ZIBELINE INTERNATIONAL™ PUBLISHING

ISSN: 2773-6202 (Online)
CODEN: JTIOCC

Journal of Technology & Innovation (JTIN)

DOI: http://doi.org/10.26480/jtin.02.2024.63.65

REVIEW ARTICLE

ADVANCEMENTS IN AI-POWERED FACIAL RECOGNITION FOR SECURE USER AUTHENTICATION IN E-LEARNING ENVIRONMENTS

Temitope Oluwafunmilayo Adetunji

School of Computing, Department of Data Science, Robert Gordon University, United Kingdom.
****Corresponding Author Email: t.adetunji@rgu.ac.uk***

ARTICLE DETAILS

Article History:

Received 23 June 2024
Revised 15 July 2024
Accepted 08 August 2024
Available online 14 August 2024

ABSTRACT

Strong security protocols are essential to guarantee user authentication and data integrity amidst the rapidgrowth of e-learning platforms. Artificial Intelligence (AI)-based facial recognition has grow into a widely used technology in the modern world with anextensive range of applications. Using machine learning and algorithmic methodologies, the technology analyzes and recognizes faces in digital photos or videos. In this review paper we explores recent developments in artificial intelligence (AI)-assisted facial recognition technologies designed to enhance user authentication and security in computer-based assessments within e-learning platforms. We examine the evolution of facial identity verification, discuss current challenges and solutions, and offer insights into the potential of these technologies to revolutionize the e-learning landscape. The study emphasizes how AI-powered facial recognition could transform e-learning security by promoting integrity in academia, preventing misconduct, and enhancing trust.

KEYWORDS

e-learning platforms, Artificial Intelligence, authentication, facial recognition, machine learning and algorithmic methodologies.

1. INTRODUCTION

These days, there is a tremendous increase in the number of online learning resources that offer creative ways to educate individuals and other internet users. When compared to traditional education, online learning offers a variety of efficient and effective benefits. Although online exams and certificates are growing in popularity, they have several limitations. These include the potential for contract cheating, impersonation, and plagiarism, all of which have the potential to degrade the caliber of online instruction and evaluation and create issues for the administrations of the colleges who offer it. Surahman and Wang contended that as online education grows, there may be a rise in cheating and the detrimental effects that would arise from academic dishonesty, such as plagiarism, which is not a recent occurrence but has been more prevalent in recent years (Surahman and Wang, 2022; Mellar et al., 2018). Exam cheating has existed since the introduction of written tests, but the use of electronic gadgets in the cheating process has raised new concerns (Ahmadi, 2020). A group researchers speculated that the extent of online assessment cheating may be exaggerated, but that the issue may actually be much worse (Mellar et al., 2018). He believes that there are currently no really reliable methods for confirming a student's identification on an e-learning or distance education platform.

As a result, there is increasing interest in improving authentication procedures by utilizing cutting-edge technology like artificial intelligence (AI). In recent years, there have been notable improvements in certain technologies, such as AI-powered facial recognition. Facial biometrics ensures e-learning systems are reliable and successful while bringing competitive authentication techniques and advancements to the table. It is recommended to employ facial biometrics to ensure user authenticity. This will decrease the likelihood of cheating and other user authentication irregularities while also giving learners an efficient authentication solution. When a user verifies their identification, the authentication system categorizes their face biometric traits based on how closely their features match each other. Through the use of machine learning algorithms, facial recognition technology analyzes and recognizes distinctive facial traits, offering a convenient and safe means of authentication (Sharma et al., 2022). With the e-learning sector expanding at an accelerating rate, online learning requires high-quality features that offer students varying levels of satisfaction. By comparing specific facial traits from an image with a facial database, face recognition technology may identify and authenticate a person from a digital image or video frame (Gathuri et al., 2019).

2. LITERATURE REVIEW

2.1 Evolution of Facial Recognition Technology

During the 1960s, Woody Bledsoe, Helen Chan Wolf, and Charles Bisson were among the pioneers in the creation of automated facial recognition technology (FERET) (Gupta et al., 2023). At first the system were not very practical or scalable because they needed human input to define the facial features. Regardless ofearly difficulties, later advances—such as Takeo Kanade's system in 1970—sought to computerize the recognition process (Lehmuskallio and Meyer, 2022). Yet, reliability was an issue at this point. The Defense Advanced Research Project Agency (DARPA) and the Army Research Laboratory (ARL) started the FERET program in 1993, marking a critical breakthrough in the advancement of automated face recognition capabilities for security and law enforcement (Ramachandra et al., 2023).

Consequently, businesses like Vision Corporation, Miros Inc., and Viisage Technology initiated the commercialization of the face recognition technology.There was an observation of extensive usage of facial recognition technology, mostly in (Department of Motor Vehicles) DMV offices, where it was employed to stop identity theft during the issue of driver's licenses (Kauder, 2021). Furthermore, law enforcement administrations started integrating facial recognition technology into criminal identification systems. One instanceof this is Minnesota, which implemented the FaceIT system in 1999. In order to increase recognition precision, feature-based techniques such as statistical Principal

Quick Response Code	Access this article online	
	Website: www.jtin.com.my	**DOI:** 10.26480/jtin.02.2024.63.65

Cite The Article: Temitope Oluwafunmilayo Adetunji (2024). Advancements in Ai-Powered Facial Recognition for Secure User Authentication in E-Learning Environments. *Journal of Technology & Innovation, 4(2): 63-65.*

component analysis (PCA) and linear discriminant analysis (LDA) were engaged in facial recognition study during the 1990s (Taskiran et al., 2020).

Gabor filters and elastic bunch graph matching were first used in Christoph von der Malsburg's Bochum system to augment face identification and recognition. The Viola–Jones method, which was developed in 2001, allowed for even further progress in real-time face detection by quickly and accurately identifying faces in video data (Taskiran et al., 2020). This technique made it easier to put facial recognition technology to use in a variety of contexts, such as teleconferences and user interfaces. Facial recognition technology is becoming increasingly important in security and military operations, as seen by recent uses, such as Ukraine's employment of Clearview AI software to identify dead soldiers and identify possible spies (Severi et al., 2022). On the other hand, moral questions about its use in combat emphasize the necessity of responsible use and open governance structures.

2.2 Computer-Based Assessmentswithin E-Learning

Online learning evaluations play a crucial role in the advancement of education, particularly when it comes to assessing whether or not a student's progress is sufficient based on exam results. Additionally, it offers numerous benefits, particularly for educators (Al-Maqbali et al., 2022). These include the ability to quickly create online tests, administer exams using a computer, and easily track answers while taking the test. The user's identity is verified by face recognition software based on their physical patterns. Eye sensor monitoring is utilized to control the user's behavior during the exam, providing a strict feeling of user verification. Here, artificial intelligence technology enhances the integrity of online learning, which is rife with cheating and plagiarism (Taskiran et al., 2020).

Online learning evaluations play a crucial role in the advancement of education, particularly when it comes to assessing whether or not a student's progress is sufficient based on exam results. Additionally, it offers numerous benefits, particularly for educators. These include the ability to quickly create online tests, administer exams using a computer, and easily track answers while taking the test (Kaur et al., 2020). Quick access to assessment results without having to spend time reviewing and making corrections, as well as simple computation of test result trends. Additionally, the ability to take exams online without having to physically be at a specific place and receive results right away are two more advantages for students.

Prior to configuring the system, the user or learner checks the sensitivity of the size, noise, backdrop clutter, and face orientation. Face recognition analysis of the authorized photograph is next performed, confirming that you may move forward with the online exam assessment (Makrushin et al., 2018). The advanced approach of facial recognition has potential benefits over traditional user authentication, including more dependable results, reduced online exam anomalies (such as cheating or suspicious behavior), robust identity validation, and increased data efficiency for educators and potential users (Al-Maqbali et al., 2022).

2.3 AI-Powered Facial Recognition Algorithms:

AI Face recognition procedures involvemultiplestages to detect and evaluate human faces in digital images or video footage. Here is an overview of the process

2.4 Facial Detection

Facial detectioninvolves locating and extracting faces using algorithmic methods from an image or video whichis the first step in facial recognition (Kaur et al., 2020). Majority of facial detection systems employ either feature-based or machine learning-based to identify facial featuressuch as eyes, noses, and mouths, feature-based methods apply mathematical models and predefined criteria (Hasan et al., 2021). Alternatively, machine learning techniques utilize trained models, like convolutional neural networks (CNNs), to extract features and patterns from big datasets. Viola-Jones, Haar Cascade, and MTCNN are popular facial recognition algorithms (Koh et al., 2023).

2.5 Facial Alignment

The next stage of facial recognition after facial detection is face alignment. It involves standardizing and transforming recognized faces into a single reference framework (Adjabi et al., 2020). By aligning the individual faces with a reference model, facial alignment algorithms compensate for variations in the face's position, size, tilt, and brightness. This system dramatically improves facial recognition's precision and robustness by reducing noise and distortion in face photos, (Jabberi, 2023). Examples include Active Shape Models (ASMs), Active Appearance Models (AAMs), and Facial Landmark Detection.

2.6 Facial Verification

The next stage of facial recognition is facial verification, which involves verifying or disproving the identity of a particular face in comparison to a reference face (Guo, 2023). Algorithms for facial verification compare two face representations and determine how similar or dissimilar they are in order to determine how likely it is that they belong to the same person. Effective face verification techniques include Support Vector Machines (SVMs), K-Nearest Neighbors (KNNs), and Siamese Networks. They are commonly used for authentication and access control applications, such as opening mobile devices or entering secure areas.

2.7 Facial Identification

Facial identification is the last stage of facial recognition, which involves giving a name or label to a given face using a database of faces that have been identified. Algorithms for facial recognition search the database for the closest or most similar match to the requested face, providing the matching identity or a list of possible candidates. Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), and DeepFace are popular facial identification algorithms that are often used for recognition and classification tasks, such as photo tagging or suspect identification.

3. Problems and Challenges of Facial Recognition

There are a number of issues and concerns with facial recognition using AI that need to be resolved accrding to (Buolamwini and Gebru, 2018; Deng et al., 2019; Liao et al., 2021). Here are a few of them:

- Bias: a group researcher stated that one of the main issues with facial recognition software is bias (Deng et al., 2019). The data that is utilized to train AI algorithms can lead to bias. Inequitable treatment may result from the algorithm's poor performance on particular demographics if the data is not diverse.

- Privacy issues: The use of facial recognition technology also presents privacy issues, especially when it is done without the subjects' knowledge or consent. Concerns have also been raised regarding the potential for unwanted access to facial recognition data (Buolamwini and Gebru, 2018; Liao et al., 2021).

- Accuracy: Although advances in facial recognition technology have been made recently, accuracy remains a challenge. Errors in identification can result from false positives and false negatives (Deng et al., 2019; Liao et al., 2021).

- Obstruction and lighting: Differences in illumination can have an effect on facial recognition technology, and objects that obsruct facial characteristic e.g hats or glasses—might complicate face recognition (Buolamwini and Gebru, 2018).

- Ethical concerns: There has beenethical issues with respect to human rights and civil liberties when using facial recognition technology in surveillance and law enforcement applications presents (Deng et al., 2019; Liao et al., 2021).

It is vital to make and enforce appropriate policies and measures for facial recognition technology so as toresolve these issues. Using a variation of datasets, maintaining security and privacy, enhancing precision and taking into consideration the moral implications of face recognition technology (Buolamwini and Gebru, 2018; Deng et al., 2019; Liao et al., 2021).

4. Future of AI and Facial Authentication

Artificial Intelligence-driven facial recognition technology has great potential to improve user authentication processes in e-learning systems in the future. It is projected that progresses in convolutional neural networks (CNNs), one type of deep learning algorithm, would increase the accuracy and reliability of facial recognition (Chen et al., 2020). These advancements will make it simple to integrate facial authentication into e-learning platforms, giving students secure access to lesson plans and exam questions. Moreover, the establishment of multimodal biometric systems that integrate speech or keyboard dynamics with facial recognition would advance the robustness and resistance of authentication against spoofing assaults (Makrushin et al., 2018). Furthermore, accessible and effective utilization of facial authentication systems across various e-learning contexts will be made possible by developments in edge computing and cloud-based solutions (Korolkova et al., 2019).

5. Conclusion

Applications connecting human-computer interaction are continually changing to improve usability in a number of ways. Among this, online education, which makes use of facial recognition technology to enhance the learning experience in virtual classrooms and digital libraries. Even while studies indicate that facial recognition can improve learning results, it's critical to recognize that facial recognition has shortcomings. For face recognition technology to be dependable and successfully implemented in educational contexts, these constraints must be addressed through more research and development efforts.

References

Adjabi, I., Ouahabi, A., Benzaoui, A., and Taleb-Ahmed, A., 2020. Past, present, and future of face recognition: A review. Electronics, 9 (8), Pp. 1188.

Ahmadi, H., 2020. Cheating in Education: A Focus on Plagiarism.

Buolamwini, J., and Gebru, T., 2018. Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of the 1st Conference on Fairness, Accountability and Transparency, Pp. 77-91.

Chen, Z., Wei, X., Cai, Z., and Xie, L., 2020. Deep learning-based facial expression recognition for e-learning systems: A review. IEEE Access, 8, Pp. 91311-91329.

Deng, W., Liu, J., and Wang, Z., 2019. Understanding privacy concerns and user acceptance of facial recognition technology: The role of facial identification and location tracking capabilities. Information & Management, 56, Pp. 103160.

Gathuri, J.W., Luvanda, A., Matende, S., and Kamundi, S., 2014. Impersonation challenges associated with e-assessment of university students. Journal of Information Engineering and Applications, 4 (7), Pp. 60-68.

Guo, Z., and Kennedy, L., 2023. Policing based on automatic facial recognition. Artificial Intelligence and Law, 31 (2), Pp. 397-443.

Gupta, O.P., Agarwal, A.P., and Pal, O., 2023. A study on Evolution of Facial Recognition Technology. In 2023 International Conference on Disruptive Technologies (ICDT) (pp. 769-775). IEEE.

Hasan, M.K., Ahsan, M.S., Newaz, S.S., and Lee, G.M., 2021. Human face detection techniques: A comprehensive review and future research directions. Electronics, 10 (19), Pp. 2354.

Jabberi, M., Wali, A., Chaudhuri, B.B., and Alimi, A.M., 2023. 68 landmarks are efficient for 3D face alignment: what about more? 3D face alignment method applied to face recognition. Multimedia Tools and Applications, 82 (27), Pp. 41435-41469.

Kauder, M.M., 2021. Out of the Shadows: Regulating Access to Driver's License Databases by Government Agencies. Drake L. Rev., 69, Pp. 463.

Kaur, S., Kumar, P., and Kumaraguru, P., 2020. Deepfakes: temporal sequential analysis to detect face-swapped video clips using convolutional long short-term memory. Journal of Electronic Imaging, 29 (3), Pp. 033013.

Koh, R.L.X., 2023. Identity prediction with uncovered facial features while wearing mask [Doctoral dissertation, UTAR].

Korolkova, O., Selim, H., and Sidorenko, D., 2019. Privacy-preserving biometric authentication in e-learning systems: A survey. ACM Computing Surveys, 52 (5), Pp. 1-34.

Lehmuskallio, A., and Meyer, R., 2022. Experimental indices: Situational assemblages of facial recognition.

Liao, Q.V., Koepke, A.S., Kuipers, B., and Savvides, M., 2021. Facial recognition technologies in the wild: A call for a Federal Office. Science, 372, Pp. 131-133.

Makrushin, A., Neubert, T., Dittmann, J., and Vielhauer, C., 2018. Comparative study of biometric hashing for voice and face modalities. Multimedia Tools and Applications, 77 (2), Pp. 1727-1754.

Mellar, H., Peytcheva-Forsyth, R., Kocdar, S., and Karadeniz, A., 2018. Addressing cheating in e-assessment using student authentication and authorship checking systems: teachers' perspectives. *International Journal for Educational Integrity, 14 (1), 2. DOI: 10.1007/s40979-018-0025-x

Ramachandra, A.C., Khan, R.A., Bharat, R., Nasir, M.D., and Rajesh, N., 2023. Security and Safety System using Facial Characteristics. In 2023 International Conference on Applied Intelligence and Sustainable Computing (ICAISC) (pp. 1-5). IEEE.

Severi, Misty, 2022. Ukraine uses facial recognition software to identify dead Russian soldiers.

Sharma, S., Bhatt, M., and Sharma, P., 2020. Face Recognition System Using Machine Learning Algorithm. In 2020 5th International Conference on Communication and Electronics Systems (ICCES), pp. 1-5). DOI: 10.1109/ICCES48766.2020.9137850

Surahman, E., and Wang, T.H., 2022. Academic dishonesty and trustworthy assessment in online learning: A systematic literature review. Journal of Computer Assisted Learning, 38 (6), Pp. 1535-1553.

Taskiran, M., Kahraman, N., and Erdem, C.E., 2020. Face recognition: Past, present and future (a review). Digital Signal Processing, 106, Pp. 102809.