International Journal of Innovative Computing, Information and Control
Volume **19**, Number **2**, April **2023**

ICIC International ©2023 ISSN 1349-4198
pp. **419–430**

LIVENESS DETECTION WITH RANDOMIZED CHALLENGE-RESPONSE FOR FACE RECOGNITION ANTI-SPOOFING

Christian Widjaya and Arya Wicaksana*

Department of Informatics
Universitas Multimedia Nusantara
Jl. Scientia Boulevard, Gading Serpong, Tangerang 15810, Indonesia
christian.widjaya@student.umn.ac.id; *Corresponding author: arya.wicaksana@umn.ac.id

Received August 2022; revised November 2022

Abstract. *Commercial face recognition engines are vulnerable to spoofing attacks: photo attacks and video attacks. Liveness detection addresses spoofing attacks by measuring the liveness (activity) of the face in real time. This study contributes to the liveness detection with randomized challenge-response authentication for existing face recognition systems. It asks the user to respond to one of the challenges, i.e., opening the mouth, eye blinking, and turning the head at random. The aim is to provide the existing facial recognition system with an anti-spoofing feature to mitigate photo and video attacks. The proposed approach yields an accuracy of 99% and an F-score of 98.99%. This study demonstrates the effectiveness of the randomized challenge-response authentication for face recognition anti-spoofing against photo and video attacks.*
Keywords: Anti-spoofing, Authentication, Biometric, Face recognition, Liveness detection, Photo attack, Randomized challenge-response, Video attack

1. **Introduction.** Commercial facial recognition systems are vulnerable to spoofing attacks [1]. About 70% of the spoofing databases could bypass the commercial off-the-shelf facial recognition (COTS) systems [2,3]. Photo and video attacks are the most commonly used types due to the high level of facial exposition, i.e., photos and videos spread on social media and CCTV footage, and the low cost of tools to perpetuate the attack [4]. Spoofing attacks pose imminent security threats to facial recognition systems and raise concerns about the study of countermeasures [1,5,6].

Several methods could address face spoofing attacks: motion analysis, contextual-based analysis, texture analysis, image quality analysis [7], and life sign [8], in addition to recent studies on deep learning methods for liveness detection and control [5,9,10]. Life sign is an indicator used in liveness detection to measure specific movements of the face [11], such as a blink of an eye [12], or request a response from the user in real time such as a smile [13]. The life sign approach can be achieved by asking the users to perform a task to verify the liveness of the face image: challenge-response [14].

The motivation of this study is to expand the work of the anti-spoofing system in [7,15]. The aim is to provide or improve the security of existing face recognition systems against face spoofing attacks: photos and videos since photo and video attacks are the most commonly used types of face spoofing attacks. Enhanced deep learning methods are proven to be successful in face recognition anti-spoofing. However, deep learning methods depend heavily on the quality and quantity of data. Existing face recognition systems such as [16-18] could not always afford the resources required for deep learning methods. Thus,

DOI: 10.24507/ijicic.19.02.419

a straightforward and lightweight approach that could be applied directly to existing face recognition systems is favorable.

This study contributes to the randomized challenge-response face anti-spoofing system. The randomization of challenges increases the difficulty for attackers to predict and prepare an attack against the challenge-response authentication. The proposed approach is implemented and tested on a prototype face recognition system with Dlib and OpenCV. Security evaluation tests the proposed system with photo and video attacks under various testing scenarios.

The rest of this paper is organized as follows. Section 2 describes the preliminaries related to the study. Section 3 describes the research methods. Section 4 explains the results and discussion. Finally, Section 5 concludes this paper with some suggestions for future work.

2. Preliminaries.

2.1. Facial features.

Facial features are found by finding a landmark representing a different point in most images under consideration, for example, the location of the pupil of the left eye. A set of landmarks creates a shape, representing the shape as a vector containing all pairs of variables x and y from all points in the shape [20]. These landmark points are also known as facial annotations [21,22]. Figure 1 illustrates the facial annotation using the iBUG 300-W dataset.

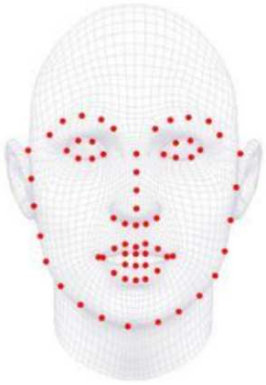


FIGURE 1. Facial annotation on the iBUG 300-W dataset [23]

2.2. Liveness detection.

Liveness detection determines whether a person's face is genuine or synthesized by measuring the liveness (activity) of the face [11]. Several methods that can be used in liveness detection are by analyzing the texture, analyzing the frequency [24], and measuring the movement of facial features (coordinates of the face) in the given image/frame [11]. Asking the user to smile is measurable by a mathematical formula using facial annotations [13]. Figure 2 shows 68 facial annotation points from the iBUG-300 dataset using the Dlib library. The Dlib yields an accuracy of 99.38% (Labeled Faces in the Wild benchmark) and could also extract face annotations required for liveness detection [19].

The coordinate of facial landmark points obtained from using Dlib, as shown in Figure 2, helps the establishment of the formulation of the eye aspect ratio (EAR) and mouth aspect ratio (MAR), introduced in [26]. Distances between the facial landmark points are required to calculate the eye and mouth shape during the challenge-response process. In addition, the angle of the camera viewpoint is also calculated to measure the angle of the face. The angle measurement of the camera viewpoint is illustrated in Figure 3.

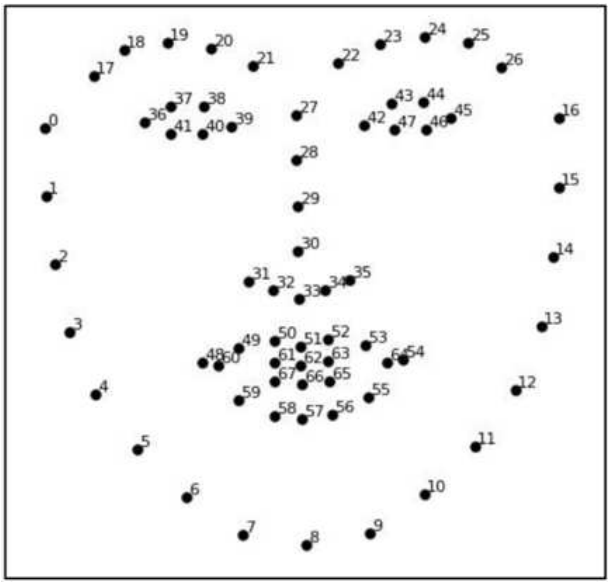


FIGURE 2. The 68 facial landmark points obtained with Dlib [25]

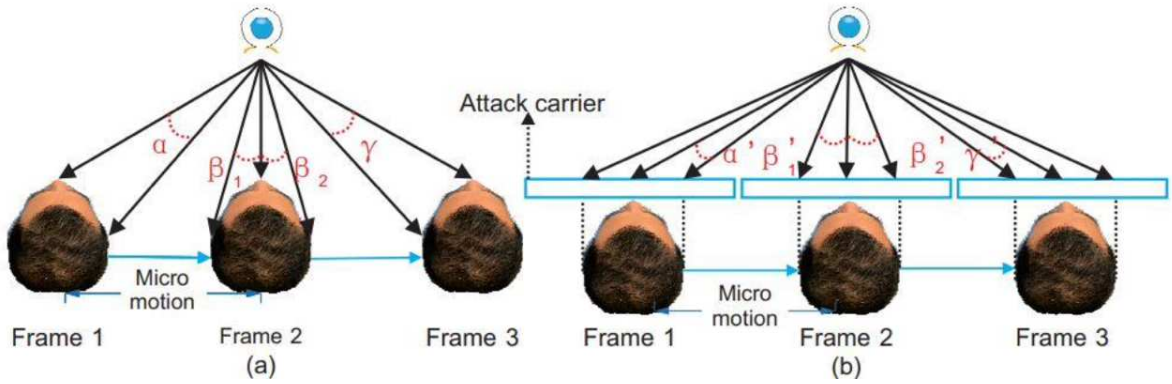


FIGURE 3. The angle of the camera viewpoint reflects the facial motion's relative depth among different key points [15].

Definition 2.1. *The EAR formula calculates eye openness by measuring the eye coordinates in a frame. The points are chosen between* p_{36} *and* p_{41} *for the right eye and* p_{42} *and* p_{47} *for the left eye from the 68 facial landmark points.*

$$EAR_{right} = \frac{(p_{40} + p_{41}) - (p_{37} + p_{38})}{2 * (p_{39} - p_{36})} \tag{1}$$

$$EAR_{left} = \frac{(p_{46} + p_{47}) - (p_{43} + p_{44})}{2 * (p_{45} - p_{42})} \tag{2}$$

Definition 2.2. *The MAR formula calculates mouth openness by measuring the mouth coordinates, in this case, all the coordinates of the centremost part of the mouth, excluding the lips.*

$$MAR = \frac{(p_{65} + p_{67}) - (p_{61} + p_{63})}{2 * (p_{64} - p_{60})} \tag{3}$$

In the living scene (a), the angle α between the nose and right ear gets smaller with the face moving right ($\alpha > \beta_2$), while the angle β_2 between the left ear and nose gets larger ($\beta_1 < \gamma$). However, in the spoofing scene (b), $\alpha' < \beta_2'$, and $\beta_1' > \gamma'$. Angle β_1 is the angle between the left ear and nose, and angle β_2 is the angle between the right ear and nose.

After a person changes their face position or turns their head, the new result of β_1 is γ, and the new result of β_2 is α. In the case of a human face, if the face moves to the left or rotates the head to the left, then α is greater than β_2 ($\alpha > \beta_2$), and vice versa if the face moves to the right or rotates the head to the right, then γ is greater than β_1 ($\gamma > \beta_1$). In the case of a printing attack, this is reversed: ($\alpha < \beta_2$) and ($\gamma < \beta_1$) [15].

2.3. **Spoofing attack.** There are two types of attacks in the biometric system: direct and indirect. In a direct attack, an impersonator can change their biometric characteristics to avoid identification (obfuscation) or claim an authorized user's identity by posing alone (zero-effort attack) or presenting the faked biometric properties of the user (spoofing or presentation attack). Spoofing attacks can be the most dangerous because they do not require expert programming skills such as indirect attacks. Unlike zero-effort attacks, spoofing attacks pose a significant threat to security, especially considering the false acceptance rate of biometric systems [27].

The common spoofing attacks in facial recognition are photo attacks, video attacks, and 3D mask attacks. Photo and video attacks are the most commonly used types because of the high level of facial exposition, such as photos and videos spread on social media and CCTV footage, and the low cost of high-resolution cameras, printers, and screens. A photo attack is carried out by displaying a photo of the person concerned to the facial recognition sensor. Photo attacks can be carried out by printing other people's faces onto paper to be displayed (printed attack) or displayed on an electronic screen. Real most recent user photos can be obtained immediately with the help of social media, and printing the photo to carry out the attack is effortless and low-cost. A video attack is an attack that records another person's face as a video and displays it on an electronic screen, which is more advanced than a photo attack. Unlike photo attacks, which only show faces and textures, video attacks also show dynamic movements (eye blinks, mouth movements, etc.), making them more difficult to detect [4].

3. Methods.

3.1. **Design.** The liveness detection challenges designed in this study are blinking, smiling, and turning the head. These challenges are given to the user at random. Users are pre-registered to the system, and users' faces are captured and stored in the face database. The system flow is shown in Figure 4.

The system checks for only one face capture at a time to proceed with the authentication process. The process continues to the liveness detection part: randomized challenge-response. One of the three predefined challenges is asked to the user to respond appropriately. The system still checks for more than one face in the video frame to avoid penetration of photo and video attacks during the challenge-response authentication step. The given user's response is processed by the "verifying user feedback" module described in Figure 5. The module uses the formulas and extended rules to decide the challenge-response authentication.

The system finally returns with authentication success upon receiving the appropriate response from the user. This proves that the user uses the face recognition system directly in person. An authentication failure message is set out when the user fails to respond correctly to the given challenge. This direct approach allows straightforward implementation on most existing face recognition systems with moderate computational resources. The liveness detection design in this study aimed to demonstrate the concept by using Dlib and OpenCV for the face recognition processing tools. Both libraries are open-source and available online.

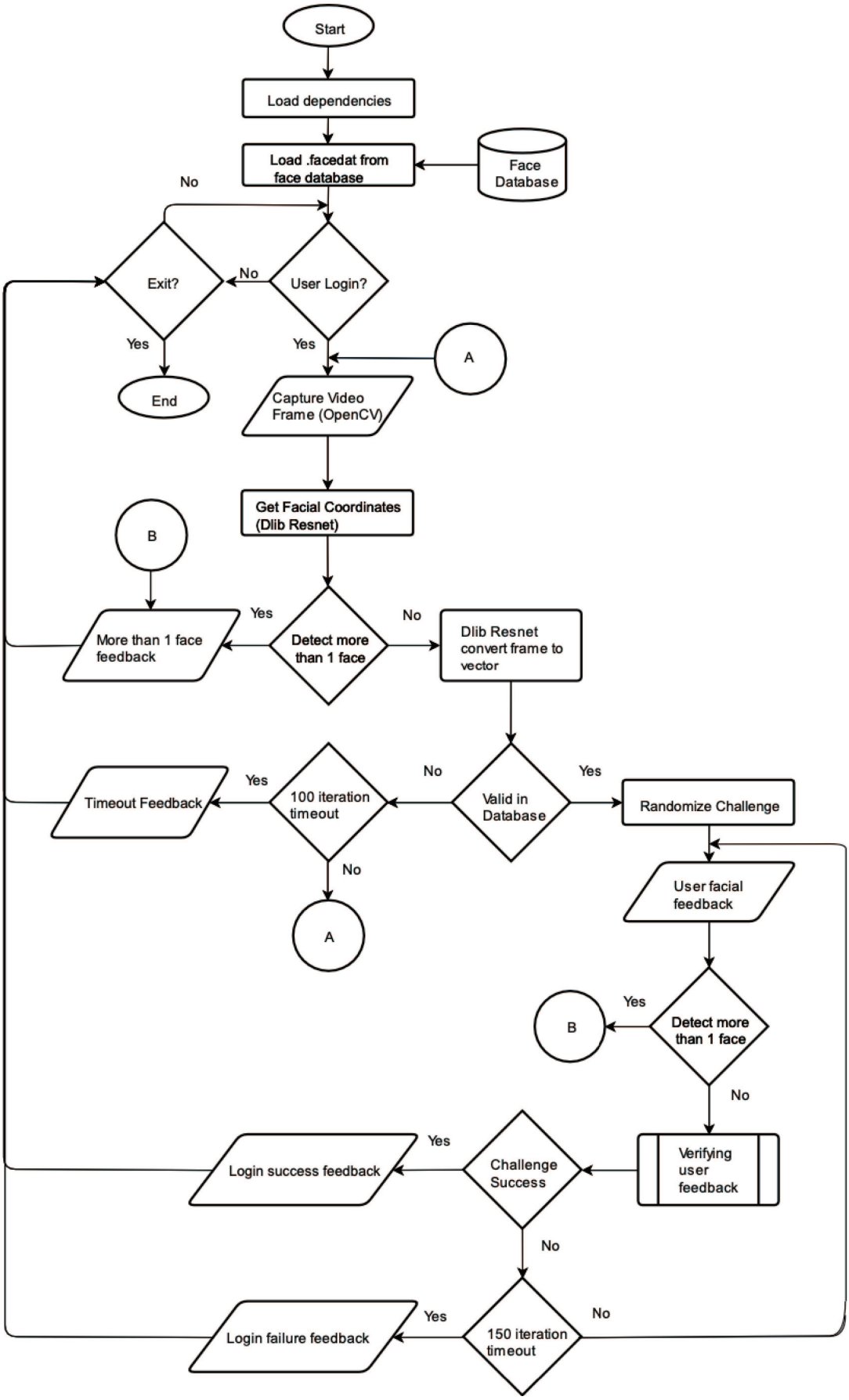


FIGURE 4. Main flowchart

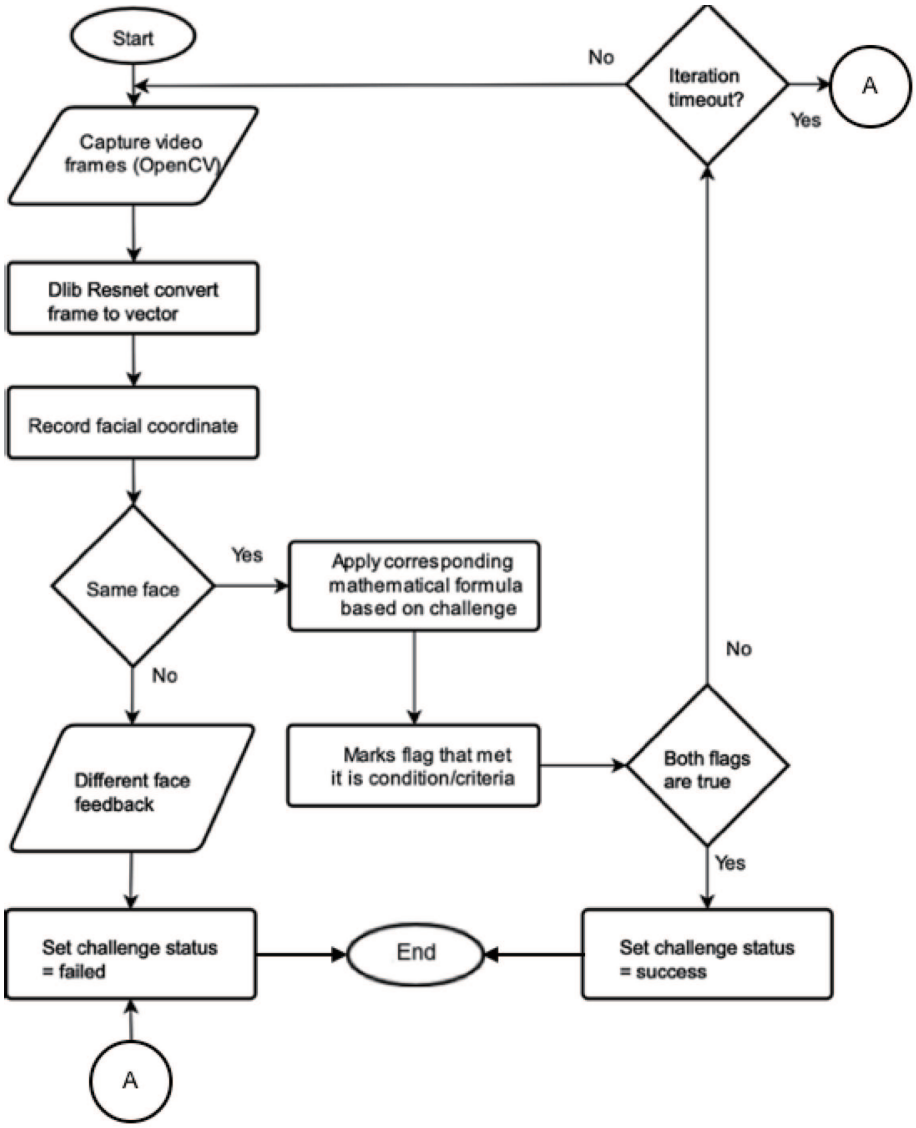


FIGURE 5. Flowchart of verifying user feedback

3.2. **Implementation.** The prototype face recognition system is built using C++ language using OpenCV as a library to capture video frames and Dlib to recognize a person's face and get facial coordinates. Dirent is a library that is used to retrieve files from folders systematically. The library is compiled using the CUDA 10.2 framework, a framework provided by NVIDIA to perform computing on the Graphical Processor Unit (GPU) manufactured by NVIDIA. The camera hardware used is Logitech C270. Data variables used by liveness detection are taken from the Dlib library function results from the received webcam frame.

The interface is designed for full computer screens with Full HD/2K (1920×1080) resolution. Even though it is designed for Full HD, the position and size of the object are proportional to the screen size, except for the feedback screen continuously measuring 640×480 with the standard OpenCV size. The login button turns on face detection against video frames from the camera. The feedback screen displays the video frame, plus a red face detection box when the login button has been pressed until it is cleared within ten milliseconds. Part "Realtime Date/Clock" displays the hour and time up to seconds.

FIGURE 6. The prototype system graphical user interface

TABLE 1. Dlib threshold configuration test

No.	Number of faces	Face recognition threshold	Challenge-response threshold	Expected outcome
1	1	60%	60%	Able to recognize the face and accept the login
2	1	50%	50%	Able to recognize the face and accept the login
3	1	40%	40%	Able to recognize the face and accept the login
4	1	40%	50%	Able to recognize the face and accept the login
5	1	40%	60%	Able to recognize the face and accept the login
6	2	40%	60%	Detect two faces and reject login

Feedback Message Box displays the system's feedback and challenges to the user. The user is expected to respond to the challenge within 10 seconds. The graphical user interface implementation is shown in Figure 6.

The face recognition process on Dlib uses a threshold, and the default from Dlib is 60%. The threshold is adjustable, and testing is conducted to find the best threshold for this study. The details are described in Table 1. On the challenge-response authentication part, the time duration is given to the user to respond to the challenge. The duration for this purpose is best set to 10 seconds from the experiments conducted.

3.3. **Testing.** There are ten users involved in the testing and evaluation of this study. The photo attack dataset is created by capturing the face photos of each user five times with different poses. The video attack dataset is created by recording each user performing various tasks at random (blinking, smiling, turning head).

3.4. **Evaluation.** The evaluation of the system is to measure the performance of the proposed approach in terms of accuracy and F-score. Four scenarios are created along with the data to measure the performance, and Table 2 describes the four scenarios used for evaluation.

Table 2. Performance evaluation scenarios

Scenario	Details	Expected outcome
A	• 10 persons • Each person does the response-challenge 5 times	Able to recognize the face and accept the login (true positive)
B	• 10 persons • Each person does not do the response-challenge 5 times	Able to recognize the face but reject the login (true negative)
C (Photo attack)	• Photo of 10 users • Each photo is applied 5 times • Photo is faced directly to the camera	Able to recognize the face but reject the login (true negative)
D (Video attack)	• Video of 10 users • Video playback against the system • 720p video resolution	Able to recognize the face but reject the login (true negative)

4. **Results and Discussion.** The Dlib configuration test results show that the parameters configured for case number five are the best among the rest. Since face recognition is not the focus of this study, the face recognition threshold is set to 40%. The challenge-response threshold is set to 60% because 40% and 50% make the system unable to recognize the face during the challenge-response authentication step. The evaluation results are presented in Table 3.

Table 3. Performance evaluation results

Scenario	Expected outcome	True positive	True negative	False positive	False negative
A	Able to recognize the face and accept the login (true positive)	48	0	0	2
B	Able to recognize the face but reject the login (true negative)	0	50	0	0
C (Photo attack)	Able to recognize the face but reject the login (true negative)	0	50	0	0
D (Video attack)	Able to recognize the face but reject the login (true negative)	0	50	0	0

The performance evaluation results show that the approach proposed in this study is direct yet effective. The liveness detection feature can withstand spoofing attacks from the four scenarios. Figures 7 and 8 display the five attempts of Christian (Scenario A)

FIGURE 7. Scenario A: Christian

FIGURE 8. Scenario B: Eli

and Eli (Scenario B). Figures 9 and 10 display the five attempts of photo attack (Scenario C) and video attack (Scenario D) for user Stephen Jonathan.

In Scenario C, a photo attack uses the same user's face photo, and the photo is printed on A4 paper and shown directly facing the camera. In Scenario D, a video attack is carried out using a video recording of the same user created using the same camera (Logitech C270). The video duration matches the challenge-response authentication window period (ten seconds). The video is played on a smartphone and shown facing the camera. The system successfully rejects the login and avoids the exploitation of both photo and video attacks for all users.

The system checks the user's face during the challenge-response authentication process. Any changes on the face during this process cause the system to reject the login. There is a probability that the attack matches the challenge coincidentally. However, the probability gets smaller by adding more challenge-response, including combining multiple challenge-response tasks for the authentication.

In Figure 10, the user's face is detected and recognized. However, the video becomes blurry on the camera when given a challenge. Hence, the system is unable to detect anything. Due to the random factor of the challenge-response authentication, the recorded user video does not match the task. Thus, the system rejects the malicious login attempt. The attack dataset and scenario are developed assuming that the attackers are outsiders. In both Scenarios C and D, the system successfully withstands all attacks.

5. **Conclusions.** This study demonstrates the effectiveness of the randomized challenge-response authentication for face recognition anti-spoofing. The approach proposed in this study is directed at existing face recognition systems to have an additional anti-spoofing

FIGURE 9. Scenario C (photo attack): Stephen

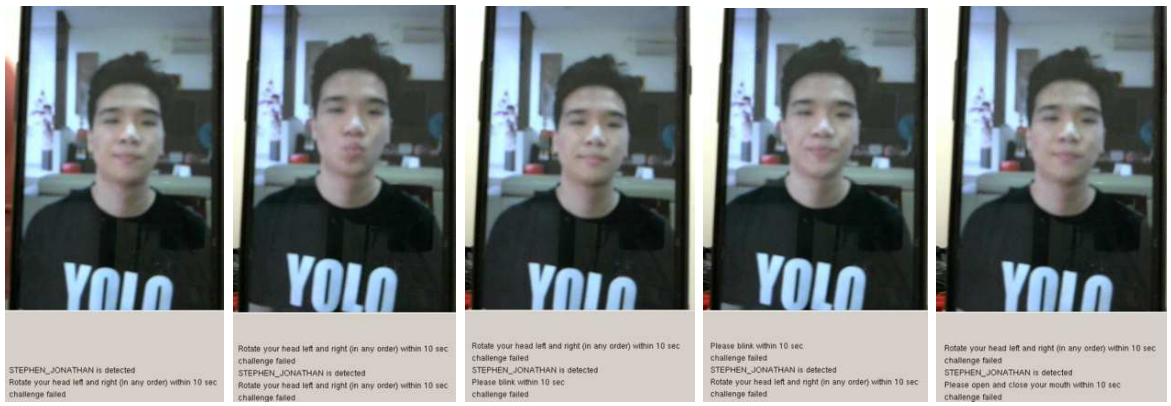


FIGURE 10. Scenario D (video attack): Stephen

security feature. Thus, this paper does not discuss issues related to the face recognition part used in this study. Based on the testing and evaluation, the approach successfully withstands photo and video attacks. The randomized challenge-response authentication thwarts all 200 malicious attempts, including 100 photo and video attacks in the testing.

The probability of getting the same challenge and attack could be diminished by adding more challenge-response and combining multiple challenge-response tasks for the authentication process. The randomization of challenges already reduces the predictability factor of the standard challenge-response authentication, increasing the difficulties for attackers to penetrate the system with insufficient resources. More challenge-response tasks would improve the system's authentication security and avoid coincidental matches.

The system's accuracy is 99%, and the F-score is 98.99%. These results are obtained from the test involving ten users with five login attempts each in 4 different scenarios. The limitation of this approach is that it requires user cooperation in responding to the given challenge(s) correctly within the specified time window. Factors such as time processing delay and face recognition threshold affect the system's liveness detection performance.

Acknowledgment. The authors would like to thank Universitas Multimedia Nusantara for the support of this research work.

REFERENCES

[1] L. Li, P. L. Correia and A. Hadid, Face recognition under spoofing attacks: Countermeasures and research directions, *IET Biometrics*, vol.7, no.1, pp.3-14, DOI: 10.1049/iet-bmt.2017.0089, 2017.

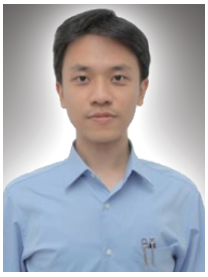
[2] D. Wen, H. Han and A. K. Jain, Face spoof detection with image distortion analysis, *IEEE Trans. Inf. Forensics Secur.*, vol.10, no.4, pp.746-761, 2015.

[3] B. Rhodes and C. Rollet, *Facial Recognition Systems Fail Simple Liveness Detection Test*, https://ipvm.com/reports/live-detect, Accessed on Oct. 03, 2022.
[4] J. Hernandez-Ortega, J. Fierrez, A. Morales and J. Galbally, Introduction to face presentation attack detection, in *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection*, S. Marcel, M. S. Nixon, J. Fierrez and N. Evans (eds.), Cham, Springer, 2019.
[5] A. Sabaghi, M. Oghbaie, K. Hashemifard and M. Akbari, Deep learning meets liveness detection: Recent advancements and challenges, *arXiv.org*, arXiv: 2112.14796, 2021.
[6] Z. Akhtar, C. Micheloni and G. L. Foresti, Biometric liveness detection: Challenges and research opportunities, *IEEE Secur. Priv.*, vol.13, no.5, pp.63-72, 2015.
[7] Z. Boulkenafet, Z. Akhtar, X. Feng and A. Hadid, Face anti-spoofing in biometric systems, in *Biometric Security and Privacy*, R. Jiang, S. Al-maadeed, A. Bouridane, D. Crookes and A. Beghdadi (eds.), Springer, 2017.
[8] T. Blcher, L. Garralda, J. Schneider, C. Zimmermann and W. Stork, A low-cost life sign detection method based on time series analysis of facial feature points, *International Conference on Bio-Inspired Systems and Signal Processing*, 2017.
[9] N. Ebrahimpour, M. A. Ayden and B. Altay, Liveness control in face recognition with deep learning methods, *Eur. J. Res. Dev.*, vol.2, no.2, pp.92-101, DOI: 10.56038/ejrnd.v2i2.36, 2022.
[10] R. Koshy and A. Mahmood, Enhanced deep learning architectures for face liveness detection for static and video sequences, *Entropy*, vol.22, no.10, DOI: 10.3390/e22101186, 2020.
[11] S. Parveen, S. Ahmad, M. Hanafi and W. Adnan, Face anti-spoofing methods, *Curr. Sci.*, vol.108, no.8, pp.1491-1500, 2015.
[12] G. Pan, L. Sun, Z. Wu and S. Lao, Eyeblink-based anti-spoofing in face recognition from a generic webcamera, *2007 IEEE 11th International Conference on Computer Vision*, Rio de Janeiro, Brazil, pp.1-8, DOI: 10.1109/ICCV.2007.4409068, 2007.
[13] O. Deniz, M. C. Santana, J. Lorenzo-Navarro, L. Anton-Canalis and G. Bueno, Smile detection for user interfaces, in *Advances in Visual Computing. ISVC 2008. Lecture Notes in Computer Science*, Berlin, Heidelberg, Springer, 2008.
[14] S. Chakraborty and D. Das, An overview of face liveness detection, *Int. J. Inf. Theory*, vol.3, no.2, pp.11-25, 2014.
[15] Z. Wang et al., Exploiting temporal and depth information for multi-frame face anti-spoofing, *arXiv.org*, arXiv: 1811.05118, 2018.
[16] Indrabayu, I. S. Areni, A. Bustamin and V. Aza, Real-time face recognition system as personal assistant for people with blindness, *ICIC Express Letters, Part B: Applications*, vol.13, no.2, pp.203-210, DOI: 10.24507/icicelb.13.02.203, 2022.
[17] A. Archilles and A. Wicaksana, Vision: A web service for face recognition using convolutional network, *Telkomnika (Telecommunication Comput. Electron. Control.)*, DOI: 10.12928/TELKOMNIKA.v18i3.14790, 2020.
[18] V. Kurniawan, A. Wicaksana and M. I. Prasetiyowati, The implementation of eigenface algorithm for face recognition in attendance system, *2017 4th International Conference on New Media Studies (CONMEDIA)*, Yogyakarta, Indonesia, pp.118-124, DOI: 10.1109/CONMEDIA.2017.8266042, 2017.
[19] D. King, *High Quality Face Recognition with Deep Metric Learning*, http://blog.dlib.net/2017/02/high-quality-face-recognition-with-deep.html, Accessed on Aug. 05, 2022.
[20] S. Milborrow and F. Nicolls, Locating facial features with an extended active shape model, *Proc. of the 10th European Conference on Computer Vision: Part IV*, pp.504-513, 2008.
[21] C. Sagonas, G. Tzimiropoulos, S. Zafeiriou and M. Pantic, A semi-automatic methodology for facial landmark annotation, *2013 IEEE Conference on Computer Vision and Pattern Recognition Workshops*, Portland, OR, USA, pp.896-903, DOI: 10.1109/CVPRW.2013.132, 2013.
[22] C. Sagonas, G. Tzimiropoulos, S. Zafeiriou and M. Pantic, 300 faces in-the-wild challenge: The first facial landmark localization challenge, *IEEE International Conference on Computer Vision Workshops*, Sydney, NSW, Australia, pp.397-403, DOI: 10.1109/ICCVW.2013.5, 2013.
[23] C. Sagonas, E. Antonakos, G. Tzimiropoulos, S. Zafeiriou and M. Pantic, 300 faces in-the-wild challenge: Database and results, *Image Vis. Comput.*, vol.47, pp.3-18, 2016.
[24] G. Kim, S. Eum, J. Suhr, D. Kim, K. Park and J. Kim, Face liveness detection based on texture and frequency analyses, *2012 5th IAPR International Conference on Biometrics (ICB)*, New Delhi, India, pp.67-72, DOI: 10.1109/ICB.2012.6199760, 2012.
[25] P. Korshunov and S. Marcel, Speaker inconsistency detection in tampered video, *2018 26th European Signal Processing Conference (EUSIPCO)*, Rome, Italy, pp.2375-2379, DOI: 10.23919/EUSIPCO.2018.8553270, 2018.

[26] P. Awasekar, M. Ravi, S. Doke and Z. Shaikh, Driver fatigue detection and alert system using non-intrusive eye and yawn detection, *Int. J. Comput. Appl.*, vol.180, no.44, 2018.
[27] N. Erdoemut and M. Sébastien, Introduction, in *Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks*, M. Sébastien, M. S. Nixon, J. Fierrez and N. Evans (eds.), Springer, 2014.

Author Biography

Christian Widjaya received a B.Sc. degree in Informatics from Universitas Multimedia Nusantara, Indonesia, in 2021. His research interest is computer security and game design, and he is currently working as a game developer.



Arya Wicaksana is a lecturer at the Department of Informatics at UMN. He received a Master's Degree in VLSI Engineering from Universiti Tunku Abdul Rahman (UTAR). He successfully demonstrated the UTAR first-time success ASIC design methodology on a multi-processor system-on-chip project using 0.18 μm processing technology in 2015. His main research interests are blockchain applications and computational intelligence. He recently worked on blockchain-based decentralized autonomous social media. He has served as an invited reviewer in IEEE ACCESS, IJNMT, and IFERP and an invited author in IntechOpen and other scientific publications.