2020

Ansigtsgenkendelse

Ansigtsgenkendelse som teknologi, og hvilken effekt anvendelsen af den har.

GRUPPE: S2024791300

EKSAMEN: U24791

FRANS AUGUST NAUTRUP RAVN STADSBJERG - 69215, HAMED TOUNSI - 68841, MATHIAS ULRIK PONZANI – 69354 OG RASMUS LAUE PETERSEN – 68907

VEJLEDER: OLE MONRAD

ROSKILDE UNIVERSITET | HUMTEK

Frans August Nautrup Ravn Stadsbjerg - 69215
Hamed Tounsi - 68841
Mathias Ulrik Ponzani – 69354
Rasmus Laue Petersen – 68907

03/06/2020
Roskilde Universitet | HUMTEK

Abstract

In this report we investigate the aspects of facial recognition as a technology and it's implementation in our society as surveillance and convenience in everyday life. This will be uncovered by applying different tools, methods and theories, such as TRIN-Model and Shoshana Zuboffs views and theory of surveillance capitalism. We have conducted our own experiment with use of the HIC-program to illustrate some the problems that might appear within 2D facial recognition. This indicated that the illumination and colours within the images had an effect on the result. Furthermore we look into the legislations within EU and Denmark to reveal the effects it has on the distribution of this technology. The report concludes that facial recognition has evolved to a degree where its use has surpassed other biometric data recognition technologies. Although we acknowledge that face recognition technology has challenges, that other biometric data recognition systems don't.

Indholdsfortegnelse

Indledning

Denne rapport vil gå i dybden med ansigtsgenkendelsesteknologi og hvordan denne teknologi fungerer. Til dette anvendes TRIN-modellen. Rapporten vil derudover beskæftige sig med lovgivningen omkring teknologien inden for Europas og Danmarks grænser. I løbet af rapporten vil der blive arbejdet med Shoshana Zuboffs teori om overvågnings kapitalisme og Everett Rogers' innovation teori. Med disse teorier for øje, ønsker vi at undersøge de barrierer, der kan være en udfordring for teknologien. Herefter vil der blive udført et eksperiment med HIC-programmet, der skal være med til at give en visuel fremstilling af problematikkerne som denne teknologi besidder. Da vil en diskussion fremgå i rapporten, hvor de tekniske aspekter og lovgivningens påvirkning blive diskuteret. Ultimativt vil rapporten give en konklusion på vores problemformulering, *"Hvordan fungerer ansigtsgenkendelse som teknologi, og hvilken effekt har anvendelsen af teknologien?"*.

Problemfelt

I nedenstående tekst uddybes det område vi ønsker at arbejde med, inden for face recognition technology.

Ansigtsgenkendelsesteknologi bliver i stigende grad en del af hverdagsbilledet i samfundet, og ofte uden at befolkningen er klar over det. Teknologien bliver i høj grad benyttet kommercielt af firmaer som Apple og Facebook. I 2017 udsendte Apple deres første Iphone som i stedet for fingeraftryks teknologi, anvendte Face ID. Hvor vi førhen brugte personlige koder og fingeraftryk som sikkerhedsforanstaltninger, bruger man, blot tre år efter Face ID´s lancering, primært ansigtsgenkendelse i nyere mobile enheder (Savov, 2017). Det sociale medie facebook, benytter sig af ansigtsgenkendelses teknologi til at analysere billeder og videoer af brugerne, så firmaet kan identificerer den pågældende bruger på nye billeder. Facebooks brug af teknologien var omdrejningspunktet for et søgsmål mod firmaet. Det var en gruppe borger fra den amerikanske delstat Illinois som stod bag, da de mente at Facebook ulovligt gemte data fra millioner af bruger uden at have deres samtykke. Sagen blev afsluttet i januar 2020 efter at parterne indgik et forlig,

og Facebook endte med at skulle betale 3,7 milliarder kroner("Facebook indgår milliardforlig og afværger retssag om ansigtsgenkendelse", 2020).

Selv om den kommercielle brug af ansigtsgenkendelsesteknologi til tider har været kontroversiel, så bliver teknologien i endnu højere grad anvendt i det offentlige rum. Kina er det land i verden hvor teknologien er mest udbredt i netop det offentlige rum. I 2019 blev det obligatoriske at borgerne i Kina skulle have deres ansigt scannet hvis de ville købe et simkort (Moltke, 2020). Det er derudover kommet frem at den kinesiske stat benytter ansigtsgenkendelse til masseovervågning af visse befolkningsgrupper heriblandt den etniske minoritetsgruppe Uighurerne, der bliver udsat for konstant overvågning og kan ikke bevæge sig frit omkring uden deres adfærd bliver registreret ("One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority", 2020).

Motivation

Vi finder det interessant at noget vi bruger som sikkerhed, samtidigt kan bruges til at identificere os ud fra fotografier på sociale medier og overvågningskameraer. Det ses i stigende grad at data skrabet fra de sociale medier kan bruges til at identificere individer med uhyggelig høj nøjagtighed. Det kan være et vigtigt og revolutionerende værktøj når dette er brugt til at opklare forbrydelser langt hurtigere end man før har været vant til (Hill, 2020). Men der er også en lang række problematikker forbundet med en teknologi som med utrolig lethed kan forbinde et billede med alt den information der findes på internettet om individet der er afbilledet. Teknologi som er designet til at beskytte os og vores personlige data, kan altså blive brugt imod os, og være med til at fjerne alle former for personlig anonymitet. Det kan derfor virke paradoksalt at en sikkerhedsteknologi kan være med til at gøre fremtiden mere usikker og der ligger et kæmpe ansvar hos de teknologivirksomheder som er med til at drive udviklingen af de enheder som vi alle sammen i højere grad bliver mere afhængige af, i takt med verden bliver mere og mere digitaliseret.

Det er samtidigt relevant da vi samfundsmæssigt ser et større fokus på teknologien og en stor del af samfundet i forvejen bruger teknologien. Politiet bruger nummerpladegenkendelse via mobile

patruljer og faste kamera installationer, hvilket kan være med til at bane vejen for udbredelsen af ansigtsgenkendelse inden for håndhævelse af loven (Datatilsynet, 2015). Derfor er det også et teknologiområde som kræver væsentlig opmærksomhed fra lovgivernes side.

Dette tekniske aspekt har blandt andet motiveret os til at undersøge denne problemstilling, og undersøge hvordan ansigtsgenkendelses anvendt i praksis, kan være med til at øge eller forringe sikkerheden samt hvilke konsekvenser udbredelsen af teknologien kan have, da det kan få en betydelig indvirkning på vores samfund i fremtiden. Ansigtsgenkendelse er et teknologisk system som bygger på en række af de mest banebrydende teknologier såsom Big data, maskinlæring i form af billedgenkendelse, og kunstig intelligens. Det er alle teknologier med utroligt spændende perspektiver, men bringer samme tid risiko for at teknologierne kan skabe en række utilsigtede konsekvenser, både i positiv og negativ forstand.

Problemformulering

Vi vil derfor gerne undersøge hvordan ansigtsgenkendelse fungere i praksis og som teknologisk system, samt de eksterne faktorer der har indflydelse på teknologiens fortsatte udvikling.

Hvordan fungerer ansigtsgenkendelse som teknologi, og hvilken effekt har anvendelsen af teknologien?

Til at besvare vores problemformulering har vi udarbejdet en række arbejdsspørgsmål.

Arbejdsspørgsmål:

- Hvad er ansigtsgenkendelse teknologi?
- Hvordan fungerer de centrale mekanismer og processer der udgør ansigtsgenkendelses teknologi?
- Hvordan bliver ansigtsgenkendelsesteknologi anvendt som overvågning?
- Hvilke metoder bliver der anvendt for at sikre en høj præcisering af ansigtsgenkendelse?

- Hvilke udfordringer har udbredelsen af ansigtsgenkendelse ift. lovgivning?

Metode

Vi vil i denne del af rapporten komme ind på de metoder, vi mener er brugbare ift. vores projekt, heriblandt er deduktiv metode og komparativ metode. Derudover har vi også tilføjet TRIN-modellen til dette afsnit, som vi nedenfor vil redegøre for.

TRIN-modellen

Vi anerkender at TRIN-modellen ikke ses som en metode, men vi vil i denne rapport arbejde metodisk ved anvendelse af TRIN-modellen. Den metodiske anvendelse af TRIN-modellen opstår, ved at vi analyserer teknologien ud fra et sæt retningslinjer som modellen stiller til rådighed. Vi har i denne forbindelse gjort os overvejelser omkring hvilke delelementer der er relevante for vores projekt at kigge nærmere på. I dette afsnit vil vi gennemgå og redegøre de forskellige trin i TRIN-modellen. Her ønsker vi at argumentere for hvilke dele af modellen vi finder relevante ift. vores projekt.

1. Teknologiens indre mekanismer og processer

Trin 1 af TRIN-modellen beskæftiger sig med at skabe en forståelse for, hvordan en teknologi fungerer. Dette punkt går altså i dybden med hvilke principper, der gør teknologien mulig (Jørgensen, 2019). Trin 1 i modellen vil derfor være yderst relevant at kigge på ift. ansigtsgenkendelsesteknologi. Dette er relevant da vi ved at kigge på teknologien gennem processerne heri, vil få et dybere indblik i underliggende algoritmer og databaser som anvendes i teknologien.

2. Teknologiske artefakter

Under dette trin bliver der gået i dybden med de forskellige komponenter, der er til for at teknologien kan fungere. Der vil altså blive kigget på de delelementer som ansigtsgenkendelsesteknologi er bygget op omkring (Jørgensen, 2019). Vores rapport kommer ikke til at beskæftige sig med en dybdegående undersøgelse af dette punkt, med f.eks. kameraet som artefakt, men i langt højere grad med tankerne og metodikken der bliver anvendt i teknologien. Hertil bliver der selvfølgelig beskrevet i TRIN-modellen, at informationen i sig selv, altså den viden der er anvendt til at udvikle koden, er et artefakt (Jørgensen, 2019). Her kigger vi allerede på algoritmer gennem bl.a. trin 1. Vi vil undervejs komme ind på bestemte artefakter der er med til at skabe teknologien, men det er ikke noget vi kommer til gå explicit i dybden med.

3. Teknologiers utilsigtede effekter

Dette trin vil gå i dybden med utilsigtede effekter som følge af teknologiens udvikling. I henhold til ansigtsgenkendelse er det som oftest negative effekter, da firmaerne der producerer denne teknologi, typisk har fundet de positive effekter at lancere teknologien med (Jørgensen, 2019). Det vil være yderst interessant for os at kigge på de utilsigtede effekter ved ansigtsgenkendelsesteknologi. Nu bliver denne teknologi så også brugt til overvågning, bl.a. gennem systemet Clearview AI, som vi vil komme ind på længere nede i rapporten (Hill, 2020). Det vil derfor være interessant at kigge på hvordan teknologiens utilsigtede effekter, hænger sammen med de indre mekanismer og processer.

4. Teknologiske systemer

Under punkt 4 i TRIN-modellen bliver der kigget både på et makro system og et delsystem. Her menes altså at man både kan se på hvilke komponenter i selve teknologien der får den til at virke, men også hvordan teknologien kan indgå i et langt større system med andre eksemplarer af samme teknologi (Jørgensen, 2019). Igennem dette punkt, vil det være interessant at kigge på hvordan de forskellige komponenter spiller hver deres rolle i teknologien, altså delsystemet. Det kan omhandle hvordan en database og en algoritme interagerer med hinanden. Derudover ønsker vi også i denne rapport, at kigge på hvordan teknologien fungerer i et makro system, altså hvilke aktører som spiller en rolle i at få denne teknologi til at fungere.

5. Modeller af teknologier

Trin 5 i modellen beskæftiger sig med at skabe en dybere forståelse for hvordan en teknologi fungerer, gennem at kunne etablere viden omkring en teknologi, i en form for model. Dette kan eksempelvis være en visualisering af teknologien (Jørgensen, 2019). Inden for dette punkt vil vi lave et eksperiment ved brug af HIC-programmet der er et billedegenkendelsesprogram, hvilket udfolder sig senere under kapitlet, HIC-eksperimentet. Da 2D ansigtsgenkendelse bygger på mange af de samme principper som normal billedegenkendelse, ønsker vi derfor gennem dette eksperiment, at uddybe en forståelse for hvordan et billedegenkendelsesprogram fungerer, og hvordan man potentielt kan manipulere det.

6. Drivkræfter og barrierer for udbredelse af teknologier

I dette punkt ses der på hvordan en teknologi implementeres i samfundet, og hvilke barriere der måtte opstå i den forbindelse (Jørgensen, 2019). Det er væsentligt for at opnå dette at vi kigger på lovgivningen omkring ansigtsgenkendelsesteknologi. Gennem dette punkt vil vi derfor kunne gå i dybden med hvilke samfundsmæssige problematikker teknologien kan stå over for.

Det er derfor vores intention at gå i dybden med punkterne 1,3,4,5 og 6. Efterladt er punkt 2, "teknologiske artefakter", som vi ikke finder relevant at gå voldsomt i dybden med ift. vores projekt.

Den deduktive metode

Vi vil som tidligere beskrevet udføre et eksperiment i denne rapport. Til udførelsen af dette eksperiment vil vi gøre brug af den deduktive metode. Ved at gøre dette har vi en baggrundsviden inden for feltet, som vi baserer en hypotese på baggrund af. Herefter udfører vi eksperimentet for så at reflektere over de observationer vi foretager os under eksperimentet. Ud fra disse observationer kan vi lave en analyse og dermed af- eller bekræfte vores hypotese, ud fra hvad der

er hændt under eksperimentet. Herefter vil det være muligt at kunne måle de resultater vi får, op mod vores eksisterende viden ("Deduktion, induktion og abduktion", n.d.). Hertil kommer vi naturligvis også til at anvende den viden vi fremlægger i rapporten. Det er på baggrunden af denne viden, at vi kan foretage os kvalificerede bud på, hvordan HIC-programmet vil behandle billedet vi giver.

Komparativ metode

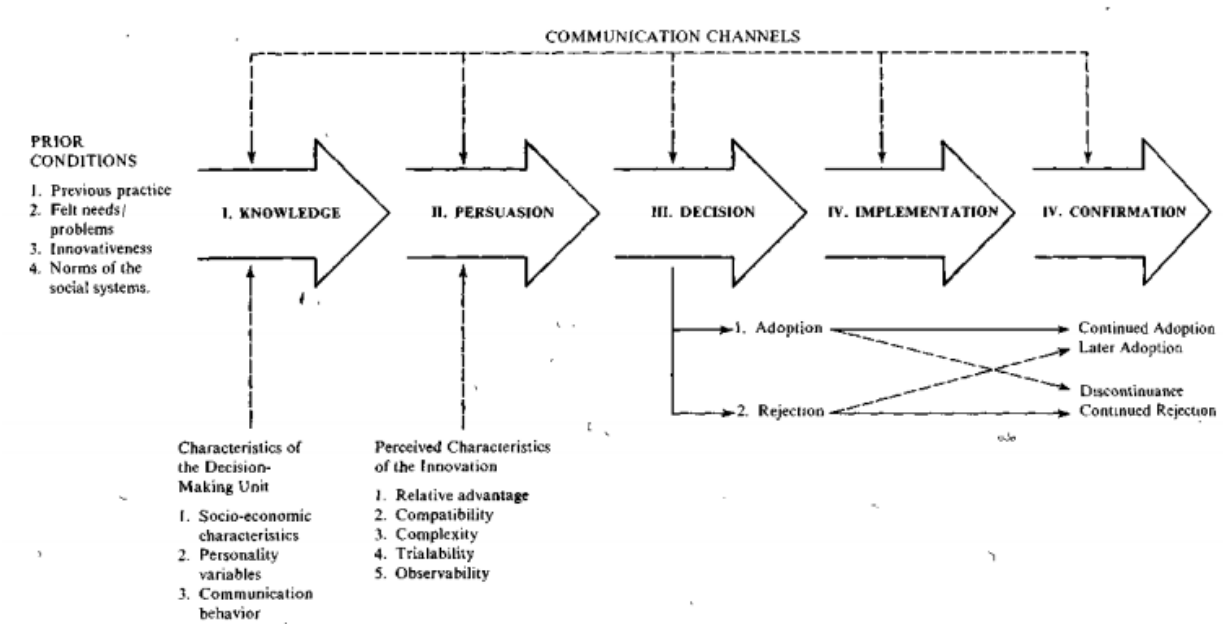
Denne metode anvendes til at holde et sæt data op mod et andet. Man sammenligner altså datasæt eller observationer med hinanden (Boje, 2020). Dette vil hjælpe os med at analysere den data vi får på baggrund af at udføre vores HIC-eksperiment. Derudover ønsker vi også at anvende denne metode i vores søgen af empiri. Dette kan gøres ved at måle de forskellige kilder op mod hinanden for at få skabt et mere nøjagtigt billede af hvor troværdig visse kilder kan være og dermed få opbygget en stærkere kildekritik.

Teori

I dette afsnit vil vi komme ind på de forskellige teorier vi tager udgangspunkt i. Hertil har vi udvalgt innovation teori og overvågningskapitalisme.

Innovation teori

Vi ønsker blandt andet i denne rapport at tage et kig på innovation teori. Dette gøres med henblik på at kunne diskutere udbredelsen af teknologien i samfundet. Her vil vi kigge på Everett Rogers' teori. Denne teori beskriver udbredelsen af teknologien og hvilke kriterier der skal opfyldes for at en teknologi kan etablere sig i et samfund. Heri indgår 4 faktorer for teknologiens udbredelse: opfindelsen, kommunikationskanaler, tid og brugeren (Rogers, 1983). I denne rapport finder vi det mest interessant at kigge på kommunikationskanalerne, og Rogers' opbygning af dem. Han deler kommunikationskanalerne op i 5 dele i en model som ses nedenfor.



Figur 1, Kommunikationkanalers faser (Rogers, 1983)

Denne model er inddelt i 5 faser. De 5 faser er viden, overbevisning, beslutning, implementation og bekræftelse. Første fase omhandler den viden, som indgår i skabelsen af en teknologi. Her dannes det udgangspunkt som er med til at teknologien skal fungere. Anden fase går ud på at teste teknologien. Herefter bliver teknologien evalueret og der bedømmes om den er klar til fase 3. Fase 3 er der hvor beslutningen, om hvorvidt teknologien er klar til bredere implementering. Det er herefter i fase 4 man lancerer teknologien til en bredere gruppe og får det implementeret. I sidste fase, altså fase 5, hvor den endelige beslutning omkring teknologien foretages. Det er altså i den sidste fase teknologien altså får lov til at fortsætte eller om den bliver annulleret. Grunden til vi finder det mest relevant i vores projekt at beskæftige os med denne model er, at vi kan komme ind på den viden der ligger til grunde for teknologien under første fase. Herefter vil vi kunne, ud fra denne teori, kigge på de udfordringer og barrierer der måtte være i implementeringen af teknologien i anden fase. I den forbindelse kan vi også kigge på det som ligger til grunde for fase 3, altså beslutningen for implementeringen i samfundet. Gennem denne teori og model, vil vi altså kunne nemmere give udtryk for hvilke udfordringer ansigtsgenkendelsesteknologi måtte have ift. implementeringen i samfundet med henblik på lovgivningen i Danmark.

Overvågningskapitalisme

I bogen ”The age of surveillance capitalism” giver Shoshana Zuboff en længere definition på overvågningskapitalismen, som kan forkortes til at det er en ny økonomisk orden der udnytter menneskelig oplevelse som gratis råvare til reklame praksis med udvinding, forudsigelse og salg. Derudover beskriver hun det som en parasit økonomisk logik, hvor produktionen af varer og tjenester er underlagt en ny global arkitektur for adfærdsændring og en mutation af kapitalisme der er præget af rigdom, viden og magt der hidtil er uset i menneskets historie.

Zuboff giver et eksempel på hvor overvågningskapitalismen har ramt os, nemlig *Smart Home*. Hun referer til et projekt kaldet ”Aware Home” der blev skabt af en gruppe videnskabsmænd og ingeniører i *Georgia Tech*. Disse videnskabsmænd og ingeniører forestillede sig et system i hjemmet der består af et netværk af sensorer. Disse sensorer ville samle personlig information om individerne der bor i hjemmet, hvilke kun de har adgang til. I dag er ”Smart Home” markedets anslået værdi 36 mia. dollars. De forestillinger videnskabsmændene og ingeniørerne fra Georgia Tech havde til teknologien, har vist sig ikke at være andet end forestillinger, da teknologien tog en helt anden retning. For en teknologi som *Nest thermostat* udfører mange af de opgaver som man forestillede i *Aware Home* projektet, så som at indsamle information om brugerne og miljøet via sensorer. Til forskel for hvordan man havde forestillet sig i *Aware Home* projektet så uploader *Nest thermostat* brugerens data til Googles servere, hvor de derefter bliver delt med andre smart enheder, personale og tredjeparter. Dette kan selvfølge kun lade sig gøre hvis brugeren giver tilladelse ved at acceptere servicevilkårene. Hvilket brugeren nærmest tvinges til, for hvis brugeren ikke accepterer disse vilkår, vil det resultere i at funktionaliteten og sikkerheden af termostaten vil blive kompromitteret. Dette kan føre til at man får frosne rør og røgalarmer der ikke virker.

Overvågningskapitalismen har altså taget magten og udnytter brugerens oplevelse med teknologien/tjenesten og oversætter det til adfærdsdata. Et produkt som en termostat, telefon eller en smart lyspære der kan styres fra en app, er ikke bare det som man forventer, men de er også overvågningsapparater. De gør ikke bare som du beder dem om at gøre, de registrerer hvad du beder dem om, hvornår og hvordan du gør det, og sender den information ind til producentens

servere. Noget af den data bliver brugt til at forbedre teknologien/tjenesten, men resten vil blive brugt til at analysere brugernes adfærd og forudsige hvad forbrugerne vil gøre i morgen og fremover. Den information om forbrugernes adfærd, vil så blive brugt til at producere forudsigelses produkter. Zuboff definer disse produkter som stort set alle produkter der kaldes ”smart”. Alle disse produkter er nemlig koblet til internettet, delvist for at skabe en lethed eller fordel for forbrugeren, men i høj grad også for at kunne videregive forbrugerens information til producenten og tredjeparter.

Overvågningskapitalismen ved alt om forbrugeren, men forbrugeren kan ikke vide noget om hvordan producenten opererer, hvordan informationen bliver behandlet eller hvilke andre parter den bliver delt med.

Anvendelse af overvågningskapitalisme

Shoshana Zuboff pointerer herudover at hjemmet er privat og dermed er et ”helle” man kan trække sig tilbage til efter arbejdsdagen er omme. Med tiden er vores hjem blevet plastret til med forskellige teknologiske artefakter der kan overvåge os i eget hjem, kameraer i fjernsyn, overvågningskamera, webcam i computer, stemmestyret smarthome systemer som google assistent og amazons alexa. Alle disse teknologier har besværliggjort muligheden for privatliv, alle handlinger der bliver udført med og i nærheden af nævnte teknologier bliver analyseret og brugt af andre systemer.

I henhold til ansigtsgenkendelse bliver der forsket i brug af denne til online eksamener for at autentificere og modvirke snyd i form af ophavsret. Tager vi udgangspunkt i 48 timers eksamener på Roskilde Universitet, er det svært at opfange studerende der får andre til at lave deres skriftlige eksamen. Ansigtsgenkendelse inkorporeret i et program der sammenkobler brug af tastaturet i f. eks. Word, med løbende registrering af brugeren via webcam, vil kunne forebygge dette. Da programmet kun søger efter den unikke kode ud fra brugerens ansigt for at få match med den registrerede studerende, vil det ikke krænke privatlivet i form af masseovervågning (Li-jun YU, Ke-feng LI. 2017. Issa T. Et al 2017).

Lignende systemer bliver efterspurgt af arbejdsgivere der vil holde øje med deres medarbejdere når de arbejder hjemmefra. Det er især under Corona krisen hvor folk arbejder hjemmefra, at brugen af arbejdspladser bliver udfordret. (Morrison, 2020)

Et andet sted hvor teknologien vinder ind, er i brugen af betalingsmetoder. Som del af dette tester Nets brug af ansigtsgenkendelse som betalingsmetode i en kantine med 1000 brugere på Østerbro i København. Før dette har Nets forsøgt sig med en anden biometrisk identifikation ved brug af fingeraftryk betaling på Copenhagen Business School.(Nets tester betaling med ansigtet, 2019) det viser en tendens til at man ikke bare forsøger at udfase pengesedler, men også gøre kreditkort overflødige. At gå direkte fra udfasning af kontanter til betaling via ansigtsgenkendelse er et stort skridt for de fleste da man udskifter en fysisk interaktion og følelse af kontrol med penge, til at være en form for ubevidst handling. Ser man på det fra et fem årigt perspektiv er vi gået fra et udgangspunkt med mindre brug af kontanter, til brug af kontaktløse kreditkort, og endt med en mulig implementering af en betalingsmetode der ikke kræver at man har nogle former for fysiske genstande med sig for at betale.

For at give en smagsprøve på hvad vi kan forvente af politiets fremtidige brug af ansigtsgenkendelse vil vi bruge deres tilgang til nr. plade genkendelse. Politiet bruger i dag nr. plade genkendelse til at identificere biler der ikke har forsikring, tidligere spritkørsel, efterlysning osv. Teknologien bliver brugt i politipatruljer og faste installationer langs bestemte strækninger der gemmer alle registrerede nr. plader på en database i 30 dage.(Datatilsynet, 2015) Ved at overføre brugen af dette system til fremtidige brug af ansigtsgenkendelse vil vi i realiteten være masseovervåget i de områder man vælger at bruge ansigtsgenkendelse.

Et sted der allerede gør brug af lignende systemer er Kina, de har over 200 millioner registrerede overvågningskameraer, men har indenfor det seneste år sat bestemte overvågningskameraer op der specifikt er lavet til ansigtsgenkendelse. De registrere alle og belønner og straffer ud fra folks handlinger. Belønningen består af at alle borgere får tildelt en bestemt ”score” som angiver deres status set i regeringens øjne. (Kobie, 2019)

Lovgivning

Hvad er biometrisk data?

Ifølge Europa-Parlamentets og Rådets forordning (persondataforordningen), så er biometriske data *"personoplysninger, der som følge af specifik teknisk behandling vedrørende en fysisk persons fysiske, fysiologiske eller adfærdsmæssige karakteristika muliggør eller bekræfter en entydig identifikation af vedkommende, f.eks. ansigtsbillede eller fingeraftryksoplysninger"* (Europa Parlamentet, 2016).

Persondataforordningen gør det klart i artikel 9, stk. 1, at behandling af særlige kategorier af personoplysninger, herunder tilhøre biometriske data, er forbudt medmindre et af en række forhold gør sig gældende. Der nævnes ti forhold, vi vil kun nævne dem vi mener er mest relevant for ansigtsgenkendelses teknologien.

Første forhold er, *"Den registrerede har givet udtrykkeligt samtykke til behandling af sådanne personoplysninger til et eller flere specifikke formål, medmindre det i EU-retten eller medlemsstaternes nationale ret er fastsat, at det i stk. 1 omhandlede forbud ikke kan hæves ved den registreredes samtykke."* (Europa Parlamentet, 2016). Det vil sige at hvis brugen giver samtykke til en virksomhed som Apple, Samsung eller Google, så har de tilladelse til at behandle borgerens personlige data som fingeraftryk og billeder. Dog kan den enkelte medlemsstat forbyde behandlingen af personoplysninger, selvom borgeren giver samtykke.

Andet forhold er, *"Behandling er nødvendig for at overholde den dataansvarliges eller den registreredes arbejds-, sundheds- og socialretlige forpligtelser og specifikke rettigheder, for så vidt den har hjemmel i EU-retten eller medlemsstaternes nationale ret eller en kollektiv overenskomst i medfør af medlemsstaternes nationale ret, som giver fornødne garantier for den registreredes grundlæggende rettigheder og interesser."* (Europa Parlamentet, 2016).

Tredje forhold er hvis *"Behandling er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser i tilfælde, hvor den registrerede fysisk eller juridisk ikke er i stand til at give samtykke."* (Europa Parlamentet, 2016). Dette kan f.eks. gælde i tilfælde af at politiet

mener at der er behov for at overvåge en person der kan være til fare for sig selv eller andre. Det kan være selvmordstruede personer der er i psykotisk tilstand eller en mulig terrorist. Det vil derudover også være til gavn for politiet at have adgang til en sådan type data, i tilfælde af at en borger forsvinder.

Fjerde forhold er, *"Behandling foretages af en stiftelse, en sammenslutning eller et andet organ, som ikke arbejder med gevinst for øje, og hvis sigte er af politisk, filosofisk, religiøs eller fagforeningsmæssig art, som led i organets legitime aktiviteter og med de fornødne garantier, og på betingelse af at behandlingen alene vedrører organets medlemmer, tidligere medlemmer eller personer, der på grund af organets formål er i regelmæssig kontakt hermed, og at personoplysningerne ikke videregives uden for organet uden den registreredes samtykke."* (Europa Parlamentet, 2016). Dette kan f.eks. være en organisation der har til formål at hjælpe og beskytte hjemløse personer og derfor ønsker at indsamle nyttige informationer om de hjemløse i en database. Den information kunne være brugbar hvis organisationen forsøger at skaffe jobs til de hjemløse.

Femte forhold er, *"Behandling vedrører personoplysninger, som tydeligvis er offentliggjort af den registrerede."* (Europa Parlamentet, 2016) Det vil sige at det er tilladt at bruge f.eks. billeder som bliver offentliggjort på internettet, om det så er via sociale medier, et forum eller blogs. Ud fra beskrivelsen af loven, er det kun et af disse forhold der skal finde sted for at lovliggøre brugen af biometriske data. Det vil altså sige at hvis femte forhold gør sig gældende så er det også virksomheder der arbejder med gevinst for øje, der har lov til at bruge de offentliggjorte data. Et eksempel på en virksomhed som har udnyttet dette er Clearview. Virksomheden har udnyttet lovgivningen i USA, som er nogenlunde det samme som EU når det gælder behandlingen af personoplysninger, og indsamlet alle offentliggjorte billeder og videoer på Facebook, Youtube, Venmo og andre offentlige medier (Hill, 2020).

Det sjette forhold er *"Behandling er nødvendig af hensyn til samfundsinteresser på folkesundhedsområdet, f.eks. beskyttelse mod alvorlige grænseoverskridende sundhedsrisici eller sikring af høje kvalitets- og sikkerhedsstandarder for sundhedspleje og lægemidler eller medicinsk udstyr på grundlag af EU-retten eller medlemsstaternes nationale ret, som fastsætter passende og*

specifikke foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder, navnlig tavshedspligt." (Europa Parlamentet, 2016). I sådan et tilfælde som vi befinder os i nu (2020), hvor en pandemi har ramt hele verden, så kan dette forhold gøre sig gældende. For hvis et af EU-medlemsstaterne laver et udgangsforbud, så kan regeringen bruge overvågningskameraer til at holde styr på hvilke borgere der opholder sig uden for hjemmet og om disse borger har en tilladelse til dette.

Dog er der et yderligere krav til at behandling af særlig kategorier af personoplysninger skal tillades under disse forhold og det er at *"oplysninger behandles af en fagperson, der har tavshedspligt i henhold til EU-retten eller medlemsstaternes nationale ret eller regler, der er fastsat af nationale kompetente organer, eller under en sådan persons ansvar, eller af en anden person, der også har tavshedspligt i henhold til EU-retten eller medlemsstaternes nationale ret eller regler, der er fastsat af nationale kompetente organer."* (Europa Parlamentet, 2016). Dette er med til at sikre borgernes ret til privatliv, ved at deres oplysninger ikke kommer ud i offentligheden. Dette sikkerhedsnet beskytter borgens information om seksualitet, politisk, religiøst og filosofiske holdninger, fagforeningsmæssigt tilhørsforhold og biometrisk data som fingeraftryk. På den anden side så beskytter det ikke borgerens ansigts biometri, da det er noget der altid er blottet for offentligheden. Især hvis der er tale om data der er offentliggjort af borgeren, så som billeder på nettet, hvilket i så fald giver alle der har adgang til internettet adgang til disse billeder. Men det er måske også i orden? For ser man nærmere på det så er ansigtets biometriske data alene uden andet af borgerens data ikke så harmfuldt alligevel. For et billede uden et navn eller en adresse knyttet til det, er i det enkelte tilfælde ikke så brugbart. Desuden ser vi hinandens ansigter i offentligheden hver dag og det har aldrig været farligt for vores privatliv. For det er oplysninger så som politisk, religiøst og filosofiske holdninger der kan være noget der kan bruges imod en. Derfor må lovgivningen have fokus i at beskytte disse særlige oplysninger for at sikre borgeres rettigheder. Dog er det stadigvæk vigtigt at beskytte borgeres billeder da det er kombinationen af særlige oplysninger og ansigts biometrisk data, der kan skabe størst risici overfor borgernes rettigheder.

En af de ting der er vigtig at bide mærke i, er at disse forhold gør sig gældende for en stor del af den danske befolkning. Især forhold fem, da den dækker alle der gør brug af sociale medier.

Hvilket i 2017 var 71% af alle borger mellem 15-89 år (Danmarks Statistik, 2018). Disse borgere har givet samtykke til at deres oplysninger kan bruges af de sociale medier og derudover også af andre virksomheder da alle billeder, videoer og informationer på sociale media betragtes som offentliggjort. Dette giver virksomheder muligheden for at kunne bygge store databaser op med borgeres billeder og videoer fra sociale medier, og bruge det til udvikling af ansigtsgenkendelses teknologier.

Vores felt i et historisk perspektiv

Historisk set har der været interesse i ansigtsgenkendelsesteknologi som forskningsfelt tilbage til 1960'erne. I 1964 forsøgte Bledsoe, Chan og Bisson at programmerer en computer til at genkende ansigter. Deres program bestod i at administratoren skulle lokaliser øre, øjne, mund og næse på et fotografi, og programmet kunne derefter måle afstanden mellem disse referencepunkter, og dermed komme med et bud på hvem der var på billedet. Men på grund af den besværlige fremgangsmåde fik deres forsøg ikke stor opmærksomhed eller anerkendelse(Zhou og Xiao, 2018, s. 6-7).. Peter Hart fra Stanford Research Institute, fandt dog forskningen interessant, og arbejdede videre med deres arbejde. Hart fik bedre resultater da han valgte at benytte sig af billedsæt i stedet for sæt af referencepunkter i ansigtet som Bledsoe, Chan og Bisson havde valgt at bruge. Harts positive resultater var startskuddet til en lang række forskningsprojekter, som alle forsøgte at frembringe den mest optimale metode til ansigtsgenkendelse(Zhou og Xiao, 2018, s. 6-7). I 1970erne var det Goldstein, Harmon, og Lesk som forsøgte sig. De udviklede en metode hvori de identificeret 21 forskellige markøre som var specifikke til for det pågældende ansigt, så som hårfarve og tykkelsen på læberne. Denne metode havde en høj genkendelses nøjagtighed, men grundet den besværlige proces, som indebar manuel måling og placering af de 21 unikke markør, var metoden ikke brugbare til identifikation af større mængder af ansigter(Zhou og Xiao, 2018, s. 6-7). I 1991 foreslog Turk og Pentland at man kunne benytte sig af en metode til ansigtsgenkendelse som var baseret på *principal component analysis* (PCA), som er en proces hvori man konverter datasæt med mange dimensioner til et datasæt med færre dimensioner, hvilket

medfører at de konverterede datasæt bliver mere konsistente og ensartede(Slavkovic & Jevtic, 2012 s. 121). Dette medførte at Turk og Pentland kunne udvikle den såkaldte *Eigenface* algoritme, som sidenhen er blevet betragtet som standarden inden for ansigtsgenkendelse, og en lang række af de algoritmer som efterfølgende er blevet udviklet, baserer sig på de samme grundlæggende ideer som Eigenface algoritmen. I 1997 lykkedes det for Christoph von der Malsburg at udvikle et system som kunne identificer ansigter fra billeder som var uklare, hvilket ikke havde været muligt indtil da. Dette bevirkede at forskningen inden for ansigtsgenkendelse bevægede sig i to retninger, 2d og 3d(Zhou og Xiao, 2018, s. 6-7). De første forsøg på at anvende 3-dimensionale skete allerede i 1980erne, hvor brugen af en krumnings metode gav en 100% genkendelses nøjagtighed på en lille database med 3d billeder. I et studie fra 1996 viste at det var muligt at opnå en højere nøjagtighed, hvis man benyttede sig af billeder af ansigtet fra forskellige vinkler. I takt med at 3d-scannings teknologi er blevet billigere og mere udbredt, er forskningen på området også blevet mere udbredt. I det seneste årti er algoritmerne inden for ansigtsgenkendelse forfinet til at have en succesrate på 99,8% mod 95% i 2010. Forbedringen er sket ved at ændre det dybe komplekse neurale netværk, convolutional neural network (CNN)(Patrick G, Mei N, Kayee H. 2018)

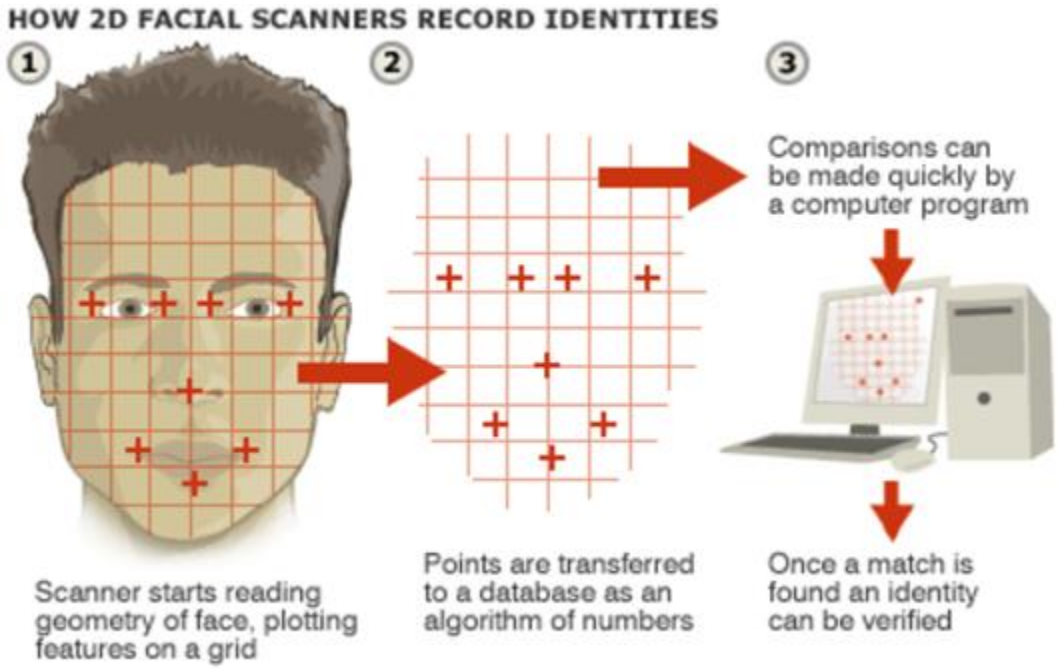
Teknologiens indre mekanismer og processer

2-dimensionel Ansigtsgenkendelse

Vi vil her redegøre for opbygningen af ansigtsgenkendelse som en del af et teknologisk system og hvordan selve processen forløber fra at et ansigt bliver filmet til at det registreres i billedet og identificeres i form af et match i en database.

2 dimensional (2D) og 3 dimensional (3D) ansigtsgenkendelse er to fremgangsmåder til at opnå det samme mål, identifikation af et givent ansigt. Sat op imod andre biometriske identifikationsmetoder (Iris scanning, fingeraftryk, håndflade) er både 2D og 3D

ansigtsgenkendelse den mindst påtrængende fremgangsmåde da udførelsen ikke registreres af mennesker når de bliver udsat for identificering via ansigtsgenkendelse.



Figur 2 -Udtagning af nøglepunkter samt konvertering for at opnå et match og derved identificere fremtrædende på billedet. (BBC News UK)

2D ansigtsgenkendelse fungere ved brug af 2 dimensionelle billeder i modsætning til 3D ansigtsgenkendelse der gør brug af et 3 dimensionalt kort den laver via flere 2D billeder. Ansigtsgenkendelse kan altså via flere 2D billeder skabe et 3D kort over et ansigt, modsat kan man via et 3D billede udtage et 2D billede. Dette er relevant da forskellige programmer gør brug af disse metoder, 3D-2D, 3D-3D, 2D-2D systemer. (Ioannis A, George T. 2017)

Da 2D ansigtsgenkendelse ikke har samme vidtgående datasæt som 3D er det mere udsat ved brug i omgivelser med dårlig belysning eller pga. hår, briller og hovedbeklædning samt poseringen på billedet. For at opnå højeste mulig succesrate kræver det at personen kigger direkte ind i kameraet uden at lave nogle ansigtsudtryk og lysindfaldet skal falde så der ikke optræder skygger i ansigtet. Sidstnævnte minder meget om politiets retningslinjer for billede til pas og kørekort. Fejlraten er højere når man udelukkende bruger 2D ansigtsgenkendelse når man kun har et fotografi at gå ud fra da det er sjældent at et tilfældigt billedet af en person lever op til nævnte kriterier.

I stedet for at søge på øjne enkeltvis har man ud fra eksisterende billeder lavet en skitse for hvilket område øjne vil optræde i et ansigt. Denne metode er påvirket af afstanden mellem kameraet og personen og med formodningen om at øjne vil optræde horisontalt på billedet. I nogle tilfælde vil denne metode opfatte øjenbryn som øjne hvilket tilføjer en ny funktion til at imødegå dette, at der skal være hud synligt i et givent område under de to steder skitsen forventer øjnene er i ansigtet. Metoden vil nu ikke fejlagtigt registrer øjenbryn som øjne, da der ikke kun optræder hud. For at finde det område søges der efter det område med mindste forskel mellem værdier i pixels inden for rammen af skitsen. Når øjne er fundet, vil ansigtsgenkendelse programmet registrere fremtrædning/position af ansigtet i relation til det registrerede ansigt. (Thomas D. H. 2005 kap. 4.1).

Som nævnt skal ansigtsgenkendelse lokalisere bestemte kendetegn i ansigtet og derefter bliver de tildelt bestemte punkter som giver os en værdi. Kendetegn i ansigtet er følgende 20 punkter;
højre øjenbryn inderste kant=1, yderste kant=2,
venstre øjenbryn inderste kant=3, yderste kant=4
højre øje øverste kant=5, nederste kant=6, inderste kant=7, yderste kant=8
venstre øje øverste kant=9, nederste kant=10, yders kant=11, indereste kant=12
Tippen af næsen=13, højre hjørne næsen=14, venstre hjørne næsen=15, øverste kant af overlæben=16, nederste kant af underlæben=17, højre mundvige=18, venstre mundvige=19 nederste kant af hagen=20.

Euklids afstande

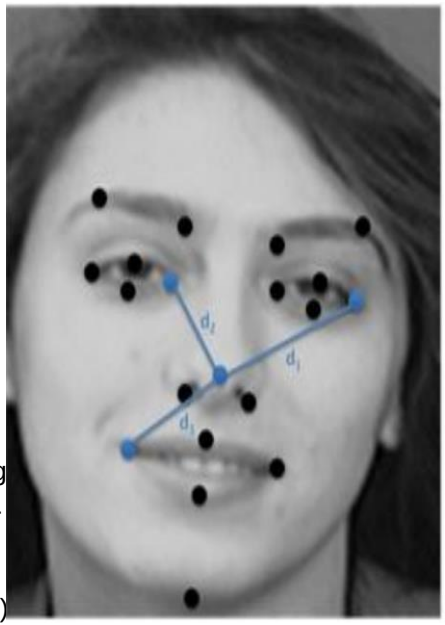
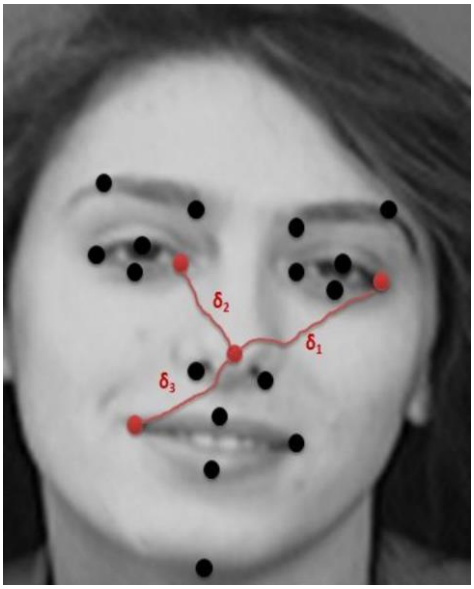


Fig ɔrer for e(pkt. 8), t. 12)

(Rachid Ahdid Et al. 2016)

Geodesic afstand



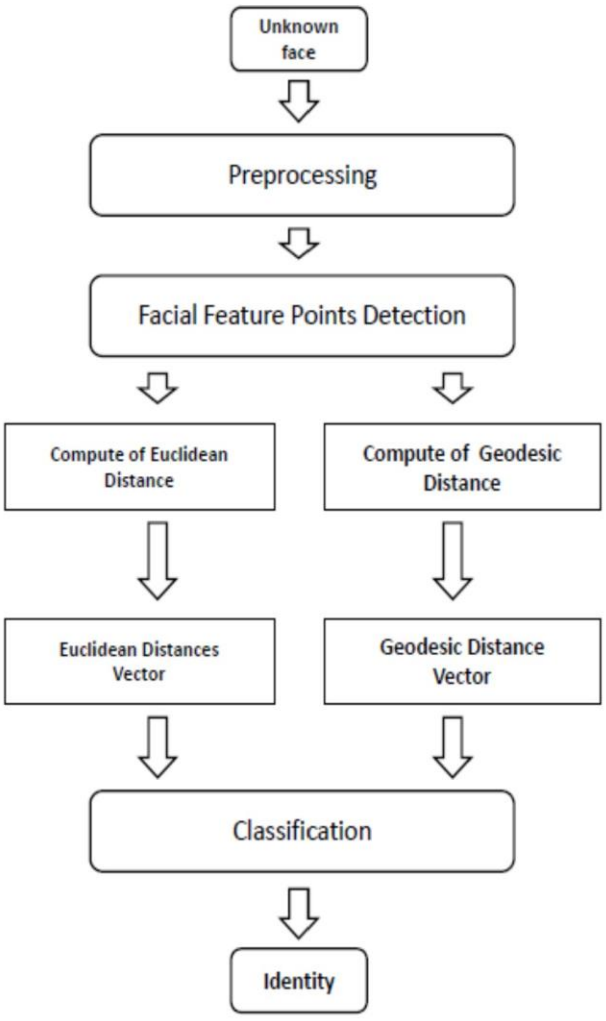
Figur 4 – her vises samme vektorer men hvor de følger ansigtets kurver. (Rachid Ahdid Et al. 2016)

De 20 punkter kan forbindes med 190 kombinationer og på den måde give 190 afstande der giver unikke kendetegn i form af numeriske værdier der kan identificere ud fra et billede.

Ovennævnte afstande bliver målt som den Euklidske afstand og geodesic´s afstand, forskellen på disse to er at euklids afstand bliver målt som den korteste vej mellem to punkter i ansigtet og geodesic´s afstand bliver målt som den korteste afstand mellem to punkter uden at slippe overfladen af ansigtet. Udregning af Euklids afstand udføres ved at tage de to punkter fra vektorens start og slut og trække fra hinanden

Vektor mellem to punkter

Ser man på figur 3 er der tre forskellige vektorer imellem tre kendetegn, de bliver udregnet ud fra euklids afstand for bagefter at blive udregnet ud fra geodesics afstand. De værdier er regnet frem til efter to gange 190 vektorer i euklids og geodesic´s afstand er selve værdien et ansigt bliver identificeret ud fra.(ACIT, 2016)



Figur 5(Rachid Ahdid Et al. 2016)

De pixels der udgøre et billede har en bestemt sat værdi der er givet ud fra en sensor der måler afstanden. De fleste smartphones har i dag funktionen HDR i kameraet, HDR er forkortelse for

High Dynamic Range imaging, bliver også omtalt som HDRI. Dynamic Range, er afstanden mellem den rene sorte- og hvide farve i et billede, afstanden bliver omtalt i ”stops”. For ansigtsgenkendelse er det bedre med flere stops, da de gengiver langt flere detaljer i skyggeområder på billeder. Videoovervågning filmer ikke i HDR.

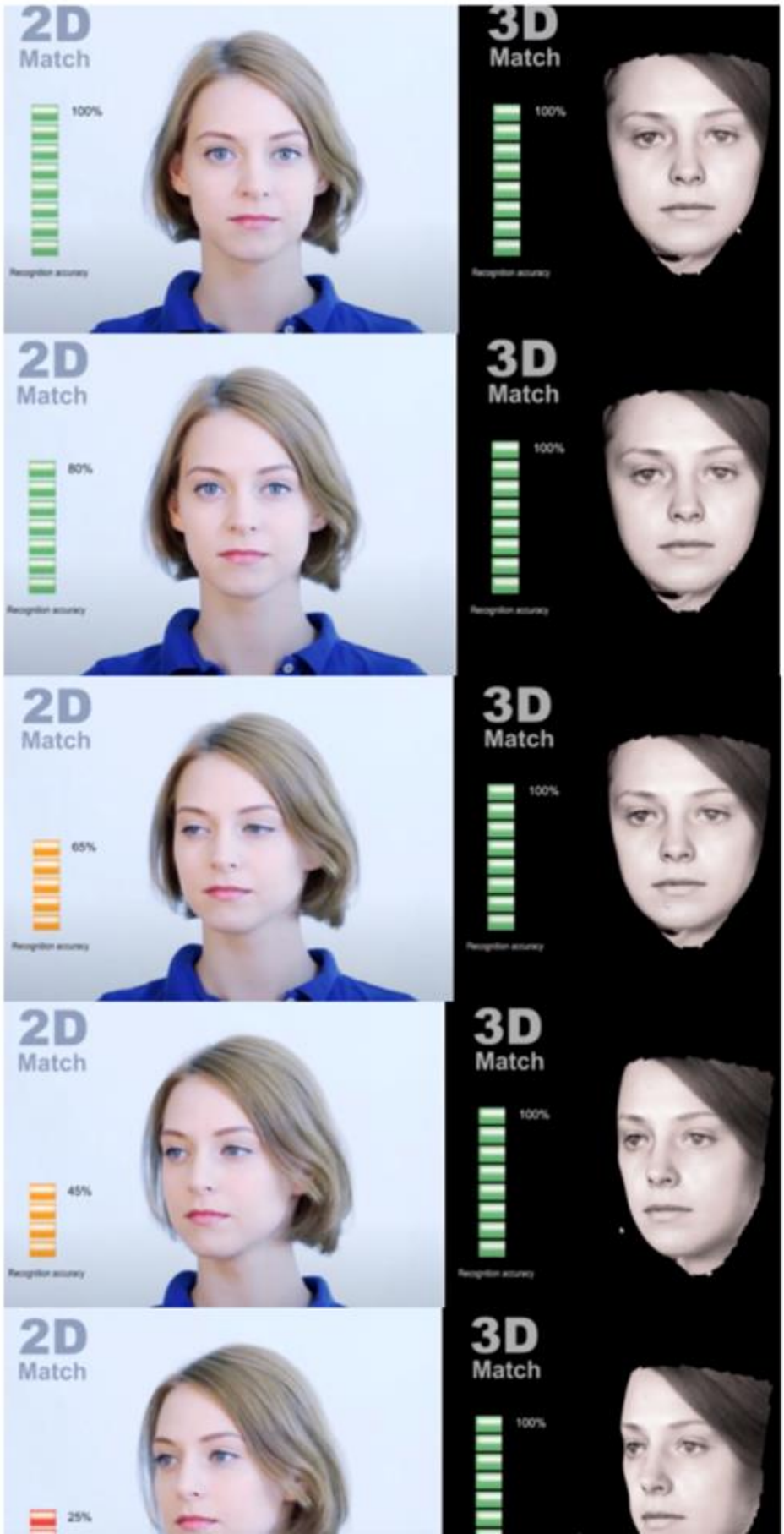
Ved brug af 2D ansigtsgenkendelse via et overvågningskamera vil kameraet først registrere om der optræder ansigter og derefter udtage flere 2D billeder for hvert ansigt og udregne forskellige værdier ud fra afstanden mellem øjne, næse, mund, øjenbryn og øre. De værdier (matematiske) den kommer frem til, uploades til en database hvorpå den søger et match som vil give den endelige identifikation.

Brug af 2D ansigtsgenkendelse

Som beskrevet med krav til pasfoto er det en del af de nye biometriske pas der bliver lavet i Europa for at øge sikkerheden. I dagligdagen bruges det til at låse smartphone op og digitale kameraer bliver solgt med funktionen så den automatisk genkender personer og tagger dem i ens fotoalbum. Sociale platforme som Facebook bruger det også til at identificere dets brugere i videoer og billeder uploadet til platformen. Tivoli i København ansøgte om at anvende et system der gjorde brug af 2D ansigtsgenkendelse, det skule bruge som adgangssystem til gæsterne når de gik ind i forretninger der også havde adgang fra gaden. Systemet skulle hjælpe med at adskille betalende kunder fra tivoli og folk der kom fra gaden uden retmæssig adgang. (Adgangskontrol ved brug af ansigtsgenkendelse, 2009)

2D ansigstgenkendelse

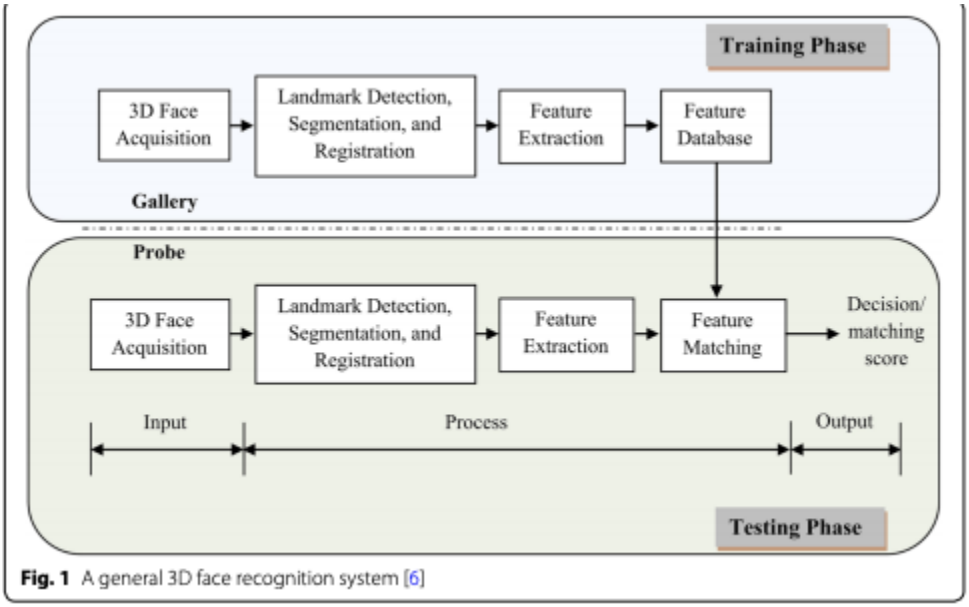
Vi vil her redegøre for opbygningen af ansigtsgenkendelse som en del af et teknologisk system og hvordan selve processen forløber fra at et ansigt bliver filmet til at det registreres i billedet og identificeres i form af et match i en database.


2D
Match
100%
Recognition accuracy
3D
Match
100%
Recognition accuracy
2D
Match
80%
Recognition accuracy
3D
Match
100%
Recognition accuracy
2D
Match
65%
Recognition accuracy
3D
Match
100%
Recognition accuracy
2D
Match
45%
Recognition accuracy
3D
Match
100%
Recognition accuracy
2D
Match
25%
3D
Match
100%

Figur 6– Viser hvor stor påvirkning poseringen har på et 2D billede i forhold til 3D, (3D facial recognition system VOCORD FaceControl 3D, 2016)

3-dimensionel ansigtsgenkendelse

I Dette afsnit vil vi beskrive hvordan et generalt 3D ansigtsgenkendelsessystem virker.
Den generelle proces der muliggør ansigtsgenkendelse ved brug af 3D-billeder kan overordnet inddeles i 2 faser, som hver især består af 4 trin (Zhou og Xiao, 2018, s.1).



Figur 7 - de 2 faser bestående af 4 trin (Zhou og Xiao, 2018, s.1)

Den første fase er træningsfasen, som består det 1. trin *3D face Acquisition,* hvor billeder bliver genereret ved hjælp af en særlig scanningsteknologi som gør det muligt at modeller ansigtet i 3D. Der findes overordnet 2 forskellige metoder til at frembringe 3D billeder.
Den aktive acquisition fungerer ved brug af et system der udsender infrarøde stråler som oplyser ansigtet, og derefter måler det reflekteret lys som bliver sendt tilbage fra ansigtet, hvilket gør det muligt at genererer ansigtets form i 3D(Zhou og Xiao, 2018, s. 2-3). Inden For aktiv acquisition

findes der to forskellige metoder til at forme 3D modeller. Der findes den triangulære baseret metode, som fungerer ved at scanningsteknologien måler de eksakte vinkler fra hvor de infrarøde lysstråler er når de bliver sendt fra scanneren og lysets vinkel når det bliver reflekteret tilbage til scanneren. Man kan derfor trianguler refleksionspunktet, og ved at grupperer disse refleksionspunkterne i takt med at scanneren bevæger sig ned langs ansigtet, bliver der skabt et 3D billede. Den triangulations baserede metode skaber nogle meget præcise billeder, men er meget tidskrævende, hvilket begrænser anvendeligheden i visse scenarier(Zhou og Xiao, 2018, s. 2-3).

Det andet aktive acquisition system der findes, kaldes for *structured light based*, og er systemer som findes i en række underholdnings systemer, såsom Microsofts Kinect(Zhou og Xiao, 2018, s. 2-3). Kinect virker ved at systemet udsender lys fra en infrarød projekter ud i lokalet, herefter måler en chip hvor langt lyset har rejst på hver pixel, og dette gør det muligt at få et 3D billede af de objekter eller personer der er i lokalet("How It Works: Xbox Kinect", 2020). *Structured light based* systemer er langt hurtigere til at skabe 3D billeder end systemer der anvender den triangulære metode, men til gengæld er de også mere upræcise.

De *passive acquisition* systemer er en betegnelse for de systemer som ikke aktivt interagerer med objektet der skal 3D modellers. I sted opfanger de passive systemer det lys der naturligt udstråler fra objektet. Dette gøres oftest ved at anvende et eller flere lysfølsomme kamera som tager billeder af det samme objekt fra forskellige vinkler og finder fælles referencepunkter som kan bruges til at skabe et 3D billede af objektet (WEINMANN, 2018 s. 21-22).

Efter man har indsamlet 3D ansigts data i det for første trin bliver man nødt til at rydde op i den, for at fjerne forstyrrende elementer.
Det trin i figur 7 kaldes *Preprocessing* og er nødvendigt da der er en række elementer computeren ikke kan bruge til at adskille en person fra en anden. Hår, øre, hals, smykker og briller er alle elementer der skal fjernes fra data, for at kunne lave en nøjagtig identifikation. Dette skyldes at artefakter såsom smykker og briller kan fjernes eller udskiftes, og kan derfor ikke bruges til at identificerer en person set ud fra en computers perspektiv. Det samme gælder halsen og ørene,

som heller ikke er pålidelige identifikationspunkter, da de skifter karakter afhængige af hvordan hovedet vender (Zhou og Xiao, 2018 s.3-4).

Efter denne proces står man tilbage med ”rene” 3D ansigtsmodeller, som kan blive brugt som input i en *feature extraction* algoritme, som er det trejde trin i fugur x, som kan identificer unikke ansigtstræk som gør en nøjagtig identifikation mulig. Der findes grundlæggende to møder at udfører feature extraction på. Den globale tilgang er den meste ligefremme og går ud på at man bruger hele ansigtet som en samlet vektor til at få et korrekt match. Alternativt kan man benytte sig af den lokale tilgang, hvor man bryder ansigtet op i dele, såsom næsen eller munden, og sammenligner dem med eksisterende billeder i databasen(Zhou og Xiao, 2018 s.3-4). Det er den samme proces som sker i test fasen, dog med den forskel at outputtet er en nøjagtighed score der beskriver sandsynligheden for at der er et match på de eksisterende billeder i databasen.

Teknologiske systemer

Ansigtsgenkendelse er en teknologi som er gjort op af et stort teknologisk system. For at udvikle et brugbare ansigtsgenkendelses program kræver det en række teknologiske subsystemer til at træne programmet. Der indgår en stor mængde hardware i systemet, såsom kameraer og scannere der bruges til at indsamle den nødvendige mængde billeddata til at træne programmet. Derudover er det vigtigt at systemet har den nødvendige computerkraft til at behandle de massive datamængder der skal analyseres. Det er vigtigt at adgang til databaser med tilstrækkelig mængde billeder når programmets algoritme skal trænes, hvis det skal være muligt at opnå en høj genkendelses rate. Det samlede teknologiske system er komplekst og er udgjort af række subsystemer, som alle kunne være interessante at beskrive i dybden. I denne opgave har vi dog valgt at fokuserer på at beskrive sammenhængen mellem to af de centrale elementer i systemet. Vi vil derfor en følgende afsnit beskrive hvordan databaser og algoritmer er essentielle for hvordan ansigtsgenkendelses programmet udvikles.

Databaser

I dette afsnit af projektet, vil vi komme ind på forskellige typer af databaser. Herefter vil vi uddybe databasernes brug, og forklare relevansen af dem i den samlede ansigtsgenkendelsesteknologi.

FERET-databasen

FERET-databasen er en database, der blev udviklet på baggrund af en algoritme, og ikke den anden vej rundt. Den blev udviklet med FERET-algoritmen for øje, og var essentiel for at algoritmen kunne fungere. Både databasen og algoritmen blev udviklet i samarbejde med Defence Advancement Research Technology og National Institute of Standard Technology (Shafin et al., 2019). Databasen består af 14126 billeder af mennesker, hvoraf billederne er taget af 1199 forskellige mennesker. Billederne blev taget over 2 år, og for nogle af individerne kunne der gå op imod 2 år mellem det første billede blev taget til det sidste blev taget. Dette var enormt interessant, da man tidligere ikke havde testet ældelses effekten i den grad, da det kom til ansigtsgenkendelse. Dermed kunne man bedre få et billede af de indre udfordringer når det kom til forstyrrelser i billedet (Face Recognition Technology (FERET), 2017). Billederne blev taget under semi-kontrolleret forhold, hvilket betyder at billederne blev taget i det samme sæt omgivelser. Dette resulterede i at billederne en form for "rød tråd". Det samme kamerasæt blev brugt til alle billederne, for at beholde en form for konsekvent kvalitet. Dog betød det også at kameraet, da det skulle sættes op manuelt, tog billeder med små forskelle (Face Recognition Technology (FERET), 2017).

Yale Face Database

Der findes Yale Face Database A og Yale Face Database B. I dette afsnit vil vi fokusere på Yale Face Database B, da det er den mest anvendte (Shafin et al., 2019). Databasen består af 5850 billeder, udelukkende i gråtone. Billederne er blevet taget af 10 individer, som hver især har stået i 9 forskellige stillinger. For hver stilling har man derefter taget 64 billeder, med hver sin

lydindstilling. Derudover har hvert individ også fået taget et ekstra "kontrol" foto, hvilket dermed giver et totalt antal fotos på 5850 (Yale Face Database, 2001). De 9 forskellige stillinger

billederne er taget i er 1 billede taget direkte på fronten af individet. De næste 5 blev taget lidt længere væk, med 12 graders forskel fra kameraets optiske akse. De sidste 3 blev taget endnu længere tilbage med ca. 24 grader mellem positionerne. Til hvert billede blev der brugt en blitz med de 64 forskellige lysindstillinger. Blitzene blev styret af en computer, koblet til et kamera med en framerate på 30 frames/second. Det tog dem dermed omkring 2 sekunder at tage alle billederne af individerne. Dermed opnåede man minimale ændringer hos individet, mellem de forskellige billeder. Det sidste kontrolfoto blev taget lige for uden nogen blitz (Yale Face Database, 2001).

Disse databaser er vigtige for de forskellige algoritmer der bliver anvendt til ansigtsgenkendelsesteknologi, da de er med til at træne programmet. Dette fænomen kaldes også maskinlæring. Gennem maskinlæring kan programmet opstille beslutnings træer, og alt efter hvilken algoritme der kører træffer den beslutningerne ud fra forskellige ting. Det kan være til som farve, form på øjne, mund eller næse, kendetegn i ansigtet, eller måske en helt fjerde. Et program opstiller ikke blot 1 beslutningstræ, men enormt mange, for at give et så præcist svar som muligt (Russell and Norvig, 2010). Her vil flertallet af beslutningstræer som regel bestemme udfaldet, også kaldet ensemble-klassifikation (Christiansen, n.d.).

Algoritmer

Dette afsnit vil grundlæggende beskrive hvad en algoritme er, og hvordan de fungerer. Vi vil herefter komme med et eksempel på en af de mest anvendte typer at algoritme når man arbejder med ansigtsgenkendelse. En algoritme er løsningen på et problem/opgave ud fra eksisterende erfaring i håndteringen af problem/opgave. Ligesom en samlemanual til en Ikea reol giver simple instruktioner der skal følges trin for trin for at løse problemet med at samle det.

En algoritme er utvetydig, så der vil altid danne sig et valg ud fra de foruddefinerede handlemuligheder. En opskrift er således en algoritme, trin for trin guider den brugeren til at få et resultat ud fra den givne algoritme (opskrift). Denne opskrift giver måske forskellige handlingsmuligheder der gør, øger succesraten for at få løst eventuelle problemer der opstår hvis

man for eksempel ikke har en ingrediens der er krævet. I det tilfælde kan opskriften give alternative valgmuligheder ligesom der både guides i hvordan kødet kan steges på grillen og indenfor på en stegepande når man køber sparreribs.

Algoritmer programmeret til computere er svært at læse for mennesker derfor kan samme algoritme brugt af computeren vises simplificeret af et rutediagram/flowchart. Det er sådan de udvikles. Fra at man får en ide om løsningen på et problem viser man det via en tegnet rute i et diagram for at visualisere løsningen, herefter programmere man algoritmen. Noget som går igen i algoritmer er løkker, en løkke er gentagelsen af en beregning sådan en udførelse kaldes en iteration hvilket betyder det samme som gentagelse Fejl i algoritmer vil give et forkert resultat eller blive ved i uendelighed med at beregne ud fra de definerede løkker. Jo større en datamængde en algoritme skal arbejde med jo længere tid tager det, men jo stærkere hardware komponenter i den brugte computer jo hurtigere finder algoritmen resultatet (Clausen, 2012). Det er altså selve styrken i computeren der kan være afgørende for løsning af komplekse algoritmer. Dette er relativt da udviklingen af teknologi gør det muligt for størstedelen af befolkningen at lære og løse dagligdags algoritmer. For at sætte det i perspektiv kan en smartphone i dag det samme og endda mere end computeren der stod for den første månelanding i 1969 (Eskildsen & Sonne, 2019). Indenfor ansigtsgenkendelsesteknologi er algoritmer uundværlige. Det er algoritmer der gør det muligt at omdanne billeder til data som er anvendeligt når man skal prøve at identificer et ansigt. Alt afhængigt af hvilken algoritmer man vælger at benytte sig af, kan man udvinde forskellige datapunkter fra et billede og forskellige algoritmer har hver deres fordele og ulemper. Der findes en stor mængde algoritmer indenfor ansigtsgenkendelsesteknologi, men der findes nogle algoritmer som ligger til grund for størstedelen af dem der er mest udbredt.

Eigenfaces er måske den mest anvendte algoritme når det komme til ansigtsgenkendelse. Det er en algoritme som bliver anvendt i vidt udstræk på grunden af dens simplicitet. Eigenfaces store styrke er at den kan gøre komplekse data med mange dimensioner simpel med at identificerer nogle essentielle træk i ansigtet. Ansigtet har mange forstyrrende elementer som gør det svære for en computer at komme med et korrekt match, men ved at reducer antallet af dimensioner og fjerne de elementer som ikke kan anvendes, kan man gøre identifikationen hurtigere og reducerer den

mængde computerkraft der skal anvendes. Ulempen ved Eigenfaces er at den virker bedst på billeder der er taget lige på (Slavkovic & Jevtic, 2012 s. 121-124).

HIC-eksperiment

I denne del af rapporten ønsker vi at udføre et eksperiment for at skabe en visuel repræsentation af ansigtsgenkendelsesteknologi. Til dette benytter vi os af HIC-programmet. Nedenfor ses en redegørelse for programmet og dens metodebrug, som det bruger til at genkende billeder, efterfulgt af eksperimentet, og dertilhørende overvejelser og analyse.

HIC-program

HIC-programmet er et program udviklet af Henning Christiansen. Henning er knyttet til Roskilde Universitet, og er professor på Institut for Mennesker og Teknologi (IMT). HIC står for Henning's Image Classifier, og er udviklet som et billedegenkendelsesprogram til Processing. Vi har haft Henning som underviser i vores TSA II-kursus, hvor der var fokus på kunstig intelligens. Vi har derfor allerede arbejdet med HIC-programmet, og ved at vi vil kunne foretage nogle interessante forsøg med det, til vores projekt. Vi ønsker derfor at udføre et eksperiment med HIC-programmet. Eksperimentet vil demonstrere en teknisk forståelse for- og en visualisering af hvordan 2D ansigtsgenkendelsesteknologi fungerer. Dette vil også give os muligheden for at få et datasæt som vi ville kunne analysere på. Dette vil være med til at demonstrere nogle potentielle fordele og/eller ulemper ved 2D ansigtsgenkendelsesteknologi. Vi anerkender dog at programmet er udviklet som ren billedgenkendelse, og ikke specifikt designet til ansigtsgenkendelse, men kører efter de samme principper som 2D ansigtsgenkendelsesteknologi kører efter.
Programmet har 2 "hovedkomponenter", som man som bruger selv medbringer til programmet; en database og testbilleder. Programmet fungerer sådan, at man loader en række billeder fordelt i forskellige klasser af mapper, som er navngivet efter hvilken kategori billeder der ligger i dem. Dette navn husker programmet som en klasse (Christiansen, 2016). Her udvælger programmet en række små kvadrater, også kaldet subwindows, på hvert billede, som den husker. Som standard er

programmet indstillet til at tage 100 subwindows, af 16x16 pixels hver (Christiansen, 2016). Her træner programmet så en række beslutningstræer til at genkende disse pixels. Når programmet så kører, og man vælger at man skal teste sine testbilleder, tages en række subwindows af det testbillede man kører igennem. Her beslutter hvert beslutningstræ, hver især, hvilken af klasserne af databasebilleder, det nye testbillede falder inden for (Geurts, Ernst & Wehenkel, 2006). Da alle beslutningstræerne har afgivet deres valg, er det flertallet blandt beslutningstræerne, som afgør hvilken klasse billedet hører inden under. Denne type af beslutningstræer og billedgenkendelse teknik, kaldes *Extremely Randomized Trees*, eller kan forkortes til *Extra Trees* (Christiansen, 2016).

Eksperimentet

Eksperimentet vil blive sat op omkring at danne en database af 3 af vores gruppemedlemmer. Der vil blive taget 9 billeder af hver person, som vil kunne bruges til at træne programmet. Altså oprette en database som programmet kan anvende (bilag 1). Vi vil herefter udtage 1 test person, hvor vi tager billeder af personen, i forskellige belysninger, tøj farver, osv. for at illustrere hvilke parametre, der udfordrer HIC programmet, og dens metode, hvorpå den genkender billeder. Forsøget starter med at vi har en subwindow størrelse på 16x16px og 100 subwindows pr. billede. Der tages derudover også 100 subwindows af billederne der testes. Vi kører her også med 100 beslutningstræer. Vi nedskalerer også billederne til 500x500px, grundet udfordringer omkring at tage billederne, som vil blive forklaret som det næste.

Udfordringer i udførelsen af eksperimentet

Grundet den, nu heldigvis aftagende, pandemi, har vi haft svært ved at mødes, hvilket også har resulteret i at vi har stået overfor nogle udfordringer i udførelsen af eksperimentet. Da vi har taget billederne hver for sig, har vi anvendt 3 forskellige kameraer. Dog tager alle vores kameraer udmærket billeder, og vi kan langt hen ad vejen komme uden om dette problem, ved at skalere billederne ned til et lavere antal pixels. En anden udfordring vi har stået over for, er at vores database billeder, ikke kommer til at kunne være 100% identiske i omgivelserne. Vi har forsøgt at

tage billederne i så neutrale omgivelser som overhovedet muligt. Vores store problem er bare at det kan være de helt små ting som kan ændre vores resultat. Noget så simpelt som lysindfald, skygger og nuancen af den hvide væg vi hver især står op af. Vi har forsøgt at komme rundt om dette problem ved at vi har aftalt et tidsrum på dagen hvor vi alle skulle tage de 9 billeder, i et lyst og sydvendt rum. Dernæst har vi aftalt at vi så vidt muligt undgår nogen form for skygger på de 9 billeder. På denne måde kan vi komme udfordringerne om lysindfald og skygger til livs, på bedste vis.

Justering og test

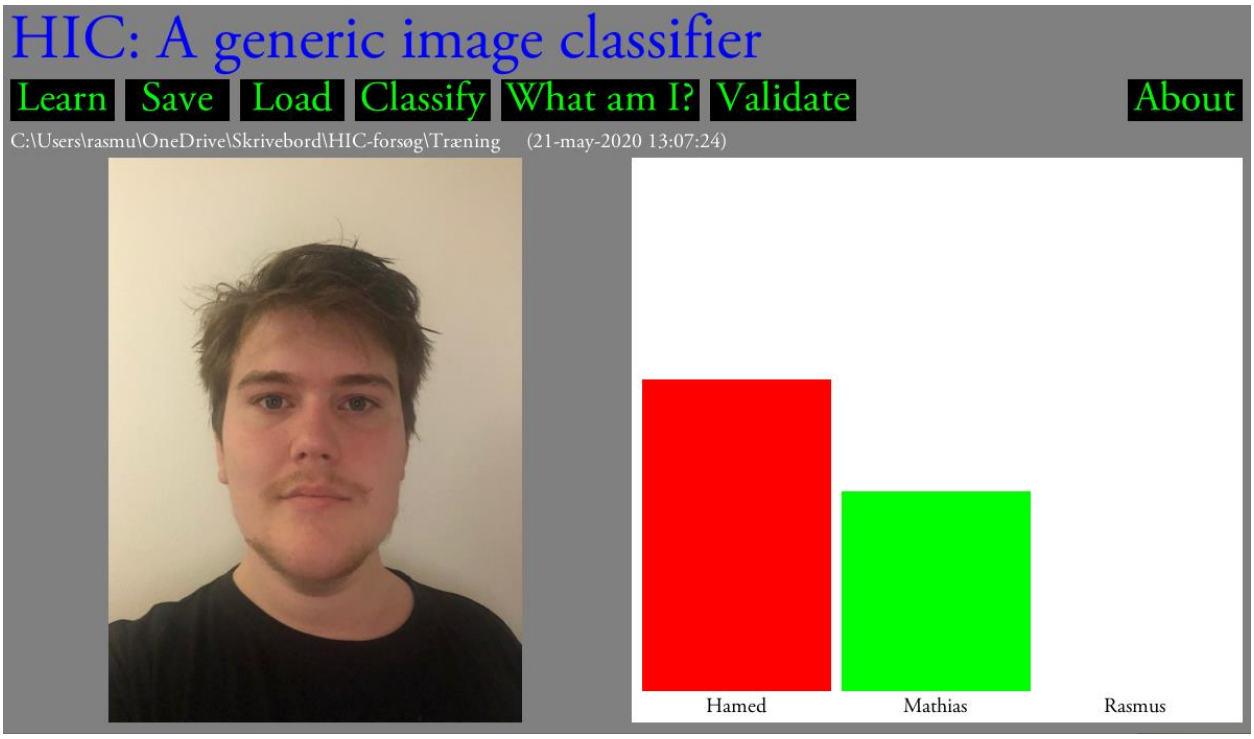
Billederne til at teste med, blev taget af gruppemedlemmet Rasmus. Det første billede vi brugte, var en test for at se om programmet kunne benytte sig af databasen. Allerede her kunne vi se at vi stødte ind i problemer i det vores telefoner tog billeder i forskellige formater. Efter en hurtig rettelse kørte alle vores billeder nu i JPG format. Resultatet er som følger:

Test 1:

Test 2:

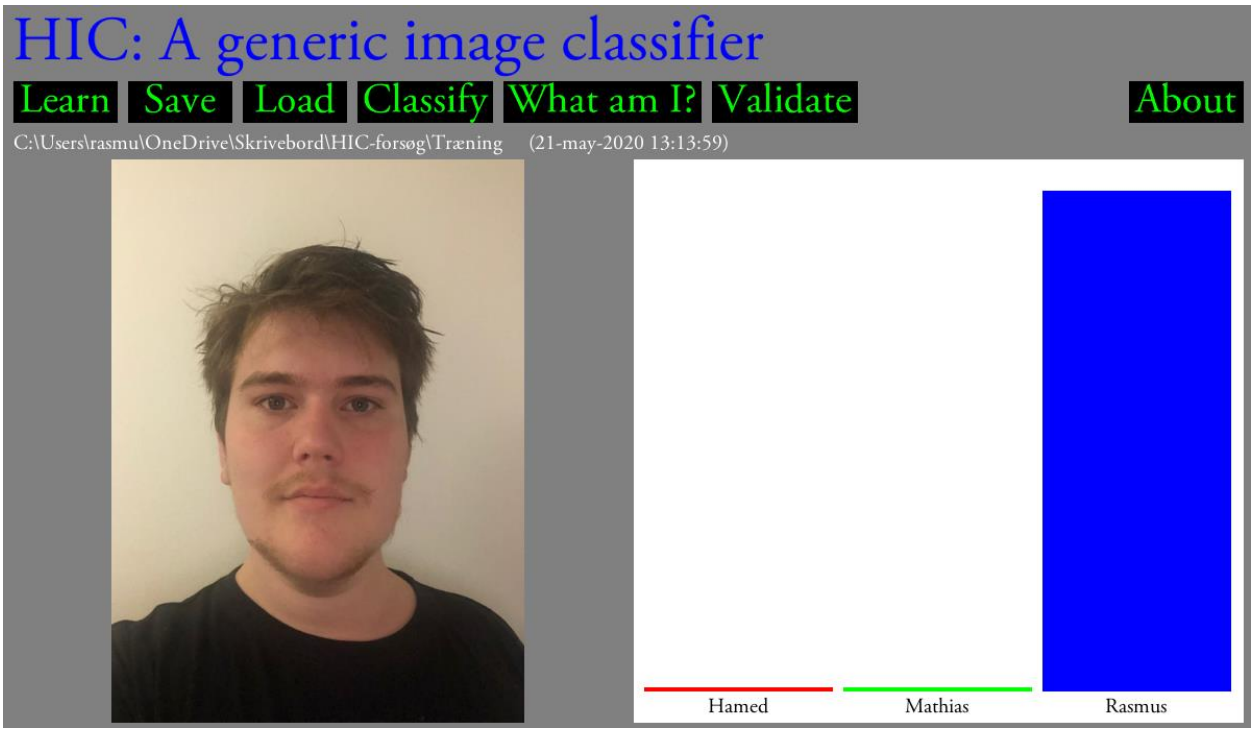

HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\rasmu\OneDrive\Skrivebord\HIC-forsøg\Træning (21-may-2020 13:07:24)
Hamed
Mathias
Rasmus

Test 3:



Eftersom dette ikke gav nogen mening, valgte vi derfor at prøve at fjerne nedskaleringen, for at se om det havde en effekt.

Test 4:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\rasmu\OneDrive\Skrivebord\HIC-forsøg\Træning
(21-may-2020 13:13:59)
Hamed
Mathias
Rasmus

Test 5:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\rasmu\OneDrive\Skrivebord\HIC-forsøg\Træning
(21-may-2020 13:13:59)
Hamed
Mathias
Rasmus

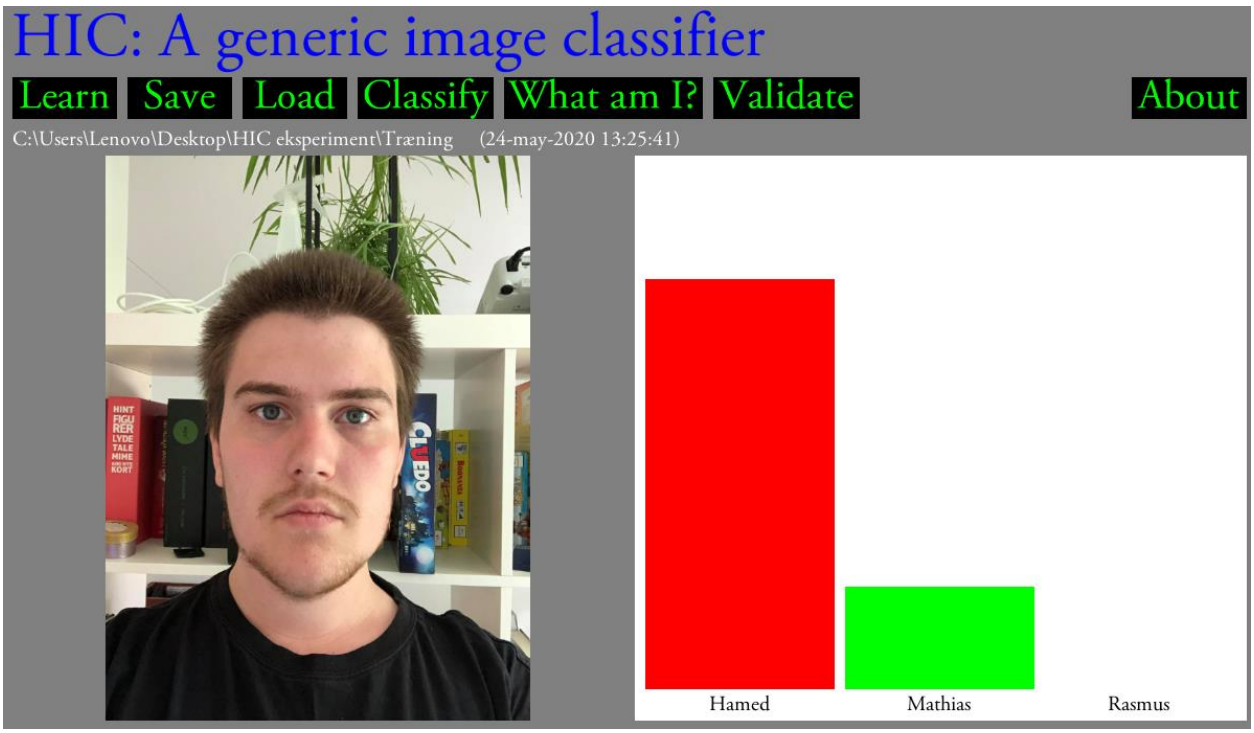
Test 6:

Straks kan vi se at præcisionen er langt højere end den var før. Vi får stadigvæk en smule miksede resultater, men programmet er overvejende enig med, at det er et billede af Rasmus. Så her besluttede vi os for, at vi ville udføre resten af eksperimentet uden nedskalering, da det viser sig, at give mere præcise resultater. Det kan formentlig skyldes den hvide baggrund, der er på alle billederne i databasen. Så når vi nedskalerer billernem, risikerer vi at der i virkeligheden kommer en del hvidt med blandt de pixels, som bliver brugt.

Baggrund

Nu hvor vi vidste at programmet fungerede som vi gerne ville have det til, med det første test billede, besluttede vi os for at udfordre programmet lidt. Vi valgte derfor at tage et billede med en forstyrrende baggrund, for at se om det havde en påvirkning på beslutningen. Billedet og dataen ses nedenfor.

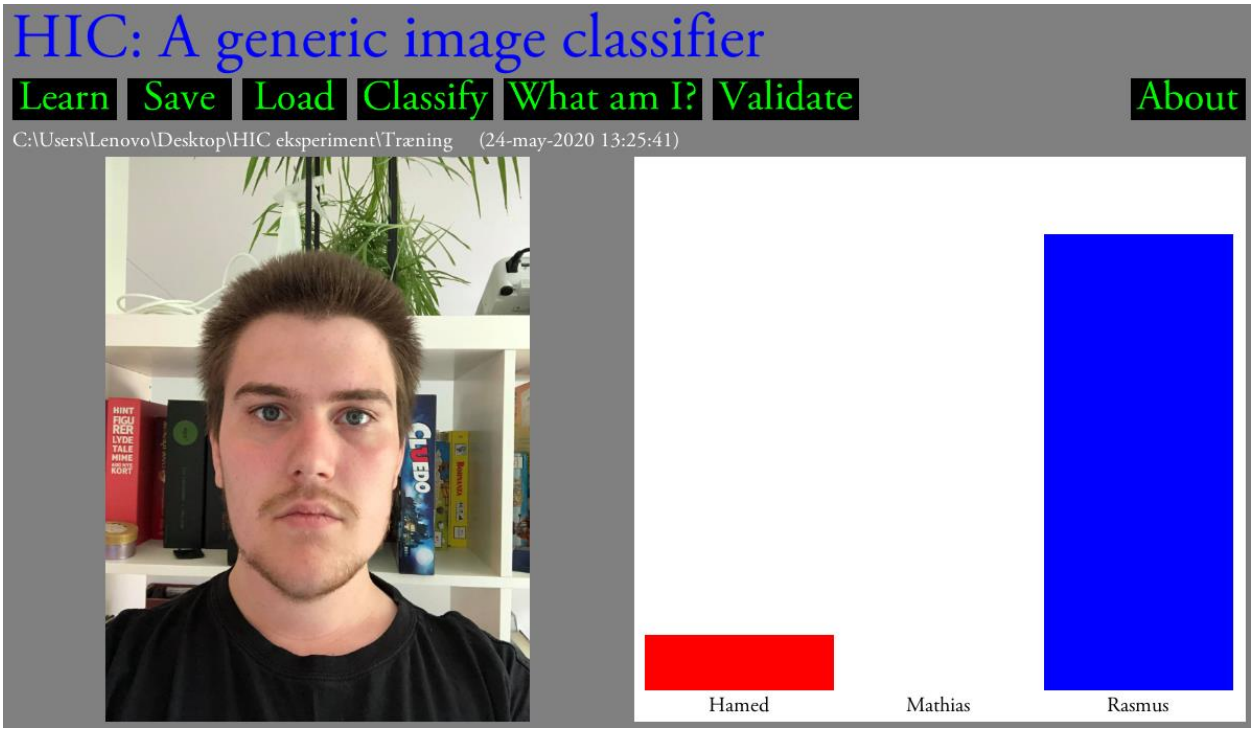
Test 1:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\Lenovo\Desktop\HIC eksperiment\Træning (24-may-2020 13:25:41)
Hamed
Mathias
Rasmus

Test 2:

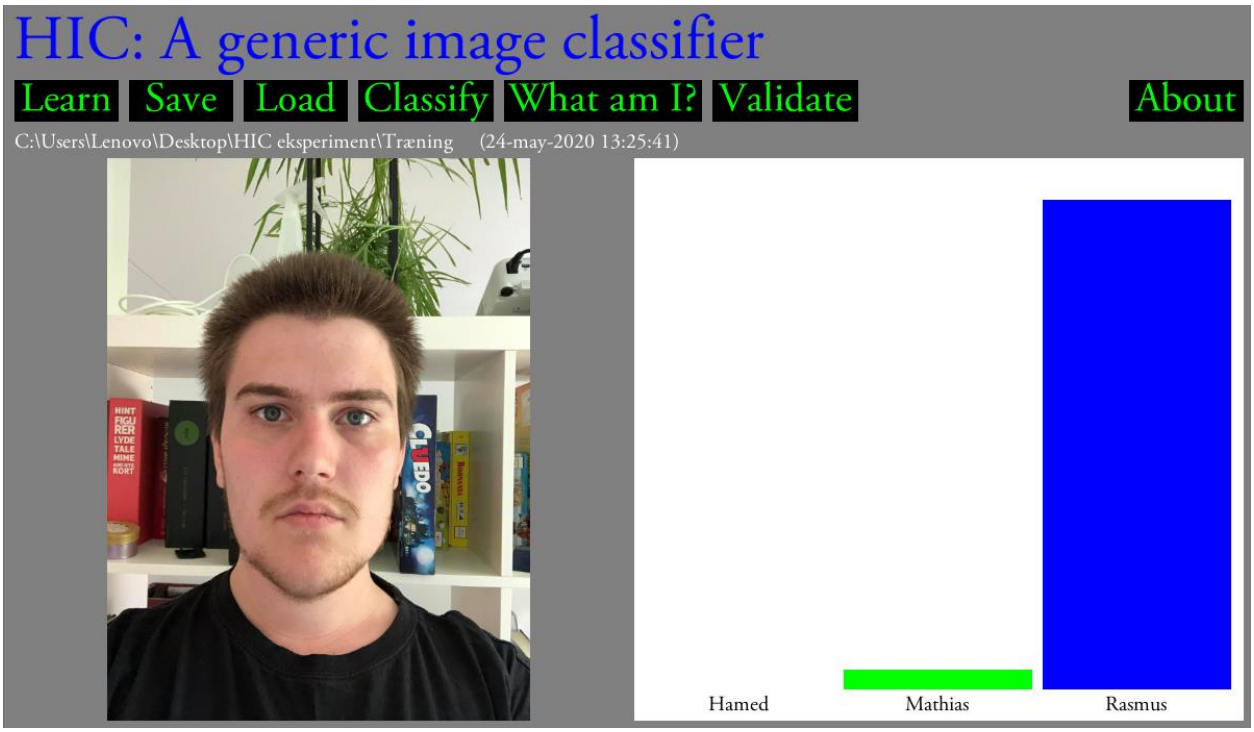

HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\Lenovo\Desktop\HIC eksperiment\Træning (24-may-2020 13:25:41)
Hamed
Mathias
Rasmus

Test 3:

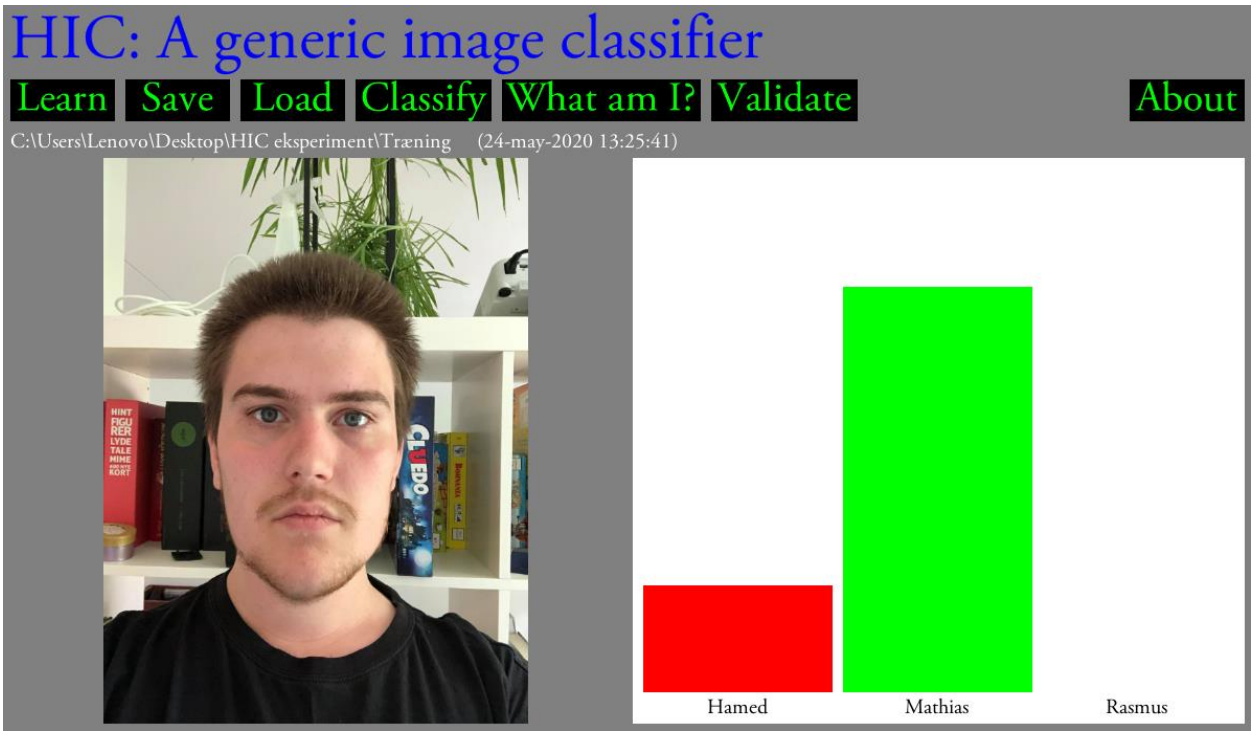


Det ses tydeligt på det første af de 3 test vi kørte, at der var en forskel i hvad programmet mente. Dog er det ikke entydigt med kun 3 test, så vi besluttede os for at køre 6 mere igennem. Resultatet ses nedenfor.

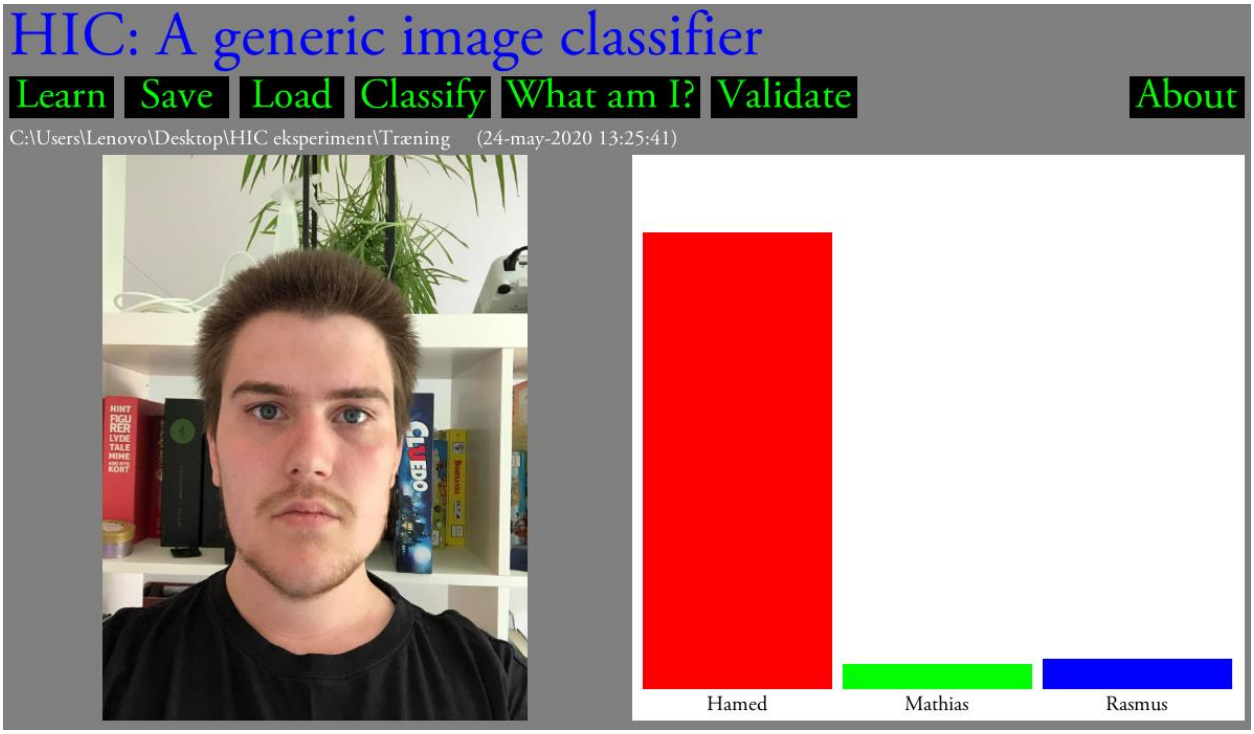
Test 4:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\Lenovo\Desktop\HIC eksperiment\Træning (24-may-2020 13:25:41)
Hamed
Mathias
Rasmus

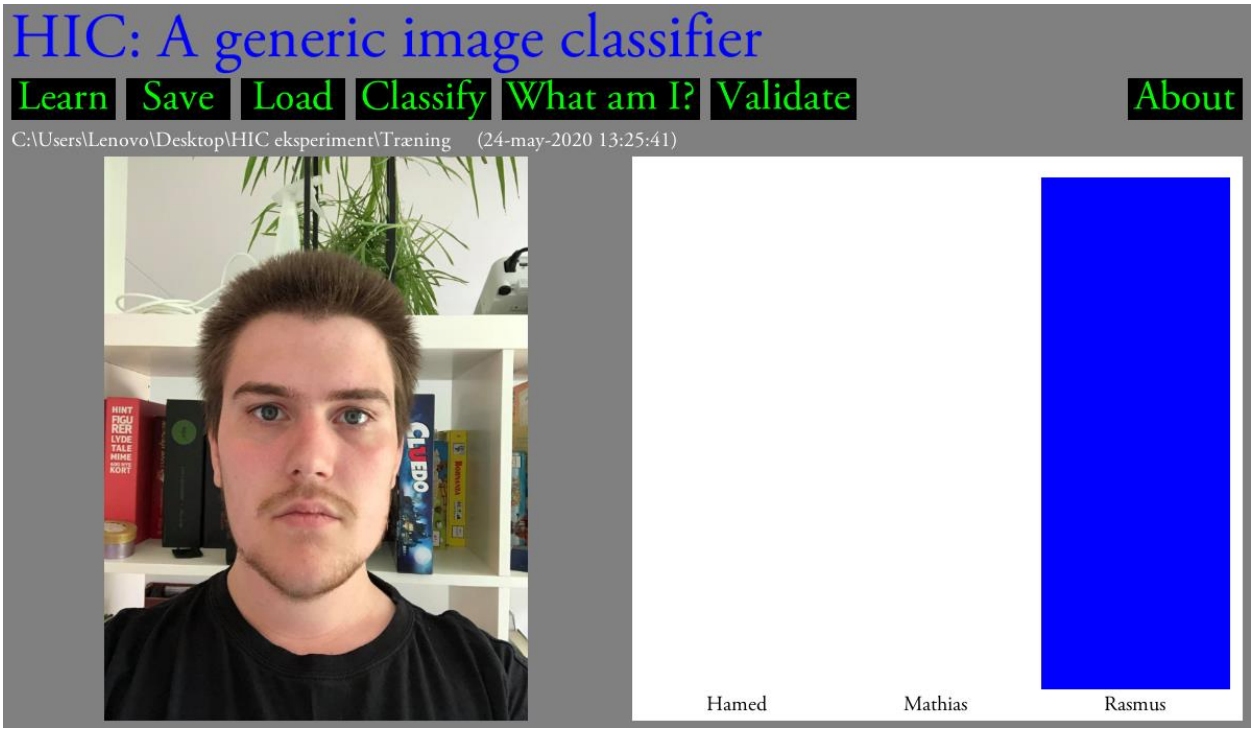
Test 5:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\Lenovo\Desktop\HIC eksperiment\Træning (24-may-2020 13:25:41)
Hamed
Mathias
Rasmus

Test 6:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\Lenovo\Desktop\HIC eksperiment\Træning (24-may-2020 13:25:41)
Hamed
Mathias
Rasmus

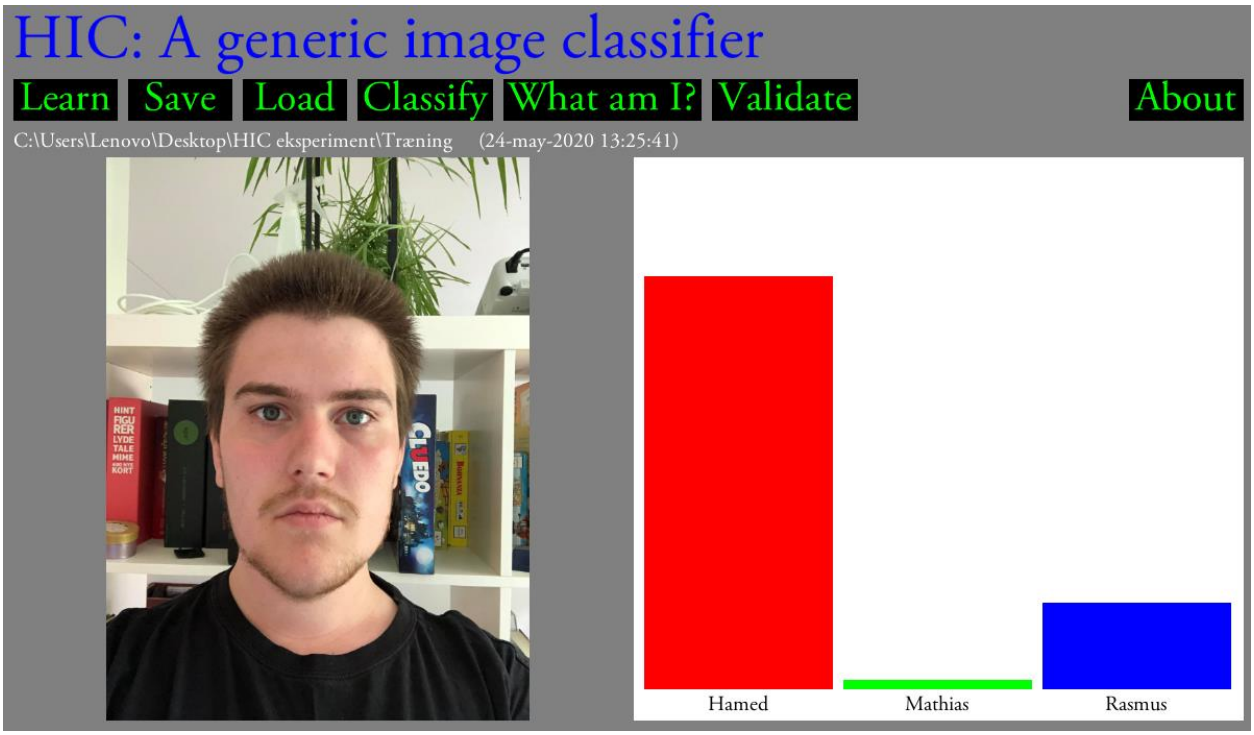
Test 7:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\Lenovo\Desktop\HIC eksperiment\Træning (24-may-2020 13:25:41)
Hamed
Mathias
Rasmus

Test 8:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\Lenovo\Desktop\HIC eksperiment\Træning (24-may-2020 13:25:41)
Hamed
Mathias
Rasmus

Test 9:

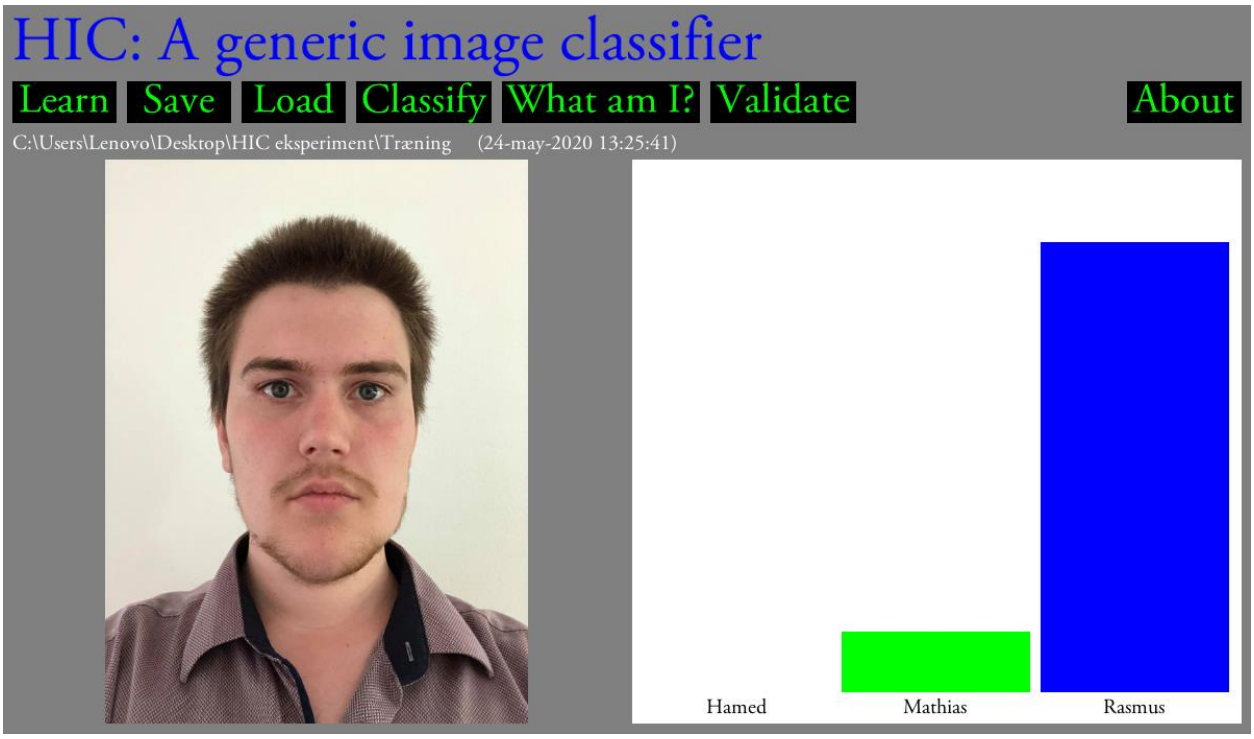


Her blev det meget tydeligere for os, at baggrunden klart havde en effekt på hvilken beslutning programmet kommer frem til. Det kan skyldes de mange farver der lige pludselig bliver introduceret i baggrunden, frem for den helt hvide baggrund.

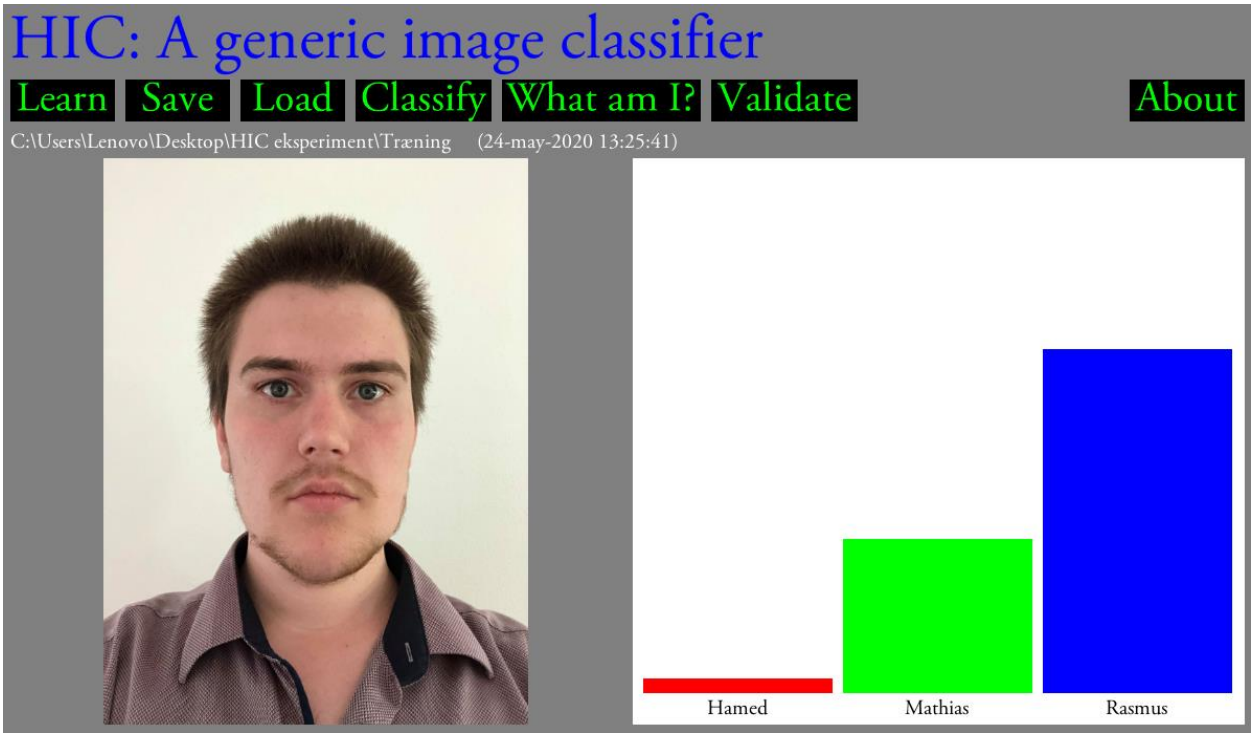
Tøjfarve

Nu hvor vi har fået demonstreret hvor let påvirkelig programmet er på farver, kunne det være interessant at se hvordan ændringer i tøj farven, dog stadig med en hvid baggrund, kunne ændre resultaterne. Her iførte vores testperson, Rasmus, sig i en lyserød/lilla skjorte, for at ændre den ellers sorte t-shirt. Nedenfor ses resultaterne.

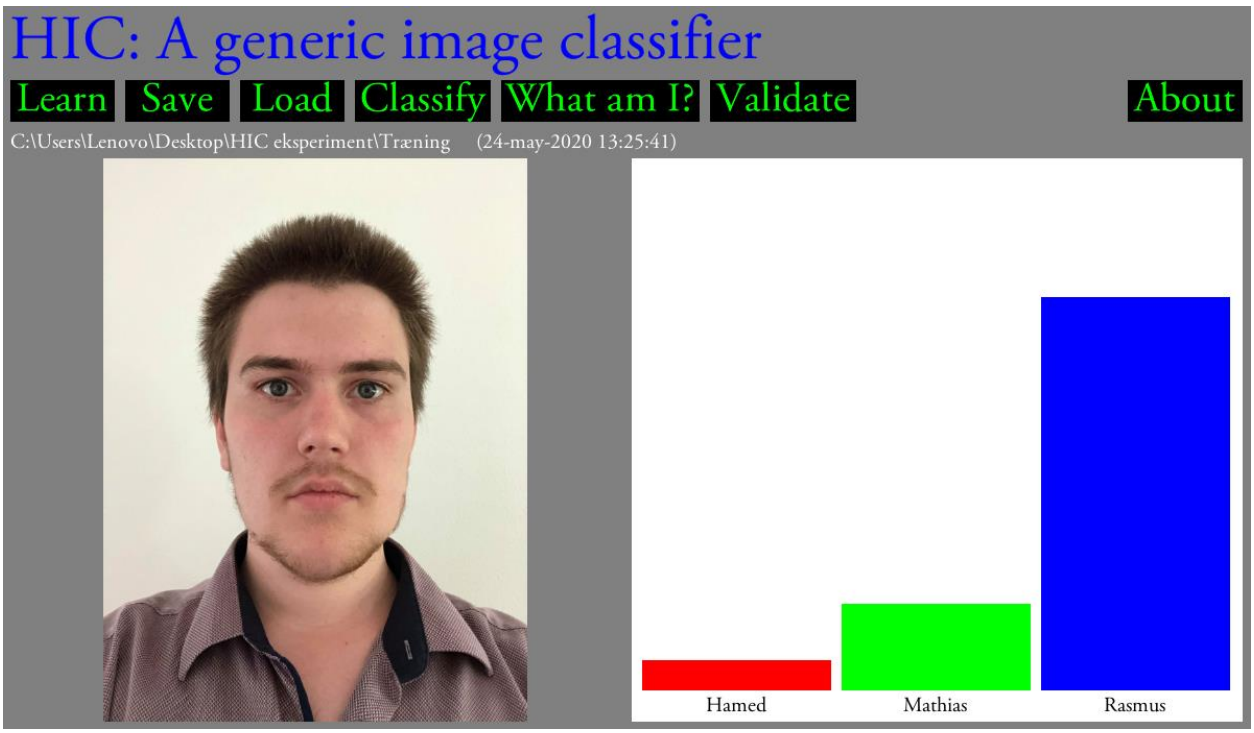
Test 1:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\Lenovo\Desktop\HIC eksperiment\Træning (24-may-2020 13:25:41)
Hamed
Mathias
Rasmus

Test 2:

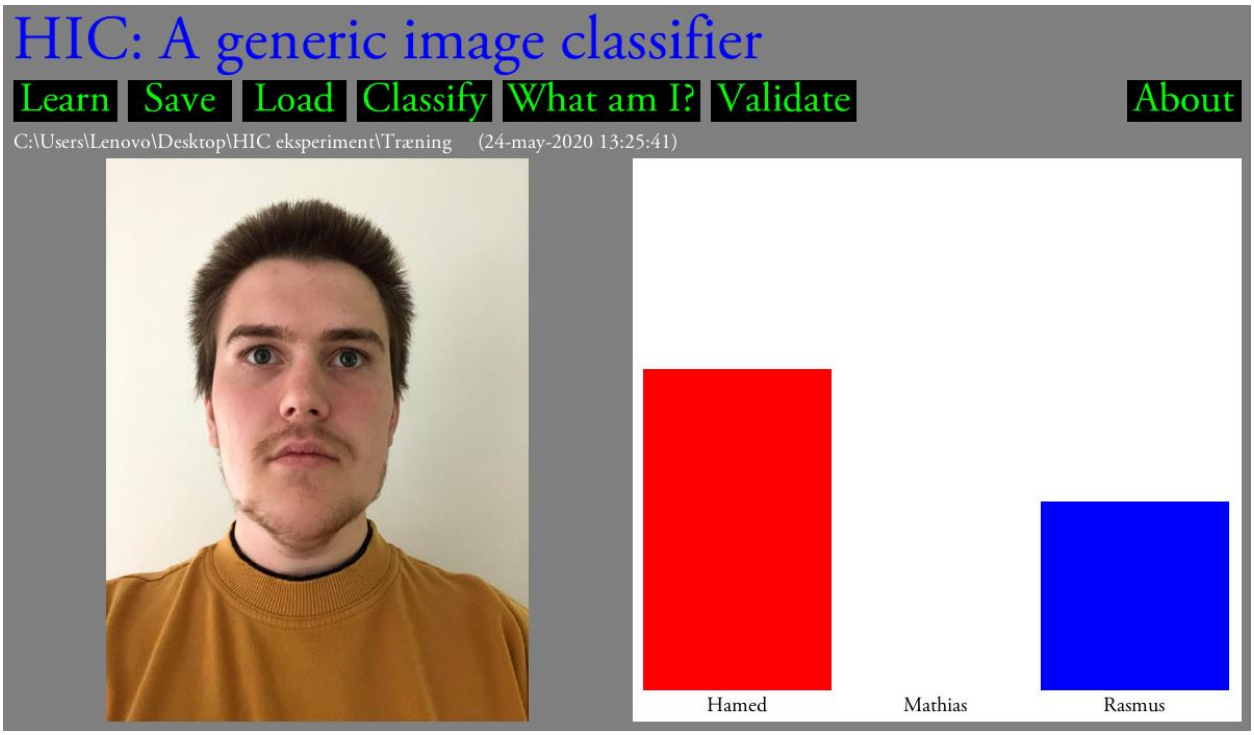

HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\Lenovo\Desktop\HIC eksperiment\Træning (24-may-2020 13:25:41)
Hamed
Mathias
Rasmus

Test 3:

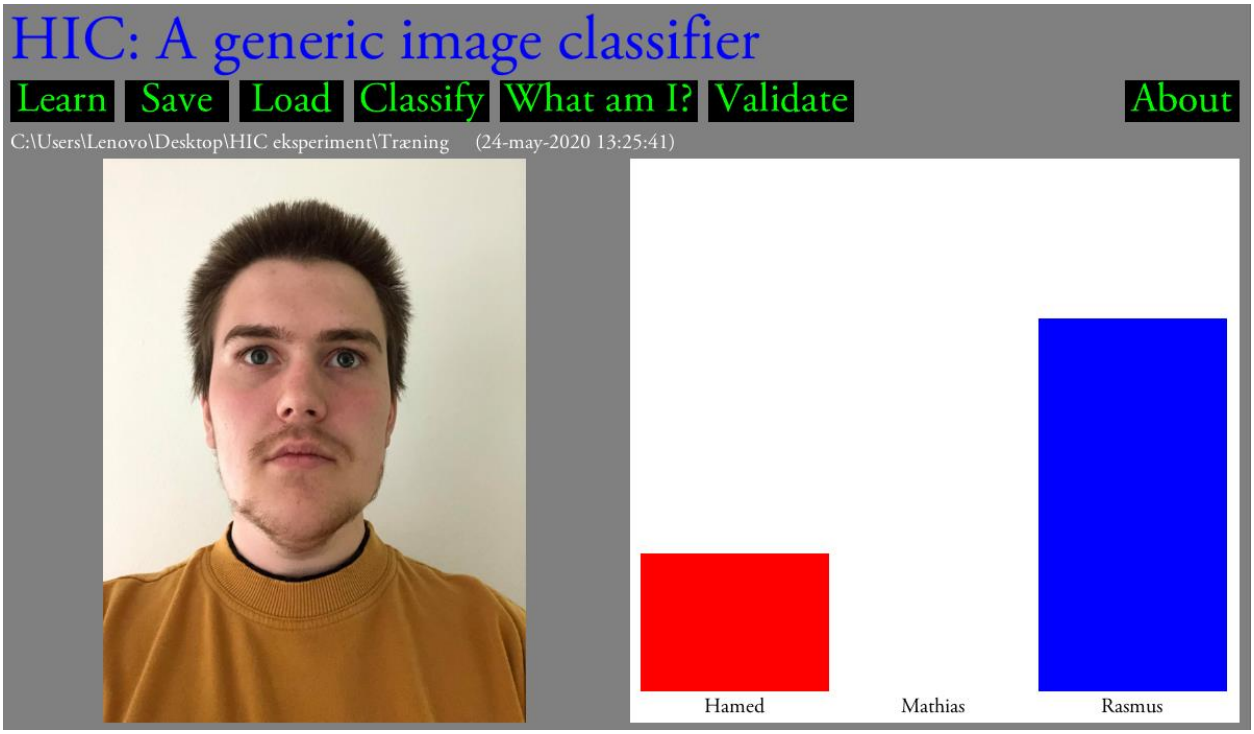


Her afveg programmet ikke det store. Dette giver meget god mening, eftersom ingen af billederne i databasen havde farver i den nuance. Dog havde Hamed en gul t-shirt på, hvor Mathias og Rasmus begge havde sort på. Derfor kunne det være interessant at teste en gul farve i tøjet hos Rasmus, og se om den registrerer billedet, som et af Hamed. Dette gjorde vi, da Rasmus iførte sig en gul trøje. Nedenfor ses resultatet.

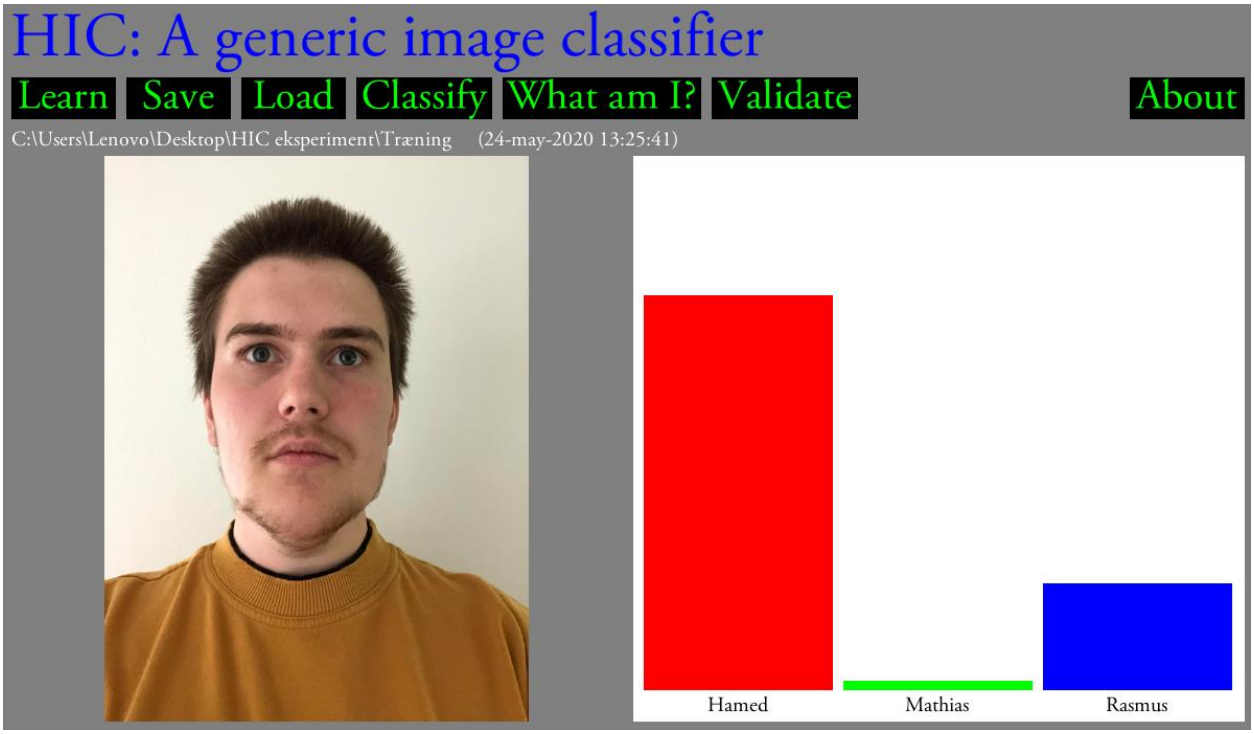
Test 4:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\Lenovo\Desktop\HIC eksperiment\Træning (24-may-2020 13:25:41)
Hamed
Mathias
Rasmus

Test 5:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\Lenovo\Desktop\HIC eksperiment\Træning (24-may-2020 13:25:41)
Hamed
Mathias
Rasmus

Test 6:

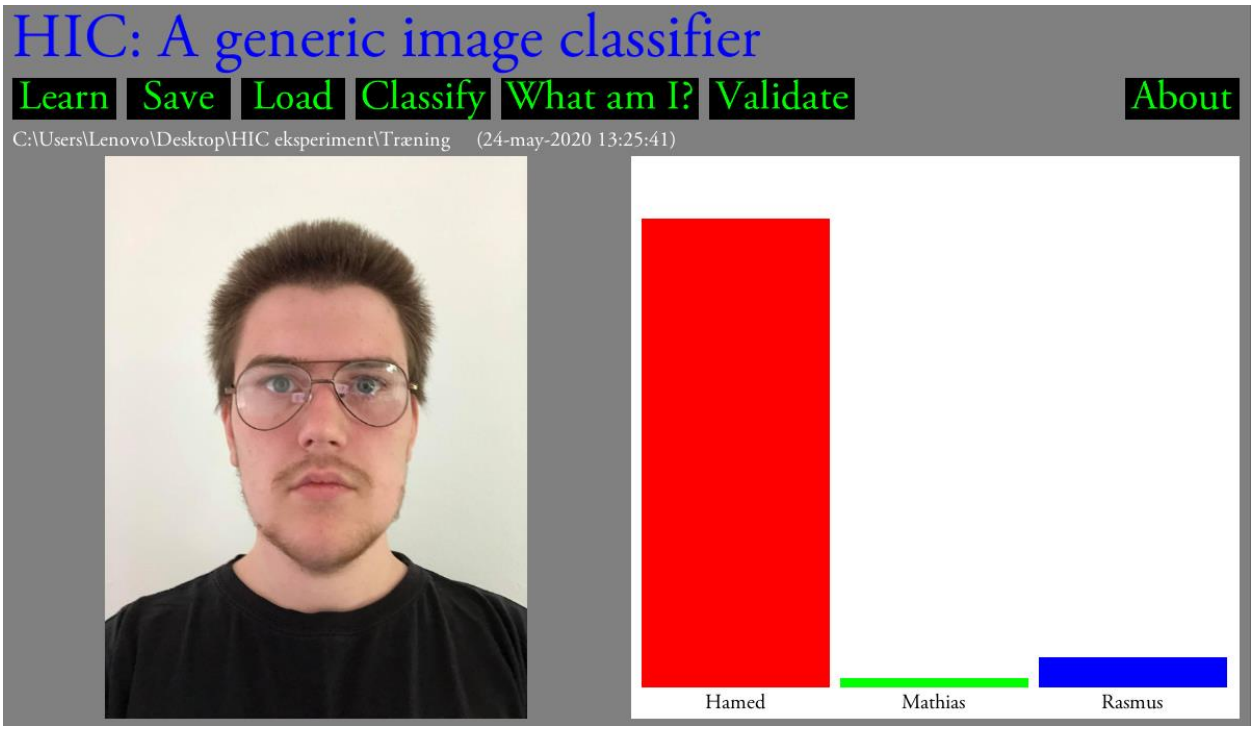


Det er meget mere tydeligt, at i der i den gule nuance bliver begået flere fejl, hen imod Hamed. Dette sker sandsynligvis fordi der er flere pixels i billedet som kan fejlagtigt anses som værende en del af de billeder der ligger under Hameds mappe i databasen. Dog vægter den også stadig Rasmus højt, da der naturligvis stadigvæk er mange af de subwindows som bliver taget, som ligner matcher billederne i hans databasen.

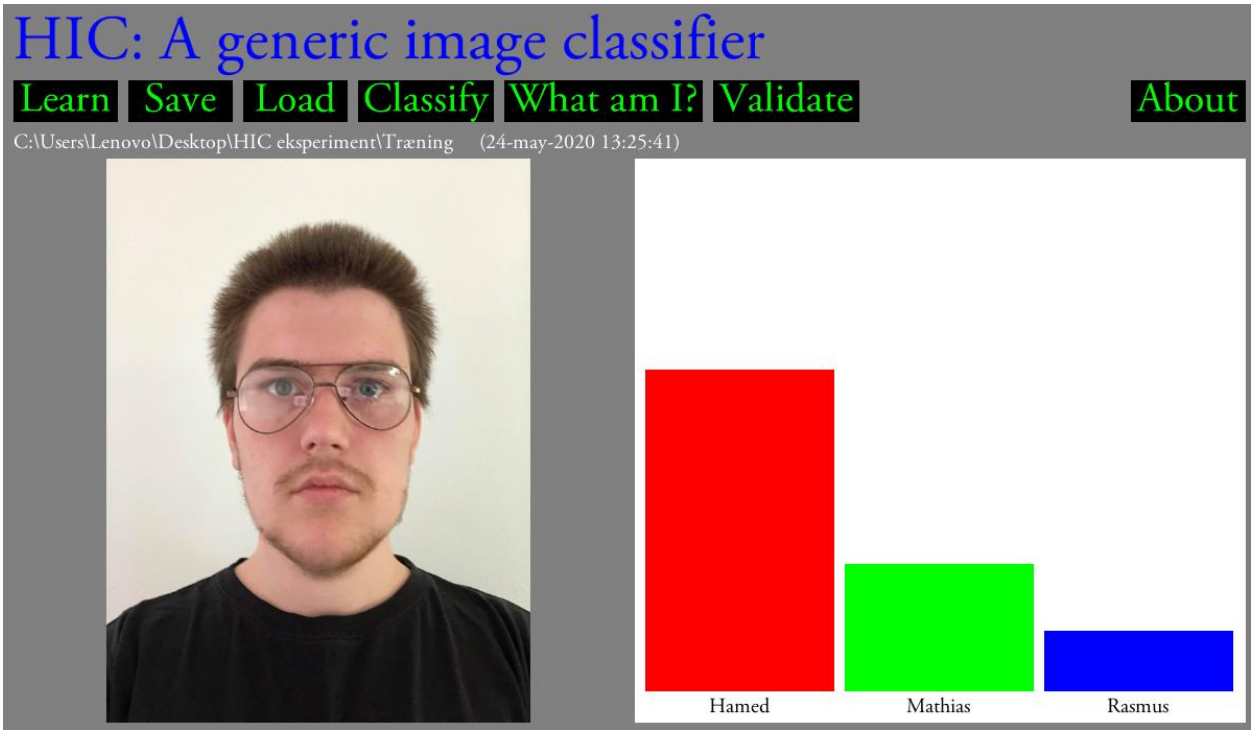
Briller

Nu har vi testet med at udfordre programmet med farver, og det kunne nu være interessant at forstyrre de subwindows der bliver taget fra testpersonens ansigt. Vi har derfor besluttet os at prøve at køre et billede gennem HIC-programmet hvor Rasmus har briller på. Vi bruger stadigvæk den hvide baggrund og den sorte t-shirt, for at kunne teste udelukkende om brillerne har en effekt. Da der dermed er så meget hvidt på billederne, kan vi derfor risikere et meget spredt resultat. Resultatet ses nedenfor.

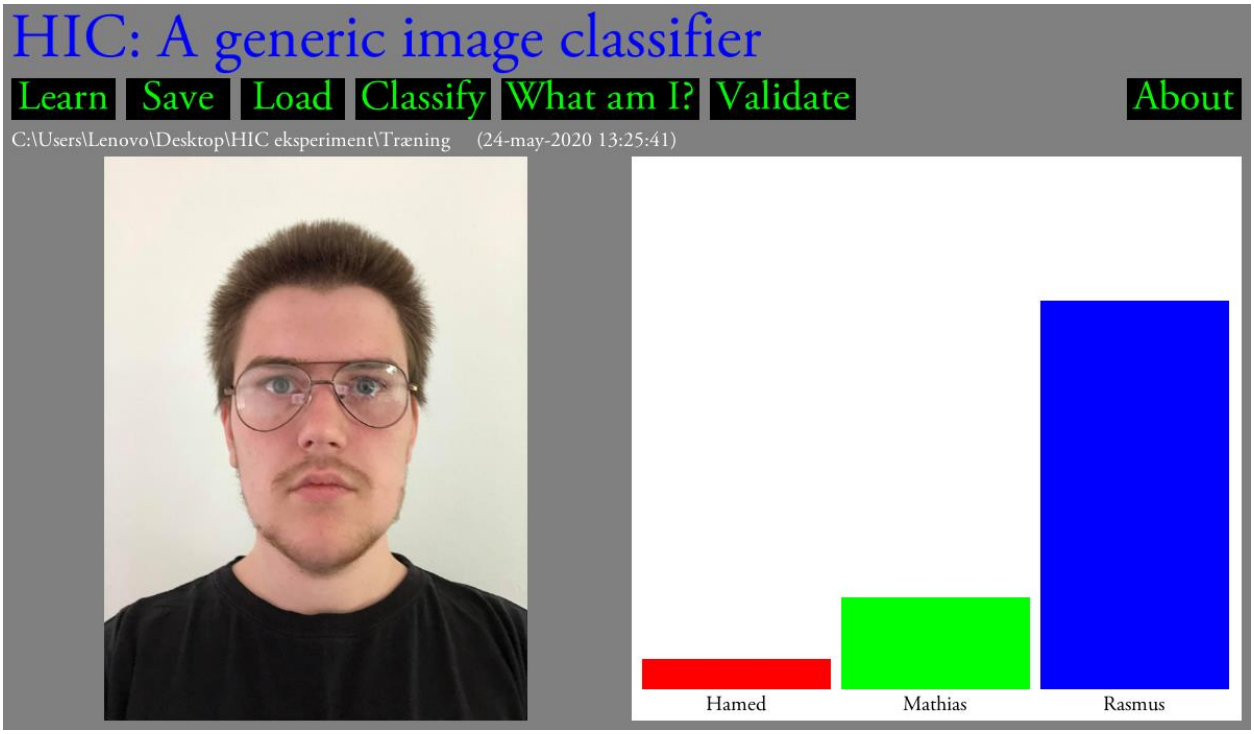
Test 1:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\Lenovo\Desktop\HIC eksperiment\Træning (24-may-2020 13:25:41)
Hamed
Mathias
Rasmus

Test 2:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\Lenovo\Desktop\HIC eksperiment\Træning (24-may-2020 13:25:41)
Hamed
Mathias
Rasmus

Test 3:

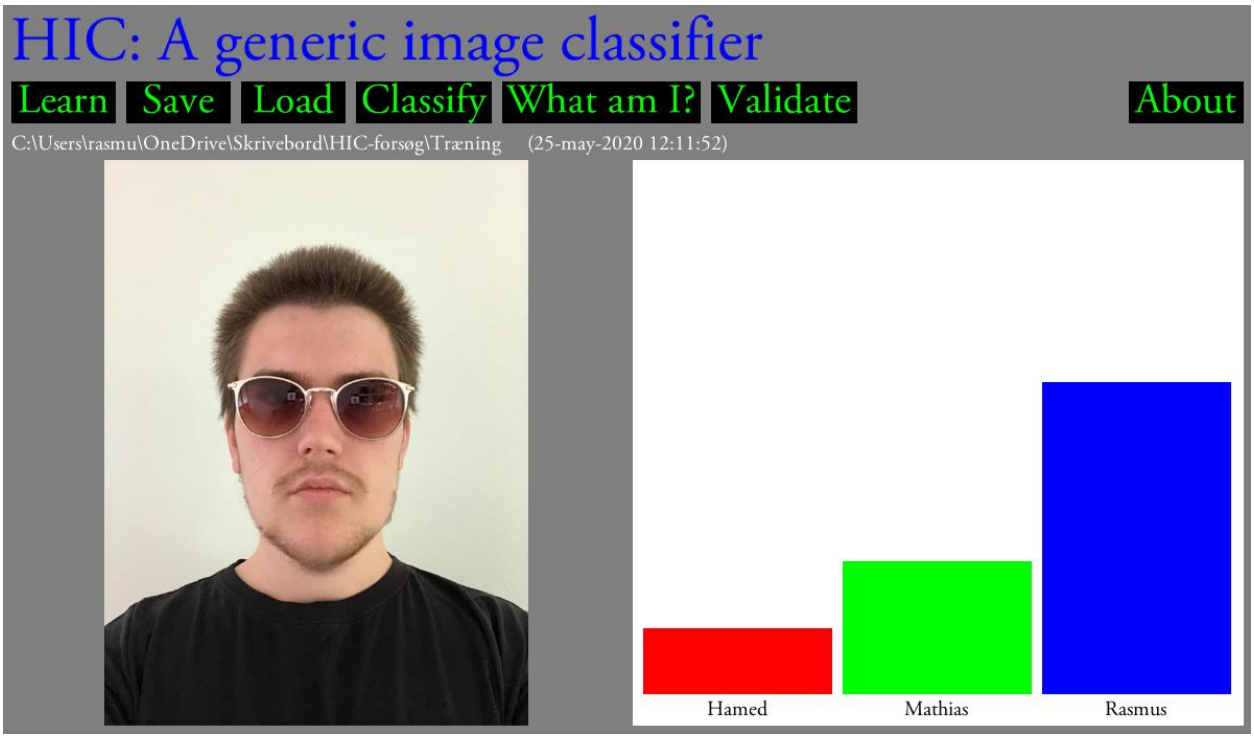

HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\Lenovo\Desktop\HIC eksperiment\Træning (24-may-2020 13:25:41)
Hamed
Mathias
Rasmus

Det er helt tydeligt, at brillerne har haft en forvirrende effekt på programmet. Programmet er meget spredt på alle 3 i databasen, bortset fra 1 gang, hvor programmet klassificerede billedet som værende Hamed. Dette kan være grundet i en række ting. Der er en smule genskær i glasset, som kan forvirre programmet. Derudover er der kommet en række uvante pixels om øjnene, som ikke har været der før. Sidst kan det også skyldes, at når programmet ikke har kunne genkende de pixels om ansigtet, er der istedet lagt vægt på de pixels den kunne få til at passe, i.e. tøjfarve, baggrunden og hårfarve.

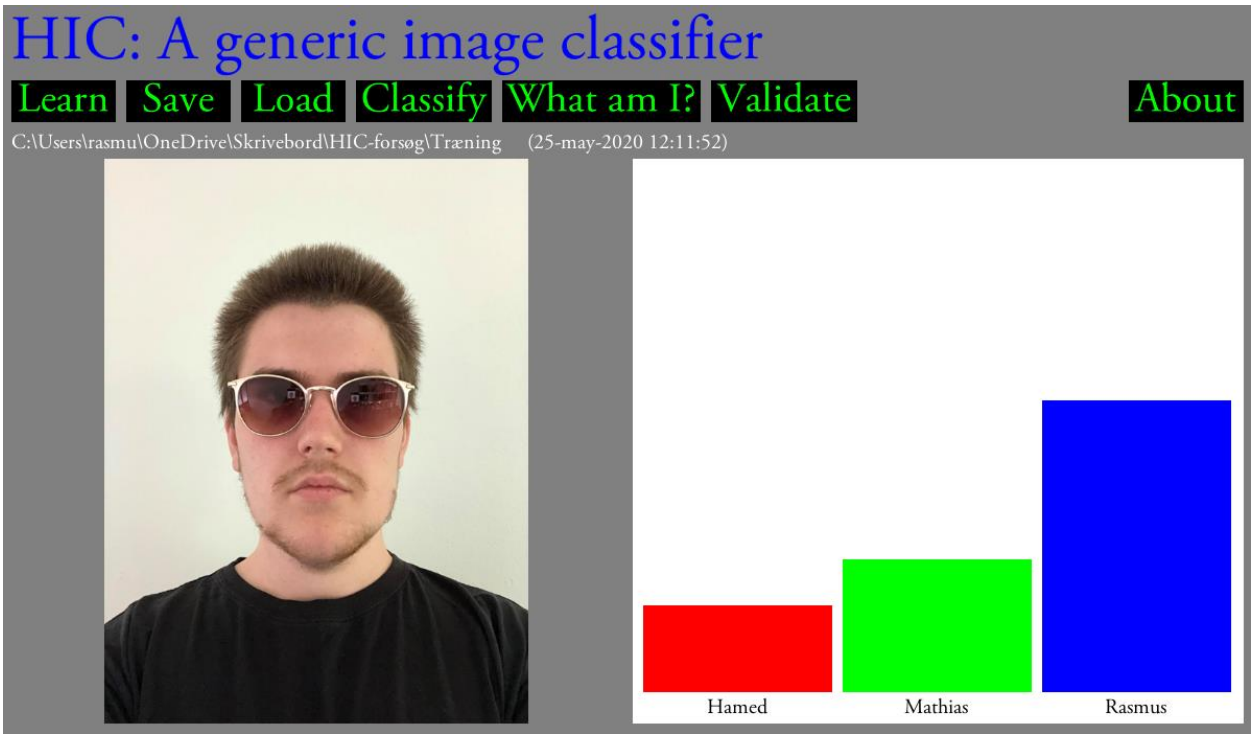
Solbriller

Nu hvor vi har testet det af med briller, og der er opstået en klar forvirring i programmet, har vi besluttet os for at prøve at teste af med solbriller, for at se om det kunne skabe en endnu større effekt end de normale briller Dette kan formentlig ske ved at der er større genskin i solbrillerne når de er sorte, og at man på ingen måde kan se øjnene inden under. Vi gav derfor Rasmus et par solbriller på og resultatet kan ses nedenfor.

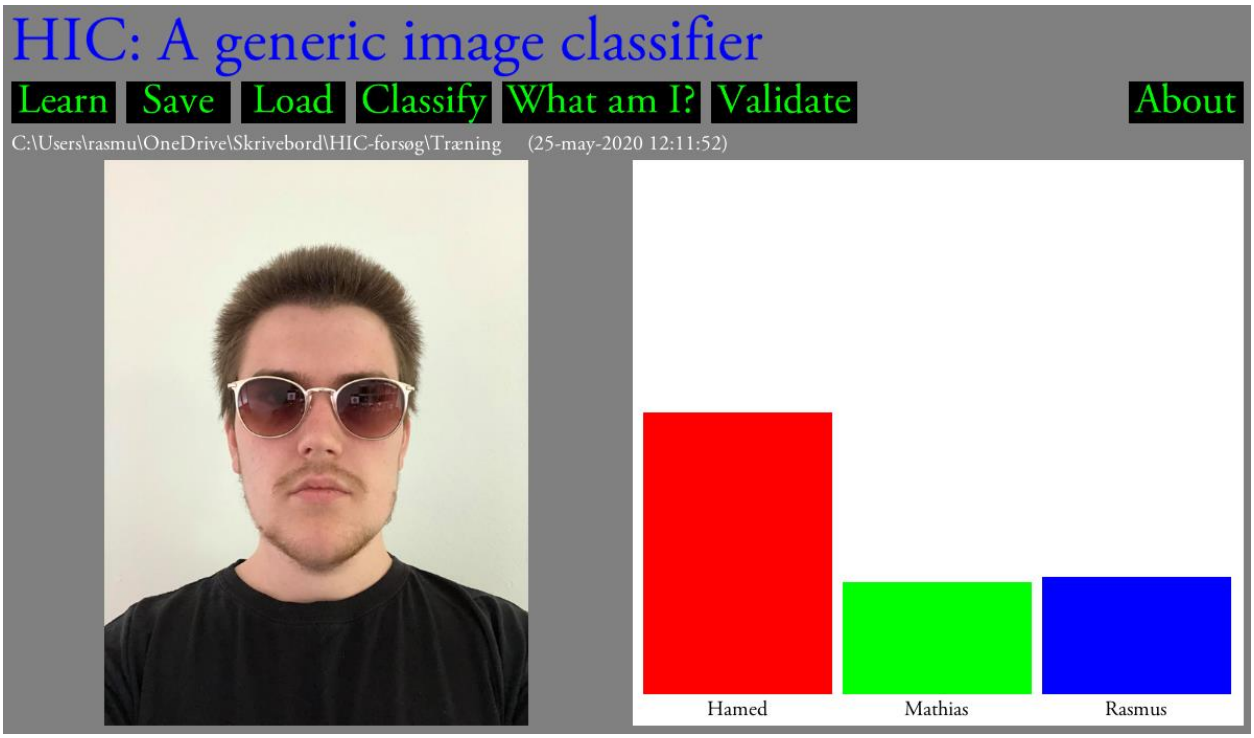
Test 1:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\rasmu\OneDrive\Skrivebord\HIC-forsøg\Træning (25-may-2020 12:11:52)
Hamed
Mathias
Rasmus

Test 2:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\rasmu\OneDrive\Skrivebord\HIC-forsøg\Træning (25-may-2020 12:11:52)
Hamed
Mathias
Rasmus

Test 3:



I dette forsøg opstod der klart mere tvivl, end med de normale briller. Selv i test 1 og 2 viste HIC-programmet overvejende enighed om at det var Rasmus på billedet, men dog stadigvæk med større usikkerhed end tidligere, med de normale briller. I den sidste test kom programmet til konklusionen, at det er Hamed på billedet, dog med en voldsom stor usikkerhed. Dette kan som sagt skyldes at man fjerner en kæmpe del af ansigtet på Rasmus, og programmet kan dermed ikke gå efter det.

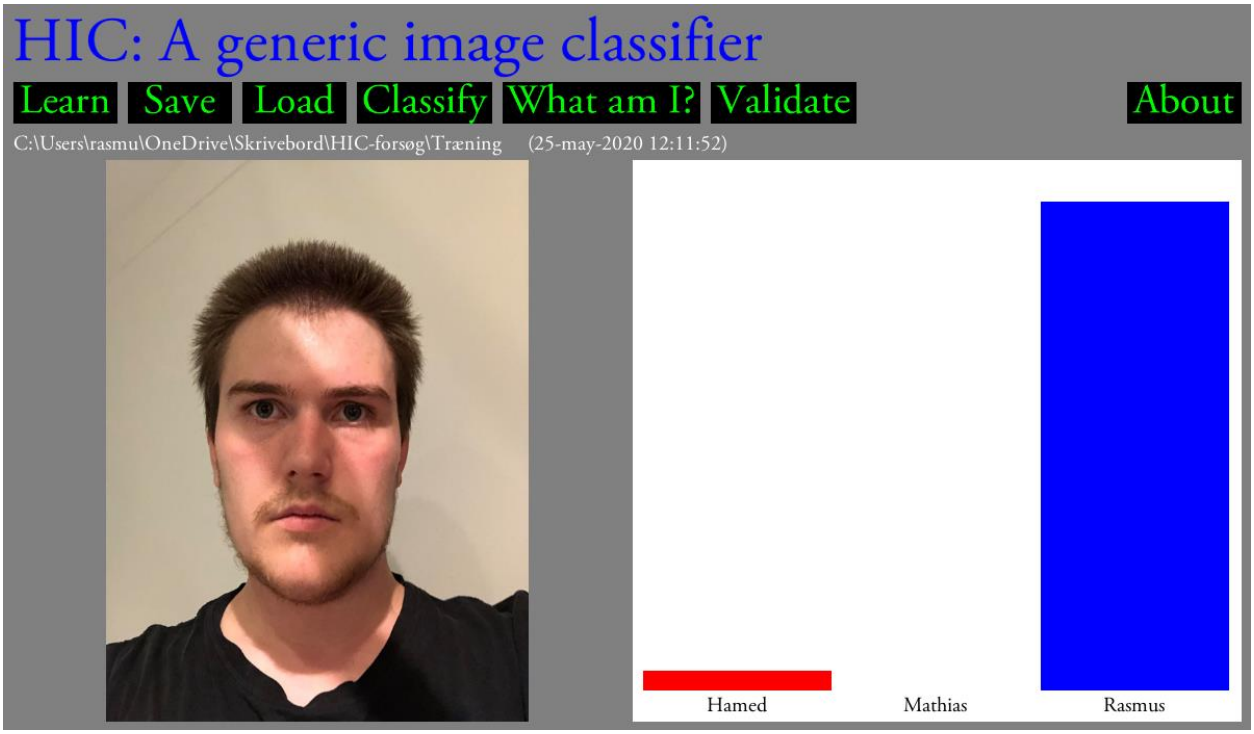
Skygge

Nu har vi så vist at det kan have en stor betydning for programmet, at mørklægge visse dele af ansigtet. Med det i mente besluttede vi os for, at tage et billede med en skygge der løb hen over Rasmus' ansigt. Det var dog en udfordring at få en kraftig nok skygge til helt at mørklægge en stribe af hans ansigt. Billedet samt resultatet af forsøget ses nedenfor.

Test 1:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\rasmu\OneDrive\Skrivebord\HIC-forsøg\Træning (25-may-2020 12:11:52)
Hamed
Mathias
Rasmus

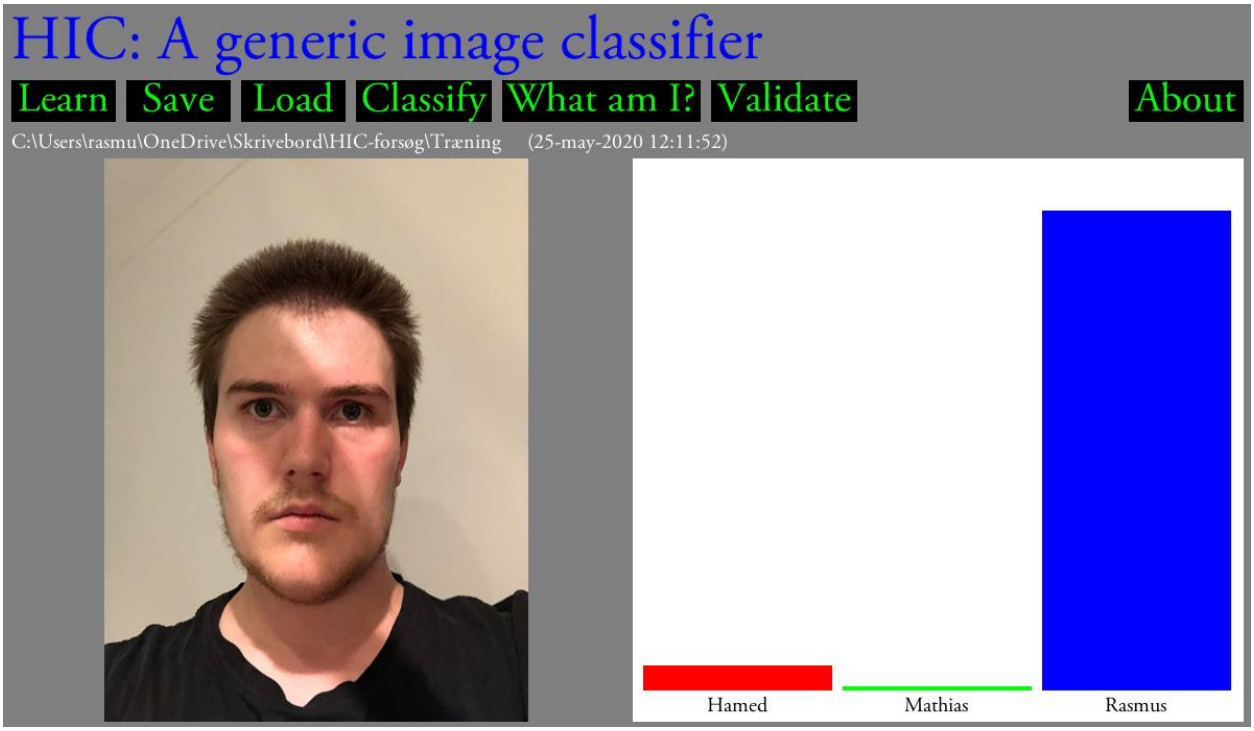
Test 2:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\rasmu\OneDrive\Skrivebord\HIC-forsøg\Træning (25-may-2020 12:11:52)
Hamed
Mathias
Rasmus

Test 3:

Her er der meget bred enighed blandt de forskellige forsøg. For at få et klarere billede af om det bare er en tilfældighed laver vi derfor en række test mere.

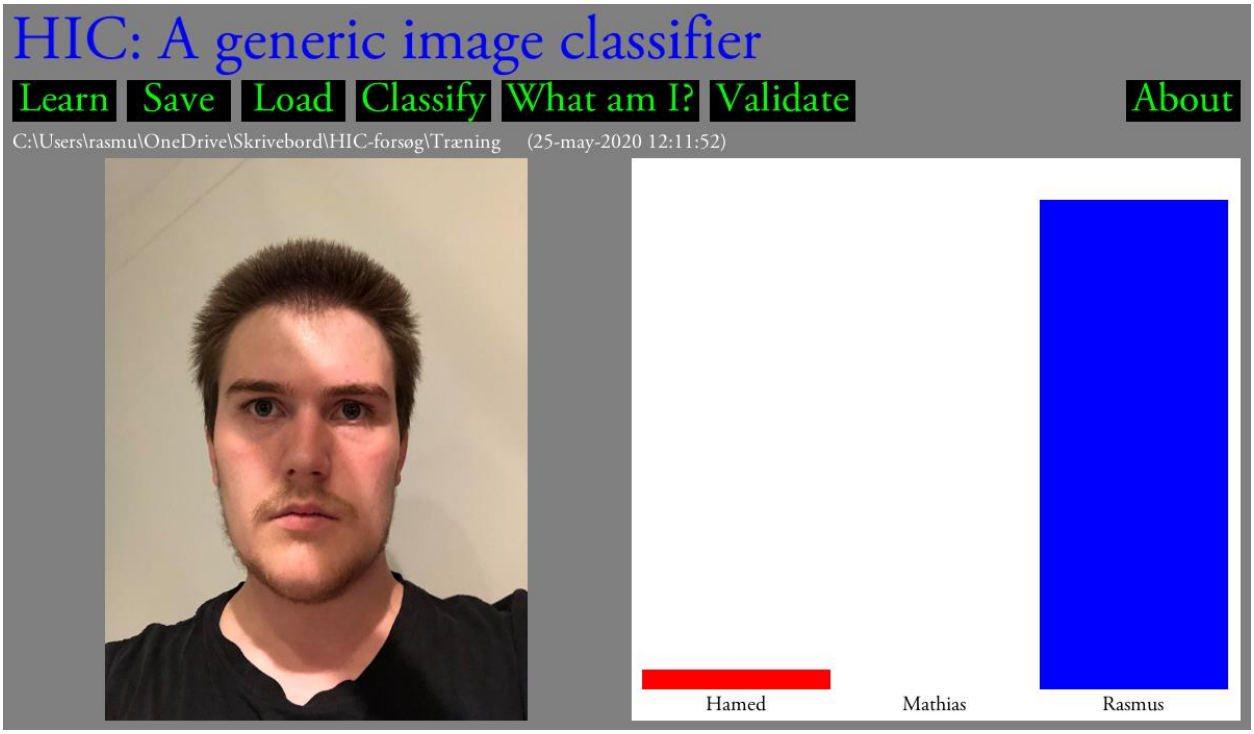
Test 4:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\rasmu\OneDrive\Skrivebord\HIC-forsøg\Træning (25-may-2020 12:11:52)
Hamed
Mathias
Rasmus

Test 5:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\rasmu\OneDrive\Skrivebord\HIC-forsøg\Træning (25-may-2020 12:11:52)
Hamed
Mathias
Rasmus

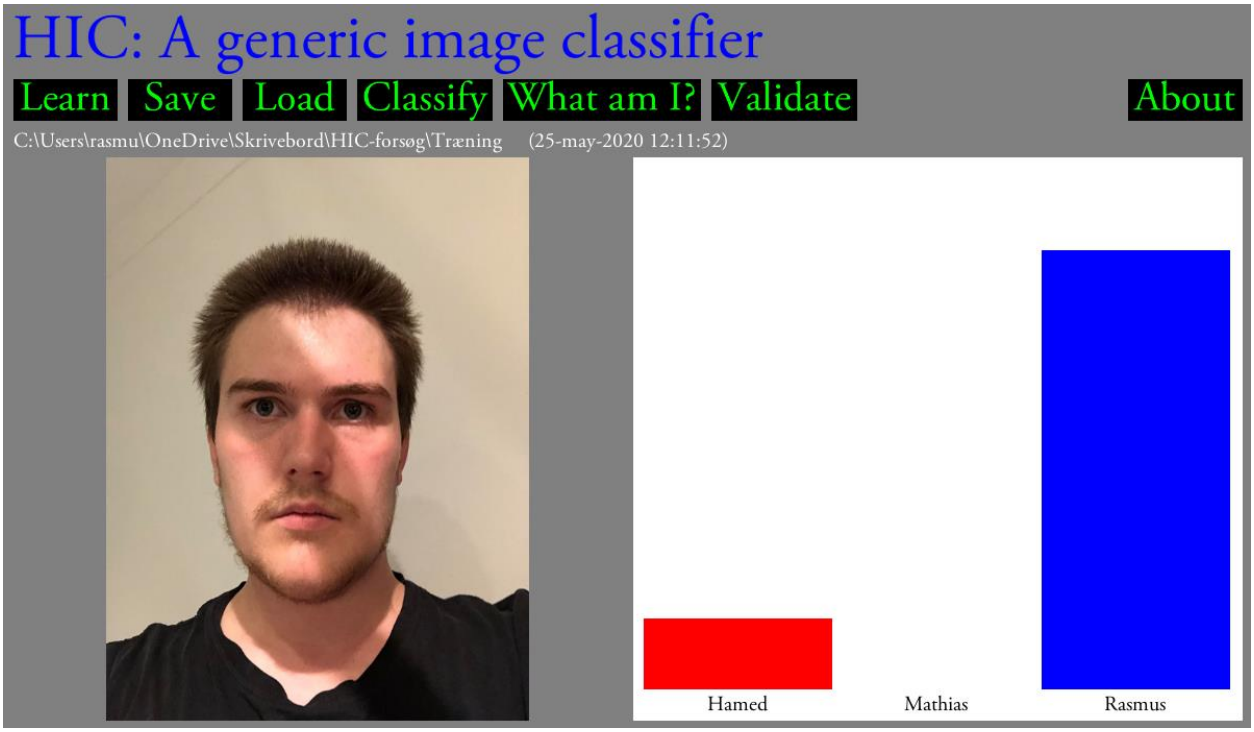
Test 6:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\rasmu\OneDrive\Skrivebord\HIC-forsøg\Træning (25-may-2020 12:11:52)
Hamed
Mathias
Rasmus

Test 7:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\rasmu\OneDrive\Skrivebord\HIC-forsøg\Træning (25-may-2020 12:11:52)
Hamed
Mathias
Rasmus

Test 8:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\rasmu\OneDrive\Skrivebord\HIC-forsøg\Træning (25-may-2020 12:11:52)
Hamed
Mathias
Rasmus

Test 9:

Det er nu helt tydeligt, at skyggen skaber en forvirring. Dette kan skyldes en forvirring da den ikke kan genkende de mørkere pixels hos Rasmus. Det er også værd at lægge mærke til, at skyggen også bliver kastet på væggen bag Rasmus, hvilket naturligvis skaber en anden nuance af hvid, en der ellers er på database-billederne af Rasmus. Dette kan være med til at genkende den hvide baggrund, som værende en af de andre fra databasen.

Mørke

Nu da vi kan se at en skygge har en så stor effekt, har vi forsøgt at begrænse mængden af lys i billedet, så vi får et væsentligt mørkere billede af Rasmus. Ideen her er at programmet formentlig vil have svært ved at genkende personen på billedet, og at vi derfor kommer til at opnå et meget spredt resultat. Derfor vil vi fra starten af teste det 9 gange, så vi får bedre indblik i hvad mørket gør ved resultatet. Billeder og resultat ses nedenfor.

Test 1:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\rasmu\OneDrive\Skrivebord\HIC-forsøg\Træning (25-may-2020 12:11:52)
Hamed
Mathias
Rasmus

Test 2:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\rasmu\OneDrive\Skrivebord\HIC-forsøg\Træning (25-may-2020 12:11:52)
Hamed
Mathias
Rasmus

Test 3:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\rasmu\OneDrive\Skrivebord\HIC-forsøg\Træning (25-may-2020 12:11:52)
Hamed
Mathias
Rasmus

Test 4:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\rasmu\OneDrive\Skrivebord\HIC-forsøg\Træning (25-may-2020 12:11:52)
Hamed
Mathias
Rasmus

Test 5:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\rasmu\OneDrive\Skrivebord\HIC-forsøg\Træning (25-may-2020 12:11:52)
Hamed
Mathias
Rasmus

Test 6:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\rasmu\OneDrive\Skrivebord\HIC-forsøg\Træning (25-may-2020 12:11:52)
Hamed
Mathias
Rasmus

Test 7:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\rasmu\OneDrive\Skrivebord\HIC-forsøg\Træning (25-may-2020 12:11:52)
Hamed
Mathias
Rasmus

Test 8:


HIC: A generic image classifier
Learn
Save
Load
Classify
What am I?
Validate
About
C:\Users\rasmu\OneDrive\Skrivebord\HIC-forsøg\Træning (25-may-2020 12:11:52)
Hamed
Mathias
Rasmus

Test 9:

Som forudset kunne programmet ikke finde ud af at genkende Rasmus. Hvad der dog er interessant er, at der ikke i en eneste af testene blev besluttet at det var Rasmus på billedet. HIC-programmet skiftede mellem Mathias og Hamed, men dog skrånede programmet mest mod Hamed. En potentiel grund til programmet favoriserede Hamed og Mathias frem for Rasmus, kan være at de begge har markant mørkere hår end Rasmus har. En grund til at HIC-programmet derudover favoriserede Hamed over Mathias, kan have at gøre med at Hamed er mørkere i huden end Mathias, og at programmet dermed mente at den mørkere hud på Rasmus' billede, stemte mere over ens med Hameds hud.

Samlede resultat

Efter en række forskellige tests af forskellige usikkerheder er det klart at se, at først og fremmest har baggrunden en klar effekt. Det så vi både med den rodede baggrund og med skygge- og mørke-billedet. Dernæst havde belysningen også en klar effekt på hvorvidt der var fejl i beslutningen eller ej. Briller og solbriller havde en effekt i at forvirre programmet, men ikke i lige så høj grad som at

manipulere med belysning og baggrund. Det lykkedes os også at manipulere resultatet med tøj farver, dog kun med den gule, da der ikke var nogen i databasen Rasmus kunne forveksles med da han havde den lyserøde/lillae skjorte på. Alt i alt kan vi konkludere at hvis der ikke er de store forstyrrelser på de billeder man vil have klassificerede virker metoden om extremely randomized trees udmærket i dette program. Dog kan belysningen virkelig ændre på resultatet, da det kan ændre alt programmet opsnapper fra hudfarve og hårfarve til baggrunden osv.

Potentielle fejlkilder

Som tidligere nævnt i udfordringerne omkring udførelsen af forsøget, havde vi problemer med at tage billederne samlet, som resulterede i at der var 3 forskellige kameraer i brug. Det havde vi allerede forklaret inden, men en anden fejlkilde er, at de testbilleder vi har taget, blev taget med det samme kamera som Rasmus' database billeder blev taget med. Dermed kan det have en effekt på hvorvidt Rasmus bliver favoriseret. Dernæst har vi også baggrunden, som vi i forsøget har afdækket, har en betydelig indflydelse på hvordan billederne bliver klassificeret. Da vi har taget billederne hver for sig, betyder det derfor at vi også har haft forskellige baggrunde. På trods af at vi alle har taget en hvid baggrund, har der været forskelle i belysning, nuance af hvid og lofter. Dette kan derfor have været med til at ændre på resultatet, frem for hvis vi bare havde taget alle billederne på den samme lokation.

Utilsigtede effekter

I dette afsnit vil vi uddybe de utilsigtede effekter af teknologien. Her vil vi komme ind på hvor teknologien er svag og har huller.

Teknologiens svage sider

Som beskrevet tidligere i vores eksperiment med HIC-programmet, oplevede vi store svagheder inden for det program og dens metodebrug, når det kom til at introducere farver og belysning

programmet ikke var klar på. Dog sker dette ikke kun inden for HIC-programmet, men er et generelt problem inden for 2D ansigtsgenkendelse (Zhao & Chellappa, n.d.). Det er bl.a. også et problem med hvilken vinkel billedet bliver taget fra, da det kan have en effekt på hvordan et ansigtsgenkendelsessystem vil klassificere billedet. Det er dog ikke kun inden for 2D ansigtsgenkendelsesteknologi der opstår problemer. Inden for 3D ansigtsgenkendelsesteknologi er der naturligvis også en række potentielle problemer, som kan resultere i fejl i ansigtsgenkendelse. Her er et af de mest udbredte problemer overtræning af et ansigtsgenkendelsprogram (Christiansen, 2020). Overtræning er en effekt af, at et program der ikke har generaliseret under sin træning. Dette kan forekomme hvis et program har for mange frihedsgrader og ikke bliver holdt øje med. Her lærer programmet at læse alle sine egne træningsbilleder i databasen til perfektion, men kommer til at have svært ved at læse fremmed og udefrakommende data (Christiansen, 2020). Derfor vil man naturligvis ikke kunne stole 100% på det resultat som et overtrænet program tilbyder en. Et andet problem man kan støde på inden for ansigtsgenkendelsesteknologi , er den manglende evne til at kunne genkende nogle minoriteter med med mørk hud. Dette er et problem som eksempelvis tech giganten Google er stødt ind i (Wong, 2019). En af grundene til at dette er svært for nogle typer af ansigtsgenkendelsesteknologi, kan være at det er baseret på Eigenfaces. Her kan problemet, egentlig ret simpelt, være skyld i at databasen for mørkere minoriteter ikke er stor nok. Man kunne potentielt komme denne udfordring til livs, ved at udvide mængden af billeder i databasen, med mørke minoriteter som motiv. Dette er også en løsning som Google anvender (Wong, 2019).

Diskussion

I dette afsnit vil vi diskutere både de teknologiske udfordringer ansigtsgenkendelsesteknologi har og hvordan lovgivningen i Europa og Danmark har påvirket udbredelsen af teknologien.

Teknologiens udfordringer

Teknologier baseret på biometrisk data er i kraftig vækst. Fingeraftryksscanning er blevet en teknologi som man kan støde på i alt fra mobiltelefoner til køen i Crazy daisy("Godkendt med et

fingertryk", 2020). Samtidig bliver dit ansigt scannet når du går til fodbold på Brøndby stadionen for at sikre at du ikke har karantæne("Ansigtsgenkendelse - Brøndby IF", 2020). I takt med at biometriske teknologier vinder indpas i samfundet, bliver man som borger i højere grad opmærksom på at der er stor forskel på hvordan interaktionen med teknologierne påvirker individet. Teknologier som fingeraftrykksscanning og irisscanning har en anden karakter end ansigtsgenkendelses teknologi, da det kræver at individerne fysik interagerer med teknologien. individet ved derfor hvornår teknologien bliver anvendt, og det er derfor nemmere at tage et aktivt valg om hvorvidt man vil interagerer med teknologien eller ej. Det samme valg har man ikke hvis man som individ befinder sig i et område, hvor ansigtsgenkendelse bliver anvendt. Det er næsten umuligt at vide hvorvidt ansigtsgenkendelse finder sted eller ej, hvis der ikke er en klar skiltning. Ansigtsgenkendelses usynlighed er en fordel i forhold til andre biometriske teknologier når det kommer til udviklingen af kommercielle brugsmuligheder. Da det ikke er nødvendigt at være i fysisk kontakt med teknologien, bliver det muligt at udvikle en række services som gør det nemmere og hurtigere, et eksempel kan være når man handler ind og kun betaler ved at bruge ansigtet. Udvalgte barer i London bruger ansigtsgenkendelse til at betjene kunderne i baren i den rigtige rækkefølge, alt efter hvem der kom først("Ansigtsgenkendelse er overalt omkring os", 2020). Det sker uden man som kunde er klar over at man er under påvirkning af teknologien. Man vil som kunde opleve en forbedret service uden nogen dårlige oplevelser. Ansigtsgenkendelses usynlige karakter kan være med til at gøre interaktion med teknologien behageligt, da der ikke er noget fysisk artefakt at forholde sig til. Man bliver fri for at skulle trække et nummer og trykke på den samme skærm som resten af kunderne i banken har berørt. Man skal blot træde ind og vente på at det bliver din tur.

Ansigtsgenkendelse har også den fordel i forhold til andre biometriske teknologier, at den både kan identificere og verificer et stort antal personer på samme tid.

Ansigtsgenkendelse er dog mere begrænset af de forhold, hvorunder teknologien bliver anvendt, end anden biometrisk teknologi. Fingeraftrykksscanning er ikke på samme måde afhængig af, at lysforholdene skal være gode, eller at vinklen skal være på en bestemt måde for at få en høj nøjagtighed.

Ser man på politiets tilgang til anvendelse af nummerplade genkendelse, bruger de det både som masseovervågning af biler via deres faste installationer og til at stoppe bilister der har begået lovovertrædelser som manglende forsikring eller tidligere straffet.(FDM 20/5-2017) Der er betydelig forskel på disse to systemer da den første leder efter et match, ligesom med ansigtsgenkendelse og det andet overvåger al færdsel. Dette er væsentligt da politiet vil udvide brugen af ansigtsgenkendelse, for en overførelse af deres brug af nummerplade genkendelse til brug af ansigtsgenkendelse, vil folk der ikke har begået kriminalitet blive overvåget i samme grad som kriminelle, vel og mærke uden at mærke det fysisk. Nick Hækkerup, Danmarks justitsminister har i relation til udvidelsen af overvågning i det offentligheden udtalt at, mere overvågning er lig med mere frihed (Information 10/12-2019). Indføres systemet, vil staten have adgang til samme overvågning af borgere som i Kina, det kræver en diskussion i samfundet om hvad der er acceptabel overvågning for at sikre håndhævelse af loven, og hvad der krænker vores ret til at færdes frit i det offentlige rum uden at blive overvåget. Man kan diskutere hvilken forskel der er på at vi i forvejen efterlader et digitalt aftryk ved brug af smartphones. I det første tilfælde skal politiet henvende sig til teleselskaber for at få udleveret disse oplysninger, men ved overvågningskameraer opsat af staten, vil der ikke være kontrol af brugen fra politiets side. Det åbner samtidig op for, at man i fremtiden vil have mulighed for at algoritmer overvåger færdselsmønstre og bringer borgere i søgelyset pga. en mindre overtrædelse af f.eks. færdselsloven. Netop det bliver brugt i Kina, bare i form af et pointsystem hvor man mister point for at gå over for rødt, når en borger er nede på et bestemt niveau af point, vil de ikke kunne bruge visse dele af infrastrukturen som tog og på den måde blive sanktioneret på anden vis en økonomisk.

I forhold til fremtidig brug af ansigtsgenkendelse inden for afvikling af online eksamener som tidligere nævnt, vil det foregå med foranstaltninger så det ikke overvåger alle handlinger begået foran computeren. Brugen af dette system vil udelukke snyd inden for uddannelse og åbne for muligheden af flere online eksamener.

Brugen af biometriske pas giver staten to typer af biometriske data, fingeraftryk og billede, kobler man databasen til et fremtidigt system af ansigtsgenkendelse vil man kunne identificere alle med biometrisk pas. Biometriske pas er på den anden side også til gavn for brugeren, da de er skabt for at sikre mod identitetstyveri og gøre rejsetiden brugt i lufthavnen mindre.

Lovens påvirkning på teknologiens udbredelse

Europa-parlamentets persondataforordning skaber et sikkerhedsnet til borgerne for at deres biometriske data ikke bliver brugt af bla. Virksomheder der har gevinst for øje. Det er gjort ved at man har forbudt behandlingen af særlige kategorier af personoplysninger, herunder biometriske data (Europa Parlamentet, 2016). Dog har man valgt at åbne op for behandlingen af disse typer data under visse specifikke forhold. På den måde har EU ikke lukket døren for udviklingen og udbredelsen af teknologien helt. Man har blot valgt at begrænse den for at sikre sig, at den ikke løber løbsk, da det kan føre til en større usikkerhed blandt befolkningen, især for minoritetsgrupper.

Det første forhold der tillader behandlingen af biometriske data er at borgeren har givet samtykke til behandlingen af den type data. Her kan man tale om en begrænsning af teknologiens brug og dermed også dens udbredelse, da man er afhængig af borgerens samtykke. Dette gør at borgerne i EU landene har magten til at selv at vælge hvem der har adgang og muligheden til at benytte sig af ansigtsgenkendelses teknologi. Det vil sige at i det tilfælde hvor en virksomhed ønsker at benytte sig af teknologien, er det op til borgerne om der skal gives adgang til det eller ej. Det er op til borgerne om de kan stole nok på den virksomhed til at give dem adgang til deres personlige oplysninger.

Derudover giver mange af de resterende forhold kun tilladelse til behandling af den type data hvis det er nødvendigt for at beskytte borgernes rettigheder, fysiske vitale interesser og/eller borgernes politiske, religiøse eller filosofiske holdninger. Disse forhold giver altså kun adgang til staten, sundhedsvæsenet og vise stiftelser, sammenslutninger eller foreninger. Her bliver døren for virksomheder der har gevinst for øje lukket og begrænser brugen til nødvendighed. Dette har også en betydning for udviklingen og forbedringen af teknologien, da videnskabsmænd og ingeniører bliver begrænset til kun at kunne foretage test af frivillige og dem selv.

På den anden side så kan der argumenteres for at forhold fem, *"Behandling vedrører personoplysninger, som tydeligvis er offentliggjort af den registrerede."* (Europa Parlamentet, 2016), skaber et stort smuthul for alle de andre begrænsninger loven sætter, især i den moderne

verden vi lever i idag, hvor sociale medier er så udbredt. Forhold fem tillader behandlingen af denne type data, hvis det vedrører personoplysninger som tydeligvis er offentliggjort af den registrerede. Det vil sige at billeder og videoer der er offentliggjort på de sociale medier, kan bruges af bla. Virksomheder med gevinst for øje. Det giver altså adgang til alt hvad der er offentliggjort af de 71% af den danske befolkning der bruger facebook (Danmarks Statistik, 2018). Man skal så lige tage i betragtning, at det ikke er alle dem der bruger facebook der har offentliggjort dere billeder og videoer. Stadigvæk så ved enhver der bruger facebook at det er størstedelen af brugerne der har billeder af dem selv, deres venner, deres børn og familie. Hvilket giver teknologien masser af muligheder både til at blive bedre, da man har mange billeder der kan bruges til at teste og træne maskinen, og udbrede sig. Og som nævnt tidligere så er der allerede virksomheder som Clearview der har udnyttet dette og indsamlet nok billeder fra sociale medier til at bygge en database stor nok til at bygge teknologien og sælge adgangen til den videre (Hill, K. 2020). Flere vil ønske at benytte sig af teknologien hvis de kan se fordel for i det, at teknologien har potentiale og bliver bedre med tiden og selvfølge at det er lovligt at implementer den og benytte den.

Konklusion

Ansigtsgenkendelse er en teknologi som er i kraftig udvikling, og inden for de seneste år er anvendelsen blevet udbredt til en række områder.

Ud fra det seneste årtis forskning og brug af ansigtsgenkendelse, har det opnået en sikkerheds rate i match på 99.8% og endt med blive den mest alsidige metode til identificering af individer. Den seneste udvikling har udfordret brugen af ansigtsgenkendelse i forhold til loven og resulteret i direkte handling fra Europa parlamentet, for at skabe retningslinjer i indsamling og brugen af data i forbindelse med overvågning. Hvilket er med til at begrænse brugen af teknologien til en vis grad, da det sætter yderligere krav til behandlingen af personoplysninger. Dog giver det stadigvæk rum til udbredelse af teknologien. Der skal blot tages hensyn til retningslinjerne der har til formål at sikre borgernes rettigheder og som giver dem en mulighed for at bibeholde deres privatliv. Det vækker dog stadigvæk bekymring, da vi i et dansk perspektiv ikke har et klart overblik om politiets

bemyndigelser til brug af teknologien og om det vil blive brugt i samme udstrækning som nummerpladegenkendelse.
Vi kan konkludere at ansigtsgenkendelse åbner op for nye arbejdsmetoder inden for områder, som afholdelse af online eksamener og overvågning, i alt fra arbejdsgivers kontrol af hjemmearbejdende til masseovervågning fra statens side, uden at man fysisk mærker overvågningen.

Ansigtsgenkendelsesteknologi er stadigvæk påvirket af miljøet hvor i teknologien bliver brugt, og kan derfor ikke opnå en lige så høj genkendelses nøjagtighed som i de test miljøer systemerne bliver udviklet i. Det er derfor vigtigt for teknologiens fremadrettede udbredelse, at det bliver muligt at genskabe de lukkede miljøers høje nøjagtighed i den virkelige verden.

Litteraturliste

3D facial recognition system VOCORD FaceControl 3D. (2016). Retrieved 1 June 2020, from https://www.youtube.com/watch?v=FRq0qXOoBAc

Ansigtsgenkendelse - Brøndby IF. (2020). Retrieved 1 June 2020, from https://brondby.com/klub/stadion/stadionoverblik/ansigtsgenkendelse/

Ansigtsgenkendelse er overalt omkring os. (2020). Retrieved 1 June 2020, from https://heartbeats.dk/slut-med-at-blive-sprunget-over-i-barkoeen-ansigtsgenkendelse-er-overalt-omkring-os/

BIOMETRIC DATA, FACE. Retrieved 1 June 2020, from http://news.bbc.co.uk/2/shared/spl/hi/guides/456900/456993/html/nn2page1.stm

Boje, T. (2020). komparativ metode | lex.dk – Den Store Danske. Retrieved 29 May 2020, from https://denstoredanske.lex.dk/komparativ_metode

Clausen, J(2012), Algoritmer Retrieved 1 June 2020, from

https://denstoredanske.lex.dk/algoritme?utm_source=denstoredanske.dk&utm_medium=redirect&utm_campaign=DSDredirect

Christiansen, H. (2016). *HIC: An image classification system based on supervised machine learning*. Roskilde: Roskilde Universitet.

Christiansen, H. (2020). *Vigtige begreber om maskinlæring*. Roskilde: IMT, Roskilde Universitet.

Danmarks Statistik. (2018). *It-anvendelse i befolkningen 2017*. Agnes Tassy. https://www.dst.dk/da/Statistik/Publikationer/VisPub?cid=20739

Datatilsynet, Adgangskontrol ved brug af ansigtsgenkendelse. (2009). Retrieved 1 June 2020, from https://www.datatilsynet.dk/tilsyn-og-afgoerelser/historiske-afgoerelser/2009/jun/adgangskontrol-ved-brug-af-ansigtsgenkendelse/

Datatilsynet, Udtalelse til Rigspolitiet om brug af automatisk nummerpladegenkendelse. (2015) Retrieved 1 June 2020, from

https://www.datatilsynet.dk/tilsyn-og-afgoerelser/historiske-afgoerelser/2015/mar/udtalelse-til-rigspolitiet-om-brug-af-automatisk-nummerpladegenkendelse/

Deduktion, induktion og abduktion. Retrieved 29 May 2020, from https://atumidt.dk/sites/default/files/aktiviteter/forskningsstrategier_mc.pdf

Europa Parlamentet. (2016). EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679 af 27. april 2016. *Den Europæiske Unions Tidende*.

Eskildsen, E., & Sonne, F. (2019). Månelandingen fylder 50: Her er alt, du skal vide, om missioner og konspirationer. Retrieved 2 June 2020, from https://videnskab.dk/teknologi-innovation/maanelandingen-fylder-50-her-er-alt-du-skal-vide-om-missioner-og-konspirationer

Facebook indgår milliardforlig og afværger retssag om ansigtsgenkendelse. (2020). Retrieved 1 June 2020, from https://www.computerworld.dk/art/250564/facebook-indgaar-milliardforlig-og-afvaerger-retssag-om-ansigtsgenkendelse

Geist, A. (2019). Her er et grotesk argument for mere overvågning – og det kommer fra justitsministeren. Retrieved 1 June 2020, from https://www.information.dk/indland/leder/2019/12/grotesk-argument-mere-overvaagning-kommer-justitsministeren

Geurts, P., Ernst, D., & Wehenkel, L. (2006). *Extremely randomized trees*.

Godkendt med et fingertryk. (2020). Retrieved 1 June 2020, from https://amtsavisen.dk/artikel/godkendt-med-et-fingertryk

Hill, K. (2020). The Secretive Company That Might End Privacy as We Know It. Retrieved 29 May 2020, from https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

How It Works: Xbox Kinect. (2020). Retrieved 28 May 2020, from https://www.jameco.com/Jameco/workshop/howitworks/xboxkinect.html

Ioannis A.Kakadiaris, George Toderici, Georgios Evangelopoulos, Georgios Passalis, Dat Chu, Xi Zhao, Shishir K. Shah, Theoharis Theoharis. 3D-2D face recognition with pose and illumination normalization, 2015 https://www.sciencedirect.com/science/article/pii/S1077314216300480

Jensen, A. (2016). Politiets nye øjne tjekker alle nummerplader. Retrieved 1 June 2020, from https://fdm.dk/nyheder/2017-10-politiets-nye-ojne-tjekker-alle-nummerplader

Jørgensen, N. 2019: Fremlæggelse d. 26.8.2019. Præsentation af Teknologiske systemer og artefakter. "Teknologiske systemer og artefakter I", Humanistisk-Teknologisk Bacheloruddannelse, Roskilde Universitet.

Kobie, N. (2019). The complicated truth about China's social credit system. Retrieved 1 June 2020, from https://www.wired.co.uk/article/china-social-credit-system-explained

Mikhalchuk, O. (2020). Using AI and biometrics to enhance exam proctoring. Retrieved 1 June 2020, from https://www.biometricupdate.com/202001/using-ai-and-biometrics-to-enhance-exam-proctoring

Moltke, H. (2020). ANALYSE Derfor vil EU bremse ansigtsgenkendelse. Retrieved 1 June 2020, from https://www.dr.dk/nyheder/penge/analyse-derfor-vil-eu-bremse-ansigtsgenkendelse

Morrison, S. (2020). Just because you're working from home doesn't mean your boss isn't watching you. Retrieved 1 June 2020, from https://www.vox.com/recode/2020/4/2/21195584/coronavirus-remote-work-from-home-employee-monitoring

Nets tester betaling med ansigtet. (2019). Retrieved 1 June 2020, from https://www.nets.eu/dk-da/nyheder/Pages/Nets-tester-betaling-med-ansigtet.aspx

One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority. (2020). Retrieved 1 June 2020, from https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

P. Jonathon Phillips, W. Todd Scruggs, Alice J. O'Toole, Patrick J. Flynn, Kevin W. Bowyer, Cathy L. Schott, Matthew Sharpe. FRVT 2006 AND ICE 2006 Large-Scale Results, 2007 https://web.archive.org/web/20070706093140/http://www.frvt.org/FRVT2006/docs/FRVT2006andICE2006LargeScaleReport.pdf

Patrick Grother, Mei Ngan, Kayee Hanaoka. Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf

Rachid AHDID, Khaddouj TAIFI, Said SAFI and Bouzid MANAUT Department of Mathematics and Informatics, Sultan Moulay Slimane University, Beni Mellal, Morocco Departement of Physics, Sultan Moulay Slimane University, Beni Mellal. "Euclidean & Geodesic Distance between a Facial Feature Points in Two-Dimensional Face Recognition System", ACIT, Morocco, 2016 https://acit2k.org/ACIT/images/stories/year2014/month1/proceeding/37.pdf

Rogers, E. (1983). *Diffusion of Innovations* (3rd ed.). New York.

Savov, V. (2017). iPhone X announced with edge-to-edge screen, Face ID, and no home button. Retrieved 2 June 2020, from https://www.theverge.com/2017/9/12/16288806/apple-iphone-x-price-release-date-features-announced

Slavkovic, M., & Jevtic, D. (2012). Face recognition using eigenface approach. *Serbian Journal Of Electrical Engineering*, *9*(1), 121-130. doi: 10.2298/sjee1201121s

Thomas David Heseltine, 2005 Face Recognition: Two-Dimensional and Three-Dimensional Techniques, The University of York, Department of Computer Science https://www-users.cs.york.ac.uk/~nep/research/3Dface/tomh/PhD-Heseltine.pdf

Traoré, I., Nakkabi, Y., Saad, S., Sayed, B., Ardigo, J., & Quinan, P. (2017). *Ensuring Online Exam Integrity Through Continuous Biometric Authentication*. Springer International Publishing. Retrieved from https://www.uvic.ca/engineering/ece/isot/assets/docs/Ensuring%20Online%20Exam%20Integrity%20Through%20Continuous%20Biometric%20Authentication-chapter.pdf

WEINMANN, M. (2018). *RECONSTRUCTION AND ANALYSIS OF 3D SCENES*. [Place of publication not identified]: SPRINGER INTERNATIONAL PU.

Wen Yi Zhao, Rama Chellappa - Imagebased Face Recognition: Issues and Methods https://face-rec.org/interesting-papers/General/Chapter_figure.pdf

Wong, J. (2019). Google reportedly targeted people with 'dark skin' to improve facial recognition. Retrieved 27 May 2020, from https://www.theguardian.com/technology/2019/oct/03/google-data-harvesting-facial-recognition-people-of-color

Yu, L., & Li, K. (2017). Application of Face Recognition Technology in the Exam Identity Authentication System. Retrieved 1 June 2020, from https://pdfs.semanticscholar.org/0d61/997e282eab329be793bacf1140e3e13613e2.pdf

Zhao, W., & Chellappa, R. *Image-based Face Recognition: Issues and Methods*. Retrieved from https://face-rec.org/interesting-papers/General/Chapter_figure.pdf

Zhou, S. & Xiao, S. 2018: "3D face recognition: a survey", Human-centric Computing and Information Sciences, 2018, vol.8(1), pp.1-27.

Zuboff S., The Age of Surveillance Capitalism - The Fight for the Future at the New Frontier of Power s. 495