

Fingeravtryck och ansiktsigenkänning

- En studie av biometri i praktiken



Projektuppgift i Informationssäkerhet

Sara Hörlin

sarho837@student.liu.se

Peter Löfgren

petlo539@student.liu.se

Handledare

Niclas Wadströmer

Fingeravtryck och ansiktsigenkänning - En studie av biometri i praktiken

Peter Löfgren Sara Hörlin
Linköpings universitet, Sverige
Email: {petlo539, sarho837}@student.liu.se

1. Sammanfattning

Vi har i denna rapporten gjort en litteraturstudie kopplat med en empirisk studie av hur biometriska system används i praktiken och då speciellt fingeravtryck och ansiktsigenkänning. Dessa används av polisen men även mer och mer vid inpasseringskontroller. Dessutom används båda dessa i de nya passen och vi har därför inriktat oss på att studera dessa för att se om de på något sätt kompletterar varandra. Vi har kommit fram till att de kompletterar varandra bra på de biometriska egenskaper som vi har valt att jämföra dessa emellan. Skälet till att de används i passen tror vi dock inte är för att de kompletterar varandra utan för att ansiktsigenkänning alltid har använts och är den lättaste metoden för manuell jämförelse medan fingeravtryck är en bättre och säkrare metod och att man gradvis vill gå över till denna för att höja säkerheten i identifieringen.

2. Inledning

Rapporten ingår som en obligatorisk del i kursen TDDC03 informationssäkerhet vid Linköpings tekniska högskola.

Vi har valt att undersöka hur fingeravtryck och ansiktsigenkänning används praktiskt för att verifiera personers identitet och identifiera personer. Anledningen till att vi har valt dessa är att de nya passen kommer att innehålla båda teknikerna efter 2007. Vi tycker därför att det är intressant att undersöka om dessa två tekniker kompletterar varandra, och i så fall hur.

2.1 Frågeställning

De frågor som vi undersökt i den här rapporten är:

- Var används fingeravtryck och ansiktsigenkänning i praktiken och finns det egenskaper som gör att de kompletterar varandra?
- Vilka fördelar och nackdelar finns med dessa tekniker och vilka är de viktigaste skälen till att använda eller inte använda dem?

- Vilka biometriska system används idag i praktiken och vilken teori ligger bakom dessa och då speciellt fingeravtryck och ansiktsigenkänning?

2.2 Metod

Vi har använt oss av litteraturstudier samt gjort ett studiebesök på polismyndigheten i Linköping. Där intervjuade vi Anita Bines chef för passenheten och Jessica Granath passhandläggare.

2.3 Avgränsningar

Vi kommer bara att gå in kort på andra biometriska system och där bara nämna vad som kan användas som biometrisk identifierare. Detta för att läsaren ska få en bild av vilka olika identifierare som finns och skapa sig en referens.

2.4 Målgrupp

Den förväntade målgruppen till den här rapporten är personer som har läst någon grundläggande kurs i datasäkerhet och är intresserade av hur biometriska system fungerar.

3. Identifiering och verifiering

I detta kapitel beskrivs allmänt vad biometrisk identifiering och verifiering är samt olika egenskaper som används för klassificering av dessa system. Källan till denna information är föreläsningar i kursen TDDC03, speciellt med Tina Lindgren. [6]

3.1 Biometriska system

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

När vi talar om biometrisk igenkänning så handlar det om den tredje kategorin, *något man är*. I detta begrepp ingår allting som har med det fysiska att göra till exempel fingeravtryck, gångstil eller signaturer.

Det finns två olika sätt att använda biometri, det första är **verifikation**. Personen i fråga anger vem han/hon är och den biometriska egenskapen jämförs med den som finns i databasen för den personen, om det bedöms stämma så är identiteten verifierad. Denna teknik ska svara på frågan ”Är jag den jag säger att jag är?”. Verifikation används oftast i så kallad positiv igenkänning det vill säga i fall då personen medverkar till igenkänningen.

Det andra sättet är **identifikation**, då ska personen istället identifieras. Det betyder att man måste jämföra egenskapen med alla i databasen, eller åtminstone tills man får en träff. Detta innebär att vi måste göra N jämförelser istället för en som vid verifikation. Denna teknik ska svara på frågan ”Vem är jag?”. Identifikation används oftast i så kallad negativ igenkänning alltså i fall då personen inte aktivt medverkar till igenkänningen eller inte vill bli igenkänd. Biometriska metoder är lämpliga att använda till både positiv såväl som negativ igenkänning.

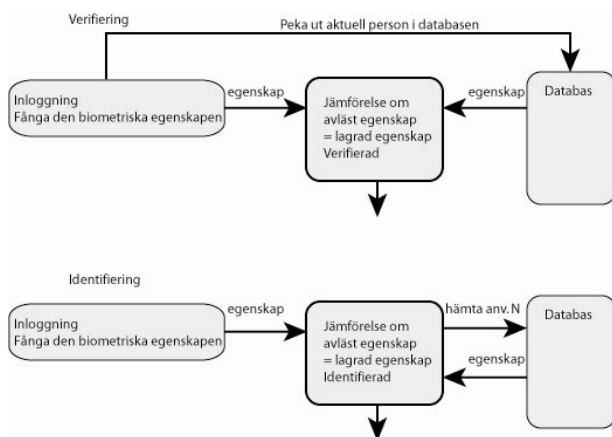


Bild 1: Anropschema för verifiering och identifiering.

3.2 Falsk acceptans och falskt avvisande

Vid avläsning kommer data inte att vara helt identiskt med originalet. Detta kan vid till exempel fingeravtryck bero på hur noga man mäter och faktorer som kan förändra är hur hårt man trycker sitt finger emot eller hur snabbt man drar. Detta innebär att för att systemet ska vara användbart så måste ett viss intervall av olikheter accepteras. Detta innebär att fingeravtryck från olika personer kan identifiera samma person. En annan effekt kan vara att en person inte identifieras som den han/hon är

När en person identifieras som någon som man inte är kallas detta falsk acceptans och då någon inte identifieras som den man är kallas detta för falsk avvisning.

Detta skapar en balansgång mellan dessa två fel. Ju mer olikheter som systemet accepterar desto mer smidigt kommer det att fungera för användarna att använda. Då mindre olikheter accepteras fås en högre säkerhet i identifieringen, men detta kan skapa mycket irritation då legitima användare refuseras.

3.3 Biometrisk klassificering

Det finns vissa biometriska egenskaper som bör tas i beaktande då man bestämmer sig för vilket system man ska använda. Det kan även finnas vissa krav på prestanda som måste uppfyllas. Nedan beskrivs de egenskaper som allmänt används för att beskriva biometriska egenskaper.

Egenskaper som är relaterade till personer.

- **Universalitet** Att kännetecknet finns på alla människor.
- **Unikhet** Hur olika kännetecknet är från person till person.
- **Permanens** Hur mycket kännetecknet kan förändras över tiden.
- **Insamlingsbarhet** Hur lätt det är att mäta kännetecknet.

Egenskaper som är mer systemrelaterade:

- **Prestanda** Avser krav på systemet relaterat till hastighet, resurser och säkerhet.
- **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.

3.4 Livsdetektion

Livsdetektion innebär att man på något sätt verifierar att den biometriska egenskap man mäter faktiskt sitter på en levande person. Det är nödvändigt i de flesta biometriska system för att bekräfta att man mäter på en levande person och inte på ett falskt objekt som efterliknar en person.. Till exempel vid ansiktsgenigenkänning kan man mäta temperaturer i ansiktet och huvudrörelser för att säkerställa att det inte bara är en bild som hålls framför kameran.[1]

4. Biometriska egenskaper

I detta kapitel beskrivs olika biometriska system. Störst vikt har lagts vid fingeravtryck och ansiktigenkänning där även praktiska exempel på tillämpningar har tagits upp.

4.1 Iris

Mönstret i en persons iris är unikt för alla människor och är konstant hos en individ från ca ett års ålder till livets slut förutsatt att ögat inte skadas på något sätt. Identifiering kan ske med hjälp av iris genom att en digital bild tas av ögat, från vilket mönstret i iris kan läsas av. Nackdel med iris är att det av en allmänhet anses integritetskränkande eftersom man till exempel kan utläsa annat än just identiteten som till exempel vissa sjukdomar. Dessutom är utrustningen relativt dyr jämfört med andra tekniker. [6], [8]

4.2 Tal

Taligenkänning baserar sig på att akustiska egenskaper människor emellan har visat sig skilja sig åt. De akustiska mönstren beror dels på storleken på munnen och strupen och dels på inlärd beteendemönster såsom tonhöjd, tonfall och dialekt. Denna akustiska karaktäristik kallas för talavtryck (fritt översatt från "voiceprint"). Nedan listas de tre sätt som man kan använda röstigenkänning.

- **Textberoende** Är beroende av att användaren säger en bestämd text.
- **Textberoende** Användaren kan säga vad som helst.
- **Textbestämd** Användaren måste säga en viss text bestämd av datorn.

Taligenkänning kan lämpa sig för verifiering av en person men är oftast inte tillräckligt unikt för att kunna användas för identifiering. En människas röst påverkas av personens hälsa, stress, känslor och så vidare, dessutom kan bakgrundsbrus eller oväsen störa och till råga på allt så har vissa människor väldigt lätt att härma andra vilket gör tekniken ganska så känslig. [2]

4.3 Handådror

En människas mönster av ådror är en unik biometrisk egenskap. Detta mönster skiljer sig till och med mellan enäggstvillingar. En persons handådror kan skannas med hjälp av en infraröd kamera. Genom att personen vars hand skannas knyter handen hårt blir ådrorna mer framträdande och lättare att läsa av. En nackdel är att infraröda sensorer är dyra relativt annan biometrisk utrustning till exempel fingertrycksavläsare. [1]

4.4 Handigenkänning

Även handen är i viss bemärkelse unik och handgeometri har länge varit och är en av de äldsta metoderna. Användaren placerar handen på en läsare och mätningar görs av längd, bredd, tjocklek av huden på handen och fingrarna. System som känner av blodflödet i handen för att undvika förfalskning finns också. [12],[13]

4.5 Fingeravtryck

Fingeravtrycket är unikt för varje person och bildas redan i fosterstadiet. Fingeravtryck är permanent under hela livstiden vilket gör det till en attraktiv biometrisk identifierare. Avtrycket är relativt enkelt att mäta genom att placera fingret på en sensor som läser av fingrets mönster. Fingeravtrycket sparas som en bild i verifieringssystemet. Vid verifieringen jämförs det inlästa avtrycket med ett redan lagrat fingeravtryck för den aktuella personen. Man jämför olika kännetecken hos fingeravtrycken och oftast positionen och riktningen av speciella mönster. [1], [11]

Fingeravtrycksigenkänning i praktiken

Polisen utnyttjar fingeravtryck vid brottsplatser. Fingeravtrycket penslas med ett medel till exempel sot, som reagerar och gör att avtrycket klart kan urskiljas mot bakgrunden. Därefter fotograferas avtrycket och jämförs mot AFIS (Automated Fingerprint Identification System) för att identifieras. [5]

En ny lag som träder i kraft tvingar flygbolag att utföra identifikation av passagerare både vid incheckning och ombordstigning. Detta för att man ska kunna verifiera att den som checkat in bagage är densamma som flyger med planet och att ingen checkar in bagage och sedan inte åker med. Lagen har kommit till efter senare års terrorhot.

SAS har valt att lösa detta genom att använda fingeravtryck för att verifiera att den som checkar in är densamma som går ombord på planet. Ett avtryck tas efter identifiering och ytterligare ett tas vid ombordstigning och jämförs med det första. Systemet används inte i dagsläget men kommer att träda i kraft under 2006. [4]

Fingeravtryck används mer och mer även som inloggning till datorer och som nyckel till dörrar. Exempel där detta används är inom sjukvården, bankväsendet, regeringsbyggnader med flera. [3]

4.6 Ansiktsgenkänning

Fördelar med att identifiera någon med hjälp av ansiktet är att det är lätt att göra utan att personen i fråga är medveten om det och att det har en hög acceptans hos allmänheten. Nackdelar är att ansikten kan likna varandra, till exempel inom familjer och att det kan förändras över en tidsrymd till följd av exempelvis viktförändring, hår, mustasch och skäggbeklädnad. Negativ ansiktsgenkänning går att undvika genom olika förklädnader. [1]

Teknik för automatisk ansiktsgenkänning

Vid automatisk igenkänning av en ansichtsbild plockas relevant information i bilden ut och jämförs med motsvarande information från bilder i en databas. En metod för att jämföra två ansichtsbilder automatiskt är att skapa egenansikten. [7], [9], [10]

Egenansikten

Varje ansikte innehåller mönster. Exempel på mönster är hur näsa, mun och ögon ser ut och hur dessa förhåller sig till varandra. Dessa mönster kan extraheras ur en ansichtsbild med hjälp av en metod som heter Principal Component Analysis (PCA). Mönstren för en ansichtsbild lagras i en egenvektor av vilket en spökbild av ansiktet skapas, detta kallas egenansikte. Av de värden som finns representeras i egenvektorn beräknas ett viktat tal utgående från de värden som finns där. Egenansikten som bygger på bilder av samma person innehåller viktade tal som ligger mycket nära varandra. Vid automatisk ansiktsgenkänning skapas ett eller med fördel flera egenansikten av en person. Egenansiktenas viktade tal kan sedan jämföras med, i en databas, lagrade egenansiktens värden. [9], [10]

Ansiktsgenkänning i praktiken

Automatisk ansiktsgenkänning kan kombineras med kameraövervakning. Kameraövervakning används oftast på platser där krav på hög säkerhet råder som banker, flygplatser, militäranläggningar och platser som har ett polisiärt intresse. Ett exempel på detta är polismyndigheten i West Yorkshire i England. [16]

Polisen i West Yorkshire var för ett par år sedan först inom polisområdet att införa ett system för automatisk ansiktsgenkänning (AFR). Bilder av personer som begår brott tas från filmer som fås genom att känsliga ställen kameraövervakas. Detta är till exempel områden med hög brottstatistik. Bilden från kameraövervakningen skannas och jämförs med kända bilder av brottslingar i polisens databas.

Bilderna jämförs genom att till exempel avståndet mellan ögonen mäts. Enligt West Yorkshire polisen är antal jämförelser som behövs göras med bilder i databasen

också begränsat då man oftast vet en del saker om förövaren som att en inbrottstjuv brukar begå inbrott i närheten av sitt eget hem. Enligt West Yorkshire polisen har införandet av AFR kunnat leda till att fler brottslingar kunnat gripas. [14],[15]

Senast i mars berättade CNN i en artikel om två studenter i HAIFA, Israel som utvecklat en 3D-skanner för ansiktsgenkänning. Huden i en persons ansikte skannas med hjälp av en serie av ljusmönster. Avståndet mellan olika punkter i ansiktet beräknas. Alla uppmätta avstånd får sedan representeras av raka linjer i ett tredimensionellt rum. På detta sätt återskapas en abstrakt bild av ansiktet. Fördelen med denna teknik är att den är oberoende av ljusförhållanden och ansiktsvinkel. [17]

5. Empiri

Vi har med vårt arbete varit intresserade av att ta reda på hur ansiktsgenkänning och fingeravtryck används i praktiken. Eftersom båda dessa biometrisk egenskaper kommer att utnyttjas i de nya passen har vi varit speciellt intresserade av att ta reda på hur dessa fungerar.

Anita Bines och Jessica Granath vid polismyndigheten i Linköping arbetar med framställning av de nya passen. I de nya passen är kraven på bilden högre än i de gamla. Bilden ska vara tagen rakt framifrån och ansichtsuttrycket måste vara neutralt. Detta för att bilden ska vara väl anpassad för automatisk ansiktsgenkänning berättar Jessica Granath. Fotograferingen sker idag direkt på polisstationen med en speciell kamera som anpassar sig efter den fotograferades längd. Förutom den synliga bilden i passet lagras bilden också digitalt i passet i ett datachip. I detta chip lagras också personens andra uppgifter som finns i passet samt signatur och i framtiden är det tänkt att även fingeravtryck ska komma att lagras här. Redan idag används informationen i chippet i de nya passen vid flygplatser i Sverige, till att jämföra en persons ansichtsbild med bilder av efterlysta personer i en databas enligt Anita Bines. Båda poliserna tycker att det nya passsystemet både är enklare och säkrare än de gamla. De vet inte hur svårt eller lätt det är att förfälska informationen som finns i chippet men påpekar att de nya passen skapades för att öka säkerheten. Som poliser har de ingen möjlighet att ändra på informationen i chippet då passet väl är skapat. Ingen av poliserna kan dock svara på hur pass stor förbättring med avseende på säkerhet som kommer att ske då om ett par år även fingeravtryck kommer att lagras i passen.



Bild 2: En passterminal hos polismyndigheten.

På bilden ser vi en passterminal hos polisen. Terminalen är utrustad med en kamera för att ta kort på ansiktet. En fingeravtrycksläsare för att i framtiden läsa av fingeravtryck som kommer att vara tvunget att sparas i passet. Den har även en platta där signaturen registreras. All denna biometrisk identifikation sparas sedan tillsammans med den personliga informationen på ett chip i passet. För att kunna läsa av informationen på chippet måste poliserna placera passet nära en apparat som sedan trådlöst läser av informationen på chippet.

6. Analys och diskussion

	Universalitet	Unikhet	Permanens	Insamlingsbarhet	Prestanda	Acceptans	Kringgående
Fingeravtryck	M	H	H	M	H	M	H
Ansiktsgenkänning	H	L	M	H	L	H	L

Tabell 1: Visar en jämförelse mellan fingeravtryck och ansiktsgenkänning.

Klassificering av fingeravtryck och ansiktsgenkänning

Vi har valt att titta på en klassificering av fingeravtryck och ansiktsgenkänning med avseende på de egenskaper som nämndes i kap 2.1. Tabellen är hämtad från [1] dock fanns inga motiveringar. En egenskap bedöms efter hur väl den överensstämmer med automatisk fingeravtrycksavläsning respektive ansiktsgenkänning. Skalan som används är:

H = Högt överensstämmande
M = Medel överensstämmande
L = Lågt överensstämmande

Vi tycker att klassificeringen är rimlig. Nedan följer vår egen motivering.

Universalitet

Alla människor har ett ansikte och därför klassas detta som **H**. De flesta människor kan ge ett fingeravtryck men då det finns personer som förlorat alla sin fingrar klassas detta som **M**.

Unikhet

Ansiktsdrag kan vara väldigt lika och svåra att särskilja framför allt på personer inom samma familj, därför klassificeras detta med **L**. Fingeravtryck däremot har bevisats vara unika [6] och klassas därför som **H**.

Permanens

Ansiktet förändras över tiden beroende på ålder, vikt skäggbeklädnad med mera. Större förändringar sker dock under en längre tidsperiod och är därför inte speciellt svåra att med jämna intervall uppdatera. Klassas därför som **M**. Fingeravtryck förändras inte alls över tiden och klassas därför som **H**.

Insamlingsbarhet

Bilden som tas för ansiktsgenkänning kan tas med en vanlig digitalkamera och kan dessutom tas på ett längre avstånd. Personen som skall verifieras/identifieras behöver inte ens vara medveten om det. Detta genererar klassningen **H**. För att läsa av fingeravtrycken så måste personen samarbeta och speciell utrustningen krävs. Dock är utrustningen billigt och lätt att få tag i [6] och därför klassas fingeravtryck med **M**.

Prestanda

En ansiktsbild innehåller många egenskaper som måste läsas av vid automatisk verifiering/identifiering för att inte blandas ihop med andra ansiktsbilder. Detta gör avläsning av ansikte till en relativt långsam process jämfört med till exempel fingeravtryck som har unika egenskaper som är relativt lätta att identifiera och läsa av. Ansiktsgenkänning klassas därför som **L** medan fingeravtryck klassas som **H**.

Acceptans

Ansiktet visar man alltid och manuell verifiering förekommer dagligen mot id-kort och passerkort med mera. Detta innebär att ansiktsverifiering/identifiering redan från början är en väldigt accepterad metod. Klassas därför som **H**. Fingeravtryck kräver att personen interagerar med en läsare. Fingeravtrycksavläsning är ofta

förknippat med polisen och brottslighet där detta använts i över 100 år. Detta gör att en del människor har en negativ inställning till denna metod. Dock blir denna teknik allt mer vanlig och utbredd vilket lett till att den gamla kriminellstämpeln allt mer suddas bort. Klassas som **M**.

Kringgående

Ett ansikte är lätt att förändra och därmed kan man ganska lätt undgå negativ igenkänning. Dessutom kan det räcka med ett foto för att lura ett system om det har dålig liv detektion. Detta medför en klassificering **L**. Fingeravtryck kräver med avancerade metoder för att lura systemen med till exempel artificiella fingeravtryck eller att man hotar någon och därmed får det klassificeringen **H**.

Praktiska tillämpningar

Under vårt arbete har vi kommit i kontakt med ett flertal företag som är aktiva i branschen. De trender som vi har kunnat tyda genom att se på deras kunder visar att ansiktsgenkänning förekommer inom bankbranschen och bevakningsbranschen. Som bevakningskunder kan allt från polismyndigheter till flygplatser räknas in.

Fingeravtryck används mer och mer eftersom utrustningen är så billig. De områden som har störst kundkrets är polisen världen över. Men det används även till inloggnings till datorer och inpasseringskontroller.

7. Slutsats

Ur analysen ovan framgår att varje egenskap uppfylls högt av antingen ansikte eller fingeravtryck. Ur detta drar vi slutsatsen att fingeravtryck och ansikte är lämpliga komplement vid biometrisk identifiering/verifiering. Om detta är anledningen till att båda dessa används i de nya passen har vi inte fått svar på. En annan teori till att de används där är för att de båda har hög acceptans hos allmänheten.

Den främsta anledningen till lagring av bild och annan information i chippet är för att det ska vara svårare att förfälska passen och inte för man på automatiskt vis ska kunna identifiera personer baserat på ansiktscbilder. Ansiktsgenkänning kommer alltså även i framtiden att ske manuellt. Fingeravtrycksgenkänningen kommer sedan att tillföra en helt ny nivå av säkerhet eftersom dess mätdata generellt har en lägre falsk acceptans. Vi tror att det kommer att medföra mindre manuellt arbete vid passkontrollerna.

En annan säkerhetsaspekt som egentligen inte har med de biometriska egenskaperna att göra är att informationen från chippet avläses trådlöst. Detta gör att informationen kan hämtas utan att ha fysisk tillgång till passet och så fort

någon har listat ut hur detta kan göras tror vi att identitetsstölder blir väldigt lätta.

Vi anser att ansiktsgenkänning endast är lämpligt för verifiering av identitet eftersom ansikten inte är tillräckligt unika för att identifiera en person. Dock anser vi att det kan användas som identifiering om mängden personer i databasen är väldigt begränsad eller som hjälp vi bildupptagningar vid brott för att kunna få en ledtråd till vem det skulle kunna vara. De områden där det i vår studie visat sig att ansiktsgenkänning används är på bevakningsområden till exempel flygplatser, polisiära och militära områden och i andra sammanhang då det handlar om negativ igenkänning.

Fingeravtryck anser vi vara en väldigt tillförlitlig teknik vad det gäller unikheten. Dock har det visat sig att det inte är speciellt svårt att göra artificiella fingeravtryck och vi tror att i framtiden kommer inte endast fingeravtryck att kunna användas utan det kommer krävas multimodala system som förlitar sig till mer än en egenskap. Dessutom tror vi att bevisning i brottsutredningar inte heller längre kommer att kunna förlita sig på fingeravtryck längre. Troligtvis kommer DNA att krävas för att binda människor i framtiden.

8. Källförteckning

[1] Handbook of fingerprint recognition

<http://bias.csr.unibo.it/maltoni/handbook/>
2006-03-20

[2] Diaphonics

<http://www.diaphonics.com/faq.php>
2006-04-24

[3] Precise Biometrics

<http://www.precisebiometrics.com/>
2006-04-27

[4] Datainspektionen

http://www.datainspektionen.se/pdf/beslut/SAS_fingeravtryck.pdf
2006-04-27

[5] Statens kriminaltekniska laboratorium

<http://www.polisen.se/inter/nodeid=6893&pageversion=1.html>
2006-04-27

[6] Föreläsningslides Biometri

Tina Lindgren
<http://www.ida.liu.se/~TDDC03/lectures/slides/biometrics1.pdf>

<http://www.ida.liu.se/~TDDC03/lectures/slides/biometrics2.pdf>

2006-04-26

[7] International biometric group, facial recognition

http://www.biometricgroup.com/reports/public/reports/facial-scan_tech.html
2006-03-24

[8] LG iris division

<http://www.lgiris.com/iris/>
2006-03-24

[9] Face Recognition Using Eigenfaces, Matthew A. Turk et Al, 1991

<http://ieeexplore.ieee.org/iel2/340/3774/00139758.pdf?arnumber=139758>
2006-03-29

[10] Eigenface-based facial recognition, Dimitri PISSARENKO, February 13, 2003

<http://openbio.sourceforge.net/resources/eigenfaces/eigenfaces-html/facesOptions.html>
2006-03-30

[11] Fingeravtryck

<http://www.ida.liu.se/~TDDC03/oldprojects/2004/final-projects/prj013.pdf>
2006-03-29

[12] Hand Geometry Recognition | Biometrics

http://www.hrsLtd.com/identification_technology/hand_recognition.php
2006-04-24

[13] An online biometric authentication system based on eigenfingers and fingergeometry.

Slobodan Ribaric and Ivan Fratric
<http://signal.ee.bilkent.edu.tr/defevent/papers/cr1269.pdf>
2006-04-24

[14] CCTV scanned for criminal faces, BBC

http://news.bbc.co.uk/1/hi/england/west_yorkshire/3605296.stm
2006-04-06

[15] West Yorkshire police

<http://www.westyorkshire.police.uk/section-item.asp?sid=6&iid=111>
2006-04-06

[16] Wikipedia

http://en.wikipedia.org/wiki/Closed-circuit_television
2006-04-06

[17] Twins crack face recognition puzzle, CNN

<http://www.cnn.com/2003/TECH/ptech/03/10/israel.twins.reut/>
2006-04-18