

TDDC03 Projects, Spring 2005

Ansiktsbiometri

- project 17

Anders Ek, 800109
Olov Hagner, 791122

Supervisor: Viiveke Fåk

Ansiktsbiometri

Anders Ek, Olov Hagner
Linköpings universitet
andek346@student.liu.se, oloha468@student.liu.se

Sammanfattning

Den här rapporten syftar till att ge en övergripande bild av hur ansiktsgenkänningssystem fungerar och används. Dessutom hur de relaterar till de etiska aspekter som finns kring ämnet. Rapporten är skriven av universitetsstuderande för andra universitetsstuderande. Undersökningen baseras på en litteraturstudie av olika rapporter om ämnet. Anledningen till detta är att då ämnesområdet är i ständig utveckling anser vi det vara viktigt att få aktuell information.

Biometri handlar om personliga egenskaper som kan användas för igenkänning av individer. Detta kan ske genom att analysera fysiska attribut eller handlingar. Exempel på biometriska igenkänningsmetoder är fingeravtryck, signatur och ansiktsgenkänning.

Inom ansiktsgenkänning finns två huvudgrenar, igenkänning från stillbild och igenkänning från video. Automatisk igenkänning från stillbild går i tre steg: ansiktsdetektering, extrahering och igenkänning. Igenkänningsfasen delas mellan att arbeta med hela ansiktet, holistiskt, eller att fokusera på ansiktsdrag. När det handlar om igenkänning från video delas de olika faserna upp i områdena ansiktssegmentering, poseberäkning, ansiktsföljning och ansiktsmodellering. Både igenkänning från stillbild och video lider dock av svårigheter att hantera olika poser och belysningar, vilka är problem som ännu inte lösts tillfredställande.

Det finns ett flertal användningsområden för ansiktsgenkänning. Det kan bland annat användas för verifikation av identitet som till exempel vid bankomater eller inpassering till säkerhetskänsliga områden. Men det kan även användas för identifikation av individer, både vid offentliga och privata platser. Det finns exempel på identifikationssystem som använts på flygplatser i syfte att identifiera kända terrorister.

När det handlar om större system kommer också den etiska aspekten att spela in. Frågan om ansikten kan betraktas som integritetskänsliga är inte enkel att svara på. Aspekter med offentlig övervakning som använder ansiktsgenkänning har dock vissa inneboende etiska problem, vilket gör att det i dagsläget är svårt se som realistiskt att införa i stor skala.

1. Introduktion

1.1. Bakgrund

I dagsläget är det numera vanligt att använda såväl biometriska som minnesbaserade system för identifiering och verifiering av identitet. Diskussionen pågår kring hur biometriska egenskaper kan användas för detta och huruvida det är möjligt med tanke på integritet, religiösa och kulturella motsättningar samt rent tekniska förutsättningar. Inom biometrin har ansiktsgenkänning lanserats som ett möjligt alternativ i bland annat pass för att öka säkerheten. Det finns en mängd andra användningsområden som kan anses vara lämpade att använda sig av den här metoden. Ansiktsgenkänning är en metod som ännu inte används i någon större omfattning och fortfarande utvecklas.

1.2. Syfte

Vi planerar att undersöka ansiktsgenkänningssystem utifrån funktion, uppbyggnad, etik och användningsområden.

1.3. Målgrupp

Vår målgrupp är universitetsstuderande med teknisk inriktning, dock inte experter på säkerhetsfrågor. Vi kommer därför att försöka anpassa rapporten utifrån detta.

1.4. Frågeställning

Vi vill veta hur ett system för biometrisk ansiktsgenkänning fungerar, vi vill också titta på vilka fördelar och nackdelar sådana system kan ha. Med speciell fokus på etiska aspekter, då främst hur individens personliga integritet påverkas.

1.5. Metod

För att nå fram till önskvärda resultat har vi beslutat oss att använda litteraturstudier som metod i projektet. Vi kommer att fokusera på forskningsrapporter i den mån de finns tillgängliga och följa upp med tryckt litteratur. Anledningen till att vi till största del tänker använda oss

av forskningsrapporter är att det är ett område som utvecklas snabbt. Därför anser vi att så färsk information som möjligt är att föredra. Eftersom vi enbart använder oss av andras material kan man se rapporten som en sammanställning av andras resultat.

1.6. Metodkritik

När man förlitar sig på andras verk kan det ibland vara svårt att veta hur pass oberoende författarna är i sin bedömning. De som säljer eller använder en teknik vill nog sällan berätta om systemets nackdelar. Då en del källmaterial baseras på artiklar är det också viktigt att försöka utröna vilken ståndpunkt författaren har i frågan från början.

2. Biometrisk igenkänning

Vid igenkänning av människors identitet brukar man dela in metoderna i tre kategorier:

- Något man har, till exempel ett passerkort
- Något man kan, till exempel ett lösenord
- Något man är, till exempel fingeravtryck

Biometrisk igenkänning utgörs av den tredje kategorin. Även fysiska handlingar som till exempel gångstil och signatur räknas till den. Då biometrisk system ger positiva och negativa svar baserat på analys av mätdata finns det alltid risk att användare kan bli felaktigt nekade eller felaktigt godkända. Detta kallas falsk negativ respektive falsk positiv. Har man ett system där det är mycket viktigt att ingen kommer in otillbörligt försöker man givetvis se till att mätdata ska stämma bra överens med den mall man jämför med. Beroende på hur mycket variationer man tillåter får man alltid fler falska negativa vid låg tillåten variation och tvärtom fler falska positiva vid hög variation. Detta medför att det alltid finns en balansakt mellan dessa två faktorer.

2.1. Verifikation

När man vill bekräfta att en person är den som hon utger sig för att vara kallas det för verifikation. En person lämnar då något biometriskt kännetecken samt sin identitet till ett system som sedan matchar det mot motsvarande kännetecken som finns sparad i systemet för den identiteten. Systemet väljer sedan att godkänna verifikationen eller underkänna den. Blir en person felaktigt nekad kallas det för en falsk negativ och blir en person felaktigt godkänd kallas det för en falsk positiv. Beroende på användningsområde är det viktigt att välja den metod som passar bäst för ändamålet. För åtkomst av känslig data vill man förstås inte ha några falska positiva medan man för exempelvis inloggning på sin hemdator

antagligen inte vill bli nekad för ofta. Verifikation används också för positiv igenkänning vilket syftar till att flera personer inte ska kunna dela på en identitet.

2.2. Identifikation

Vid identifikation lämnas ett biometriskt kännetecken från en okänd person till systemet som sedan jämför det med kända personer i någon slags databas. Man genomför alltså en 1:N matchning. Identifikation används även vid negativ igenkänning vilket betyder att man fastställer huruvida personen är den hon säger att hon inte är. Det låter kanske krångligt men syftar till att motverka användningen av flera identiteter. Till skillnad från andra igenkänningsmetoder som till exempel passerkort kan negativ igenkänning enbart genomföras med biometrisk metoder.

2.3. Egenskaper

Personliga kännetecken som används i ett biometriskt igenkänningssystem bör ha vissa egenskaper för att systemet ska vara användbart. Dessutom finns det ett antal egenskaper hos systemet som är önskvärda. Dessa egenskaper gör det enklare att välja vilket system som ska användas för olika tillämpningar.

Personliga egenskaper:

- **Universalitet**
Alla människor ska ha kännetecknet
- **Unikhet**
Inga människor ska ha exakt likadana kännetecken.
- **Permanens**
Kännetecknet ska inte förändras för mycket över tid
- **Insamlingsbarhet**
Kännetecknet ska vara möjligt att mäta

Systemegenskaper:

- **Prestanda**
Relaterar till systemets hastighet och precision både i avseende på resurser och omgivning som påverkar.
- **Acceptans**
Ger ett mått på i vilken utsträckning människor är beredda att acceptera användandet av systemet.
- **Kringgående**
Ger en bild av hur svårt det är att lura systemet

2.4. Andra metoder

Det finns en mängd andra biometrisk metoder som kan användas för verifikation och identifikation och fler dyker upp hela tiden. Det finns ett flertal metoder som använder sig av ögats karakteristik, det finns metoder som baseras på rörelser, röst och även lukt. Nedan beskrivs några av de vanligaste metoderna för att ge en

bild av hur olika metoder det finns för biometrisk igenkänning.

2.4.1. Fingeravtryck

När man analyserar fingeravtryck för att utvinna en individuell profil undersöker man mönstret av åsar och dalar i fingeravtrycket. Man tittar på både hela fingeravtrycket samt mindre kännetecken som till exempel där åsar delar på sig, bildar öglor eller bågar. Ett fingeravtryck ger mycket information vilket gör att det är en mycket pålitlig metod för att identifiera människor. Den mall som sparas vid en fingeravtrycksscanning är inte själva fingeravtrycket som en bild utan en mängd data. Denna data är uppbyggd så att man inte kan rekonstruera fingeravtrycket utifrån den informationen. Detta gör man av säkerhetsskäl så att ingen ska kunna kopiera någons fingeravtryck utifrån den sparade mallen. Den klassiska metoden för att ta fingeravtryck är med hjälp av bläck men idag finns andra metoder som till exempel optiska sensorer, värmesensorer och ultraljudssensorer. Eftersom man använt sig av fingeravtryck för identifikation väldigt länge anses det vara en välutvecklad och säker metod. Det finns metoder för att lura fingeravtryckssensorer, vissa går ut på att man skapar en kopia i något material medan andra går ut på att man förstärker kvarliggande fingeravtryck på sensorerna. Det är inte särskilt svårt att utföra dessa attacker men de kräver ändå en viss ansträngning.

2.4.2. DNA

Alla människor förutom enäggstvillingar har olika DNA, det betyder att man i princip med total säkerhet kan identifiera vem som helst med hjälp av det. Men i dagsläget används det främst inom den kriminaltekniska verksamheten. Detta beror på flera faktorer, bland annat är det enkelt att stjäla någon annans DNA från till exempel ett hårstrå. DNA-analys är dessutom komplicerad och tidskrävande vilket gör det svårt att använda i realtidssystem. Dessutom kan informationen från en människas DNA användas till att utläsa personlig information som man kanske inte vill dela med sig av.

2.4.3. Signatur

En persons namnteckning har använts väldigt länge för att säkra att en person är den han utger sig för att vara. Till skillnad från de metoder vi beskrivit hittills är signaturen inte någon del av ens kropp utan en handling som utförs av kroppen. Därmed påverkas signaturen av såväl känslotillstånd som fysiskt tillstånd vilket medför att signaturen kan variera betydande, inte minst med tiden. Signaturer är enklare att kopiera än de flesta andra biometriska kännetecken, därför har man på senare tid utvecklat metoden genom att bland annat registrera trycket från pennan på underlaget för att få fler parametrar i jämförelsen.

3. Allmänt om ansiktsgenkänning

När vi människor känner igen någon vi möter sker detta ofta genom att titta på den personens ansikte. Det har visat sig att människor har mycket bra resurser för att analysera ansiktsdrag och komma ihåg hur andra ser ut. Tyvärr är det inte lika enkelt att automatisera den processen med hjälp av kameror och algoritmer. Det har visat sig att olika ljusförhållanden, ansiktsvinklar, frisyrändringar med mera skapar stora problem.

3.1. Användningsområden

Det finns många förslag på möjliga användningsområden för ansiktsgenkänning. Metoden kan användas till både identifikation och verifikation av identitet. Till skillnad från de flesta andra biometriska igenkänningsmetoderna kan ansiktsgenkänning utföras utan aktiv medverkan från deltagare och dessutom på avstånd. Användningsområden kan variera från vanlig verifikation vid till exempel inpassering till identifiering av individer i en folkmassa. Man kan dela upp tillämpningarna i tre huvudgrupper; kommersiella, statliga och kriminaltekniska. Ur ett historiskt perspektiv av igenkänningssystem kan man se att kommersiella tillämpningar ofta använt sig av system med lösenord eller PIN-koder, det vill säga någonting man kan. Statliga tillämpningar har i större utsträckning använt sig av någonting man har, till exempel polislegitimation. Inom det kriminaltekniska området har man tidigare använt sig av experter för att matcha biometriska kännetecken mot personer. Möjliga och redan existerande tillämpningar av ansiktsgenkänning redovisas nedan.

3.1.1. Kommersiella tillämpningar

Idag används bland annat ansiktsgenkänning vid vissa bankomater i USA istället för PIN-kod. Många kasinon använder sig av ansiktsgenkänning för övervakning och inpasseringskontroll.

3.1.2. Statliga tillämpningar

Många länder börjar i dagsläget införa biometrisk information i pass. Ett av förslagen på metod som ska användas är just ansiktsgenkänning. En mall av passinnehavaren sparas på ett chip och den mallen jämförs sedan med personen som använder passet.

I Illinois använder man ansiktsgenkänning för att försäkra sig om äktheten hos id-kort och förhindra stöld av identiteter. Kännetecken från ansiktet lagras i en mall som jämförs med bilden på id-kortet. Man använder systemet både för verifikation och positiv igenkänning, det vill säga att bara en person använder identiteten.

3.1.3. Kriminaltekniska tillämpningar

Inom det här fältet kan man tänka sig att använd ansiktsgenkänning vid bland annat identifiering av lik som matchas mot körkortsregistret.

Man har använt ansiktsgenkänning för att identifiera brottslingar vid idrottsevenemang. År 2001 använde sig arrangörerna av finalen i amerikansk fotboll, Super Bowl, av ansiktsgenkänning med hjälp av videokameror för att identifiera kända brottslingar som skulle se matchen. Tanken var att man skulle kunna bevaka dem extra för att säkerställa säkerheten på arenan. Man satte upp kameror vid ingångarna till arenan som filmade samtliga som gick in. Deras ansikten digitaliserades och jämfördes med bilder i ett av FBI:s register. Åskådarna blev inte informerade om att man skulle ta bilder av dem och matcha mot brottslingar. Av de 72 000 åskådare som gick på matchen fick man 19 träffar, varav de flesta var fiktjuvar eller sålda matchbiljetter på svarta börsen. Ingen av dessa personer blev arresterad för något brott under matchen.

Efter terrorattackerna mot World Trade Center föreslog man användning av kameror på flygplatser för att identifiera kända terrorister. Tester av ett sådant system genomfördes i början av 2002 på Boston Logan International Airport. Man ville undersöka om det var möjligt att identifiera terrorister som rörde sig på flygplatsen med hjälp av bilder från videokameror. Försöket genomfördes under tre månader med två olika system. Man använde foton från 40 flygplatsanställda som skulle kännas igen. Resultatet av testet var att systemet missade 38% av de möjliga positiva träffarna. Det fanns möjlighet att låta en mänsklig operatör ta beslut om möjliga träffar eller överlåta det helt åt systemet. Vid mänsklig inblandning fick man mindre än en procents falska positiva men vid automatisk drift fick man mer än 50% falska positiva. Man ansåg från flygplatsens sida att den manuella inblandningen som krävdes för ett bra resultat var alldeles för hög för att det skulle vara önskvärt att installera systemet. Ett liknande test genomfördes i maj samma år på Palm Beach International Airport i Florida men avbröts då man inte heller där fick de önskade resultaten.

3.2. För- och nackdelar

En stor fördel med biometri jämfört med andra igenkänningsmetoder är att du alltid har din biometriska information med dig. Det finns ingen möjlighet att tappa bort den eller glömma bort den. Ett problem med detta är dock att om någon lyckas stjäla din information har du ingen möjlighet att byta ut ditt kännetecken som till exempel med ett lösenord som blir avslöjat. Därför bör man se till att den mall som lagras inte kan användas till att återskapa det biometriska kännetecknet. När det gäller ansiktsgenkänning är det väldigt enkelt att stjäla det

biometriska kännetecknet genom att helt enkelt ta en bild av personen och använda för att lura systemet. Detta problem finns för de flesta biometrimetoder men är särskilt stort för ansiktsgenkänning eftersom det inte ens krävs att du är på samma plats som personen vars kännetecken du vill åt.

Relaterar vi ansiktsgenkänningssystem till de egenskaper för biometriska igenkänningssystem som beskrevs tidigare får vi följande resultat:

- **Universalitet**

Alla människor har ett ansikte, därmed behöver man inte använda något extra system för de som faller utanför ramen.

- **Unikhet**

Tester visar att det är svårt att urskilja helt unika kännetecken för ansikten. Även de bästa systemen kan inte med någon större säkerhet peka ut enskilda individer.

- **Permanens**

Med tiden förändras våra ansikten. När vi blir äldre förändras ansiktet på många sätt. Viktförändringar påverkar ansiktsformen i många avseenden. Öron och näsa ändrar också storlek i viss mån. Utseendet kan även förändras markant genom användande av glasögon, byte av frisy, skägg osv. För verifikationssyftet är detta inget större problem eftersom man inom till exempel företag kan välja att uppdatera informationen med jämna mellanrum. Däremot får man problem vid allmän identifikation av exempelvis brottslingar eftersom de knappast frivilligt infinner sig för att ta nya bilder.

- **Insamlingsbarhet**

Som vi tidigare nämnt är det enkelt att samla in data för ansiktsgenkänning. Det behövs ingen fysisk kontakt eller dyr utrustning.

- **Prestanda**

Det är svårt att ange huruvida ett biometriskt system har bra prestanda eller inte eftersom man måste göra bedömningen med hänsyn till användningsområdet. Ansiktsgenkänning har ganska höga värden för falska positiva vilket gör det mindre lämpligt för användning i känsliga sammanhang. Det finns tydliga bevis på att ansiktsgenkänning fungerar bättre i mindre populationer. Ökningar av storleken hos databasen ger tydliga försämringar i precision.

- **Acceptans**

Ansiktsgenkänning har hög acceptans, människor är vana vid att få sin bild tagen och det finns inga problem med kopplingar till kriminalitet som till exempel vid fingeravtryck.

- **Kringgående**

Det är i dagsläget ganska enkelt att lura ansiktsgenkänningssystem. Det finns exempel på lyckade attacker där man använt fotografier och bilder på dataskärmar för att lura systemet.

3.3. Prestanda

Den amerikanska regeringen utför regelbundet tester av ansiktsgenkännings teknik. Detta test kallas FRVT (Face Recognition Vendor Test) och är ett opartiskt test som görs av de ledande systemen för ansiktsgenkänning. Det senaste testet genomfördes 2002 med tio deltagare. En datamängd bestående av cirka 37000 bilder som deltagarna inte sett förut användes för testerna. Man testade identifikation och verifikation både inomhus och utomhus. Resultaten visade att systemen var mycket känsliga för normala ljusvariationer utomhus men inte inomhus. De bästa systemen hade en igenkänningsgrad utomhus på 50% när man tillät 1% falska positiva. När man undersökte hur storleken på databasen påverkade systemens prestanda såg man att identifikationsgraden minskade med två till tre procent för varje fördubbling av datamängden. Dessutom märkte man att prestandan minskade med drygt fem procent för varje år som gått sedan bilden som användes tagits.

3.3.1. Verifikation

Verifikationstestet genomfördes med flera bilder av samma individ tagna vid olika tillfällen. Man gjorde testerna med tre olika procentsatser av tillåtna falska positiva. För 0,1% falska positiva fick man en verifikationsgrad på 82%, det vill säga 82% av de legitima användarna blev korrekt verifierade. Vid 1% falska positiva blev verifikationsgraden 90% och vid 10% falska positiva blev den 96%.

3.3.2. Identifikation

I identifikationstestet gav man systemet en oidentifierad bild som sedan jämfördes med bilderna i databasen. Resultatet gavs i form av en sorterad lista på de n mest troliga kandidaterna. Om rätt person fanns med bland de n kandidaterna ansågs det vara en korrekt identifikation. Man gjorde tre tester med liststorlek på 1, 10 och 50 kandidater. För 1 kandidat gav det bästa systemet en identifikationsgrad på 73%, för 10 fick man 82% identifikationsgrad och för 50 kandidater fick man 87% som bäst.

4. Tekniker för automatiserad ansiktsgenkänning

4.1. Ansiktsgenkänning från stillbilder

Arbetet med att känna igen ett ansikte ifrån bild kan delas upp i tre grova steg. Det första är att detektera och grovt normalisera ansiktet i fråga, alltså att extrahera den nödvändiga informationen från bilden. I det andra steget ska ansiktsdragen extraheras och en mer noggrann normalisering göras, för att sedan i det tredje steget användas för att göra en identifiering eller verifikation.

De båda första stegen kan vara väldigt krävande för systemet om bilden har varierande bakgrund eller om det förekommer "skräp" (clutter) i bilden. Det sista steget är också krävande, mycket beroende på databasens storlek. Dessa tre steg är dock inte nödvändigtvis helt separerade. [Zhao et al. 2003]

4.2. Ansiktsdetektering

För att då automatiskt hitta den del av bilden som innehåller ansiktet finns olika alternativ. Vi tänker inte gå in så djupt på denna del av processen, utan nämner bara teknikerna.

Fram till mitten av nittioalet forskades det mest på metoder för att segmentera ett enda ansikte från antingen en enkel eller komplex bakgrund. Dessa gick ut på att använda en mall för ett helt ansikte, mall för vissa ansiktsdrag med mera. Senare forskning har fokuserat på att bygga system som kan lära sig hitta ansikten genom använda information från stora mängder bildprov. Mer färsk forskning går ut på använda 3D-teknologi och rotationer i djupet. [Zhao et al. 2003]

Gällande ansiktsdetektering är det som ofta med biometri ett problem mellan "false negative" och "true positive". Detta har dock visat sig bli betydligt bättre om systemet inte bara känner till hur ett ansikte ser ut, utan också vet hur det inte ser ut. Systemet tränas alltså att känna igen falska positiva och blir därmed betydligt bättre. [Zhao et al. 2003]

4.3. Extrahering av ansiktsdrag

Ansiktsdragen spelar en viktig roll för hur ansiktsgenkänningen sedan utförs. Många system behöver denna information, utöver det holistiska ansiktet arbetar, som komplement eller som nödvändig del. Exempelvis egenansikten behöver sådan information för att kunna normalisera ansiktet. Extraheringen kan delas upp i tre olika typer: generiska metoder som baseras på kanter, kurvor eller linjer, metoder som använder mallar (feature-template-based) för ansiktsdrag som exempelvis ögon, samt strukturell matchning som geometriska egenskaper. Där den senare är en nyare, mindre begränsad variant. Att använda mall-baserade metoder för att hitta exempelvis ögon har visat sig svårt då en person har glasögon eller blundar. [Zhao et al. 2003]

En metod är ASM (Active Shape Model) som använder en statistiskt framtagen modell, vilken numer har utvecklats till AAM (Active Appearance Model) samt till SOS (Shape Optimized Search). Metoden utgår alltså från en mängd kartlagda ansiktens värden för att utifrån dessa anpassa en modell som passar bilden i fråga, se exempel i figur 1. Där den modellen vrids för att passa ansiktet på så många punkter som möjligt. [Cristinacce & Cootes 2004]



Figur 1. Kartlagt träningsansikte

4.4. Ansiktsgenkänning

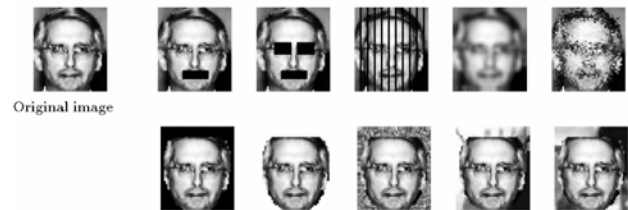
Det finns flera olika angreppssätt för att angripa problemet med att göra själva ansiktsgenkänningen. Dessa olika sätt kan delas upp i tre grupper: holistisk matchning, ansiktsdragsmatchning (feature-based matching) och en hybridvariant av de båda andra.

Ordet holism betyder att man anser var ting som helhet är viktigare än delar som utgör tinget. En holistisk matchningsmetod går alltså ut på att se på ansiktet som helhet för att utifrån detta göra matchningen. Ansiktsdragsmatchning kan då sägas vara nästan motsatsen till den holistiska, eftersom man här enbart ser på vissa av de delar som ingår i helheten. [Zhao et al. 2003]

4.4.1. Holistisk matchningsmetod

En faktor som lett utvecklingen inom holistisk matchning, är användningen av egenbilder eller egenansikten (egen översättning: eigenpictures respektive eigenfaces), vilka ingår i området PCA (Principal Component Analysis). Detta är en metod för att inte behöva arbeta med redundant information, vilket finns gott om i naturliga bilder. När det gäller begränsad mängd objekt som ansiktsbilder vilka är normaliserade utifrån skala, translation och rotation är redundansen till och med högre. Med egenbilder uttrycks alltså bildinformation i vektorer (x) som är linjärkombinationer av en ortogonal bas (Φ_i). Matematiskt uttryckt $\Phi_i : x = \sum_{i=1}^n a_i \Phi_i \approx \sum_{i=1}^m a_i \Phi_i$ (där $m < n$) där egenvärdesproblemet $C\Phi = \Phi\Lambda$ löses (C är kovariansmatrisen till x). Att uttrycka informationen på denna form gör att ansiktsgenkänningen blir betydligt mindre känslig för suddiga bilder, bilder där information saknas eller förändrad bakgrund. Vilket illustreras i figur 2. Att dessutom öka mängden träningsbilder genom att även använda spegelbilderna har visat ge positiva resultat. Det ska också sägas att tekniken med egenbilder ofta används för såväl ansiktsdetektering, det vill säga

steg ett av det automatiska ansiktsgenkänningssystemet. [Zhao et al. 2003]



Figur 2. Korrekt identifierade elektroniskt modifierade bilder.

Från egenbilderna kan också bilderna rekonstrueras med god kvalitet, se figur 3.



Figur 3. Rekonstruerade bilder från figur 2.

I ett system som använder egenbilder lagras bildinformationen alltså som vektorer i databasen. Dessa element har också ett viktvärde, vilket beräknas genom en projektion ur vektorerna, som då fungerar som identifierare. Vid identifiering söks det i databasen efter det element med närmast vikt, vilket då blir träffen. Senare har detta dock utvecklats och en metod som utvecklades av Moghaddam och Pentland använder en Bayesian analys mellan skillnader i bilder. Denna tar hänsyn till skillnader mellan bilder på samma individ (intrapersonal variations) och skillnader i identitet (extrapersonal variations). Denna använder sedan sannolikhetsfördelningar för att göra identifieringen. [Zhao et al. 2003]

Egenansikten är dock inte den enda modellen för att representera och identifiera ansikten inom forskningen som vunnit mark. Fischeransikten som är en LDA/FLD-baserad (Linear Discriminant Analysis/Fisher Linear Discriminant) metod kan beskrivas som att arbeta med MDF (Most Discriminating Features), till skillnad från egenansikten som arbetar med MEF (Most Expressive Features). Fischeransikten byggs av vektorer som fås genom att kombinera FLD med PCA projektioner. I tester har Fischeransikten visats mest effektiva, men inga tester har dock gjorts på stora mängder individer (inga över 500). [Zhao et al. 2003] [Liu & Wechsler 2000]

4.4.2. Matchning genom ansiktsdrag

Det finns många olika system som enbart ser på delar av ansiktet för att göra identifikationen. Ett av de mer välsedda och bättre systemen är EBGM (Elastic Bunch Graph Matching), vilket använder information hämtad i

en mängd specificerade punkter, vilka inkluderar ögon, näsa och mun. I dessa punkter extraheras Gabor jets, amplitudvektorer från ett bildfilter, vilka används för att bygga en ansiktsgraf. Algoritmen utför sedan identifikation genom att jämföra dessa Gabor jets i de specificerade punkterna i grafen. Det elastiska är att samtliga träningsbilders Gabor jets på en individ finns lagrade i samma graf, vilket ger ökad flexibilitet och förbättrat utförande. [Zhao et al. 2003] [Givens et al. 2004]

4.4.3. Hybridvarianter

Det finns också metoder som använder idéer från både den holistiska och ansiktsdragsmatchningen, vilka då kallas hybridvarianter. Bland dessa finns även PCA där man utöver egenansikten tänker sig egenmun, egenögon och så vidare. Även idéer om att härma ögats begränsningar och på så sätt kunna ta bort den redundanta informationen, har framkommit. Där man alltså skulle representera ansiktet i en 2D-array och bara fokusera på informationen i dessa punkter. Andra varianter där ansiktet delas upp i formparametrar och formlösa parametrar, och där identifiering utgår från ansiktsform och gråskalemodeller. De senaste idéerna rör 3D-rendering, där endast tre bilder från var individ behövs för att skapa en 3D-modell över individen. Denna roteras och ljussätts på olika sätt för att sedan träna identifieraren. [Zhao et al. 2003]

4.5. Ansiktsgenkänning från bildsekvenser

Att göra en ansiktsgenkänning från en bildsekvens (eller videosekvens) kan ses som en utveckling av dito från en stillbild. Med en videosekvens finns dock fördelarna med att ett ansikte i rörelse är enklare att känna igen. Men nackdelar med video är kvaliteten ofta är låg, det filmas utomhus och inomhus förändras ljuset då individen rör sig. Den del av bilden som innehåller ansiktet är ofta liten, ibland så liten 15 x 15 pixlar, där stillbilder ofta har 128 x 128 pixlar att arbeta på. De tekniker som är stora delar av ansiktsgenkänning från video är ansiktssegmentering (face segmentation), poseberäkning (pose estimation), ansiktsföljning (face tracking) och ansiktsmodellering (face modeling). [Zhao et al. 2003]

4.5.1. Ansiktssegmentering och poseberäkning

Tidiga varianter ansiktssegmentering använde enkla algoritmer som titta på förändring i pixlar mellan bilderna i sekvensen, för att segmentera ansikten. Sådana metoder fungerar dock dåligt när det finns flera objekt som rör sig i sekvensen. Mer moderna metoder använder rörelse och färginformation för att hitta kandidatbilder som kan innehålla ansikten. Dessa bilder analyseras sedan på samma sätt som stillbilder för att detektera

ansiktet. Givet en ansiktsregion i bilden kan viktiga ansiktsdrag lokaliseras. Dessa ansiktsdrag används sedan för att beräkna posen, vilken är nödvändig att känna till för att kunna syntetisera virtuell frontalbild. Det finns även metoder som klarar ansiktssegmentering och poseberäkning simultant utan att extrahera ansiktsdrag. [Zhao et al. 2003]

4.5.2. Ansikts- och ansiktsdragsföljning

När ett ansikte är lokaliserat, kan det och ansiktsdragen följas. Denna ansiktsföljning (face tracking) är kritisk för att kunna rekonstruera en ansiktsmodell, och ansiktsdragsföljningen viktigt för att kunna identifiera ansiktsuttrycket. Följningen handlar alltså om uppskatta rörelser, men är svårt då ansikten har delar som är för släta för att kunna uppskatta rörelsen korrekt. Följning och modellering kan ses som duala processer eftersom följningen är begränsad av den generiska 3D-modellen och individuella modeller blir bättre genom denna följning. [Zhao et al. 2003]

Ansiktsföljning kan delas upp i tre delar: huvudföljning, som handlar om att följa huvuden genom rotationer och translationer, ansiktsdragsföljning, vilket inkluderar rörelser vid tal, ansiktsuttryck och andra muskelrörelser, samt komplett följning, vilket är de båda andra delarna samtidigt. [Zhao et al. 2003]

En metod för att följa huvuden använder sig av punkter på huvudet med höga hessianska värden (Hessian values). Flera sådana punkter följs sedan och 3D-rörelseparametrarna kan på så sätt beräknas. Det finns även liknande metoder som använder 3D-modeller direkt, samt andra som beräknar 3D-rörelser och deformationer direkt från bildstyrkan (image intensity). Metoder för att följa ansiktsdrag använder ofta gränsen mellan sökt ansiktsdrag och resten av ansiktet för att hitta detta ansiktsdrag. Det kan handla om mungipor, där läpparna slutar och så vidare. Det finns också system som använder informationen om olika ansiktsdrag. Metoden går ut på att en tom ansiktsmall och sedan utanpå den kunna variera mallen för munnen mellan att le och vara ledsen eller ett öppet öga med ett blinkande. [Zhao et al. 2003]

4.5.3. Ansiktsmodellering

Ansiktsmodellering inkluderar 3D-modellering av både form och struktur. Beroende på ljussättning kan strukturmodellering bli komplicerad, vilket tas upp mer senare i rapporten. För att beräkna 3D-former används ofta SfM (Structure from Motion) som uppskattar 3D-djupet utifrån vissa, för bilden, intressanta punkter. Andra metoder använder ofta deformerbare eller förändringsbara 3D-modeller som matchas mot bildsekvenserna. [Zhao et al. 2003]

4.5.4. En variant av ansiktsgenkänning från video

Medan de flesta ansiktsgenkänningsalgoritmer tar stillbilder som indata, finns det vissa som använder videosekvenser. Eftersom det detekterade ansiktet kan röra sig i bildsekvensen, finns det osäkerhet i såväl följning som i igenkännandet. Istället för att arbeta med dessa båda osäkerheter var för sig utförde Zhao et. al simultan följning och igenkänning. Då det handlar om igenkänning från stillbild till video, används funktioner som tar hänsyn till kinetiken i videon för att på så sätt kunna bygga en provvideo ur databasen som jämförs med videon, för på så sätt kunna identifieras. [Zhao et al. 2003]

4.6. Belysning och posevariation

Ansiktsgenkänning i en okontrollerad miljö är fortfarande väldigt svårt och beror i stort på de två faktorerna belysning från olika vinklar, samt ansiktsvinkel eller pose. Detta trots att i princip alla system gör en ansats att hantera problemen. Det finns dock vissa idéer om hur dessa problem kan lösas, men de är svåra att implementera och gör systemen långsamma.

4.6.1. Belysningsproblemet

Belysningsproblemet är ett stort problem och skillnader i bilder på samma person med olika skuggspel och ljusa partier är så stora att de gör ansiktena mer olika än om de kommit från olika individer med samma ljussättning. [Zhao et al. 2003]



Figur 4. Skillnader i med olika ljussättning hos två individer (radvis).

Generellt är belysningsproblemet svårt och mycket forskning har gjorts på att komma tillrätta med det. Det finns olika ansatser som bland annat heuristiska försök, vilka ofta används i olika system. Dessa går ofta ut på att normalisera kontrast eller intensitet i bilden för att på så sätt minska ljusets inverkan. Det finns också heuristiska metoder som går ut på att ignorera några av de mest betydande särdragen för att minska känsligheten för ljus. Detta kräver dock att de mest betydande skillnaderna enbart är beroende på ljuset, vilket inte alltid är fallet. [Zhao et al. 2003]

Andra försök går ut på bildjämförelser av en individ för att komma runt problemet. Bilderna representeras på

olika sätt, för att använda de kombinerade styrkorna med var representationsmodell. Ingen av representationsmodellerna är på egen hand okänsliga för ljuset, men tillsammans blir de mer okänsliga. [Zhao et al. 2003]

Klassbaserade försök går ut på att exempelvis simulera en ljuskon på bilderna i databasen för att efterlikna försöksbilden. [Zhao et al. 2003]

I modellbaserade försök används en ansiktsmodell i 3D syntetisera den virtuella bilden från en given bild under önskade ljusförhållanden. Om 3D-modellen är okänd är detta dock svårt att göra noggrant. Modellen har dock den fördelen att skillnaden i 3D-former hos de flesta ansikten inte är dramatisk. [Zhao et al. 2003]

4.6.2. Poseproblemet

Då det förekommer stora variationer i poser försämrats prestandan hos systemen markant. Då variationer i poser och olika ljussättning förekommer blir det än mer svårt, men eftersom detta är verkligheten med exempelvis bevakningskameror är dessa viktiga problem att lösa. Med variationer i poser menas ofta rotationer ut ur planet, eftersom rotationer i planet generellt är ett betydligt enklare problem. Tidiga metoder gick ut på enbart fokusera på ansiktsdrag som inte förändras med posen, men då dessa hanterar större vinklar dåligt, eftersom de blir osynliga, är det inte en hållbar lösning. [Zhao et al. 2003]

Metoder som använder många olika bilder i olika vinklar är variant som delvis används. Enklare varianter av detta som använder mallbaserade metoder har dock sina begränsningar då det krävs väldigt många olika bilder och därmed stora databaser, de klarar inte av ljussättningsproblemet eller olika ansiktsuttryck och beräkningarna blir ytterst kostsamma då det handlar om iterativa metoder. En annan mer sofistikerad variant av detta skulle då för varje pose också beakta en mängd olika ljussättningar. Detta är principiellt en bra idé om det inte vore för de väldigt kostsamma beräkningarna, som gör att det inte fungerar i praktiken. [Zhao et al. 2003]

Hybridförsök, som tränar på många bilder men bara använder en, är den mest använda strategin hittills och har visat sig fungera bättre än övriga. Exempel på hybrider är till exempel utökningen av egenansikten. Detta går ut på att för varje individ skapa ett egenansikte för varje pose. En annan metod är en variant av EBGM (Elastic Bunch Graph Matching), där transformationen av Gabor jets studeras då ansiktet roteras, vilket har visats sig vara en av de bättre metoderna hittills. Även AAM (Active Appearance Model), som använder sig av enbart tre exempelbilder per person i rotationen 0°, 45° och 90°, har visat sig fungera godkänt. Det speciella med denna metod är att den använder sig av olika ansiktsdrag för

varje pose. AAM hävdas kunna klara rotationer på upp till 90°, det vill säga profilbilder, och ändå kunna identifiera subjektet. [Zhao et al. 2003]

Metoder som bara använder en bild har inte visat sig fungera bra i praktiken och har ej heller varit lika uppmärksammade i forskningen som de övriga metoderna. [Zhao et al. 2003]

5. Etiska aspekter

5.1. Personlig integritet

Collste avgränsar i sin rapport i SOU1997:39 begreppet personlig integritet och börjar tala om självkontroll. Förlorad kontroll över sin egen person eller över känsliga personliga uppgifter kan upplevas som kränkande. Det kan vara att vara kontrollerad av någon annan eller att man förlorat kontrollen över omfattningen på spridningen av känsliga uppgifter såsom medicinska uppgifter. Dessa integritetskänsliga uppgifter har ofta det gemensamt att det rör personliga, eller privata, förhållanden. [Collste 1997]

Collste går vidare och ställer frågan om det går att dra en gräns mellan integritetskänsliga uppgifter och de som inte är det. Han konstaterar att det är de uppgifter som är privata eller avvikande från normen som ofta betraktas som känsliga. Collste konstaterar att det inte finns något givet svar på denna fråga och att det ofta är subjektivt. [Collste 1997]

Den personliga integriteten kränks när det sker ett intrång i personens privatliv, eller när personen förlorar kontrollen över sin privata sfär. Kränkning av personen ses då som ett bredare begrepp än då den personliga integriteten kränks. Alla kränkningar är kränkningar av personen, men inte nödvändigtvis av den personliga integriteten. [Collste 1997]

Collste skriver att en rimlig avgränsning för integritetskänsliga uppgifter är sådana "uppgifter som de flesta individer i ett visst samhälle inte vill ska spridas om sig görs offentliga". Men som brasklapp tillägger han att enskilda individers upplevelser av att vara kränkta kan vara kränkningar om det finns rimlig grund för upplevelsen. [Collste 1997]

Collste väljer att definiera begreppet personlig integritet genom att definiera kränkningar av detsamma. Hans slutsats är alltså att personers integritet kränks då "det sker ett intrång i deras privata sfär och/eller då uppgifter om dem, som det finns rimliga skäl att beteckna som integritetskänsliga, sprids". Dessa uppgifter kan gälla personers egenskaper, uppfattningar eller handlingar". [Collste 1997]

5.1.1. En rättighet?

När vi nu har en aning om som innefattas i begreppet personlig integritet, kommer då frågan om detta är

rättighet i samhället? Collste beskriver rättighet som ett välgrundat anspråk, det vill säga skyldigheter för omgivningen. Alltså varje person har ett välgrundat anspråk till att omgivningen respekterar hans eller hennes personliga integritet. Detta betyder då tillämpat på register innehållande information om personer att medborgarna har ett berättigat anspråk att registerinnehavaren hanterar uppgifterna på ett sådant sätt den personliga integriteten respekteras. Skälen till denna rättighet är enligt Collste att personer bör respekteras, att inte skapa onödigt rädsla och frustration kring uppgiftssamlande och kränkning i samband med detta, att information kan användas för påtryckningar och maktutövande och att viss information kan ge upphov till trakasserier eller förtroendeförminskning. [Collste 1997]

Collste menar att dessa skäl väger tungt och starkt talar för den personliga integriteten som rättighet, men vidare säger han att finns tillfällen då denna rättighet måste ge vika då den ställs i konflikt en annan etisk rättighet. Ett sådant fall skulle vara då medicinska uppgifter behöver offentliggöras för att rädda livet på andra människor. Det rör sig alltså om en prima facie-rättighet, vilket är "en giltig och välgrundad rättighet som dock i en konkret handlingssituation kan sättas ur spel om den kommer i konflikt med någon annan rättighet som väger tyngre". [Collste 1997]

5.2. Är lagrad ansiktsinformation integritetskänslig?

De olika tekniker som finns använder olika metoder och olika värden för att känna igen ett ansikte. Vilket framkom vid användning av till exempel egenansikten en ansiktsrepresentation vilken kan återskapas till en ansiktsbild med god kvalitet. Andra metoder som EBGM använder informationen i vissa punkter, de så kallade Gabor jets. Från denna metod är det alltså svårt att återskapa ett ansikte.

Är då ett ansiktes biometrisk information integritetskänslig information? Frågan är inte helt enkel att svara på, men kan sägas ha med riskerna för missbruk att göra.

5.3. Risker med videoövervakning med ansiktsgenkänning

Då det handlar om ansiktsgenkänning i samband med publik videoövervakning finns det mycket åsikter om hur den personliga integriteten äventyras. Ägre menar att potentialen för missbruk är stor, detta speciellt då information från olika videoövervakningssystem kopplas samman för att på så sätt kunna ingå i en större struktur. På detta sätt skulle en individ identifieras och kunna spåras geografiskt från plats till plats. I fel skulle sådan information kunna användas för att utöva social kontroll,

då exempelvis användas för att stävja publika aktiviteter som syftar till att motarbeta maktsfärer, till exempel vid demonstrationer. [Agre 2001]

Han menar att det också finns en fara i att ansiktsgenkänning inte kräver mycket samarbete med subjektet som identifieras, bilder kan tas på långa avstånd med bra objektiv. [Agre 2001]

Bowyer menar dock att detta delvis kan komma till rätta med. I en analogi med telefonavlyssning bestämmer en åklagare huruvida subjektet ska utsättas för en dylik undersökning. Detsamma kan alltså komma att gälla om en individ ska bevakas eller ej, genom att finnas i bevakningsdatabasen eller inte. En sådan procedur kan alltså utformas för att integriteten, i alla fall i detta avseende, bevaras. [Bowyer 2003]

Då det handlar om ansiktsgenkänning utomhus är förhållanden, vilket tidigare sagts, långt ifrån optimala. Detta göra identifiering svårare och speciellt den ökade risken med falska positiva orsakar problem. I ett scenario där personer rör sig i misstänkta områden, exempelvis platser med mycket drogförsäljning, och individer på denna plats loggas i ett ansiktsgenkänningssystem, kan oskyldiga försättas i obekväma situationer. Då databasen växer ökar också risken för detta. [Agre 2001]

Detta till trots är falska positiva även förekommande hos människor. Det finns många exempel då en oskyldig blivit anmäld av en iakttagare som misstagit denne för en efterlyst brottsling. [Bowyer 2003]

Att allmänheten är dåligt införstådd med hur sådana system fungerar och vad de kan användas till gör situationen också att de kan missledas och därmed äventyra det demokratiska systemet, det vill säga att det inte är folket som styr. [Agre 2001]

Det är också svårt att effektivt meddela till allmänheten att en plats är övervakad och ännu svårare att inskaffa korrekt samtycke. [Agre 2001]

6. Resultat

Potentialen för ansiktsgenkänning i olika tillämpningar är stor. Det finns en del användningsområden där det redan existerar fungerande lösningar och ett antal som i framtiden mycket väl kan tänkas komma på fråga. Baserat på de tester som gjorts är det främst inom identifikation som ansiktsgenkänning har sin största marknad. Med tanke på den relativt höga andelen falska positiva som erhålls då man använder sig av metoden för verifikation är det ett område som behöver utvecklas mer. Dock måste man alltid relatera metoden till den tänkta användningen. Alla biometriska metoder har sina fördelar och nackdelar som gör att de passar bättre eller sämre för olika tillämpningar. Ansiktsgenkänning är dock ett expansivt område som

inte har nått sin fulla potential vilket sannolikt betyder att vi kommer se nya tekniker som ger ännu bättre resultat i framtiden. Detta gör att diskussionerna kring den personliga integriteten kan komma att förändras i takt med att tekniken förändras. För den individuella integriteten kan det vara viktigt att inte kunna återskapa ansikten ur en databas med identifierbara subjekt.

7. Diskussion

Metoderna bakom ansiktsgenkänning bygger på flera olika angreppssätt. Vissa fokuserar på ansiktet som en helhet medan andra bygger på enstaka ansiktsdrag. Utveckling sker även inom tredimensionella analysmetoder vilket kräver mer än en bild. Detta är fallet då man till exempel använder sig av videoövervakning. I USA speciellt efter attentatet mot WTC startades många hetsiga diskussioner som gick ut på att införa videoövervakning med ansiktsgenkänning på många offentliga platser. Denna information skulle sedan analyseras och jämföras mot exempelvis kända medlemmar av al Qaida. Ett sådant scenario lider många brister, men det var en fullt uppblåst diskussion. Med dagens teknik skulle ett sådant system kräva enorma resurser och ändå inte räcka till, detta med tanke på populationens storlek. System som utvecklas har ännu inte nått tillräckligt låga falska positiva för att kunna hantera sådana applikationer och idag är det mer användbart som verifikationssystem. Trots detta är medger dock inte system samma säkerhet som vissa alternativ.

Diskussionen kräver att man definierar vad personlig integritet är samt till vilken utsträckning samhället ska skydda den. Collste säger att personlig integritet kan innefatta en individs egenskaper speciellt om det är något som uppfattas som avvikande från normen. Historiskt sett har man länge använt personliga särdrag för att terrorisera människor tillhörande olika folkgrupper. Nazismens ansiktsmätning och förföljning av judar ger ett skräckscenario på hur sådana här uppgifter skulle kunna missbrukas. Man får dock tänka på att vissa ansiktsdrag inte nödvändigtvis är att betrakta som integritetskänsliga. Det gäller att skilja på ett fotografi av en människa och de mallar som används för ansiktsgenkänning. Det finns stora skillnader mellan olika länder avseende hur man skyddar integritet. I vissa länder är det helt tillåtet att övervaka offentliga platser medan man i andra länder måste söka tillstånd och informera de som vistas på platsen.

8. Referenser

[] W. Zhao, R. Chellappa, P.J. Phillips och A. Rosenfeld, "Face Recognition: A Literature Survey", ACM Computing Surveys, ACM Press, 2003-12, pp. 400-454

[] D. Cristinacce och T.F. Cootes, "A Comparison of Shape Constrained Facial Feature Detectors", IEEE, 2004-05, pp. 1-6

[] G. Givens, J.R. Beveridge, B.A. Draper, P. Grother och P.J. Phillips, "How Features of the Human Face Affect Recognition: a Statistical Comparison of Three Face Recognition Algorithms", IEEE, 2004-04-07, pp. 1-4

[] C. Liu och H. Wechsler, "Learning the Face Space – Representation and Recognition", ICPR'2000, IEEE, 2000-09, pp. 1-5

[] Scott Berinato, "Face Recognition Hype Is Over", CIO Magazine Nov 1, <http://www.cio.com/archive/110103/tl_biometrics.html>

[] P.E. Agre, "Your Face Is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places", *Whole Earth*, Winter 2001, pp. 74-77

[] G. Collste, "Pulutredningen – Bilaga 4 personlig integritet", SOU 1997:39, pp. 790-801 <<http://www.regeringen.se/content/1/c4/13/35/1fea52d6.pdf>>

[] K.W. Bowyer, "Face Recognition Technology: Security versus Privacy", IEEE Technology and Society Magazine, IEEE, Spring 2004, pp. 1-18

[] P.J. Phillips, P. Grother, R.J. Micheals, D.M. Blackburn, E Tabassi och J.M. Bone "FRVT 2002: Evaluation Report", Mars 2003 <http://www.frvt.org/DLs/FRVT_2002_Evaluation_Report.pdf>

[] Anil K. Jain, Arun Ross, Salil Prabhakar, "An Introduction to Biometric Recognition", IEEE Biometrics, Vol 14, No 1, Januari 2004 <http://biometrics.cse.msu.edu/JainRossPrabhakarCSVt_v15.pdf>

[] "Facial Recognition – Part 1", Biometric Technology Today, Volume 11, October 2003 pp. 10-11 (714) 761-1784.