Fake Face ID und Cybercrime

Dr.-Ing. Sebastian Götz
Technische Universität Dresden - Fakultät Informatik

Software früher

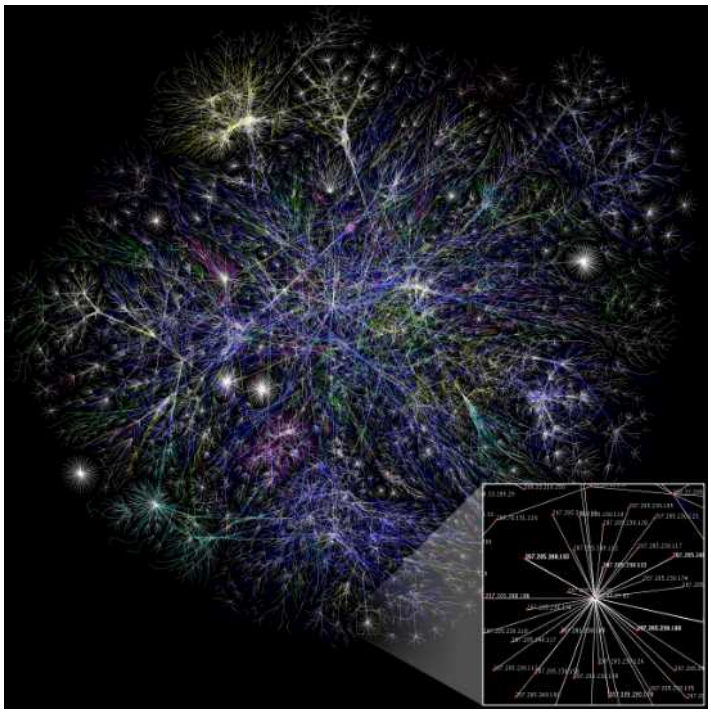
- Imperative Programmierung
- Für eine Eingabe kann genau nachvollzogen werden, was passiert und warum.

© Lawrence Livermore National Laboratory

Rasanter Technologischer Wandel

Stufe 1: Das Internet

- Modems
- „Geh bitte aus dem Internet, ich will telefonieren“
- Software läuft nicht mehr nur auf einem PC sondern wird vernetzt



(CC BY 2.5)

Stufe 2: Mobiltelefone:

- Software muss aktuelle Umgebungsbedingungen beachten (z.B. Helligkeit)
-

Nokia 101 (1992) [CC-BY-4.0, Santeri Viinamäki] vs. Android Smartphones [CC-BY-2.5, Google]

Stufe 3: Mobiles Internet

- Früher: „Ausversehen den Internetknopf drücken wird teuer“
- Heute: „immer online“

© pixabay.com

Stufe 4: Web 2.0

- Früher: Inhalte nur vom Betreiber
- Heute: Inhalte im Internet werden von den Nutzern erstellt (Youtube, Facebook, etc.)

© pixabay.com

Stufe 5: Internet of Things

- Früher: PC, Laptop, Smartphone mit Internetverbindung
- Heute: Kaffeemaschine, Lampen, Smart Watch, Kühlschrank, Waschmaschine mit Internetverbindung

© pixabay.com

Konsequenz 1: Software ist überall!

Konsequenz 2: Wir sind uns nicht mehr bewusst, welche Informationen von uns wir der Software offenbaren.

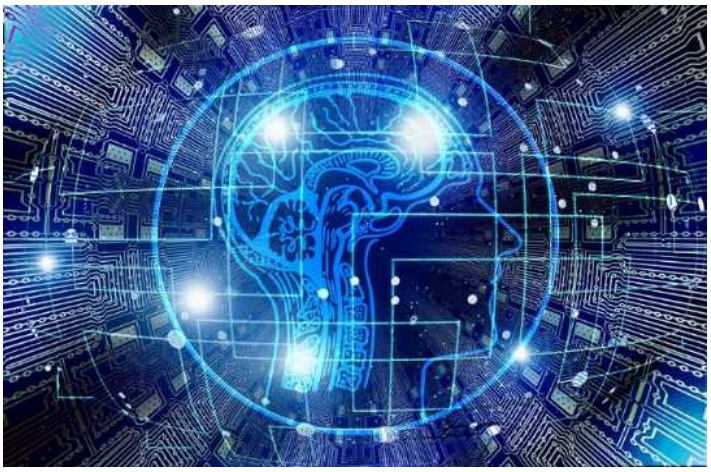
- Beispiel: „Alexa, bitte spiele meine Lieblingsmusik!“
- Alexa weiß / kann ableiten:
  - wann man zuhause ist
  - ob man alleine ist
  - in welcher Stimmung man ist
  - und vieles mehr

© pixabay.com

Soziale Arbeit muss bei ihren Klienten ein Bewusstsein für private Daten im digitalen Zeitalter schaffen.

Software heute: künstliche Intelligenz

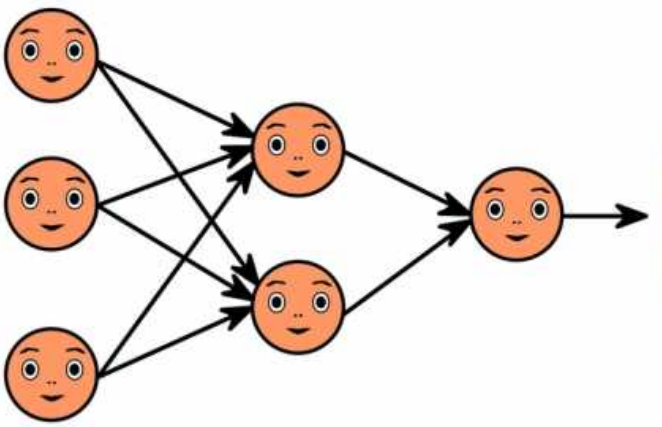
- Für eine Eingabe ist nicht mehr nachvollziehbar was passiert und warum!
- Warum ist das so?
  - Software wird nicht mehr geschrieben
  - Software entsteht durch Beobachtung und Imitation!



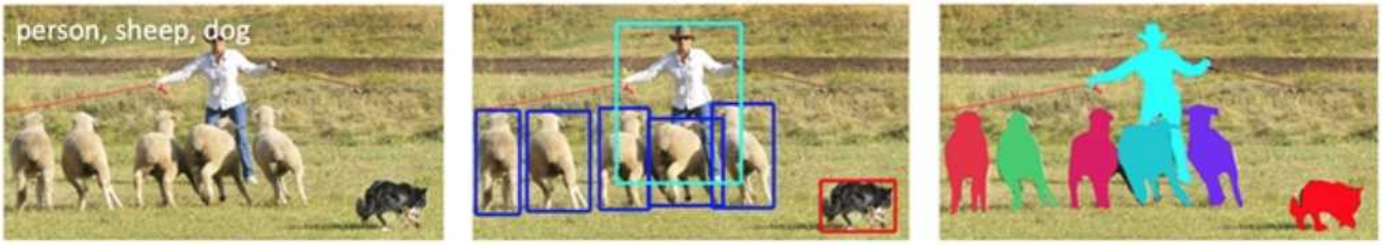
Software heute: neuronale Netze

- Heutige Software ist dem menschlichen Gehirn nachempfunden

© pixabay.com



© pixabay.com



2 grundlegende Arten von neuronalen Netzen werden unterschieden

1. Diskriminative Netze zur Klassifikation (siehe oben)
   - z.B.: Auf Facebook.com mit Firefox: Rechtsklick auf ein Bild -> Google Suche nach „Bild könnte enthalten …“

Bild/Video/Ton/Text → Text (Metadaten)

2. Generative Netze
   - Probiere selbst: http://nvidia-research-mingyuli-u.com/gaugan

Text (Metadaten) → Bild/Video/Ton/Text

- Software lernt durch Beobachtung
- Durch die fortschreitende Vernetzung bieten wir der Software immer mehr Daten
- Was die Software tut ist für Menschen nicht mehr nachvollziehbar
  - Jede Entscheidung/Handlung beruht nur noch auf Zahlen
- Unser Verhalten wird zukünftig immer stärker imitiert

Was heute bereits möglich ist:
- Romane generieren
- Videos von Menschen generieren

Bilder generieren, die von Fotos nicht zu unterscheiden sind

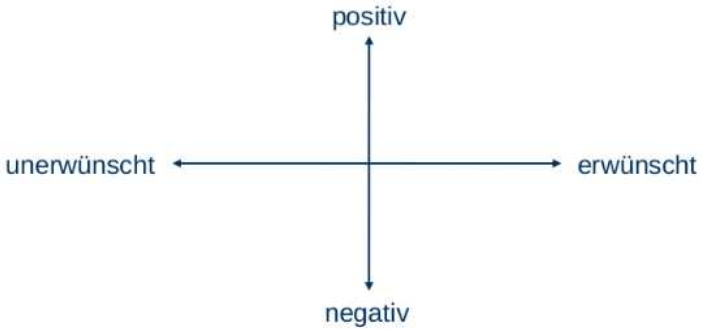
© http://whichfaceisreal.com/

Frage danach, welches der beiden Bilder echt ist und welches generiert?
→ Abstimmung im Chat
manche sagen rechts ist echt& andere links
Antwort: Rechts ist das echte Bild und links ist generiert

- Stimmen generieren: https://spik.ai/
- Bilder generieren: https://experiments.runwayml.com/generative_engine/

Emergenz

- Problem: Emergenz
- Software tut nicht mehr das, was wir ihr vorschreiben
- Durch das Zusammenspiel von Menschen und Technik entsteht Verhalten, dass nicht vorhersagbar ist, d.h. nicht direkt auf das Verhalten der einzelnen Teile (Menschen, Systeme) zurückzuführen ist.



Emergenz: Beispiel

- Youtube schlägt Videos vor, die man vermutlich sehen will („Recommender System“)
- Dazu beobachtet Youtube, welche Videos man sich anSchaut
  Erwünschtes Ziel: hohe Nutzerzufriedenheit, lange Verweildauer
  Unerwünschter Nebeneffekt:
  - Der Algorithmus lernt, dass Menschen immer extremere Inhalte sehen wollen
  - Er lernt auch, dass Menschen, die extreme Inhalte sehen, leichter vorhersagbar sind
  - Der Algorithmus extremisiert den Nutzer (durch eine sich zuspitzende Informationsblase)

Potentiale und Herausforderungen

- Die Medienkompetenz aller muss deutlich verbessert werden
  - Welche Informationen von uns und unserer Umwelt stellen wir Software zur Verfügung?
  - Welche Folgen hat die Nutzung von Technik für den Einzelnen? (Facebook, Youtube, …)
  - Wie erkennt man eine (sich zuspitzende) Informationsblase?
  - Wie kann man selbst für positive, erwünschte Emergenz sorgen? (konstruktive Herangehensweise)
  - Wie kann man unerwünschte, negative Emergenz vermeiden?

Voraussetzung:

- grundlegendes Verständnis verfügbarer Informationstechnologie
- Wissen über den kapitalistischen Hintergrund

Software ist nur scheinbar kostenlos.
Wir bezahlen mit unseren Daten.

Fragerunde:

Nachfrage zu positiv erwünschter Emergenz, als fruchtbare Schnittstelle zw. Informatik und SoA? Wie ist das möglich?
Szenarien durchspielen, die durch das Benutzen der Software entstehen

- komplexere Simultationen nachstellen

Bsp.: Youtube, bevor man es der Öffentlichkeit vorstellt simmulieren um herauszufinden was für emergentes Verhalten in der Software steckt

- um sich davor zu Schützen müssen ethische Schranken eingebaut werden
- gewisse Grundregeln und Grundbedingungen in Software mit einbinden

Bsp: Computer darf keinen Menschen schaden, was darf das System und wo sind die Grenzen der KI?
KI könnte Barieren ausschalten, um das zu umgehen gibt es einen relativ neuen Ansatz:

- vorgeben von Zielen ist eigentlich falsch
- das heutige Ziel kann in 10 Jahren durchaus angepasst werden
- Ungenauigkeit, die der Mensch der Software geben hat, unter der Anleitung der Menschen

→ Schutz vor negativer Emergenz
Literaturtipp: Stuart Russell "Human Compatible"
Philipp: Thema Daten
Daten haben keinen richtigen Wert
Verständnis dafür zu haben oder zu entwickeln, wie viel Wert haben denn die Daten die ich Preis gebe?
Was schadet es mir oder der Gesellschaft wenn ich diese Daten preisgebe?
Aufgrund von fehlendem Wissen vielleicht?
Wert kann man teilweise erfragen, Bsp.: Krankenkasse: was kostet mein/der Datensatz?

Daten haben nicht immer zwangsläufig negativen Einfluss
Bsp.: Google: Dienste kpönnen nur sinnvoll genutzt werden, indem sie von vielen Nutzern genutzt werden
-->Restaurantempfehlungen als Bsp.

- für alle wertvolles Tool, egal ob man bewertet hat oder nicht
- 2 Dinge möglich:
  1. Google verdient damit viel Geld, während man selbst nichts davon hat
  2. Google hat die Daten & könnte entscheiden diese nicht mehr kostenlos anzubieten, oder diese zu manipulieren ohne das man selbst einen Einfluss hat auch wenn man etwas bewertet hat
- kann schnell ins Gegenteil umkippen

man kann nie sicher sein, das mit den Daten das passiert was man will
Durch Bezahlung besseres ranking?
Es gibt mittlerweile Onlinekurse, wie man Webpräsenz am besten zu erstellen hat, um möglichst weit oben zu landen bei einer Googlesuche
je mehr Daten ausgewertet werden und das Ergebnis zur Verfügung gestellt wird, umso schwerer ist es einen Überblick zu behalten
immer mehrere positive und negative Aspekte
Google kann bspw. suchanfragen verwenden:

- In welchen Regionen sind Zahnbürsten für Kinder besonders beliebt? → Wissen an Industrie weitergeben → google kann Analyseergebnisse verkaufen und die jeweiligen gezielten Regionen weitergeben, also wo ist die Nachfrage besonders groß?
- man selbst stellt Daten zur Verfügung
- Klarheit was daraus abgeleitet wird muss nicht zwingend der Realität entsprechen

Was sind deine und meine Daten wert? Unterschiede gibt es ja auch zwischen europäischen oder asiatischen Menschen zusätzliche Diskussion nötig: Was heißt das für Jugendliche? Was sind deren Daten wert?
deren Daten werden ihnen wieder angeboten, in Form von Produkten können wiederrum die persönlichkeit formen und der Indentitätsentwicklung beitragen.
Müssen aufmerksamer werden diesbezüglich!
Forschung, dass das immer extremer wird, wie bei Youtube immer extremere Beispiele werden angezeigt
Wie ist das Gegenbeispiel der Kochkurse da gemeint?
Es gibt wenig gegenbeispiele
Beim kochen schaut sich jemand normale Rezepte an, sobald vegetarische Gerichte gesucht werden, wird der Algorythmus als nächstes vegane Rezepte anzeigen und so weiter → youtube algorythmus hat sich dementsprechend angepasst, um immer konkretere Sachen zu finden
Welches Gesicht ist echt und welches ist generiert?
an gewissen Kriterien kann man es schon erkennen, man muss aber genau hinschauen
Anekdote: Captures → Frage ob man ein Roboter ist
Kachelbilder auswählen, auf denen Beispielsweise Ampeln zu finden sind neuronales Netz wird trainiert für den Hersteller im Endeffekt weiß es der Computer besser

Danke an alle :)

Links aus dem Chat von BBB:

http://nvidia-research-mingyuliu.com/gaugan/

Kurioser Input - Microsoft hatte mal einen Twitter-Bot mit KI gebaut. Nach 16 Stunden musst er deaktiviert werden, weil er rassistische Posts veröffentlicht hat:
https://en.wikipedia.org/wiki/Tay_(bot)

https://www.amazon.de/Human-Compatible-AI-Problem-Control/dp/0241335205

falls mal jemand generierte bilder braucht:
https://thispersondoesnotexist.com/

Sollte es weitere Beispiele wie Captcha geben, bitte gern dokumentieren :-)

https://addons.mozilla.org/en-US/firefox/addon/buster-captcha-solver/

LET‘S PLAY SMARTE JUGENDARBEIT II

04./05.05.2020 auf wechange.org

Tagungsdokumentation

SLJ
SÄCHSISCHE LANDJUGEND E.V.

Herausgeberin:

Sächsische Landjugend e.V.
März 2021

Leitungs- und Koordinierungsstelle
Sächsische Landjugend e.V.
Unterer Kreuzweg 6
01097 Dresden

buero@landjugend-sachsen.de

https://landjugend-sachsen.de

Redaktion, Satz und Layout:
Christian Hager

mit Dank an folgende Personen, ohne die diese Dokumentation nicht möglich gewesen wäre:
Tom Pannwitt (SJR Leipzig) für die Aufarbeitung der Chats, Markus Kollotzek (WECHANGE.org) ohne den es kein Tagungshaus gegeben hätte; Arne Vogelgesang (internil) für den Zusatzeinsatz; Monique Lepom und Konstanze Großmann für die ganzen Transkripte und Protokolle

SACHSEN Die Sächsische Landjugend e.V. wird mitfinanziert durch Steuermittel auf der Grundlage des von den weiblichen, männlichen und diversen Abgeordneten des Sächsischen Landtages beschlossenen Haushaltes