

Press release**Technische Universität Chemnitz****Dipl.-Ing. Mario Steinebach**

02/07/2024

<http://idw-online.de/en/news828325>Cooperation agreements, Research results
Electrical engineering, Information technology, Mechanical engineering
transregional, nationalTECHNISCHE UNIVERSITÄT
IN DER KULTURHAUPTSTADT EUROPAS
CHEMNITZ**Vertrauen stärken: Chemnitzer Forschende verbessern Datenschutz bei Augmented-Reality-Anwendungen****Forschende der Professur Produktionssysteme und -prozesse der TU Chemnitz haben eine datenschutzgerechte Augmented-Reality-Lösung entwickelt, bei der Gesichter erkannt und verfremdet werden, ohne das Tracking zu beeinträchtigen.**

Eine der größten Hürden beim Einsatz von Augmented Reality (AR) in Unternehmen ist der Schutz sensibler Daten. Das Problem: Bei AR-Anwendungen auf Tablets, Smartphones oder Datenbrillen wird die gesamte reale Umgebung des Nutzenden mit Hilfe von Sensoren erfasst und ausgewertet, ohne personenbezogene bzw. vertrauliche Daten zu schützen. Dabei stellen sich die Fragen: Was geschieht mit den erfassten Informationen? Wo werden sie gespeichert, wofür werden sie verwendet und wer gibt sie an wen weiter?

Vor diesem Hintergrund haben Wissenschaftlerinnen und Wissenschaftler der TU Chemnitz gemeinsam mit der Advanced Realtime Tracking GmbH aus Oberbayern im Projekt „TrustAR“ eine datenschutzgerechte AR-Lösung entwickelt, die sensible Informationen im Kamerabild erkennt, verfremdet und weiterhin ein akkurates und stabiles Trackingergebnis gewährleistet. „Ziel des Projektes war es – wie der Name TrustAR schon verrät – das Vertrauen in die Augmented-Reality-Technologie zu stärken und ihre Nutzbarkeit in Unternehmen zu verbessern“, erklärt Sven Winkler, wissenschaftlicher Mitarbeiter der Professur Produktionssysteme und -prozesse.

Als potentielle Anwendungsbereiche nennt Winkler beispielsweise die Wartung und Reparatur von komplexen Produktionsanlagen, das Qualitätsmanagement oder den Vertrieb. Dabei müssen sowohl der Persönlichkeitsschutz der Mitarbeitenden als auch der Schutz vertraulicher Dokumente beachtet werden. Die Forschenden legten bei ihrer Entwicklung besonderen Wert darauf, kritische Daten – wie biometrische Informationen zur Gesichtserkennung – bereits vor der Weiterverarbeitung herauszufiltern und damit eine spätere, datenschutzrechtlich relevante Auswertung mit Hilfe von Algorithmen zu verhindern. „Gleichzeitig wollten wir natürlich das Tracking nicht verlangsamen oder behindern, weil das für die künftigen User nicht praktikabel wäre“, so Winkler.

Deshalb haben die Projektmitarbeitenden zwei technische Lösungen entwickelt, die aufeinander abgestimmt sind: Der erste Baustein ist ein Datenschutzmodul für die Bildaufnahme und Anonymisierung. Es erkennt Personen im Video mit einer Zuverlässigkeit von mehr als 95 Prozent und anonymisiert Gesichter in unter zehn Millisekunden, selbst wenn diese nicht frontal der Kamera zugewandt sind. Durch diese Schnelligkeit ist die notwendige Echtzeitfähigkeit der Augmented-Reality-Lösung gewährleistet. Die Forschenden haben außerdem in einer Studie verschiedene Arten der Maskierung (Schwärzung, Verpixeln, Verschleiern) miteinander verglichen. Es zeigte sich, dass die daran beteiligten Probandinnen und Probanden das größte Vertrauen in verschleierte oder verwischte Maskierungen hatten, und dass das Ausschneiden von Bildinformationen den besten Schutz bietet, da diese Bildinformationen nicht mehr vorhanden sind und deshalb später nicht mehr missbräuchlich wiederhergestellt werden können. „Die Erkennung von Dokumenten und Papierformen im Videostream gestaltete sich wesentlich schwieriger als die Gesichtserkennung, weil nicht immer gewährleistet ist, dass das Dokument in ausreichender Qualität und Sichtbarkeit im aufgenommenen Bild zu sehen ist“, berichtet Winkler.

Der zweite Baustein in der neu entwickelten AR-Anwendung ist ein Lokalisierungsmodul, das in der realen Umgebung des Nutzers wichtige Objekte – beispielsweise Maschinen oder Ersatzteile für Reparaturen – erkennt, verortet und diese Informationen der AR-Anwendung zur Verfügung stellt. Dafür wurde eine Künstliche Intelligenz trainiert, die als Eingangsdaten nur künstliche Bilder des Objekts erhielt. Durch das Anonymisieren wurden neue, nicht reale Bildinformationen eingebracht, auf welche die KI erst angepasst werden musste. „Das heißt, dass unser Projektpartner, die ART GmbH, die üblicherweise eingesetzten Lokalisierungsalgorithmen zur Objekterkennung und Posenschätzung neu justieren und auf diese Besonderheiten anlernen musste“, erklärt Winkler.

Die Ergebnisse dieses Vorhabens könnten in Zukunft auch für den Einsatz von Telepräsenz-Robotern im öffentlichen Raum von Nutzen sein, bei denen Videoaufnahmen von unbeteiligten Passantinnen und Passanten ohne deren Einverständnis nicht erlaubt sind.

Das Projekt „TrustAR“ wurde im Rahmen des Zentralen Innovationsprogramms Mittelstand (ZIM) von September 2021 bis Dezember 2023 durch das Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des deutschen Bundestags mit 208.000 Euro gefördert.

contact for scientific information:

Sven Winkler, Telefon +49 (0)371 531-33528, E-Mail sven.winkler@mb.tu-chemnitz.de



Die neu entwickelte Augmented-Reality-Anwendung anonymisiert automatisch die aufgenommenen Personen und erkennt gleichzeitig dank des Lokalisierungsmoduls wichtige Bauteile.

Foto: Katja Klöden