ZIBELINE INTERNATIONAL™ PUBLISHING

ISSN: 2773-6202 (Online)
CODEN: JTIOCC

Journal of Technology & Innovation (JTIN)

DOI: http://doi.org/10.26480/jtin.02.2024.66.71

REVIEW ARTICLE

AI-BASED FACIAL AUTHENTICATION IN EDUCATION: IMPLICATIONS FOR ACADEMIC INTEGRITY AND TECHNOLOGICAL ADVANCEMENT

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

This review examine the importance of AI-based facial authentication to enhance academic honesty in the evolving online education environment. The landscape of education is growing due to technological advancements; maintaining acceptable learning results will become more challenging with the move to digital platforms. Explains the development and history of face recognition technology, focusing on the increasing use of artificial intelligence (AI) in its combination to create trustworthy biometric authentication systems. Focuses on the accuracy and reliability of these technologies' use in person identification by examining in-depth AI-based face registration and authentication processes. The study examines the drawbacks of online education, comprising the increase in potential for dishonesty and impersonation, and how AI-based facial expressions can lessen these problems. It scrutinizes the research on the demise of conventional systems for avoiding online fraud and the rise of fresh instances of academic dishonesty, such as collective fraud and quackery. The following section of the paper addresses the numerous uses of facial recognition technology in education, ranging from virtual learning environments and e-assessment security to campus security and attendance control. It draws attention to how this technology may be used to progress resource allocation, streamline workflows, and create more individualized learning opportunities. The study also discourses privacy and ethical issues associated to the use of facial recognition in educational settings, stressing the need for accountable and open use that places a robust emphasis on safety of students' rights and interests. This review make available insight into the transformational possibility of this technology in maintaining authenticity and quality of education in the digital era by observing the convergence of academic integrity and AI-based authentication.

KEYWORDS

Artificial intelligence, authentication, facial recognition, online education, technology.

1. INTRODUCTION

In recent times, there has been an increase in the prevalence and innovation of facial recognition technology, which employs algorithms to recognize individuals in static photographs or videos (Qiang, et al., 2022). The incorporation of artificial intelligence (AI) into facial recognition systems is one example of such innovation. The system converts the facial data into a biometric template, which is a digital representation of the person's facial features (Verganti et al., 2020). When a person attempts to access a system, their face is scanned, and the system uses AI algorithms to compare the scan with the stored biometric template. The system converts the facial data into a biometric template, which is a digital representation of the person's facial features. When a person attempts to access a system, their face is scanned, and the system uses. AI algorithms to compare the scan with the stored biometric template (Betrand, et al., 2023; Ndubuisi et al., 2024).

Academic integrity is considered the core principle in education that ensures students undergo learning with honesty and ethical principles. It encompasses values of honesty, trust, fairness, and responsibility, and is very critical in the credibility and quality of education. It sustains academic standards through the dedication of students to learning (Holden et al., 2021). This fosters a culture of professionalism and integrity within the student body. Academic integrity is a foundational pillar that aims to instill honesty, confidence and accountability in students in an effort to demonstrate their commitment to learning and as a result can help create a positive culture of integrity (McCabe and Pavela, 2004).

Modern technology has placed a strong impact on education with the approach to personalized learning, interactive learning, and ease of access, collaboration, efficiency, and availability of resources, skill development, continuous learning, data-driven insights, and a global perspective (Raja and Nagasubramani, 2018). Adaptive software and online resources are used to create personalized learning plans, while interactive learning through virtual labs, simulations, and educational games increases understanding and retention. Technology has made education more accessible to people worldwide, including those with disabilities, through online courses and specialized learning apps (Aggarwal, 2023). Online platforms foster global learning communities, allowing for collaboration regardless of physical location. Teachers are able to concentrate on teaching when administrative activities are automated. The internet offers an enormous array of resources, for example open educational resources, enhancing the educational experience (Zamiri and Esmaeili, 2024).

Digital literacy and other 21st-century skills are developed through exposure of the educational system to technology. Online learning environment offers lifelong learning beyond traditional schooling (González-Salamanca et al., 2020). Educational technologies monitors student progress, giving data-driven insights to tailor teaching strategies. Global perspectives are also provided by technology, preparing students for a globalized world (Agarwal et al., 2024). An important factor in technological advancement is improving educational system. Opportunities for creativity are increased, personalized learning is supported, and formalized learning is enhanced.

Quick Response Code	Access this article online	
	Website: www.jtin.com.my	**DOI:** 10.26480/jtin.02.2024.66.71

Cite The Article: Temitope Oluwafunmilayo Adetunji (2024). Ai-Based Facial Authentication in Education: Implications for Academic Integrity and Technological Advancement. *Journal of Technology & Innovation, 4(2): 66-71.*

Technology can make learning more engaging for students and provide greater variety, allowing for more personalized and interactive instruction. With the help of distance learning systems, technology has proven essential for the sustainability of education during crises such as the COVID-19 pandemic (Boshkut et al., 2020; Haleem et al., 2022). At the center of cutting-edge innovation and academic integrity, AI-based facial verification in education is a game-changing breakthrough. Strong verification methods are more important than ever to guard against fraud and preserve the integrity of academic achievements as educational institutions use digital platforms for learning and assessment (Gallent, 2023).

1.1 Brief History of Facial Authentication

In 1964, computer programming for facial recognition was investigated by American researchers Bledsoe (Stevens and Keyes, 2021). They envision a semi-automated process in which users input twenty computer measurements, like the length of the mouth or the width of the eyes. To make the method better, 21 additional markers (such lip width and hair color) were introduced in 1977. 1988 saw the introduction of artificial intelligence as a way to improve upon previously employed theoretical tools, which had numerous flaws. Using mathematics, or "linear algebra," it was possible to simplify and alter images without the need for human markers.

In 1991, Alex Pentland and Matthew Turk of the Massachusetts Institute of Technology (MIT) unveiled Eigenfaces, the first facial recognition system that worked (Turk, 2023). Eigenfaces employs the Principal Component Analysis (PCA) statistical technique. The Face Recognition Grand Challenge (FRGC) competition was launched in 2005 with the goal of promoting and developing face recognition technology to support existing facial recognition research (Adjabi, 2020). Everything goes faster in 2011 because deep learning, a machine learning approach based on artificial neural networks, is used (Srinivas et al., 2022). The computer chooses which points to compare since more photos help it learn.

In 2014, Facebook's in-house Deepface algorithm allows it to identify faces (Dirin and Kauttonen, 2020). The social network asserts that their algorithm is around 97% closer to how well the human eye performs. The development of facial recognition technology today has prompted numerous investments in business, industry, law, and government applications. As an example, Apple recently released updates that included a facial recognition tool that is currently being used by retail and banking (Petrescu, 2019). Mastercard developed the Selfie Pay facial recognition system for online transactions. In 2019, Chinese consumers who wish to purchase a new phone will have to give the operator permission to scan their faces. By utilizing a live facial recognition-based intelligent surveillance system, Chinese police caught a suspect in "economic crime" in 2018 during a concert after his face was recognized among a crowd of 50,000 people using a national database (Adjabi et al., 2022).

2. Literature Review

Academic dishonesty can take various forms, but the most prevalent ones are data fabrication, plagiarism, copying and pasting, and peeking at other people's work (Saleem et al., 2021). Academic fraud damages educational institutions' reputations by producing inaccurate evaluations of students' performance and perhaps inaccurate student grades. Research fraud is an important ethical issue that threatens academic integrity (Mulenga and Shilongo, 2024). Academic fraud severely injures the standing of educational institutions and the credibility of their graduates (Utami, and Purnamasari, 2021). Dishonesty has been detected in various ways. Organizations have used various strategies such as technology-based solutions and ethical education to combat fraud (Asaro et al., 2023) Through technology, such as plagiarism detection software, turnitin.com, or digital essay scanning, educational institutions can ensure that their students are held accountable for their actions (Alua et al., 2023).

Technological advances have accelerated research in this area. Alrubaish*et al*. suggest enhancing the current techniques in order to develop a model that identifies the intention to cheat (Yulita et al., 2023). The algorithm is supported by a range of devices and technology, including an eye-tracking system and a heat detector connected to a security camera. (Klaib et al., 20). Students who want to cheat release a specific spectrum of heat from their bodies because of the connection between their bodies and emotions. Because of the heat rays, the camera will concentrate and recognize the faces of the students. In order to determine whether or not a student is going to cheat, it will next recognize the pupils' eyeballs and begin analyzing their movements21. (Ong et al., 2023). Ultimately, detecting students who plan to cheat would be greatly aided by the use of this technique. Its use would also not be restricted to educational environments; other sectors might employ it with only little modifications (Cotton et al., 2023).

A 360-degree security camera is used in a unique exam proctoring system described by (Turani et al., 2020). The safety of online tests is the primary worry. Because of this, a delivery mechanism must guarantee both the identity of the test-taker and the test's whole validity. This study investigates the use of 360-degree security cameras rather than traditional webcams to increase test security and reduce stressful limits. Furthermore, this study provides an automated proctoring paradigm that can be used to enhance the proposed method and reduce cheating. It does this by eliminating the need for real-time proctoring and scheduling constraints. Online testing is a seamless process and a biometric-secure infrastructure makes it easy to validate and employed an alternative hardware-related method (Turani et al., 2021).

The system hardware, which is utilized to monitor the visual and audio environment of the testing site, consists of a wear-cam, a camera, and a microphone. Their paper describes an online test-taking automated multimedia analytics system. The most important behavioral inputs are continuously assessed by the six main parts of the system, which are text detection, audio detection, active window detection, gaze estimation, and phone detection. They combined the continuous estimating components and added a temporal sliding window to create higher-level characteristics that may be used to classify whether a test-taker is cheating at any time during the exam (Noorbehbahani et al., 2022). Research advancements depend not only on hardware but also on machine learning-based computer vision. Through the use of machine learning innovations, computer vision has improved its ability to process images, recognize objects, and track, leading to more accurate and reliable research.

This detection is successfully accomplished by the use of computer vision. Using machine learning, systems can become more intelligent. Due to this growing intelligence, computer vision systems can now more accurately detect suspicious activity. Technological developments in deep learning processing also have an immediate impact. Several studies have used this approach to identify suspicious behavior in online and offline testing. Usually CNN is used (Ong et al., 2023). In many applications, including industrial automation, medicine, and pedestrian monitoring, CNN frequently uses transfer learning for object recognition (Cengiz et al., 2021). Additionally, it is anticipated that transfer learning will be useful in detecting online exam fraud, as this study shows. There are now only a few English-language online exam cheating detection systems accessible. https://www.autoproctor.com is one such application (accessed on May 2, 2024). Thus, software in the Indonesian language is still required to assist educators with different backgrounds and levels of education (Yulita et al., 2023).

3. AI-based Facial Authentication: How it Works

The two main steps in facial recognition are registration and authentication. The steps are explained below.

3.1 Registration of the Registrar

Facial data collection: An individual's face is thoroughly scanned at the beginning of the registration process. Typically, the camera on the user's device performs this initial scan, securing the biometric data. The scan uses machine learning to provide a 3D representation of the user's facial body, ensuring accuracy and reliability (Phadke, 2023). The scans yield a 3D representation of the user's facial anatomy using machine learning, ensuring precision and dependability. Facial data, extracted in the preceding stage, is projected onto a unique biometric template known as a "faceprint"(Boulos, 2021). This template contains the features of the subject's face, such as the distance between essential landmarks like the eyes, and the measurements from the forehead to the chin. The faceprint uniquely identifies each person's digital ID. (Kanakam et al., 2023).

3.2 Authentication

Face matching algorithms: Every time a person tries to log in, the system captures a new photo of their face. This scan is compared to the stored biometric template. Access is allowed if the system determines that the two scans accurately match. If there is a discrepancy, the user can be asked to try again or provide another form of identity (Ukamaka et al., 2023).

Confirming the identity of the user: Recent years have seen a tremendous improvement in facial recognition technology accuracy, with the most advanced algorithms reaching precision close to that of a person. With the advancement of machine learning and artificial intelligence, the recognition rates have been improved for a large variety of demographics

by addressing the issues with varying lighting, angles, and demographic biases. It is key to bear in mind that it all depends on the permissions for devices of users, software, and hardware to determine the power behind the performance of facial recognition authentication. This integration assures a seamless and safe experience. (Ukamaka et al., 2023).

4. Challenges to Academic Integrity in Online Education

Students can commit acts of dishonesty with increased ease without any presence of physical supervision. Facial authentication powered by AI can prevent this through ensuring that only the person enrolled in a course is the one attending and taking assessments. A major concern has been the erosion of traditional measures to prevent online cheating (Rodrigues et al., 2023). Ghizlane and Reda noted that a significant obstacle to online proctoring is the lack of automated and continuous monitoring systems together with insufficient authentication procedures as opposed to physical (Ghizlane and Reda, 2019).

Without specialist equipment, it is thought to be nearly impossible to conclusively prove a student's cheating in a classroom (Bilen and Matros, 2021; Moukhliss et al., 2019). According to a number of studies, there is a greater likelihood of cheating when there are technological difficulties, poor proctoring, insufficient supervision, and a general perception that integrity in online settings is not being upheld (Gamage et al., 2020; Verhoef and Coetser 2021; Noorbehbahani et al., 2022). Furthermore, having easy access to the internet has made cheating more appealing. This was made abundantly clear when the 2020 Advanced Placement Exams were given in the United States without proctoring. Google searches for exam-related keywords increased dramatically in frequency. Pupils who behaved dishonestly were also identified. According to research, proctored online tests usually result in a GPA rise of half a grade (Dendir and Maxwell, 2020; Diarsini., et al., 2022). As can be expected, these rewards have enhanced the motivation and rationale for the perpetration of academic misdeeds, thereby growing skepticism in the educational system. As applied in the "simultaneous-move game," Bilen and Matros argued that many students balance the utility of online cheating with the associated costs.

Recent studies have, however, noted the new wave of cheating behaviors, particularly over contract and collaborative cheating (Turani et al., 2021). A method, termed "ghosting," refers to giving homework assignments or test administration to another person than the enrolled student in order to evade plagiarism detection software (Ralston, 2021). The growth of this practice has been prompted by pressures to post good grades, lack of safety measures online, and student fatigue. Moreover, the ways of performing collaborative cheating have transformed; this is now done through the use of digital communication applications, file sharing, and study aid sites as a way of collaborating without permission. These new ways of cheating, which are difficult to manage, dent the credibility of online education (Dick et al., 2002).

5. Facial Recognition Technologies in Education

In light of this divisive backdrop, we must think about how these technologies are being used in the unique setting of education. Although it is rarely brought up in discussions about facial recognition in society, one public space where this technology is starting to be adopted and used widely is schools (Andrejevic and Selwyn, 2019). Facial recognition systems have now been made available to hundreds of US schools, with manufacturers "pitching the technology as an all-seeing shield against school shootings. Systems that claim to identify unauthorized individuals have also been designed to employ video object classification, which has been trained to identify objects resembling guns, in addition to more subdued types of "anomaly detection," like when students show up at school wearing different clothes, bags, or other items of clothing (Andrejevic and Selwyn, 2019).

School officials are expected to be able to use these technologies to determine who is initially on campus and to monitor those who have been identified throughout the school. According to the SAFR education system's marketing, "schools can stay focused and better analyze potential threats" by knowing where students and staff are (SAFR 2019). Schools also use facial recognition technology for attendance tracking, which promises to do away with the mistakes and omissions that come with having human teachers call rolls repeatedly for large class sizes (Deepan et al., 2023). This type of facial recognition technology is becoming more and more frequent in countries like the UK and Australia where school shootings and unwanted campus incursions remain rare. The Australian facial recognition roll-call system, "LoopLearn," for example, has allegedly been able to save teachers up to 2.5 hours of work a week. In some places, automated registration systems are also thought to be a useful tool for resolving issues with "proxies" and "fake attendance," particularly in nations like India where it is customary to use false attendance records.

In addition to campus security and tracking real persons, facial recognition technology is being used in many "virtual learning" settings. For example, facial recognition systems are now under development to ensure the validity of various components of online courses. One way to do this is to restrict access to online learning resources (Andrejevic and Selwyn, 2019). Another is the authentication of online learners through the use of webcam-based facial recognition (Valera et al., 2020). In a similar vein, the application of facial recognition technology to the security of online assessments is gaining traction. Finally, face detection methods are becoming more and more popular as a measure of student "engagement" and learning. Studies and research in this area, for example, suggest that recognizing transient "facial actions" can be a useful indicator of students' (non)engagement with virtual learning environments; these moments can be associated with boredom, confusion, delight, flow, irritation, and surprise (Rooj et al., 2023).

When it comes to learning, brow-raising, lip dimpling, and eyelid tightness are seen to be highly perceptive facial expressions. Some argue that "facial microexpression states"—that is, facial states lasting less than 0.5 seconds—have a strong link with conceptual acquisition and may offer valuable insights into learners' thoughts. Overall, emphasis is being drawn to the face as a "continuous and non-intrusive way of understanding certain facets of the learner's current state of mind" (). In fact, a great deal of this work stems from the subject of "emotion learning analytics," which has long attempted to use facial recognition to extract indications of learning in higher education. Learning scientists have focused on utilizing facial recognition to recognize "academic emotions" that represent achievement (pleasure, fear, and frustration) as well as "epistemic" emotions deriving from cognitive processing, social emotions, and engagement with the learning issue.

Dewan assert that recognizing these emotions from facial expressions can provide insight into problems related to knowledge, stimulation, anxiety, and/or annoyance (Dewan, 2019). Some educationalists are eagerly anticipating the widespread use of facial learning detection as a result of these mostly experimental advancements. According to Vinutha there may be opportunities in the near future to obtain a "real-time" understanding of which student groups are "productive" and other situations "where the overall activity is not productive (Vinutha, 2022)." Because automated learning systems may be made to be highly customized, integration of these systems into student learning interfaces is encouraged. This allows for real-time recognition and reaction to specific students while keeping track of their achievements and emotional states. When these systems finally replace and enhance teacher-centered forms of instruction, they must be able to "recognize" and respond to individual students. The online economy's long-standing promise of customization is supported by automated technologies, which can modify it to provide individualized tutoring at a fraction of the cost of hiring human teachers (Mouta et al., 2023).

6. Advances in the Use of the Facial Authentication in the Educational Field

A biometric method named Biotest was created by Kalikova, Koukol *and*Krcal to identify students during exams and tests at random intervals. The teacher can determine whether a student's identification was successful by using this software. A notification is sent to the teacher via the system if a student's identity is not confirmed three times (Thongkanchorn et al., 2021). Fayyoumi and Zarrad created a facial authentication software in the same field of study to help students identify themselves when taking tests online. In order to ensure that the student who started the exam is the same one who finished it and to prevent fraud, the researchers not only configured the software during the online exam login process, but they also conducted continuous monitoring (at short intervals) during the exam period.

The face recognition protection algorithm was proposed by that can identify attackers and prevent them from entering restricted areas accessible only to authorized users (Ovezan et al., 2019). Their proven solution consists of two components: a web browser for facial recognition and recognition, and verification of the use of facial authentication software is identified. The software operates as follows: upon the user's entry to the concerned area, the user's webcam begins to take various photographs, which are then sent to the program's database for subsequent comparison and analysis with an actual student photo. An alert is sent out if the user is not who he claims to be (Nigam et al., 2021).

7. Streamlining Administrative Processes and Resource Allocation

Some of the most important implications of facial recognition technology in respect to streamlining administrative processes and optimizing resource allocation in education are discussed below.

7.1 Automated Attendance

Facial recognition can automate attendance tracking in classrooms to reduce the administrative burden on teachers and to free up more time for instruction. (Pramod et al., 2023).

7.2 Efficient Resource Allocation

Facial recognition, through attendance and access control, can assist in allocating resources more efficiently for educational institutions, further saving costs and improving resource utilization. (Alam, 2022).

7.3 Security on Campus

Facial recognition can improve the security of the campus by ensuring only authorized individuals are admitted to certain areas. This reduces the number of physical checks by security and improves security in general. (Manimuthu et al., 2022).

7.4 Streamlined Administrative Processes

By streamlining administrative procedures like student registration, enrollment, and library access, facial recognition can make learning more effective and convenient for both staff and students (Siew et al., 2023).

7.5 Personalized Learning Experience

Facial recognition can be used in analyzing the facial expressions and engagement levels of students for inputs to personalize learning experiences and, therefore, improve the learning outcomes of the student. (Jaiswal and Arun, 2021). Facial recognition has the potential to effectively streamline administrative procedures and much more in education by enhancing resources put to use, resulting in a much more efficient and effective environment in which students and educators can learn.

8. Enhancing Student Engagement and Personalizing the Learning Experience

Facial recognition technology in education is one of the ways through which a lot can be done to improve student engagement and make the learning process qualitatively better.

8.1 Emotion Recognition for Engagement Analysis

Analyzing the expressions of students is the ability of face recognition to understand what their emotions are, which can be indicative of engagement. This technology, more popularly known as affective computing, will make it possible for teachers to adapt teaching strategies in real time to better suit the needs of the students, leading to improvement in learning outcomes (Lee et al., 2022).

8.2 Personalized Learning Paths

Personalized Learning Paths: It is through identifying the point at which a student becomes confused or disengaged that educators are able to insert personalized content or support. Such individualized approaches may help to make learning more effective by referring to the individual challenges and strengths that each learner possesses. (Tetzlaff et al., 2021).

8.3 Adaptive Learning Platforms

These platforms can employ facial recognition to modify the hard level of the material or the speed of instruction. For example, if a pupil seems to be tired, the platform might give additional challenging material to re-engage them (Alam, 2022).

8.4 Feedback and Assessment

Beyond traditional assessments, facial recognition can provide immediate feedback by interpreting students' non-verbal cues. This can be particularly useful in large classrooms or online settings where personal interaction is limited (Pabba and Kumar, 2021).

8.5 Enhanced Interaction in Virtual Learning Environments

Facial recognition can bring a new level of interactivity to virtual classrooms. By animating avatars or triggering responses based on students' expressions, the technology can create a more immersive and responsive learning environment (Alam, 2022). While these points emphasize the transformative possibility of facial recognition in learning environment, it's also vital to navigate the ethical concerns such as privacy, consent, and data security. Successful integration into the educational system is dependent on making sure the technology is accountable and transparent. The aim should continuously be to advance the educational experience without compromising the rights and well-being of students.

9. Conclusion

The potential for the integration of AI-based facial authentication in education to augment academic integrity and improve the educational experience is great, especially as education increasingly moves online. This paper discusses the history and technological development of facial recognition, including its accuracy and reliability for biometric authentication. It outlines the issues of online education: the rebirth of sophisticated academic cheating and how AI-based facial authentication will ensure the persons that sit for the assessment are enrolled. Applications are also put forward for facial recognition in campus security to the virtual learning environment, with the need for responsible and transparent implementation so that the privacy and rights of students are properly safeguarded. In a nutshell, AI-based facial authentication promises to provide a safer, more efficient, and personalized educational environment that shall raise the quality and credibility of education in the digital age.

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. https://doi.org/10.3390/electronics9081188

Agarwal, P., Swami, S., and Malhotra, S.K., 2024. Artificial intelligence adoption in the post COVID-19 new-normal and role of smart technologies in transforming business: a review. Journal of Science and Technology Policy Management, 15 (3), Pp. 506-529.

Aggarwal, D., 2023. Integration of innovative technological developments and AI with education for an adaptive learning pedagogy. China Petroleum Processing and Petrochemical Technology, 23 (2), Pp. 709-714. https://doi.org/10.5281/zenodo.7778371

Akram, M., Durrani, G., and Siddique, A.R., 2021. Unriddling academic dishonesty through the lens of teacher and student perceptions. NUST Journal of Social Sciences and Humanities, 7 (1), Pp. 63-77.

Alam, A., 2022. Employing Adaptive Learning and Intelligent Tutoring Robots for Virtual Classrooms and Smart Campuses: Reforming Education in the Age of Artificial Intelligence. In: Shaw, R.N., Das, S., Piuri, V., Bianchini, M. (eds) Advanced Computing and Intelligent Technologies. Lecture Notes in Electrical Engineering, vol 914. Springer, Singapore. https://doi.org/10.1007/978-981-19-2980-9_32

Alua, M.A., Asiedu, N.K., andBumbie-Chi, D.M., 2023. Students' perception on plagiarism and usage of turnitin anti-plagiarism software: the role of the library. Journal of Library Administration, 63 (1), Pp. 119-136.

Andrejevic, M., and Selwyn, N., 2019. Facial recognition technology in schools: critical questions and concerns. Learning, Media and Technology, 45 (1), Pp. 115-128. DOI: 10.1080/17439884.2020.168601.

Asaro, A.K., Sayidah, N., Assagaf, A., Marcelinno, Y.N., Rohimah, S., andJaapar, A., 2023. Fraud Prevention And Detection Through Information Technology: From The Perspective Of Internal Auditor's. In Proceeding of International Conference on Multidisciplinary Research, 1 (1), Pp. 302-324.

Atoum, Y., Chen, L., Liu, A.X., Hsu, S.D.H., and Liu, X., 2017. Automated online exam proctoring. IEEE Transactions on Multimedia, 19 (7), Pp. 1609-1624. https://doi.org/10.1109/TMM.2017.2656064

Betrand, C.U., Chinazo, J., Onyema, M.E., and Benson-Emenike, M., 2023. Authentication system using biometric data for face recognition. International Journal of Sustainable Development Research, 9 (4). https://doi.org/10.11648/j.ijsdr.20230904.12

Bilen, M., and Matros, R., 2021. An Exploratory Study of College Students' Attitudes Toward Cheating and Plagiarism in Online Courses. Journal of the Scholarship of Teaching and Learning, 21 (4), Pp. 44-63.

Boulos, M., 2021. Facial Recognition and Face Mask Detection Using Machine Learning Techniques. Theses, Dissertations and Culminating Projects. https://digitalcommons.montclair.edu/etd/728

Cengiz, E., Yılmaz, C., and Kahraman, H., 2021. Classification of human and vehicles with the deep learning based on transfer learning method. Düzce University Journal of Science and Technology, 9, Pp. 215-225. https://doi.org/10.29130/dubited.842394

Cotton, D.R.E., Cotton, P.A., and Shipway, J.R., 2023. Chatting and cheating: Ensuring academic integrity in the era of ChatGPT. Innovations in Education and Teaching International, 61 (2), Pp. 1-12. https://doi.org/10.1080/14703297.2023.2190148

Deepan, K., Kumar, S.M., Maheswari, M., and Balaji, A.S., 2023. Face recognition system using in attendance for educational institutions. International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), 12 (4). DOI: 10.17148/ IJARCCE.2023.124176.

Dendir, S., and Maxwell, N., 2020. Perspectives on Academic Dishonesty in Online Courses: A Case Study. Journal of Education for Business, 95 (1), Pp. 37-43.

Dewan, M.A.A., Murshed, M., and Lin, F., 2019. Engagement detection in online learning: A review. Smart Learning Environments, 6 (1), Pp. 1. https://doi.org/10.1186/s40561-018-0075-6

Dick, M., Sheard, J., Bareiss, C., Carter, J., Joyce, D., Harding, T.S., and Laxer, C., 2002. Addressing student cheating. ACM SIGCSE Bulletin, 35 (2), Pp. 172-184. DOI: 10.1145/960568.783000.

Dirin, A., and Kauttonen, J., 2020. Comparisons of facial recognition algorithms through a case study application. International Journal of Interactive Mobile Technologies (iJIM), 14 (14), Pp. 121. https://doi.org/10.3991/ijim.v14i14.14997

Gallent Torres, C., Zapata-González, A., and Ortego Hernando, J.L., 2023. The impact of generative artificial intelligence in higher education: A focus on ethics and academic integrity. RELIEVE - RevistaElectrónica de Investigación y EvaluaciónEducativa, 29 (2), Pp. 1-19.

Gamage, K.A., Silva, E.K.D., and Gunawardhana, N., 2020. Online delivery and assessment during COVID-19: Safeguarding academic integrity. Education Sciences, 10 (11), Pp. 301.

González-Salamanca, J.C., Agudelo, O.L., and Salinas, J., 2020. Key competences, education for sustainable development and strategies for the development of 21st century skills: A systematic literature review. Sustainability, 12 (24), Pp. 10366. https://doi.org/10.3390/ su122410366

Haleem, A., Javaid, M., Qadri, M.A., and Suman, R., 2022. Understanding the role of digital technologies in education: A review. Sustainable Operations and Computers. Advance online publication. https://doi.org/10.1016/j.susoc.2022.05.004

Holden, O.L., Norris, M.E., and Kuhlmeier, V.A., 2021. Academic integrity in online assessment: A research review. Frontiers in Education, 6. https://doi.org/10.3389/feduc.2021.639814

Kanakam, T.K., Jubilson, A., Emani, B., Anuhya, M., Sighakolli, S., Chintala, V., and Dhanavanthini, P., 2023. A concise survey on biometric recognition methods. International Journal of Computing and Digital Systems, 14 (1), Pp. 1-1.

Khan, M., Ward, R.D., and Ingleby, M., 2009. Classifying Pretended and Evoked Facial Expressions of Positive and Negative Affective States using Infrared Measurement of Skin Temperature. ACM Transactions on Applied Perception, 6 (1). DOI: 10.1145/1462055.1462061.

Klaib, A.F., Alsrehin, N.O., Melhem, W.Y., Bashtawi, H.O., and Magableh, A.A., 2021. Eye tracking algorithms, techniques, tools, and applications with an emphasis on machine learning and Internet of Things technologies. Expert Systems with Applications, 166, Pp. 114037.

Lee, W., Allessio, D., Rebelsky, W., Satish Gattupalli, S., Yu, H., Arroyo, I., Woolf, B.P., 2022. Measurements and interventions to improve student engagement through facial expression recognition. In International Conference on Human-Computer Interaction (pp. 286-301). Cham: Springer International Publishing.

McCabe, D.L., and Pavela, G., 2004. Ten (updated) principles of academic integrity: How faculty can foster student honesty. Change: The Magazine of Higher Learning, 36 (3), Pp. 10-15. https://doi.org/10.1080/00091380409605574

Mouta, A., Pinto-Llorente, A.M., and Torrecilla-Sánchez, E.M., 2023. Uncovering Blind Spots in Education Ethics: Insights from a Systematic Literature Review on Artificial Intelligence in Education. International Journal of Artificial Intelligence in Education. https://doi.org/10.1007/s40593-023-00384-9

Mulenga, R., and Shilongo, H., 2024. Academic integrity in higher education: Understanding and addressing plagiarism. Acta Pedagogia Asiana, 3 (1). https://doi.org/10.53623/apga.v3i1.337

Ndubuisi, O.J., Adene, G., Sunday, B.T., Mbonu, C.E., and Gift-Adene, A.U., 2024. Digital Criminal Biometric Archives (DICA) and Public Facial Recognition System (FRS) for Nigerian criminal investigation using HAAR cascades classifier technique. World Journal of Advanced Engineering Technology and Sciences, 11 (2), Pp. 029-043.

Nigam, A., Pasricha, R., Singh, T., andChuri, P., 2021. A Systematic Review on AI-based Proctoring Systems: Past, Present and Future. *Education and Information Technologies, 26 (5), Pp. 6421-6445. https://doi.org/10.1007/s10639-021-10597-x

Noorbehbahani, F., Mohammadi, A., andAminazadeh, M., 2022. A systematic review of research on cheating in online exams from 2010 to 2021. Education and Information Technologies, 27 (6), Pp. 8413-8460. https://doi.org/10.1007/s10639-022-10927-7

Noorbehbahani, F., Mohammadi, A., andAminazadeh, M., 2022. A systematic review of research on cheating in online exams from 2010 to 2021. Education and Information Technologies, 27 (6), Pp. 8413-8460.

Ong, S.Z., Connie, T., and Goh, M.K.O., 2023. Cheating detection for online examination using clustering-based approach. JOIV: International Journal on Informatics Visualization, 7 (3-2), Pp. 2075-2085. https://doi.org/10.30630/joiv.7.3-2.2327

Ong, S.Z., Connie, T., and Goh, M.K.O., 2023. Cheating detection for online examination using clustering-based approach. JOIV: International Journal on Informatics Visualization, 7 (3-2), Pp. 2075-2085. https://doi.org/10.30630/joiv.7.3-2.2327

Owayjan, M., Dergham, A., Haber, G., Fakih, N., Hamoush, A., and Abdo, E., 2019. Face Recognition Security System. In New Trends in Networking, Computing, E-learning, Systems Sciences, and Engineering (pp. 343-348). Springer International Publishing. https://doi.org/10.1365/s43439-022-00052-z

Pabba, C., and Kumar, P., 2021. An intelligent system for monitoring students' engagement in large classroom teaching through facial expression recognition. Expert Systems. https://doi.org/10.1111/e xsy.12839

Petrescu, R.V., 2019. Face Recognition as a Biometric Application. SSRN Electronic Journal. https://doi.org/10.2139/SSRN.3417325

Phadke, S., 2013. The importance of a biometric authentication system. SIJ Transactions on Computer Science Engineering and its Applications (CSEA), 1 (4). https://doi.org/10.9756/SIJCSEA/V1I4/0104550402

Qiang, J., Wu, D., Du, H., Zhu, H., Chen, S., and Pan, H., 2022. Review on facial-recognition-based applications in disease diagnosis. Bioengineering (Basel), 9 (7), Pp. 273. https://doi.org/10.3390/bioengineering 9070273

Raja, R., and Nagasubramani, P.C., 2018. Impact of modern technology in education. Journal of Applied and Advanced Research, 3 (S1), Pp. 33. https://doi.org/10.21839/jaar.2018.v3iS1.165

Ralston, S.J., 2021. Ghosting Inside the Machine: Student Cheating, Online Education, and the Omertà of Institutional Liars. Pp. 251–264. https://doi.org/10.1007/978-3-030-72154-1_14

Rodrigues, M.M.M., Silva, R., Borges, A., Franco, M., and Oliveira, C., 2023. Artificial intelligence: threat or asset to academic integrity? A bibliometric analysis. Kybernetes, DOI:10.1108/K-09-2023-1666.

Rooj, S., Routray, A., and Mandal, M.K., 2023. Feature-based analysis of thermal images for emotion recognition. *Engineering Applications of Artificial Intelligence, 120 (1), Pp. 105809. DOI: 10.1016/j.engappai.2022.105809.

Saleem, M., Akram, G., Durrani, A.K., and Siddique, A.R., 2021. Unriddling academic dishonesty through the lens of teacher and student

perceptions. NUST Journal of Social Sciences and Humanities, 7 (1), Pp. 63-77.

Srinivas, T., Aditya Sai, G., and Mahalaxmi, R., 2022. A comprehensive survey of techniques, applications, and challenges in deep learning: A revolution in machine learning. International Journal of Mechanical Engineering, 7 (5), Pp. 286-296.

Tetzlaff, L., Schmiedek, F., and Brod, G., 2021. Developing personalized education: A dynamic framework. Educational Psychology Review, 33, Pp. 863-882. https://doi.org/10.1007/s10648-020-09570-w

Thongkanchorn, K., Suksriupatham, N., Imaromkul, T., Kanchanapreechakorn, S., Wiratsudakul, A., Chuachan, U., and Kusakunniran, W., 2021. Analysing muzzle pattern images as a biometric for cattle identification. *International Journal of Biometrics, 13 (4), Pp. 367. https://doi.org/10.1504/IJBM.2021.10038945

Tucker, A., 2023. The Flexible Face: Unifying the Protocols of Facial Recognition Technologies.

Turani, A.A., Alkhateeb, J.H., andAlsewari, A.A., 2020. Students online exam proctoring: a case study using 360 degree security cameras. In 2020 emerging technology in computing, communication and electronics (ETCCE) (pp. 1-5). IEEE.

Turani, A.A., Alsewari, A.A., and Alkhateeb, J.H., 2021. Students online exam proctoring: A case study using 360 degree security cameras. In 2020 International Conference on Emerging Technology in Computing, Communication and Electronics (ETCCE). IEEE. https://doi.org/10.1109/ETCCE51779.2020.9350872

Ukamaka, B.C., Juliet, O.C., Benson-Emenike, M., and Allswell, K.D., 2023. Authentication system using biometric data for face recognition. International Journal of Sustainable Development Research, 12 (4), Pp. 68-78. https://doi.org/10.11648/j.ijsdr.20230904.12

Utami, D.P.W., and Purnamasari, D.I., 2021. The impact of ethics and fraud pentagon theory on academic fraud behavior. Journal of Business and Information Systems, 3 (1), Pp. 49-59.

Valera, J., Valera, J., and Gelogo, Y., 2015. A Review on Facial Recognition for Online Learning Authentication. In 8th International Conference on Bio-Science and Bio-Technology (BSBT), 16–19. IEEE.

Verganti, R., Vendraminelli, L., andIansiti, M., 2020. Innovation and design in the age of artificial intelligence. Journal of product innovation management, 37 (3), Pp. 212-227.

Verhoef, A.H., and Coetser, Y.M., 2021. Academic integrity of university students during emergency remote online assessment: An exploration of student voices.

Vinutha, D.C., Kavyashree, S., Vijay, C.P., and Raju, G.T., 2022. Innovative Practices in Education Systems Using Artificial Intelligence for Advanced Society. In S. K. Panda, R. K. Mohapatra, S. Panda, and S. Balamurugan (Eds.), *Advances in Intelligent Systems and Computing* (Chapter 16). Wiley. https://doi.org/10.1002/9781119884392.ch16

Yan, W.J., Wu, Q., Chen, Y.H., Liang, J., and Fu, X., 2013. How Fast Are the Leaked Facial Expressions: The Duration of Micro-Expressions. Journal of Nonverbal Behavior, 37 (4). DOI: 10.1007/s10919-013-0159-8.

Yulita, I.N., Hariz, F.A., Suryana, I., andPrabuwono, A.S., 2023. Educational innovation faced with COVID- 19: deep learning for online exam cheating detection. Education Sciences, 13 (2), Pp. 194.

Zamiri, M., and Esmaeili, A., 2024. Methods and technologies for supporting knowledge sharing within learning communities: A systematic literature review. Administrative Sciences, 14 (1), Pp. 17. https://doi.org/10.3390/admsci14010017