Design and development of face recognition-based security system using expression game as liveness detection

Yunan Yusmanto [a,1], Harits Ar Rosyid [a,2,*], Aji Prasetya Wibawa [a,3]

[a] Faculty of Engineering, State University of Malang, Malang, Indonesia
[1] yunan.yusmanto.2205348@students.um.ac.id; [2] harits.ar.ft@um.ac.id; [3] aji.prasetya.ft@um.ac.id
* corresponding author

ARTICLE INFO

Article history
Received July 1, 2024
Revised July 27, 2024
Accepted December 8, 2024

Keywords
Face recognition,
Liveness detection,
Biometric security
Security system,
Face expression

ABSTRACT

Face recognition as a security system has undergone significant developments, but challenges in live detection are still a major issue in preventing fraud. Liveness detection is a method that helps face recognition security more resistant to fraud. This research aims to address this issue by developing an innovative security system that integrates face recognition with a facial expression game, enhancing live detection and user engagement. The primary objectives are to ensure seamless integration, maintain a fun and challenging user experience, and demonstrate practical applicability. We applied a Waterfall method in our research to ensure a straightforward approach. We successfully applied this system for the door lock-unlock mechanism, simulating a restricted area. YuNet, a face detection model runs in the web interface and controls the NodeMCU to either lock or unlock the door. The study concluded 95% success rate from the participants in making facial expressions: Smile, Normal, and Sad. However, expressing Sadness within the 3-second timeframe posed some difficulties. The average duration for completing the mini-game was approximately 16.31 seconds from the start. The integration of a facial expression game as a liveness detection required careful design to balance security and user engagement that is fun to experience. This research underscores the significance of addressing current challenges in biometric security by integrating an interactive element into the live detection process. The developed system contributes to the field by enhancing the robustness and user experience of face recognition security systems, demonstrating potential for broader application in restricted access scenarios.

1. Introduction

Security is critical and requires innovative solutions to protect sensitive space or data access. Recent technology in biometric identification has improved to accommodate that. One of these is face recognition, which offers convenience and security. In this context, it provides deep insights into face recognition in real-world scenarios, highlighting technological advances in Deep Learning and the challenges that arise in its implementation [1], [2]. This confirms the importance of technological innovation in overcoming biometric security barriers [3].

While face recognition technology has significantly advanced, particularly through deep learning techniques such as Convolutional Neural Networks (CNNs), it still faces critical challenges. For example, while CNNs enhance feature extraction and system accuracy, they do not entirely resolve issues related to liveness detection, which remains a major vulnerability. This gap is particularly evident in scenarios where high-quality photos or videos can deceive existing systems. Therefore, there is an urgent need to address these limitations by developing methods that integrate both robust facial recognition and effective liveness detection.

https:doi.org/10.31763/businta.v8i2.756

Despite these advancements, face recognition-based security systems face several challenges and limitations. Fraud attempts, such as using photos or videos to spoof the system, present significant hurdles. One of the most pressing issues is the inadequacy of traditional liveness detection methods, which fail to provide a seamless and user-friendly experience. This research specifically addresses the need for more effective and user-centric liveness detection solutions. By improving these aspects, the study aims to enhance the overall reliability and adoption of face recognition systems. For instance, National Institute of Standards and Technology (NIST) has conducted several studies related to face recognition systems. One of their studies found that even the best of the 89 commercial facial recognition algorithms tested had error rates between 5% and 50% in matching digitally applied face masks with photos of the same person [4]. Traditional liveness detection methods, such as blink detection or lip movement analysis, aim to prevent such fraud but often prove cumbersome and inconvenient for users, particularly in scenarios requiring quick and seamless access. In a systematic review on face liveness detection methods, researchers noted that the complexity and user interaction required by current systems contribute to user dissatisfaction. The study calls for more intuitive and seamless methods to improve user experience while maintaining security [5]. These cumbersome methods can lead to poor user compliance and dissatisfaction, which poses a significant barrier to the widespread adoption of face recognition-based security systems.

Face recognition has emerged as a crucial technology for biometric authentication, significantly enhanced by the advent of deep learning through Convolutional Neural Networks (CNNs). CNNs are highly adept at automatically learning and extracting essential features from facial images, making them exceptionally effective. These networks can manage various challenges, such as lighting variations, different poses, and occlusions, thus improving the accuracy and robustness of face recognition systems. Deep learning-based face recognition systems have been shown to achieve performance levels comparable to human accuracy, making them a reliable tool for identity verification in diverse applications such as images [6].

However, fraud attempts also occurred, such as using photos or videos, comprehensively investigate various methods and challenges in face recognition, including its security aspects, emphasizing the importance of liveness detection in face recognition systems to avoid fraud [5], [7], [8]. Currently available liveness detection methods, such as those discussed in the literature, often pose challenges when applied to physical access control scenarios due to their cumbersome nature for users. Studies indicate that traditional liveness detection techniques can be inconvenient and uncomfortable for users, particularly in quick and seamless access scenarios [9]. Integrating liveness detection with an engaging mini-game is a potential solution. This approach aims to transform the verification process from a potential burden into an enjoyable challenge, enhancing user experience and compliance.

The specific objectives of this research are to develop and implement a novel liveness detection method that integrates face recognition with a facial expression game, evaluate its effectiveness in enhancing security and user experience, and compare its performance against traditional liveness detection methods. The study aims to demonstrate that gamification can improve user compliance and satisfaction while maintaining or improving the accuracy of liveness detection in biometric security systems. For example, research has explored the gamification of security protocols, demonstrating that well-designed game elements can effectively increase user engagement and satisfaction [10]–[13].

Moreover, good game design can bolster user immersion in any situation. Studies in game design suggest that immersive experiences significantly improve user interaction and satisfaction. By creating an engaging and seamless liveness detection experience through mini-games, users are more likely to perceive the process as less intrusive and more enjoyable, improving overall system usability and acceptance. Well-crafted game experiences can mitigate the perceived burden of security measures, making them more user-friendly and effective in real-world applications [13], [14]. Hence, this research proposes a face recognition-based security system utilizing a facial expression game to verify liveness.

The research follows the Waterfall methodology, a linear and sequential approach to software development. This involves distinct phases: requirement gathering, analysis, system design, implementation, testing, deployment, and maintenance. YuNet, a CNN-based face detection model, is employed for facial recognition, while a facial expression game is integrated to enhance liveness detection. Additionally, a web interface facilitates user interaction, and the Node MCU ESP8266 controls the door lock mechanism. This research expects a breakthrough in integrating biometric identification and liveness detection via a game.

2. Method

2.1. Research Procedures

This research applies a waterfall method to ensure that the research process runs in a structured and defined manner. The research process is divided into sequential stages to revisit the previous stages when needed. Detailed explanation of the waterfall method as show in Fig. 1 [15], [16].

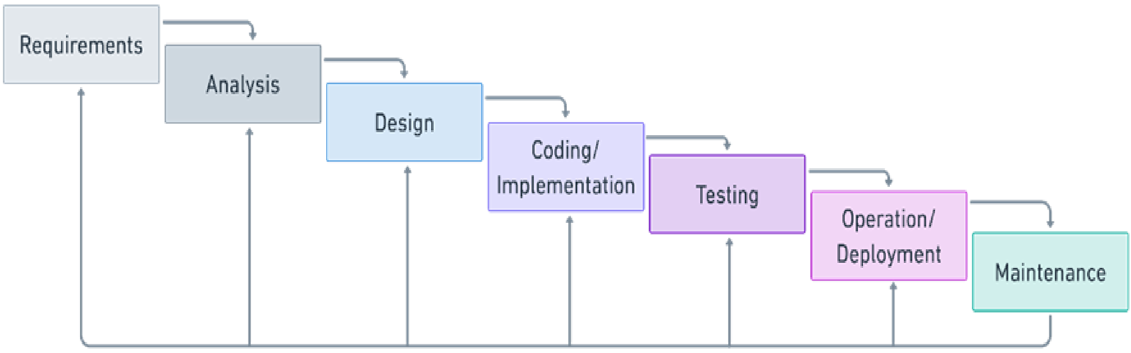


Fig. 1. Waterfall Model

2.2. Waterfall method explained

The following explains each stage of the waterfall method:

- Requirements:
  The test case for this security system is the door lock-unlock mechanism. This mechanism is a simulation of security access using face recognition. Based on this test case, it is apparent that this research requires hardware and software elements. The hardware components include nodeMCU, a relay, a power supply, a solenoid, a router, a webcam/camera, and a PC or laptop. The software element comprises Visual Studio Code for Python programming, Arduino IDE for programming nodeMCU, YuNet as the core library for face recognition method [17], and facial expression [18], [19].

- Analysis:
  Based on the requirement analysis, we conducted a system analysis to picture the correlations between these components. Fig. 2 illustrates the workflow of a face recognition-based security system integrated with an expression game for liveness detection. The process begins by capturing and sending a user’s face image via a web interface accessible through a browser. The back-end processes the retrieved image to verify the user’s identity and detect liveness by analyzing facial expressions [9], [20]. A successful verification sends an ‘unlock’ signal to the NodeMCU 8266 microcontroller. The signal activates the solenoid lock, allowing the door or gate to unlock. This system ensures that only an authenticated and alive user can gain entry.

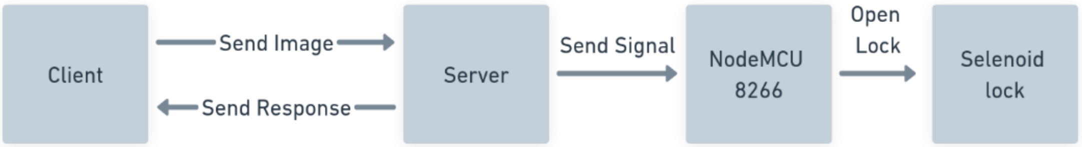


Fig. 2. System chart in outline

- Design

  We have designed three phases to enable our system to run as expected. The first phase is recording users' faces on the admin page. These faces will have the privilege to access the restricted area/spaces. The flow chart of the face recording as show in Fig. 3.

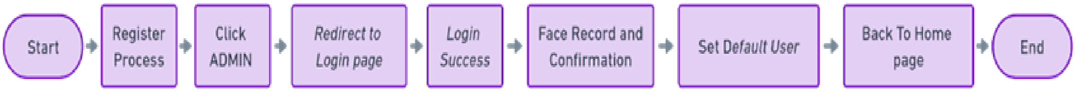


Fig. 3. Procedure face recording and user default set in the admin page

The second phase is a flowchart for the security system based on face recognition and facial expression games as show in Fig. 4.

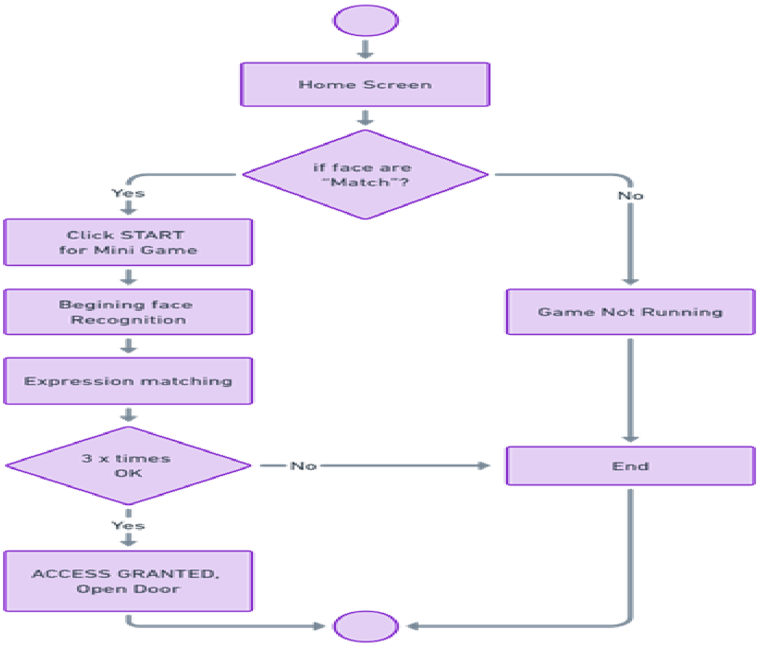


Fig. 4. Security System Flowchart

The third phase is the game design. It has minimal design elements to ensure seamless integration of the game for the biometric security system. Three facial expressions are the challenges in the liveness detection game: Sad, Neutral, and Smile. The game rule is that a user should make three facial expressions sequentially as challenged by the mini gamein a limited time a three-second time limit for each expression. Mathematically, there are $3^3 = 27$ combinations available. However, given that there are no subsequent expressions in the game challenge and at least two expressions in each challenge [21], [22], only 12 challenges the users (see Table 1).

Table.1 Expression Combinations in Mini Games

No.	Expression combinations		
	1st Expression	*2nd Expression*	*3rd Expression*
1	Smile	Sad	Normal
2	Smile	Normal	Sad
3	Smile	Sad	Smile
4	Smile	Normal	Smile
5	Normal	Sad	Smile
6	Normal	Smile	Sad
7	Normal	Sad	Normal
8	Normal	Smile	Normal
9	Sad	Normal	Smile
10	Sad	Smile	Normal
11	Sad	Normal	Sad
12	Sad	Smile	Sad

- The coding stage involves programming face recognition, facial expression recognition, and the mini-game. The environment is web-based access, wherein Python's Yunet is the core for communicating between a user and the lock-unlock control.
- Two tests will be used in the testing stage: a Black Box test and a User Acceptance Test (UAT). The Black Box Test tests the basic functionality of the system. An expert in programming should complete ten items in the black box testing (binary response) [23], [24]. Meanwhile, other participants should complete nine items in the UAT (4-scale Likert) [25], [26]. For this purpose, at least ten users of different genders and races should participate.
- The deployment system requires that it has successfully passed all the tests. To determine the appropriate sample size for our study, we utilized the Slovin method, which is designed for calculating sample sizes from a known population size with a specified margin of error. For our study, we assume the total population consisted of 100 potential users (including relatives, staff, and students from a specific department). We aimed for a 15% margin of error. Using the Slovin formula we estimated the sample size is around 31 participants. Here is the following calculations:

$$n = \frac{N}{1+N.e^2} \tag{1}$$

where N is the total population size and eee is the margin of error, we calculated the sample size as follows:

$$n = \frac{100}{1+100.(0.15^2)} \approx 30.72 \tag{2}$$

We collected data using random sampling with a questionnaire and facial recording, capturing only one image of each participant's face. This facial image was then analyzed using the YuNet algorithm to determine facial expressions such as Smile, Sad, and Normal. Validation techniques included functional testing of the biometric system, accuracy of the lock mechanism, and responsiveness of the nodeMCU system. We performed rigorous testing of the developed security system to evaluate its performance. This included benchmarking against established security systems and comparing the system's performance in terms of accuracy, reliability, and speed. Specific tests involved verifying the correct operation of the biometric recognition system, the effectiveness of the lock-unlock mechanism, and the stability of the nodeMCU connectivity. Then, we embed the lock-unlock mechanism into a miniature door. Fig. 5 shows the interconnection between components of the system. Here, we assemble a nodeMCU 8266 system connected to a WIFI network. This nodeMCU controls a relay that drives a solenoid as a door lock [19]. The nodeMCU actively 'listens' to the biometric security system signals.

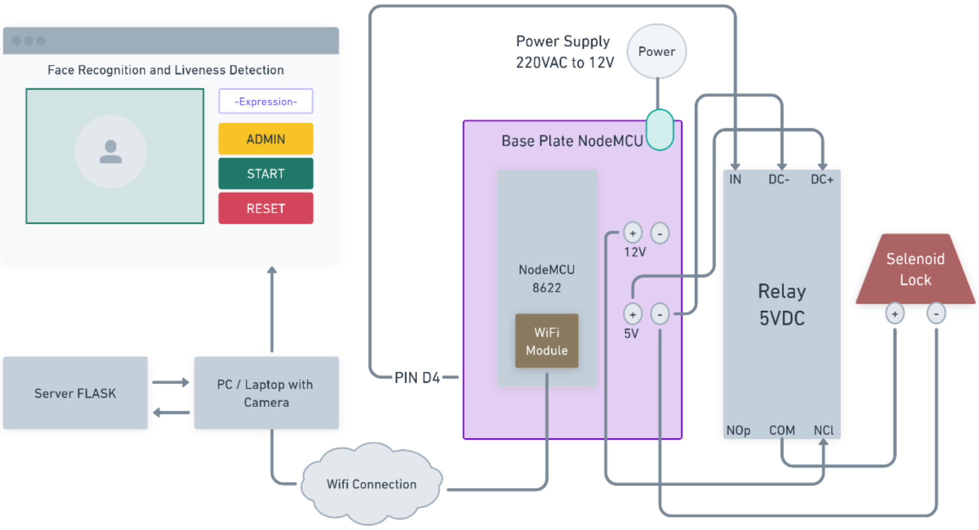


Fig. 5. System implementation and interconnection

- The maintenance phase involves modifying software to meet new customer and market trends, improving functionality, and adapting to changing environments. We expect the system to be applicable in an actual case by following the miniature prototype deployment

3. Results and Discussion

This research produced a web-based front-end with a Python back-end developed using the YuNet library. Meanwhile, we wrote the program for the hardware components using Arduino IDEA [27], [28].

3.1. Implementation of Face Recognition and Live Detection-Based Security Systems

The template is designed so that author affiliations are not repeated each time for multiple authors of the same affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization). This template was designed for two affiliations.

Fig. 6 shows the miniature prototype of our proposed system that integrates face recognition and liveness detection using facial expression games. We designed the system for environments with limited access, optimal for under 30 users, without the need for large databases.

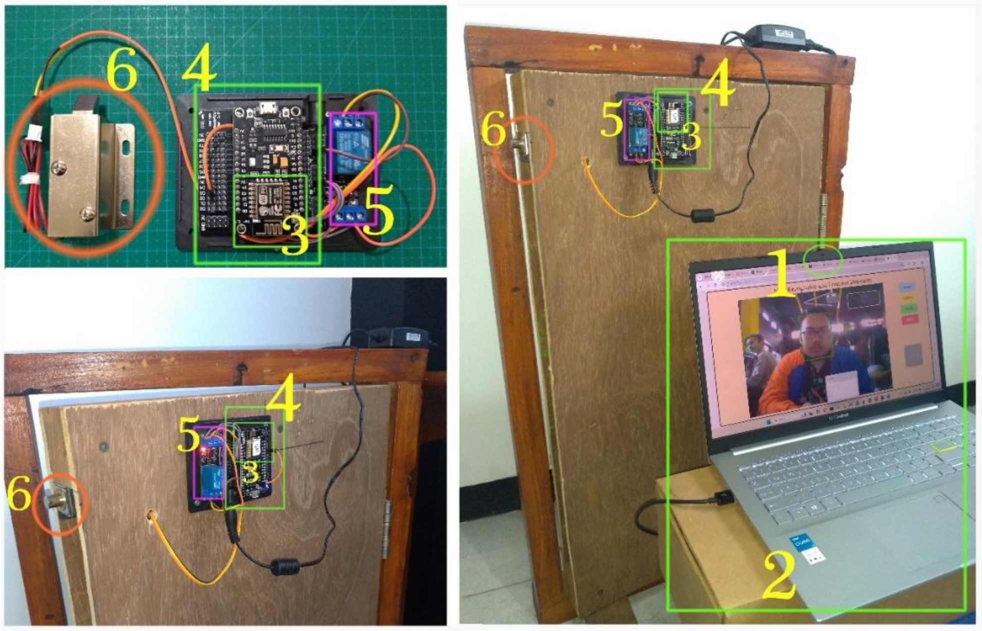


Fig. 6. The Integrated System

The system consists of several main components:

- PC/Laptop with Camera: Used to capture images of the user's face for recognition and liveness detection.
- FLASK Server: an application server that runs face recognition and liveness detection logic [29].
- Wi-Fi Module: Connects NodeMCU with a local network for communication with the FLASK server [30].
- NodeMCU ESP8266: Used as the primary controller that connects hardware with the web server [31].
- A relay that drives the solenoid to lock or unlock.
- A Solenoid lock is a digitally controlled door lock

Fig.7 shows the appearance of the front end from the user's perspective:

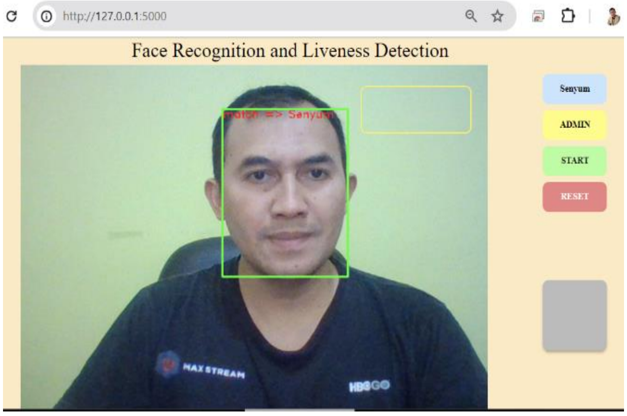
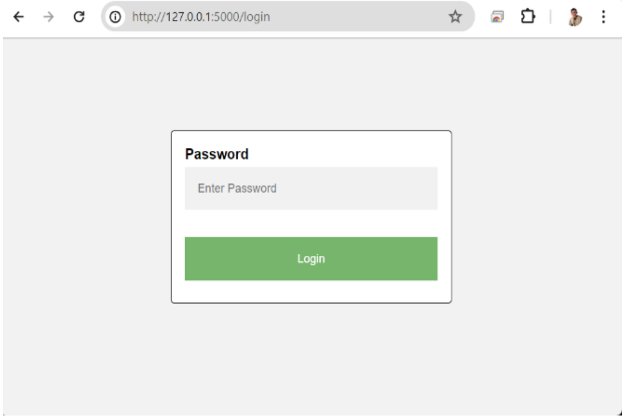


Fig. 7. Front-end look

3.2. Verification Process and Access Control

The following are the steps in the verification process:

- Admin Registration and Login
  - The process starts with the administrator logging in through an admin page to set up new users and record their faces as show in Fig. 8.



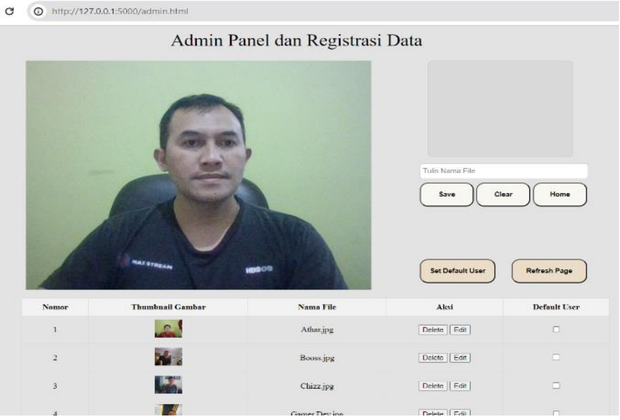
Password

Enter Password

Login

Fig. 8. Verification Page

  - After a successful login, the admin can record faces and set the default user. Users should ensure that their face is visible during the face capture as show in Fig. 9.



Admin Panel dan Registrasi Data

Nomor	Thumbnail Gambar	Nama File	Aksi	Default User
1		Athar.jpg	Delete Edit	□
2		Booss.jpg	Delete Edit	□
3		Chizz.jpg	Delete Edit	□
4		Gamer Dev.jpg	Delete Edit	□

Fig. 9. Admin Panel

- Verification
  - Face detection verification see Fig. 10

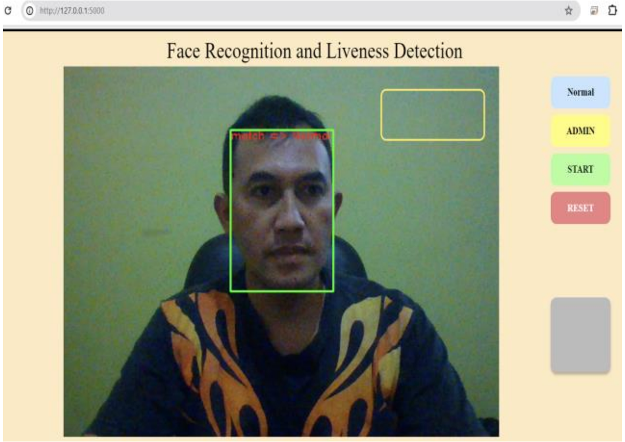


Fig. 10. Face detection

- Once a successful face detection has been made, the user can proceed to the liveness detection via an expression mini-game. Fig. 11 shows the liveness detection in action.

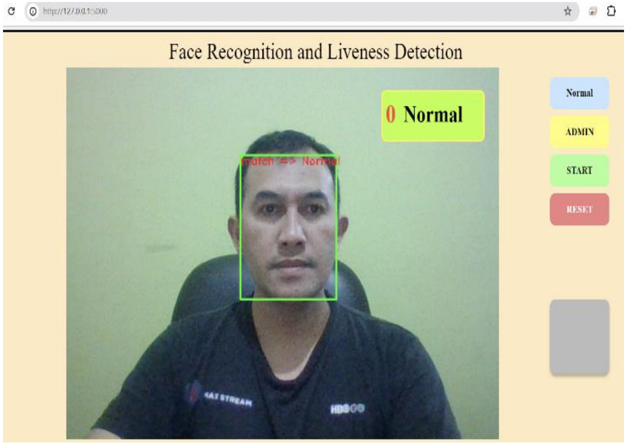


Fig. 11. Example expression according to the requested yellow box

- In the 3-second time limit, an expression challenge (the text on the top-right side) shows. After three completed challenges, the system displays the Access Granted indicator on the bottom right side of the page. From this point, the system sends a signal to unlock the door for 5 seconds as show in Fig. 12.

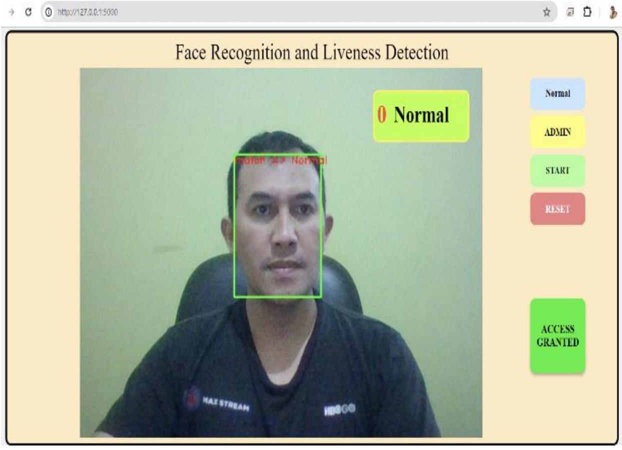


Fig. 12. The user has completed three challenges, and the “Access Granted” box appears

3.3. Black box test and UAT Result

See Table 2 for the resulting Black box test completed by an expert in programming:

Table.2 Black Box Test Result

No.	Feature Tested	Testing Steps	Expected Result	Status (Pass/Fail)
1	Admin Login	Enter valid credentials and click login	Admin logs in successfully	Pass
2	Admin Login	Enter invalid credentials and click login	Error message appears	Pass
3	Face Registration	Register a new user's face	Successfully recorded face	Pass
4	Expression Verification	Display smile, sad, and neutral expressions	The system recognizes all expressions	Pass
5	Expression Verification	Display incorrect expressions	The system rejects the verification	Pass
6	Solenoid Lock Activation	Perform correct verification	Solenoid lock opens	Pass
7	Solenoid Lock Activation	Perform incorrect verification	The Solenoid lock remains closed	Pass
8	Reset Button	Click the reset button	System resets	Pass
9	Wi-Fi Connection	Disable Wi-Fi on NodeMCU	System displays an error message	Pass
10	Power Outage	Turn off and on the power supply	System returns to the initial state	Pass

Table 3 shows the result of UAT

Table.3 UAT from Participant

No.	Sample Question						
	Question	*1*	*2*	*3*	*4*	*Total User Response*	*Average*
1	Did you find the user interface easy to use? User Response: (1) Very Difficult - (4) Very Easy	0	0	2	8	10	3,8
2	Did the admin login process go smoothly? User Response: (1) Very Difficult - (4) Very Easy	0	0	0	10	10	4
3	Did the face registration process work well? User Response: (1) Very Difficult - (4) Very Easy	0	0	2	8	10	3,8
4	Did the system correctly recognize your facial expressions? User Response: (1) Very Difficult - (4) Very Easy	0	0	2	8	10	3,8
5	Do you feel that the facial expression verification is secure enough? User Response: (1) Very Insecure - (4) Very Secure	0	0	3	7	10	3,7
6	Did the solenoid lock function correctly after a successful verification? User Response: (1) Very Poorly - (4) Very Well	0	0	1	9	10	3,9
7	Do you think the system is effective in preventing identity fraud? User Response: (1) Very Ineffective - (4) Very effective	0	0	4	6	10	3,6
8	Did the reset button work as expected? User Response: (1) Very Poorly - (4) Very Well	0	0	1	9	10	3,7
9	What is your overall experience with using this system? User Response: (1) Very Poor - (4) Very Good	0	0	2	8	10	3,8

The feedback from ten participants is positive across all aspects evaluated. Here are the main takeaways:

- Ease of Use: The user interface is generally perceived as very easy to use, with a high average rating of 3.8. This indicates that most users found it user-friendly.
- Admin Login Process: This aspect received a perfect score, with all respondents rating it as very easy, resulting in an average rating of 4. This suggests that the admin login process is highly efficient and user-friendly.
- Face Registration and Recognition: The face registration process and the system's ability to recognize facial expressions received an average rating of 3.8. This indicates a positive experience, though there may be room for minor improvements.
- Security: The Security of the facial expression verification system received an average rating of 3.7, showing that while most users feel secure, a few have concerns that should be addressed accordingly.
- Solenoid Lock Functionality: The functionality of the solenoid lock after verification received a high rating of 3.9, indicating reliable performance.
- Effectiveness in Preventing Identity Fraud: This aspect received the lowest average rating (3.6), suggesting that while most users find it practical, there is a perception that it can improve.
- Reset Button: The reset button's functionality is rated positively, with an average of 3.7, showing general satisfaction with its performance.
- Overall Experience: The overall experience with the system is rated highly, with an average of 3.8, indicating that users are delighted.

In addition, we also recorded the duration when users use this system. Regarding the overall time required for face recognition from the start to receiving "Access Granted," the average duration across 10 attempts was calculated to be 16.31 seconds. Table. 4 shows the response durations from 10 users.

Table.4 User access duration

Attempt	1	2	3	4	5	6	7	8	9	10
Time (seconds)	17,82	18,61	16,87	16,15	15,29	15,67	15,60	15,43	16,22	15,44

3.4. Discussion

From the results based on the experiments and tests show that our system is working properly. However, several anomalies and extreme findings were observed during the testing phase. One significant challenge was encountered when the system attempted to differentiate between identical twins. The facial recognition system, which relies on detecting facial features and encoding them into an array, found it difficult to distinguish between twins. As a result, the system consistently identified both faces as matching, leading to potential security vulnerabilities in scenarios involving identical twins.

Another notable finding was related to the detection of sad expressions. Several users experienced difficulties in expressing sadness within the 3-second window provided by the system. This led to a failure to capture the sad expression within the allotted time, highlighting a limitation in the system's ability to accurately recognize and respond to this facial expression. This issue suggests a need for further refinement in the algorithm to accommodate a wider range of emotional expressions more effectively.

From a social point of view, these findings raise important questions about the inclusivity and reliability of biometric systems in diverse real-world applications. The difficulty in distinguishing between identical twins highlights potential privacy and security concerns, particularly in contexts where precise identification is crucial. Furthermore, the challenge in recognizing sad expressions within a limited time frame points to broader issues of user experience and accessibility. If the system cannot reliably capture a range of emotional states, it may affect user trust and satisfaction. Addressing these concerns is essential to developing a more robust and socially adaptable biometric system that considers the nuances of individual differences and emotional expression.

These findings have significant implications for our research objectives and contribute to the existing literature on facial recognition and liveness detection systems. The challenge in distinguishing identical twins aligns with previous studies [32] that highlight the limitations of current facial recognition technologies in dealing with genetically similar individuals. This underscores the need for more advanced algorithms that can detect subtle differences, perhaps by incorporating additional biometric data or environmental factors.

The difficulty in capturing sad expressions within the time limit relates to broader research on emotion recognition in AI systems [33]. Our findings suggest the temporal aspect of emotion expression is a critical factor underexplored in existing literature. This opens up new avenues for research into dynamic emotion recognition systems that can adapt to individual differences in expression timing and intensity.

The overall success rate of 95% for smile and normal expressions demonstrates the potential of our integrated facial expression game approach for enhancing liveness detection. This aligns with recent studies [34] that emphasize the importance of user engagement in security systems. However, the lower success rate for sad expressions highlights the need for a more nuanced approach to emotion recognition, particularly for complex or subtle emotions.

Our research contributes to the growing body of literature on biometric security by demonstrating the feasibility of integrating gamified elements into liveness detection. The average completion time of 16.31 seconds for the facial expression mini-game suggests a balance between security and user convenience, an aspect that is often challenging to achieve in biometric systems [35].

Another compare the results of the study with findings from existing literature or similar research studies as show in Table 5.

- Rathgeb, C., Dantcheva, A., & Busch, C. (2021). Impact and detection of facial beautification in face recognition: An overview. IEEE Access, 9, 58950-58969 [36].
- Rao, S., Huang, Y., Cui, K. and Li, Y., 2022. Anti-spoofing face recognition using a metasurface-based snapshot hyperspectral image sensor. *Optica*, *9*(11), pp.1253-1259 [37].

Table.5 Comparation Aspect of Method

Aspect	Current Study	Rathgeb et al. (2021)	Rao et al. (2022)
Overall Face Recognition Accuracy	95% success rate for smile and normal expressions	92.5% (average across multiple datasets)	97.98% (for anti-spoofing accuracy)
Twin Differentiation	Identified as a significant challenge, with difficulty distinguishing between identical twins	Not specifically addressed	Not specifically addressed
Emotion Recognition Accuracy	95% success rate for smile and normal expressions, with challenges for sad expressions	Not addressed	Not addressed (focused on liveness detection, not emotion recognition)
Liveness Detection Method	Expression-based liveness detection using YuNet algorithm, also integrated facial expression game approach	Various methods reviewed, including texture and motion analysis	Hyperspectral imagingusing metasurface-based sensor
Average Authentication Time	16.31 seconds for the facial expression mini-game	Not specified	50 ms for capturing hyperspectral image (full authentication time not specified)

Comparing our results with recent advanced research in anti-spoofing face recognition reveals interesting contrasts in approach and performance. **Rathgeb et al. (2021)** reported an average overall accuracy of **92.5%** across multiple datasets, which is slightly lower than our system's **95%** face recognition accuracy. This suggests that our system is highly effective, particularly in recognizing smile and normal expressions.

While our study encountered challenges in twin differentiation, this specific aspect was not addressed in either **Rathgeb et al. (2021)** or **Rao et al. (2022)**. Our system's unique contribution lies in its ability to recognize emotions, achieving **95%** accuracy for smile and normal expressions, although with lower accuracy for sad expressions. Neither of the compared studies addressed emotion recognition, focusing instead on other aspects such as anti-spoofing and liveness detection.

The most significant difference lies in the liveness detection method. Our approach utilizes a facial expression game, which engages the user and potentially offers a more interactive experience. **Rathgeb et al. (2021)** reviewed various methods, including texture and motion analysis, while **Rao et al. (2022)** employed a sophisticated hyperspectral imaging technique using a metasurface-based sensor, which can detect subtle spectral differences between real skin and spoofing materials.

In terms of authentication time, our system averages **16.31 seconds,** which includes the time for the user to complete the facial expression game. **Rao et al.'s** system captures a hyperspectral image in just **50 ms,** although the total authentication time is not specified. This suggests that their method might offer faster authentication, but possibly at the cost of user engagement.

These comparisons highlight the diverse approaches in tackling the challenge of secure face recognition and anti-spoofing. While **Rao et al.'s** method offers high accuracy and potentially faster operation through advanced hardware, our system provides a more comprehensive approach including emotion recognition and user interaction. Future work could explore integrating aspects of both approaches to create a system that is both highly secure and user-friendly.

One limitation encountered in this study is the prototype nature of the user interface (UI/UX), which may have influenced the outcomes of user testing. The prototype interface may not fully represent the final product's usability and functionality, potentially affecting user interactions and the overall user experience. This limitation should be taken into consideration when interpreting the results and planning future iterations of the system.

The practical implications of these findings are significant for real-world applications. The difficulty in distinguishing between identical twins suggests that biometric security systems need to incorporate additional verification methods or biometric data to ensure reliability in high-security environments. The challenge in recognizing sad expressions within a short timeframe indicates a need for systems to be adaptable to different emotional states and expressions, which is crucial for user acceptance and trust. These improvements can enhance the inclusivity and accuracy of biometric systems, making them more applicable and effective in diverse settings. Furthermore, the integration of gamified elements into liveness detection not only enhances security but also improves user engagement, potentially increasing the adoption of biometric technologies in everyday applications.

4. Conclusion

The results of usability and UAT testing show that this face recognition and liveness detection-based security system is working as expected. With high accuracy and speed, and positive user experience, the system has enormous potential for use in environments with limited access. The key findings of this study include significant challenges in distinguishing between identical twins, as the system struggled to differentiate between faces with similar features, leading to potential security vulnerabilities. Additionally, participants experienced difficulties in expressing sadness within the 3-second window provided by the system, highlighting limitations in the system's ability to accurately capture and interpret this emotional state. These findings underscore the need for improvements in facial recognition algorithms to address these issues.

However, there are some areas that need improvement, especially related to lighting conditions and clarity of expression instructions. Further development should focus on improving detection algorithms, improving interfaces, and training users to ensure the system can function optimally in a variety of conditions and is easy for all to use, This conclusion aligns with the research objectives stated in the Introduction, as the study aimed to develop a robust face recognition system and identify areas for improvement. The research successfully addressed the gaps by evaluating the system's performance and providing actionable insights into its strengths and limitations.

Recommendations include*:*

- **Enhance Security Features**: Since the Security of facial expression verification and the system's effectiveness in preventing identity fraud received slightly lower ratings, focusing on enhancing these features could improve user confidence and satisfaction.
- **Minor Tweaks in User Interface**: While the user interface received a high rating, continuous minor improvements could ensure it remains user-friendly as expectations evolve.
- **Detailed User Feedback**: Collecting more detailed feedback on specific concerns related to security and fraud prevention could provide insights into targeted improvements.

By addressing these areas, the system can ensure even higher satisfaction and reliability in future evaluations. Looking ahead, potential future research directions could involve developing a database system for a wider range of users and addressing the tailgating aspect with additional safety factors. These explorations could significantly advance the field of biometric security technology.

In addition to the design and development of face recognition-based tools, there are several obstacles that need to be developed again in future research, such as using a database system for a wider range of users. However, the equipment that has been used today as a prototype is sufficient as a basic need for access to limited space. The tailgating aspect also needs to be considered again as the addition of more relevant safety factors [38], [39]. The results of the system's implementation and evaluation show that the integration of face recognition with liveness detection through expression games can significantly improve the system's security. The system not only offers more accurate biometric verification but also provides a better and challenging user experience. With its high accuracy and effectiveness in preventing fraud, the system offers a valuable contribution to the development of face recognition-based security technology.

References

[1] M. Wang and W. Deng, "Deep face recognition: A survey," *Neurocomputing*, vol. 429, pp. 215–244, 2021, doi: 10.1016/j.neucom.2020.10.081.

[2] A. P. Wibawa, W. A. Yudha Pratama, A. N. Handayani, and A. Ghosh, "Convolutional Neural Network (CNN) to determine the character of wayang kulit," *Int. J. Vis. Perform. Arts*, vol. 3, no. 1, pp. 1–8, Jun. 2021, doi: 10.31763/viperarts.v3i1.373.

[3] S. B. R. Prasad and B. S. Chandana, "Mobilenetv3: a deep learning technique for human face expressions identification," *Int. J. Inf. Technol.*, vol. 15, no. 6, pp. 3229–3243, 2023, doi: 10.1007/s41870-023-01380-x.

[4] M. Ngan, P. Grother, and K. Hanaoka, "Ongoing Face Recognition Vendor Test (FRVT) part 6A:," National Institute of Standards and Technology, Gaithersburg, MD, Jul. 2020. doi: 10.6028/NIST.IR.8311.

[5] S. Khairnar, S. Gite, K. Kotecha, and S. D. Thepade, "Face Liveness Detection Using Artificial Intelligence Techniques: A Systematic Literature Review and Future Directions," *Big Data Cogn. Comput.*, vol. 7, no. 1, p. 37, Feb. 2023, doi: 10.3390/bdcc7010037.

[6] A. P. Wibawa *et al.*, "Decoding and preserving Indonesia's iconic Keris via A CNN-based classification," *Telemat. Informatics Reports*, vol. 13, p. 100120, 2024, doi: 10.1016/j.teler.2024.100120.

[7] R. Koshy and A. Mahmood, "Enhanced Deep Learning Architectures for Face Liveness Detection for Static and Video Sequences," *Entropy*, vol. 22, no. 10, p. 1186, Oct. 2020, doi: 10.3390/e22101186.

[8] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, "Face recognition: A literature survey," *ACM Comput. Surv.*, vol. 35, no. 4, pp. 399–458, 2003, doi: 10.1145/954339.954342.

[9] D. Srivastava, P. Shukla, and A. K. Sahani, "Face Verification System with Liveness Detection," in *2021 IEEE 18th India Council International Conference (INDICON)*, 2021, pp. 1–5, doi: 10.1109/INDICON52576.2021.9691561.

[10] V. V Zolotarev, S. O. Knyazuk, and E. A. Maro, "Liveness Detection Mechanisms to Enhance Robustness of Authentication Methods in Game-Based Educational Services," in *2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, 2020, pp. 566–570, doi: 10.1109/ITQMIS51053.2020.9322889.

[11] M. R. Dronky, W. Khalifa, and M. Roushdy, "A Review on Iris Liveness Detection Techniques," in *2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS)*, 2019, pp. 48–59, doi: 10.1109/ICICIS46948.2019.9014719.

[12] N. Rogmann and M. Krieg, "Liveness Detection in Biometrics," in *2015 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2015, pp. 1–14, doi: 10.1109/BIOSIG.2015.7314611.

[13] H. A. Rosyid, M. Palmerlee, and K. Chen, "Deploying learning materials to game content for serious education game development: A case study," *Entertain. Comput.*, vol. 26, pp. 1–9, May 2018, doi: 10.1016/j.entcom.2018.01.001.

[14] H. A. Rosyid, A. Y. Pangestu, and M. I. Akbar, "Can Diegetic User Interface Improves Immersion in Role-Playing Games?," in *2021 7th International Conference on Electrical, Electronics and Information Engineering (ICEEIE)*, 2021, pp. 200–204, doi: 10.1109/ICEEIE52663.2021.9616732.

[15] S. M. Khan, *Waterfall Model Used in Software Development Reference: Software Requirements Engineering Waterfall Model*. pp. 1-3, 2023. [Online]. Available at: https://www.researchgate.net/profile/Sardar-Mudassar-Khan-2/publication/371902449.

[16] U. S. Senarath, "Waterfall methodology, prototyping and agile development," *Tech. Rep.*, pp. 1–16, 2021, [Online]. Available at: https://www.researchgate.net/profile/Udesh-S-Senarath/publication/353324450.

[17] W. Wu, H. Peng, and S. Yu, "YuNet: A Tiny Millisecond-level Face Detector," *Mach. Intell. Res.*, vol. 20, no. 5, pp. 656–665, 2023, doi: 10.1007/s11633-023-1423-y.

[18] Make It CA, "NodeMCU ESP8266: Details and Specifications," *Website*, 2024.

[19] S. Barai, D. Biswas, and B. Sau, "Estimate distance measurement using NodeMCU ESP8266 based on RSSI technique," in *2017 IEEE Conference on Antenna Measurements & Applications (CAMA)*, 2017, pp. 170–173, doi: 10.1109/CAMA.2017.8273392.

[20] M. M. Hasan, M. S. U. Yusuf, T. I. Rohan, and S. Roy, "Efficient two stage approach to detect face liveness : Motion based and Deep learning based," in *2019 4th International Conference on Electrical Information and Communication Technology (EICT)*, 2019, pp. 1–6, doi: 10.1109/EICT48899.2019.9068813.

[21] H. A. Rosyid, S. Patmanthara, and I. R. Cahyudi, *Game development*. Ahlimedia Book, 2021.

[22] I. Patidar, K. S. Modh, and C. Chattopadhyay, "Artificially Intelligent Game Framework Based on Facial Expression Recognition BT - Computer Vision, Pattern Recognition, Image Processing, and Graphics," 2020, pp. 312–321, doi: 10.1007/978-981-15-8697-2_29.

[23] Z. Aghababaeyan, M. Abdellatif, L. Briand, S. R., and M. Bagherzadeh, "Black-Box Testing of Deep Neural Networks through Test Case Diversity," *IEEE Trans. Softw. Eng.*, vol. 49, no. 5, pp. 3182–3204, 2023, doi: 10.1109/TSE.2023.3243522.

[24] I. Bhatti, J. A. Siddiqi, A. Moiz, and Z. A. Memon, "Towards Ad hoc Testing Technique Effectiveness in Software Testing Life Cycle," in *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, 2019, pp. 1–6, doi: 10.1109/ICOMET.2019.8673390.

[25] E. Alégroth, M. Nass, and H. H. Olsson, "JAutomate: A Tool for System- and Acceptance-test Automation," in *2013 IEEE Sixth International Conference on Software Testing, Verification and Validation*, 2013, pp. 439–446, doi: 10.1109/ICST.2013.61.

[26] A. Sadaj, M. Ochodek, S. Kopczyńska, and J. Nawrocki, "Maintainability of Automatic Acceptance Tests for Web Applications—A Case Study Comparing Two Approaches to Organizing Code of Test Cases BT - SOFSEM 2020: Theory and Practice of Computer Science," 2020, pp. 454–466, doi: 10.1007/978-3-030-38919-2_37.

[27] D. Garlan and M. Shaw, "An introduction to software architecture," in *Advances in software engineering and knowledge engineering*, World Scientific, 1993, pp. 1–39, doi: 10.1142/9789812798039_0001.

[28] O. E. Amestica, P. E. Melin, C. R. Duran-Faundez, and G. R. Lagos, “An Experimental Comparison of Arduino IDE Compatible Platforms for Digital Control and Data Acquisition Applications,” in *2019 IEEE CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*, 2019, pp. 1–6, doi: 10.1109/CHILECON47746.2019.8986865.

[29] M. Grinberg, *Flask web development*, 2nd ed. “ O’Reilly Media, Inc.,” p. 30, 2018. [Online]. Available at: https://www.oreilly.com/library/view/flask-web-development/9781491991725/.

[30] J. Hunt, “Flask Web Services,” in *Advanced Guide to Python 3 Programming*, Springer, 2023, pp. 575–581, doi: 10.1007/978-3-031-40336-1_51.

[31] K. P., D. M., L. B. M., and G. N., “Design and Development of NodeMCU Based Smart IoT Door System,” in *2023 4th International Conference on Smart Electronics and Communication (ICOSEC)*, 2023, pp. 398–403, doi: 10.1109/ICOSEC58147.2023.10275975.

[32] Y. Sun, X. Wang, and X. Tang, “Deep learning face representation from predicting 10,000 classes,” in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2014, pp. 1891–1898, doi: 10.1109/CVPR.2014.244.

[33] S. Li and W. Deng, “Deep facial expression recognition: A survey,” *IEEE Trans. Affect. Comput.*, vol. 13, no. 3, pp. 1195–1215, 2020, doi: 10.1109/TAFFC.2020.2981446.

[34] V. M. Patel, R. Chellappa, D. Chandra, and B. Barbello, “Continuous user authentication on mobile devices: Recent progress and remaining challenges,” *IEEE Signal Process. Mag.*, vol. 33, no. 4, pp. 49–61, 2016, doi: 10.1109/MSP.2016.2555335.

[35] S. Bhattacharya, G. S. Nainala, P. Das, and A. Routray, “Smart attendance monitoring system (SAMS): a face recognition based attendance system for classroom environment,” in *2018 IEEE 18th international conference on advanced learning technologies (ICALT)*, 2018, pp. 358–360, doi: 10.1109/ICALT.2018.00090.

[36] C. Rathgeb, A. Dantcheva, and C. Busch, “Impact and detection of facial beautification in face recognition: An overview,” *IEEE Access*, vol. 7, pp. 152667–152678, 2019, doi: 10.1109/ACCESS.2019.2948526.

[37] S. Rao, Y. Huang, K. Cui, and Y. Li, “Anti-spoofing face recognition using a metasurface-based snapshot hyperspectral image sensor,” *Optica*, vol. 9, no. 11, pp. 1253–1259, 2022, doi: 10.1364/OPTICA.469653.

[38] J. Akati and M. Conrad, “Anti-Tailgating Solution Using Biometric Authentication, Motion Sensors and Image Recognition,” in *2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, 2021, pp. 825–830, doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech52372.2021.00137.

[39] M. O. Oloyede, G. P. Hancke, and N. Kapileswar, “Evaluating the effect of occlusion in face recognition systems,” in *2017 IEEE AFRICON*, 2017, pp. 1547–1551, doi: 10.1109/AFRCON.2017.8095712.