Maschinelles Lernen

Am Beispiel der Gesichtserkennung wird deutlich, welche Möglichkeiten maschinelles Lernen bietet und welche Risiken sich dabei ergeben können.

Unter dem maschinellen Lernen versteht man Technologien, mit deren Hilfe Computersysteme Wissen durch Erfahrung sammeln können. Grundlage des Lernprozesses sind große Datenmengen, die als Trainingsmaterial dienen und über statistische Methoden ausgewertet werden.

Hinter maschinellem Lernen stehen mathematische Modelle und bestimmte Algorithmen, die sich für verschiedene Anwendungsfälle verwenden lassen. Die Modelle selbst werden von Mathematikern entwickelt und von Datenspezialisten (Data-Scientists) angewendet und angepasst. Diese Algorithmen werden in Computer-Programmen eingesetzt, die dank dieser Algorithmen Bewertungen und Entscheidungen aufgrund von Trainingsdaten liefern können.

Die Ergebnisse haben immer die Qualität von statistischen Aussagen, beispielsweise ein Maß an Zuverlässigkeit – ausgedrückt als eine Wahrscheinlichkeit. Diese kann beispielsweise bei Gesichtserkennung (mittels neuronaler Netze) zwischen 20 und über 90 Prozent liegen, abhängig von der Einsatzweise, den Vorgaben, dem Lernmaterial und der Qualität der Bilder, die die zu erkennenden Gesichter enthalten.

Welche Algorithmen haben für maschinelles Lernen Bedeutung? Viele Algorithmen, die für maschinelles Lernen verwendet werden, stammen aus der Statistik. Ein Beispiel dafür sind Algorithmen der Regressionsanalyse: Zusammenhänge zwischen unterschiedlichen

Gesichtserkennung: Merkmale wie Abstände, Flächen, Winkel werden erkannt und mit Bildpunkten vermessen.

Parametern werden durch Regressionsanalyse gefunden und für Vorhersagen verwendet. Dadurch können beispielsweise aus Daten über Werbeinvestitionen Aussagen über Verkaufszahlen getroffen werden. Kundenverhalten in Geschäften oder auf Webseiten lässt auf deren weiteres Kaufverhalten schließen, in Folge können Anbieter Maßnahmen treffen, um Kunden zu beeinflussen. Ausschlaggebend ist, dass Zusammenhänge erkennbar werden und dadurch Schlüsse möglich werden.

Genau dazu dienen die großen Datenmengen, die *Google* oder *Amazon* sammeln. Andere Algorithmen verwenden Entscheidungsbäume, die aber nicht unveränderlich sind, sondern sich an die Daten anpassen können. Dabei ist es auch möglich, dass verschiedene Entscheidungsbäume zugleich und unabhängig voneinander durchlaufen werden.

Wie funktionieren neuronale Netzwerke? Neuronale Netze verwenden Mechanismen, die in Nervensystemen entdeckt wurden, beispielsweise in den Leiterbahnen unseres Sehsystems. Dabei werden die Inputs (Reize einzelner Sehzellen) durch Vernetzung mehrerer Ebenen von Nervenzellen verändert, um bestimmte Arten von Reizen hervorzuheben und eine Filterung durchzuführen.

Digitale neuronale Netze müssen lernen, um verwendbar zu sein. Die Inputsignale werden dabei durch vernetzte Filterschichten geschickt und die Gewichtungen (Filterstärke, positive oder negative Wirkung) schrittweise solange angepasst, bis das neuronale Netz die Lernbeispiele richtig erkennen kann.

Speziell bei neuronalen Netzen mit vielen Schichten ist die genaue Funktionsweise nicht unmittelbar nachvollziehbar. Neuronale Netze können wie andere Modelle des maschinellen Lernens auch falsch angelernt werden oder auch eine Überanpassung erfahren (Overfitting). Dabei wird die Prognose zu sehr an die Lerndaten angepasst und kann nicht mehr allgemeingültig verwendet werden. Ein gutes Lernmodell kann nie hundertprozentige Sicherheit in der Aussage erreichen, das wäre ein Zeichen der Überanpassung.

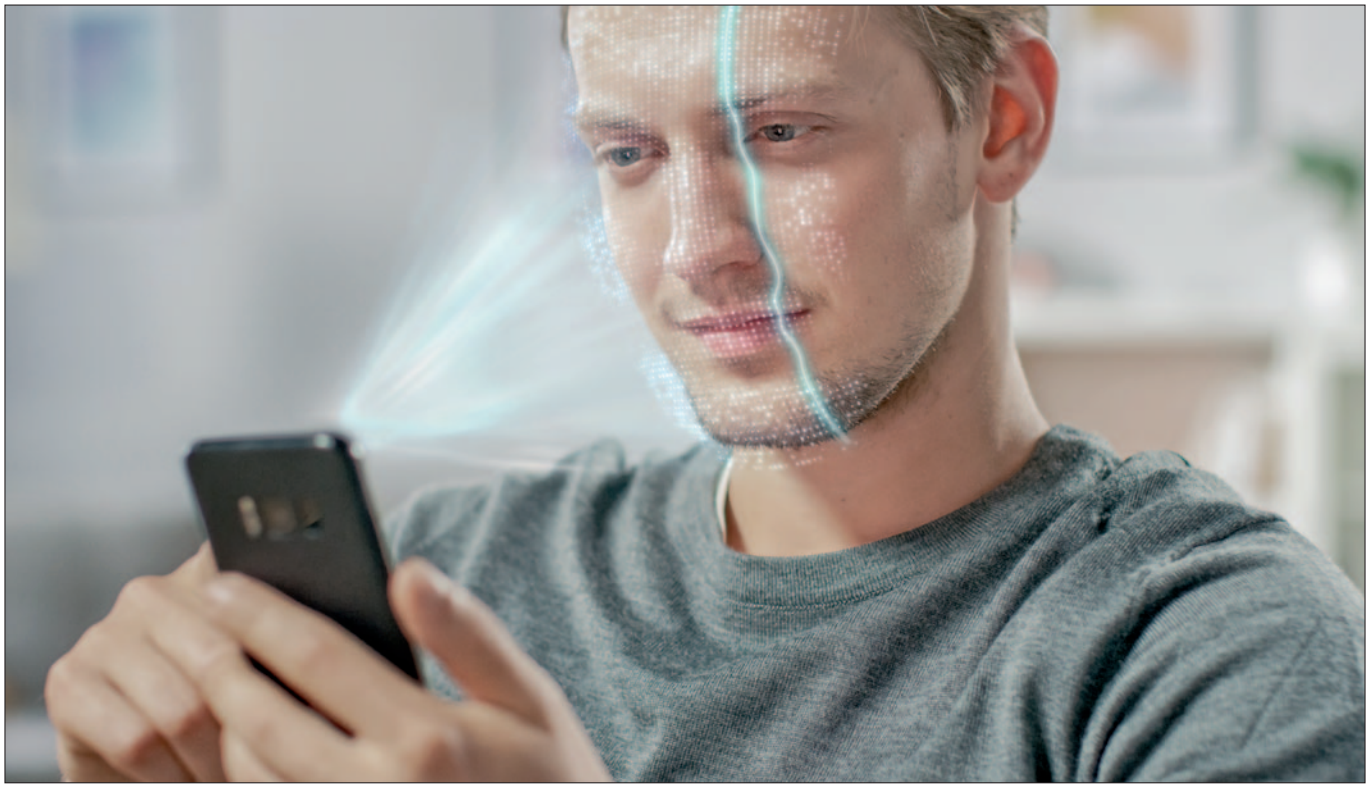
Wie funktioniert Gesichtserkennung? Es gibt verschiedene Modelle für die Aufgabe der Gesichtserkennung. Diese unterscheiden sich einerseits nach den Anwendungsgebieten, andererseits auch grundsätzlich nach der Technologie. Ältere Systeme nutzten 2D-Analyse: Dies funktioniert am besten mit Fotos, die idealerweise unter definierten Bedingungen aufgenommen werden. Die Richtlinien für die EU-Passfotos berücksichtigen dies. Manche Systeme verwenden eine Analyse der Bildpunkte. Diese Systeme lassen sich durch Bildmanipulationen, die für das menschliche Auge unsichtbar bleiben, komplett verwirren. Andere Systeme identifizieren die Topografie des Gesichts und vermessen die genauen geometrischen Daten. Diese Art von Systemen ist heute zuverlässig, können schwerer überlistet werden, benötigen dennoch zuverlässige Aufnahmen aus geeigneten Richtungen.

3D-Gesichtserkennung verwendet beispielsweise Streifenlichtprojektion, um die räumliche Lage und Beziehung von Kennzeichen genau zu analysieren. 3D-Analyse kann Gesichter auch aus unterschiedlichen Richtungen besser identifizieren, war aber ursprünglich nicht so zuverlässig, wie die älteren 2D-Systeme.

Wie lässt sich Overfitting vermeiden? – Die Bedeutung von Lern- und Testdaten.

Maschinelles Lernen geschieht in Form eines schrittweisen, wiederholenden (iterativen) Prozesses. Die Prognose des Systems wird dabei immer mit den tatsächlichen Ergebnissen verglichen. Für eine bestimmte, abgeschlossene Menge an Daten kann das System nahezu beliebig genau trainiert werden, wenn das das Modell zulässt – also beispielsweise mit einem neuronalen Netz. Deshalb ist es nötig, dass zur Verifizierung andere Daten als die Lerndaten verwendet wer-

FOTO: RA2 STUDIO/STOCK.ADOBE.COM



Gesichtserkennung: Lichtpunkte oder -balken werden auf das Gesicht projiziert, um sicherzustellen, dass es sich um ein echtes Gesicht und nicht nur um ein zweidimensionales Abbild handelt.

FOTO: GORODENKOFF/STOCK.ADOBE.COM

den. Der Verifizierungsprozess ist auch Teil der Iteration. Wenn also sehr viele Lernvorgänge in einem neuronalen Netz durchlaufen werden, kann auch eine Anpassung an die Verifizierungsdaten passieren. Deshalb werden drei Datensammlungen verwendet, beziehungsweise die vorhandenen Daten in drei Töpfe gegeben: Topf 1: die eigentlichen Lerndaten, Topf 2: die Verifizierungsdaten, Topf 3: Testdaten, die am Ende des Lernprozesses verwendet werden, um die Zuverlässigkeit mit noch nicht verwendeten Daten zu überprüfen.

Die meisten Gesichtserkennungssysteme leiden unter dem Problem ungenügender Lerndaten. Es wurde festgestellt, dass so gut wie alle Gesichtserkennungssysteme große Unterschiede in der Erkennungsrate, abhängig von Geschlecht und Hautfarbe, aufweisen: Weiße Männer werden am besten erkannt, schwarze Frauen am schlechtesten. Dies ist direkt auf die Verfügbarkeit von Lerndaten zurückzuführen. Nachdem Joy Buolamwini, eine US-amerikanische Wissenschaftlerin am MIT, Boston, dies im Jahr 2018 nachwies, haben einige Firmen – *IBM, Microsoft* und *Face++* ihre Software wesentlich verbessert, andere hingegen nicht: *Google* etwa, das noch immer Afroamerikaner als Gorillas identifiziert hat, oder *Amazon,* das seine Gesichtserkennung an US-Polizeibehörden verkauft, trotz einer Fehlerquote von mehr als 20 Prozent bei Frauen mit dunkler Haut.[1]

Problematische Aspekte der Gesichtserkennung. Gesichtserkennung wird auf verschiedene Weise missbraucht. Eines der zuverlässigsten Systeme zur Gesichtserkennung ist in Russland verfügbar und kann von jedem benützt werden: *NTechLab* hat *FindFace.ru* entwickelt, das sich als erweiterte Dating-App versteht – anhand eines Fotos einer Person lässt sich diese ausfindig machen, indem sämtliche sozialen Netzwerke nach der Person durchsucht werden. Die App dient damit dem Stalking, aber auch, um beispielsweise Schauspieler in Hardcore Pornos zu outen und an den Pranger zu stellen. In den USA sammeln Unternehmen in Zusammenarbeit mit den Behörden Gesichtsdaten. Es wurde bereits 2016 bekannt, dass das FBI auf nicht näher bestimmte Weise so eine Datenbank von 117 Millionen Personen aufgebaut hat.[2] Ein Nebeneffekt der Gesichtserkennung ist die Möglichkeit für „Deep Fakes“: Durch das Know-how der Gesichtsanalyse und Synthese lassen sich künstliche Gesichter erzeugen. Dabei können Gesichtsdaten aus Fotos mit gefilmten Personen verknüpft werden, oder in Echtzeit fabrizierte gefälschte Filme erzeugt werden, etwa für gefälschte Interviews.[3] Es gibt auch humoristische Beispiele dafür, wenn auch nicht in Echtzeit erzeugt, wie Jim Meskimens „A Deeper Look Into The Life Of An Impressionist“, auf *Youtube* verfügbar.[4]

In der nächsten Folge geht es um die Frage, ob Big Data und maschinelles Lernen mit dem Datenschutz – Stichwort DSGVO – in Einklang gebracht werden kann.

Michael Werzowa

Der Autor ist Experte für Netzwerk- und Datensicherheit, Vorstand der IoT Austria – The Austrian Internet of Things Network.

Anmerkungen:

[1]https://netzpolitik.org/gesichtserkennung-kritik-macht-algorithmen-genauer-nicht-nur-fuer-weisse-maenner/

[2]Lily Hay Newman: „Cops have a database of 117M faces. You're probably in it“, Wired, 18.10.2016

[3]www.lvz.de/Nachrichten/Digital/Wie-Algorithmen-unsere-Gesichter-auslesen

[4]https://youtu.be/5rPKeUXjEvE.