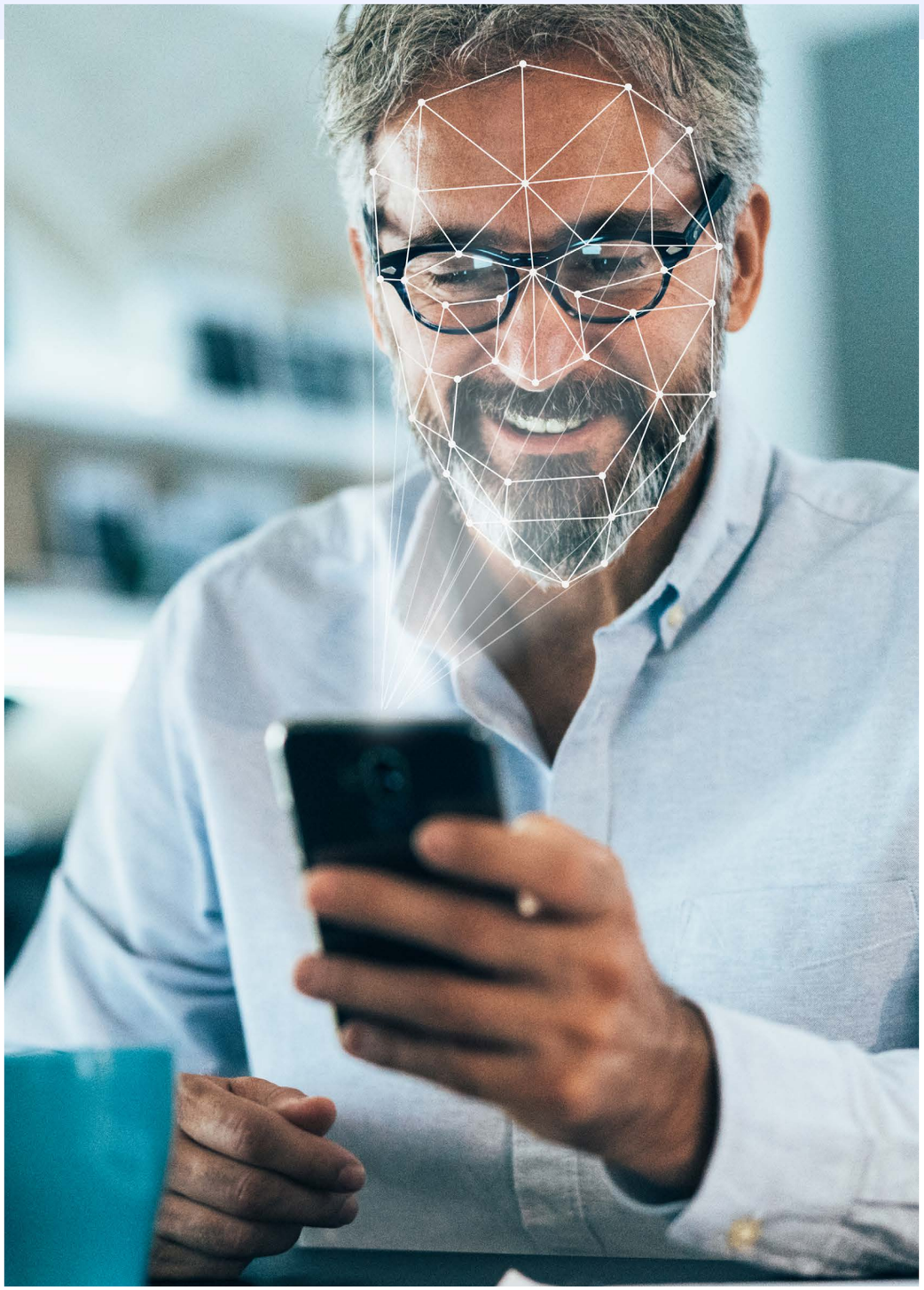
Dataetisk Råd

Hvad er **ansigts-genkendelse?**

Indhold



Hvad er ansigtsgenkendelse?

Ansigtsgenkendelse er computersoftware, som kan analysere billeder for at opdage, evaluere og identificere ansigter. Teknologien har et stort potentiale på en lang række områder, og anvendes også allerede i dag af både myndigheder, virksomheder og private borgere til så forskellige opgaver som adgangskontrol på mobiltelefoner, kundeanalyse i indkøbscentre og eftersøgning af mistænkte i videomateriale.

Ansigtsgenkendelse er også en moderne teknologi, som kan vække stærke følelser. Dette baggrundspapir fra Dataetisk Råd præsenterer ansigtsgenkendelse som teknologi for at give interesserede et bedre grundlag for at reflektere over og tage stilling til anvendelsen af ansigtsgenkendelse.

I **første afsnit** nedenfor introduceres **ansigtsgenkendelse som teknologi.** Vi skitserer processen for ansigtsgenkendelse, og nogle af de forskellige former den kan antage. Vi illustrerer undervejs hvordan ansigtsgenkendelse kan virke på forskellige måder, ved at præsentere en række eksempler på, hvordan teknologien anvendes i praksis.

En af forudsætningerne for ansigtsgenkendelse er maskinlæring af kunstig intelligens til billedanalyse. I **afsnit to** præsenterer vi **dybe neurale netværk** som det tekniske fundament for ansigtsgenkendelse. Vi fremhæver i den forbindelse både nogle af de særlige styrker som sådanne algoritmer har, og nogle af de udfordringer som deres anvendelse kan rejse.

Ansigtsgenkendelse kan være kontroversielt. En sober vurdering af fordele og ulemper ved ansigtsgenkendelse kræver, at man overvejer præcis hvordan den konkrete form for ansigtsgenkendelse virker. I **afsnit tre** skitserer vi en række af de faktorer, som kan være relevante for vurderingen af **fordele og ulemper** ved anvendelse af ansigtsgenkendelse.

Sekretariatet for Dataetisk Råd
Oktober 2022

1.

Hvordan virker ansigtsgenkendelse?

Ansigtsgenkendelse er grundlæggende software, som kan analysere et billede for at opdage ansigter på billedet. Ovenpå denne første analyse kan softwaren foretage yderligere analyser af de ansigter, som er blevet opdaget. Ansigtsgenkendelse kan eksempelvis udlede et ansigts matematiske struktur, og sammenligne denne struktur med strukturen for kendte personer eller med almindelige strukturer for forskellige grupper. Med disse informationer kan ansigtsgenkendelse yderligere forsøge for eksempel at identificere en person, eller at bestemme demografiske karakteristika som køn, alder eller etnicitet.

På et overordnet niveau kan man skelne mellem mindst fem centrale opgaver for ansigtsgenkendelse (Hupont et al 2022):

- Ansigtsopdagelse
- Biometrisk analyse
- Personidentifikation
- Demografisk identifikation
- Udtryks- og affektidentifikation

Ansigtsopdagelse

Den første og mest elementære opgave for ansigtsgenkendelse er at finde ud af hvor i billeddata, der findes ansigter. Denne ansigtsopdagelse er forudsætningen for, at andre, mere komplekse opgaver kan udføres.

Ved ansigtsopdagelse forsøger algoritmen at finde strukturer i billeddata, som minder om de strukturer menneskelige ansigter plejer at have: øjne, næse, mund, hage, ører, osv., placeret i nogenlunde regelmæssige forhold til hinanden.

Analysens resultat kan være en matematisk afgrænsning af et eller flere ansigter i billeddata.

Ansigtsfokus på digitale kameraer
Den måske mest almindelige erfaring med ansigtsopdagelse er, når det anvendes af digitale kameraer til automatisk at stille skarpt på ansigter.
De fleste moderne mobiltelefoner er udstyret med både et kamera og med software, som forsøger at opdage ansigter, for at kameraet automatisk kan indstilles således at ansigter placeret centralt i billedet er i fokus. Det hjælper i de fleste situationer brugeren med at tage gode billeder. (Rahman & Kehtarnavaz 2008)

Biometrisk analyse

Det næste skridt i anvendelsen af ansigtsgenkendelse er typisk at lave en biometrisk analyse af de ansigter, som er blevet opdaget i billeddata.

Algoritmen analyserer billeddata for at aflæse ansigtets form, og måle den matematiske struktur for de geometriske hovedtræk i ansigtet. Hvert ansigt har unikke særpræg, som kan måles i ca. 80 nodalpunkter. Sådanne hovedtræk omfatter afstand mellem øjnene, øjenhulernes dybde, afstanden fra pande til hage, kindbenenes form samt læbernes, ørernes og hagens kontur.

Målene på disse nodalpunkter sammenfattes i et ”ansigtsaftryk” – en unik matematisk model, som repræsenterer et ansigt. Hver person har sit eget unikke ansigtsaftryk, på samme måde som vi kender fra fingeraftryk.

Automatisk billedbeskæring på digitale platforme
En anden anvendelse som mange mennesker møder jævnligt er automatisk billedbeskæring på digitale platforme. Mange hjemmesider og sociale medier viser en mindre, beskåret del af et billede, som brugere eller udviklere har delt. I mange tilfælde anvender digitale platforme ansigtsopdagelse til automatisk at beskære det oprindelige billede, uden at ansigtet på de personer, som optræder centralt i billedet, skæres bort. (Shamma 2020; Vincent 2021)

Personidentifikation

Når man hører ordet ”ansigtsgenkendelse”, vil mange nok umiddelbart tænke på den form, som handler om at identificere personer.

Personidentifikation hviler på de to første former for ansigtsgenkendelse. For at identificere personer på et billede, skal software først opdage ansigter, og derpå analysere strukturen for disse ansigter. Efterfølgende kan en algoritme sammenligne ansigtsaftryk som findes i billedet med kendte ansigtsaftryk i en database. Til sidst vurderer algoritmen hvor meget de opdagede og kendte ansigtsaftryk matematisk minder om hinanden. (Kortli et al 2020; Li et al 2020)

Kameralås på mobilen

Den måske mest almindelige erfaring med individuel verifikation er brugen af kameralås på mobiltelefoner. Mange telefoner giver mulighed for, at telefonen tager et billede af brugeren, og analyserer ansigtet. Når brugeren efterfølgende skal låse telefonen op, kan kameraet igen analysere brugerens ansigt, og sammenligne med det gemte ansigtsaftryk. Hvis de to ansigter vurderes at være identiske, er brugerens identitet verificeret, og mobilen låser op. Data kan genereres og lagres lokalt, så det kun er brugeren selv, som har adgang til det.

Analysen kan bruges både til individuel verifikation og til bredere identifikation. Ved en verifikation bliver det opdagede ansigtsaftryk sammenlignet med ansigtsaftrykket fra en bestemt person i databasen. Hvis algoritmen vurderer, at der er tilstrækkelig stor lighed mellem de to ansigtsaftryk, så bekræfter den, at der er tale om den samme person.

Automatisk billedsortering og -tagging

En almindelig erfaring med anvendelse af personidentifikation er automatisk billedsortering eller -tagging. Mange mobiltelefoner og digitale platforme er udstyret med funktioner, der kan identificere personer på billederne, og hjælpe brugere med automatisk at sortere billeder eller foreslå tags, som identificerer personer på billederne. Det giver eksempelvis brugeren mulighed for at søge i eller hurtigt gennemse billeder af bestemte personer.

Ved bred identifikation bliver det opdagede ansigtsaftryk sammenlignet med alle ansigtsaftryk i databasen. Algoritmen analyserer ligheden med hvert af de kendte ansigtsaftryk, og vurderer sandsynligheden for, at der er tale om den samme person. Resultatet, som gives til brugeren, kan være en eller flere kendte personer, hvis ansigtsaftryk minder tilstrækkeligt meget om det registrerede ansigtsaftryk til, at det er sandsynligt, at de(t) kunne være den samme person.

Demografisk identifikation

Ansigtsgenkendelse forbindes ofte med personidentifikation. Teknologien kan imidlertid også bruges til at analysere andre typer information. Et oplagt eksempel er demografisk identifikation, hvor algoritmen forsøger at fastslå eksempelvis køn, alder eller etnicitet for personer på et billede.

For at analysere sådanne demografiske informationer, trænes algoritmen til at genkende dem. Ved at træne på store datasæt, kan en læringsalgoritme bygge en model for sammenhænge mellem visse mønstre i billeddata, og de relevante demografiske karakteristika. (Zheng et al 2020) Efterfølgende kan algoritmen anvende modellen til at klassificere opdagede ansigter i et konkret billede.

Kundesegmentering i butikker

Mange butikker kan have interesse i at vide, hvilke kundegrupper som besøger butikken, for eksempel for at undersøge effekten af kampagner, eller variationer i hvilke grupper, som handler på forskellige tidspunkter. Demografisk identifikation kan hjælpe med at skabe et sådant overblik, ved at registrere antallet af forskellige typer kunder på forskellige tidspunkter. Disse data kan være aggregerede, og behøver ikke at kobles til kunders personlige identitet. (Zetland 2021)

Ansigtsgenkendelse kan kombinere demografisk og personidentifikation, men kan også anvende demografisk identifikation alene. I dette tilfælde registrerer ansigtsgenkendelsen kun, at der på billedet er en person med de pågældende demografiske karakteristika, men ikke hvilken person, der er tale om.

Demografisk identifikation er typisk en sværere opgave for ansigtsgenkendelse end personidentifikation, blandt andet fordi personer i forskellig grad minder om eller afviger fra de generelle mønstre, som modellen har fundet. Det kender vi også fra menneskelige vurderinger, hvor det eksempelvis ind imellem kan være vanskeligt at vurdere en persons alder, fordi de ikke ser ud på den måde, som er typisk for deres aldersgruppe.

Afsløring af seksuel orientering

I et berømt studie har forskere vist, at en specialtrænet algoritme var i stand til at vurdere personers seksuelle orientering, ved at analysere profilbilleder fra et datingsite. Med fem billeder som reference kunne algoritmen skelne mellem hetero- og homoseksuelle mænd i 91% af tilfældene, og mellem hetero- og homoseksuelle kvinder i 83% af tilfældene. I begge tilfælde var dette langt mere præcist, end når mennesker forsøgte samme opgave. (Wang & Kosinski 2018)

Udtryks- og affektidentifikation

Den sidste centrale opgave for ansigtsgenkendelse er analyse af personers ansigtsudtryk, for derved at vurdere deres følelser. Er personen stresset eller afslappet? Glad eller ked af det? Bange eller tryg? Mennesker signalerer ofte deres følelser gennem ansigtsudtryk, og en analyse af disse udtryk giver derfor mulighed for at software kan forsøge at vurdere, hvad de pågældende personer føler.

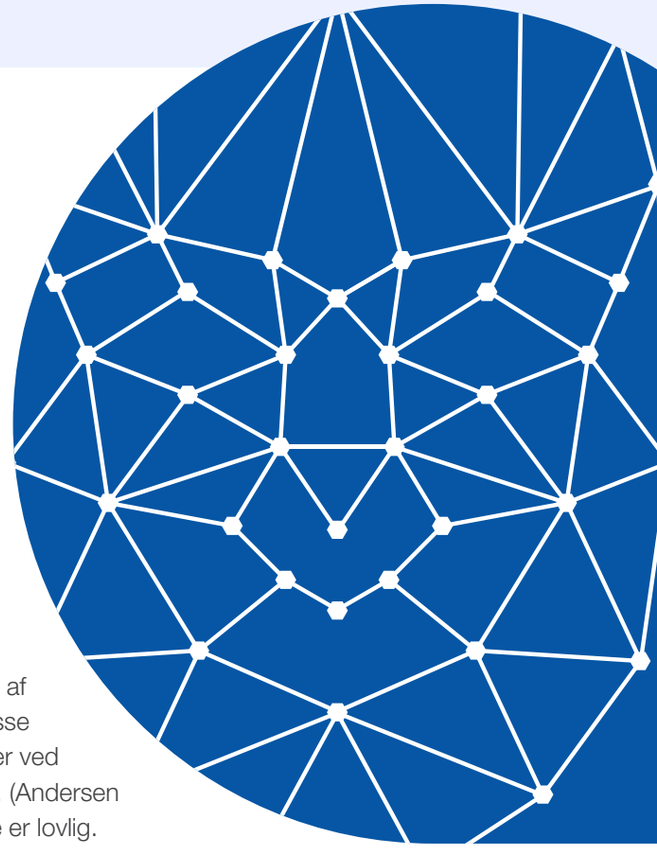
Software til udtryks- og affektidentifikation går til opgaven på samme måde, som med demografisk identifikation ovenfor. En læringsalgoritme træner en model på et stort sæt træningsdata, som knytter visse strukturer i billeder af personers ansigter sammen med ansigtsudtryk og følelser. Det måske mest enkle eksempel er, at en mund formet på bestemte måder er et smil, og at dette typisk er forbundet med glæde. (Ko 2018; Li & Deng 2020)

Ligesom for demografisk identifikation kan udtryks- og affektidentifikation kobles sammen med personidentifikation, men også anvendes selvstændigt. I dette tilfælde giver anvendelsen alene information om, at der på billedet er personer med visse ansigtsudtryk, men ikke hvem disse personer er. Og ligesom for demografisk identifikation har udtryks- og affektidentifikation vist sig at være teknisk vanskeligere end personidentifikation. (Xu et al 2021)

Kundetilfredshed og lyssky adfærd i butikker

Mange butikker kan have interesse i at registrere kunders udtryk og affekt, for eksempel for at vurdere, om de har været tilfredse med oplevelsen af at handle. Ansigtsgenkendelse kan eksempelvis registrere en kundes udtryk når kunden træder ind i butikken, og sammenligne med udtrykket når kunden forlader butikken. Data kan aggregeres, og behøver ikke at være koblet til kundens personlige identitet. Butikker kan også have interesse i at registrere mistænkelig adfærd. Ansigtsgenkendelse kan eksempelvis forsøge at registrere udtryk og adfærd som ofte er forbundet med butikstyveri, og gøre personalet opmærksom på dette, når denne adfærd opdages. (Zetland 2021)

Tre centrale eksempler



1

Adgangsbegrænsning til fodboldstadion

Et kendt eksempel på ansigtsgenkendelse i Danmark er Brøndby Stadions anvendelse til at identificere fans, som er blevet sat på en karantæneliste. Systemet tager billeder af tilskuere ved indgangene til stadion, og sammenligner disse med billeder af fans, som er blevet bortvist fra stadion. Hvis en af disse fans genkendes, giver systemet besked til kontrollører ved indgangen, som kan afvise den pågældende person. (Andersen 2020) Datatilsynet har vurderet, at denne anvendelse er lovlig. (Datatilsynet 2019)

2

Adgangskontrol i fitnesscentre

Nogle danske fitnesscentre anvender ansigtsgenkendelse med personidentifikation til at give kunder adgang til centret. (se e.g. JustFace) I nogle tilfælde er dette et valgfrit alternativ til et traditionelt nøglekort, i andre tilfælde forudsætter medlemskab af centret, at kunden giver samtykke til ansigtsgenkendelse. Formålet kan dels være indsamling af statistik om hvordan kunder bruger centerets faciliteter, men det er typisk at sikre, at kun medlemmer af centret har adgang til faciliteterne.

Datatilsynet udtalte i en afgørelse fra 2022 en advarsel til et fitnesscenter, som anvendte ansigtsgenkendelse på denne vis, fordi kunder ikke blev anmodet om samtykke til brugen af ansigtsgenkendelse til indsamling af statistisk information, og fordi kameraet var placeret ved centerets indgang således, at det kunne behandle personer, som ikke var kunder i centeret, og som derfor ikke havde samtykket til databehandlingen. (Datatilsynet 2022) Til gengæld vurderede Datatilsynet at centerets anvendelse af ansigtsgenkendelse til brug for adgangskontrol var lovlig, for de kunder som havde afgivet informeret samtykke til dette.

3

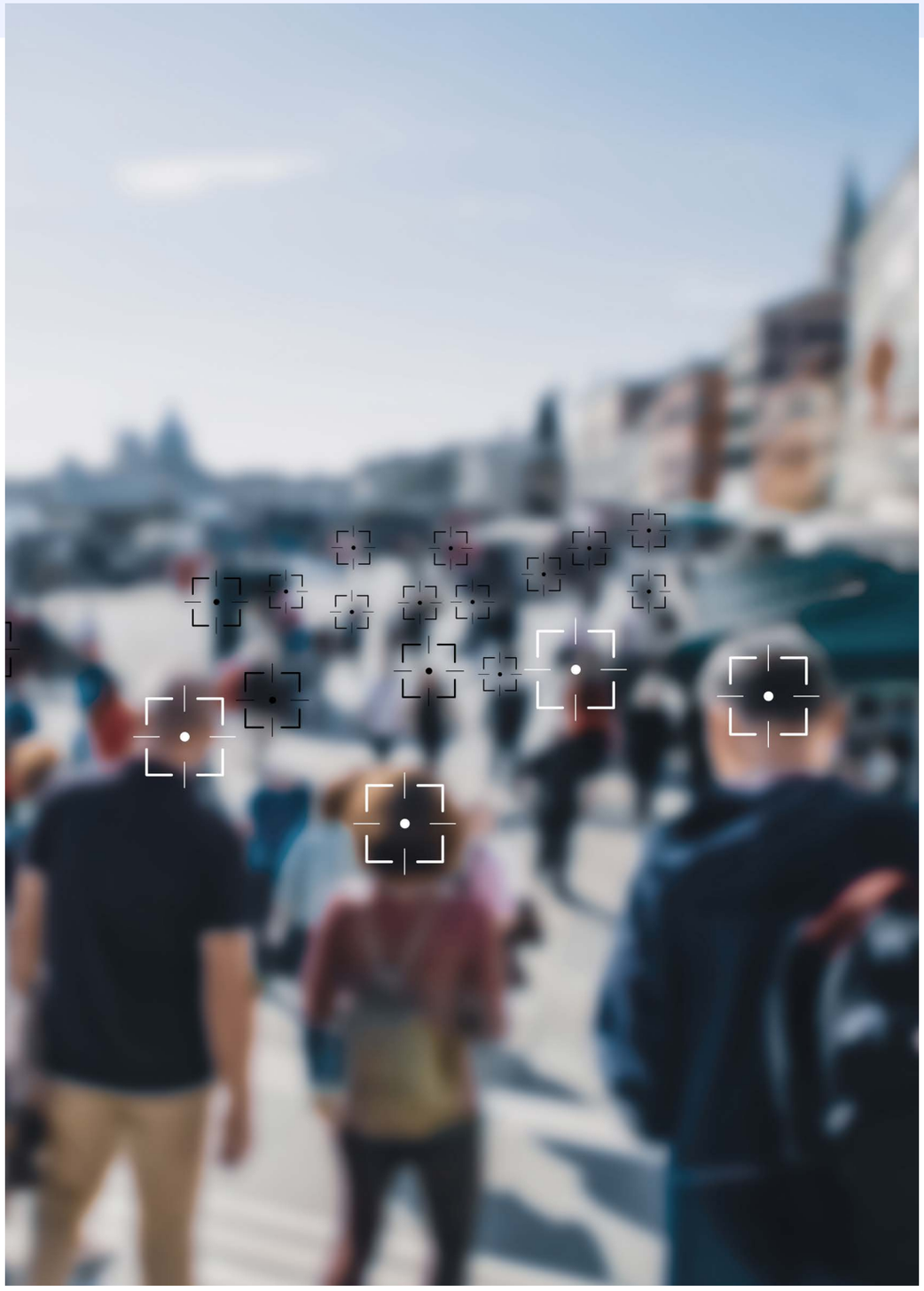
Politiets brug af ansigtsgenkendelse i det offentlige rum

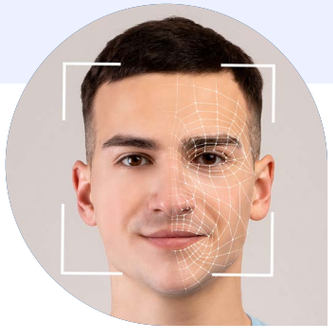
En af de mest omdiskuterede anvendelser af ansigtsgenkendelse er når politi bruger det til personidentifikation. Politi i blandt andet USA og UK har anvendt ansigtsgenkendelse i kropskameraer båret af politifolk på patrulje, og i stationære kameraer opsat på offentlige steder. (Government Accountability Office 2021; Lee & Chin 2022; Woodhams 2021) Ansigtsgenkendelse kan i denne sammenhæng anvendes til at identificere de personer, som politiet interagerer med, og til automatisk at opdage eftersøgte personer, således at politiet kan pågribe dem.

Politi i Danmark anvender kun ansigtsgenkendelse i forbindelse med paskontrol i lufthavne. (Justitsministeriet 2018) I lufthavnen kan ansigtsgenkendelse verificere rejsendes identitet, ved at sammenholde information i passet med et billede af den pågældende som tages på stedet. (CPH 2017)

Imidlertid har Københavns Politi talt for at give politiet mulighed for at bruge ansigtsgenkendelse (Hansen 2019), ligesom KMD har talt for at give politiet mulighed for at bruge ansigtsgenkendelse til eftersøgning efter hollandsk model. (Jayatissa 2022)

I den hollandske model har politiet oprettet en særlig biometri-enhed med ansvar for ansigtsgenkendelse. Når politiet ønsker at identificere en person på et billede, for eksempel en mistænkt som optræder på videomateriale, så sender de materialet til den særlige enhed med en forespørgsel om at få identificeret den pågældende. Biometri-enheden oplyses ikke om sagen, men har adgang til politiets database med personer, og politiets software til at sammenligne materialet med denne database. Hvis søgningen identificerer den pågældende person, og resultatet er tilstrækkeligt pålideligt, så sendes information om vedkommendes identitet retur til de politifolk, som efterforsker den konkrete sag. (World Economic Forum 2021)





2.

Hvordan lærer computeren at genkende ansigter?

Datavidenskab har arbejdet med ansigtsgenkendelse i flere årtier. Indtil omkring 2012 havde software til ansigtsgenkendelse imidlertid relativt lav præcision. Algoritmerne havde ofte svært ved at genkende ansigter når lysforholdene varierede, eller når ansigter på billederne ikke var i samme størrelsesforhold. Det ændrede sig med introduktionen af ansigtsgenkendelse baseret på træning af dybe neurale netværk. (Li et al. 2020; Taskiran et al. 2020; Wang & Deng 2021)

Et neuralt netværk er en avanceret algoritme, som består af en samling af forbundne knudepunkter, en slags digitale "neuroner", der hver for sig udfører matematiske operationer på det data, som netværket fodres med.

Knudepunkterne i det første lag modtager data fra et datasæt, for eksempel billeddata. Når et knudepunkt har udført sine matematiske operationer på disse data, så sender det resultatet videre til et eller flere knudepunkter i netværkets næste lag. Disse knudepunkter tager data fra netværkets første lag som input, og udfører en ny serie af operationer. Det sidste knudepunkt leverer algoritmens samlede resultat.

Dette resultat kan for eksempel være hvor i billeddata algoritmen har opdaget ansigter, hvilken matematisk struktur algoritmen har udledt af et opdaget ansigt, eller hvor meget de matematiske strukturer for to ansigter minder om hinanden.

Neurale netværk kan være mere eller mindre komplekse afhængigt af hvor mange knudepunkter netværket indeholder, og af hvor mange lag disse knudepunkter er organiseret i. Enkle opgaver kan ofte løses af relativt enkle neurale netværk, mens komplekse opgaver som billedanalyse ofte kræver mere komplekse neurale netværk med mange knudepunkter og lag.

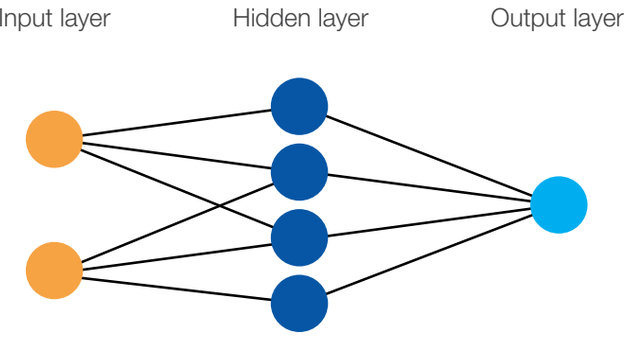
I dag er mange programmer til ansigtsgenkendelse i stand til at udføre nogle opgaver på niveau med eller bedre end mennesker. Det gælder eksempelvis verifikation. Omvendt er der opgaver, hvor det stadig er vanskeligt at træne ansigtsgenkendelse med høj kvalitet. Det gælder for eksempel demografisk identifikation. (Hupont et al 2022; Zheng et al 2020)

Dybe neurale netværk kan ikke meningsfuldt specificeres af mennesker. Neurale netværk trænes derfor med maskinlæring, hvor en læringsalgoritme gradvist tilpasser de operationer som hvert knudepunkt udfører, indtil netværket er blevet så godt til at løse opgaven som muligt.

Kombinationen af maskinlæring og kompleksitet gør, at dybe neurale netværk typisk er meget uigennemsigtige. Det er vanskeligt for mennesker at forstå, præcis hvordan det neurale netværk fungerer, og at forudsige hvilket svar det vil levere for et givet input. (Weitz et al. 2019; Molnar 2022, chapter 10)

Maskinlæring betyder også, at algoritmens kvalitet afhænger af hvilke træningsdata udvikleren har adgang til. For at udvikle velfungerende ansigtsgenkendelse vil udvikleren typisk have brug for et stort datasæt, som minder om de data, som algoritmen vil møde, når den tages i anvendelse. Det har de seneste år vist sig at være en væsentlig udfordring for udvikling af ansigtsgenkendelse, at skaffe træningsdatasæt som på engang er store, af høj kvalitet, og repræsentative for de forskellige grupper, som algoritmen efterfølgende skal anvendes på.

Et simpelt neuralt netværk



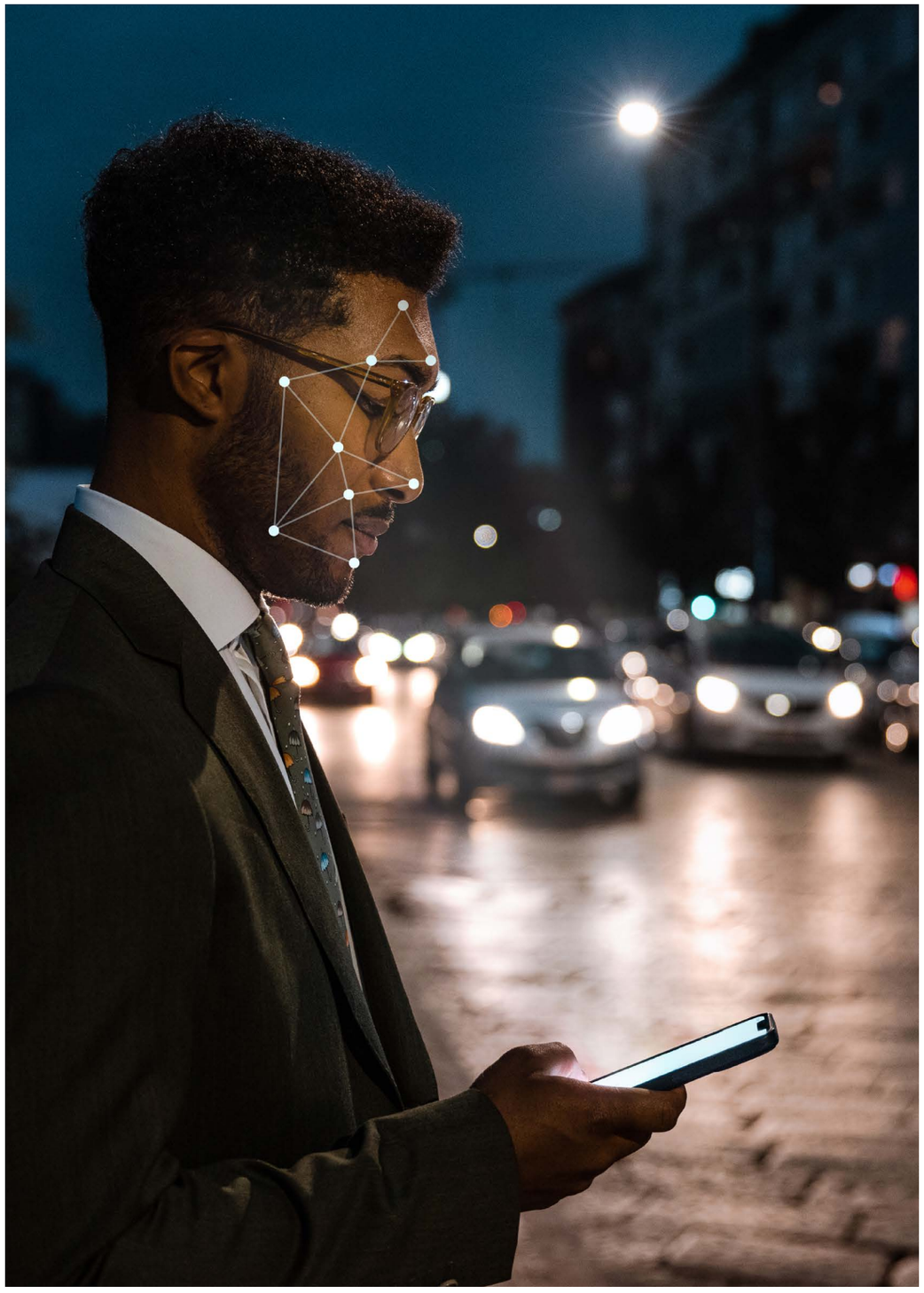
3.

Hvad er relevant for at vurdere ansigtsgenkendelse?

Anvendelse af ansigtsgenkendelse har i nogle tilfælde været kontroversiel. Kritikere har rejst bekymringer om eksempelvis indskrænkning af privatliv og uønskede incitamenter (Access Now et al 2021), indsamling og anvendelse af private data (Skovgaard 2021; Heikkilä 2022), variationer i præcision og fejltyper over relevante grupper (Bacchini & Lorusso 2019; Grother et al. 2019; Robinson et al. 2020), og misbrug af teknologien blandt andet i form af såkaldt "function creep" (Brey 2004; Smith & Miller 2022).

Ansigtsgenkendelse er imidlertid ikke én ting, men en type teknologi med mange forskellige anvendelser. Vurderingen af fordele og ulemper ved en specifik anvendelse af ansigtsgenkendelse kan afhænge af en række faktorer.

Faktor		Eksempler
Formål	Hvad er den intenderede effekt af at anvende teknologien?	Adgangsbegrænsning; eftersøgning af en specifik person; kundesegmentering
Samtykke	Har de personer, som teknologien anvendes på, samtykket til anvendelsen?	Samtykke med mulighed for at tilgå den samme tjeneste uden anvendelse af ansigtsgenkendelse hvis samtykke nægtes; samtykke obligatorisk for at tilgå en tjeneste; intet samtykke
Adgang til data	Hvem har adgang til de data som teknologien anvender og genererer?	Data lagres lokalt og kan kun tilgås af den enkelte bruger; data lagres centralt og kan tilgås af udviklere
Dataproduktion	Hvilke data genererer ansigtsgenkendelsen?	Ansigtsopdagelse; biometrisk ansigtsaftryk; en-til-en verifikation; en-til-mange identifikation; demografiske data; udtryks- og/eller affektdata
Database	Hvilke data trækker teknologien på i trænings- og anvendelsesfaserne?	Specialiserede træningsdatabaser; sociale medier; offentlige registre; brugerdata
Aktør	Hvem anvender teknologien?	Offentlige myndigheder, virksomheder; privatpersoner
Målgruppe	Hvem anvendes teknologien på?	Børn og unge; patienter; kunder; medarbejdere; personer i det offentlige rum
Anvendelsesområde	Hvor anvendes teknologien?	Det offentlige rum; arbejdspladser; fængsler; butikker; uddannelsesinstitutioner
Kvalitet	Hvor mange og hvilke fejl begår teknologien?	Præcision; genkald; F1-score; AUC
Fejl	Hvilken betydning har de fejl som teknologien begår?	Bruger kan ikke låse sin mobil op; forkert person identificeres som eftersøgt; kamerafokus fungerer dårligt for visse grupper



Litteratur

Access Now, Amnesty International, European Digital Rights, Human Rights Watch, Internet Freedom Foundation, Instituto Brasileiro de Defeso do Consumidor (2021): “Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance.” 7 June.

Andersen, T. (2020): “Sådan fungerer Brøndby Stadions ansigtsgenkendelse.” Version2. 17. februar.

Bacchini, F. & Lorusso, L. (2019): “Race, again: how face recognition technology reinforces racial discrimination.” Journal of Information, Communication and Ethics in Society, vol. 17 (3): 321-335. https://doi.org/10.1108/JICES-05-2018-0050

Brey, P. (2004): “Ethical aspects of facial recognition systems in public places.” Journal of information, Communication and Ethics in Society, vol. 2 (2): 97-109. https://doi.org/10.1108/14779960480000246

CPH (2017): ”Automatisk paskontrol indviet i Københavns Lufthavn.” 18. juni.

Datatilsynet (2019): ”Tilladelse til behandling af biometriske data ved brug af automatisk ansigtsgenkendelse ved indgange på Brøndby Stadion.” 24. maj.

Datatilsynet (2022): “Datatilsynet har truffet afgørelse i en sag om brugen af et system til ansigtsgenkendelse.” 17. marts.

Government Accountability Office (2021): “Facial Recognition Technology: Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used By Employees.” 13 July.

Grother, P., Ngan, M., & Hanaoka, K. (2019): "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects." National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8280

Hansen, F.M. (2019): "Københavns Politi vil bruge ansigtsgenkendelse." Version2. 24. oktober.

Heikkilä, M. (2022): "The walls are closing in on Clearview AI." MIT Technology Review, May 24.

Hupont, I., Tolan, S., Gunes, H., & Gómez, E. (2022): "The landscape of facial processing applications in the context of the European AI Act and the development of trustworthy systems." Nature Scientific Reports vol 12: 10688. https://doi.org/10.1038/s41598-022-14981-6

Jayatissa, H. (2022): "KMD: Politiet skal have mulighed for at bruge ansigtsgenkendelse." Altinget. 22. september.

Justitsministeriet (2018): "Endelig besvarelse af spørgsmål nr. 926." 21. august.

Ko, B.C. (2018) "A Brief Review of Facial Emotion Recognition Based on Visual Information." Sensors vol. 18 (2): 401. https://doi.org/10.3390/s18020401

Kortli, Y., Jridi, M., Falou, A.A., & Atri, M. (2020): "Face Recognition Systems: A Survey." Sensors vol. 2 (2): 342. https://doi.org/10.3390/s20020342

Kulager, Frederik (2021): "Nu aflæser butikker dit humør, køn, alder og etnicitet." Zetland. 17. maj.

Lee, N.T. & Chin, C. (2022): "Police surveillance and facial recognition: Why data privacy is imperative for communities of color." Brookings Institute Report. 12 April.

Li, L., Mu, X., Li, S., & Peng, H. (2020): "A Review of Face Recognition Technology." IEEE Access vol. 8: 139110-139120. https://doi.org/10.1109/ACCESS.2020.3011028

Li, S. & Deng, W. (2020): "Deep Facial Expression Recognition: A Survey." IEEE Transaction on Affective Computing. https://arxiv.org/abs/1804.08348

Molnar, C. (2022): "Interpretable Machine Learning." https://christophm.github.io/interpretable-ml-book/

Rahman, M.T. & Kehtarnavaz, N. (2008); "Real-time face-priority auto focus for digital and cell-phone cameras." IEEE Transactions on Consumer Electronics vol. 54 (4): 1506-1513. https://doi.org/10.1109/TCE.2008.4711194

Robinson, J.P., Livitz, G., Henon, Y., Qin, C., Fu, Y., & Timoner, S. (2020): "Face Recognition: Too Bias, or Not Too Bias?" Conference on Computer Vision and Pattern Recognition (CVPR) Workshops. https://arxiv.org/abs/2002.06483

Shamma, D.A. (2020): "Behind Twitter's Biased AI Cropping and How to Fix It." Medium. 29 September.

Skovgaard, L. (2021): "Kæmpebøde til kontroversiel ansigtsgenkendelse: Datatilsyn straffer Clearview AI." Version2, 2. december.

Smith, M., & Miller, S. (2022): "The ethical application of biometric facial recognition technology." AI & Society, vol. 37: 167-175. https://doi.org/10.1007/s00146-021-01199-9

Swedish Data Protection Authority (2019): "Supervision pursuant to the General Data Protection Regulation (EU) 2016/679 – facial recognition used to monitor the attendance of students."

Taskiran, M., Kahraman, N., & Erdem, C.E. (2020): "Face recognition: Past, present and future (a review)." Digital Signal Processing vol. 106: 102809. https://doi.org/10.1016/j.dsp.2020.102809

Vincent, J. (2021): "Twitter's photo-cropping algorithm prefers young, beautiful, and light-skinned faces." The Verge. 10 August.

Wang, M. & Deng, W. (2021): "Deep Face Recognition: A Survey." Neurocomputing vol. 429: 215-244. https://doi.org/10.1016/j.neucom.2020.10.081

Wang, Y. & Kosinski, M. (2018): "Deep neural networks are more accurate than humans at detecting sexual orientation from facial images." Journal of Personality and Social Psychology vol. 114 (2): 246-257. https://psycnet.apa.org/doi/10.1037/pspa0000098

Weitz, K., Hassan, T., Schmid, U., Garbas, J.U. (2019): "Deep-learned faces of pain and emotions: Elucidating the differences of facial expressions with the help of explainable AI methods." tm - Technisches Messen, vol. 86 (7-8): 404-412. https://doi.org/10.1515/teme-2019-0024

World Economic Forum (2021): "A Policy Framework for Responsible Limits on Facial Recognition – Use Case: Law Enforcement Investigations." October.

Woodhams, S. (2021): "London is buying heaps of facial recognition tech." Wired. 27 September.

Xu, T., White, J., Kalkan, S., & Gunes, H. (2021): "Investigating Bias and Fairness in Facial Expression Recognition." European Conference on Computer Vision. https://arxiv.org/abs/2007.10075

Zheng, X., Guo, Y., Huang, H. Li, Y. & He, R. (2020): "A Survey of Deep Facial Attribute Analysis." International Journal of Computer Vision vol.128: 2002–2034. https://doi.org/10.1007/s11263-020-01308-z

Grafisk design: omw.dk

NATIONALT
CENTER FOR ETIK

Ørestads Boulevard 5
2300 København S
dketik@dketik.dk
nationaltcenterforetik.dk

Dataetisk
Råd