

BUZZWORD

#FightClub



Ende der 1990er-Jahre kam der Film „Fight Club“ mit Brad Pitt und Edward Norton in die Kinos, in dem sich – das ist kein Spoiler – die beiden regelmäßig treffen, um sich im fairen Faustkampf zu vermöbeln.

Es dauerte nicht lange, da fanden auch in der Realität englische Banker diese Idee ganz cool und trafen sich abends öffentlichkeitswirksam zur stümperhaften Prügelei im Amateuring. Die Idee dahinter: Wer blutet und Schmerz empfindet, der fühlt sich lebendig – oder wie Brad Pitt. Es war ein klassischer Fall von „life imitates art“ – das Leben imitiert die Kunst.

Fast 30 Jahre später imitiert nun die Kunst das Leben. Oder noch genauer: Das Leben imitiert mithilfe der Kunst das Leben, das einst die Kunst imitierte (die auf einem Buch von Chuck Palahniuk basiert). Vereinfacht gesagt: Es gibt also wieder Fight Clubs. Allerdings nicht in der harten Realität, sondern innerhalb der virtuellen Grenzen des Computerspiels „Red Dead Redemption 2“. Die riesige Westernwelt bietet eigentlich auch so genug Haue, aber den Spielern reicht das Angebot wohl nicht. Deshalb verabreden sich mittlerweile jede Menge Leute in düsteren Saloons und Scheunen zum Schlagabtausch, der jedoch nach klaren Regeln ablaufen muss. So dürfen beispielsweise immer nur zwei Leute gleichzeitig in den Ring steigen und auch keine Heiltränke verwendet werden. Außerdem müssen männliche Avatare mit nacktem Oberkörper antreten. Brad Pitt lässt grüßen.

Wer sich nicht an die Regeln hält, der wird schon mal erschossen. Aber natürlich nicht in echt. Und genau an diesem Punkt kommt man ins Grübeln, denn eigentlich ist ja überhaupt nichts echt bei diesen Fight Clubs in „Red Dead Redemption 2“. Doch an dieser Stelle schließt sich der Kreis. Schließlich geht es auch im Film „Fight Club“ – Achtung, jetzt kommt doch ein Spoiler – um die Frage, was eigentlich real ist und was nicht. Wahnsinn, wie viel Metalebene in einem Computerspiel existieren kann. In echt jetzt.

Denis Krick

APP & GADGET

Diese Apps schützen vor Datenklau

Wenn möglich, sollten Onlinekonten mit Zwei-Faktor-Authentifizierung (2FA) geschützt werden. Dieser zusätzlich zum Passwort abgefragte Sicherheitscode erhöht den Schutz vor Betrug, berichtet die „PC Go“ (1/2019). Onlineanbieter wie Google, Facebook oder Amazon unterstützen etwa die 2FA über Smartphone-Apps wie den Google Authenticator, Authy, Lastpass oder den Microsoft Authenticator. Sie werden mit dem eigenen Konto verknüpft und zeigen regelmäßig einen neuen Sicherheitscode an, der bei der Anmeldung nach dem Passwort eingegeben wird.

Kaktus für doppeltes Hörvergnügen

Wenn man schon nicht miteinander reden will, dann doch wenigstens zusammen Musik hören: Dieser kleine Kaktus Audio Splitter macht es möglich. Er wird per Klinkenstecker an die Audiobuchse angeschlossen. An seinen Armen ist für zwei Kopfhörer Platz. Wenn er seinen Dienst getan hat, wird er zurück in den Topf gesteckt. Dieser kann am Schlüsselbund befestigt werden.

Info Gesehen bei radbag.de für 11,95 Euro.

Wenn Obama Trump zum Idioten macht

Mithilfe von künstlicher Intelligenz lassen sich bald täuschend echte Videos produzieren. Das könnte die Filmindustrie revolutionieren. Aber was passiert, wenn jeder die Realität verfälschen kann?

Von Anna Schughart

Die Situation ist ernst. Im Mission-Control-Center sucht die Nasa fieberhaft nach einer Lösung, um die Besatzung von „Apollo 13“ sicher zur Erde zurückzubringen. Ein Problem: Die eckigen CO₂-Filter der Raumfähre passen nicht auf die runden Buchsen der Landefähre. „Tja, dann schlage ich vor, Gentleman, dass wir lernen, ein eckiges Schwein durch ein rundes Loch zu schieben“, sagt der Flugdirektor, im Film „Apollo 13“ gespielt von Ed Harris. Ein eckiges Schwein? Soll das ein Witz sein, Galgenhumor? Nein, es ist ein Übersetzungsfehler. Statt „peg“ für „Stöpsel“ haben die Übersetzer offensichtlich „pig“ (also Schwein) verstanden.

Synchronisationen von Filmen haben oft einen schlechten Ruf. Dabei sind sie wirklich nicht einfach. Nicht nur, weil Missverständnisse entstehen können – sondern auch technisch gesehen. Besonders schwierig ist die Lippen synchronisation, also der Moment, wenn man das Gesicht eines Schauspielers sehen kann, er aber statt Englisch plötzlich Deutsch reden soll. Denn natürlich sieht ein Mund anders aus, wenn er gerade „tree“ statt „Baum“ sagt. Doch wenn die Synchronisation nicht überzeugt, dann ist die Illusion eines Films schnell dahin.

Der Mund passt sich an das Gesagte an

In Zukunft könnte es deutlich einfacher werden, Filme zu synchronisieren. Denn Wissenschaftler des Max-Planck-Instituts für Informatik in Saarbrücken haben eine Möglichkeit gefunden, die Mundbewegung und sogar den kompletten Gesichtsausdruck eines Schauspielers in einer Filmaufnahme zu verändern. Statt zu versuchen, die Übersetzung möglichst genau an die Mundbewegungen anzugleichen, könnte man damit einfach die Mundbewegungen an die Übersetzung anpassen.

Dazu nutzen die Forscher die Hilfe einer künstlichen Intelligenz (KI). Bei der Aufnahme im Studio werden der Synchronsprecher und seine Mimik als dreidimensionales Modell aufgezeichnet. Die Bewegungen überträgt die KI dann auf das Gesicht des Schauspielers. Der Synchronsprecher kann also quasi die Gesichtsbewegungen des Schauspielers kontrollieren. Die Technik passt sogar die Kopfhaltung, den Blick und das Augenzwinkern an.

Nicht nur in Filmen könnten die sogenannten „Deep Video Portraits“ zum Einsatz kommen, sondern auch bei Videokonferenzen – oder in der Postproduktion. Dem Max-Planck-Institut ist es allerdings sehr wichtig zu betonen, dass die Forscher dort ernsthafte Grundlagenforschung betreiben. Mit dem, was man über mögliche Missbräuche oder gar „Deepfakes“ in der Vergangenheit lesen konnte, will man auf keinen Fall assoziiert werden.

„Deepfakes“ produziert Pornos

Denn es ist wie so oft: Eine technische Neuerung kann so oder so verwendet werden. Tatsache ist: Mithilfe



Künstliche Intelligenzen können berühmten Politikern wie Barack Obama die Worte in den Mund legen.

FOTO: DPA, MONTAGE: RND

Das ist eine gefährliche Zeit.

Fake-Obama in einem Video des Portals „Buzzfeed“

von künstlicher Intelligenz ist es immer besser möglich, Menschen Wörter in den Mund zu legen, Videos auf eine Art zu manipulieren oder sogar von Grund auf zu erzeugen, die von echten Aufnahmen immer schlechter zu unterscheiden sind. Es ist na-

heliegend, dass damit auch Unheil angerichtet wird. Tatsächlich ist das Wort, das häufig synonym mit den neuen Möglichkeiten der Videomanipulation verwendet wird, das beste Beispiel genau dafür. Denn das Kofferwort „Deepfakes“ (von Deep Learning und Fake) ist gleichzeitig auch das Pseudonym eines Reddit-Nutzers, der 2017 mehrere Pornovideos ins Netz stellte. „Deepfakes“ hatte eine künstliche Intelligenz mittels Pornos und Filmen berühmter Schauspielerinnen trainiert. Auf den Videergebnissen waren die Gesichter von Promis wie Gal Gadot oder Emma Watson auf die Körper von Pornodarstellerinnen montiert worden. Die Videos waren schnell als unecht enttarnt. Aber was ist, wenn das irgendwann einmal nicht mehr so leicht ist?

Das Setting, der Gesichtsausdruck, die Stimme – alles stimmt. Doch dann sagt Barack Obama seltsame Sachen wie zum Beispiel, dass Donald Trump ein totaler Vollidiot sei. Oder das Killmonger – der Antagonist aus dem Film „Black Panther“ – Recht gehabt habe. Das Video, das Buzzfeed mit dem Schauspieler und Regisseur Jordan Peele im April veröffentlichte, verheimlicht nicht, dass darin nicht der echte Barack Obama spricht. Tatsächlich beginnt der Fake-Obama seine kurze Ansprache mit dem Hinweis, dass eine Ära anbreche, in der unsere Feinde jeden alles zu jeder Zeit sagen lassen können. „Das ist eine gefährliche Zeit. In Zukunft müssen wir wachsamer sein, welchen Inhalten wir aus dem Internet vertrauen“, warnt deshalb der falsche Obama.

Die Fake-Macher: Was sind GANs?

Bildmanipulation ist nicht neu – schon vor Photoshop mussten sich Menschen fragen, ob das, was ein Foto vermeintlich zeigte, wirklich real war. Doch wozu früher viel Expertise und Können nötig war, macht KI-Technologie Schritt für Schritt für jedermann zugänglich. Dazu nutzt man beispielsweise eine Technik des maschinellen Lernens, die sich Generative Adversarial Networks (GAN) nennt. Auf Deutsch: erzeugende gegnerische Netzwerke. Genau das passiert dabei nämlich: Zwei künstliche neuronale Netzwerke treten sozusagen in einen Wettstreit, trainieren sich gegenseitig. Eines von ihnen schafft ein Bild, das andere lernt, zwischen Fake und Realität zu unterscheiden. So entstehen immer bessere Fakes.

Fake-Videos für Fake News

Schon heute sind Fake News ein Problem. Was passiert, wenn falsche Stimmen und falsche Videos eingesetzt werden, um falsche Nachrichten zu produzieren? Wenn in einer aufgeheizten Situation, wie zuletzt in Chemnitz, plötzlich falsche Videos neben echten zirkulieren? Was, wenn so ein Video kurz vor einer Wahl auftaucht und nicht rechtzeitig als falsch identifiziert wird?

Noch sind es eher Experten, die überzeugende Videomanipulationen zu Demonstrationszwecken erstellen können. Und auch in beeindruckenden Simulationen wie dem Obama-Beispiel kann man, wenn man ganz genau hinschaut, Unstimmigkeiten erkennen. Doch in Zukunft wird diese Technologie immer besser und wahrscheinlich jedem und jeder zugänglich werden. Schon heute gibt es Unternehmen wie beispielsweise Lyrebird aus Kanada, mit deren Hilfe jeder seinen eigenen persönlichen Stimmenimitator erstellen kann. Dazu spricht man einfach ein paar Beispielsätze ein, wartet ein bisschen und kann dann einen Satz eintippen und ihn sich in der eigenen Stimme vorlesen lassen. Es könnte also nur eine Frage der Zeit sein, bis ein gefälschtes Video eine politische Krise auslöst.

Geht die Realität verloren?

Um es nicht so weit kommen zu lassen, arbeiten Wissenschaftler an Methoden der Verifizierung, an Möglichkeiten, mit den Videobearbeitungstechnologien Schritt zu halten, zum Beispiel. Gleichzeitig müssen die Menschen über diese Technologien Bescheid wissen, sie müssen „wach bleiben“, wie der Fake-Obama flapsig mahnt.

Reicht das – wenn „Realität“ nicht mehr „Realität“ bedeutet, wenn jeder es so aussehen lassen könnte, als sei etwas passiert? Ein großes Problem, warnt der Experte Aviv Ovadya im Gespräch mit dem „Guardian“, ist, dass die „Deepfakes“ dazu führen können, dass die Menschen allem misstrauen, was sie sehen oder hören. Wenn alles eine Fälschung ist, dann – so könnten manche überzeugt sein – glaubt man besser gar nichts mehr.

IM TEST

Apple Pay – theoretisch eine feine Sache

Der Bezahlendienst ist komfortabel und sicher, nur hat sich anscheinend dessen Start hierzulande noch nicht herumgesprochen

Von Daniel Killly

Was lange währt ... Seit Monaten vermeldeten die einschlägigen Websites und Blogs immer das Gleiche: Diese Woche soll Apple Pay in Deutschland an den Start gehen – tat es aber nicht, sondern zunächst einmal in Kasachstan. Doch nun hat die Wartezeit ein Ende: Der Bezahlendienst ist jetzt auch hierzulande verfügbar. Um 7 Uhr morgens am 11. Dezember war es so weit.

Apple Pay ist eine komfortable Sache. Die Einrichtung ist kinderleicht, die Sicherheit für Onlineverhältnisse überragend, der Einsatz

zeitparend. Ein System, das den Zahlungsverkehr auch in Deutschland revolutionieren könnte.

Selbstversuch am ersten Geltungstag: Pünktlich zum Start lag morgens um 7 Uhr eine E-Mail von American Express im Postfach. Apple Pay sei jetzt verfügbar. Also flugs die Karte über die Scanfunktion in Apples elektronischer Börse „Wallet“ eingelesen, Sicherheits-PIN eingegeben, den von Apple generierten weiteren PIN per SMS angefordert – und schon heißt es: „Ihre American-Express-Karte wurde erfolgreich zu Apple Pay hinzugefügt.“

Mit der Karte im Wallet wäre der



Blick ins Wallet, die digitale Brieftasche von Apple Pay.

FOTO: DANIEL KILLY/RND

Weg jetzt frei zum kontaktlosen Bezahlen: einfach Apple Pay öffnen, per Doppelklick auf der Seite des iPhones an ein NFC-fähiges Lesegerät

halten – fertig. Allerdings scheiterte der Selbstversuch. An der Kasse der ausgewählten Tankstelle wusste man von nichts.

Weder war den Mitarbeitern der Start von Apple Pay kommuniziert worden, noch wussten sie, dass ihr Unternehmen dabei ist. Es half alles nichts: Plastikkarte aus dem Portemonnaie holen, PIN eingeben, bezahlen. Immerhin vermeldete Wallet per Push-Mitteilung den Kauf. Das blieb für den Premierentag der einzige Vorgeschmack auf neue Zahlen.

Dabei könnte Apple Pay eine wirkliche Bezahlalternative bieten. Denn im Unterschied zu gängigen

Systemen arbeitet Apple Pay nicht mit irgendwelchen Kartendaten. Man sieht auf dem iPhone zwar die letzten vier Ziffern der abgespeicherten Kreditkartennummer. Die Nummer selbst ist aber nicht gespeichert, sondern nur eine Geräte-Accountnummer. Diese Nummer ist für Hacker völlig wertlos, weil sie keiner Karte zuzuordnen ist. Das ist ein Sicherheitsgewinn – vor allem bei Onlinekäufen. Wer mit Apple Pay (und auch Google Pay) bezahlt, hat da nichts zu befürchten. Vorausgesetzt natürlich, der deutsche Handel kriegt beizeiten mit, dass das System bei uns gestartet ist.