

Ansiktsbiometri i kriminalarbete

Ove Callheim

Email: oveca589@student.liu.se

Supervisor: Viiveke Fåk, viiveke@isy.liu.se

Project Report for Information Security Course

Linköpings universitetet, Sweden

Sammanfattning

Att använda ansiktsbiometri inom kriminalarbete verkar vara ett uppenbart användningsområde för dagens tekniskt långt utvecklade apparater inom avbildning och databehandling. Den här rapporten syftar till att ge en bakgrund till hur ansiktsbiometri används idag och hur det skulle kunna användas inom polisarbetet, samt belysa vilka problem och hinder det skulle medföra.

Att arbeta med biometri på ansiktshalter innebär att från bilder med varierande kvalitet utmäta jämförbara mått och unika ansiktsdrag med hjälp av olika algoritmer som appliceras på mätpunkterna. Det finns att antal sådana algoritmer som är effektiva för olika typer av metoder. Kvaliteten på kameror och maskiner som sköter lagring och bearbetning av mätdata utgör idag inget prestandaproblem, så tekniskt finns det inget hinder för att automatisera användandet av ansiktsbiometri inom kriminalarbete.

Den vanligaste användningen sker idag med nästan enbart manuella metoder och för att upprätthålla bevis säkerheten vid rättegångar krävs det ett mycket försiktigt bedömande av de sakkunniga. De som arbetar som sakkunniga välkomnar metoder som kan ge ett mer automatiserat sätt att bearbeta bildmaterial, men det får naturligtvis inte äventyra förtroendet för dem och för rättssäkerheten. Som det ser ut idag, finns både tekniken, kunskapen och viljan, men för ett trettio år sedan skapades regler och förordningar som gäller än idag. Dessa hindrar ett funktionellt och effektivt insamlande, lagrande och användande av ansiktsbiometriska data.

I kombination med passregister och misstankeregister skulle denna teknik bli ett mycket kraftfullt vapen i kampen mot brottsligheten, men för att det ska bli möjligt att införa, krävs förändringar i lagar och förordningar som starkt påverkar skyddandet av den personliga integriteten för medborgarna.

1. Introduktion

Ansiktsbiometri är något som vi alla använder oss av varje dag då vi ser ett ansikte och förstår att vi träffat på detta ansikte tidigare. Att känna igen någon kommer oftast av att vi känner igen specifika drag i ansiktet och har en uppfattning om hur någon ser ut sedan tidigare. Med andra ord har vi lagrat biometrisk information från ansiktet vi känner igen.

1.1 Bakgrund

Med den utveckling som tekniken för bildskapande och bildbehandling har haft och fortfarande har, är det idag möjligt att använda biometriska system för identifiering och verifiering av identitet. Det är numera mest användandet som diskuteras samt vilka restriktioner som ska gälla med avseende på integritet och motsättningar av kulturell och religiös art.

1.2 Syfte

Syftet med denna rapport är att belysa vilka möjligheter som tekniken för ansiktsbiometri ger oss och vilka problem som användandet medför i brottsbekämpande kriminalarbete.

1.3 Målgrupp

Den målgrupp som rapporten vänder sig till är universitetsstuderande med teknisk inriktning samt intresserade inom polisväsendet.

1.4 Frågeställning

Går det att på ett systematiskt och automatiserat sätt använda ansiktsbiometri i syfte till att binda en gärningsman till ett brott och vilken vikt kan sådan bevisning erkännas vid en rättegång? Kan ansiktsbiometri användas till att i förundersökningsarbetet minska antalet misstänkta ur en grupp med hjälp av jämförelse med till exempel passregistret? Hur används ansiktsbiometri i dagsläget och vilka hinder finns för en utveckling av tekniken så

att den används korrekt, med avseende på etiska och moraliska frågor, i synnerhet den personliga integriteten?

Dessa frågor ska jag diskutera i denna rapport och även om det inte finns exakta svar på alla frågor av den här typen, så ska jag försöka ge en bild om vidden av problematiken.

1.5 Metod

Jag har studerat litteratur i ämnet, sökt fakta på internet och genomfört intervjuer med anställda vid Statens Kriminaltekniska Laboratorium (SKL). Vid dessa har jag fått ta del av metoderna de använder i dagsläget. Jag har även tagit del av en studie gjord av en utredare vid Polismyndigheten i Hallands län som handlar om möjligheten att lagra och använda biometriska data kopplat till idag befintliga register. Hon har även varit behjälplig med att svara på polis-specifika frågor.

1.6 Metodkritik

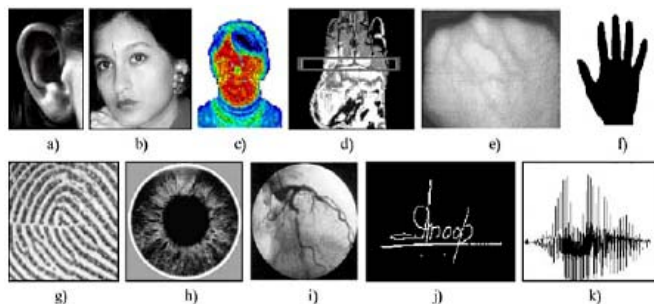
När en sådan här rapport skrivs är det viktigt med källkritik, eftersom jag förlitar mig på andras verk. Författarna av dessa kan vara påverkade av många andra faktorer, som vad de arbetar med och åsikter, exempelvis vad de anser i integritetsfrågor och dylikt.

2. Kortfattad och allmän beskrivning av biometri

Det finns flera metoder att använda vid biometrisk igenkänning. Biometri kan definieras som användningen av jämförbara beteendemässiga och fysiologiska egenskaper för att fastställa en persons identitet. En vanlig biometrisk metod som blivit den viktigaste inom kriminalarbete är studier av DNA, som har ett mycket högt bevisvärde i brottsutredningar. Det finns även flera andra biometriska metoder som enligt D. Maltoni med flera [1], används och ett urval visas i Figur 1.

Figur 1. Exempel på biometrisk igenkänning

- a) öra
- b) ansikte
- c) ansiktstermogram
- d) handtermogram
- e) handven
- f) handgeometri
- g) fingeravtryck
- h) iris
- i) retina
- j) signatur
- k) röst



Om inget annat anges kommer begreppet biometri i denna projektrapport att härnäst betyda hel eller delvis automatisk ansiktsgenkänning/skanning.

2.1 Verifikation

Ett begrepp som återkommer ofta inom biometrin är verifikation som innebär att avgöra om personen verkligen har den identitet som påstås. Detta genomförs praktiskt genom att jämföra biometriska data från ett foto eller inskanning med det som finns registrerat sedan tidigare. Resultatet visar om mönstren matchar eller inte.

2.2 Identifikation

Identifiering är ett annat begrepp inom biometrin som på sätt och vis kompletterar verifikationen genom att det innebär att avgöra vem en person troligtvis är. På samma sätt som en verifikation används biometriska data från ett foto eller inskanning, men nu mot ett befintligt register av möjliga personer. Dessa jämförelser kan sedan via olika metoder bygga upp en rankinglista på vem personen som ska identifieras troligtvis kan vara.

2.3 Enrollering

Det första steget i en biometrisk matchning är en enrollering. Detta innebär att en persons data för första gången samlas in, analyseras, bearbetas och lagras i ett register. Inom kriminalarbete finns det många lagar och förordningar om hur enrollering ska genomföras och framförallt om hur och hur länge dessa biometriska data får sparas i ett register. För att erhålla en säkrare metod och få ett högre bevisvärde krävs bilder som kan analyseras i tre dimensioner.

3. Allmänt om ansiktsgenkänning

Ansiktsgenkänning anses vara ett av de säkrare underlagen vid biometrisk identifiering eftersom de delvis bygger på genetiska egenskaper. Det uppfattas inte kränkande att någon tar en bild av ansiktet, det vill säga acceptansen av metoden är hög. Att de flesta metoder för ansiktsgenkänning utgår från exempelvis fotografier ökar osäkerheten, då de utgör tvådimensionella data. Osäkerheten som uppstår med ansiktsbilden beror främst till huvudets tredimensionella

(3D) position, ansiktsaccessoarer såsom exempelvis glasögon, ljusförhållanden på platsen där bilden tas (inomhus/utomhus), ansiktsbehåring, ansiktsuttryck samt åldrande.

3.1 Tillämpningar av ansiktsgenkänning

Det finns enligt Anders Ek och Olov Hagner [4] tre större användningsområden för biometriska metoder inom ansiktsgenkänning:

1. **Kommersiella tillämpningar**, exempelvis använda ansiktsgenkänning istället för PIN-kod.
2. **Statliga tillämpningar**, ett konkret exempel är att infoga biometrisk information i pass, för att säkra att endast en person använder identiteten.
3. **Kriminaltekniska tillämpningar**, där ett exempel kan vara att identifiera lik som matchas mot pass- eller körkortsregistret.

Den här rapporten behandlar därmed till största delen kriminaltekniska tillämpningar, men även delvis statliga tillämpningar.

3.2 Viktiga steg för ansiktsgenkänningsmetoder

För att använda tekniken med ansiktsgenkänning krävs fem steg i metoderna:

1. Förvärvandet av bild (exempelvis från en övervakningskamera).
2. Bearbetning av bild (omvandla bilden till ett bearbetningsbart format).
3. Extrahering av distinkta karakteristiska (för att identifiera synliga anletsdrag används olika matchningsmetoder)
4. Skapande av mönster (sökningsskript som använder olika bilder som underlag).
5. Matchning av mönster (själva sökningen i registret).

Metoderna som idag används vid Statens kriminaltekniska laboratorium (SKL) grundar sig i dessa fem steg, även om inte alla stegen utförs vid laboratoriet enligt Klas Brorsson Låthén [3].

4. Aktuella metoder för kriminaltekniska tillämpningar vid SKL

Skulle det vara möjligt att använda fotografier av personer från exempelvis ett kameraövervakningssystem tillsammans med biometriska programvaror för automatisk ansiktsgenkänning i ett spaningsskede av en förundersökning? Sökningar skulle kunna göras i passregistrets ansiktsbilder med tillhörande biometriska data eller bland daktningsfotografierna (referensfotografier tagna i samband med att någon häktats eller anhållits för misstanke om brott), för att på så sätt få fram ett urval av möjliga personer.

4.1 Dagens metoder

På SKL utförs ansiktsgenkänning i dagsläget på så sätt att en bild på en misstänkt manuell jämförs med en eller flera bilder från exempelvis ett övervakningssystem för att eventuellt kunna verifiera identiteten.

En manuell jämförelse är i dagsläget, enligt Klas Brorsson Låthén [3], överlägsen de datoriserade metoderna med avseende på säkerheten i utförandet. Arbetssättet förutsätter dock att det finns en eller flera misstänkta i ärendet och dessa arbeten sker på beställning från förundersökningsledare hos polisen. En automatiserad metod skulle i dagsläget ge ett stort antal falska positiva, det vill säga ge felaktig träff vid jämförelsen. Därför kan den inte utgöra någon absolut bevisning i ett brottsärende. Vidare är även de idag använda metoderna inte tillräckliga som ensam bevisning, men fungerar tillfredsställande som stödbevisning till exempelvis DNA.

SKL använder sig av ett bedömningsunderlag vid ansiktjämförelser [5], där speciella detaljer (som är eller födelsemärken), höger och vänster öra, höger och vänster öga, ögonlocken, ögonbrynen, näsans form, nästippen, näsvingarna, näsborrarna, munnens form, överläppen och underläppen, tänderna, ansiktets form, hårfästet, skäggväxt, pannans form, kindernas form, hakans form, och halsens utseende granskas och bedöms vid verifieringarna. Detta arbetssätt kräver dock att det finns en misstänkt för brottet, bilder på den misstänkte samt bilder från till exempel ett övervakningssystem för att utföra verifieringen.

Sedan lämnas ett sakkunnigutlåtande [6], där resultatet graderas från -4 (sannolikheten att den uppställda hypotesen är sann bedöms i praktiken som utesluten), till +4 (sannolikheten att uppnått resultat kan härröra från en annan hypotes är i praktiken utesluten).

Det finns även en metod som är lite mer automatiserad. För att skapa en rankinglista av misstänkta genomförs en referensbild från exempelvis en övervakningskamera med en population av misstänkta. Via de biometriska mätningarna som genomförs så skapas en sannolikhetslista och denna kan vara till hjälp vid kriminalundersökningsarbetet.

Denna metod använd mycket sparsamt i Sverige och kan inte utföras vid SKL ännu, men de undersöker för närvarande system som skulle kunna appliceras på svensk lagstiftning och datalagar.

5. Gällande lagstiftning

I Sverige har vi en mycket stark lagstiftning för att skydda den enskilda individens integritet och här ska jag nämna några av de regler som gäller för en sådan här typ av verksamhet.

5.1.1 Sökningar i register

En polisman som arbetar med en brottsutredning ska redogöra för vem som skäligen misstänkts för brottet och om det finns ett tillräckligt stort underlag för ett åtal. En förundersökningen ska även utgöra ett underlag för huvudförhandlingen och presentera bevisningen i ett sammanhang. I detta ingår det enligt Ewa-Karin Abrahamsson [2] ofta att utföra diverse dataslagningar i olika register.

Dataslagningarna styrs i sin tur av Polisdatalagen: 1§ *"Denna lag gäller utöver personuppgiftslagen (1998:204) vid behandling av personuppgifter i polisens verksamhet"* bland annat för att *"3. bedriva spaning och utredning i fråga om brott som hör under allmänt åtal."*

Personuppgiftslagens syfte enligt 1 § *"är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter."* Till personuppgifter räknas all information som kan härledas till någon levande person. Polisen får i enlighet med personuppgiftslagen 8a §, behandla personuppgifter i samband med utredning av brott. En polisman arbetar även enligt gällande bestämmelser i sekretesslagen vid behandlingen av personuppgifter.

5.1.2 Insamling, registrering och lagring av uppgifter i register

Daktningarna utförs i enlighet med Rättegångsbalkens regler: *"Av den som är anhållen eller häktad må fotografi och fingeravtryck tagas; han vare ock underkastad annan dylik åtgärd. Vad nu sagts gälle ock annan, om det erfordras för vinnande av utredning om brott, varå fängelse kan följa."* och polisen kan använda sig av dessa inhämtade biometriska data för att utreda brott. Enligt Förordningen om fingeravtryck är det också så att fingeravtryck samt fotografi **ska** tas om ovan förutsättningar är uppfyllda.

Däremot är det **inte** tillåtet, enligt Polisdatalagen, att spara fotografier från daktning eller ytterligare biometriska data digitalt, varken i signalementregistret eller passregistret. Dessa register är tillståndspliktiga och polisen ansöker hos/anmäler till Datainspektionen, som utfärdar tillstånd/godkänner anmälningar, för att få ha och använda registren.

Vidare anger Passlagen att biometrisk information från passbilden **inte** får sparas i ett register eller utsättas för datasökningar.

Allt detta sammantaget får den lite märkliga konsekvensen att det är tillåtet att spara passbilder som inskannade papperskopior, det vill säga digitala fotografier, men det är inte tillåtet att spara daktningsfotografierna digitalt.

Vidare sker enligt Ewa-Karin Abrahamsson [2] en extrahering av biometriska data vid en passkontroll. De

biometriska datauppgifterna förstörs direkt efter kontrollen och får inte sparas i ett register. Om en passkontrollstation kan extrahera biometriska data ur en digital bild i passets chip, kan en brottsling förmodligen genomföra samma sak från vilka inskannade fotografier eller digitala bilder som helst. Den biometriska informationen finns redan tillgänglig, fast i en annan form.

5.1.3 Samkörning av olika register

Datainspektionen har en uppgift att se till att myndigheter inte genomför otillåtna samkörningar av register. En offentlig sektor i ett icke-demokratiskt samhälle kan utgöra ett mycket stort integritetshot mot den enskilde medborgaren. Den offentliga sektorn kan tvinga människor att lämna ifrån sig information, eftersom den har lagen på sin sida och har även möjlighet att samköra register från många olika källor vilket ökar graden av intrång i integriteten. I ett demokratiskt samhälle är det meningen att den offentliga sektorn ska stå för goda och ädla syften, men det hindrar inte alltid missbruk och annan olämplig användning av personlig information.

6. Framtiden

Det finns flera mer eller mindre kommersiella system som använder sig av olika algoritmer för att utläsa biometriska mätdata, som kan vara användbara för kriminaltekniska ändamål. Ett exempel på sådant är Eigenface [7] med Automatic face processing [8] som vidareutveckling. De flesta systemen är enligt Klas Brorsson Låthén [3] bra på olika saker och typer av bilder. Detta kommer av just det faktum att det används olika algoritmer för att framställa mätdata. Vidare ställer de alternativa systemen även olika krav på bilderna som ska analyseras.

Denna problematik gör det komplicerat att finna *ett* system som kan hantera samtliga bilder och det kommer att ta tid innan det kan införas fullständiga system för automatiserad behandling för ansiktsbiometri i svenskt kriminalarbete. Men på sikt kommer det att genomföras, då samhällsvinsterna vida överskrider svårigheterna. Den automatiserade behandlingen av ansiktsbiometriska data kommer att vara ett bra komplement till den manuella jämförelsemetod som finns idag.

Vidare kommer dessa nya system troligen aldrig att nå samma bevisvärde vid rättegångar som exempelvis DNA, men de kommer att fungera som mycket god stödbevisning.

7. Sammanfattning

Registrering av biometriska data gällande ansiktsdrag verkar anses vara så integritetshotande att det för tillfället inte ges möjlighet att lagra ansiktsbiometriska data på ett användbart sätt. Kompetensen och tekniken

finns enligt Ewa-Karin Abrahamsson [2] redan idag för att polisen i ett spaningsskede av en förundersökning skulle kunna använda sig av datoriserade biometriska ansiktsgenkänningsmetoder för att identifiera misstänkta från bilder av olika slag, exempelvis kameraövervakningsbilder. Vidare finns heller inga biometriska data extraherade från ansikten lagrade i, eller kopplade till, passregistret och signalementsregistret. Det krävs ganska omfattande ändringar i lagar och förordningar för att det ska kunna ske i framtiden.

Så svaren på frågeställningarna i denna rapport kan sammanfattas med att det skulle vara användbart med ansiktsbiometri i kriminalarbete och att det går att skapa system för detta. Resultat från användandet av sådana skulle fungera att använda i rättsprocesser, men med nu gällande lagar och förordningar är det inte möjligt att implementera sådana system med tanke på den personliga integriteten.

8. Diskussion

Enligt datainspektionen så sparas i nuläget betydligt mycket mer integritetskränkande information i polisens register än vad ytterligare biometriska data och digitala bilder i form av daktningsfotografier skulle utgöra.

Lagstiftningen på området har inte hunnit med i den tekniska utvecklingen och lagarna bygger på tekniken som fanns på 1970-talet. Det kan även finnas en hos människan inbyggd rädsla historiskt att registrera biometriska data såsom ansiktsdrag digitalt, då sådan verksamhet kan associeras till exempelvis andra världskrigets Nazityskland och dess rasregistrering.

Med en lagstiftning som följer dagens teknikutveckling och medborgarnas krav på brottsupplärning samt trygghet i samhället, skulle det vara möjligt att upprätta ett register av biometriska data av misstänkta brottslingar (av en typ som exempelvis DNA-registret utgör idag). Detta register skulle sedan kunna användas för att på ett automatiserat sätt göra jämförelser med bilder från exempelvis övervakningskameror. Vidare skulle passregistret mycket väl kunna användas för identifiering om det var tillåtet att registrera och spara biometriska data tagna från passfoton. För att detta ska bli verklighet krävs att vi alla funderar på om vi inte är beredda att minska skyddet av vår personliga integritet för att bekämpa kriminaliteten.

Referenser

- [1] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, "Handbook of Fingerprint Recognition", Springer, New York, 2003
- [2] Ewa-Karin Abrahamsson, Polismyndigheten i Hallands län, "Kan biometri vara ett hjälpmedel för

att identifiera misstänkta från kameraövervakningsbilder?", Specialarbete vid Kriminalteknisk grundutbildning 2007-2008 och telefonintervju.

- [3] Intervju SKL, Klas Brorsson Låthén, april 2008.
- [4] Anders Ek, Olov Hagner, TDDC03 Project, "Ansiktsbiometri - project 17", Spring 2005.

Bilagor

- [5] Ansiktsjämförelse, blankett från SKL
- [6] Sakkunnigutlåtande, blankett från SKL

Internetkällor

- [7] Eigenface-based facial recognition, Dimitri PISSARENKO, February 13 2003, <http://openbio.sourceforge.net/resources/eigenfaces/eigenfaces-html/facesOptions.html>, 2008-04-23
- [8] Automatic face processing, <http://et.wcu.edu/aidc/BioWebPages/lfa.htm>, 2008-04-23