ZIBELINE INTERNATIONAL™ PUBLISHING

ISSN: 2773-6202 (Online)
CODEN: JTIOCC

Journal of Technology & Innovation (JTIN)

DOI: http://doi.org/10.26480/jtin.02.2024.72.74

REVIEW ARTICLE

ETHICAL CONSIDERATIONS IN AI-DRIVEN FACIAL AUTHENTICATION FOR ONLINE TESTING AND EXAMINATIONS

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 12 August 2024
Available online 14 August 2024

ABSTRACT

Artificial intelligence (AI)-powered facial recognition technology has turn out to be more prevalent in online testing and exams, encouragingbetter security and swift authentication processes. Nevertheless, ethical matters are necessary to be carefully deliberated putting it to practice. The ethical concernsabout the usage of AI-powered facial recognition in online assessments are explored in this paper. Via athoroughresearch of its advantages and disadvantages, we elucidate the complicated relationship between technical progress and moral issues. Privacy concerns are judiciously considered, as well as the possibility for illegal surveillance and the biases existing in facial recognition software. Furthermore, we offer a set of ethical standards for online learning environments that safeguard user identities and regard privacy rights. We hope to add to the creation of moraloutlines that uphold justice, accountability, and transparency in the use of facial recognition technology for virtual testing and exams by deal with these moral problems and supporting accountable deployment.

KEYWORDS

Ethical considerations, artificial intelligence, facial recognition, Examinations, Privacy concerns, Virtual learning environments

1. INTRODUCTION

Exams and tests are a crucial component of our educational system's process of determining a student's level of understanding.Exams, assessments, and grades are a few of the vital tools used by learning institutions to evaluate students' performance in order to ensure that students finish their tests accurately and that there is no cheating or other improper activity, most exams include certain standards that students must follow when writing them. Exams can be administered and pupils can be efficiently monitored by educational institutions (Albreiki et al., 2021). An efficient method of image evaluation, which has accrue attention recently for security and Surveillance use is facial recognition. Facial recognition isthe method of authenticatingsomeone's identify using their face. It records, examines, and contrasts the patterns according to the features of the subject's face, including their mouth, nose, eyes, and chin. It is employed to grant authorized and authenticated access to a service or system.This biometric identification method utilize the biometric configurations on a human face (Sukmandhani et al., 2019; Venkateswar et al., 2019).

One of the three pillars of education, together with pedagogy and curriculum, is assessment (Barber, 2021). The four fundamentals of artificial intelligence in education (AIED) is Examinations,learning personalization, automated learning systems, and intelligent learning environments, according to Chaudhry and Kazim's comprehensive study of the area (Chaudhry and Kazim's, 2022). Assessment is defined as "any appraisal (or judgment or evaluation)... of work or performance" in an educational setting (Valentine et al., 2021). Recently, there has been a remarkablegrowth in the usageof artificial intelligence (AI) driven facial recognition in assessments.There was a boost in AI and adaptive learning technology between the years 2011 to 2021 tripling the worth, and they are expected to surpass immersive learning technologies as top studied topic in future, according to studies on assessments pertaining to digital education in higher education (Lim et al., 2022). It is widely believed by stakeholders that artificial intelligence (AI) has the potential to offer a more equitable and comprehensive evaluation system that would assess students over an extended period of time and from an evidence-based, value-added standpoint (Chaudhry et al., 2022).

Concerns of its own are raised when AI is used in assessments. Implementing AI involves operational and technical system implementation challenges.It may be argued that these issues involve fewer gray areas than the difficulty of negotiating the limits and borders of ethics (Morley et al., 2023). The use of AI-based assessments may provide ethical challenges that evaluators, as assessment practitioners, must recognize, appreciate, and uphold. The reviewgoalsis to explore the moralfeaturesconnected to the use of AI-powered facial recognition technologies in online assessments and tests. The paper specifically attempts to examine the benefits and cons of putting such technology into reality, talk about potential privacy issues, and offer standards for moral behavior to protect user identities during assessments carried out in online learning settings.

2. LITERATURE REVIEW

One of the three pillars of education, together with pedagogy and curriculum, is assessment (Barber, 2021). The meticulous analysis of facial pictures has been a vital toolbox for police enforcement organizations since the nineteenth century. Due to the transition from manual techniques to facial recognition technologies (FRT), the use offacial recognition has greatly enhanced this major tool in the 21st century. Using artificial intelligence (AI) and algorithms, can automatically extract and compare features, as well as every nuance of their measurement(anantrasirichai et al., 2022). This allows a more official matching and identification of a person by comparing the face with other data.

This may occasionally be accomplished by introducing other biometric data, such as eye recognition data. One-to-one matching makes it possible to positively identify a person in a particular setting (Palma et al., 2022).

Quick Response Code	Access this article online	
	Website: www.jtin.com.my	**DOI:** 10.26480/jtin.02.2024.72.74

Cite The Article: Temitope Oluwafunmilayo Adetunji (2024). Ethical Considerations in Ai-Driven Facial Authentication for Online Testing and Examinations. *Journal of Technology & Innovation, 4(2): 72-74.*

On the other hand, one-to-many usage possibilities and implications are made possible when an identified image is used in conjunction with other data banks or lakes. When considering machine learning, algorithms, and AI, matching that can examine data at scale makes newopportunities as well as challenges. The FRT implementation and data collection context may be crucial in determining how individuals' security and privacy concerns in various circumstances are addressed (Almeida et al., 2021).

3. Possible Advantage and Disadvantage of Facial Recognition

3.1 Benefitsof Facial Recognition System

The primary benefit of face recognition technology lies in its ability to interpret biometric data automatically and digitally using an individual's digital image or live video stream for a range of uses. The advantages are itemized below:

3.1.1 Security via Biometrics Verification

One benefit of a face recognition system is that it can be used in biometric security. It can be found in personal electronics like PCs, tablets, and smartphones as well as in workplace identity and access control systems. (Siddiqui et al., 2020).

3.1.2 Automated Image Recognition Feature

You can make the system capable of automatically recognizing images. Take Facebook as an illustration. This social networking site allows for automatic tagging and can identify images of its users. Contemporary smartphones are equipped with an improved camera feature that includes face recognition (Bucher, 2022).

3.1.3 Utilization in Security and Law Enforcement

Another important advantage is the use of facial recognition in law enforcement and security systems. This relates to both its biometrics application and its automated picture recognition capability. With a system that makes a unique facial profile for each person, less intrusive monitoring and identification are realizable.

3.1.4 Enhancing Human-Computer Interaction:

The scheme is compatible with modern augmented and virtual reality apps. Snapchat, Instagram, and TikTok filters depend on both augmented reality and facial recognition technology. Recently, mixed reality headsets show how facial recognition technology can advance human-computer interactions.

3.1.5 Offers Devices with Added Features

It's also significant to recall that giving devices facial recognition software involve giving them more features and functionalities. The Face ID biometric security feature, augmented reality support, and different camera functions or computational photography abilities of an iPhone are all supported by the same technology (Riccio et al., 2022).

4. Detriments and Limitations of Facial Recognition System

In spite of the earlier listed benefits and uses, face recognition technology has limitations and shortcomingsassociated to questions about its effectiveness and contentious uses.

4.1 Problems with Efficiency and Reliability

The ineffectiveness and unreliability of facial recognition technology in comparison to other biometric systems, like fingerprints, is one of its main drawbacks. Variables including lighting, expression, image or video quality, and software and hardware capabilities can affect the system's reliability or accuracy as well as its overall performance (Alsaadi, 2021).

4.2 Additional Reports Concerning Its Reliability

A lot of information have caught attention to the flaws in some systems. According to an advocacy group, the precision rate of the systems used by law enforcement in the United Kingdom was only 2%. A different study claims that the installations in Florida and London did not enhance police enforcement (Patrick, 2023).

4.3 Fears about Potential Racial Bias

According to an American Civil Liberties Union study, in tests involving individuals of color, Amazon's Rekognition algorithm failed over 40% of the erroneous matches. False matches in the system have been blamed for maintaining racial bias. Leslie highlights a further drawback of facial recognition technology (Leslie, 2020).

4.4 Varying Performance across Different Systems

The underlying technologies also affect a system's capabilities. Some Android smartphones rely on the front-facing cameras, which results in an inferior or unreliable system. iPhones and iPads have an improved application of three-dimensional mapping since they use infrared (Kortli, 2020).

4.5 Possible Privacy Law Problems

Another main shortcoming of face recognition technology is the possibility of privacy rights violation. Businesses are required by the Illinois Biometric Information Privacy Act to get informed consent prior to collecting biometric data. It has also been criticized that the system's use for mass identification leads to widespread surveillance and profiling (Kortli, 2020).

5. Ethical Concerns in Facial Recognition for Online Examinations

However, it is still challenging to strike a balance between privacy concerns and the advantages of facial recognition technology. Policymakers, tech developers, and privacy activists need to collaborate and have constant conversations in order to establish the proper regulation balance (Patel, 2024). By combining different viewpoints and areas of knowledge, regulations that effectively safeguard privacy and permit the ethical and responsible use of facial recognition technology can be developed. Facial recognition technology has a big impact on online assessment; it increases security while also posing privacy issues (Kostka et al., 2021). On the one hand, facial recognition technology used in online assessment systems offers a reliable way to verify test-takers' identities, lowering the likelihood of cheating and preserving the integrity of the exams.

This method provides a robust authentication approach that can help prevent impersonation and illegal access to assessments in remote learning situations where traditional invigilation techniques may not be feasible (Saqib and Moon, 2023). However, there are significant privacy concerns raised by the growing use of facial recognition in online assessments. The use of surveillance tools can raise concerns about breaches of privacy and unwarranted monitoring, even when employed for security purposes (Malik et al., 2024). Students may feel anxious or uneasy knowing that their facial data is being captured and analyzed during tests, particularly if they haven't provided their express consent. Additionally, the potential for biases in facial recognition algorithms jeopardizes the impartiality and equity of judgments, which concerns the possibility of unfair treatment or discrimination against specific people or groups (Jones et al., 2020; Orwat, 2020).

Online assessment systems' collection and storage of face data also poses security risks, such as the possibility of data breaches or illegal access to personal data. Due to the vast amounts of personal data involved, including biometric IDs and facial pictures, robust data protection protocols are required to safeguard test-takers' confidentiality and privacy (Jain et al., 2021). In order to offer rules for the proper use of personal data and guarantee that assessment providers are held accountable, regulations such as the General Data Protection Regulation (GDPR) of the European Union are crucial (Tzanou, 2020). Managing the convergence of security and privacy concerns requires striking a balance.facial recognition technology and online evaluation. Even though facial recognition provides useful tools for improving exam security, its implementation needs to respect people's right to privacy and provide fairness and transparency in evaluation procedures. Fostering trust and confidence in online assessment systems necessitates careful consideration of ethical principles, stakeholder interaction, and adherence to legal standards (Almeida et al., 2022).

6. Ethical Guidelines and Recommendations

Transparency and explainability are important ethical considerations for facial recognition systems. People need to be aware of the precise methods used, kept, and gathered for their facial data. Building trust and enabling people to make informed judgments can be achieved by transparent practices and the capacity to elucidate the decision-making processes of these systems (Matheus et al., 2020). Obtaining informed permission is an essential part of protecting one's privacy. People should have complete control over the use of their facial data and be fully informed about how it will be used. Ensuring people's autonomy and privacy rights requires putting in place transparent consent methods and opening up data processing procedures. Incorporating stakeholders from other areas is crucial to effectively address the intricate concerns surrounding the intersection of privacy and facial recognition technologies. Policymakers, tech developers, privacy advocates, and members of civil society must

work together to create comprehensive and adaptable frameworks that reduce risks, protect privacy, and promote innovation (Gill and Germann, 2022).

7. Facial Recognition and Privacy in the Future

Future developments in facial recognition technology should bring about more accurate algorithms that address biases. Techniques to lessen bias and guarantee justice in these systems are being developed by researchers and developers, which will lessen the likelihood of discrimination. However, continued legal and regulatory review and adaptation are necessary for the proper development and use of facial recognition technology. Getting the right balance between the benefits of face recognition-driven by AI and the defense of an individual's right to privacy. Proactive actions and ongoing cooperation are needed to handle new privacy issues and guarantee that moral issues govern the application of face recognition technology in the future (Martinez-Martin, 2021).

8. Conclusion

There are advantages and disadvantages to consider when examining the ethical aspects of AI-powered facial recognition for online assessments and tests. This technology creates serious privacy concerns, including the possibility of unjustified surveillance, biases, and security breaches, even while it also has the ability to improve security and tailor experiences in online evaluations. To properly handle these issues, cooperation between legislators, IT developers, and privacy activists is essential. Ensuring accountable and moral use of facial recognition technology in online evaluations requires the establishment of comprehensive regulatory frameworks that incorporate concepts of transparency, informed consent, and fairness. By doing this, we may provide a setting in virtual learning settings where privacy and creativity coexist peacefully, encouraging faith in the moral standards governing AI-driven facial recognition.

Refferences

Albreiki, B., Zaki, N., and Alashwal, H., 2021. A systematic literature review of student'performance prediction using machine learning techniques. Education Sciences, 11 (9), Pp. 552.

Almeida, D., Shmarko, K., and Lomas, E., 2022. The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. AI and Ethics, 2 (3), Pp. 377-387.

Almeida, D., Shmarko, K., and Lomas, E., 2022. The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. AI and Ethics, 2 (3), Pp. 377-387.

Alsadi, A., Berardi, D., Callegati, F., Melis, A., and Prandini, M., 2021. A security monitoring architecture based on data plane programmability. In 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit) (pp. 389-394). IEEE.

Anantrasirichai, N., and Bull, D., 2022. Artificial intelligence in the creative industries: a review. Artificial intelligence review, 55 (1), Pp. 589-656.

Barber, W., Harrison, R., VanOostveen, R., and Childs, E., 2021. Building Better Online Communities in the Post Pandemic World. In ECEL 2021 20th European Conference on e-Learning (p. 59). Academic Conferences International limited.

Bucher, T., 2022. Facing AI: conceptualizing 'fAIcecommunication'as the modus operandi of facial recognition systems. Media, Culture & Society, 44 (4), Pp. 638-654.

Chaudhry, M.A., and Kazim, E., 2022. Artificial Intelligence in Education (AIEd): A high-level academic and industry note 2021. AI and Ethics, 2 (1), Pp. 157-165.

Geetha, M., Latha, R.S., Nivetha, S.K., Hariprasath, S., Gowtham, S., and Deepak, C.S., 2021. Design of face detection and recognition system to monitor students during online examinations using Machine Learning algorithms. In Proceedings of the 2021 International Conference on Computer Communication and Informatics (ICCCI -2021) (pp. 1–6). Coimbatore, India.

Gill, A.S., and Germann, S., 2022. Conceptual and normative approaches to AI governance for a global digital ecosystem supportive of the UN Sustainable Development Goals (SDGs). AI and Ethics, 2 (2), Pp. 293-301.

Jain, A.K., Sahoo, S.R., Kaubiyal, J., 2021. Online social networks security and privacy: comprehensive review and analysis. Complex & Intelligent Systems, 7 (5), Pp. 2157-2177.

Jones, K.M., Asher, A., Goben, A., Perry, M.R., Salo, D., Briney, K.A., and Robertshaw, M.B., 2020. We're being tracked at all times: Student perspectives of their privacy in relation to learning analytics in higher education. Journal of the Association for Information Science and Technology, 71 (9), Pp. 1044-1059.

Kortli, Y., Jridi, M., Al Falou, A., and Atri, M., 2020. Face recognition systems: A survey. Sensors, 20 (2), Pp. 342.

Kostka, G., Steinacker, L., and Meckel, M., 2021. Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States. Public Understanding of Science, 30 (6), Pp. 671-690.

Leslie, D., 2020. Understanding bias in facial recognition technologies. arXiv preprint arXiv:2010.07023.

Lim, C.K., Haufiku, M.S., Tan, K.L., Farid Ahmed, M., and Ng, T.F., 2022. Systematic review of education sustainable development in higher education institutions. Sustainability, 14 (20), Pp. 13241.

Malik, A.S., Acharya, S., and Humane, S., 2024. Exploring the Impact of Security Technologies on Mental Health: A Comprehensive Review. Cureus, 16 (2).

Martinez-Martin, N., Luo, Z., Kaushal, A., Adeli, E., Haque, A., Kelly, S.S., and Milstein, A., 2021. Ethical issues in using ambient intelligence in health-care settings. The lancet digital health, 3 (2), Pp. e115-e123.

Matheus, R., Janssen, M., and Maheshwari, D., 2020. Data science empowering the public: Data-driven dashboards for transparent and accountable decision-making in smart cities. Government Information Quarterly, 37 (3), Pp. 101284.

Orwat, C., 2020. Risks of Discrimination through the Use of Algorithms. Berlín: Federal Anti-Discrimination Agency.

Palma, D., and Montessoro, P.L., 2022. Biometric-based human recognition systems: an overview. Recent Advances in Biometrics, 27, Pp. 1-21.

Patel, K., 2024. Ethical reflections on data-centric AI: balancing benefits and risks. International Journal of Artificial Intelligence Research and Development, 2 (1), Pp. 1-17.

Patel, K., 2024. Ethical reflections on data-centric AI: balancing benefits and risks. International Journal of Artificial Intelligence Research and Development, 2 (1), Pp. 1-17.

Patrick, L., 2023. How to Save Face & the Fourth Amendment: Developing an Algorithmic Auditing and Accountability Industry for Facial Recognition Technology in Law Enforcement.

Riccio, F.M.V., Almeida, M.S., Vasconcelos, S.M., Pires, L.G., and Nicodemos, R.L.F., 2022. Embankment supported by low area replacement ratio stone columns, monitoring and numerical studies. KSCE Journal of Civil Engineering, 26 (2), Pp. 619-629.

Saqib, M., and Moon, A.H., 2023. A systematic security assessment and review of Internet of things in the context of authentication. Computers and Security, 125, Pp. 103053.

Sukmandhani, A.A., and Sutedja, I., 2019. Face recognition method for online exams. In International Conference on Information Management and Technology (ICIMTech) (pp. 175–179). Jakarta/Bali, Indonesia.

Tzanou, M., 2020. Personal data protection and legal developments in the European Union. IGI global.

Valentine, N., Durning, S., Shanahan, E.M., and Schuwirth, L., 2021. Fairness in human judgement in assessment: a hermeneutic literature review and conceptual framework. Advances in Health Sciences Education, 26, Pp. 713-738.

Venkateswar Lal, P., Nitta, G.R., and Prasad, A., 2019. Ensemble of texture and shape descriptors using support vector machine classification for face recognition. Journal of Ambient Intelligence and Humanized Computing.