ZIBELINE INTERNATIONAL™ PUBLISHING

ISSN: 2590-4043
CODEN: AEMCDV

Acta Electronica Malaysia (AEM)

DOI: http://doi.org/10.26480/aem.02.2024.52.56

CrossMark

RESEARCH ARTICLE

THE ROLE OF MACHINE LEARNING ALGORITHMS IN ENHANCING THE ACCURACY AND THE RELIABILITY OF FACIAL IDENTITY, VERIFICATION IN ONLINE ASSESSMENT

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 22 June 2024
Revised 25 July 2024
Accepted 28 July 2024
Available online 19 August 2024

ABSTRACT

This study scrutinizes exactly how machine learning algorithms can considerably advance the accuracy and reliability of facial identity verification systems used in online examinations. the paper examines how different machine learning (ML) methods are integrated into AI-powered facial recognition systems and assess how well they work to improve accuracy and resilience through a thorough investigation. The algorithms' effectiveness was evaluated in several contexts and the way they might advance safe user authentication in online learning settings. This study shed more light the innovative potential of machine learning in strengthening the safety and integrity of online examinations by examining existing developments and addressing future concerns. Furthermore, we contribute to the discussion around machine learning in learning technology by emphasizing the importance of the underlying further promoting accuracy and reliability. By applying ML technologies, one may achieve a reliable and organized verification process in the digital learning environment (DLE). To wrap up, this study emphasizes the importance of such machine learning achievements as a more reliable and safe ground for online testing. This achievement will contribute to better education and academic activity with regard to the scholarly integrity.

KEYWORDS

machine learning, online examinations, facial recognition, algorithm.

1. INTRODUCTION

Online tests are a popular way for students to convey their knowledge, and online learning environments are gaining more and more importance and necessity at the Higher Education level. In addition, they can also tell a teacher a lot about their students' knowledge and understanding and what they still need help with. Online tests come in different form, but they all provide students with an easy and effective way to show what they know. Currently, most schools use online resources and application forms for student assessment. This is in contrast to traditional pen-and-paper tests that have been in place for a long time. "E-assessment" refers to the technology that is utilized to improve the assessment process. Throughout the course of the evaluation process, technology may be employed at any point or at every stage (Doğan et al., 2020).

The current institutional infrastructure and instructional approach determine where and when to use the technology. Stand-alone e-assessment technologies are used by several universities and training organizations to manage assessment assignments (Mark, 2023). Education practice demonstrates that, for a number of reasons, the integration of assessment within a Learning Management System (LMS) is the most favored method for carrying out e-assessment (Prendes-Espinosa et al., 2021). (1) It is a useful method for structuring the learning process for students in an online setting where e-assessment activities are offered alongside the course materials and assignments as a crucial step in the learning process; (2) It makes it possible to easily evaluate students' knowledge gains with the goal of enhancing them and boosting their motivation to learn; There are many obstacles to overcome in online assessment, including controlling the scalability of exams, preserving academic integrity, and assuring question security. There is a constant need for creative solutions because traditional approaches frequently fail in these domains (Gudiño et al., 2021).

One possible technique to overcoming these difficulties is device learning facial identification and verification. Through using facial reputation algorithms, educational institutions might also installation reliable biometric authentication structures that essentially verify that the character taking the check is, in reality, the authorized scholar. Furthermore, for the duration of exams, machine learning algorithms can interpret behavioral cues and facial expressions to help pick out times of dishonest or other questionable pastime. Also, through limiting get entry to evaluation content based on verified user identities, facial reputation technology can enhance question protection via lowering the possibility of unlawful get entry to or leakage (Jain et al., 2021). These technologies additionally facilitate remote proctoring, which makes it feasible to look at students in actual time at the same time as they take assessments. Periodically, automated structures can verify the identity of students and identify any anomalies or unapproved individuals within the evaluation placing.

In short, the use of machine learning technology for facial recognition and authentication provides a comprehensive approach to improve the accuracy, security, and reach of online tests Educational institutions can leverage these developments to ensure a fair and reliable testing system and maintain academic standards in the digital age (Kaddoura et al., 2022).

2. LITERATURE REVIEW

2.1 Machine Learning Algorithms in Facial Identity Verification

Depending on the output properties, digital image processing algorithms can be categorized into low, mid, and high levels of processing. Image processing methods are used by face recognition systems to identify unique and specific features on a person's face. The capacity of face recognition algorithms to recognize individuals under difficult situations,

Quick Response Code	Access this article online	
	Website: www.actaelectronicamalaysia.com	**DOI:** 10.26480/mecj.02.2024.52.56

Cite The Article: Temitope Oluwafunmilayo Adetunji (2024). The Role of Machine Learning Algorithms in Enhancing the Accuracy and The Reliability of Facial Identity, Verification in Online Assessment. *Acta Electronica Malaysia, 8(2): 52-56.*

such as dim illumination, poor image quality, and an unusual angle of view (a photo shot from above that looks down on an unfamiliar person), varies. It uses machine learning algorithms that locate, pick up, record, and examine face traits in order to compare them with pictures of specific people stored in an already-existing database.

Trace detection, face alignment, feature extraction, face identification, and face verification are the four challenges that a machine must overcome to identify a face. The demand for a biometric security framework has increased recently in order to provide protection against theft, fraud, and other issues. A prominent place has been earned for face recognition among all biometric-based technologies. It may be used for both surveillance and authentication, which establishes a person's identification and helps find them, respectively (Sarkar et al., 2020; Dargan and Kumar 2020; Adjabi et al., 2020).

3. Machine Learning Algorithms

The integrity and security of online searches largely depend on reliable and effective methods of authentication. Face recognition algorithms are important in this field because they provide advanced methods for correctly recognizing people based solely on their visual characteristics these algorithms fall into two categories: approaches based on templates and methods based on geometry. Template-based methods, which are a subset of face recognition algorithms, are developed using statistical tools such as support vector machines (SVM), principal component analysis (PCA), linear discriminant analysis (LDA), kernel approaches, or trace transformation (El et al., 2021). By building templates or facial features and attributes These techniques enable the identification of specific individuals through comparison with stored patterns Because of their accuracy and simplicity, template-based techniques are often used online so search systematically and is particularly good at dealing with differences in appearance (Tretschk et al., 2023).

However, geometry-based object recognition methods investigate local facial features and their geometric relationships. These algorithms, also known as feature-based methods, focus on identifying specific landmarks or face features and estimating their spatial structure High detection rate and fast processing time the popular Viola-Jones algorithm is a widely used geometry-based technique face recognition Occurs Generally, the algorithm consists of four main steps:

- feature selection,
- feature evaluation,
- feature learning to create a classifier,
- cascading classifiers, which collectively contribute to its effectiveness in facial detection tasks (Rusia et al., 2023).

In machine learning, several algorithms have been used to identify faces in online search environments. These include:

1. Eigenface method: A technique based on principal components analysis (PCA) that represents a face image in high dimensional space as a vector and recognizes individuals based on the most important principal features

2. Convolutional Neural Networks (CNNs): Deep learning models precisely made for visual data processing, CNNs have revealedoutstanding performance in face recognition tasks by simply learning hierarchical representations of different facial features on the forest.

3. Support Vector Machines (SVM): Supervised learning algorithm excellent in classification tasks by finding the best hyperplane separating classes in higher dimensions

4. Local Binary Pattern Histogram (LBPH): A texture-based method that captures the local texture patterns of facial images and constructs histograms for classification, delivering high accuracy in face recognition applications.

Each of these machine learning algorithms offers unique strengths and capabilities, making them a valuable tool to increase the accuracy and reliability of facial recognition in online search algorithms the use of these advanced techniques provides educational institutions can establish robust authentication mechanisms and protect the integrity of online research (Kortli et al., 2020).

4. Roles of Machine Learning in Online Assessment

Printing test papers, preparing question papers, ensuring that the right students are taking tests, proctoring (monitoring) tests and taking appropriate actions to prevent misconduct are the basic tasks of implementing the examination system.

4.1 Scheduling Examinations

Printing the test plan or schedule is the first step in the testing process. Machine learning has played an important role in programming since 1980. ML with artificial intelligence is a key component in programming examinations. The ML has already ruled the commercial industries in scheduling, execution, and automation. Now, ML is applied to education, payrolls, generating timetables, and conduction of examinations (Kaddoura et al., 2022). Universities allow students to study concurrently with extra-credit courses, which can lead to standardized testing schedules. It would be difficult to do the setting manually in this overlap. ML has a model capable of self-organizing (Kumar et al., 2020). Advanced strategies with iterative machine learning and optimization techniques will help foolproof online or virtual exams. Neural networks and decision trees play an important role in the process generation of this ML-based model through the iterative evolution method. In the testing process, ML significantly reduces the workload of teachers and researchers (Hutter, KotthoffandVanschoren, 2019).

4.2 Question Paper Generation Precaution

During the exam, students may utilize the internet to look up exam questions and answers using Google or other search engines. In order to deter web browsing, the questions could be reworded and replaced verbatim based on this perspective (Golden andKohlbeck, 2020). Using machine learning to generate randomized multiple-choice questions is an additional technique. To cut down on the number of questions that repeatedly involve cooperative cheating, these questions could be included in the online exam's question paper (Tiongand Lee, 2021).

4.3 Authentication of Students

Before the test, confirming the identification of the student is essential to prevent impersonation. It is possible to use machine learning techniques to verify a student's identification. Multimodal authentication approaches are used to authenticate individuals in certain difficult instances, like twins.

4.4 Proctoring (Supervision) of Examinations

Exam proctoring necessitates ongoing observation and identity verification of the students. Before the test even starts, the student's face is first entered into a database. An ML-based Convolutional Neural Network (CNN) gathers photos for face identification and effectively confirms the student's identity for ongoing face validation (Asepand Bandung, 2019). In order to verify student attendance, the machine learning algorithms take a picture of the student's face throughout the test and compare it with the gathered photos. During online proctoring, this approach is automatic and ongoing (Ghizlane, HichamandReda, 2019). Online exams frequently employ PROCTORU, an ML-based proctoring program.

A student's multiple behavioral shifts can be captured by the ML. The head, hand, andeyes movements are tracked and are created as data points with webcam scanning. Suppose the symptom of mismatch pattern is detected, then immediately sent to theknowledge of the admin to keep close watch the abnormal student behavior safeguardingthe security and integrity of the examination (Slusky, 2020). The ML with computer visionis ideal for face recognition and gesture detection in image processing. Real-time facerecognition is possible by ML in OPENCV proctoring tool. The unsupervised examinationis feasible due to ML (Pandey et al., 2020). The PROCTORIO tool with ML is used for livedetection of human faces with automation. ML also supports the ID verification processduring proctoring examinations. In order to provide greater coverage of the student's surroundings during online proctoring, a 360-degree security camera was suggested.

During an examination, movement is monitored, and sound is recorded. Using machine learning techniques, the security camera and webcam can keep an eye on the students' surroundings (Turani et al., 2020). Both recorded and live proctoring benefit from this technique. In the authentication stage of the inspection process, data analytics is made possible by artificial neural networks that use machine learning. One of machine learning's specialties is its capacity to extract the necessary information from unstructured data and label it, which is then utilized in proctoring tool recognition and detection (Bhardwaj, 2020). In order to provide greater coverage of the student's surroundings during online proctoring, a 360-degree security camera was suggested. During an examination, movement is monitored, and sound is recorded.

Using machine learning techniques, the security camera and webcam can

keep an eye on the students' surroundings (Turani et al., 2020). Both recorded and live proctoring benefit from this technique. In the authentication stage of the inspection process, data analytics is made possible by artificial neural networks that use machine learning. One of machine learning's specialties is its capacity to extract the necessary information from unstructured data and label it, which is then utilized in proctoring tool recognition and detection (Bhardwaj, 2020). Emerging AI technologies impact exam management in a far better way (Vincent-Lancrinand Van der Vlies, 2020). Mathematical and statistical analysis demonstrated that machine learning (ML) proved efficient in maintaining speed and fairness (Wang et al., 2021). The evidence suggests ML and ML-based proctoring is influential and trustworthy in all the revisited cases.

4.5 Fraud or Cheat Detection

Technological developments encourage unsupervised practices and remote proctoring; yet, there is a risk of fraud and cheating when taking the test. The act of cheating on an online evaluation is known as "Academic Dishonesty." Either in-situ or a-posteriori detection can be used to detect cheating. Although location detection is ideal for live proctoring, ANNs and SVMs are often used to provide a posteriori detection (Küppers et al., 2022).

4.5.1 Plagiarism

Students often write notes during examinations. Statistical methods can be used to compare text patterns. Fingerprints and term frequency matrices (TFM) are used to find the columns of words in the rows of the matrices. Although there is some timing associated with this method, the second method of plagiarism detection is based on word-initiation patterns using the Smith-Waterman algorithm-Lewinstein distance. Levenstein distance is used to quantify how much a data string has changed in relation to another data string. These techniques are within the category of structured approaches for data plagiarism detection. Clustering is an unsupervised machine learning technique that can be based on density, graphs, or prototypes; hybrid algorithms are also occasionally used. In the digital tests, the cosine similarity and machine learning techniques with Levenstein distance proved helpful in identifying instances of plagiarism (Anzén, 2022).

4.5.2 Fraud (Malpractice) Detection

The webcam serves as the human eyes in the virtual environment. The web-based supervision has a webcam as the primary input device preventing misconduct during the examination time (Hylton, Levy and Dringus, 2016). The fraud detection ML algorithms initially perform the data cleaning and multiple variable creations. The essential features are selected, and the models are trained to detect the incident of potential fraud occurrence (Wei et al., 2020). The fraud detection module is designed with ML, and the threshold is set to verify fraud occurrence. Multimodal biometric verification with activity analysis is a feature of the module. In order to detect any instances of fraud in online proctoring, the detecting module continuously monitors, gathers data, and takes pictures (Haytom et al., 2020). VFOA (visual focus of attention) refers to head position recognition and gaze tracking using machine learning in in-situ detection. The cheat detection threshold for this model is X. The proctor is alerted to potential cheating and becomes more watchful when the VFOA value is greater than X (Indi et al., 2021).

4.5.3 Multiple Account Detection

Many students create many fictitious profiles in Massive Open Online Courses (MOOCs) in an attempt to get the answer to the question. This issue is resolved by the CAMEO detector, which is based on machine learning. It also identifies the harvester and the master account (Ruipérez-Valiente et al., 2019). Any charges are used to extract the right response, which results in a certificate. (d) Intelligence agent for e-cheating: Machine learning can be integrated into the testing system to identify instances of online cheating. The agent is capable of handling misconduct related to modifications in behavior and Internet protocol. Such academic dishonesty can be detected by the DNN, NN, and LSTM algorithms (Tiongand Lee, 2021).

4.5.4 Liveliness Spoof Detection

A student's liveliness can be used to identify fraud. There are instances where students use pictures or graphics to mimic the liveliness.

4.5.5 Anomaly Detection

Students' test results are subjected to the LSTM algorithm, which compares the results with the students' prior test, assignment, quiz, and other performance metrics results. If a student's final score differs from the predetermined tolerance limit, an anomaly is identified, and if there are scores that are inconsistent, possible cheating or fraud is identified (Santandreu et al., 2021).

4.6 Reliability and Accuracy of Machine Learning in Online Assessment

Facial recognition technology gains more and more tractionevery minute. Furthermore, using facial features and data to identify individuals and set them apart from others is becoming increasingly helpful for various purposes, such as airport security heightened awareness or loss prevention for entertainment venues. Image sharpness, illumination, and shot position are some of the variables that can affect the accuracy of facial recognition technology in the absence of obstacles in the path of clear facial images. The right chipset and camera for your model are essential for accuracy. That said, it is important to understand all of the factors (Adjabi et al., 2020). The accuracy of facial recognition technology can be measured by several key parameters:

- Speed: Speed and ease of use make facial recognition technology popular. Higher FPS can improve performance and accuracy. With the continuous advancement of hardware and chipset technology, there are many device options on the market to meet customers' needs in terms of speed, power, form factor and affordability

- False Recognition (FAR): FAR is the category of cases in which the face recognition system mistakenly recognizes a recognizable face as belonging to the subject. Stated differently, FAR refers to the number of times the system has produced a "false positive". The FAR of a face detection system depends on many variables, e.g.

1. Quality of testing and training face image sets. Lower quality images will produce more false positives.

2. Number of faces in the database. Generally, larger database for lower FAR.

3. Level of specific analyzers.

In general, a highly focused search (such as detecting a particular person's face in a crowd) will result in a higher false alarm ratio (FAR) than a less focused search (such as any person's face).

- False Rejection Rate (FRR): It's vital to understand the feasible inaccuracy of facial popularity era because it gets more broadly used. The fraction of legitimate users that the gadget mistakenly rejects is called the fake rejection price, or FRR, and it serves as one indicator of face recognition accuracy. Numerous variables, together with person participation, face angle, and lights conditions, would possibly impact FRR. Higher FRR systems are normally much less precise than lower FRR structures. The FRR have to be taken into account when choosing a facial recognition device, alongside other accuracy metrics just like the false popularity fee (FAR) and receiver operating characteristic (ROC).

- Face Attributes and Illumination Invariance: Model-based and appearance-based strategies are the two fundamental ways to acquire posture and illumination invariance. Using a 3-D face version, the model-based approach creates photos of the face in diverse lighting fixtures conditions and from diverse angles. The look-based technique uses a set of snap shots that spans quite a few positions and lighting situations rather than a face version.

- Live Face detection in FRS camera: The FRS camera is equipped with artificial intelligence (AI) training technology, which enables it to recognize only live faces. This eliminates the possibility of spoofing and displays high-resolution photographs for identification, thereby mitigating the problem of proxy access.

- Self-Learning: Since the camera is AI-based, it uses its self-learning technology to identify human characteristics on a regular basis and improves detection and recognition accuracy.

- Support for Multiple Analytics: By loading database libraries into the camera or server, the FRS camera may be used for Multipurpose Applications such as VIP recognition, Stranger detection, Loitering detection, Blacklist person detection, etc. and can generate alarms on a real-time basis on the Command Center.

- Analysis of gender and age groups: The quality of the image being studied has a significant impact on the accuracy of facial recognition technologies. It will be more challenging for the software to accurately identify someone if the image is grainy or taken from an

angle that obscures their face. Furthermore, gender analysis may have an impact on how accurate facial recognition software is (Meena et al., 2022; Cao et al., 2021; Alzahrani, 2022).

4.7 Future of Secure User Authentication in E-Learning

Machine learning algorithms can play an important function in figuring out and stopping attempts to bypass facial recognition structures using mask, deep fakes, or other methods. These algorithms can be skilled on diverse datasets containing numerous varieties of spoofing attempts to research patterns indicative of fraudulent conduct.

4.7.1 Spoofing Detection

Biometric authentication methods are still vulnerable to spoofing attacks. The phrase "liveness detection" in biometrics describes a system's ability to ascertain if a face, fingerprint, or other biometric was indeed obtained from a live person present at the moment of capture, or if it was a fake artifact or dead body part. Therefore, we must figure out how to handle spoofing issues that arise during student authentication prior to the online test (Baaqeel and Olusanya, 2022).

4.7.2 Liveness Detection of Face

Facial recognition technology is increasingly being used in applications, such as online test verification and smartphone unlocking. But as this technology becomes more widespread, security becomes a bigger concern, especially when it comes to preventing fake attempts, with uninvited users trying to use faces photos or other tricks to fool the system various methods have been proposed in the academic literature, in particular they emphasize 3D geometric features, texture analysis, and liveness identification (Farrukh et al., 2020).

Methods based on Liveness: The first line of protection in opposition to spoofing assaults in face recognition systems is liveness detection. According to Emphasize the significance of incorporating dynamic physiological signs of existence, inclusive of eye blinking, lip movement, and facial expressions, to differentiate among real faces and static photographs. Blink detection, as an instance, has been widely studied as a reliable method for anti-spoofing protection. By leveraging techniques like eye issue ratio calculation and landmark role tracking, researchers have advanced actual-time systems capable of discerning between open and closed eyes, for this reason improving the system's resilience towards image attacks.

Text-based methods: Text-based methods offer an alternative to counter spoofing in face recognition. For example, Wang *et al* propose the use of physical models to distinguish real faces from face-printed photos based on textural attributes. By analyzing differences in images reflection and estimating noise in images, these methods aim to detect anomalies associated with spoofed images. Furthermore, advances in deep learning have facilitated the development of robust representations that incorporate texture attributes and eye blink cues, providing improved protection against attacks refers to the object

Methods based on 3D geometric: In addition to liveness detection and texture analysis, leveraging three-D geometric functions give a promising way for enhancing the security of face recognition system. By reconstructing the 3D facial shape from 2D pictures and analyzing intensity maps, researchers can distinguish among real faces with a true 3D shape and fause faces with a 2D appearance. Saragih*et al*. Endorse methods that exploit the variations in reconstructed 3D systems between actual faces and planar photographs, thereby imparting a further layer of protection against spoofing assaults (Varshney et al., 2022; Ur Rehman et al., 2023).

5. Continuous Authentication (Dynamic Authentication)

Beyond these methodologies, continuous authentication, also referred to as dynamic authentication, plays an essential role in ensuring the integrity of face recognition systems, mainly within the context of online examinations. Continuous consumer authentication, categorized into physiological, behavioral, and multi-modal biometrics, includes ongoing verification of the consumer's identification at some stage in the examination session. Face recognition, in particular, gives a continuing authentication experience for users, constantly accumulating photos and evaluating them to the base picture saved in the database to verify the person's identity.

6. Continuous Authentication Based on Physiological Biometrics (Face Recognition):

Continuous authentication, classified into physiological, behavioral, and multi-modal biometrics, entails ongoing verification of the person's identity all through the exam session. Face popularity, specifically, offers a seamless authentication revel in for users, continuously gathering pictures and evaluating them to the bottom photo saved in the database to verify the person's identity (Dahia et al., 2020; Kiyani et al., 2020).

7. Conclusion

Machine learning (ML) is now being use in online exams. Online tests are now more secure thanks to face identity verification. Some facial recognition algorithms are even better than humans at recognizing faces. Many professors and students have found that ML-powered online testing systems have made their jobs much simpler. Teachers have benefited from the reduction in the time and effort required to administer and organize exams. They've also profited from the input provided by internet testing tools. Students will be benefited as machine learning methods are more secure and convenient to give tests. In online exams, artificial intelligence still plays a little role. May expect seeing more AI technologies in online exams, to the point where there will be no need for human interaction in the exams.

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.

Anzén, E., 2022. The viability of machine learning models based on levenstein distance and cosine similarity for plagiarism detection in digital exams. Available at http://kth.diva-portal.org/smash/get/diva2:1271998/FULLTEXT02.pdf (accessed on 31March 2022)

Baaqeel, H., and OlusanyaOlatunji, S., 2022. Spoofing detection on adaptive authentication System-A survey. IET Biometrics, 11 (2), Pp. 87-96.

Bhardwaj, R., 2020. Online exam management system using deep learning. InternationalJournal of Creative Research Thoughts, 8, Pp. 4185.

Cao, C., 2021. Holoscopic 3D perception for autonomous vehicles (Doctoral dissertation, Brunel University London).

Dahia, G., Jesus, L., and Pamplona, S.M., 2020. Continuous authentication using biometrics: An advanced review. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 10 (4), Pp. e1365.

Dargan, S., and Kumar, M., 2020. A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. Expert Systems with Applications, 143, Pp. 113114.

Doğan, N., Kıbrıslıoğlu, N., Kelecioğlu, H., and Hambleton, R.K., 2020. An overview of e-assessment. Hacettepe Üniversitesi Eğitim Fakültesi Dergisi, 35 (Special Issue), Pp. 1-5.

Ghizlane, M., Hicham, B., Reda, F.H., 2019. A new model of automatic and con-tinuous online exam monitoring. In: 2019 International Conference on Sys-tems of Collaboration Big Data, Internet of Things and Security (SysCoBIoTS).DOI 10.1109/syscobiots48768.2019.9028027.

Golden, J., Kohlbeck, M., 2020. Addressing cheating when using test bank questions inonline classes. Journal of Accounting Education, 52, Pp. 100671. DOI 10.1016/j.jaccedu.2020.100671.

Gudiño, P.S., Jasso Peña, F.D.J., and de La Fuente Alcazar, J.M., 2021. Remote proctored exams: Integrity assurance in online education?. Distance Education, 42 (2), Pp. 200-218.

Haytom, M., Rosenberger, C., Charrier, C., Zhu, C., Regnier, C., 2020. Identity verification and fraud detection during online exams with a privacy compliant biometric system. In: Proceedings of the 17th international joint conference on e-business and telecommunications. DOI 10.5220/0009874104510458.

Hutter, F., Kotthoff, L., Vanschoren, J., 2019. Automated machine learning. New York:Springer International Publishing DOI 10.1007/978-3-030-05318-5.

Hylton, K., Levy, Y., Dringus, L.P., 2016. Utilizing webcam-based proctoring to determisconduct in online exams. Computers and Education, 92-93, Pp. 53–63. DOI 10.1016/j.compedu.2015.10.002.

Indi, C.S., Pritham, V., Acharya, V., Prakasha, K., 2021. Detection of malpractice in e-examsby head pose and gaze estimation.

International Journal of Emerging Technologies inLearning (iJET), 16 (08), Pp. 47–60. DOI 10.3991/ijet.v16i08.1599.

Jain, A.K., Deb, D., and Engelsma, J.J., 2021. Biometrics: Trust but verify. IEEE Transactions on Biometrics, Behavior, and Identity Science, 4 (3), Pp. 303-323.

Kaddoura, S., Husseiny, F.A., 2021. On-line elarning on information security based on critical thinking andragogy. World Transactions on Engineering and Technology Education, 19 (2), Pp. 157–162.

Kaddoura, S., Popescu, D.E., and Hemanth, J.D., 2022. A systematic review on machine learning models for online learning and examination systems. PeerJ Computer Science, 8, e986.

Kamalov, F., Sulieman, H., SantandreuCalonge, D., 2021. Machine learning basedapproach to exam cheating detection. PLOS ONE, 16 (8), Pp. e0254340. DOI 10.1371/journal.pone.0254340.K

Kiyani, A.T., Lasebae, A., Ali, K., Rehman, M.U., and Haq, B., 2020. Continuous user authentication featuring keystroke dynamics based on robust recurrent confidence model and ensemble learning approach. IEEE Access, 8, Pp. 156177-156189.

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

Küppers, B., Opgen-Rhein, J., Eifert, T., Schroeder, U., 2022. Cheating detection: identifyingfraud in digital exams. Available at https://www.eunis.org/download/2019/EUNIS_2019_paper_52.pdf (accessed on 31 March 2022)

Lu, W., Vivekananda, G.N., Shanthini, A., 2022. Supervision system of English online teaching based on machine learning. In: Progress in artificial intelligence. New York: Springer. DOI 10.1007/s13748-021-00274-y

Marks, A., 2023. Toward Sustainable E-Assessment–Critical Factors. In The 2nd Global Trends in E-Learning Forum (GTEL 2023).

Meena, M.S., Pare, S., Singh, P., Rana, A., and Prasad, M., 2022. A Robust Illumination and Intensity invariant Face Recognition System. International Journal of Circuits, Systems and Signal Processing.

Pandey, A.K., Kumar, S., Rajendran, B., Bindhumadhava, B.S., 2020. e-Parakh: unsupervisedonline examination system. In: 2020 IEEE region 10 conference (TENCON). Piscat-away: IEEE, Pp. 667–671 DOI 10.1109/TENCON50793.2020.9293792.

Prendes-Espinosa, M.P., Gutiérrez-Porlán, I., García-Tudela, P.A., 2021. Collaborative work in higher education: Tools and strategies to implement the e-assessment. Workgroups eassessment: Planning, implementing and analysing frameworks, Pp. 55-84.

Ruipérez-Valiente, J.A., Muñoz Merino, P.J., Alexandron, G., Pritchard, D.E., 2019. Usingmachine learning to detect multiple-account cheating and analyze the influenceof student and problem features. IEEE Transactions on Learning Technologies, 12 (1), Pp. 112–122 DOI 10.1109/TLT.2017.2784420.

Rusia, M.K., and Singh, D.K., 2023. A comprehensive survey on techniques to handle face identity threats: challenges and opportunities. Multimedia Tools and Applications, 82 (2), Pp. 1669-1748.

Sarkar, A., and Singh, B.K., 2020. A review on performance, security and various biometric template protection schemes for biometric authentication systems. Multimedia Tools and Applications, 79 (37), Pp. 27721-27776.

Slusky L., 2020. Cybersecurity of online proctoring systems. Journal of International Technology and Information Management 29:56–83.

Tiong, L.C., Lee, H.J., 2021. E-cheating prevention measures: detection of cheating atonline examinations using deep learning approach—a case study. ArXivpreprint.arXiv:abs/2101.09841.

Tretschk, E., Kairanda, N., BR, M., Dabral, R., Kortylewski, A., Egger, B., Golyanik, V., 2023. State of the Art in Dense Monocular Non-Rigid 3D Reconstruction. In Computer Graphics Forum, 42 (2), Pp. 485-520.

Turani, A.A., Alkhateeb, J.H., Alsewari, A.A., 2020. Students online exam proctoring: a casestudy using 360 degree security cameras. In: 2020 emerging technology in computing, communication and electronics (ETCCE).DOI 10.1109/etcce51779.2020.9350872.

Ur Rehman, A., Belhaouari, S.B., Kabir, M.A., and Khan, A., 2023. On the use of deep learning for video classification. Applied Sciences, 13 (3), Pp. 2007.

Vamsi, M., Ashwin, S., Kajendran Student. 2021. Remote online proctoring system.International Journal of Creative Research Thoughts, 9, Pp. 2320–2882.

Varshney, A., Lamba, S., Garg, P., 2022. A Comprehensive Survey on Event Analysis Using Deep Learning. In 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), Pp. 146-150.

Vincent-Lancrin, S., Van der Vlies, R., 2020. Trustworthy artificial intelligence (AI)in education: promises and challenges. Available at www.oecd-Ilibrary.orgDOI 10.1787/a6c90fa9-en.

Wang, X., Zhang, D., Asthana, A., Asthana, S., Khanna, S., Verma, C.S., 2021. Design of Englishhierarchical online test system based on machine learning. Journal of Intelligent Systems, 30, Pp. 793–807. DOI 10.1515/jisys-2020-0150.

Wei, Y., Qi, Y., Ma, Q., Liu, Z., Shen, C., Fang, C., 2020. Fraud detection by machine learning.In: 2020 2nd international conference on machine learning, big data and business intel-ligence (MLBDBI). Piscataway: IEEE, Pp. 101–115 DOI 10.1109/MLBDBI51377.2020.00025.