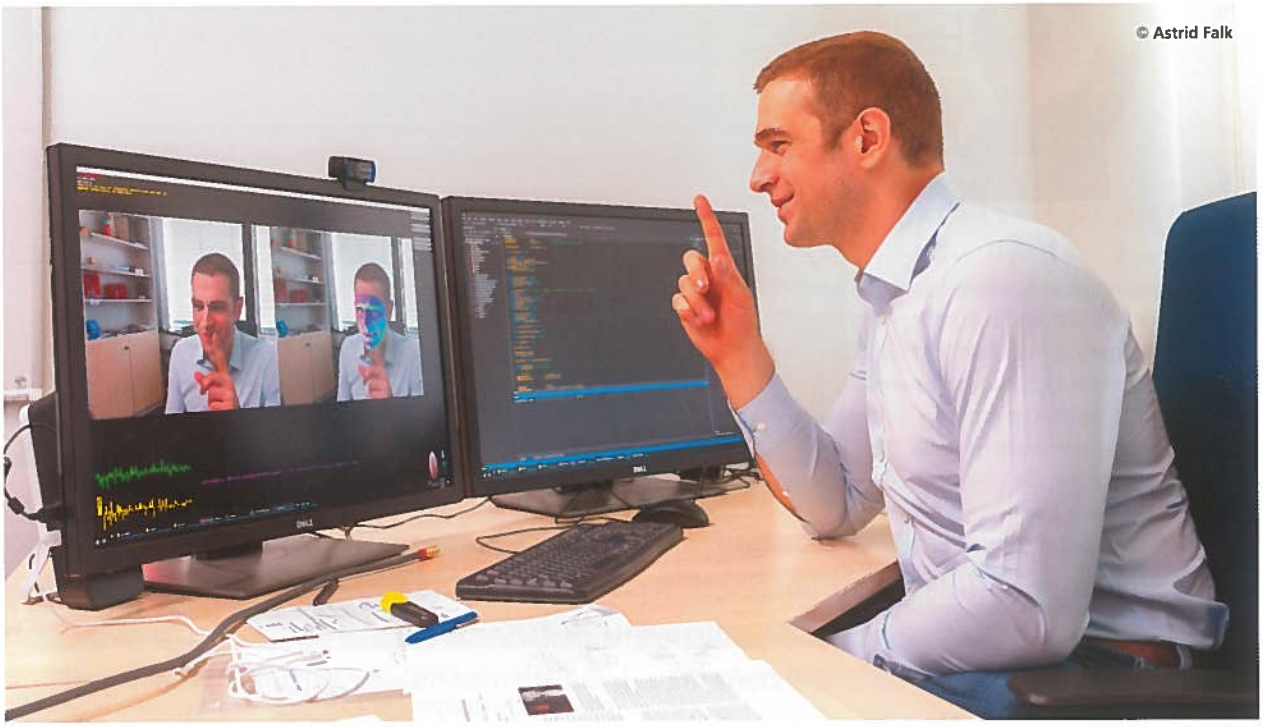
Mit FaceForensics gegen Fakes

Autorin: Doris Herrmann / TUM

Forscher des Visual Computing Lab der TUM spüren manipulierte Videos auf



Mithilfe grafischer Verfahren entsteht in Echtzeit ein manipuliertes Video, das ganz real aussieht.

In einem YouTube-Video US-Präsident Donald Trump mal eben Russland den Krieg erklären oder Aktivistin Gretha Thunberg über den Jugendklimagipfel ablästern lassen – mit der richtigen Software ist das seit Jahren kein Problem mehr. An der Fakultät für Informatik der Technischen Universität München (TUM) haben bereits 2016 Dr. Justus Thies und Prof. Matthias Nießner vom Lehrstuhl für Graphik und Visualisierung gemeinsam mit externen Forscherkollegen mit der Software „Face2Face", einem speziellen Algorithmus, Gesichter in einem Video nach Belieben verändert. Jetzt wollen die Wissenschaftler mit dem Algorithmus „FaceForensics" helfen, Videomanipulationen im Netz einfacher aufzuspüren.

Mithilfe grafischer Verfahren lässt sich in Echtzeit die Mimik einer Person vor einer herkömmlichen 3D-Webcam aus auf eine Person in einem beliebigen Video ganz einfach übertragen. Durch eine eingespielte Tonspur kann man dem „echten" Protagonisten dann Sätze in den Mund schieben, die so nie gesagt wurden. Solche Videos entstehen durch täuschend echte Manipulation.

Die Sache hat gute Seiten: In Zukunft könnte Fake-Software bei Simultanübersetzungen oder Filmsynchronisationen eingesetzt werden. 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.

Prof. Matthias Nießner leitet das Visual Computing Lab der TUM.

Doch Videomanipulation ist auch gefährlich: Die Ergebnisse sind schwer von der Realität zu unterscheiden und niemand merkt, dass der Inhalt nicht echt ist. Schlimme Schäden für Politik, Wirtschaft und Gesellschaft sind zu befürchten.

Prof. Matthias Nießner studierte an der Universität Erlangen-Nürnberg Informatik und erhielt 2010 sein Diplom. Daraufhin begann er seine Promotion unter der Betreuung von Prof. Günther Greiner, ebenfalls an der Universität Erlangen-Nürnberg.

Die Doktorarbeit zum Thema "Subdivision Surface Rendering using Hardware Tessellation" wurde 2013 mit Auszeichnung abgeschlossen.

Im Anschluss erhielt Prof. Nießner eine Gastprofessur an der Stanford University. Seit 2017 ist er Professor an der TUM und leitet das Visual Computing Lab der Fakultät für Informatik.

„Fake-Videos als solche zu erkennen ist besonders in den Sozialen Medien schwierig. Sie sind dort meist komprimiert und werden schlecht aufgelöst hochgeladen", sagt Prof. Matthias Nießner. „Dieselben Methoden, die zur Manipulation von Videos genutzt werden, können aber auch Fälschungen zuverlässig aufspüren – selbst bei schlechter Bildauflösung." Nießner ist seit 2017 Professor an der Fakultät für Informatik der TUM und leitet das Visual Computing Lab. Sein Forschungsgebiet liegt im Bereich der 3D-Digitalisierung zwischen den Feldern der Computergrafik, Computer Vision und künstlicher Intelligenz (KI).

Damit eine KI entscheiden kann, ob ein Video manipuliert ist, muss sie Muster solcher Fälschungen wiedererkennen. Um erlernen zu können, was wiederkehrende Elemente sind, brauchen neuronale Netze einen gewaltigen Input an Fake-Videos. Da in der Forschung solche Videos bislang manuell mit Bild- und Videobearbeitungsprogrammen manipuliert werden mussten, fehlte die nötige Menge solcher Trainingsdaten. Mit aktuellen Deep Learning-Methoden und grafischen Verfahren hat Nießner nun erstmals mit automatischen Verfahren einen umfangreichen Datensatz aufgebaut. Dazu nutze er unter anderem die von ihm entwickelte Software „Face2Face", mit der sich die Mimik einer Person in Echtzeit auf eine andere Person übertragen lässt. Mithilfe des neuen Datensatzes konnte er seinen Algorithmus „FaceForensics" mit mehr als 1,8 Millionen Frames aus über tausend gefälschten Videos trainieren. „Als wir die neuronalen Netze mit unserem Datensatz trainierten, haben wir uns ganz besonders auf die Gesichtsregionen in den stehenden Bildern konzentriert", sagt Andreas Rössler, Forscher im Visual Computing Lab. „Dadurch erkennt ‚FaceForensics' Deep Fakes und Videos, die mit ‚Face2Face' oder ‚FaceSwap' manipuliert wurden, besser als andere derzeit verfügbare Softwares." „FaceForensics" übertrifft auch routinierte Sachverständige. Sind Fake-Videos stark komprimiert, identifizieren ungeübte Menschen diese laut Nießners Studie lediglich mit einer Wahrscheinlichkeit von knapp über 50 Prozent richtig. „FaceForensics" ordnet hingegen 78 Prozent der einzelnen Frames und damit auch der Videos richtig ein.

Um Videomanipulationen im Netz künftig einfacher aufspüren zu können hat Nießners Team „FaceForensics" für die Communities in den Bereichen KI, Grafik, Computer Vision und Digitale Forensik zugänglich gemacht. Anhand der vom Visual Computing Lab erstellten Daten kann auch die Zuverlässigkeit von anderen Erkennungsansätzen getestet werden. Schon jetzt nutzen circa 800 Institutionen „FaceForensics".

Anfang 2018 verbreitete sich die „FakeApp", mit der Nutzer relativ einfach Gesichter in Videos austauschen können. Kann bald jeder mit Deep Fake-Videos Proms & Privates das Leben schwer machen? „Fake-News und Verschwörungstheorien werden auch mit viel weniger ‚Beweisen' geglaubt", sagt Prof. Nießner, „Deep Fakes sind dazu gar nicht nötig."

Mithilfe eines neuen Datensatzes konnten die TUM Wissenschaftler den Algorithmus „FaceForensics" mit mehr als 1,8 Mio. Frames aus über tausend gefälschten Videos trainieren.

KONTAKT

Prof. Matthias Nießner
Visual Computing Lab
Technische Universität München
Fakultät für Informatik
Boltzmannstraße 3
85748 Garching, Germany
E-Mail: niessner@tum.de
https://niessnerlab.org