Hvordan fungerer ansiktsgjenkjenning?

Ansiktsgjenkjenningsteknologi, heretter omtalt som FRT (Facial recognition technology), er et underfelt i et større felt av mønstergjenkjenningsteknologi. Mønstergjenkjenningsteknologi bruker statistiske metoder for å hente fram mønstre fra data for så å sammenligne disse mønstrene med andre mønstre som er lagret i en database. Et mønstergjenkjenningssystem oppfatter ikke et ansikt som et menneske ville ha oppfattet det, men den plukker opp et sett av mønstre på «pikselnivå». Da er det viktig for systemet å klare å lokalisere og oppdage et ansikt slik at bare dataene fra ansiktet blir analysert, og ikke bakgrunnen. Mønstrene som plukkes ut kalles en ansiktsmal, og det er denne malen som sammenlignes med andre maler fra databasen. En ansiktsmal skiller seg ut fra et fotografi fordi den bare inneholder data som er nødvendig for å analysere et ansikt.

Noen ansiktsgjenkjenningssystemer er designet for å beregne sannsynlighetspoeng mellom en ukjent person og en spesifikk ansiktsmal i en database, i stedet for å bare identifisere en ukjent person. Disse systemene vil komme med flere ulike mulige matcher og rangerer de ut ifra sannsynlighet, i stedet for å bare komme med én match. FRTs varierer i deres evne til å identifisere et menneske under krevende forhold, som f.eks. dårlig lys, lav oppløsning eller dårlige vinkler.

Når det kommer til feil med FRT er det to begreper man må forstå; falsk negativ og falsk positiv:

* En «falsk negativ» er når ansiktsgjenkjenningalgoritmen mislykkes i å finne en match av en persons ansikt til et bilde som er i databasen. Med andre ord vil ansiktsgjenkjenning algoritmen returnere null resultat.
* En «falsk positiv» er når ansiktsgjenkjenning algoritmen finner en match av en persons ansikt til et bilde som er i databasen, men matchen er feil.

Ansiktsgjenkjenningalgoritmer

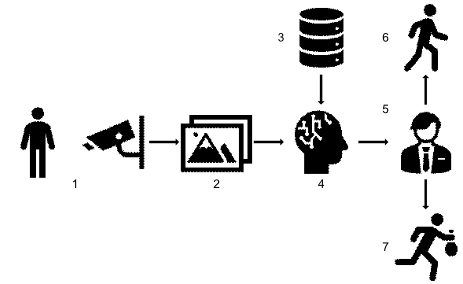
Det er fire steg i en ansiktsgjenkjenningsprosess. De er å finne ansiktet, normalisering, ansiktstrekkutdrag og det siste steget er ansiktsgjenkjennelse.

1. Ansiktsgjenkjenning. For et menneske vil det være veldig lett å gjenkjenne et ansikt i et bilde, men det er ikke fullt så enkelt for en datamaskin. Den må bestemme seg for hvilke piksler som er en del av et ansikt og hvilke piksler som er en del av bakgrunnen. På et passfotografi er bakgrunnen svart eller hvit, så da blir det lett for datamaskinen å bestemme seg, men når datamaskinen skal finne et ansikt på et vanlig bilde/fotografi blir det mye mer komplekst. Vanligvis leter datamaskinen etter typiske ansiktstrekk, som f.eks. øynene.
2. Normalisering. Etter at datamaskinen har funnet ansiktet i et bilde, må bildet bli standardisert i form av størrelse, belysning, etc. relativt til galleriet av bilder i databasen. For å normalisere en ansiktsmal er det viktig at ansiktstrekkene lokaliseres nøyaktig. Ved hjelp av ansiktstrekkene kan algoritmen reorientere bildet litt, slik at det ligner mest mulig på de andre malene i databasen.
3. Ansiktstrekkutdrag. Etter at ansiktsmalen har blitt normalisert vil trekkene til ansiktet bli fremhevet/tatt ut. Det vil da bli laget en matematisk representasjon av trekkene som kalles for en biometrisk mal. Det varierer i hvordan ulike ansiktsgjenkjenningsalgoritmer oversetter ansiktsmalen til en matematisk presentasjon, men det viktigste for de er at det lagres maksimalt med informasjon i de biometriske malene som blir laget.
4. Ansiktsgjenkjenning. Til slutt vil algoritmen sammenligne den biometriske malen sammen med de andre i databasen for å finne en eller flere mulige matcher.

Hva kan man bruke FRT til?

* Verifisering av identitet
  + Verifisering av identitet er den enkleste oppgaven for FRT. Bildet av en person som er ansatt i en bedrift er lagret i en database, slik at systemet bare trenger å sammenligne ansiktsmalen med bilder av den personen den hevder å være. Dette representerer et «one-to-one»-problem. Det kan man gjøre med adgangskort for å vise hvilken identitet man skal sjekke. Da er det to mulige utfall; enten så blir identiteten bekreftet eller så blir den ikke bekreftet. Det er to mulige feil systemet kan gjøre; «falsk avvis» og «falsk aksept». Når systemet avviser en person som faktisk er den personen som den hevder, så er det en «falsk avvis». Hvis systemet aksepterer en person som ikke er den personen som den hevder, så er det en «falsk aksept»
* Identifisering av identitet
  + Identifisering av identitet er mer kompleks enn verifisering av identitet. FRT må sammenligne ansiktsmalen med alle bildene i databasen. Dette representerer et «one-to-many»-problem. Videre trenger vi å skille mellom lukket-sett identifiseringsproblemer og åpent-sett identifiseringsproblemer. I et lukket-sett identifiseringsproblem så vet vi at identiteten til personen er i databasen, dvs. at vi vet at vi kan identifisere personen. I et åpent-sett identifiseringsproblem så vet vi ikke om identiteten til personen er i databasen, dvs. at vi ikke vet om personen kan bli identifisert med den dataen vi allerede har. Hvis det ikke er en match i et lukket-sett identifiseringsproblem, vet vi at systemet har gjort en feil, men hvis vi ikke får en match i et åpent-sett identifiseringsproblem vet ikke om systemet har gjort en feil eller at bildet av identiteten som skal sjekkes er i databasen. Der FRT brukes i dag pleier det å være åpent-sett identifiseringsproblemer i stedet for lukket-sett.

Figur 1 viser en typisk måte FRT kan brukes for å identifisere en tyv som er plukket opp på et overvåkningskamera.



Figur

1. Et kamera plukker opp et ansikt
2. Dataene fra ansiktet plukkes ut og malen lagres og sendes til algoritmen som skal analysere dataene
3. En database som inneholder andre ansiktsmaler
4. Algoritmen analyserer ansiktsmalene og sender dataene til et menneske
5. Et menneske verifiserer matchen
6. Algoritmen gjorde en feil (en «falsk positiv»)
7. Algoritmen hadde rett og tyven ble funnet.