Deepfakes

Die gefährliche Macht künstlicher Täuschung

Deepfakes:

- Sind mittels künstlicher Intelligenz erstellte Medieninhalte
- Erste Deepfake Welle über Reddit verbreitet

Technologie:

VISUELLE MEDIEN 	**AKUSTISCHE MEDIEN** 
GENERATIVE ADVERSARIAL NETWORKS bestehend aus einem Generator (erzeugt realistische Daten) und einem Diskriminator (unterscheidet echte von generierten Daten) werden in einem Wettbewerb miteinander trainiert, sodass der Generator immer bessere und täuschend echte Daten produziert.	**TEXT ZU SPRACHE – VERFAHREN** Nutzen eines akustischen Modells, das Sprachmerkmale vorhersagt, und eines Vocoders, der diese in Audiosignale umwandelt. Durch Deep Learning kann das System Stimmen imitieren, durch Erlernen der Stimmcharakteristika einer Person
AUTOENCODER bestehend aus einem Encoder (wandelt Eingabedaten in eine komprimierte Darstellung um) und einem Decoder (rekonstruiert daraus die ursprünglichen Daten), wobei das Modell lernt, wichtige Merkmale zu extrahieren und unwichtige Informationen zu verwerfen.	**IMITATIONSVERFAHREN** Analyse des Verhaltens, der Stimme oder des Erscheinungsbildes einer Person, um diese auf neue Situationen anzuwenden, sodass realistisch wirkende Nachbildungen entstehen.

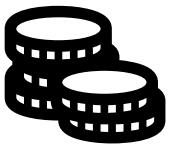
Open Source Tools:

- DeepFaceLab, Reface App, Faceswap App

Anwendung:

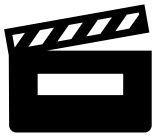
- Erstellung ist schnell, kostengünstig und massenhaft. Menschen haben eine grundsätzliche Neigung, emotional auf diese Medien zu reagieren.

➔ Deswegen gibt es zahlreiche Anwendungen der KI.



- Politik:
  - Verbreitung von Desinformation, Diskreditierung von Politikern, Einsatz in bewaffneten Konflikten, Manipulation von Wahlen

- Kriminalität:
  - Identitätsdiebstahl, Rufschädigung, Betrug, Täuschung von Sicherheitsvorkehrungen, Erpressung, …..



- Social Media und Filmbranche:
  - Kreativität
  - Unterhaltung durch z.B Memes
  - Einsatz in der Filmproduktion, z.B. Verjüngerungen, Effekte

Wie geht es weiter, und was können wir tun?:

Mit der Verbesserung der Technologie, werden auch Deepfakes immer realistischer und schwerer erkennbar

- Fehlerhafte Details am Körper
- Bildfehler, z.B. Beleuchtung, Schatten, …
- Unnatürliche Stimmen
- Unnatürliche Gestiken der Personen

Rechtliche Regelungen:

- Für den speziellen Fall „Deepfakes“ gibt es in Deutschland noch keine speziellen rechtlichen Regelungen. Stattdessen wird es durch Normen aus verschiedenen Rechtsgebieten erfasst (z.B. Recht am eigenen Bild, …)

Wichtigste Punkte der Debatte über die ethischen Aspekte von Deepfakes:

- Es ist NICHT moralisch vertretbar das Bild einer Person (egal ob Privatperson oder öffentliche Person) ohne deren Einwilligung in einem manipulierenden Kontext zu verwenden.
  - Auch wenn die Person einen öffentlichen Job hat, hat man nicht das Recht sie online diskreditieren oder lächerlich zu machen
  - Jede Person hat Gefühle und Deepfakes führen zu Verletzungen dieser
  - Deepfakes dringen in die Privatsphäre ein

- Deepfakes sollten TEILWEISE als kreative Freiheit und nicht als Verstoß gegen das Persönlichkeitsrecht betrachtet werden
  - Wenn der Zweck des Deepfakes negative Folgen mit sich zieht => Totale Ablehnung des Deepfakes, z.B. kompromittierende Videos einer Person online
  - Wenn aber Zweck des Deepfakes: Unterhaltung, künstlerische Auslebung, usw. *UND* das Deepfake kenntlich gemacht wird mit „mit KI generiert“, dann ist es okay

- Deepfakes untergraben das Vertrauen in Medien und Informationen DEUTLICH
  - Man sollte Medieninhalte immer hinterfragen und im Hinterkopf haben, dass es sich um Deepfakes handeln kann
  - Unabhängig von Deepfakes sollte man aber online immer seinGehirn einschalten und nicht alles glauben was man liest, sondern lieber nochmal nachhaken

- Man sollte Deepfakes TROTZ ihres positiven Nutzens als gefährlich betrachten
  - Es gibt natürlich positive Aspekte die man nicht vergessen darf und die uns den Alltag erleichtern
  - *ABER*: oft wird so Schwachsinn verbreitet, der für eine große Menschenmenge zugänglich ist, auf welchen vor allem jüngere Nutzer reinfallen
  - Trotzdem sollte man positive/ negative Aspekte betrachten
  - Wichtig ist auch hier das man mitdenken muss und versuchen soll wahr von falsch zu unterscheiden um den positiven Nuten von Deepfakes überwiegen zu lassen

Quellen:

- https://www.bundesregierung.de/breg-de/aktuelles/was-sind-deep-fakes-2230226
- https://optimit.de/blog/deepfakes-grundlagen-und-hintergruende-die-jeder-kennen-sollte
- https://www.heise.de/hintergrund/Deepfakes-KI-gegen-KI-9339715.html
- https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes.html
- https://www.thedeepfake.report/stories/history-of-fake
- https://www.swp-berlin.org/10.18449/2023A43/
- https://www.deutschlandfunk.de/ki-wahlen-manipulation-kuenstliche-intelligenz-fake-news-deepfakes-100.html
- https://www.welt.de/wirtschaft/webwelt/video195189665/Deepfake-Video-Mark-Zuckerberg-schwaermt-von-Weltherrschaft-verblueffend-echt.html
- https://www.bpb.de/lernen/bewegtbild-und-politische-bildung/556809/deepfakes-als-unterhaltung/
- https://www.pxl-vision.com/de/blog/deepfakes-und-identitaetsdiebstahl
- https://www.spiegel.de/netzwelt/netzpolitik/pentagon-fake-bild-von-explosion-sorgt-fuer-aufregung-a-d4510a09-07d6-4d63-b72d-2c3bf28b52a9
- https://x.com/kirkdborne/status/1367694004352081922