Pertanika Proceedings 1 (3): 45 - 49 (2025)

PERTANIKA JOURNALS

PERTANIKA PROCEEDINGS

Journal homepage: http://www.pertanika.upm.edu.my/

Minimizing Face Spoofing Attacks with Liveness Detection in Cross-Platform Mobile Attendance Systems

Bagus Subagja, Dian Anggraini* and Asyifa Imanda Septiana

Software Engineering, Kampus Cibiru, Universitas Pendidikan Indonesia, 40625 Bandung, Jawa Barat, Indonesia

ABSTRACT

Attendance systems have now implemented many of the most recent technologies, such as the use of facial recognition to verify and validate student attendance in lecture classes. However, face recognition technology in the attendance systems is still prone to fraud with attacks using artificial faces through various media, such as printed photos or pre-recorded videos. Therefore, a liveness detection system is needed that can minimize the fraud. The liveness detection system using the randomized challenge-response method, with several randomly given challenges within a time limit, can indicate whether the detected face is genuinely alive. This liveness detection system is implemented in a cross-platform mobile-based digital attendance application called "My Attendance" developed using the Flutter framework. Student attendance records are stored and can be viewed by lecturers as proof of attendance in lecture classes. The results of the study show that this liveness detection system can minimize the occurrence of fraudulent artificial face attacks, achieving 100% performance accuracy when tested on 30 respondents from students of the Software Engineering study program at the Indonesian Education University. This system could be an effective and efficient solution for applying face recognition systems to the attendance process.

Keywords: Attendance system, face spoofing attack, liveness detection, mobile cross-platform

ARTICLE INFO

Article history:
Received: 30 April 2025
Published: 17 July 2025

DOI: https://doi.org/10.47836/pp.1.3.009

E-mail addresses:
bagussubagja@upi.edu (Bagus Subagja)
dian.anggraini@upi.edu (Dian Anggraini)
asyifa@upi.edu (Asyifa Imanda Septiana)
* Corresponding author

INTRODUCTION

Technology nowadays has developed and influenced various fields in human life, which has become a necessity in daily activities. One of the fields that has implemented sophisticated technology now is the attendance system found in the educational environment that uses face recognition (Sunaryono et al., 2021).

e-ISSN: 3083-9475

Technology has advanced rapidly and has had a significant impact on many aspects of human life, becoming an essential part of daily activities. One notable field that has adopted sophisticated technology is the educational environment, where attendance systems now use facial recognition technology.

Problem Statement

However, face recognition systems are generally vulnerable to spoofing fraud (Hadiprakoso & Buana, 2021) because they frequently cannot distinguish between real and fake faces, creating a significant security risk (Chakraborty & Das, 2014). Spoofing is penetrating the recognition system's biometric authentication using fake face videos and printed photos (Karmakar et al., 2021; Khairnar et al., 2023).

Research Question

To mitigate spoofing attacks in face recognition systems, implementing liveness detection is crucial for distinguishing between real and fake faces (Li et al., 2018). Given that spoofing poses a significant threat to attendance systems using face recognition technology, research is needed to minimize attendance fraud (Singh & Arora, 2017; Ramachandra & Busch, 2017). This study focuses on two aspects: developing and analyzing a liveness detection system using randomized challenge-response methods for mobile cross-platform attendance systems, and examining the failure rate of attendance attempts using this system (Biørn-Hansen et al., 2018; Zohud & Zein, 2021). These objectives aim to enhance the security and reliability of facial recognition-based attendance while evaluating the effectiveness of the proposed solution (Kaur & Kaur, 2022).

SYSTEM DEVELOPMENT FOR LIVENESS DETECTION

Randomized Challenge Response Liveness Detection Methods

The research will assess the system's effectiveness using key performance metrics such as accuracy, precision, recall, and F-score, while also analyzing failure rates in attendance experiments to provide a comprehensive evaluation of real-world performance. Researchers will conduct testing based on these four scenarios, detailed in Table 1, to represent the capabilities of the liveness detection system under study, ensuring a thorough examination of its functionality and reliability in various conditions. The liveness detection process begins with a 45-second scan featuring six random challenges, each lasting approximately 7.5 seconds. If face detection fails, the process restarts to prevent spoofing. The system captures a final facial image after successful challenge completion. The testing scenarios are shown in Table 1.

Table 1
The test scenario is given to the participant

Scenario	Description	Notes
Scenario I	Students must attend using their actual faces, ensuring successful verification and attendance through real face detection.	All students are given 20 minutes to attend scenario I.
Scenario II	Students attempting attendance with artificial video faces should fail verification, as the liveness detection system will identify them as fake faces.	Testing with the face resulting from this artificial video recording is given a chance 3 times.
Scenario III	Students using their real faces should fail the attendance verification due to a system error or malfunction.	All students are given 20 minutes to attend scenario III.
Scenario IV	Students using artificial video faces with matched movements should fail verification, as the system should identify simulated faces despite mimicked liveness gestures.	Testing with the face resulting From this artificial video recording, it is given a chance 3 times.

RESULT AND DISCUSSION

Liveness Detection System Testing Results

Based on the results of the research survey in the previous point, the confusion matrix parameter values were obtained to evaluate the performance of the tested liveness detection as shown in Figure 1.

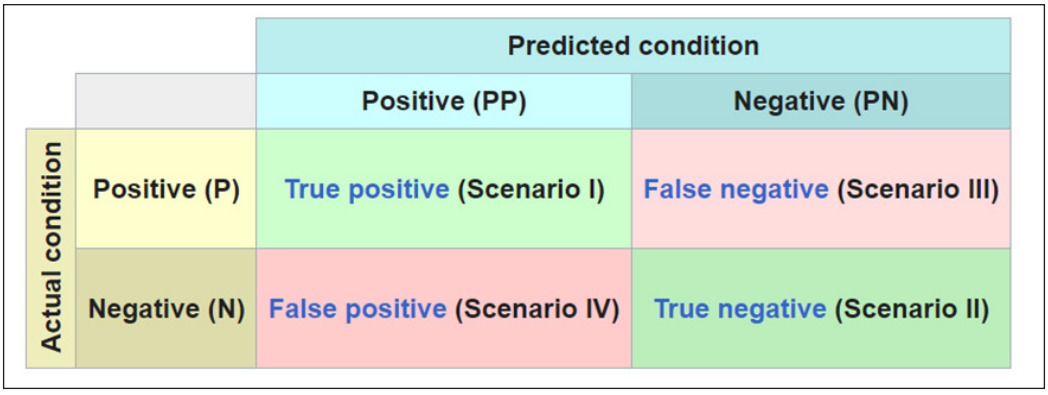

Figure 1. Testing scenarios and their relationship with confusion matrix values and the values obtained from discussion points of research survey results

The liveness detection system using a randomized challenge-response method achieved flawless results in testing, with 100% accuracy, precision, recall, and F-score. It effectively distinguished live faces from spoofing attempts without errors, proving its robustness and reliability. This highlights its potential as a highly secure solution for face recognition-based

systems, setting a new standard in liveness detection. During testing of a mobile attendance system's liveness detection, all 30 participants completed Scenarios I and III (real faces) within 20 minutes. Scenario I had a 33% initial failure rate (15/45 attempts), and Scenario III had a 23% rate (9/39 attempts). While all participants eventually succeeded, the results highlight the need to improve first-attempt success rates and system efficiency.

CONCLUSION

The liveness detection system achieved 100% accuracy in minimizing face spoofing attacks. However, analysis of Scenarios I and III revealed significant initial failure rates (33% and 23%, respectively) before all participants succeeded. While the system ultimately proved effective, these initial challenges across different conditions suggest room for improvement in consistency and user experience. The research demonstrates the system's overall success in preventing spoofing, but also highlights the need for refinements to reduce initial failures and enhance performance across various usage scenarios.

ACKNOWLEDGEMENT

The author is profoundly grateful to Universitas Pendidikan Indonesia (UPI) for the generous support and invaluable opportunity to undertake and complete this research. The resources and assistance provided by UPI have been pivotal to the successful completion of this project

REFERENCES

Biørn-Hansen, A., Grønli, T. M., & Ghinea, G. (2018). A survey and taxonomy of core concepts and research challenges in cross-platform mobile development. *ACM Computing Surveys (CSUR)*, *51*(5), 1-34. https://doi.org/10.1145/3241739

Chakraborty, S., & Das, D. (2014). An overview of face liveness detection. *International Journal on Information Theory*, *3*(2), 11–25. https://doi.org/10.5121/ijit.2014.3202

Hadiprakoso, R. B., & Buana, I. K. S. (2021). Deteksi serangan spoofing wajah menggunakan convolutional neural network. *Jurnal Teknik Informatika dan Sistem Informasi*, *7*(3), 618-626. https://doi.org/10.28932/jutisi.v7i3.4001

Karmakar, D., Mukherjee, P., & Datta, M. (2021). Spoofed facial presentation attack detection by multivariate gradient descriptor in micro-expression region. *Pattern Recognition and Image Analysis*, *31*(2), 285–294. https://doi.org/10.1134/S1054661821020097

Kaur, A., & Kaur, K. (2022). Systematic literature review of mobile application development and testing effort estimation. *Journal of King Saud University-Computer and Information Sciences*, *34*(2), 1-15. https://doi.org/10.1016/j.jksuci.2018.11.002

Khairnar, S., Gite, S., Kotecha, K., & Thepade, S. D. (2023). Khairnar, S., Gite, S., Kotecha, K., & Thepade, S. D. (2023). Face liveness detection using artificial intelligence techniques: A systematic literature review

and future directions. *Big Data and Cognitive Computing*, *7*(1), Article 37. https://doi.org/10.3390/bdcc7010037

Ramachandra, R., & Busch, C. (2017). Presentation attack detection methods for face recognition systems: A comprehensive survey. *ACM Computing Surveys*, 50(1), Article 8. https://doi.org/10.1145/3038924

Singh, M., & Arora, A. S. (2017). A robust anti-spoofing technique for face liveness detection with morphological operations. *Optik, 139*, 347–354. https://doi.org/10.1016/j.ijleo.2017.04.004

Sunaryono, D., Siswantoro, J., & Anggoro, R. (2021). An android based course attendance system using face recognition. *Journal of King Saud University - Computer and Information Sciences, 33*(3), 304–312. https://doi.org/10.1016/j.jksuci.2019.01.006

Zohud, T., & Zein, S. (2021). Cross-platform mobile app development in industry: A Multiple case-study. *International Journal of Computing*, *20*(1), 46–54. https://doi.org/10.47839/ijc.20.1.2091