ONDERZOEK: HOE VEILIG IS GEZICHTSHERKENNING?

INLEIDING

Gezichtsherkenning is hedendaags niet meer weg te denken. Het zit in allerlei verschillende apparaten, van smartphone tot laptops. Zelfs de bekende slimme deurbel Ring overweegt gezichtsherkenning te gebruiken in hun apparaten.

De technologie van gezichtsherkenning kan natuurlijk heel handig zijn om je telefoon mee te ontgrendelen of in een serieuzer geval, criminelen op te sporen. Maar ik vraag me af: Hoe veilig is gezichtsherkenning nu echt?

Dit onderzoek is gedaan doormiddel van library research.

ONDERZOEKSVRAAG

Hoe veilig is gezichtsherkenning? Dat is mijn hoofdvraag in dit onderzoek, naast mijn hoofdvraag heb ik nog deelvragen om de hoofdvraag te beantwoorden. Deze vragen zijn:

- Is gezichtsherkenning de toekomst?
- Is gezichtsherkenning veilger dan andere inlog methodes?
- Is gezichtsherkenning makkelijk te vervalsen?
- Wat is de wetgeving voor gezichtsherkenning?

GEZICHTSDETECTIE APPLICATIE

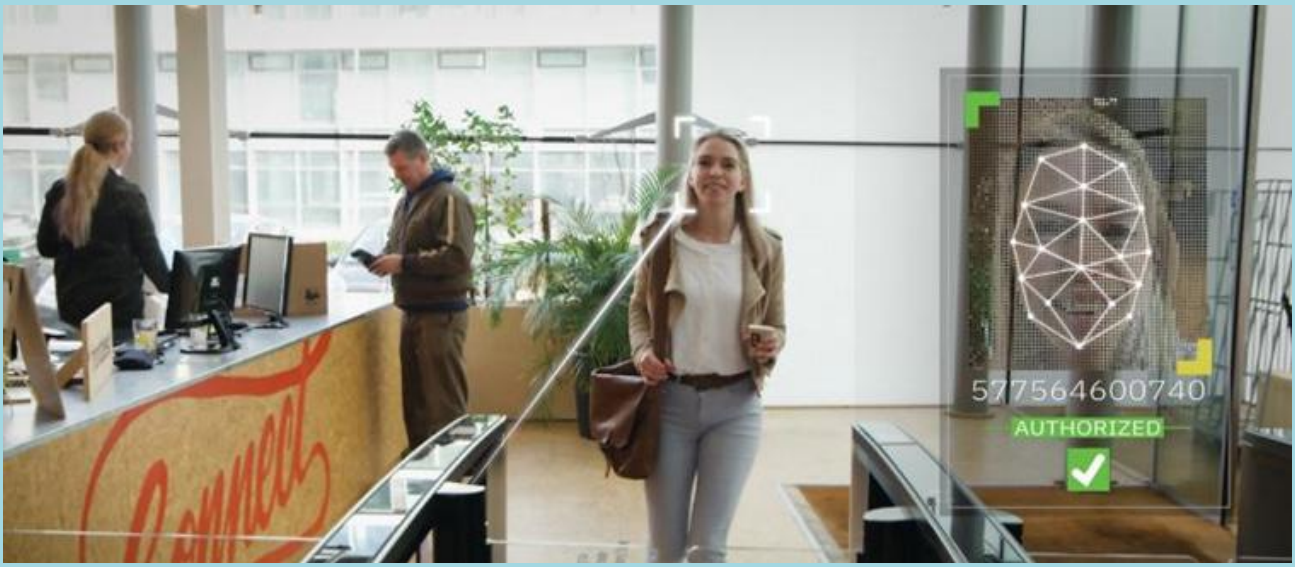
Als opdracht voor mijn sprint x heb ik een applicatie gemaakt met wat hulp van het internet. Deze applicatie is instaat om gezichten te detecteren. Wanneer je een foto of je eigen gezicht voor de camera houdt ziet hij dat het een gezicht is. Doormiddel van de Face API is het ook mogelijk om je emoties te lezen. Zo kan de applicatie zien of je blij, boos, verdrietig, bang, walgend of verrast bent.

IS GEZICHTSHERKENNING DE TOEKOMST?

DE TOEKOMST VAN GEZICHTSHERKENNING (1)

Hoewel gezichtsherkenningstechnologie voornamelijk gerelateerd is aan veiligheid en wetshandhaving, hebben recente ontwikkelingen ervoor gezorgd dat de technologie meer toepassingen heeft op andere gebieden. Denk bijvoorbeeld aan retail, marketing, financiën en zorg.

Vergeleken met andere vormen van biometrische identificatie heeft gezichtsherkenning verschillende voordelen. Het is bijvoorbeeld sneller en eenvoudiger te implementeren omdat het kan worden gebruikt met bestaande camera's en bewakingsapparatuur. Daarnaast is het praktischer en hygiënischer dan andere methoden omdat het geen fysieke interactie met de gebruiker vereist.



GEZICHTSHERKENNING OP VLIEGVELDEN

De U.S. Customs and Border Protection (CBP) heeft onlangs plannen aangekondigd om een biometrisch immigratiesysteem te installeren op Orlando International Airport.

Alle internationale reizigers worden bij aankomst en vertrek door het systeem gescand en de foto's worden vervolgens vergeleken met foto's in de database van het Department of Homeland Security. Volgens het CBP duurt het hele proces minder dan twee seconden en is de nauwkeurigheid zelfs 99%.

IS GEZICHTSHERKENNING VEILIGER DAN ANDERE INLOG METHODES?

BEVEILIGEN MET EEN PINCODE (2)

De bekendste en nog steeds meest gebruikte is de pincode. Je kan 4-cijferige of 5-cijferige codes instellen op elke smartphone. Zo'n code krijg je niet makkelijk ontcijferd. Er zijn heel veel mogelijkheden. Zo heeft hebben de meeste smartphones ook een beveiliging op het inloggen zitten. Als je een aantal keer de verkeerde code invoert word je telefoon tijdelijk geblokkeerd. Hedendaags is er software beschikbaar waarmee hackers je wachtwoord kunne kraken. Of ze proberen je pincode te stelen via een sms-phising. Maar de gemakkelijkste manier om iemands pincode te vinden is een omstander. Deze mensen kijken over je schouder mee en stelen daarna je smartphone.

BEVEILIGEN MET EEN VINGERAFDRUK

Een andere beveiligingsmethode die steeds vaker wordt gebruikt, zijn vingerafdrukken. Doordat je eigen vingerafdruk uniek is, is deze beveiligingsmethode een stuk veiliger omdat andere mensen je gegevens niet zomaar kunnen stelen. Maar ook voor deze methode hebben hackers een manier gevonden om de vingerafdruk na te bootsen. Naast de voordelen kent het ook nadelen, af en toe herkent het toestel je vingerafdruk niet als je vinger er niet goed op ligt. Voor de nieuwste apparaten moet het scherm zijn ingeschakeld voordat vingerafdrukbeveiliging kan worden gebruikt. Dat is dus minder efficiënt.

BEVEILIGEN MET GEZICHTSHERKENNING

Al een aantal jaar zijn de meeste smartphones uitgerust met gezichtsherkenning. De smartphone gebruikt de camera om je gezicht te scannen. Als het gescande gezicht overeenkomt met de opgeslagen afbeeldingsinformatie, wordt de smartphone ontgrendeld. Volgens de fabrikant is het een waterdichtingsmethode, maar dit blijkt niet het geval te zijn. Het is namelijk mogelijk om met hoge kwaliteit foto's om sommige smartphones in te loggen. Dit haalt heel de veiligheid van gezichtsherkenning weg.

IS GEZICHTSHERKENNING MAKKELIJK TE VERVALSEN?

CONSUMENTENBOND TEST (3)

Sinds een jaar testen ze bij de consumentenbond de beveiliging van gezichtsherkenning op smartphones. Volgens het onderzoek van de Consumentenbond blijkt dat 26 van de 60 geteste smartphones te ontgrendelen zijn door een goede portretfoto van de telefoongebruiker voor de selfie-lens te houden. Dit zou in principe iedereen kunnen doen die de telefoon in handen heeft.

Modellen van grote merken zoals Samsung (de Galaxy A7 en A8), Huawei (de P20, P20 Lite en P20 Pro), Nokia (model 3.1 en 7.1), Sony (Xperia XZ2 en XZ2 Compact) blijken kwetsbaar voor de zogenoemde ‘fotohack’.

Het is daarentegen niet zo dat alle modellen van de bovenstaande merken een zwakke beveiliging hebben. Van Samsung laten de Galaxy S9, S9+ en Note9 zich niet kennen en dat geldt hetzelfde voor de Huawei Mate 20 en Mate 20 Pro. De iPhone XS Max en iPhone XR blijken ook niet te bezwijken onder de fotohack.

MISLEIDEN VAN GEZICHTSHERKENNINGSSYSTEMEN (4)

Onderzoekers van het AI-bedrijf Kneron wisten gezichtsherkenningssystemen bij banken, grensovergangen en op vliegvelden voor de gek te houden met geprinte maskers van andere mensen.

De onderzoekers melden dat ze op 3 verschillende continenten met succes controlepunten hebben weten te misleiden. Het gaat hier om betaalautomaten van de Chinese bedrijven Alipay en WeChat. Naast dat hebben ze ook een grensovergang in China en een controle punt op Schiphol weten te misleiden.

Volgens de onderzoekers laten de resultaten zien dat iedereen die een masker afdrukt dat er een beetje op lijkt, in theorie een veiligheidscontrole kan doorstaan om te gaan winkelen of te vliegen in de naam van een ander persoon.

WAT IS DE WETGEVING VOOR GEZICHTSHERKENNING?

AVG-WETGEVING (5)

In de Algemene Verordening Gegevensbescherming-wet (AVG) staat dat je gezichtsherkenning alleen mag gebruiken als je de persoon die geïdentificeerd wordt, om toestemming vraagt. Zo moet je als je ontgrendeling via gezichtsherkenning instelt op je smartphone ook eerst toestemming geven.

Volgens de AVG-wet is gezichtsherkenning zonder toestemming alleen toegestaan als het om een zwaarwegend belang gaat, zoals het bestrijden van criminaliteit of terrorisme. De Europese Commissie is van plan om strengere regels op te stellen voor het gebruiken van gezichtsherkenning. Dit meldt het Financial Times in 2019.

Deze nieuwe regels zouden ervoor moeten zorgen dat je ervan op de hoogte wordt gesteld wanneer een bedrijf je gegevens gebruikt die zijn verkregen door gezichtsherkenning.

De potentie van gezichtsherkenning is groot, zolang er maar kaders worden geschept voor het veilig gebruik ervan.

VERENIGDE STATEN (6)

Tot nu toe is de regulering van technologie erg streng geweest, en mogelijke gezichtsherkenningswetten vormen daarop geen uitzondering.

In de Verenigde Staten ontvouwt zich de strijd om gezichtsherkenningstechnologie op lokaal niveau. Neem San Francisco als voorbeeld.

Zo werd gezichtsherkenning in mei 2019 daar verboden, en dat wil zeggen: het gebruik ervan bij surveillance door de politie en overheidsinstanties.

CONCLUSIE

Om de onderzoeksvraag te beantwoorden: Het is veilig, maar niet waterdicht. Zo zijn er tegenwoordig allerlei manieren om het gebruik van gezichtsherkenning te omzeilen. Zo zijn er een aantal smartphones die misleid kunnen worden door een hoge kwaliteit foto voor de camera te houden om in te loggen. Ook met gebruik van een masker is het bij sommige systemen mogelijk om ze te misleiden.

In vergelijking met andere inlog methodes zou ik gezichtsherkenning voor veiligheid op nummer 2 van de 3 zetten. Hierboven staat dus nog inloggen met je vingerafdruk, deze staat op 1 omdat je vingerafdruk uniek is niet makkelijk vervalst kan worden. Daarnaast zijn er met gezichtsherkenning wel meer mogelijkheden.

Als we dan even niet uitgaan van alle nadelen, is het wel de toekomst. Zo is het bijvoorbeeld sneller En gemakkelijker te implementeren als andere biometrische identificatiesystemen.

BRONVERMELDING

(1) Redactie Richard Van Hooijdonk. (2018, 2 november). Gezichtsherkenningstechnologie komen we binnenkort overal tegen. Richard van Hooijdonk Blog. https://blog.richardvanhooijdonk.com/gezichtsherkenningstechnologie-komen-we-binnenkort-overal-tegen/

(2) AD/MAX Vandaag. (2020, 18 februari). Wat is de beste manier om uw smartphone te beveiligen? MAX Vandaag. https://www.maxvandaag.nl/sessies/themas/media-cultuur/wat-is-de-beste-manier-om-uw-smartphone-te-beveiligen/

(3) Kulche, P. (2019, 15 april). Gezichtsherkenning op smartphone niet altijd veilig. Consumentenbond. https://www.consumentenbond.nl/veilig-internetten/gezichtsherkenning-te-hacken

(4) Holmes, A. (2019, 12 december). Gezichtsherkenning is heel makkelijk voor de gek te houden met een geprint masker, ook op Schiphol. Business Insider Nederland. https://www.businessinsider.nl/de-gezichtsherkenning-op-schiphol-is-heel-makkelijk-voor-de-gek-te-houden-met-een-geprint-masker

(5) Redactie Beleef KPN. (2021, 18 maart). Alles wat je wil weten over gezichtsherkenning. KPN.com. https://www.kpn.com/beleef/blog/gezichtsherkenning.htm

(6) Asher, C. (2020, 25 februari). Gebruik en misbruik van gezichtsherkenning. AVG. https://www.avg.com/nl/signal/facial-recognition-uses-and-abuses

Jaap Wouters ©