De camera liegt niet...

Handleiding van Helpmij.nl

Auteur: leofact

november 2019

Het zal je maar gebeuren; zomaar op een dag zie je een video langskomen met jezelf in de hoofdrol. Nota bene in je naakte niksie en, tot je afgrijzen, ook nog eens bezig met dingen waarvan je misschien niet eens wist dat ze mogelijk waren.

Dit kan je zomaar overkomen als je een bekende Nederlander bent. Kort geleden overkwam dat Dionne Stax. Het leek erop dat zij een hoofdrol speelde in een pornovideo. Bij nadere beschouwing bleek het om een nep-video te gaan waarin haar gezicht op realistische ogende manier gecombineerd was met de opnames van een porno-actrice. Mevrouw Stax was natuurlijk op zijn zachtst gezegd “not amused” en de video is inmiddels verwijderd van de site die dit geplaatst heeft.

Deepfake

Deze nep-video’s worden deepfake-video’s genoemd naar de techniek die ervoor wordt gebruikt om ze te produceren. Deze techniek is gebaseerd op een vorm van kunstmatige, of Artificiële Intelligentie (AI). De naam is een samentrekking van Deep Learning en Fake.

Hoe dan?

De techniek die gebruikt wordt, is ingewikkeld en om de techniek enigszins te kunnen begrijpen kom je van het ene begrip in het andere terecht. Ik probeer het hier op mijn eigen, onwetenschappelijke manier, kort uit te leggen:

Klik op de afbeelding om de video te zien.

Deep Learning is een vorm van kunstmatige intelligentie, die ook wel machine leren wordt genoemd. Hierbij wordt in de software grote aantallen rekenkernen geprogrammeerd (“cellen”) die onderling allemaal zijn verbonden (‘neuronen”). Dit lijkt op de manier zoals onze hersenen werken en men spreekt dan ook, net als bij de mens, van neurale netwerken. In de verbindingspaden tussen de kernen worden bepaalde voorkeuren geprogrammeerd waardoor bepaalde paden onder bepaalde omstandigheden vaker of juist minder vaak worden gebruikt. De uitkomst daarvan beïnvloed weer de toekomstige voorkeuren van deze paden. Op die manier leert het netwerk zichzelf nieuwe vaardigheden aan.

Probeer eens het volgende voor te stellen om dit leerproces te verduidelijken: je bent lekker aan het wandelen en je loopt langs een steegje waar het verschrikkelijk stinkt. De geurzenuw verstoort hier duidelijk je plezier. Als dit nog een paar keer gebeurt, word je het zat en je neemt een andere weg. De geurzenuw verstoort je weg niet langer en je hebt geleerd dat je jezelf lekkerder blijft voelen bij de andere weg en die kies je dan ook voortaan.

Om een deepfake-video te maken worden twee neurale netwerken gebruikt. Het ene netwerk produceert de video beeld voor beeld op basis van de afbeeldingen die de gebruiker aanlevert. Het tweede netwerk doet niets anders dan voortdurend controleren of de beelden levensecht lijken. Zo niet dan vervalt het beeld en wordt onmiddellijk een nieuw beeld geproduceerd. Dit proces herhaalt zich eindeloos en na verloop van tijd ontstaat een nieuwe video die de aangeleverde beelden op levensechte wijze combineert. Wanneer er op deze manier van twee neurale netwerken gebruik wordt gemaakt spreekt men van een GAN of Generative Adversarial Network. Dat weet je dit ook maar weer…

Resultaat

Op deze manier kun je een video maken waarin de hoofdrolspeler wordt verouderd of een ander geslacht krijgt of iets dergelijks. Het is daarnaast ook mogelijk de hoofdpersoon handelingen te laten uitvoeren of dingen te laten zeggen die feitelijk door een ander zijn gespeeld. Het resultaat ziet er behoorlijk natuurlijk uit, zie daarvoor deze video:

Klik op de afbeelding om de video te zien

Het is best nog ingewikkeld om zelf een deepfake-video te maken. Dat wordt echter al snel steeds eenvoudiger. Er zijn zelfs al simpel werkende apps voor ontwikkeld. Zo is in China de app Zoa viraal gegaan. Ook de gebruikersvriendelijkheid ontwikkelt zich razendsnel (zie de linken onderaan dit artikel).

Gevaar

Je kunt nog altijd enigszins zien dat de huidig geproduceerde deepfake-video's nep zijn. Je kunt dat vaak zien aan het knipperen van de ogen, de bewegingen van de mond in combinatie met de gezichtsuitdrukking en de lichaamsbewegingen ten opzichte van de bewegingen van het hoofd.

Daarnaast zijn er regelmatig vervaagde pixels te zien in deze video's. De verwachting is echter dat op korte termijn de techniek zo vervolmaakt wordt, dat het op geen enkele manier meer te zien is dat er sprake is van een deepfake video (zie de link onderaan dit artikel). Helaas kan deze techniek worden misbruikt om nepnieuws nog echter te laten lijken. Daarnaast kunnen criminelen in de verleiding komen om video's te produceren waarin mensen in compromitterende situaties zitten. Doordat de video's niet van echt zijn te onderscheiden, zou de crimineel kunnen proberen om hier hun slachtoffers mee te chanteren.

Naast deze reële gevaren heeft deze techniek ook positieve kanten. Bioscoopfilms met niet-bestaande hoofdrolspelers kunnen ongekend natuurlijk en spannend worden. Ook in het huis-tuin-en-keukengebruik zijn allerlei grappige toepassingen te bedenken.

Hopelijk vindt de industrie iets uit waardoor herkenbaar blijft of het om een originele opname gaat of dat het gaat om een gemanipuleerde deepfake-video.

Ten slotte

In deepfake-video's wordt de hoofdpersoon gemanipuleerd of speelt een rol die door een ander zijn gespeeld of gezegd. De techniek hierachter is gebaseerd op kunstmatige intelligentie en ontwikkelt zich snel. "De camera liegt niet" is daardoor een uitspraak die we niet meer kunnen gebruiken. Dit kan prachtige bioscoopfilms opleveren, maar helaas ook moeilijk te herkennen nepnieuws en mogelijk een hoop criminele narigheid. Wat wel nog altijd geldig is; een gewaarschuwd mens telt voor twee. Daar hoopt dit artikel aan bij te dragen.

Achtergrond en lezenswaardige links

Wat is deepfake, uitleg op Wikipedia.
Deep Learning, kort uitgelegd op Wikipedia.
Meer uitleg en tips om deepfake-video's te herkennen op Mediawijsheid.
Deepfake in 7 minuten gedemonstreerd (Nederlands ondertitelt) op You Tube.
In deze deepfake-video zie je hoe de maker Obama "inspreekt" (Engels) op You Tube.
Zo maak je zelf een deepfake volgens Marketingfacts.
De snelle ontwikkeling van de geloofwaardigheid volgens Express.Llve.
Uitzending van Tegenlicht over deepfake (45 minuten) op Vpro.nl.
Chinese Deep Fake-app gaat viral: Onemorething.nl.
Zorgen over de mogelijkheden van deepfake-video's door het van het Openbaar Ministerie.
Criminelen gebruiken deepfake-stem voor oplichting: Techzine.nl.
Management Dionne Stax woest over deepfake-video: Ad.nl.

Afbeeldingen; Pixabay en screenshots van You Tube.
Logobasis van Wikipedia (gebruiker Macbay),