Gesichtserkennung und KI

Informationsblatt

Hier sind einige der Hauptgründe für die Fehleranfälligkeit der Gesichtserkennung:

- Variationen in den Aufnahmen: Gesichtserkennungsalgorithmen können durch Variationen in Beleuchtung, Blickwinkel, Auflösung und Qualität der Bilder beeinträchtigt werden. Wenn die Bedingungen nicht optimal sind, kann dies zu Fehlern bei der Identifizierung führen.
- Verdeckung und Verkleidung: Wenn Teile des Gesichts verdeckt sind, zum Beispiel durch Brillen, Schals, Masken oder Kopfbedeckungen, kann die Gesichtserkennung beeinträchtigt werden. Verkleidungen können die eindeutigen Merkmale des Gesichts verschleiern und zu Fehlern bei der Identifizierung führen.
- Ähnlichkeit zwischen Personen: Manchmal können Menschen ähnliche Gesichtsmerkmale haben, zum Beispiel wenn sie verwandt sind (insbesondere eineiige Zwillinge). In solchen Fällen kann die Gesichtserkennung Schwierigkeiten haben, eine genaue Unterscheidung zwischen ihnen vorzunehmen.
- Veränderungen im Erscheinungsbild: Veränderungen im Aussehen einer Person wie Alterung, Gewichtszunahme oder -abnahme, Veränderung der Frisur oder des Bartstils können dazu führen, dass die Gesichtserkennung die Person nicht korrekt identifiziert.
- Voreingenommenheit und Diskriminierung: Gesichtserkennungssysteme können durch inhärente Voreingenommenheiten und Diskriminierung verzerrt sein. Wenn die Trainingsdaten nicht repräsentativ sind oder systematische Ungleichheiten in der Datenerfassung auftreten, kann dies zu fehlerhaften oder unfair bevorzugten Ergebnissen führen. Zur Veranschaulichung von Diskriminierungen durch Künstliche Intelligenz empfiehlt sich das Video Wie Maschinen diskriminieren (https://vimeo.com/476084538)– Facial Recognition & the Matrix of Domination von Nushin Yazdani und José Rojas.

Können biometrische Daten gestohlen werden?

Ja. Das kann beispielsweise durch einen Hackerangriff geschehen, bei dem das Referenzmuster gestohlen wird. Biometrische Daten werden aber deutlich seltener entwendet als PINs und Kennwörter. Da gestohlene biometrische Daten auch nicht ohne Weiteres von jeder beliebigen unberechtigten Person verwendet werden können, gelten entsprechende Authentifizierungsmethoden als deutlich sicherer als etwa Passwörter. Der Vorteil kann im Fall eines Diebstahls jedoch zum Nachteil werden: Biometrische Daten sind invariabel; das heißt, wenn sie einmal entwendet und zweckentfremdet wurden, lassen sie sich nicht mehr verändern, sperren oder verbessern, wie es bei gestohlenen Passwörtern der Fall ist.

Quelle: https://www.onlinesicherheit.gv.at/Services/News/Biometrische-Gesichtserkennung.html

CC BY NC SA