INNOVATIE & STRATEGIE

WETENSCHAP

Watermerk video sleutel in de strijd tegen nepnieuws

Waarom Amerikaanse defensie gebruik maakt van Amsterdams onderzoek naar beeldmanipulatie

Thomas Mensink © Monique Kooijmans

8 MEI 2018

Het manipuleren van video- en fotomateriaal levert beelden op die steeds moeilijker te onderscheiden van echt. De technologie bestaat al langer maar was vooral voorbehouden aan de filmindustrie voor het creëren van speciale effecten. Thomas Mensink leidt een onderzoeksgroep aan de UvA die onderzoek doet aan het manipuleren van beelden, maar ook aan het opsporen ervan.

Vorige week kwam de groep in het nieuws doordat de onderzoeksgroep van Amerikaanse defensie (DARPA) via de non-profit onderzoeksorganisatie SRI International gebruik gaat maken van onder meer de technologie van de groep van Mensink. Het doel is bijvoorbeeld oorlogsmisdrijven te ontdekken in beeldmateriaal. Door de inzet van nieuwe beeldbewerking is het immers steeds makkelijker gebeurtenissen te maskeren of juist te suggereren door op het goede moment gemanipuleerd beeldmateriaal te publiceren.

Mensink: "Wat nieuw is, is het gemak waarmee video's en foto's zijn te manipuleren, door gebruik te maken van computervisiontechnieken gecombineerd met machine learning/deep learning. Daarmee lukt het om geloofwaardige beelden te maken die voor velen amper van 'echt' te onderscheiden zijn."

Het ontdekken van gemanipuleerde video's wordt daardoor ook steeds lastiger. Mensink: "Ik denk dat er ook

GERELATEERDE ARTIKELEN


Slimme software zoekt op video oorlogsmisdaden


Google deelt beeldherkennings-AI als open source


Nepnieuws 3

Nepnieuws is de toekomst 4

GERELATEERDE WHITI


Sneller inno wendbare IT Retail


Hyper-conve oplossingen nadelen om voordelen


Ontzorg de zorgprofessi virtualisatie


Zeven lesse en de overst Enterprise A

Verbeter pro softwareontw door ALM en integreren

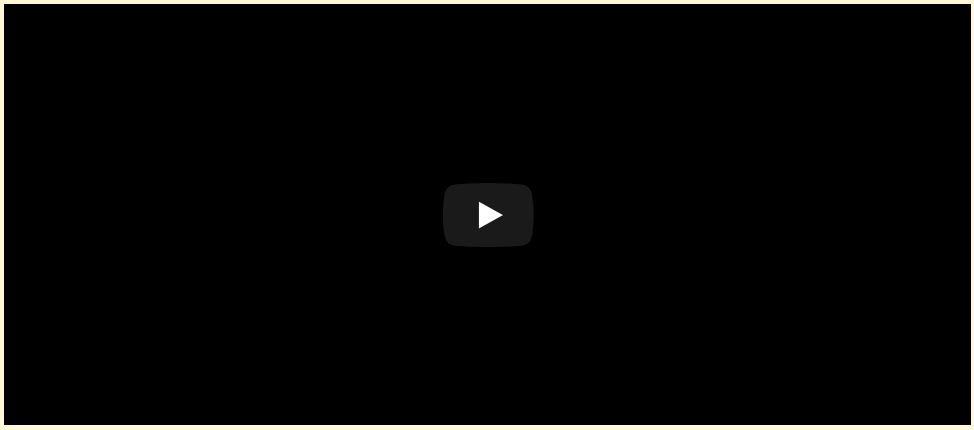
MEER WHITEPAPERS

e en Strategie op AG

onderzoek nodig is naar het "beveiligen" of "watermerken" van video's (of beelden) waarmee de authenticiteit kan worden aangetoond. Dat zou wellicht kunnen door de inzet van cryptografische berekeningen. Zo is ook WhatsApp beveiligd, of e-mail in combinatie met PGP. Wellicht bieden ook blockchain-achtige technieken uitkomst."

ZEI TRUMP DAT ECHT?

Voor het succesvol manipuleren van video's van personen spelen ook mimiek en (stem)geluid een belangrijke rol. Die aspecten goed na bootsen, is heel lastig. Bovendien, hoe bekender een persoon is, hoe moeilijker het is omdat kleine verschillen dan veel meer opvallen. In de video hieronder is te zien hoe de mimiek van Poetin en Trump kan worden aangepast.



Een belangrijk aanknopingspunt bij het speuren naar gemanipuleerde video's is de correlatie tussen het geluid van de film en het beeld van de film. Kloppen die wel met elkaar? Drie voorbeelden:

1. Als iemand praat, kunnen we de beweging van de mond relateren aan het geluid van de video. Beweegt de mond wel mee met wat er gezegd wordt. Dit doen we door rondom de mond en op de lippen punten te volgen door het beeld. Daarmee houden we bij hoe de mond beweegt in de video. Dan wordt er berekend of dat kan kloppen met het geluid van de video.
2. Een ander scenario is dat "iemand de woorden in de mond worden gelegd" door middel van video manipulatie. Als we andere video's van deze persoon hebben, dan kunnen we stem-identificatie uitvoeren en de stem in de nieuwe video vergelijken met andere video's. Deze technieken ontwikkelen we ook om dit binnen 1 video te doen, zonder dat we de computer eerst vertellen wie wie is. Die herkent wie spreekt (visueel) en of die stem consistent is met eerdere keren dat deze persoon heeft gesproken.
3. Het derde scenario gaat niet uit van personen, maar waar een video is opgenomen. Computer visie technieken kunnen herkennen waar een beeld is opgenomen (een kleine kamer, een grote hal, of buiten). Het interessante is, dat deze ruimtes allemaal een ander "galm" patroon hebben. Dus door de galm die wordt opgepikt door de microfoon te analyseren en te vergelijken met de voorspelling uit het

beeld kunnen we bepalen of de video en de microfoon in dezelfde ruimte waren. De bijdrage van het team van Mensink in het DARPA-project zit voornamelijk in de visuele analyse voor dit soort problemen: hoe kunnen we het beeld omschrijven, zodat het vergeleken kan worden met het audio signaal.

Het onderzoek naar manipulatie van beelden is fascinerend. Er bestaat inmiddels een hele gereedschapskist vol aan technologieën. Bijvoorbeeld voor een 'face swap' - het vervangen van een gezicht in een video door dat van iemand ander - wordt vaak gebruik gemaakt van 3D-modellen van gezichten om de swap zo echt mogelijk te laten lijken. "Hoe goed het werkt, hangt deels af van het perspectief." De groep van Mensink werkt aan het verder perfectioneren van de technieken. Een belangrijk onderdeel daarvan is het slimmer trainen van de deep neural networks en het verbeteren van deze netwerken. Bovendien kunnen de netwerken beter worden getraind door veel meer trainingsdata te gebruiken.

Video is lastiger

Bij het manipuleren van video's gaat het er niet alleen om dat het beeld klopt, maar ook het geluid en de mimiek. Hoe bekender de mensen in de video zijn, hoe lastiger het is deze te veranderen. Kleine verschillen vallen al snel op. Ook dat zal beter worden, denkt Mensink, met behulp van betere modellen.

Het team werkt niet alleen aan de ontwikkeling van dit soort 'gegenereerde 'video's, maar onderzoekt ook hoe deze beelden weer te herkennen zijn. Juist in deze aanpak is DARPA geïnteresseerd. Een veelgebruikte methode is het inzoomen naar de randen van een gezicht dat mogelijk is 'ingeplakt'. Vaak zijn daar 'artefacten' te zien ofwel bijwerkingen van de methoden die gebruikt zijn om het gezicht te vervangen. Daarnaast leveren dus ook het geluid en de mimiek belangrijke aanknopingspunten (zie kader) omdat de technieken nog niet zo ver zijn als voor het manipuleren van fotomateriaal.

Opsporen nog specialistenwerk

Mensink stelt dat er nog lang geen computerprogramma's bestaan die door iedereen gebruikt zouden kunnen worden om de authenticiteit van een video te beoordelen. "Deze huidige technieken en demo's laten onze staat van de techniek zien. Om ze breder toepasbaar te maken is én nog meer onderzoek voor nodig om onze huidige technieken te verbeteren, én meer tijd om er een echt programma van te maken wat bijvoorbeeld op grote schaal kan worden ingezet."

Lees meer over: beeldmanipulatie, videobewerking, deep learning
Lees meer over Innovatie & Strategie OP AG Intelligence

THIJS DOORENBOSCH
is redacteur, online coördinator en heeft als belangrijkste aandachtspunt Innovatie en Strategie.

Telefoon: +31202356411
E-mail: t.doorenbosch@agconnect.nl

VOLGORDE

NIEUWSTE EERST

OUDSTE EERST

REACTIE TOEVOEGEN

Uw reactie

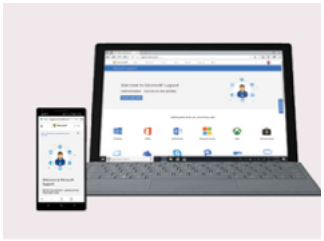
PLAATS REACTIE

LEES OOK

Software-optie leidde tot dodelijk Uber-ongeluk

Microsoft lokt app-makers met korting

Keyboardhaat MacBook Pro jaagt petitie aan

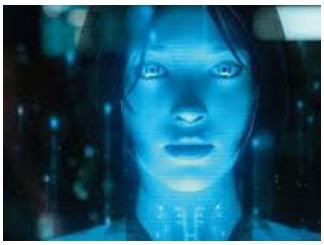


Microsoft importeert Android-smartphone Windows 10

Volvo gaat geheel voor Google

Rabobank stopt met PINpas-scanner

Windows raakt ondergeschikt aan Azure en Office 365



Chrome- en Cortana crashes na april-update Windows 10

NIEUWSOVERZICHT ▸

TOPICS

- Analytics
- Apps
- Blockchain
- Branche
- Carriere
- Datamanagement
- Governance
- Infrastructuur
- IT beheer
- Juridische zaken
- Netwerken
- Outsourcing
- Personal Tech
- Privacy
- Procesmanagement
- Software-ontwikkeling
- Storage
- Wetenschap
- Windows 10
- Zakelijke software