Detection of contract cheating in pen-and-paper exams through the analysis of handwriting style

Konstantin Kuznetsov
konstantin.kuznetsov@dfki.com
German Research Center for Artificial Intelligence (DFKI)
Saarbrücken, Germany

Michael Barz
michael.barz@dfki.de
German Research Center for Artificial Intelligence (DFKI)
Saarbrücken, Germany
University of Oldenburg
Oldenburg, Germany

Daniel Sonntag
daniel.sonntag@dfki.de
German Research Center for Artificial Intelligence (DFKI)
Saarbrücken, Germany
University of Oldenburg
Oldenburg, Germany

ABSTRACT

Contract cheating, i.e., when a student employs another person to participate in an exam, appears to become a growing problem in academia. Cases of paid test takers are repeatedly reported in the media, but the number of unreported cases is unclear. Proctoring systems as a countermeasure are typically not appreciated by students and teachers because they may violate the students' privacy and can be imprecise and nontransparent. In this work, we propose to use automatic handwriting analysis based on digital ballpoint pens to identify individuals during exams unobtrusively. We implement a system that enables continuous authentication of the user during exams. We use a deep neural network architecture to model a user's handwriting style. An evaluation based on the large Deepwriting dataset shows that our system can successfully differentiate between the handwriting styles of different authors and hence detect simulated cases of contract cheating. In addition, we conducted a small validation study using digital ballpoint pens to assess the system's reliability in a more realistic environment.

CCS CONCEPTS

• **Applied computing** → **Education**; • **Human-centered computing**; • **Security and privacy** → *Security services*;

KEYWORDS

Digital Pens; Contract Cheating; Proctoring Solutions; Writer Identification

ACM Reference Format:
Konstantin Kuznetsov, Michael Barz, and Daniel Sonntag. 2023. Detection of contract cheating in pen-and-paper exams through the analysis of handwriting style. In *INTERNATIONAL CONFERENCE ON MULTIMODAL INTERACTION (ICMI '23 Companion), October 9–13, 2023, Paris, France.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3610661.3617162

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
ICMI '23 Companion, October 9–13, 2023, Paris, France
© 2023 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 979-8-4007-0321-8/23/10…$15.00
https://doi.org/10.1145/3610661.3617162

1 INTRODUCTION

In contract cheating [Clarke and Lancaster 2006], students ask another person to do an assignment or to take an exam instead of them (impersonation attack [Holden et al. 2021]). Contract cheating is a significant and growing problem, receiving much media coverage. For instance, SBS News investigated exam impersonators and uncovered individuals allegedly paid to take multiple personal exams at universities in Australia [Potaka and Huang 2015]. Amigud [Amigud and Lancaster 2020] found that students are willing to pay up to $200 for an exam. Specialized websites offer respective services coming from all over the world. However, the market size is hard to estimate, as the imposters mostly remain unrecognized. Usually, universities perform a simple visual check to ensure that the photo on a personal ID card matches the person taking part in the exam [Moten Jr et al. 2013]. As one impersonator explained, making a fake student card is simple by swapping the student's photo with his own. More sophisticated authentication methods involve biometric data like fingerprints [Levy and Ramim 2007], eye-tracking [Bawarith et al. 2017], eye vein scans [Kigwana and Venter 2016], voice and keystroke biometrics [Norris 2019], and combinations of them [Sabbah 2017]. The proliferation of e-learning and digital technologies, especially during the COVID-19 pandemic, opened up new opportunities for cheating [Amigud and Lancaster 2019]. In many cases, students can take exams at home by logging into a learning platform and authenticating through their login credentials. This method is prone to various attacks, including credential sharing [Dobrovska 2017] and remote desktop access by a third party [Duncan and Joyner 2022; Von Gruenigen et al. 2018]. Lancaster [Lancaster and Clarke 2017] suggests that online courses are particularly susceptible to impersonation cheating. Digital onsite exams, taken using private devices, also cannot offer a sufficient level of control, as it can be easy to beat any restrictions by additional software and devices [Dawson 2016; Sindre and Vegendla 2015]. Verifying the test-taker's identity before and during an exam is essential, especially in remote learning settings. To monitor exams, both online and offline, a range of proctoring solutions has been introduced over the last years, including research approaches [Alessio and Maurer 2018; Hussein et al. 2020] and commercial products, among them Respondus (https://respondus.com), Proctorio (https://proctorio.com), and ProctorU (https://www.proctoru.com) being the most popular [Balash et al. 2021]. Proctoring solutions include surveillance tools that track head and eye movements, mouse

clicks, and other metrics to identify suspicious behavior. They extensively use video monitoring to control students. However, video monitoring is not only prone to false alarms (e.g., due to the racial bias [Teninbaum 2021]), imposing additional stress on students, but also doubtful in terms of students' privacy and personal rights [Balash et al. 2021; Nigam et al. 2021]. Despite their popularity, the academic community started criticizing such proctoring solutions, casting doubt on their efficacy and cautioning against privacy issues and an increased potential for technical issues [Goldberg 2021; Morrison and Heilweil 2020a]. Moreover, some institutions discontinued remote-proctoring software, claiming its discriminatory nature, lack of data protection, and a gross invasion of privacy [Chin 2021; Morrison and Heilweil 2020b]. Along with various face recognition techniques [Aisyah et al. 2018; Arnautovski 2019; Ghizlane et al. 2019; Idemudia et al. 2016; Joshy et al. 2018; Raj et al. 2015; Sinha et al. 2020], researchers explored more privacy-friendly approaches based on the student's personal information about the academic results and location [SMIRANI and BOULAHIA 2022], dynamic profile questions [Norris 2019], and keystroke dynamics and stylometry [Brocardo et al. 2019; Canales et al. 2011; Ison 2020; Monaco et al. 2013], each with its strengths and weaknesses. There is a need to explore additional modalities for exam proctoring, which will reduce the possibility of contract cheating and student impersonation while remaining convenient and privacy-preserving.

We investigate if digital pen input can be reliably used as an alternative modality to prevent contract cheating during online and offline paper-based exams. We propose a new method for continuous user authentication based on identifying the user's handwriting, which is assumed to be individual [Srihari et al. 2002]. On the one hand, the inter-writer variability allows us to distinguish the unique styles of different writers, especially for the same text. On the other hand, a lot of intra-variability makes it challenging to identify the authorship of random writing, as its appearance can be strongly influenced by its content. To capture the uniqueness of the handwriting, we resort to a neural network architecture capable of disentangling style from content and projecting it into a latent space. Given two handwriting samples, we use their style encodings to calculate their dissimilarity score and decide if they belong to the same writer. We developed a prototype to record user input using a digital pen and continuously authenticate the writer. The proposed system aims at preventing impersonation cheating. It can be used as a privacy-friendly modality to enforce control over students during online and offline paper-based exams. We evaluate the performance of the approach using the *DeepWriting* dataset, an extension of the IAM-OnDB dataset [Liwicki and Bunke 2005], and assess its efficacy and utility in a more realistic setting via a preliminary validation study with seven participants.

2 METHOD

Handwriting conveys semantic information, but its appearance is also expressive. For instance, stroke features have been successfully used to predict domain expertise [Oviatt et al. 2018] and cognitive performance [Barz et al. 2020; Prange and Sonntag 2022]. We expect that a stroke's style can also capture the author's identity. Continuous authentication by handwriting analysis can be considered as

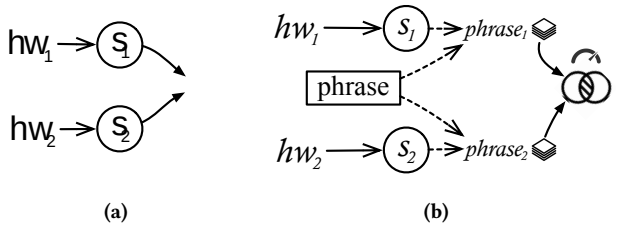

Figure 1: The overview of our comparison models. (a) The similarity is calculated between the encoded styles. (b) Handwritings with the same content *phrase* are synthesized using extracted styles; then, the similarity is calculated between the average of internal states of each generated stroke.

authorship verification problem, i.e., as a sub-task of writer identification [Stein et al. 2007], whose goal is to determine the identity of a query sample from a *predefined set* of writers. Many studies focus on writer identification [Dhieb et al. 2021; Schlapbach et al. 2008; Shivram et al. 2012; Singh and Sundaram 2015; Xing and Qiao 2016; Yang et al. 2016]. However, most of them are impractical in the open-world scenario of paper exams: it's difficult to include all authors of an exam in the set. Also, they usually require sufficient data from candidates and must be retrained for each target writer. To capture a writer's characteristics, we choose a different approach and leverage a technique initially used to *generate synthetic writings* that resemble the handwriting of a reference author [Chang et al. 2022; Graves 2013; Kotani et al. 2020; Maksai et al. 2022].

2.1 Modelling

The input to our machine learning model is digitized handwriting from digital pens. A handwriting sample is represented as a sequence of strokes, each consisting of a list of points with pen coordinates and a binary pen-up value indicating whether the pen touches the surface. As output, we aim to predict if two writings are produced by the same user. We extract the handwriting style and define a measure to compare the two styles. We employ the method of Aksan et al. [Aksan et al. 2018] to encode the writer's style and then use it to detect author impersonation. It was initially developed to *synthesize* realistic handwriting from typed text, but has a useful property. To transfer the desired look of a reference to a generated sample, it separately extracts the appearance and the content. The model disentangles the style component from the content of the writing and projects it into a continuous-valued latent space. Instead of using this hidden state as an input to guide the generative model, we introduce a similarity measure in the latent space that allows us to compare the styles of different writings ignoring their content.

The model architecture is based on a conditional variational recurrent neural network [Kingma and Welling 2014], which predicts the next stroke given the current one. The style and content are encoded as two separate latent random variables whose distributions are learned during training. The style information of handwriting is modeled by an isotropic Normal distribution and the content by a Gaussian Mixture Model. The inherent sequential nature of handwriting is captured via long short-term memory (LSTM) cells.

The model is composed of two parts: the inferencer and the synthesizer, which are trained simultaneously by reconstructing given handwriting samples. After training, the inferencer which extracts the personal style can be used independently of its complement, which generates a synthetic sample given the inferred style and the text. We refer to the original paper [Aksan et al. 2018] for a full description. We are interested in the output of the inferencer part. By comparing the output style states, we should be able to distinguish the writings of different authors. In the original approach, this state is represented by two LSTM cells (each consisting of 512 units), one for the input layer and one for the latent. In contrast to the handwriting synthesizer, which used the latent LSTM cell to initialize the generation procedure with the style information, we use the cell state of the *input* layer as an encoding of the style. Our preliminary experiments showed that this state has more capacity to describe the whole sample. To measure the distance between two style encodings, i.e., two vectors, we used cosine similarity (Figure 1a). If the distance exceeded a threshold value, the two styles, and accordingly two authors, were considered to be different. Although the latent representation of a style should capture the writer's individuality, its capacity may be insufficient for achieving high performance. To reinforce the discriminative power, we proposed another similarity measure that works on the same text samples (Figure 1b). Indeed, even though we do not have the same handwriting samples from the reference and the investigated writer, we used the other part of the model, the synthesizer, to generate synthetic strokes—let it be even a simple character sequence 'abcdefgh'—that simulate the necessary handwriting. Since the synthesizer produce the internal state for each point in a stroke, we averaged values over the whole writing. Again, we obtained 512-dimensional vectors which we compared with cosine distance measure; the obtained distance was then tested against a threshold.

A sound disentanglement of content and style requires to input character and word segmentation and recognition of handwritten input along with raw strokes. We followed the suggestion of the authors of *DeepWriting* and, in a preprocessing step, used a separate BiRNN (bidirectional recurrent neural networks) based model to classify input samples, since it was shown to perform significantly better than standard LSTM models. Like Aksan et al. [2018], the BiRNN classifier consists of 3-layer bidirectional LSTM cells with 512 units. A 1-layer fully connected network with 256 units and ReLu activation function transforms BiRNN representations into the end-of-character and beginning-of-word labels and character probabilities. The model has been implemented in Tensorflow and trained on segmented samples of handwritten text from the *DeepWriting* dataset [Aksan et al. 2018]. Given two samples of handwriting, our model produces a distance between them, estimating how different the samples are. Therefore, we can establish a process of identifying users who produce handwriting by continuously testing whether the written input is similar to the reference.

2.2 Towards Real-time Authentication in Exams

We employ our handwriting-based method for passive continuous user authentication to build a proctoring system that detects the 'contract cheating' impersonation attack during exams. We suggest using digital pens and physical paper because most students are familiar with this setup. To test the feasibility of the approach, we developed a prototype system that utilizes the Neo Smartpen N2. This digital pen allows writing on paper, resembling a regular ball pen, but it uses an optical sensor for immediate digitizing hand-drawn sketches. For this to work, it is necessary to print a subtle micro-dot pattern[1] onto the paper. To collect the data from the digital pen, we developed a recording application based on the official Android SDK [2]. The pen is connected to an Android mobile device via Bluetooth using the app. This application visualizes the pen signal in real time and streams it to a server via a Wi-Fi connection. On the server, the handwriting strokes are preprocessed and stored to be later fed into the model for comparison with a reference sample. If the dissimilarity score drops below a threshold for a couple of consecutive queries, the system can signal a possible authentication violation. A regular examination is conducted as follows. Before the exam, students are registered in the system by filling out a registration form with a digital pen. We assume that the impersonation does not occur at this step and the user can validate her identity with many factors. The handwriting sample is then stored in a database and later used as a reference sample for online authentication during exams. For that, handwriting samples are continuously transferred to the server and compared to the reference. If the system detects that the handwriting of a student does not match the reference, this should be considered a hint for the examiner to check the student's identity. The system could also identify if an impersonator is substituted during an exam.

3 EVALUATION

We (i) test the effectiveness of the authorship verification with samples from a large handwriting dataset and (ii) conduct a pilot study with real users. To study the internal validity, we used the *Deepwriting* dataset [Aksan et al. 2018], which is an extension of the well-known IAM-OnDB (IAM On-Line Handwriting Database) [Liwicki and Bunke 2005] collection. It contains writings from 294 unique authors, for a total of 85181 words, resulting in a median of 292 words per writer. We randomly split the dataset into two parts: the training set and a 20-writer hold-out test set (the authors from the test set are never seen during the model training). As the processing of long handwriting could be time-consuming, we split long samples with more than 300 strokes into parts using end-of-character labels. For each author from the test set, we randomly select a sample of writing (it consists of 5–15 words) and compute the corresponding style vectors, which become a reference. We want to detect whether a randomly selected sample is (a) similar to the reference sample of the corresponding author and (b) different from a randomly selected sample by another author. So, for each reference, we randomly selected 25 samples of writing from the same author and 25 samples from other random authors, which totals 500 pairs from the same authors and 500 pairs from different authors. Next, we compute the distance between styles of samples for each pair using both measures. To identify the threshold for each similarity measure, we used a small subset of data from the training set. Finally, we constructed the confusion matrix with the results of correct and incorrect identification. We repeated the sampling

[1] https://www.neosmartpen.com/en/ncode-pdf/
[2] https://github.com/NeoSmartpen/Android-SDK2.0

Table 1: The results of the author identification on the *Deepwriting* dataset using different similarity measures.

Dataset	Similarity	Accuracy	Sensitivity	Specificity	AUC
Deepwriting	Sim (A)	80.5%	79.8%	82.2%	0.88
	Sim (B)	87.5%	89.5%	87.8%	0.95
Pilot study	Sim (B)	81%	82%	78%	0.83

procedure over 10 trials and computed mean accuracy, sensitivity, specificity, and AUC score of identification. The results of the identification experiments are summarized in Table 1. The evaluation shows that our latent style space is sufficiently descriptive to be used for authorship verification. The similarity (A) achieves an accuracy of 80.5%. Manual investigation revealed that some strokes are not as characteristic as others and cannot represent the writer's style well, leading to errors. The similarity (B) performs better with an accuracy of 87.5%. The specificity increased by around 5.6%, indicating fewer false alarms were produced. In Figure 2 we show the ROC curves of both metrics. The ROC curves and AUC score indicate that the model based on a comparison of generated synthetic samples offers a better trade-off characteristic between sensitivity and specificity. These results have been produced on one short stroke sequence per writer. Increasing the number of test samples per writer and averaging the predictions would increase accuracy, smoothing out individual outliers. We also compared our method to an approach proposed by Kotani et al. [2020]. They leveraged Decoupled Style Descriptors to generate the handwriting. In their paper, they report the performance of their approach using the writer recognition task. We followed their description but modified the task to be writer verification. Although the writer identification accuracy is high (up to 97.86%), their model does not perform as well in the writer verification, showing an accuracy of 72%.

To assess the external validity, we conducted a small pilot study involving 7 participants (colleagues from our institute, 6 males and 1 female, average age 30). We used the Neo SmartPen N2 pen and our recording app to collect the data. The participants were asked to write two arbitrary sentences of their choice with the digital pen on a specially prepared paper. We used one sentence as a reference and compared it with all the others, imitating an impersonation

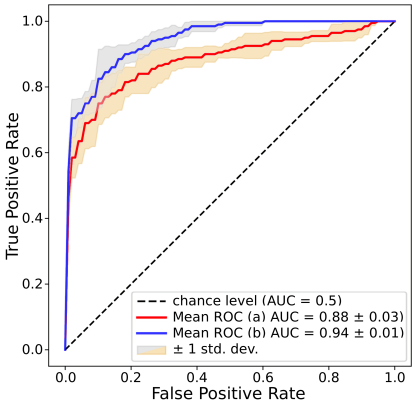

Figure 2: ROC curves for both similarities

cheating attempt. We split all sentences into parts and operated on small chunks. We predicted writer ownership for each split and used majority voting for final predictions. The model achieved an accuracy of 81%. Further manual evaluation of results showed that the underlying handwriting model sometimes failed to reconstruct the style of connected cursive script accurately. This shortcoming was also stated by Aksan et al. [2018].

4 DISCUSSION

The results of the experiments show the potential of our approach. On a 20-writer test set we achieved an accuracy of 87.5%, while in a pilot study, the model showed slightly worse performance (81%). These results leave room for improvement and facilitate further investigation of the limits of the proposed technique, as well as strategies to overcome them. We believe that our approach can benefit from the use of additional input dimensions, like timestamps and pressure, as they are harder to imitate. Incorporating siamese networks—shown to be effective for signature identification—into our model can potentially increase overall precision. Since handwriting may be affected by various factors, such as physical conditions, stress, or time pressure, our next step will be to assess the robustness of the approach to intra-writer variability. In addition, it would be essential to explore whether our model suffers from a bias against a faction of the population based on their gender, age, and other factors. Since the model is not perfect and produces false positives, this might result in unjustified inspections and critically affect the examinee's performance. By changing the decision threshold, one can decrease the number of false alarms at the expense of a reduced detection rate. We envision our approach to be used in combination with other proctoring methods, like the student's performance history analysis. In this work, we focus on the analysis of plain handwriting. Potentially, the approach can be adapted for other content, like math expressions and chemical formulas. Besides, the way we disentangle the style and content of handwriting should allow processing not just English but other West-European languages without additional model updates; though, non-Latin languages (e.g., Arabic or Chinese) would likely require retraining.

5 CONCLUSION

We proposed an approach for continuous authentication using digital pens and handwriting analysis. We suggest using it during exams to prevent impersonation cheating of students. Our method is based on a deep neural network architecture that disentangles style from content. The style information is used to uniquely identify the writer online using only a few samples of reference data. We proved the effectiveness of the approach by testing it on a large *DeepWriting* handwriting dataset. Along with the model, we developed a prototype and conducted a verification study to show the feasibility of the approach.

ACKNOWLEDGMENTS

This work was partially funded by the German Federal Ministry of Education and Research under grant number 01IW23002 (No-IDLE), by the Lower Saxony Ministry of Science and Culture, and the Endowed Chair of Applied Artificial Intelligence of the University of Oldenburg.

REFERENCES

Siti Aisyah, Yoanes Bandung, and Luki B Subekti. 2018. Development of continuous authentication system on android-based online exam application. In *2018 international conference on information technology systems and innovation (ICITSI)*. IEEE, 171–176.

Emre Aksan, Fabrizio Pece, and Otmar Hilliges. 2018. DeepWriting: Making digital ink editable via deep generative modeling. *Conference on Human Factors in Computing Systems - Proceedings* 2018-April (2018). https://doi.org/10.1145/3173574.3173779

Helaine Alessio and Karsten Maurer. 2018. The impact of video proctoring in online courses. *Journal on Excellence in Col-Lege Teaching* 29, 3 (2018), 1–10.

Alexander Amigud and Thomas Lancaster. 2019. 246 reasons to cheat: An analysis of students' reasons for seeking to outsource academic work. *Computers & Education* 134 (2019), 98–107.

Alexander Amigud and Thomas Lancaster. 2020. I will pay someone to do my assignment: an analysis of market demand for contract cheating services on twitter. *Assessment and Evaluation in Higher Education* 45, 4 (2020), 541–553. https://doi.org/10.1080/02602938.2019.1670780

Lj Arnautovski. 2019. Face recognition technology in the exam identity authentication system-implementation concept. *Proceedings of Papers* (2019), 50.

David G Balash, Dongkun Kim, Darika Shaibekova, Rahel A Fainchtein, Micah Sherr, and Adam J Aviv. 2021. Examining the examiners: Students' privacy and security perceptions of online proctoring services. In *Proceedings of the Seventeenth Symposium on Usable Privacy and Security*.

Michael Barz, Kristin Altmeyer, Sarah Malone, Luisa Lauer, and Daniel Sonntag. 2020. Digital pen features predict task difficulty and user performance of cognitive tests. In *Proceedings of the 28th ACM Conference on User Modeling, Adaptation and Personalization*. 23–32.

Razan Bawarith, Abdullah Basuhail, Anas Fattouh, and Shehab Gamalel-Din. 2017. E-exam cheating detection system. *International Journal of Advanced Computer Science and Applications* 8, 4 (2017).

Marcelo Luiz Brocardo, Issa Traore, and Isaac Woungang. 2019. Continuous authentication using writing style. *Biometric-based physical and cybersecurity systems* (2019), 211–232.

Omar Canales, Vinnie Monaco, Thomas Murphy, Edyta Zych, John Stewart, Charles Tappert Alex Castro, Ola Sotoye, Linda Torres, and Greg Truley. 2011. A stylometry system for authenticating students taking online tests. *P. of Student-Faculty Research Day, Ed., CSIS. Pace University* (2011).

Jen-Hao Rick Chang, Ashish Shrivastava, Hema Koppula, Xiaoshuai Zhang, and Oncel Tuzel. 2022. Style equalization: Unsupervised learning of controllable generative sequence models. In *International Conference on Machine Learning*. PMLR, 2917–2937.

Monica Chin. 2021. *University will stop using controversial remote-testing software following student outcry.* https://www.theverge.com/2021/1/28/22254631/university-of-illinois-urbana-champaign-proctorio-online-test-proctoring-privacy

Robert Clarke and Thomas Lancaster. 2006. Eliminating the successor to plagiarism? Identifying the usage of contract cheating sites. In *Proceedings of 2nd international plagiarism conference*. Northumbria Learning Press, 19–21.

Phillip Dawson. 2016. Five ways to hack and cheat with bring-your-own-device electronic examinations. *British Journal of Educational Technology* 47, 4 (2016), 592–600.

Thameur Dhieb, Houcine Boubaker, Wael Ouarda, Sourour Njah, Mounir Ben Ayed, and Adel M. Alimi. 2021. Deep bidirectional long short-term memory for online multilingual writer identification based on an extended Beta-elliptic model and fuzzy elementary perceptual codes. *Multimedia Tools and Applications* 80, 9 (2021), 14075–14100. https://doi.org/10.1007/s11042-020-10412-8

Dana Dobrovska. 2017. Technical Student Electronic Cheating on Examination. In *Interactive Collaborative Learning: Proceedings of the 19th ICL Conference-Volume 1*. Springer, 525–531.

Alex Duncan and David Joyner. 2022. On the necessity (or lack thereof) of digital proctoring: Drawbacks, perceptions, and alternatives. *Journal of Computer Assisted Learning* 38, 5 (2022), 1482–1496. https://doi.org/10.1111/jcal.12700

Moukhliss Ghizlane, Belhadaoui Hicham, and Filali Hilali Reda. 2019. A new model of automatic and continuous online exam monitoring. In *2019 international conference on systems of collaboration big data, internet of things & security (SysCoBIoTS)*. IEEE, 1–5.

David Goldberg. 2021. Programming in a pandemic: Attaining academic integrity in online coding courses. *Communications of the Association for Information Systems* 48, 1 (2021), 6.

Alex Graves. 2013. Generating sequences with recurrent neural networks. *arXiv preprint arXiv:1308.0850* (2013).

Olivia L Holden, Meghan E Norris, and Valerie A Kuhlmeier. 2021. Academic integrity in online assessment: A research review. In *Frontiers in Education*, Vol. 6. Frontiers Media SA, 639814.

Mohammed Juned Hussein, Javed Yusuf, Arpana Sandhya Deb, Letila Fong, and Som Naidu. 2020. An evaluation of online proctoring tools. *Open Praxis* 12, 4 (2020), 509–525.

Samson Idemudia, Mohd Foad Rohani, Maheyzah Siraj, and Siti Hajar. 2016. A smart approach of E-Exam assessment method using face recognition to address identity theft and cheating. *International Journal of Computer Science and Information Security (IJCSIS)* 14, 10 (2016).

David C. Ison. 2020. Detection of online contract cheating through stylometry: A pilot study. *Online Learning Journal* 24, 2 (2020), 142–165. https://doi.org/10.24059/olj.v24i2.2096

N Joshy, G Kumar, P Mukhilan, M Prasad, T Ramasamy, and H Student. 2018. Multi-factor authentication scheme for online examination. *International Journal of Pure and Applied Mathematics* 119, 15 (2018), 1705–1712.

Ivans Kigwana and Hein Venter. 2016. Proposed high-level solutions to counter online examination fraud using digital forensic readiness techniques. In *Proceedings of the 11th International Conference on Cyber Warfare and Security, ICCWS 2016*. 407–414.

Diederik P Kingma and Max Welling. 2014. Stochastic gradient VB and the variational auto-encoder. In *Second international conference on learning representations, ICLR*, Vol. 19. 121.

Atsunobu Kotani, Stefanie Tellex, and James Tompkin. 2020. Generating Handwriting via Decoupled Style Descriptors. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 12357 LNCS (2020), 764–780. https://doi.org/10.1007/978-3-030-58610-2_45 arXiv:2008.11354

Thomas Lancaster and Robert Clarke. 2017. Rethinking Assessment By Examination in the Age of Contract Cheating. , 215–228 pages.

Yair Levy and M Ramim. 2007. A theoretical approach for biometrics authentication of e-exams. *Nova Southeastern University, USA* (2007), 93–101.

Marcus Liwicki and Horst Bunke. 2005. IAM-OnDB-an on-line English sentence database acquired from handwritten text on a whiteboard. In *Eighth International Conference on Document Analysis and Recognition (ICDAR'05)*. IEEE, 956–961.

Andrii Maksai, Henry Rowley, Jesse Berent, and Claudiu Musat. 2022. Inkorrect: Online Handwriting Spelling Correction. (2022). arXiv:2202.13794 http://arxiv.org/abs/2202.13794

John V Monaco, John C Stewart, Sung-Hyuk Cha, and Charles C Tappert. 2013. Behavioral biometric verification of student identity in online course assessment and authentication of authors in literary works. In *2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*. IEEE, 1–8.

Sara Morrison and Rebecca Heilweil. 2020a. *How teachers are sacrificing student privacy to stop cheating.* https://www.vox.com/recode/22175021/school-cheating-student-privacy-remote-learning

Sara Morrison and Rebecca Heilweil. 2020b. *University will stop using controversial remote-testing software following student outcry.* https://www.vox.com/recode/22175021/school-cheating-student-privacy-remote-learning

James Moten Jr, Alex Fitterer, Elise Brazier, Jonathan Leonard, and Avis Brown. 2013. Examining online college cyber cheating methods and prevention measures. *Electronic Journal of E-learning* 11, 2 (2013), pp139–146.

Aditya Nigam, Rhitvik Pasricha, Tarishi Singh, and Prathamesh Churi. 2021. A Systematic Review on AI-based Proctoring Systems: Past, Present and Future. *Education and Information Technologies* 26 (2021), 6421–6445. Issue 5. https://doi.org/10.1007/s10639-021-10597-x

Mark Norris. 2019. University Online Cheating–How to Mitigate the Damage. *Research in Higher Education Journal* 37 (2019).

Sharon Oviatt, Kevin Hang, Jianlong Zhou, Kun Yu, and Fang Chen. 2018. Dynamic handwriting signal features predict domain expertise. *ACM Transactions on Interactive Intelligent Systems (TiiS)* 8, 3 (2018), 1–21.

Elise Potaka and Cecily Huang. 2015. *Pens For Hire: how students cheat, and how they get away with it.* https://www.sbs.com.au/news/the-feed/article/pens-for-hire-how-students-cheat-and-how-they-get-away-with-it/5v3erlpij

Alexander Prange and Daniel Sonntag. 2022. Modeling Users' Cognitive Performance Using Digital Pen Features. *Frontiers in Artificial Intelligence* 5 (2022).

RS Vishnu Raj, S Athi Narayanan, and Kamal Bijlani. 2015. Heuristic-based automatic online proctoring system. In *2015 IEEE 15th International Conference on Advanced Learning Technologies*. IEEE, 458–459.

Yousef W Sabbah. 2017. Security of online examinations. *Data Analytics and Decision Support for Cybersecurity: Trends, Methodologies and Applications* (2017), 157–200.

Andreas Schlapbach, Marcus Liwicki, and Horst Bunke. 2008. A writer identification system for on-line whiteboard data. *Pattern recognition* 41, 7 (2008), 2381–2397.

Arti Shivram, Chetan Ramaiah, Utkarsh Porwal, and Venu Govindaraju. 2012. Modeling writing styles for online writer identification: A hierarchical bayesian approach. In *2012 International Conference on Frontiers in Handwriting Recognition*. IEEE, 387–392.

Guttorm Sindre and Aparna Vegendla. 2015. E-exams versus paper exams: A comparative analysis of cheating-related security threats and countermeasures. *Department of Computer and Information Science (IDI)* 8, 1 (2015), 34–45.

Gautam Singh and Suresh Sundaram. 2015. A subtractive clustering scheme for text-independent online writer identification. In *2015 13th International Conference on Document Analysis and Recognition (ICDAR)*. IEEE, 311–315.

Prakash Sinha, Aman Yadav, et al. 2020. Remote proctored theory and objective online examination. *International Journal of Advanced Networking and Applications* 11, 6 (2020), 4494–4500.

Lassaad K SMIRANI and Jihane A BOULAHIA. 2022. An Algorithm based on Convolutional Neural Networks to Manage Online Exams via Learning Management System Without using a Webcam. *International Journal of Advanced Computer Science and Applications* 13, 3 (2022).

Sargur N Srihari, Sung-Hyuk Cha, Hina Arora, and Sangjik Lee. 2002. Individuality of handwriting. *Journal of forensic sciences* 47, 4 (2002), 856–872.

Benno Stein, Moshe Koppel, and Efstathios Stamatatos. 2007. Plagiarism analysis, authorship identification, and near-duplicate detection PAN'07. In *ACM SIGIR Forum*, Vol. 41. ACM New York, NY, USA, 68–71.

Gabe Teninbaum. 2021. Report of ExamSoft's ExamID Feature (and a Method to Bypass It). *The Journal of Robotics, Artificial Intelligence & Law* 4 (2021).

Dirk Von Gruenigen, Fernando Benites de Azevedo e Souza, Beatrice Pradarelli, Amani Magid, and Mark Cieliebak. 2018. Best practices in e-assessments with a special focus on cheating prevention. In *2018 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, 893–899.

Linjie Xing and Yu Qiao. 2016. Deepwriter: A multi-stream deep CNN for text-independent writer identification. In *2016 15th international conference on frontiers in handwriting recognition (ICFHR)*. IEEE, 584–589.

Weixin Yang, Lianwen Jin, and Manfei Liu. 2016. DeepWriterID: An End-to-End Online Text-Independent Writer Identification System. *IEEE Intelligent Systems* 31, 2 (2016), 45–53. https://doi.org/10.1109/MIS.2016.22