

Automatisiertes Proctoring mittels Machine Learning

Studenten



Kevin Pfister



Nicolas Gattlen

Aufgabenstellung: Das Ziel dieser Arbeit bestand darin, ein Tool oder eine Methode zu entwickeln, die es ermöglicht, mittels spezialisierter Software zu erkennen, ob ein Prüfungsteilnehmer oder eine Prüfungsteilnehmerin während einer Online-Prüfung betrügerische Handlungen begeht. Der Einsatz einer solchen Software bietet den Vorteil, dass Online-Prüfungen effektiv durchgeführt werden können. Zudem ermöglicht es, dass Programmierprüfungen nicht mehr manuell, sondern in einem kontrollierten und überwachten Umfeld absolviert werden können. Der Fokus dieser Arbeit lag speziell auf der Überwachung der Offline-Aktivitäten der Prüfungsteilnehmenden. Dies umfasst die Beobachtung von auffälligen Körperbewegungen und Sprachaktivitäten.

Vorgehen / Technologien: Unser Ansatz zielte darauf ab, die Benutzerfreundlichkeit unserer Software sowohl für Studierende als auch für Lehrende zu maximieren und einen strukturierten Prozess zu etablieren. Der Ablauf beginnt damit, dass der Studierende die Software aktiviert, die mittels einer Webcam ein Video aufzeichnet und über ein ausgewähltes Mikrofon den Ton erfasst. Nachdem die Prüfungsaufgaben gelöst wurden, wird die Software beendet. Der Studierende erhält dadurch eine Video- und Audiodatei, die er eigenständig an einen schulischen Server übermitteln kann. Nachdem der Schulserver alle Audio und Videodateien erhalten hat. Kann der Professor mittels einer Webseite die Video und Audiodateien Analysieren. Während der Analyse wird bei jedem Prüfungsteilnehmer die Video und Audiodatei analysiert. Dabei wurden bestimmte Kriterien von uns ausgewählt auf welche sich die Videoanalyse stützen soll.

Gesichtserkennung: In jedem Frame des Videos soll überprüft werden, ob genau eine Person anwesend ist. Dies ist wichtig, da Prüfungen in der Regel Einzelarbeiten sind. Sollte keine oder mehr als eine Person erkannt werden, wird dies als Betrugsversuch gewertet.

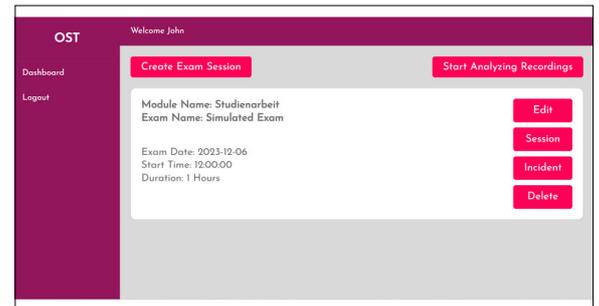
Munderkennung: Das System muss ständig den Mund erkennen können. Dies dient dazu, heimliche Gespräche aufzudecken, auch wenn das Mikrofon während der Prüfung absichtlich ausgeschaltet ist. Ein Betrugsversuch wird deklariert, sobald der Mund sich öffnet, um die Spracherkennung zu schützen.

Kopfneigungserkennung: Die Kopfposition wird kontinuierlich überwacht, um auffällige Bewegungen, die auf einen zweiten Bildschirm oder ein externes Gerät hinweisen könnten, als Betrugsversuche zu identifizieren.

Iriserkennung: Diese Technik dient dazu, ungewöhnliches Augenschillern zu erkennen. Sie soll Prüflinge identifizieren, die zwar ihren Kopf nicht bewegen, aber dennoch nicht auf die Prüfungsaufgaben schauen

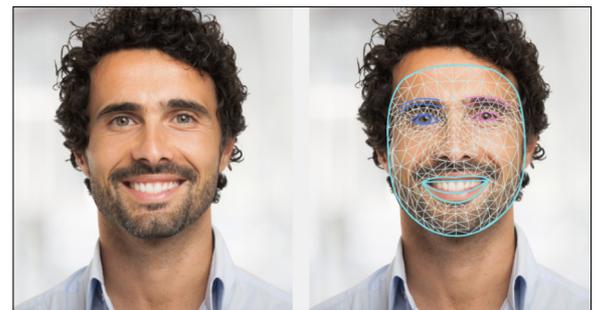
Ergebnis: Derzeit ist eine vollständig automatisierte Proctoring-Lösung noch nicht realisierbar. Menschliches Eingreifen bleibt notwendig, um zu entscheiden, ob in bestimmten Situationen Betrug vorliegt. Unsere Software hat jedoch den Analyseprozess von Audio- und Videodateien erheblich effizienter gestaltet. Als nächsten Schritt zur Verbesserung der Software könnte die Erfassung von Online-Aktivitäten in Betracht gezogen werden.

Anzeige der Proctoring Webseite Eigene Darstellung



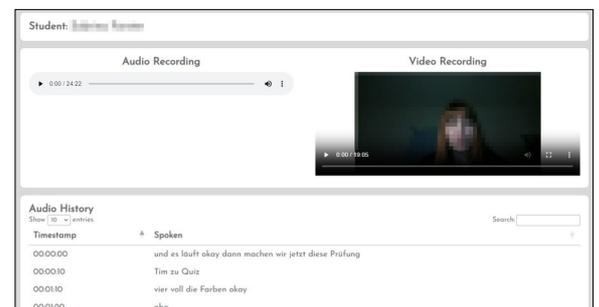
Die Gesichtserkennung von Google, welche für die einzelnen Sensoren verwendet wurde

Mediapipe Dokumentation: developers.google.com/mediapipe



Dashboard der fertigen Analyse. Mit den Video und Audio Auffälligkeiten

Eigene Darstellung



Referent
Prof. Dr. Frieder Loch

Themengebiet
Software, Software
Engineering - Core
Systems

