Rheinpfalz 18.Juni 2020

Täuschend echte Bilder

Echt oder falsch? Seit einiger Zeit können mit Hilfe von Computerprogrammen Gesichter von Personen erstellt werden, die gar nicht existieren – aber täuschend echt aussehen. Das kann Gefahren bergen. Forscher aus Kaiserslautern haben an einer Software gearbeitet, die bei dem Problem helfen soll.

VON JULIA LUTTENBERGER

Fröhlich lächelt die junge Frau in die Kamera, das schwarze Haar zur Seite gekämmt, der Halsausschnitt eines roten T-Shirts ist zu sehen. Es wirkt, als sei die Aufnahme spontan entstanden, ein Schnappschuss. Doch das stimmt nicht. Das Bild ist ein Deep Fake – ein Bild von einer Person, die gar nicht existiert. Auf die gleiche Weise lassen sich auch Videos herstellen, in denen die gezeigten Personen sprechen und sich wie reale Menschen bewegen – ohne es zu sein.

Forscht am ITWM: Franz-Josef Pfreundt. FOTO: ITWM/FREI

Möglich machen dies sogenannte neuronale Netze, die dazu trainiert werden können, hochwertige Bilder zu erzeugen. Neuronale Netze gehören zum Bereich Künstlicher Intelligenz (KI) und lernen selbstständig. Vorbild dabei ist die Informationsverarbeitung im menschlichen Gehirn. Solche Netze sind unter anderem auch in der Lage, Personen ohne Vorlage zu erschaffen. Denn ein von ihnen generiertes Bild setzt sich nicht aus Teilen vorhandener Bilder zusammen, sondern wird völlig neu erschaffen. „Dazu werden die Netze mit realen Fotos trainiert, etwa mit Bildern von Prominenten", berichtet Franz-Josef Pfreundt, Abteilungsleiter „High Performance Computing" am Fraunhofer-Institut für Techno- und Wirtschaftsmathematik (ITWM).

Mit bloßem Auge nicht zu erkennen

Mit Hilfe der neuronalen Netze können auch reale Gesichter und Videos generiert werden – etwa von Prominenten und Politikern. Bisher habe man Deep Fakes daran erkennen können, dass sie nicht blinzelten – das sei mittlerweile jedoch nicht mehr der Fall, schildert Pfreundt. Mittlerweile würden neuronale Netze mit Menschen mit offenen und mit geschlossenen Augen trainiert, womit das Problem behoben worden sei.

Deep Fakes bergen viele Gefahren. Mühelos lassen sich so zum Beispiel Politikern Sätze in den Mund legen, die sie nie geäußert haben. Welchen Videos, welchen Bildern kann bei diesen Möglichkeiten noch getraut werden? Was ist echt, was ist falsch? Und was passiert, wenn falsche Videos reale Konsequenzen nach sich ziehen?

Die Technik, mit der sich Deep Fakes erstellen lassen, existiere noch nicht so lange, erklärt Pfreundt. Das Bewusstsein für die Gefahren, die damit verbunden sein können, wachse

Hätten Sie es erkannt? Die Person auf diesem Bild existiert nicht. Ihr Bild wurde künstlich erschaffen. FOTO: ITWM/FREI

jedoch. So sehe die Bundesregierung in Deep Fakes eine Gefahr für die Demokratie, der Leiter der KI-Entwicklung bei Facebook, Joaquin Candela, schätzt Deep Fakes als „besorgniserregend" ein, wie Pfreundt schildert. Deep Fakes könnten dazu genutzt werden, Menschen zu manipulieren und sie zu belügen. Für die Forschergemeinde ist das Problem noch relatives Neuland, doch das Interesse daran, falsche Bilder und Videos zu erkennen, ist da. So haben Google und Facebook einen internationalen Forscherwettbewerb ausgerufen, um Mittel und Wege zu finden, wie sich Deep Fakes erkennen lassen, wie Pfreundt berichtet. Die bisherigen Systeme, mit denen Bilder analysiert werden, hätten eine hohe Fehlerquote.

Eine Entdeckung am ITWM könnte das ändern. Auch hier arbeiten die Forscher mit neuronalen Netzen, die mit Bildern trainiert werden. Dabei ist den Wissenschaftlern etwas aufgefallen: Bei den künstlich generierten Bildern lassen sich Abweichungen im Frequenzspektrum erkennen – und zwar immer. Aus dieser Erkenntnis haben Forscher in Kaiserslautern, Mannheim und Offenburg eine mathematische Methode entwickelt, mit der sich Deep Fakes zuverlässig erkennen lassen. Die Federführung hatte Janis Keuper, langjähriger Mitarbeiter und Berater des Fraunhofer ITWM und Professor für „Analytics and Data Science" an der Hochschule Offenburg.

Während das menschliche Auge die Unterschiede zwischen echten und unechten Personen kaum wahrnimmt, verraten es die Bilddaten. Mit dem Verfahren des ITWM sei es zu nahezu 100 Prozent möglich, zu erkennen, ob es sich bei einem Bild oder einem Video um ein Deep Fake handelt oder nicht. Für den von Google und Facebook ausgerufenen Wettbewerb kam die Erkenntnis des ITWM allerdings zu spät. Noch werde das Programm auch nicht vermarktet, bei Interesse bestünde dazu jedoch die Möglichkeit, so Pfreundt. **NILS ERKLÄRT**

IM INTERNET

Wer wissen will, wie echt die Bilder aussehen, kann sich auf der Homepage www.whichfaceisreal.com davon überzeugen.