be corrupted and lost. Additionally, it lacked network connectivity, limiting integration with other systems.
In another study by Patil and Narendra [7], the author aims to achieve an advanced security system over Raspberry Pi controlled via an Android application. The applications of their project are unlimited as each application gives rise to new applications. So, it can

be implemented in the following areas of security: car security, home security, budgeted industrial, surveillance, office cabins, and shopping malls. From remote places (depending on the communication network). However, the system required users to have an Android application installed on their phones, which is impractical for users without such devices. Moreover, the dependency on a local network limited accessibility in the absence of network connectivity.

Another study by Irjanto and Surantha [8] proposed a facial recognition process for the process of opening the door of a house that can replace the process of home security using an electronic key or RFID. They divided stages into 3 parts, namely the stages of collecting homeowner data, the data training process, and the facial recognition process using Raspberry Pi. They implemented the facial recognition process with the Convolutional Neural Network method, which was installed on a minicomputer, namely the Raspberry Pi, which will serve as a microcontroller to lock and open the door automatically. The homeowner's face controls it. They used the Viola-Jones algorithm to detect faces and the Eigenfaces algorithm to recognise people. The test results were recorded, and they achieved 95% accuracy in recognition under fluorescent lighting conditions. However, this did not include a database where the users' information would be stored for future decision-making, and it lacked network connectivity [4].

Another study by Chen et al. [9] presented a class of extremely efficient CNN models, MobileFaceNets, which use less than 1 million parameters and are specifically tailored for high-accuracy real-time face verification on mobile and embedded devices. They first make a simple analysis of the weakness of common mobile networks for face verification. Their specifically designed MobileFaceNets have overcome this weakness. Under the same experimental conditions, our MobileFaceNets achieve significantly superior accuracy as well as more than two times the actual speedup over MobileNetV2. After training by ArcFace loss on the refined MS-Celeb-1M, our single MobileFaceNet of 4.0 MB size achieves 99.55% accuracy on LFW and 92.59% TAR@FAR1e-6 on MegaFace, which is even comparable to state-of-the-art big CNN models of hundreds MB size. The fastest one of MobileFaceNets has an actual inference time of 18 milliseconds on a mobile phone. For face verification, MobileFaceNets achieve significantly improved efficiency over previous state-of-the-art mobile CNNs.

A study by Singh et al. [10] proposed that PCA (Principal Component Analysis) extracts features from facial images. The same length and width of the image are preferred; thus, images were scaled to 120×120 pixels. After pre-processing, the image is compared with faces already registered in the system through MobileFaceNet to recognise whether or not faces in the image frame exist.

According to the analysis in Table 1, the existing systems exhibit several limitations, and the proposed system aims to address these limitations in the following aspects:

1. Network Connectivity: Many current systems heavily rely on network connectivity. While this may enhance certain functionalities, it can be impractical in situations where network reliability is a concern [8]. The dependence on network connectivity can limit the system's reliability in areas with inconsistent network access.
2. Data Storage: The system presented by Gunawan et al. [4] uses memory to store data. This approach raises concerns about data integrity, as a system failure could potentially lead to data corruption and loss. Furthermore, it does not provide integration with other systems, as it lacks network connectivity.

In summary, the existing systems exhibit challenges related to resource utilisation, network dependence, data storage methods, device requirements, and the lack of comprehensive databases. The study aims to overcome the limitations related to network connectivity and data storage by leveraging advancements in mobile computing, cloud computing, and neural networks, as well as adopting an offline-first approach to optimise system performance and reliability.

METHODOLOGY

Research Methodology

The techniques used for fact-finding in this project are prototyping, research, and site visiting. In these approaches, research from different papers and website articles, were gathered as a fact for developing the system. From these facts, prototyping methods of gathering facts were used to gain a better understanding of the system and gather more information, which helped tremendously in the development process of the proposed system.

Table 1 Comparative analysis of the related works

System	Features	Advantages	Limitations
Face Recognition on Raspberry Pi [4]	Eigenface for feature extraction, PCA for classification	Achieved 90% accuracy, integrated with smart home systems	Memory-based data storage, risk of data corruption, no network connectivity
Advanced Security System over Raspberry Pi [8]	Controlled via Android application	Versatile applications (car, home, industrial security)	Requires Android app, limited to local network, impractical for users without Android devices
Facial Recognition Process using Raspberry Pi [9]	CNN for face recognition, automatic door lock/unlock	Achieved 95% accuracy under fluorescent lighting	No database for future decision-making, no network connectivity
MobileFaceNets for Face Verification [10]	Efficient CNN models, less than 1 million parameters	High accuracy (99.55% on LFW), fast verification.	Lack of practical implementation details and potential challenges not discussed.
Automatic Lecture Attendance System [11]	PCA for feature extraction, MobileFaceNet for recognition, Firebase Cloud Firestore for data storage	Real-time synchronisation, offline support	Accuracy is affected by environmental conditions, dependency on lighting, and camera angles.

System Methodology

This project used the Prototyping model because the system developed in this study is not the complete final product. Rather, it is a prototype of the final system, which is inexpensive and incomplete, having only the basic functionality compared to the final product. The prototyping Model is a software development approach that involves building, testing, and refining a prototype until an acceptable version is achieved. This model allows for partial system implementation before or during the analysis phase, enabling early customer feedback [11]-[12]. The prototype methodology is a well-established software development model that requires careful planning and system design, personnel selection, and determination of software and hardware [13]. The advantages of the Prototyping Model include its adaptability to the initial needs of software development, allowing for the identification of defined features and functions[14]-[15].

System Model

This system uses MobileFaceNets, a CNN-based model that uses no more than 1 million parameters and is specifically tailored for high-accuracy real-time face verification on mobile and embedded devices [9].

The Convolutional Neural Network (CNN) is a powerful and widely used model in various domains, including image recognition, medical imaging, speech recognition, and more. It has been continuously improved, making it one of the most successful models in artificial intelligence [16]. CNNs are specifically designed for processing data that can be presented separately, making them suitable for tasks such as

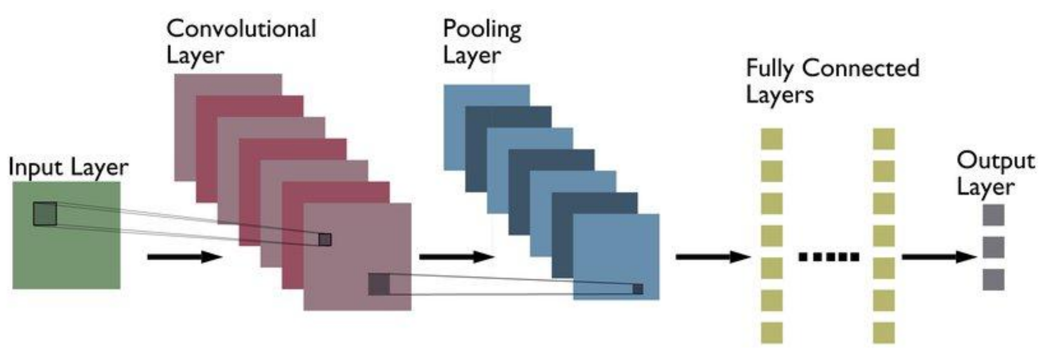

Figure 1 Basic CNN Architecture [20]

image identification and feature extraction [17]. The architecture of a typical CNN consists of stages with layers such as convolutional, batch normalisation, nonlinearity, and pooling, enabling end-to-end feature learning for data categorisation [18]. CNNs utilise a succession of layers of trainable convolution filters and optional pooling operations applied to local features, allowing for the extraction and learning of image features [19].

The MobileFaceNets model is a class of highly efficient CNN models employed for accurate real-time face verification on mobile and embedded devices [9]. This model is designed to address the weaknesses identified in common mobile networks for face verification. It achieves superior accuracy and speed compared to previous mobile CNNs, making it a suitable choice for the proposed system. Table 2 presents a comparison between MobileFaceNets and other mobile models in terms of performance.

Table 2 Performance comparison among mobile models trained on casia-webface

Network	LFW Accuracy	AgeDB Accuracy	Parameters	MAdss	Speed (CPU)
MobileNetV1	98.63%	88.95%	3.2M	574M	60ms
ShuffleNet (1x, g=3)	98.70%	89.27%	1.1M	139M	27ms
MobileNetV2	98.58%	88.81%	2.1M	299M	49ms
MobileNetV2-GDConv	98.88%	90.67%	2.1M	299M	50ms
MobileFaceNet	99.28%	93.05%	0.99M	130M	24ms
MobileFaceNet (112 X 96)	99.18%	92.96%	0.99M	112M	21ms
MobileFaceNet (96 X 96)	99.08%	92.63%	0.99M	96M	18ms
MobileFaceNet-M	99.18%	92.67%	0.92M	129M	24ms
MobileFaceNet-S	99.00%	92.48%	0.84M	126M	23ms
MobileFaceNet(ReLU)	99.15%	92.83%	0.98M	130M	23ms
MobileFaceNet (expansion factor X 2)	99.10%	92.81%	1.1M	140M	27ms

IMPLEMENTATION

This section will describe the proposed system's design, implementation, and testing. The proposed system is implemented with the following features:

1. ML Kit for Face Detection: ML Kit's face detection API is the stage where the face detects an image, identifies key facial features, and gets the contours of detected faces. Note that the API detects faces; it does not recognise people. With face detection, the information is needed to perform tasks like embellishing selfies and portraits or generating avatars from a user's photo. ML Kit can perform face detection in real-time and be used in applications like video chat or games that respond to the player's expressions. This research utilises an ML Kit to detect human faces in real-time from the image frames taken by the camera and then pass those images to MobileFaceNet for the recognition process.
2. MobileFaceNet for Face Recognition: After ML Kit detects a face, MobileFaceNet processes the detected face through pre-processing steps to enhance recognition performance. These steps may include scaling down the image to increase processing speed. The model then extracts features from the detected faces and classifies them based on comparisons with faces stored in the system's database. If a match is found, the face is recognised and labelled with the corresponding person's ID. In cases where no match is found, the face is labelled as unknown, typically indicated by a blue square around it.
3. Firebase Cloud Firestore for Databases: Cloud Firestore is a flexible and scalable database for mobile, web, and server development from Firebase and Google Cloud. It allows us to keep data in sync across client apps through real-time listeners and offers offline support for mobile and web. This allows us to build responsive apps that work regardless of network latency or Internet

connectivity. This technology was used in this research to store user data in real-time [10].

4. Firebase Cloud Storage for Storing Images: Cloud Storage for Firebase is a powerful, simple, and cost-effective object storage service built for Google scale. The Firebase SDKs for Cloud Storage add Google security to file uploads and downloads for your Firebase apps, regardless of network quality. All images of faces saved in the system are also stored in the cloud storage and retrieved anytime the system is powered on [10].

Figures 2 and 3 depict the block diagrams for registering a new user and recognition, respectively.

The proposed system is specifically optimised for mobile and embedded platforms running Android OS Lollipop or later versions. Network connectivity, whether through Wi-Fi or mobile data, is integral for real-time synchronisation, facilitating seamless interaction with Firebase services. The reliance on a functional camera underscores its importance in capturing image frames crucial for real-time face detection. The system's innovative "offline-first" approach ensures uninterrupted functionality even in the absence of a stable internet connection. Furthermore, the integration capability with magnetic or electronic doors enhances its utility for access control purposes. The system sets a minimum Android version requirement of Lolli-pop or later, aligning with contemporary Android features and ensuring optimal performance.

In testing the mobile facial recognition for an access control system, the following sequence (component

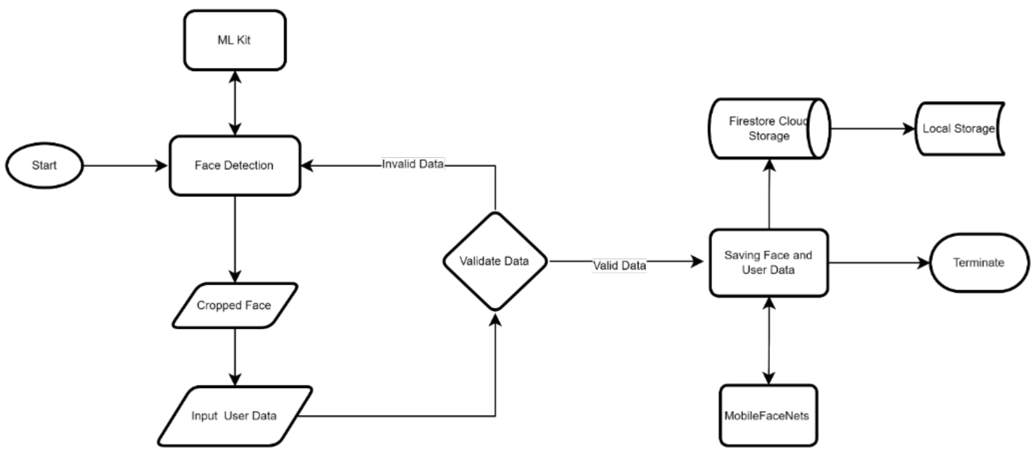

Figure 2 Flowchart diagram for registering a new user

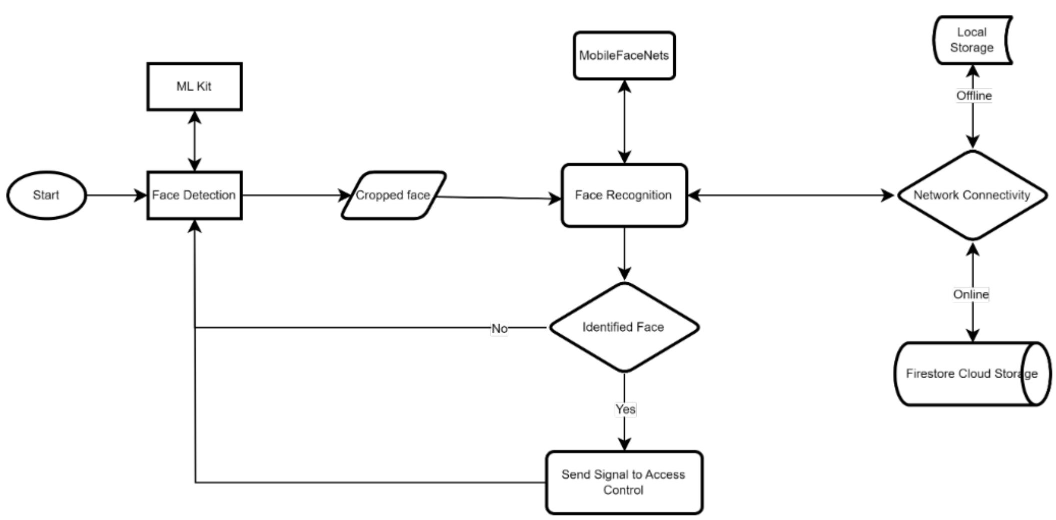

Figure 3 Flowchart diagram for recognition

testing, integration testing, then user testing) of activities was followed to conform to the most widely used modern testing processes. If defects are discovered at any one stage, they require program modifications to correct them, and this may require other stages in the testing process to be repeated. The process is, therefore, an iterative one, with information being fed back from later stages to earlier parts of the process. The system was tested by registering a new person's face, and it was successfully able to register

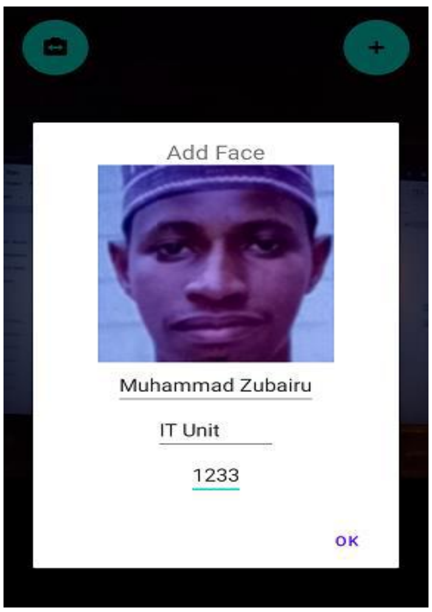

Figure 4 Illustration of registering a new user

Figure 5 Facial capture registering of a new user

and recognise the face and synchronise the user data between cloud and local storage.

RESULTS AND DISCUSSION

The system showed high accuracy in real-time face detection and recognition. It efficiently extracted and classified facial features and compared them with the stored database. If a face was successfully verified, it was labelled with the person's ID. If not, it was labelled as unknown, indicated by a blue square.

Performance Analysis

1. Registered Users: As shown in Table 3, the system achieved a high success rate for registered users, with consistent accuracy across different lighting conditions and distances. Specifically, the system maintained a 95% accuracy rate in both daylight and evening conditions at distances of 1 meter and 1.5 meters. These results underscore the system's robustness and reliability in varied environments.
2. Non-Registered Users: As presented in Table 4, the system effectively identified non-registered users, ensuring they were correctly labelled as unknown. The absence of false positives in this category

Table 3 Presentation of registered user's test results

Light	Faces	Distance			
		1.5 m		1 m	
		Success	Fail	Success	Fail
Daylight	5	5	0	5	0
Evening	5	4	1	5	0

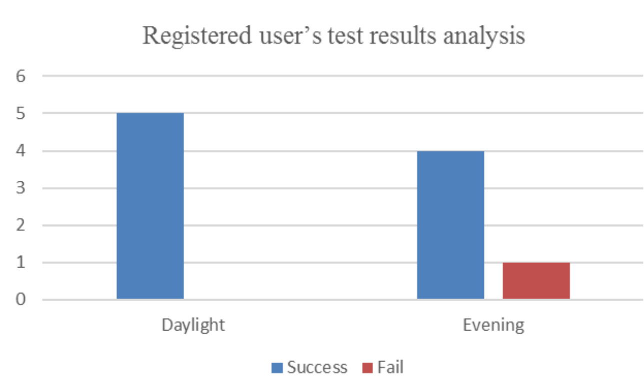

Figure 6 Illustration of registered user's test results analysis on 1.5 meters distance

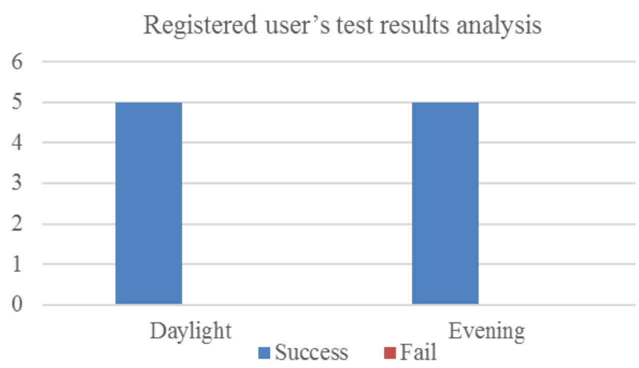

Figure 7 Illustration of registered user's test results analysis on a 1-meter distance

Table 4 Presentation of non-registered test results

Light	Faces	Distance			
		1.5 m		1 m	
		Success	Fail	Success	Fail
Daylight	5	0	5	0	5
Evening	5	0	5	0	5

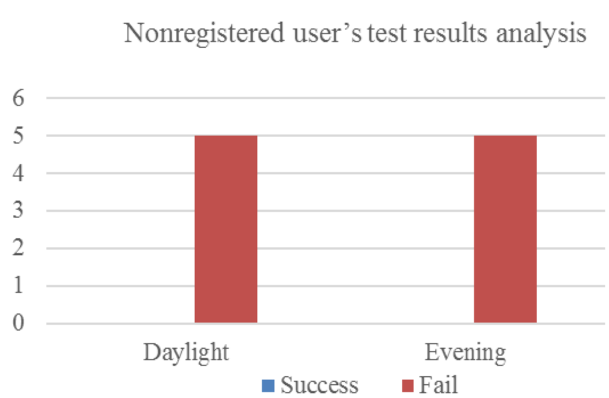

Figure 8 Illustration of non-registered user's test results analysis on 1.5 meters distance

highlights the precision of the facial recognition algorithm.

Comparison with existing studies

1. Face Recognition on Raspberry Pi: The proposed system surpasses the 90% accuracy reported by Gunawan et al. [4] by achieving a 95% accuracy rate. Additionally, our system addresses the limitations of memory-based data storage and lack of network connectivity by integrating both local and cloud storage solutions.

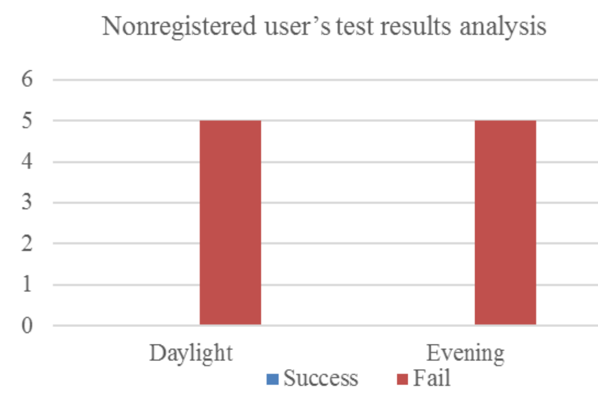

Figure 9 Illustration of non-registered user's test results analysis on 1 meter distance

2. Advanced Security System over Raspberry Pi: Unlike Patil and Narendra's [8] system, which requires an Android application, our solution is device-agnostic, enhancing user accessibility and convenience. Furthermore, our system's offline-first approach mitigates the reliance on local network connectivity.
3. Facial Recognition Process using Raspberry Pi: Irjanto and Surantha's [9] system achieved 95% accuracy under specific lighting conditions. Our system matches this accuracy level while also providing a more comprehensive data management solution through cloud integration, ensuring data persistence and reliability.
4. MobileFaceNets for Face Verification: While Chen et al. [10] demonstrated the high accuracy of MobileFaceNets, our practical implementation confirms these findings and showcases the model's applicability in real-world access control scenarios.
5. Automatic Lecture Attendance System: Singh et al.'s [11] system was highly sensitive to environmental conditions. Our system mitigates these issues by employing advanced preprocessing techniques to normalise lighting variations, thereby maintaining high accuracy across different conditions.
6. The system's performance in varying conditions and its comparison with existing works highlight its effectiveness and reliability. By addressing the limitations of previous systems, our proposed solution provides an adaptable and seamless access control mechanism suitable for various applications.

CONCLUSION

The proposed facial recognition system demonstrates strong potential for real-time and offline face detection and recognition. It effectively employs ML Kit for precise face detection and MobileFaceNet for accurate recognition against stored data, ensuring reliability. Notably, its offline-first approach optimises resource usage, ensuring a responsive user experience. Integration with Firebase services and compatibility with a wide range of Android devices contribute to its comprehensive functionality and inclusivity. Testing has confirmed successful face detection and recognition, validating its reliability in practical scenarios. The results analysis indicated that the system can successfully recognise faces at distances of 1 and 1.5 meters for registered users while a failure for non-registered users. Looking forward, future developments may focus on enhancing features and addressing any identified limitations, highlighting the system's capacity for growth. Overall, this system excels in accuracy, efficiency, integration, adaptability, and user satisfaction, marking it as a robust and user-friendly solution.

ACKNOWLEDGEMENT

The authors would like to express their sincere appreciation to the anonymous reviewers for their insightful comments and recommendations, which improved the overall quality of this research.

REFERENCES

[1] B. Leander, A. Čaušević, H. Hansson, and T. Lindström, "Toward an ideal access control strategy for industry 4.0 manufacturing systems," *IEEE Access,* vol. 9, pp. 114037-114050, 2021.

[2] Q. D. Le, T. T. C. Vu, and T. Q. Vo, "Application of 3D face recognition in the access control system," *Robotica,* vol. 40, no. 7, pp. 2449-2467, 2022.

[3] M. K. Rusia and D. K. Singh, "A comprehensive survey on techniques to handle face identity threats: challenges and opportunities," *Multimedia Tools and Applications,* vol. 82, no. 2, pp. 1669-1748, 2023.

[4] T. S. Gunawan, M. H. H. Gani, F. D. A. Rahman, and M. Kartiwi, "Development of face recognition on Raspberry Pi for security enhancement of smart home system," *Indonesian Journal of Electrical Engineering and Informatics (IJEEI),* vol. 5, no. 4, pp. 317-325, 2017.

[5] A. M. Ayub, R. Kolandaisamy, and K. K. Hooi, "Getting Smarter with Fatrix: A Facial Recognition Access Control System," in *2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA)*, 2023, pp. 149-153.

[6] H.-W. Lee, "Design of multi-functional access control system," *IEEE Access,* vol. 9, pp. 85255-85264, 2021.

[7] Y. Kortli, M. Jridi, A. Al Falou, and M. Atri, "Face recognition systems: A survey," *Sensors,* vol. 20, no. 2, p. 342, 2020.

[8] S. K. Patil and G. N. Dr Narendra, "Achieving Advanced Security System over Raspberry Pi Controlled via Android Application," *International Journal of Scientific Research in Science and Technology (IJSRST),* pp. 2395-6011, 2018.

[9] N. S. Irjanto and N. Surantha, "Home security system with face recognition based on convolutional neural network," *International Journal of Advanced Computer Science and Applications,* vol. 11, no. 11, 2020.

[10] S. Chen, Y. Liu, X. Gao, and Z. Han, "Mobilefacenets: Efficient cnns for accurate real-time face verification on mobile devices," in *Biometric Recognition: 13th Chinese Conference, CCBR 2018, Urumqi, China, August 11-12, 2018, Proceedings 13*, 2018, pp. 428-438.

[11] S. Singh, R. Rastogi, and P. S. Sharma, "Automatic Lecture Attendance System using Face Reorganization," *Matrix Academic International Online Journal Of Engineering And Technology,* vol. 3, no. 1, pp. 36-40, 2015.

[12] S. B. Basri, G. Kumar, F. F. Fahrurazi, P. E. B. Azmi, A. O. Balogun, and H. Mamman, "Current Trend of Software Requirement Engineering Process in IT Small and Medium Enterprises (SMEs)-A Systematic Literature Review," in *2023 13th International Conference on Information Technology in Asia (CITA)*, 2023, pp. 82-87.

[13] S. Basri, M. A. Almomani, A. A. Imam, M. Thangiah, A. R. Gilal, and A. O. Balogun, "The organisational factors of software process improvement in small software industry: comparative study," in *Emerging Trends in Intelligent Computing and Informatics: Data Science, Intelligent Information Systems and Smart Computing 4*, 2020, pp. 1132-1143.

[14] B. Ahmad, S. Beecham, and I. Richardson, "The case of Golden Jubilants: using a Prototype to support Healthcare Technology Research," in *2021 IEEE/ACM 3rd International Workshop on Software Engineering for Healthcare (SEH)*, 2021, pp. 68-71.

[15] M. A. S. Ekowati, "Design Prototype of Simple Jarimatic Visualization Application Model, Attracting, Motivating Early Children to Learn and Grow," *International Journal of Ethno-Sciences and Education Research,* vol. 2, no. 3, pp. 129-136, 2022.

[16] S. Mahamad, F. M. Shuhaili, S. Sulaiman, D. R. Awang Rambli, and A. O. Balogun, "Visual Signifier for Large Multi-Touch Display to Support Interaction in a Virtual Museum Interface," *Applied Sciences,* vol. 12, no. 21, p. 11191, 2022.

[17] S. M. Fati, A. Muneer, A. Alwadain, and A. O. Balogun, "Cyberbullying Detection on Twitter Using Deep Learning-Based Attention Mechanisms and Continuous Bag of Words Feature Extraction," *Mathematics,* vol. 11, no. 16, p. 3567, 2023.

[18] I. N. Husada and H. Toba, "Pengaruh Metode Penyeimbangan Kelas Terhadap Tingkat Akurasi Analisis Sentimen pada Tweets Berbahasa Indonesia," *Jurnal Teknik Informatika dan Sistem Informasi,* vol. 6, no. 2, 2020.

[19] X. Luo, X. Tong, Z. Hu, and G. Wu, "Improving urban land cover/use mapping by integrating a hybrid convolutional neural network and an automatic training sample expanding strategy," *Remote Sensing,* vol. 12, no. 14, p. 2292, 2020.

[20] Y. Nam and C. Lee, "Cascaded convolutional neural network architecture for speech emotion recognition in noisy conditions," *Sensors,* vol. 21, no. 13, p. 4399, 2021.