DEEPFAKE – WIE KÜNSTLICHE INTELLIGENZEN NEWS MANIPULIEREN KÖNNEN

Veröffentlicht am 13. September 2018 von Karishma

Was bedeutet Deepfake und was haben künstliche Intelligenzen damit zu tun? Wir erklären Dir die virale Verbreitung von manipulierten Videos und wie Du sie erkennst. Dass solche Technologien auch mit positiven Absichten verwendet werden können und welche Vorteile sie zukünftig bringen, kannst Du in unserem neuen Blogartikel nachlesen.

Das war ich nicht! Das ist die Reaktion vieler Sänger, Schauspieler und sogar Politiker, die Videos von sich in den News entdecken, in denen sie allerdings nicht mitgespielt haben. **Künstliche Intelligenzen** sind dafür verantwortlich. Mit verschiedenen Apps und Programmen werden Gesichter von Prominenten auf andere Körper projiziert. Die **Grenze** zwischen Fake und Realität kann dabei schnell **verwischen**.

Wir zeigen Dir, wie Du Deepfake Videos erkennst und wie die Technik **auch mit guten Absichten** genutzt werden kann, um Dir einen Spaß mit deinen Freunden zu erlauben.

WAS BEDEUTET DEEPFAKE?

Der Begriff setzt sich aus den englischen Worten „**deep learning**“ und „**fake**“ zusammen. Gemeint ist die Produktion einer künstlichen Intelligenz, die eine Vielzahl von Aufnahmen einer Person scannt, um dessen Gesicht auf das eines anderen zu setzen. Dieser Lernprozess der künstlichen Intelligenz wird als **Machine Learning** bezeichnet. Ziel der Deepfakes ist, eine Person etwas sagen oder darstellen zu lassen, das sie jedoch in Wirklichkeit nicht getan hat. Es ist möglich verschiedene Gesichter zu kombinieren sowie einen Teil oder aber das komplette Gesicht zu ersetzen. **Ahnungslose** können so zum Beispiel in anstößigen Videos mitspielen. Bei den Opfern handelt es sich meist um **Personen der Öffentlichkeit**. Hintergrund der Manipulation sind das Bloßstellen und

Erpressen anderer oder aber auch einfach um Chaos zu schaffen. Um glaubhafte Fakes zu erstellen, bedarf es jedoch einiger Grundlagen: ein PC mit ausreichend Power, eine geeignete Software, sehr viele Fotos und Videos der zu manipulierenden Person und ein paar Stündchen – wohl eher Tage – Arbeitsaufwand. Und die Deepfake Manipulation ist vollbracht. Mit diesen Deepfakes ist ein **neues Zeitalter der Memes** erwacht, die **schwerwiegende Auswirkungen** wie Imageverlust, Karriereeinbußen oder auch politische Krisen zur Folge haben können.

DER ANFANG

Die Welle der Deepfakes startete mit einem Nutzer des Social-News-Aggregators reddit mit dem Pseudonym **„deepfake“**. Dieser erstellte Ende letzten Jahres Videos mit bekannten Schauspielerinnen als Darstellerinnen in pornografischen Videos, welche jedoch schnell entlarvt wurden. Nachdem der Nachrichtendienst Vice auf ihn aufmerksam wurde und dadurch die Sensation los trat, gründete der User eine **Community** beziehungsweise Forengruppe. In dieser Gruppe kann jeder bestimmte Fake Videos anfragen, selbst welche erstellen und mit den anderen austauschen. Zudem wurde die **kostenlose App „FakeApp“** veröffentlicht, welche auf künstlicher Intelligenz basiert. Die Funktionsweise ist den meisten von Euch durch die beliebte „Faceswap“ App vertraut. Ziel des Entwicklers: jeder soll die Fakes auch **ohne Programmierkenntnisse** erstellen können. Die App ist jedoch von der Komplexität her ähnlich wie Photoshop. Also klappt's wahrscheinlich nicht direkt von Anfang an und vor allem nicht, wenn man sich nicht ausgiebig mit den Funktionen beschäftigt. Zusätzlich muss eine ausreichende Menge an unterschiedlichen Aufnahmen aus verschiedenen Blickwinkeln von der jeweiligen Person zu finden sein. Diese werden benötigt, damit die künstlichen Intelligenz die Mimik der Person erlernen kann.

IST DAS ZU GLAUBEN?

Wenn zwei Gesichter kombiniert werden oder das Gesicht von einer Person der Öffentlichkeit auf das einer anderen gesetzt wird, ist der Fake natürlich offensichtlich. Doch was ist, wenn die Täuschung nicht mehr erkennbar ist? Die neuen Techniken von künstlichen Intelligenzen kommen **den Effekten Hollywoods sehr nah**, bei denen zum Beispiel das Gesicht von Schauspielern, die während der Dreharbeiten verstorben sind, künstlich reproduziert werden. Die Technologie dahinter wird immer weiter ausgebaut, damit zukünftig **täuschend echte** Fakes erstellt werden können. Es ist möglich, nur die Mundpartie relativ realitätsnah auszutauschen und die eigene Stimme so zu verzerren, bis sie der des Opfers entspricht. Nach dem Motto „meine Augen und Ohren trügen nicht“ entstehen so falsche Meldungen, die sich viral verbreiten. Im Zeitalter des Datenschutzes können Deepfakes zusätzlich Konflikte mit **Persönlichkeitsrechten** und **juristische Konsequenzen** zur Folge haben. Bei hochauflösenden Videos ist der Fake allerdings meist erkennbar. Noch.

Neuestes Deepfake Opfer US-Präsident Barack Obama

DEEPFAKE IN DER POLITIK

Nach dem Fake Video kommen **Fake News**. Auch Politiker sind bei der Deepfake Community sehr beliebt. Es gibt zum Beispiel ein Video, welches **Obama** in der typischen Kulisse im Oval Office zeigt. Zunächst spricht er glaubhafte Gesprächsthemen an. So weit so gut. Plötzlich jedoch lenkt sein Monolog auf das Thema **Trump**. „President Trump is a total and complete dipshit." Übersetzt heißt das, dass Präsident Trump ein kompletter Vollidiot sei. Die Macher des Videos wollten damit zeigen, wie Fake News von morgen aussehen könnten und dass man nicht sofort alles glauben sollte. Insgesamt 56 Stunden habe die 1-minütige Manipulation gedauert. Zunächst wurde der Mund von Obama ersetzt und der Kiefer angepasst. Daraufhin kümmerte sich FakeApp um die Feinheiten. Die Manipulation ist bei genauer Betrachtung ersichtlich, stiftet zunächst jedoch erst mal Verwirrung.

Es gibt auch weitere Deepfakes, bei denen die Fälschung auffälliger ist. Zum Beispiel wurde das Gesicht von Trump – anscheinend sehr beliebt für solche Fakes – auf das von Angela Merkel mithilfe von künstlicher Intelligenz gesetzt. Und das von Hitler auf den argentinischen Präsidenten Mauricio Macri.

Politische Deepfakes können aufgrund falscher Statements **Krisensituationen und politische Skandale** zur Folge haben. Sie können Gegnern in die Karten spielen, für Propaganda-Zwecke genutzt werden und Massen manipulieren. Der Social Media Hype verhilft solchen Fake

Videos sich in Nullkommanichts auf Facebook, Twitter und anderen Plattformen zu verbreiten und **Gerüchte** entstehen zu lassen. Die größte Gefahr entsteht, wenn die User nicht mehr hinterfragen, ob der Content wirklich Tatsachen widerspiegelt.

WIE ERKENNE ICH FAKES?

Um Fake von Realität zu unterscheiden, gibt es einige Hinweise, auf die Du achten kannst. Zunächst solltest Du die **Quelle** des Videos überprüfen. Woher kommt es und wer hat es hochgeladen? Prüfe ob das Video noch an einer anderen Stelle im Internet zu finden ist. Welche und wie viele glaubwürdige **Nachrichtendienste** verwenden dieses Video? Beim Video selber solltest Du auf Details achten wie die **Mund- und Augenpartie** beim Sprechen der dargestellten Person. Für die KI-Tools ist es meistens schwer Zähne, Lippen und Zunge realistisch wiederzugeben. Auch die Art des Blinzeln ist ein Erkennungsmerkmal. Je statischer die Gesichtszüge der Person, desto eher ist es ein Fake. **Verlangsame** das Video oder stoppe es mittendrin. Dies ermöglicht Dir, das Überlappen des Materials zu erkennen. Eine verrutschte Nase oder falsche Schattierungen entlarven die Fälschung. Die Technologie der künstlichen Intelligenz könnte allerdings auch demnächst verwendet werden, um solchen Deepfakes entgegen zu wirken und diese **zu entlarven**.

DEEPFAKE ALS PARTYKRACHER

Um auch etwas **Positives** in den Deepfakes zu sehen: Du kannst Deine Freunde oder Familienmitglieder **Hauptrollen in bekannten Filmen** spielen lassen. Am besten sucht man sich Charaktere aus, deren Kopf- und Gesichtsform der des Freundes ähneln. So wirkt es authentischer. FakeApp beziehungsweise die künstliche Intelligenz benötigt Aufnahmen um die Mimik zu analysieren und zu lernen. Da die meisten Personen auf Facebook oder anderen sozialen Medien unterwegs sind, sind dort bestimmt einige Fotos als Grundlage zu finden. Um die Fälschung allerdings realitätsnah wirken zu lassen, benötigst Du viel mehr Fotos – um die 800 im besten Fall. Damit ist es noch nicht genug, zusätzlich brauchst Du **tausende Fotos und Videos** der Person aus dem bestehenden Video. Den Rest macht die **KI-Software**. So kannst Du Deinen besten Freund zum Geburtstag zusammen mit den anderen Avengers das Universum retten lassen oder Deine beste Freundin zusammen mit Patrick Swayze ihre „Time of her life“ haben lassen.

> *„Es ist ein historischer Glücksfall, dass wir uns bisher auf Videos als Tatsachenbeweise verlassen konnten"*
>
> *Ian Goodfellow*
> *Google Experte im Bereich Künstliche Intelligenz*

IST JETZT ALLES GEFAKET?

Nein. Natürlich sind nicht alle Videos gefälscht. Jedoch wird es immer schwieriger Fake von Realität zu unterscheiden. Immer mehr Entwicklungen und verbesserte Effekte im Bereich künstliche Intelligenzen ermöglichen **glaubhaftere Täuschungen**. In der Vergangenheit waren wir es gewohnt, uns auf Videos als wahrheitsgemäße Berichterstattung zu verlassen. Doch das hat sich geändert.

Aktuell grenzt die schwierige Erstellung die Verbreitung der Deepfakes glücklicherweise noch ein. Die KI-Software benötigt **zahlreiche Aufnahmen** von der jeweiligen Person aus unterschiedlichen Perspektiven, um es wirklich realitätsnah aussehen zu lassen. Ein weiterer Vorteil ist, dass die Software in ihrer Entwicklung noch an dem Punkt ist, an dem die Fälschungen für das menschliche Auge noch ersichtlich sind. Zudem schluckt das Herstellen eines professionellen Fakes mehrere Tage. Es wird **ständig** an **Optimierungen** der FakeApp gearbeitet, damit zukünftig immer bessere Deepfakes erstellt werden können. Die Gefahr für uns ist, dass wir dann nicht mehr dem vertrauen können, was wir mit eigenen Augen sehen. Dadurch können **Skandale** aufgebauscht und die **Gerüchteküche** zum brodeln gebracht werden. Glaube daher nicht immer alles, was Du oberflächlich siehst. Schau genau hin und hinterfrage das Gezeigte. Bei Unsicherheit solltest Du Dich nur auf etablierte und glaubwürdige Medien verlassen.

Die Technologie der Deepfakes kann natürlich **auch positiv verwendet** werden. Als Parodie für die nächste Firmenfeier, als Geschenk für Freunde oder einfach aus Jux und Tollerei.

DEEPFAKE ALS MARKETINGTOOL: DER AUSBLICK

Zukünftig könnte die Technologie der künstlichen Intelligenz auch im Bereich **Marketing** immer spannender werden. In der Fashion Branche könnte so dem potenziellen Käufer zum Beispiel gezeigt werden, wie ein Kleidungsstück oder Style an ihm aussehen würde. Auch Frisuren und Haarfarben können dem Kunden so schmackhaft gemacht werden. Die Touristikbranche könnte Videosequenzen verwenden unter dem Motto „Hier könntest Du jetzt sein“. So wird Werbung **greifbarer** für den Konsumenten. Dieser sieht sich selbst in den jeweiligen Situationen, wird direkt angesprochen und kann sich damit **identifizieren**. Unternehmen können von dieser **emotionalen Einbindung** der Konsumenten durch personalisiertes Marketing profitieren. Von der Etablierung dieser Art von Marketing und vor allem von der ausgeklügelten Technologie dahinter sind wir noch einige Schritte entfernt.

Fakt ist jedoch, dass Algorithmen von künstlichen Intelligenzen weiter optimiert werden, um neben der Erstellung von Deepfakes **User Emotionen** zu analysieren und zu lernen. Verbessertes Machine Learning ermöglicht KI-Systemen eine unterstützende Funktion als **Chatbots** im Bereich

Kundenservice einzunehmen, die auf Beschwerden und Fragen eingehen. Unternehmen können den Erfolg von Werbekampagnen besser messen, indem Algorithmen die Reaktionen auswerten, wie das Abfotografieren eines Beitrages auf Instagram.

Hast Du noch Fragen bezüglich des Themas „Deepfake“ oder möchtest Anmerkungen da lassen? Dann melde Dich gerne bei uns oder hinterlasse einen Kommentar unter diesem Beitrag.

Kontakt aufnehmen