Aufgaben:

1. Sieh dir das Video (Face2Face)hinter dem Link an.
   Face2Face: Real-time Face Capture and Reenactment of RGB Videos: https://www.youtube.com/watch?v=ohmajJTcpNk
2. Fasse die im Text dargestellten verschiedenen technologischen Ansätze zusammen.
3. Erkläre das Gefahrenpotenzial der Technologien. Berücksichtige dabei auch die Möglichkeit der Manipulation in Echtzeit (real time).
4. Fasse die angedachten Sicherheitsmaßnahmen für die Aufdeckung und Bestrafung von Manipulationen zusammen.
5. Vertiefung: Bei Interesse am Thema kannst du dir diesen Artikel mit zugehörigem Video zu automatisierten KI-Manipulationen ansehen: (https://www.gamestar.de/artikel/fake-videos-nvidia-ki-faelscht-taeuschend-echte-kamera-aufnahmen,3323201.html)

Traue deinen Augen nicht

Neue Computerprogramme machen die Manipulation von Videos leicht. Das Bild wird Lüge – mit unabsehbaren Folgen

[…] In einem Erklärvideo, das auch auf YouTube zu finden ist, führt [Justus] Thies seine Technologie vor. Zu sehen ist Thies, der sich selbst dabei filmt, wie er das Gesicht verzieht – und George W. Bush, auf einem Fernseher neben ihm, der Thies' Bewegungen wiederholt. Das Video von Bush stammt ursprünglich von CNN, seine Mimik wird aber von Thies kontrolliert. Bush guckt nicht mehr, wie er im Original-Interview guckte, sondern so, wie der Informatiker es will. Thies lächelt – Bush lächelt. Thies zieht die Brauen zusammen – Bush zieht die Brauen zusammen.

Der Programmierer steuert das Gesicht des Politikers fern. Und der Fake ist nicht erkennbar. In einer E-Mail an die *ZEIT* erwähnt Thies die vielen potenziellen Anwendungsfelder seiner Technologie. In Autos könnten Warnsysteme damit das Gesicht und den Wachheitszustand eines Fahrers auch bei schwierigen Lichtverhältnissen kontrollieren, die Entertainment-Branche könnte noch wirklichkeitsgetreuere Virtual-Reality-Szenarien entwickeln. Doch Thies dürfte wohl auch das Gefahrenpotenzial seiner Technologie bewusst sein, immerhin demonstriert er sie an Politikern. Für die neueste Version von Face2Face, schreibt Thies, bräuchte es schon keine Spezialkameras mehr. Nun ist die Technik, die hinter Face2Face steckt, kompliziert und nicht gänzlich öffentlich. Die wichtigsten Codes hat Thies für sich behalten. Aber solche Arbeit, so sagt er selbst, ist reproduzierbar. Er verweist auf das jüngst von der Universität Washington veröffentlichte Projekt Synthesizing Obama, für das Wissenschaftler das Gesicht des ehemaligen Präsidenten digitalisierten und es nun reden lassen können. Sie füttern ihr Obama-Programm mit einer Audiodatei, einer Rede zum Beispiel, und das synthetische Gesicht Obamas spricht diese Rede nach. Dass es sich um eine Simulation handelt, ist kaum erkennbar. In einfacherer Form sind ähnliche Mechanismen schon im Umlauf: Russische Programmierer haben kürzlich eine Handy-App präsentiert, mit der die User Bewegungen des eigenen Gesichtes filmen und auf Gesichter in Fotos übertragen können – die Fotos werden zum Leben erweckt. Noch lässt sich damit vor allem Quatsch machen, ein Covergirl Grimassen schneiden lassen zum Beispiel. Doch je ausgefeilter die Technologie wird, desto ernster wären die möglichen Konsequenzen.

Im Bereich der Stimme ist man schon deutlich weiter. Adobe hat mit VoCo vergangenes Jahr den Prototypen eines Programms vorgestellt, das lediglich mit genug Audiomaterial gefüttert werden muss – etwa zwanzig Minuten der Stimme eines Menschen reichen –, um danach die Stimme dieses Menschen extrem realistisch simulieren zu können. Der User kann diese Stimme danach einen beliebigen Text sprechen lassen. Wörter können per Copy-and- Paste aus Sätzen ausgeschnitten oder in sie hineingebaut werden. Füttert man dieses Programm über 20 Minuten mit der Stimme von Alexander Gauland, lässt sich danach mit Gaulands Stimme spielen wie auf einem Instrument. Die Maschine imitiert seine Intonation, Stimmlage, Pausen.

Das Potenzial der Bild- und Stimmbearbeitung ist gewaltig – und könnte gegen Regierende ebenso gewendet werden wie gegen Bürger. Wie also ließe es sich einhegen? Relativ einfach könnte man die Verbreitung von manipuliertem Bild- und Tonmaterial als Verleumdung unter Strafe stellen. Deutlich schwieriger ist es, die Schuldigen auszumachen und ihre Schuld zu beweisen. Längst herrscht in der Welt der Informatik ein verzweifelter Wettlauf zwischen jenen, die Informationen manipulieren, und denen, die die Manipulation zurückverfolgen. Der Kampf zwischen Manipulatoren und Forensikern erinnert an den Wettlauf von Hase und Igel: Die Forensikerin entdeckt im Quellmaterial einer Datei einen Hinweis auf deren Manipulation und macht diesen publik – und der Manipulator bastelt als Antwort an seiner Technologie, um diesen Hinweis in der nächsten Veröffentlichung

verschwinden zu lassen. Die Forensikerin hilft dem Manipulator, Lücken zu finden und zu schließen, und arbeitet ihm damit zu. Die Auswertung von Beweismitteln braucht so immer mehr Zeit. Bis die Forensikerin der Öffentlichkeit erklären kann, ein Video sei ein Fake, hat es im Zweifel längst seine manipulative Wirkung entfaltet.

Entwickler denken solche Folgen bereits mit. Von Adobe heißt es, Audio-Dateien aus VoCo könnten nach einer Veröffentlichung des Programms mit einer Art digitalem Wasserzeichen versehen werden, das die Herkunft der Tondatei aus dem Computer nachweisen würde. Nur: Wer in manipulativer Absicht handelt und technisch gewieft ist, kann wahrscheinlich auch Wasserzeichen austricksen.

Bleibt die Hoffnung, dass die zunehmende Manipulierbarkeit sämtlicher Daten endgültig das Zeitalter der Kryptotechnik einläutet. Jede Datei, die versendet wird, erhielte von ihrem Ersteller dann eine verschlüsselte Signatur, mit der er für ihre Echtheit bürgt. Der Rezipient könnte entscheiden, ob er den Ersteller für glaubwürdig hält oder nicht. Erhielte die *ZEIT* von ihrer Korrespondentin in Syrien ein Video mit einsehbarer digitaler Signatur, wüsste die Redakteurin im Haus um die Glaubwürdigkeit des Materials, könnte es – wiederum versehen mit der eigenen Signatur der *ZEIT* – über Kanäle wie Twitter mit jenen teilen, die der *ZEIT* folgen, und die könnten digital nachvollziehen, dass das Video aus einer geprüften Quelle stammt. Eine Kette des Vertrauens. Der Rest, alles, was nicht aus solchen Ketten stammt, wäre – manipulativer Müll. Spam.

Quelle: 7. Dezember 2017 **DIE ZEIT** No 51 VON ALARD VON KITTLITZ