Student Occasional Paper Series No. 2 | July 2023

Analyzing Anti-Cheating Gaze-Tracking Programs

By Sebastian Bukvic and Charles Zhao | Edited by Aaron Brantly

Abstract

This analysis examines eye gaze-tracking technology, techniques, and usages in academic institutions to enforce integrity, and explores any privacy concerns that may constitute ethics violations. Before delving into the ethics of tracking technologies, this research focuses first on how eye gaze-tracking technologies function and have been developed. Following an examination of the technical attributes of this technology the analysis subsequently discusses its applications in academic environments. This is critical as circumstances such as the COVID-19 pandemic and its associated lockdowns have transformed the modality of classroom environments for different schools and universities to a virtual medium. Through these virtual classroom environments, cheating during assignments and tests has become more prevalent. As a result, measures to combat this have been integrated, such as a video recording of students to track their eyesight during exams. Eye gaze-tracking measures such as the one mentioned above have been scrutinized for issues with ethics, privacy, and legality, as these measures are often very invasive to one's privacy when enacted. The work concludes with an analysis of its implications on users' privacy.

Introduction

In the 21st century, it is evident that virtual modalities for class environments are becoming more commonplace. This can be attributed to circumstances such as the COVID-19 pandemic and its associated lockdowns or simply for ease of access in different university environments when people cannot always be present. As with the increase of virtual modalities for lectures, people found ways to exploit this through cheating during assignments and tests. To combat these issues, different software and programs were created with the purpose of providing anti-cheating mechanisms through eye gaze tracking. The analysis in this paper examines gaze-tracking technology, techniques, and usages in academic institutions to enforce integrity, and explores any privacy concerns that may constitute ethics violations. Before delving into the ethics of tracking technologies the next section begins by looking at how gaze-tracking technology works. Following an examination of the technical attributes of the technology the analysis subsequently discusses its applications in academic environments. Finally, the work concludes with an analysis of its implications on users' privacy.

Defining Eye Gaze-Tracking and Its Applications

Eye gaze-tracking is a technique in which an individual's eye movements are measured and analyzed so that a program or person may know where the individual is looking, what the individual is looking at, and in some more advanced eye gaze-tracking algorithms, what emotions the individual may be displaying through his eye movement and facial expressions. Vision through the human eye constitutes a critical sense. The ability to track a subject's eye movements in different applications can provide critical understanding of potential motives and emotions. Applications of eye gaze-tracking are increasingly common and occur in classroom and testing environments via virtual modalities, however, one's eye signature is completely unique to themselves, as in the case of a fingerprint, and there are many different systems that use eye gaze-tracking in security settings. As aforementioned, eye gaze-tracking has received more media and public attention recently due to its usage, albeit not widespread usage, in the proctoring of exams in virtual environments. As this technology advances, more applications will become available.

Historical Practices of Eye Tracking

Modern eye gaze-tracking techniques would not be possible without multiple studies of the eye throughout history, more specifically studies of the eye anatomy by Johannes Kepler in the seventeenth century.[1] Throughout this period, Christoph Scheiner is considered to have formulated the first forms of eye gaze-tracking through tests of the pupil to different stimuli.[2] Through the work by Christoph Scheiner and Johannes Kepler we now understand that "if you stand a person in bright sunlight and observe their pupil, you will see that the pupil constricts, decreasing in size. Whereas if you move them into a darker area with less light, the pupil will dilate, becoming larger again, demonstrating the reactivity of the pupil to light."[3] In the nineteenth century studies of the eye advanced to the point where researchers formulated

crude instruments for recording eye movements, often through tools attached to the eye; while these tools for recording eye movements were crude by most standards, they established a basic methodology for modern eye tracking studies.

The twentieth century was critical for the development of eye tracking technologies, as the biggest strides in eye tracking research occurred within that time period. Eye tracking methods moved towards more objective sources and less invasive forms of recording data as photographic methods became the primary source for the collection of eye data. Early eye gaze-tracking devices and systems in the twentieth century "relied on electrodes mounted on the skin around the eye that could measure differences in electric potential so as to detect eye movements" while others "required the wearing of large contact lenses that covered the cornea and sclera."[4] However, today even primitive forms of eye tracking can use a simple laptop web camera to track the eyesight of an individual.

How Eye Gaze-Tracking Functions

As mentioned by Stuart in his book Eye Tracking Backgrounds, Methods, and Applications, there are a few types of gaze-tracking methods: video/photo/laser-based, electro-oculography, and scleral search coils.[5] In this paper, we focus on video-based gaze tracking as it is the least invasive method as well as the simplest to use, making it the primary method used for detecting cheating. Additionally, according to Papoutsaki, in more recent times, technological advances have allowed the use of webcams and offline software to produce acceptable results in eye-tracking, making video-based gaze-tracking the cheapest method.[6] Video-based gaze-tracking primarily utilizes infrared or near-infrared light to illuminate the pupil and then records the reflection of the light off of the cornea with an infrared camera to map out the structure of the eye, finding the center of the pupil, and tracking eye rotation as well as gaze direction. The following image from Redline and Lankford's 2001 study titled Eye-movement analysis: A new tool for evaluating the design of visually administered instruments shows the change in the position of the reflection on the cornea as a person's gaze shifts.

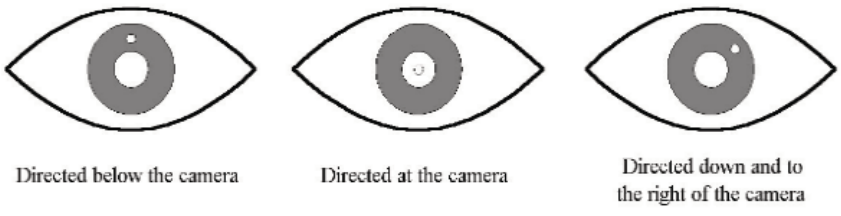

Figure 1: Eye Movement Analysis from Redline and Lankford 2001.

To determine what the user is looking at on the screen, calibration is needed. This calibration is usually in the form of fixed points on the screen that the user must look at. An example can be seen in the following image.

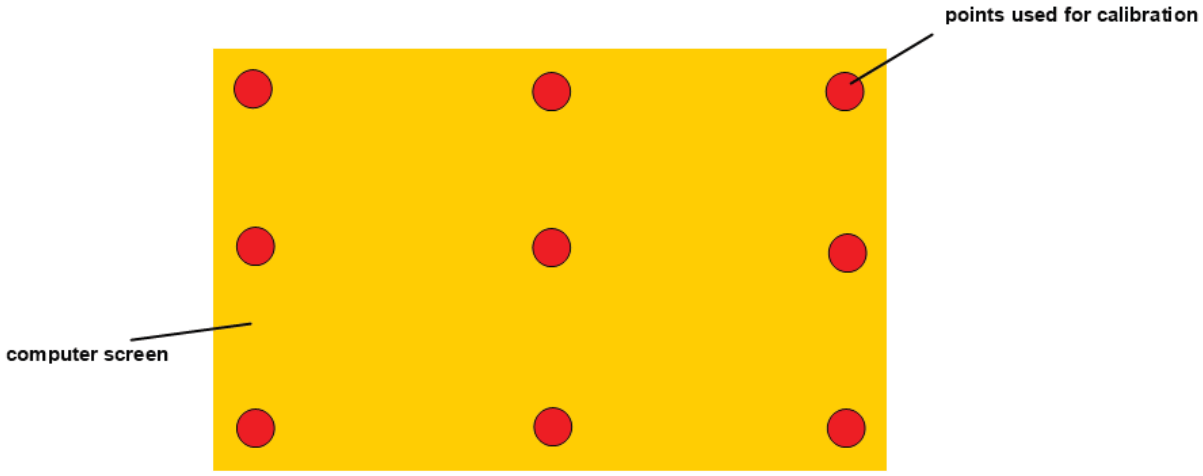

Figure 2: Gaze Training Screen

The above image demonstrates the calibration method used in a browser-based gaze-tracking plugin called E-Proctor, which uses the webcam of a laptop to perform video-based gaze-tracking. There are nine points on the screen to determine the x and y coordinates and the edges. After calibration, the data from tracking eye movements can be used to determine when the user looks off the screen or precisely where on the screen the user is looking. For example, the plugin can detect when a student tries to sneakily look off the computer screen at a source of unauthorized assistance. In the case of E-Proctor, the monitoring is live and constant, meaning upon the start of the online examination, it conducts continuous proctoring to detect any instance of suspicious behavior. In some instances, the tracking is not done in real-time but rather captured first and then used later. In either case, the data that is collected is sent to a back-end server for processing to check for odd activities.

Applications of Eye Tracking in Cheating Detection and Academic Settings

The implementation of eye tracking technology for the detection of cheating is currently primarily observed within academic institutions. With the onset of the COVID-19 pandemic, schools and universities swiftly pivoted towards remote learning environments in order to ensure the safety of students and staff. This shift has consequently led to the administration of online examinations, which has prompted the exploration of novel approaches to prevent academic

misconduct. In this context, the utilization of eye tracking for the purpose of detecting cheating has emerged as a promising solution. Specifically, the ability to monitor and analyze students' ocular movements during online assessments presents a unique opportunity to identify and mitigate instances of cheating, thereby promoting the integrity and fairness of the evaluation process.

Hence, academic organizations have incorporated anti-cheating measures such as requiring the usage of monitoring tools such as ProctorU and Proctorio during online exams.[7] At the Virginia Tech, some professors use software that does something similar known as a lockdown browser, which is an application that acts as a special web browser with certain restrictions designed to prevent cheating. The application used by professors at Virginia Tech and many other institutions is simply called LockDown Browser, made by a software company called Respondus.

According to Respondus' website, the first version of Respondus came out in 2015 for Windows, and in 2016 for Mac. The software was initially conceived as a browser application to curtail users' ability to switch to other concurrently running applications on their computer. However, Respondus has since undergone significant development, adding a new service called Respondus Monitor, which builds on top of the LockDown Browser, encompassing more robust methods for detecting and preventing academic dishonesty. The Respondus Monitor incorporates multifaceted protocols that capture audio and video data through the user's device throughout the duration of the examination. Respondus Monitor shares one common feature with the monitoring tools mentioned above: the utilization of webcams to watch the student and pick up any suspicious activity. While some do this by using a person to act as a proctor by watching the video feed generated via the webcam, others use automated tools including eye tracking. Respondus Monitor in particular says the "webcam recording itself goes through an automated "post-processing" step that utilizes computer vision technology to determine: whether the student remained in the video frame, if multiple people appear in the video frame, if the person in the video frame differs from the person who started the exam, and the position of the user's face relative to the webcam recording device".[8] To detect if the person differs throughout the exam session, Respondus claims to use a "creation of a temporary template of facial features during automated processing" that is then used "either by the server executing the Respondus Monitor software or by the automated processing" that occurs on the user's device.[9] Although it is unclear whether the "template of facial features" include the eyes, it is a likely possibility that even if it does not as of now, it will be implemented in the future to further increase the effectiveness of the Respondus Monitor.

Ethics, Legality, and Privacy Issues of Eye Tracking

As with any technology today, we must consider any implications on ethics, legality, and privacy. With the development of more advanced technology, privacy concerns have increased accordingly, as these newer technologies have more capabilities for different forms of data collection. In today's age common devices such as phones, laptops, and smart watches have the capabilities for collecting data through cameras, voice recognition, and more rudimentary forms, such as the collection of personal information in the case of credit cards, passwords, personal data, and chat logs, as well as even social security numbers that may be stored on the system. Most of these data privacy concerns are known to the general public and have been known since the introduction of smart technologies, however, concerns with eye-gaze tracking and its associated data collection have been more prevalent in recent history than years prior. To preface, humans use eye contact as a form of communication and a way to show interest in varying social circumstances. Regarding physical attributes, the age of a user can be approximated using scan paths, that study the retina of the eye through machine-based learning techniques. Furthermore, the figure below depicts the variety of attributes that eye tracking data collection can show about a person.[10]

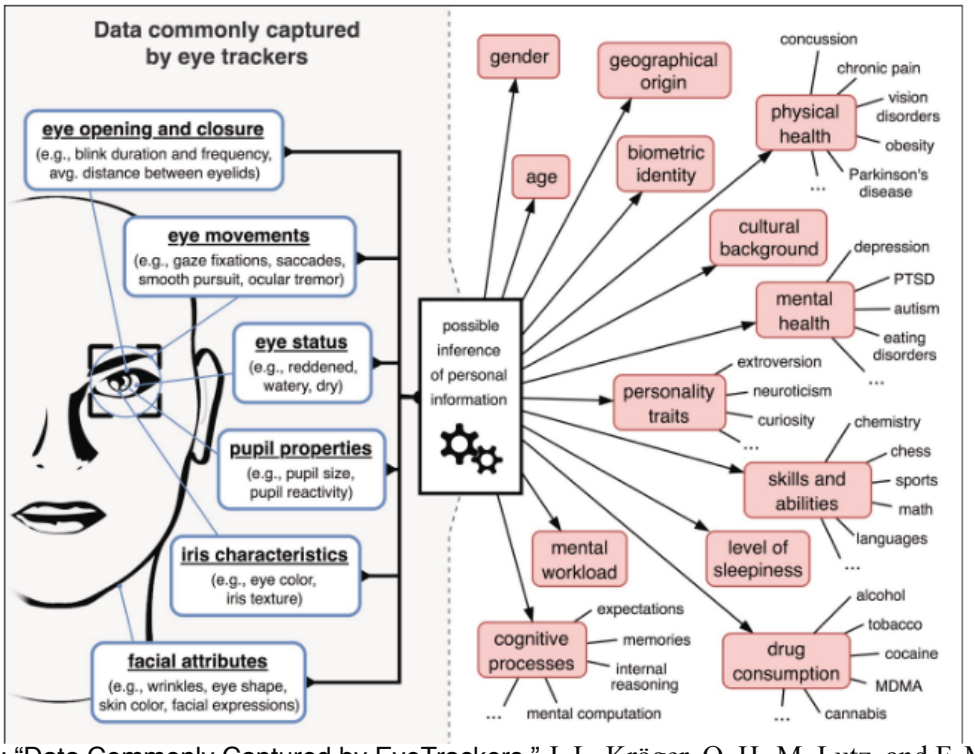

Figure 3: "Data Commonly Captured by EyeTrackers." J. L. Kröger, O. H.-M. Lutz, and F. Müller, "What does your gaze reveal about you? on the privacy implications of Eye Tracking," Privacy and Identity Management. Data for Better Living: AI and Privacy, pp. 226–241, 2020.

With the amount of information that can be extrapolated from data collection of the eye, one can reveal more about oneself than they deem to be within their consent. Machine based learning techniques through eye gaze-tracking can display a person's personal ailments, thought-processes, and personal information that may reach far beyond the purpose of the eye tracking system; if an anti-cheating eye tracking software is being used in an academic setting with the primary purpose of honest test-taking, the software may go above and beyond its primary goal and could have the ability to gather personal data about the person behind the computer screen which already poses multiple privacy and ethical concerns.

Further ethical concerns arise when people who use the anti-cheating eye tracking software are deceived about the nature of the data being collected or even coerced in sharing more facial recognition and eye data than they may understand. When anti-cheating software systems are strictly enforced by academic institutions, a student cannot simply refuse to complete an assignment or test without the anti-cheating software, they must rather agree to the terms and conditions of the software blindly to prevent undermining their grades and/or academic standing. Critical privacy concerns are evident when the fact that some anti-cheating software systems collect the eye tracking and facial recognition data, store it, and have it available for proctoring even when the assignment or exam is complete. If there were to be a data breach concerning the company behind an anti-cheating system, it could jeopardize the privacy of persons involved, especially the privacy surrounding critical personal information such as any data collected about a subject's eyes and face. Furthermore, if the data of a subject's face and eyes is exposed to the internet, it would be considerably easier for people to harm the subject's image and public standing through deepfake technology.

To address the legal concerns that anti-cheating eye tracking may pose, data collected through these systems must be secure and follow all data protection laws and policies as well as copyright laws. Any participants in assignments or exams proctored by these anti-cheating technologies should know fully the procedures of these technologies and explicitly give consent to share their facial data. In addition, any data collected must follow all data protection laws and procedures to prevent jeopardizing personal information about a user. To achieve this, the data collected must be securely stored and not sold or shared with third parties, which is a practice that often occurs. In the case of collected eye tracking data that may be considered intellectual property, the data must follow all copyright and patent laws that may be involved. The issue with upholding rules in academic settings resolves back to a lack of understanding of the risks posed by these programs. Instructors will often blindly choose a program that meets their proctoring

requirements without knowing the risks to the students involved. Students will often consent to being monitored as they rarely have options outside of continuously monitored assignment and test completion. Professors should offer clear alternative, less invasive, means of taking tests as an option available for individuals uncomfortable with using gaze tracking software.

Conclusion

Currently, anti-cheating eye gaze-tracking proctoring programs are seen in most virtual academic settings in the USA, especially in universities, as well as in many foreign countries. Due to the prevalence of proctoring systems, multiple concerns have been raised regarding the ethics, legality, and privacy of these systems. A majority of these systems were created to fill in a role brought about by the change of teaching in-person to teaching in a virtual classroom environment during COVID-19, many of the concerns raised were insufficiently considered or entirely overlooked. Eye tracking proctoring programs could provide a more honest academic process for many teachers and students alike, however, the question of ethics lingers. This research analysis provides the basis for further consideration of these programs and what issues could and should be resolved to make these proctoring systems more viable for mass usage in the future.

Endnotes

1 Simon G (1975) 14.3. On the theory of visual perception of Kepler and Descartes: reflections on the role of mechanism in the birth of modern science. Vistas Astron 18:825–832. https://doi.org/10.1016/0083-6656(75)90174-9

2 Daxecker F (1992) Christoph Scheiner's eye studies. Doc Ophthalmol 81(1):27–35. https://doi.org/10.1007/BF00155011

3 Gal O, Chen-Morris R (2010) Baroque optics and the disappearance of the observer: from Kepler's optics to Descartes' doubt. J Hist Ideas 71(2):191–217

4 Poole, Alex, and Linden J. Ball. "Eye Tracking in HCI and Usability Research." *Encyclopedia of Human Computer Interaction*, January 2006, 211–19. https://doi.org/10.4018/978-1-59140-562-7.ch034.

5 S. Stuart, Eye tracking: Background, methods, and applications. New York, NY: Humana Press, 2022.

6 A. Papoutsaki, "Scalable webcam eye tracking by learning from user interactions," Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems, 2015.

7 D. Harwell, "Mass school closures in the wake of the coronavirus are driving a new wave of student surveillance," The Washington Post, 03-Apr-2020. [Online]. Available: https://www.washingtonpost.com/technology/2020/04/01/online-proctoring-college-exams-coronavirus/. [Accessed: 25-Apr-2023].

8 Additional privacy information - respondus monitor," *Respondus*, 30-Mar-2023. [Online]. Available: https://web.respondus.com/privacy/privacy-additional-monitor/#:~:text=Respondus%20Monitor%20continually%20tracks%20the,device%20during%20an%20exam%20session. [Accessed: 26-Apr-2023].

9 Ibid.

10 J. L. Kröger, O. H.-M. Lutz, and F. Müller, "What does your gaze reveal about you? on the privacy implications of Eye Tracking," Privacy and Identity Management. Data for Better Living: AI and Privacy, pp. 226–241, 2020.

Bibliography

Redline, C. D., & Lankford, C. P. (2001). Eye-movement analysis: A new tool for evaluating the design of visually administered instruments (paper and web). In Proceedings of the Section on Survey Research Methods of the American Statistical Association

J. L. Kröger, O. H.-M. Lutz, and F. Müller, "What does your gaze reveal about you? on the privacy implications of Eye Tracking," Privacy and Identity Management. Data for Better Living: AI and Privacy, pp. 226–241, 2020.

S. Stuart, Eye tracking: Background, methods, and applications. New York, NY: Humana Press, 2022.

A. Papoutsaki, "Scalable webcam eye tracking by learning from user interactions," Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems, 2015.

D. Harwell, "Mass school closures in the wake of the coronavirus are driving a new wave of student surveillance," The Washington Post, 03-Apr-2020. [Online]. Available: https://www.washingtonpost.com/technology/2020/04/01/online-proctoring-college-exams-coronavirus/. [Accessed: 25-Apr-2023].

T. Ujbanyi, J. Katona, G. Sziladi, and A. Kovari, "Eye-tracking analysis of computer networks exam question besides different skilled groups," 2016 7th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), 2016.

Byun, Jeongmin, Jungkook Park, and Alice Oh. "Detecting Contract Cheaters in Online Programming Classes with Keystroke Dynamics." *Proceedings of the Seventh ACM Conference on Learning @ Scale*, August 12, 2020. https://doi.org/10.1145/3386527.3406726.

Coghlan, Simon, Tim Miller, and Jeannie Paterson. "Good Proctor or 'Big Brother'? Ethics of Online Exam Supervision Technologies." *Philosophy & Technology* 34, no. 4 (August 31, 2021): 1581–1606. https://doi.org/10.1007/s13347-021-00476-1.

Corrigan-Gibbs, Henry, Nakull Gupta, Curtis Northcutt, Edward Cutrell, and William Thies. "Deterring Cheating in Online Environments." *ACM Transactions on Computer-Human Interaction* 22, no. 6 (September 24, 2015): 1–23. https://doi.org/10.1145/2810239.

David-John, Brendan, Diane Hosfelt, Kevin Butler, and Eakta Jain. "A Privacy-Preserving Approach to Streaming Eye-Tracking Data." *IEEE Transactions on Visualization and Computer Graphics* 27, no. 5 (March 22, 2021): 2555–65. https://doi.org/10.1109/tvcg.2021.3067787.

Dilini, Nimesha, Asara Senaratne, Tharindu Yasarathna, Nalin Warnajith, and Leelanga Seneviratne. "Cheating Detection in Browser-Based Online Exams through Eye Gaze Tracking." *2021 6th International Conference on Information Technology Research (ICITR)*, December 1, 2021. https://doi.org/10.1109/icitr54349.2021.9657277.

Essahraui, Siham, Mohammed Amine El Mrabet, Mouncef Filali Bouami, Khalid El Makkaoui, and Ahmed Faize. "An Intelligent Anti-Cheating Model in Education Exams." *2022 5th International Conference on Advanced Communication Technologies and Networking (CommNet)*, December 12, 2022. https://doi.org/10.1109/commnet56067.2022.9993953.

EYEWARE Editors. "Understanding Eye Tracking & How It Can Work For You: Definitions ..." eyeware. Eyeware Tech SA, March 3, 2022. https://eyeware.tech/en_ca/blog/what-is-eye-tracking/.

Hausfeld, J., K. von Hesler, and S. Goldlücke. "Strategic Gaze: An Interactive Eye-Tracking Study." *Experimental Economics* 24, no. 1 (May 4, 2020): 177–205. https://doi.org/10.1007/s10683-020-09655-x.

Kariyawasam, Samadhi, Anjana Lakshan, Anuranaga Liyanage, Kaveesha Gimhana, Vijani Piyawardana, and Yashas Mallawarachchi. "Standalone Application and Chromium Browser Extension-Based System for Online Examination Cheating Detection." *2021 3rd International Conference on Advancements in Computing (ICAC)*, December 9, 2021. https://doi.org/10.1109/icac54203.2021.9671103.

Kröger, Jacob Leon, Otto Hans-Martin Lutz, and Florian Müller. "What Does Your Gaze Reveal about You? on the Privacy Implications of Eye Tracking." *Privacy and Identity Management. Data for Better Living: AI and Privacy*, March 6, 2020, 226–41. https://doi.org/10.1007/978-3-030-42504-3_15.

Liebling, Daniel J., and Sören Preibusch. "Privacy Considerations for a Pervasive Eye Tracking World." *Proceedings of the 2014 ACM International Joint Conference on Pervasive and*

Ubiquitous Computing: Adjunct Publication, September 13, 2014. https://doi.org/10.1145/2638728.2641688.

Maniar, Sarthak, Krish Sukhani, Krushna Shah, and Sudhir Dhage. "Automated Proctoring System Using Computer Vision Techniques." *2021 International Conference on System, Computation, Automation and Networking (ICSCAN)*, July 30, 2021. https://doi.org/10.1109/icscan53069.2021.9526411.

Oravec, Jo Ann. "Ai, Biometric Analysis, and Emerging Cheating Detection Systems: The Engineering of Academic Integrity?" *Education Policy Analysis Archives* 30 (December 6, 2022). https://doi.org/10.14507/epaa.30.5765.

Ozdamli, Fezile, Aayat Aljarrah, Damla Karagozlu, and Mustafa Ababneh. "Facial Recognition System to Detect Student Emotions and Cheating in Distance Learning." *Sustainability* 14, no. 20 (October 14, 2022): 13230. https://doi.org/10.3390/su142013230.

Ozgen, Azmi Can, Mahiye Uluyagmur Ozturk, Orkun Torun, Jianguo Yang, and Mehmet Zahit Alparslan. "Cheating Detection Pipeline for Online Interviews." *2021 29th Signal Processing and Communications Applications Conference (SIU)*, June 9, 2021. https://doi.org/10.1109/siu53274.2021.9477950.

Pleasants, Jacob, John M Pleasants, and Barbara Pleasants. "Cheating on Unproctored Online Exams: Prevalence, Mitigation Measures, and Effects on Exam Performance." *Online Learning* 26, no. 1 (2022). https://doi.org/10.24059/olj.v26i1.2620.

Poole, Alex, and Linden J. Ball. "Eye Tracking in HCI and Usability Research." *Encyclopedia of Human Computer Interaction*, January 2006, 211–19. https://doi.org/10.4018/978-1-59140-562-7.ch034.

Rodriguez, M. Elena, Ana-Elena Guerrero-Roldan, David Baneres, and Ingrid Noguera. "Students' Perceptions of and Behaviors toward Cheating in Online Education." *IEEE Revista Iberoamericana de Tecnologias del Aprendizaje* 16, no. 2 (May 2021): 134–42. https://doi.org/10.1109/rita.2021.3089925.