Autoencoders for Anomaly detection in exam surveillance

BENATALLAH Rayan Ibrahim, SAYOUD Lynda , MALLEK Lina, BENAZZOU Fatima. Visual Computing Master's students, Computer Science Faculty, USTHB University

1. Introduction

Nowadays, the issue of cheating in exams is becoming a growing concern in the field of education, casting doubt on the fairness of exams and challenging the reliability of academic results. Faced with this disconcerting reality, it is imperative to explore innovative solutions that enhance academic standards and contribute to a more precise evaluation of students.

It is from this perspective that our approach takes shape, built upon the integration of a specific deep learning technique, we shall distinctly define cheating from normal cases within an exam room through the use of anomaly detection with autoencoders.

To delve deeper into the specific mechanisms of autoencoders, the upcoming sections will explore their application in the realm of cheating detection in exams.

2. Method

The conventional approach to mitigating cheating in exams (see figure 1) often involves enumerating known cheating instances, a daunting task given the myriad ways in which students may engage in dishonest behavior. In contrast, our methodology adopts a novel perspective by employing autoencoders for anomaly detection without the need to explicitly define all cheating instances.

Figure 1. Sample image from our dataset

Autoencoders for Anomaly detection in exam surveillance

, BENATALLAH Rayan Ibrahim, SAYOUD Lynda , MALLEK Lina, BENAZZOU Fatima. Visual Computing Master's students, Computer Science Faculty, USTHB University

Data Preparation

We commenced our study by assembling a dataset comprising exclusively normal, non-anomalous exam instances by capturing a 2-minute video of students in a class where cheating didn't take place, extracting its frames to end up with over 3500 pictures. This deliberate choice was grounded in the recognition that obtaining a comprehensive set of cheating instances is impractical. The autoencoder was trained exclusively on this pristine dataset to learn the inherent patterns of legitimate exam behavior.

Model architecture and training

Our autoencoder architecture is tailored for anomaly detection in the context of exam surveillance (see figure 2). The model, implemented using the Keras framework, follows a symmetric encoder-decoder structure. The encoder progressively reduces the spatial dimensions of the input, capturing key features, while the decoder up-scales the encoded representation to faithfully reconstruct the original input. The choice of the mean squared error (MSE) as the loss function and the Adam optimizer underpins the training process, aligning with our objective of minimizing reconstruction errors for anomaly detection.

Dual-Threshold Anomaly Detection

However, after delving into further research, we discovered that depending only on the reconstruction error may not be adequate for effective anomaly detection. This insight was particularly emphasized in the "Robust Anomaly Detection in Images using Adversarial Autoencoders" [6], where our exploration deepened, leading us to uncover another factor – Kernel Density Estimation (KDE) from DigitalSreeni on YouTube [7]. This addition aims to further enhance anomaly detection efficiency, complementing the reconstruction error.

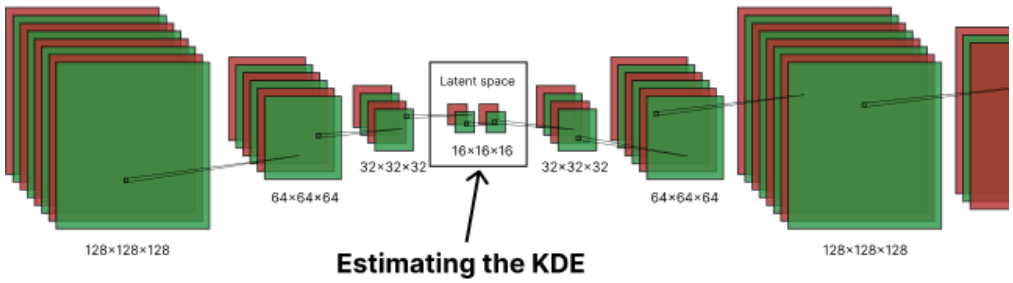

Figure 2. Model architecture

Autoencoders for Anomaly detection in exam surveillance

BENATALLAH Rayan Ibrahim, SAYOUD Lynda , MALLEK Lina, BENAZZOU Fatima. Visual Computing Master's students, Computer Science Faculty, USTHB University

Observation

After splitting our trained autoencoder, using our trained encoder helped us estimate the KDE of the latent representation of both normal and anomalous data.
Simultaneously, we perform a reconstruction error analysis on both normal and anomalous data using the trained autoencoder. This step ensures a comprehensive assessment, considering both the spatial characteristics in the latent space and the fidelity of reconstructed instances.

Thresholds setting

Guided by the observations from the KDE analysis and reconstruction error metrics, we establish dual thresholds. The first, a soft threshold, identifies instances with a moderate deviation from the expected pattern, prompting a closer examination. The second, a hard threshold, serves as a more stringent criterion, unequivocally flagging instances with a significant deviation as anomalies.

3. Results

Testing the model on images
In this section, we delve into the practical implementation of our proposed approach and showcase the results obtained through the figure 3.

Testing the model on video
Our program processes input videos by extracting individual frames and analyzing each one to check if it's an anomaly or not. Frames depicting anomalies are specifically identified and saved in a designated 'anomalies' folder (see Figure 4).

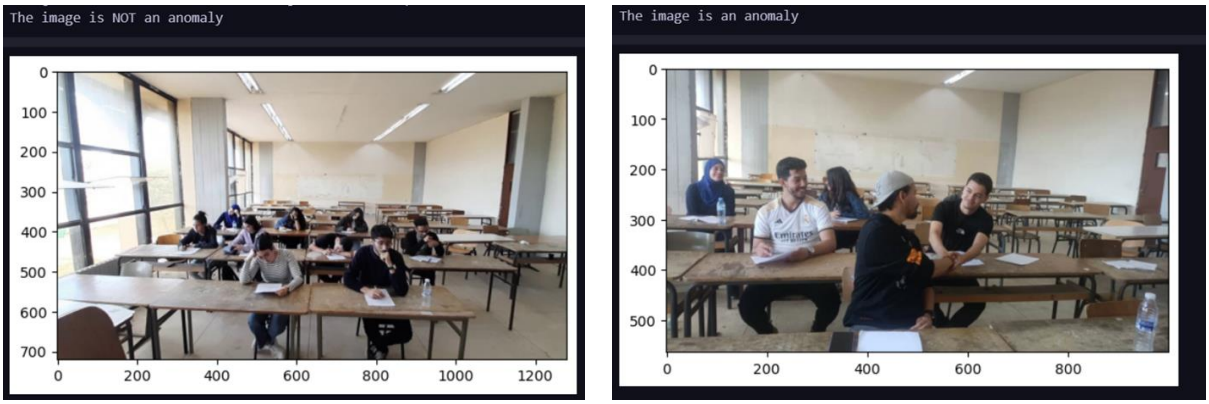

Figure 3. Non anomaly (left) and anomaly detection (right)

Autoencoders for Anomaly detection in exam surveillance

BENATALLAH Rayan Ibrahim, SAYOUD Lynda , MALLEK Lina, BENAZZOU Fatima. Visual Computing Master's students, Computer Science Faculty, USTHB University

Conclusion

In conclusion, while our approach with autoencoders for exam surveillance offers unparalleled advantages in precision and adaptability, ongoing vigilance and refinement is essential to address the ever-changing landscape of educational environments and student behaviors. This system represents a crucial step toward maintaining the integrity of examinations in an era of technological advancements and evolving academic challenges.

As part of our future work, we aspire to enhance the capabilities of our current model. Our upcoming focus involves the introduction of segmented anomaly detection to refine the results further. This segmentation will allow us to pinpoint and visualize specific individuals engaged in anomalous activities during exams, providing a more granular and insightful analysis. This expansion aims to improve the precision and interpretability of our cheat detection system, contributing to its effectiveness.

References

[1] Subash Palvel, Exploring Autoencoders in Deep Learning, Sep 12, 2023,[en ligne], Available on: https://subashpalvel.medium.com/exploring-autoencoders-in-deep-learning-2dd41a689104

[2]Pouya Hallaj, Anomaly Detection with Autoencoders, Sep 26, 2023, [online], available on: https://medium.com/@pouyahallaj/anomaly-detection-with-autoencoders-956893b60aef

[3] Subham Sarkar, Anomaly Detection in Images — AUTOENCODERS, Analytics Vidhya, Jun 13, 2021, [online], available on: https://medium.com/analytics-vidhya/anomaly-detection-in-images-autoencoders-b780abf88f51

[4] ANURAG SINGH CHOUDHARY, Unveiling Denoising Autoencoders, Jul 06, 2023, [online], available on: https://www.analyticsvidhya.com/blog/2023/07/unveiling-denoising-autoencoders/

[5] Anay Dongre, Overview of Autoencoders, Jan 1, 2023, available on: https://dongreanay.medium.com/overview-of-autoencoders-52c777418937

[6] Laura Beggel , Michael Pfeiffer , Bernd Bischl ,Robust Anomaly Detection in Images using Adversarial Autoencoders, Jan 18, 2019, page 10, available on: https://arxiv.org/pdf/1901.06355.pdf

[7] DigitalSreeni, 260 - Identifying anomaly images using convolutional autoencoders, march 9,2022, available on: https://www.youtube.com/watch?v=q_tpFGHiRgg&t=268s

Figure 4. Cheating Detected Frame in 'Anomalies' Folder