Fortgeschrittene Gesichtserkennung

Neben spezialisierten Entwicklungsfirmen aus dem Sicherheitsbereich arbeiten alle großen Internet-Konzerne an der Weiterentwicklung von Gesichtserkennungs-Software, sodass diese bereits Eingang in Alltagsgeräte wie Smartphones und sogar Spielzeug gefunden hat (siehe Thema Digitales Spielzeug). Dabei wird zunehmend Künstliche Intelligenz verwendet, um die Bilderkennungsraten zu verbessern. Derzeit liegen die Erkennungsraten bei Bildern aus bestehenden Datenbanken – abhängig von deren Qualität – bei ca. 80%. Das heißt von 100 analysierten Bildern wurden 80 einem anderen Bild einer Person richtig zugeordnet. Bei Bildern aus Überwachungsanlagen hingegen ist man derzeit noch sehr weit davon entfernt. Hier liegt im Gegensatz dazu die Rate der falsch-positiven Zuordnungen bei teilweise mehr als 90%.[1] Verbesserungen basieren vor allem auf dem mittlerweile riesigen Bestand von Bildern im Netz, an denen die Software „trainiert“ werden kann. So hat Facebook neben dem Eigenbestand von Bildern seiner etwa 2,2 Milliarden UserInnen auch Zugriff auf die Datenbank des bildorientierten Social-Media-Kanals Instagram. Die dort verfügbaren 3,5 Milliarden „öffentlichen“ Fotos, die unter 17.000 Hashtags gefasst waren, wurden, ohne die NutzerInnen darauf hinzuweisen, ebenfalls einer Analyse unterzogen und dienten so zur Erhöhung der Treffergenauigkeit.[2] Kommuniziertes Ziel dabei war es, den Komfort für die NutzerInnen zu erhöhen und den Prozess der Beschriftung oder „Markierung“ von Freunden und Bekannten, die auf im Netzwerk veröffentlichten Fotos erscheinen, zu beschleunigen. Andere Akteure wie etwa PimEye und Clearview[3] haben andere Ziele und sehen in der anlasslosen Analyse von Milliarden von frei verfügbaren Bildern im Netz ein Geschäftsmodell (Schaber et al. 2020).

Ein wesentlicher Sprung in der Genauigkeit wird erwartet, sobald 3D-Bilder von Gesichtern verfügbar sein werden (Kuusi and Vasamo 2014). Zudem sind für die nahe Zukunft auch Fortschritte in der Verbindung von Informations- und Kommunikationstechnologien und genetischen Informationen absehbar, die wahrscheinliche Bilder von Gesichtern konstruieren können sollen. Wenn genetische Informationen aus einer menschlichen Zelle mit einer umfangreichen Gesichtserkennungsdatenbank kombiniert werden, kann diese Art von Software mögliche Gesichter der Person, zu der die Zelle gehört, vorschlagen.[4] Der umgekehrte Fall, aus zwei Bildern auf genetische Verwandtschaft bzw. Zugehörigkeit zu schließen, wird be-

[1] derstandard.at/story/2000118416980/polizei-von-detroit-gesichtserkennung-liegt-in-96-prozent-der-faelle-falsch.

[2] futurezone.at/digital-life/facebook-analysierte-35-milliarden-instagram-fotos-ohne-wissen-der-user/400031245.

[3] pimeyes.com/en und clearview.ai.

[4] theconversation.com/dna-facial-prediction-could-make-protecting-your-privacy-more-difficult-94740.

reits heute angeboten.[5] Diese Entwicklungen lassen Anwendungen im Sicherheits- und Überwachungsbereich entstehen, die die Detektion eines Menschen aufgrund von DNA-Spuren aus einer Menge heraus möglich machen werden. Dies führt insbesondere dazu, dass kritisch hinterfragt werden sollte, ob durch derzeitige Methoden der Anonymisierung genetischer Daten die Anonymität tatsächlich aufrechterhalten werden kann (siehe Thema „Digitalisierung und Anonymität"). Für das Parlament stellt sich die Frage, wie mit neuen Technologien umgegangen werden soll.[6] Wie können BürgerInnen vor Missbrauch geschützt werden? Und wie soll im Angesicht versprochener sicherheitspolitischer Zugewinne und dem demokratiepolitisch notwendigen und grundrechtlichen zugesicherten Recht auf Privatsphäre der Einsatz derartiger Technologien im Bereich der inneren Sicherheit geregelt werden?

Zitierte Quellen

Kuusi, O. und A.-L. Vasamo (2014). 100 opportunities for Finland and the world. Helsinki, Committee for the Future.

Schaber, F., Strauß, S. und Peissl, W. (ITA), 2020, *Der Körper als Schlüssel? – Biometrische Methoden für Konsument*innen*, November 2020, Wien: Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften epub.oeaw.ac.at/ita/ita-projektberichte/2020-03.pdf.

[5] faceitdna.com.

[6] amnesty.at/mitmachen/actions/schluss-mit-gesichtserkennung/.