International Journal of Innovation and Applied Studies
ISSN 2028-9324 Vol. 41 No. 2 Dec. 2023, pp. 588-597

http://www.ijias.issr-journals.org/

Face Liveness Detection and Tracking in a Remote Exam Monitoring System

Konan YAO[1], Tiemoman KONE[1], Behou Gérard N'GUESSAN[1], and Koffi Fernand KOUAME[2]

[1]Department of Analysis, Decision and Information, Computer Science and Digital Science, Université virtuelle de côte d'Ivoire, Abidjan, Côte d'Ivoire

[2]Department of Remote Sensing and Geospatial Intelligence, Computer Science and Digital Science, Université Virtuelle de Côte d'Ivoire, Abidjan, Côte d'Ivoire

ABSTRACT: In the growing context of online exam surveillance to ensure academic integrity, biometric authentication through facial recognition has become a common practice. However, the efficacy of this method is being questioned due to the potential vulnerability associated with the use of printed images to bypass the monitoring system. This vulnerability raises significant concerns regarding the security and authenticity of online assessments, thereby necessitating a deeper exploration of more reliable and secure facial liveness detection methods. In this study, we proposed a real-time approach for detecting facial liveliness within an anti-fraud device during online exams, leveraging facial recognition technology. Our focus was on employing a convolutional neural network algorithm to extract distinctive facial features. Convolutional neural networks, known for their adeptness in pattern detection and recognition, were at the core of our investigation. We delved into analyzing facial liveliness through two distinct approaches. Firstly, we meticulously examined facial texture, studying a dataset comprising both genuine faces and reproductions on various media such as fabric or masks. Concurrently, we implemented a method centered on detecting eye blinking. Regarding the implementation with the neural network algorithm, the results unveiled a precision rate of 57% for skin texture analysis, highlighting the inherent challenges of this method. Conversely, the eye blinking approach exhibited significantly better performance, with a precision of 96%, emphasizing its strong potential in detecting facial liveliness.

KEYWORDS: Academic integrity, Online exam, monitoring system, face recognition, face liveness.

1 INTRODUCTION

In the current context of remote work and online learning, educational institutions are facing a significant challenge: preventing academic malpractices such as plagiarism and cheating during examinations. This new requirement has led to the adoption of remote monitoring technology. Indeed, the use of remote monitoring is a key technology that monitors educational activities, such as online exams, for students in various geographical locations [1]. There are different types of remote monitoring, including live monitoring systems, recorded monitoring, and real-time AI-based remote exam monitoring systems [2]. AI-based systems use machine learning and/or deep learning algorithms to automatically detect cheating in real time [3], [4}. These systems ensure that the person taking the exam is the authorized candidate. Facial recognition plays a crucial role in this system [5], [6]. Facial recognition-based systems (FRS) use hardware such as the student's laptop webcam or smartphone's front camera to continuously capture the candidate's image throughout the exam. This ensures the authenticity of the candidate and maintains the integrity of the exam. However, the adoption of facial recognition as a method for verifying the identity of candidates is not without risks. Potential loopholes, such as the use of printed images [7], [8], [9], replayed videos [8], [10], [11], or face masks [12] pose a serious challenge to the integrity of remote monitoring systems. Indeed, attempting to deceive an FRS with a printed photograph involves presenting the system with a legitimate candidate's photo, collected from websites or provided by an accomplice candidate. Mediums may include paper, fabric, or images projected from a screen, such as a smartphone. In the case of videos, the legitimate candidate's face is recorded within seconds,

and the recording is used to fraudulently access the system. This method of impersonation is often challenging to detect due to its dynamic nature and texture. Concerning masks, two practices are notable. Masks made from high-quality photo cutout materials are used to replicate facial expressions, such as blinking during the exam. In the other case, a 3D mask of the legitimate candidate's face is created and used to commit fraud. This practice is known as "face spoofing," which involves deceiving facial recognition systems to gain unauthorized access.

In this article, we propose an innovative approach to detect facial liveliness by leveraging Convolutional Neural Networks (CNNs). These state-of-the-art machine learning models have significantly influenced the processing of spatial and structured data, particularly in the fields of computer vision and pattern recognition. Their use in Presentation Attack Detection (PAD) [13] in cybersecurity demonstrates their effectiveness in binary classification of fraudulent and genuine presentations.

To address this challenge, we implemented a methodology based on the use of Convolutional Neural Networks (CNNs). Firstly, we collected and analyzed a diverse dataset including genuine faces and reproductions to train the neural network. Subsequently, we trained the CNN to detect distinctive signs of facial liveliness such as eye blinking, using advanced deep learning techniques.

This paper is organized into several sections which first present a synthesis of previous studies on face appearance detection. Then we proposed an approach for detecting the liveness of faces and the results obtained. Finally, we provide conclude with final remarks.

2 MATERIALS AND METHODS

2.1 ANTI-FACE SPOOFING METHOD FOR FACIAL RECOGNITION-BASED REMOTE EXAM MONITORING

Proctoring is the process of supervising a remote examination using identification and identity authentication software. According to Alotaibi et Mahmood [14], biometric authentication is one of the most widely used methods, to the detriment of traditional name and password methods. In fact, biometric authentication is a method of identifying a person using their physiological characteristics. Features that are often used are fingerprint [15] iris [16] hand face [17], [18] etc. The most widely used approach in remote examination surveillance systems is facial feature detection [19]). Indeed, the identification process of most of these systems is carried out by taking the image of the remote user attempting the examination, and the characteristics of the image are compared with the characteristics stored in the system, which are generally data supplied at the time of registration. This process is repeated throughout the examination.

2.1.1 FACE RECOGNITION

The verification and authentication methods in online examination surveillance systems based on facial recognition have been the subject of several research studies. The authors of [20] have proposed a remote examination monitoring system that emphasizes the use of facial recognition. In their work, the student's identity is determined by employing facial recognition with the HOG (histogram of conjugate gradients) detector and OpenCV's facial recognition algorithm, the student taking the exam is identified using his or her photo. Narlagiri et al. [18] propose an automated student attendance management system that incorporates facial recognition based on the Principal Component Analysis (PCA) algorithm and the Eigenfaces strategy. This method compares test images with training images and determines the presence or absence of students. Another study by Istratova et Pustovskih [21], introduces a biometric data validation model to provide fast, efficient verification and identification of users, as well as real-time control of their access. In [19}, the authors focus their study on the facial recognition-based approach to online exam monitoring for fraud detection. They show that facial recognition methods using images are the most popular, however, gesture and posture detection optimize the system's ability to detect fraud, particularly face spoofing.

2.1.2 FACE LIVENESS

Face liveness detection in online exam monitoring systems is a technique used to check whether the presented face is a real face or a pre-recorded photo or video of the candidate which may be used to deceive the system. This method improves the system's ability to detect the genuine candidate and prevent fraud such as face spoofing. Various methods are utilized in face liveness detection systems to ascertain the presence of a real person. In Alotaibi et Mahmood [14], the authors provide an overview of techniques for detecting face liveliness in systems. They classify these techniques into two groups, namely static and dynamic methods. Static methods are generally based on texture analysis to extract discriminating features. But their performance deteriorates under varying lighting conditions. On the other hand, dynamic methods offer better performance

than static methods. However, they may be slower and more challenging to implement. The authors recommend employing deep learning [22] for liveness detection in facial recognition-based systems. Khairnar et al. [21] conduct a literature review on artificial intelligence methods employed for face liveness detection and outline future directions. As the authors Akbulut et al. [23], they show that the reliability of a facial recognition system depends on its ability to detect both facial identity and liveness. they propose a spoof detection method based on deep learning. Two different deep learning models are used for this purpose: LRF-ELM (Local Receptive Fields - Extreme Learning Machine) and CNN (Convolutional Neural Network). Shekhar et al. [24] adopt a similar approach, presenting a technique for detecting facial liveliness using an ensemble Deep Learning approach. In [25], the authors introduce an innovative system called FaceLivePlus. This system reduces computational workload and storage space while delivering significant improvements in error rates over existing approaches. The authors Rufai et al. [26] offer an in-depth review of deep learning-based methods, aiming to combat face spoofing and highlight the latest trends in deep learning approaches. They emphasize the challenge of achieving high accuracy for face presence detection algorithms and point out that deep convolutional neural networks (CNNs) deployed for face spoof detection exhibit comparatively improved accuracy. According to Ebrahimpour et al. [27], deep learning techniques promise to significantly increase facial liveness detection systems' accuracy and resolve the challenges associated with their practical implementation.

2.2 PROPOSED FACE LIVE DETECTION METHOD

The proposed method consists of a face texture analysis model and an eye-blink detection model. The method works in real-time. The operating process is as follows (figure 1):

- Face detection process
- Face liveness verification process
- Face recognition process if the response to the liveness check is affirmative.

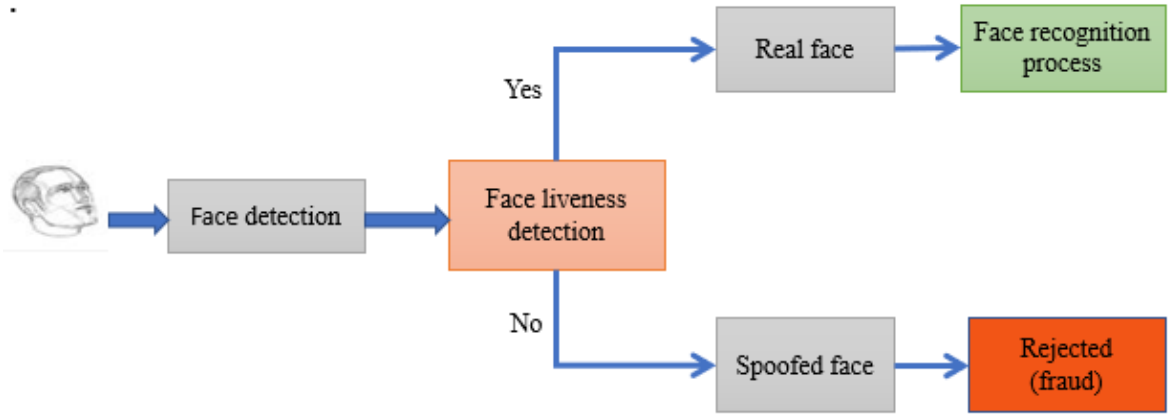

Fig. 1. Process of face verification in remote exam

2.2.1 FACE LIVELINESS DETECTION USING FACE TEXTURE ANALYSIS

The face texture analysis method employs a convolutional neural network model to distinguish between authentic and forged images. The Facial Texture Analysis technique aims to differentiate genuine from faked images by examining the unique patterns, features, and structures present on the surface of a person's face [28]. This texture analysis method is proving to be one of the facial spoofing detection approaches that is producing particularly promising results, outperforming even some of the most advanced methods [29]. In the model, facial textural features are extracted from the captured image followed by the selection of discriminative features. Using the selected textural features, a detection model based on convolutional neural networks is constructed. The model consists of four convolutional layers, four pooling layers, and fully-connected layers (Table 1). The activation function used is the Rectified Linear Unit (ReLU) function (1), while the Sigmoid function (2) serves as the output function.

$$f(x) = \max(0,x) \quad (1)$$

$$f(x) = \frac{1}{1+e^{-x}} \quad (2)$$

Table 1. The Convolution Neural Network structure

Layer(type)	Kernel-size	Output Shape
Conv2D	5x5	(None, 124,124,24)
MaxPooling2D	2x2	(None, 62, 62, 24)
Conv2D	5x5	(None, 58, 58, 24)
MaxPooling2D	2x2	(None, 29, 29, 24)
Conv2D	5x5	(None, 25, 25, 24)
MaxPooling2D	2x2	(None, 12, 12, 24)
Conv2D	5x5	(None, 8, 8, 48)
MaxPooling2D	2x2	(None, 4, 4, 48)
Flatten	---	(None, 768)
Dense	---	(None, 48)
Dropout	0.5	(None, 48)
Dense	---	(None, 48)
Dense (Sigmoid)	---	(None, 1)

Dataset: The dataset consists of 1081 real images and 960 fake images collected from the web. The "fake_face" class is labeled with the value one (1), while the "real_face" class is labeled with the value zero (0). All images have been resized to 128x128 pixels to ensure consistent dimensions throughout the dataset.

2.2.2 FACE LIVENESS DETECTION USING BLINKING EYE ANALYSIS

The use of blink analysis is presented as a technique for detecting facial impersonation. The goal is to identify the state of eye opening and closing at any given moment. Eye tracking or blink analysis is proving fundamental in the study of human-machine interactions [30] (Ezzat et al., 2023). It is also used for facial verification and authentication in surveillance systems based on facial recognition [31] (Potdar et al., 2022). These systems mainly aim to assess facial liveness to determine the presence or absence of facial spoofing [31] (Potdar, 2022, Akhdan, 2023). The detection model employed is a convolutional neural network composed of three convolution layers, three pooling layers, and fully-connected layers (table 2). The activation function utilized in this model is the ReLU function.

Table 2. The Convolution Neural Network structure

Layer (type)	Kernel-size	Output Shape
Conv2D	3x3	(None, 22, 22, 24)
MaxPooling2D	2x2	(None, 11, 11, 24)
Conv2D	3x3	(None, 9, 9, 24)
MaxPooling2D	2x2	(None, 4, 4, 24)
Conv2D	3x3	(None, 2, 2, 48)
MaxPooling2D	2x2	(None, 1, 1, 48)
Flatten	---	(None, 48)
Dense	---	(None, 48)
Dropout	0.5	(None, 48)
Dense (Sigmoid)	---	(None, 1)

Dataset: The dataset used contains 2423 subjects, of which 1192 subjects with both eyes closed are collected directly from the Internet, and 1231 subjects with eyes open selected from the Labelled Face in the Wild (LFW) database. The image format is 24x24 pixels. The class “open eye” is assigned the value one (1), while the value zero (0) is assigned the class “closed eye”.

2.2.3 EVALUATION METRICS

There are some key terms for evaluating the model including True Positive (TP), TN (True Negative), FP (False Positive), FN (False Negative), accuracy, precision, and recall. Accuracy (3): represents the proportion of correctly predicted instances relative to the total number of instances.

$$\text{accuracy}=\frac{\text{TF}+\text{TN}}{\text{TF}+\text{TN}+\text{FP}+\text{FN}} \quad (3)$$

True Positive (TP): the number of positive samples that are accurately labeled.

True Negative (TN): the number of negative samples that are accurately labeled.

False Positive (FP): the number of negative samples that are mislabelled as positive.

False Negative (FN): the number of positive samples that are mislabelled as negative.

Precision (4): represents the proportion of instances predicted as positive that is actually positive.

$$\text{precision}=\frac{\text{TP}}{\text{TP}+\text{FP}} \quad (4)$$

Recall (5): represents the proportion of positive instances actually detected by the model.

$$\text{recall}=\frac{\text{TP}}{\text{TP}+\text{FN}} \quad (5)$$

F1. score (6): is a combined measure of precision and recall, calculated as the harmonic mean of the two. It provides an overall measure of model performance.

$$\text{f1.score}=2*\frac{(\text{precision}*\text{recall})}{(\text{precision}+\text{recall})} \quad (6)$$

3 RESULTS

In this section, we present the main results of our work. The figures (figure 2. And Figure 4.) show the accuracy variation as a periodic function. The two other figures (figure 3. And Figure 5.) show the accuracy and model loss variations. The model’s accuracy refers to its ability to correctly identify whether a given image is a live face or a fake face. In this context, evolution refers to how the accuracy changes over time as the model is trained on more data. The figure shows a graph with time on the x-axis and accuracy on the y-axis. The graph may show how the accuracy improves as the model is trained on more data, or it may show how the accuracy plateaus after a certain number of training iterations.

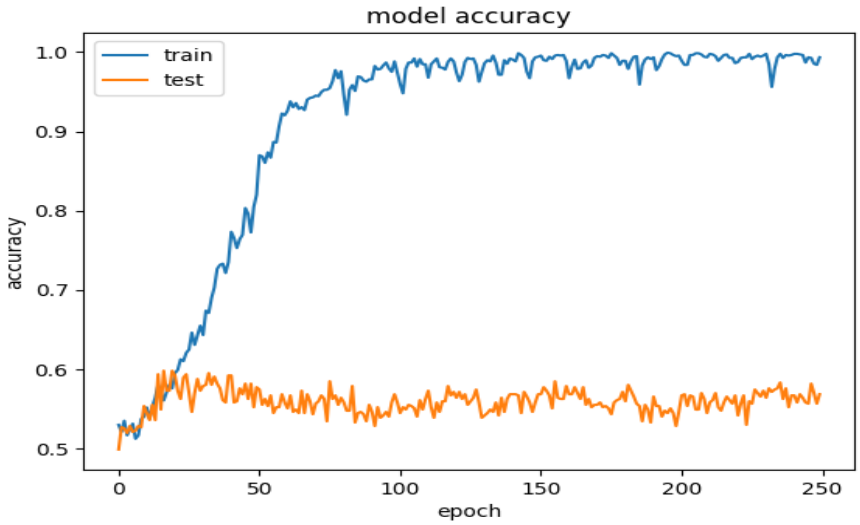

Fig. 2. Variation in the model's accuracy for face texture Analysis

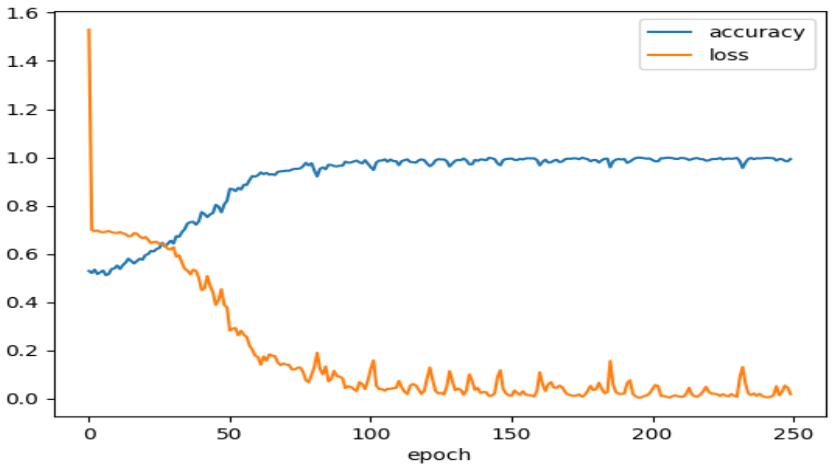

Fig. 3. Variations in accuracy and model loss for face texture analysis

The evaluation used includes accuracy, precision, recall, and f1-score. But we focused on precision and accuracy, which summarize the model's overall performance. In the case of the test data report (Table 3.) for the face texture analysis, the precision for class 0, which represents the "real_face" class, is 0.58, meaning that 58% of samples predicted as class 0 are actually class 0. For class 1 representing "fake_face", the precision is 0.55. This means that 55% of samples predicted as class 1 are actually class 1. The accuracy (overall precision) is 0.57, meaning that the model correctly classified 57% of all samples. The measurements provided allow us to evaluate the performance of the texture-based classification model on the dataset. They take into account both precision and recall for each class, as well as the overall accuracy of the model. The results indicate a fair performance of the model, which leads us to consider the use of a second method to optimize the system as a whole. It should be noted that the real and faked images were selected to present an increased resemblance, which could explain this result.

Table 3. Test data report for face texture analysis

	Precision	recall	f1-score	support
0	0.58	0.66	0.62	356
1	0.55	0.46	0.50	318
Accuracy			0.57	674
Macro avg	0.57	0.56	0.56	674
Weighted avg	0.57	0.57	0.56	674

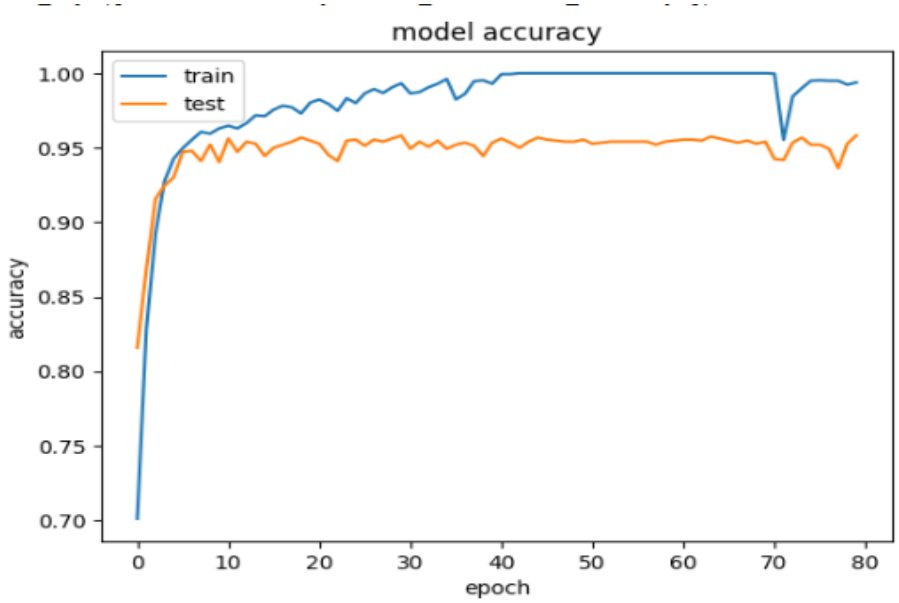

Fig. 4. Variation in the model's accuracy for blinking eye analysis

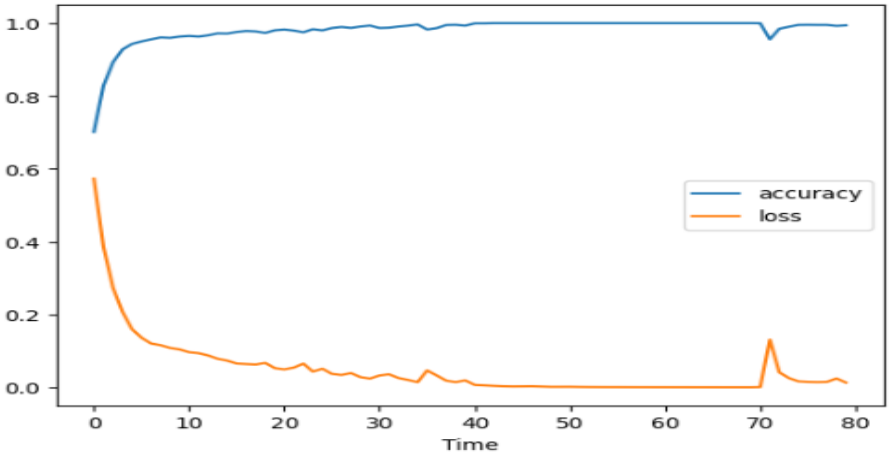

Fig. 5. Variations in accuracy and model loss for blinking eye analysis

The evaluation metrics include accuracy, precision, recall, and f1-score. However, our main focus was on precision and accuracy, as they provide an overview of the model's overall performance. In the case of the train data report (Table 4), the accuracy for class 0, i.e., the "closed eye" class, is 1.00. This indicates that 100% of samples predicted as class 0 are indeed class 0. For class 1 which represents "open eye", the precision is 1.00. This means that 100% of samples predicted as class 1 are actually class 1. The accuracy (overall precision) is 1.00, indicating that the model correctly classified 100% of all samples.

Table 4. Train data report for blinking eye analysis

	Precision	recall	f1-score	support
0	1.00	1.00	1.00	1682
1	1.00	1.00	1.00	1724
Accuracy			1.00	3406
Macro avg	1.00	1.00	1.00	3406
Weighted avg	1.00	1.00	1.00	3406

The evaluation metrics employed include accuracy, precision, recall, and f1-score. However, our main focus was on precision and accuracy, which provide a comprehensive summary of the model's overall performance. In the test data report (Table 5.), the accuracy for class 0, representing the "closed eye" class, is 0.95, meaning that 95% of samples predicted as class 0 are actually class 0. For class 1 denoting "open eye", the precision is 0.97. This indicates that 97% of samples predicted as class 1 are actually class 1. The accuracy (overall precision) is 0.96, signifying that the model correctly classified 96% of all samples.

Table 5. Train data report for blinking eye analysis

	Precision	recall	f1-score	support
0	0.95	0.96	0.96	712
1	0.97	0.95	0.96	748
Accuracy			0.96	1460
Macro avg	0.96	0.96	0.96	1460
Weighted avg	0.96	0.96	0.96	1460

4 CONCLUSION

This study focuses on facial liveness detection within the context of an online review monitoring system that utilizes facial recognition. We presented two different approaches to this detection: facial texture analysis and eye blinking detection. While the texture-based method showed an overall accuracy of 57%, we observed much more promising results with the eye-blinking-based method which achieved an accuracy of 96%. These results highlight the significance of considering facial liveness when implementing online review monitoring systems. Identifying fraudulent users and preventing facial impersonation fraud are essential elements in guaranteeing the integrity and validity of exams. Our future work aims to explore other techniques for detecting facial liveliness, including improving the performance of face matching detection.

REFERENCES

[1] S. Sapre, K. Shinde, K. Shetta, et V. Badgujar, « AI-ML based smart online examination framework », in Progresses in Artificial Intelligence & Robotics: Algorithms & Applications: Proceedings of 3rd International Conference on Deep Learning, Artificial Intelligence and Robotics, (ICDLAIR) 2021, Springer, 2022, p. 17-25.

[2] A. Nigam, R. Pasricha, T. Singh, et P. Churi, « A systematic review on ai-based proctoring systems: Past, present and future », *Education and Information Technologies,* vol. 26, nº 5, p. 6421-6445, 2021.

[3] M. M. Masud, K. Hayawi, S. S. Mathew, T. Michael, et M. El Barachi, « Smart online exam proctoring assist for cheating detection », in *Advanced Data Mining and Applications: 17th International Conference, ADMA 2021, Sydney, NSW, Australia, February 2–4, 2022, Proceedings, Part I,* Springer, 2022, p. 118-132.

[4] J. S. Ashwinkumar, H. S. Kumaran, U. Sivakarthikeyan, K. P. Rajesh, et R. Lavanya, « Deep learning based approach for facilitating online proctoring using transfer learning », in *2021 5th International Conference on Computer, Communication and Signal Processing (ICCCSP),* IEEE, 2021, p. 306-312.

[5] A. Nurpeisova *et al.,* « The Study of Mathematical Models and Algorithms for Face Recognition in Images Using Python in Proctoring System », *Computation,* vol. 10, nº 8, p. 136, 2022.

[6] W. Zhao, R. Chellappa, P. J. Phillips, et A. Rosenfeld, « Face recognition: A literature survey », *ACM Comput. Surv.,* vol. 35, nº 4, p. 399-458, déc. 2003, doi: 10.1145/954339.954342.

[7] S. V. N. V. S. Sudeep, S. Venkata Kiran, D. Nandan, et S. Kumar, « An Overview of Biometrics and Face Spoofing Detection », in *ICCCE 2020,* vol. 698, A. Kumar et S. Mozar, Éd., in Lecture Notes in Electrical Engineering, vol. 698., Singapore: Springer Nature Singapore, 2021, p. 871-881. doi: 10.1007/978-981-15-7961-5_82.

[8] M. Fang, M. Huber, et N. Damer, « Synthaspoof: Developing face presentation attack detection based on privacy-friendly synthetic data », in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition,* 2023, p. 1061-1070. Consulté le: 13 octobre 2023. [En ligne]. Disponible sur: https://openaccess.thecvf.com/content/CVPR2023W/Biometrics/html/Fang_SynthASpoof_Developing_Face_Presentation_Attack_Detection_Based_on_Privacy-Friendly_Synthetic_CVPRW_2023_paper.html.

[9] J. Hernandez-Ortega, J. Fierrez, A. Morales, et J. Galbally, « Introduction to Presentation Attack Detection in Face Biometrics and Recent Advances », in *Handbook of Biometric Anti-Spoofing,* S. Marcel, J. Fierrez, et N. Evans, Éd., in Advances in Computer Vision and Pattern Recognition., Singapore: Springer Nature Singapore, 2023, p. 203-230. doi: 10.1007/978-981-19-5288-3_9.

[10] H.-H. Chang et C.-H. Yeh, « Face anti-spoofing detection based on multi-scale image quality assessment », *Image and Vision Computing,* vol. 121, p. 104428, 2022.

[11] L. Birla et P. Gupta, « PATRON: Exploring respiratory signal derived from non-contact face videos for face anti-spoofing », *Expert Systems with Applications,* vol. 187, p. 115883, 2022.

[12] X. Ma, J. Zhang, Y. Zhang, et D. Zhou, « Exploring Masked Image Modeling for Face Anti-spoofing », in *Pattern Recognition and Computer Vision,* vol. 13534, S. Yu, Z. Zhang, P. C. Yuen, J. Han, T. Tan, Y. Guo, J. Lai, et J. Zhang, Éd., in Lecture Notes in Computer Science, vol. 13534., Cham: Springer International Publishing, 2022, p. 814-826. doi: 10.1007/978-3-031-18907-4_62.

[13] L. Li, Z. Xia, J. Wu, L. Yang, et H. Han, « Face presentation attack detection based on optical flow and texture analysis », Journal of King Saud University-Computer and Information Sciences, vol. 34, nº 4, p. 1455-1467, 2022.

[14] A. Alotaibi et A. Mahmood, « Face Liveness Detection–A Comprehensive Survey Based on Dynamic and Static Techniques », *International Journal of Computer Science and Information Security (IJCSIS),* vol. 13, nº 10, 2015.

[15] S. Hemalatha, « A systematic review on Fingerprint based Biometric Authentication System », in *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE),* IEEE, 2020, p. 1-4.

[16] S. H. Shaker, F. Q. Al-Kalidi, et R. Ogla, « Identification Based on Iris Detection Technique », *International Journal of Interactive Mobile Technologies,* vol. 16, nº 24, 2022.

[17] M. M. Taher et L. E. George, « A digital signature system based on hand geometry-Survey », *Wasit Journal of Computer and Mathematic Science,* vol. 1, nº 1, p. 1-14, 2022.

[18] S. Narlagiri, V. Malathy, et A. Chakradhar, « Biometric authentication system based on face recognition », in *AIP Conference Proceedings,* AIP Publishing LLC, 2022, p. 030010.

[19] S. G. Rabiha, I. H. Kartowisastro, R. Setiawan, et W. Budiharto, « Survey of Online Exam Proctoring Model to Detect Cheating Behavior based on Face Recognition », in *2022 8th International Conference on Systems and Informatics (ICSAI),* IEEE, 2022, p. 1-7. 12] I. Ahmad, F. AlQurashi, E. Abozinadah, et R. Mehmood, « A novel deep learning-based online proctoring system using face recognition, eye blinking, and object detection techniques», *International Journal of Advanced Computer Science and Applications,* vol. 12, nº 10, 2021.

[20] E. E. Istratova et D. A. Pustovskih, « Development and research of the biometric face recognition system based on the application of the deep learning method », *International Journal of Open Information Technologies,* vol. 10, nº 12, p. 66-74, 2022.

[21] S. Khairnar, S. Gite, K. Kotecha, et S. D. Thepade, « Face Liveness Detection Using Artificial Intelligence Techniques: A Systematic Literature Review and Future Directions », *Big Data and Cognitive Computing,* vol. 7, nº 1, p. 37, 2023.

[22] R. Koshy et A. Mahmood, « Enhanced Deep Learning Architectures for Face Liveness Detection for Static and Video Sequences », *Entropy,* vol. 22, nº 10, oct. 2020, doi: 10.3390/e22101186.

[23] Y. Akbulut, A. Şengür, Ü. Budak, et S. Ekici, « Deep learning based face liveness detection in videos », in *2017 international artificial intelligence and data processing symposium (IDAP),* Ieee, 2017, p. 1-4.

[24] S. Shekhar, A. Patel, M. Haloi, et A. Salim, « An Ensemble Model for Face Liveness Detection », arXiv.org. Consulté le: 8 août 2023. [En ligne]. Disponible sur: https://arxiv.org/abs/2201.08901v1.

[25] Y. Zhang, L. Zheng, V. L. Thing, R. Zimmermann, B. Guo, et Z. Yu, « FaceLivePlus: A Unified System for Face Liveness Detection and Face Verification », in *Proceedings of the 2023 ACM International Conference on Multimedia Retrieval,* 2023, p. 144-152.

[26] S. Z. Rufai, A. Selwal, et D. Sharma, « On analysis of face liveness detection mechanisms via deep learning models », in *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS),* IEEE, 2022, p. 59-64.

[27] N. Ebrahimpour, M. A. Ayden, et B. Altay, « Liveness control in face recognition with deep learning methods », *The European Journal of Research and Development,* vol. 2, nº 2, p. 92-101, 2022.

[28] Z. Boulkenafet, J. Komulainen, et A. Hadid, « Face spoofing detection using colour texture analysis », *IEEE Transactions on Information Forensics and Security,* vol. 11, n° 8, p. 1818-1830, 2016.

[29] L. Li, Z. Xia, J. Wu, L. Yang, et H. Han, « Face presentation attack detection based on optical flow and texture analysis », *Journal of King Saud University-Computer and Information Sciences,* vol. 34, n° 4, p. 1455-1467, 2022.

[30] M. Ezzat, M. Maged, Y. Gamal, M. Adel, M. Alrahmawy, et S. El-Metwally, « Blink-To-Live eye-based communication system for users with speech impairments », *Scientific Reports,* vol. 13, n° 1, p. 7961, 2023.

[31] A. Potdar, P. Barbhaya, et S. Nagpure, « Face Recognition for Attendance System using CNN based Liveliness Detection », in *2022 International Conference on Advances in Computing, Communication and Materials (ICACCM),* IEEE, 2022, p. 1-6.