Nr. 43/2022

Magdeburg, 21.07.2022

WIE EIN BLINZELN GEFÄLSCHTE IDENTITÄTEN ENTLARVT

Informatikerinnen und Informatiker der Uni Magdeburg erkennen mit Künstlicher Intelligenz manipulierte Bilder und Videos bei Videoidentifizierungsverfahren

Informatikerinnen und Informatiker der Otto-von-Guericke-Universität Magdeburg arbeiten an einer Software, die künftig gefälschte oder manipulierte Fotos und Videos mittels Künstlicher Intelligenz (KI) schneller und sicherer erkennen kann.

Prof. Dr.-Ing. Jana Dittmann, Dr. Christian Krätzer, Stefan Seidlitz und Dennis Siegel vom Institut für Technische und Betriebliche Informationssysteme der Magdeburger Universität suchen dafür nach Detektoren, also Nachweismitteln, die Manipulationen und Fälschungen von Bildern und Videos erkennen. Ziel ist es, eine rechtskonforme und an ethischen Leitlinien orientierte Softwareplattform zu erarbeiten, die es beispielsweise bei Videoidentifizierungsverfahren ermöglicht, Manipulationen, sogenannte Deep Fakes, zu erkennen. Die Folgen dieser Manipulationen an Fotos oder Videos für die Gesellschaft, aber auch Privatpersonen reichen von politischer Einflussnahme über Bankenbetrug und Identitätsdiebstahl bis hin zu organisierter Kriminalität.

„Der Besitz einer erfundenen, überlassenen oder gestohlenen Identität kann für Kriminelle einen großen Nutzen haben. Ein Konto unter einer anderen Identität, einer sogenannten ‚Fake-ID' zu eröffnen, von diesem Konto Geld abzuheben, einen Kredit aufzunehmen oder dadurch die Herkunft von Geld zu verschleiern sind nur einige Missbrauchsmöglichkeiten", erläutert Professorin

Otto-von-Guericke-Universität Magdeburg • Der Rektor
Abteilung Presse- und Öffentlichkeitsarbeit • Leiterin Katharina Vorwerk, M.A.
Postanschrift: Postfach 4120, 39016 Magdeburg • Hausanschrift: Universitätsplatz 2, 39106 Magdeburg
Telefon: +49 (0)391 67-58751 • Telefax: +49 (0)391 67-48266 • E-Mail: presseteam@ovgu.de
www.ovgu.de

Dittmann. „*Technische Möglichkeiten*, *bild- und videobasierte Authentifizierungsverfahren ‚auszutricksen' gibt es reichlich.*"

Die Identität einer Person eindeutig nachzuweisen, werde zunehmend anspruchsvoller, da inzwischen mit einfachen technischen Mitteln hochwertige Fälschungen von Bildern und Videos angefertigt werden könnten, so Dittmann weiter. *„Bei hochwertigen, professionell erzeugten ‚Deep Fakes' ist es für das bloße Auge fast unmöglich, diese zu erkennen. Um Fälschungen zu entlarven, konzentrieren wir uns auf den Abgleich mit weiteren Kontextprüfungen sowie forensischer und biometrischer Daten primär im Gesicht, also ein Lächeln, ein Fältchen, ein Blinzeln. Da nutzten wir die Schwächen bei der Erzeugung der Fälschung aus."*

Zunächst untersuchen mehrere Detektoren, also automatisierte Verfahrensabläufe der Bilderkennung, Videos und Bilder auf verschiedene Merkmale, die auf „Deep Fakes" hinweisen könnten. KI-basierte Algorithmen konzentrieren sich dafür auf Informationen wie z.B. Unstimmigkeiten bei der Beleuchtung, der Mimik, in der Bewegung oder auch auf vitale Parameter wie Pulsschlag oder Augenbewegungen. Die auf der Grundlage maschinellen Lernens erlangten Ergebnisse werden zusammengeführt und schließlich möglichst rechtskonform und an ethischen Leitlinien orientiert in einer Softwareplattform in Form einer Risiko- und Verdachtslandkarte visualisiert. Letztendlich beurteilt geschultes menschliches Personal abschließend, ob ein „Deep Fake", also eine gefälschte Identität vorliegt oder nicht. *„Die endgültige Identifikation liegt immer in der Hand menschlicher Experten"*, unterstreicht Prof. Dittmann. *„Wir möchten ihnen mit der Softwareplattform das nötige Instrumentarium für Entscheidungen an die Hand geben und dazu Indizien für die Manipulationen einer präsentierten Identität transparent machen, visualisieren und leicht nachvollziehbar vermitteln."*

Die Magdeburger Wissenschaftler arbeiten im Forschungsprojekt „Videoanalyse mit Hilfe künstlicher Intelligenz zur Detektion von falschen und manipulierten Identitäten (FAKE-ID)" für Videoidentifizierungsverfahren mit dem Fraunhofer-

Otto-von-Guericke-Universität Magdeburg • Der Rektor
Abteilung Publikationen und Öffentlichkeitsarbeit • Leiterin Katharina Vorwerk, M.A.
Postanschrift: Postfach 4120, 39016 Magdeburg • Hausanschrift: Universitätsplatz 2, 39106 Magdeburg
Telefon: +49 (0)391 67-58751 • Telefax: +49 (0)391 67-48266 • E-Mail: presseteam@ovgu.de
www.ovgu.de

Heinrich-Hertz-Institut Berlin, der Bundesdruckerei, der Hochschule für Wirtschaft und Recht Berlin sowie der BioID GmbH zusammen. Das Bundesministerium für Bildung und Forschung fördert das Projekt bis April 2024 mit 2,6 Millionen Euro im Rahmenprojekt „Forschung für die zivile Sicherheit“.

Kontakt für die Medien:

Prof. Dr.-Ing. Jana Dittmann, Otto-von-Guericke-Universität Magdeburg, Institut für Technische und Betriebliche Informationssysteme, Tel.: 0391 67-58966

Otto-von-Guericke-Universität Magdeburg • Der Rektor
Abteilung Publikationen und Öffentlichkeitsarbeit • Leiterin Katharina Vorwerk, M.A.
Postanschrift: Postfach 4120, 39016 Magdeburg • Hausanschrift: Universitätsplatz 2, 39106 Magdeburg
Telefon: +49 (0)391 67-58751 • Telefax: +49 (0)391 67-48266 • E-Mail: presseteam@ovgu.de