

Irisigenkänning som metod för biometrisk autentisering

Helena Raaby
helra092@student.liu.se

Andreas Johansson
andjo960@student.liu.se

TDDC03 Informationssäkerhet
Linköpings Universitet
Projektnummer 014

April 2004

Handledare

Kristin Anderson
Fredrik Claesson

Sammanfattning

Denna rapport behandlar biometrisk autentisering med hjälp av irisigenkänning, hur detta går till och hur detta används inom flygbranschen och bankvärlden. Säkerhetsproblem och skydd mot dessa tas också upp. Irisigenkänning är enligt oss ett av de bästa sätten att biometriskt autentisera användare.

1. Inledning

1.1. Bakgrund

I dagens samhälle ställs allt högre krav på säkerhet. Detta har lett till att man inom allt fler områden inom samhället testar biometrisk identifiering. Till exempel har man på flygplatser, speciellt efter den 11:e september 2001, börjat införa kontroller som använder sig av biometrisk teknik. Bland dessa olika tekniker har identifiering med hjälp av iris i ögat visat sig vara en av de effektivaste metoderna.

1.2. Syfte

Syftet med denna rapport är att ge en introduktion till hur autentisering med hjälp av iris fungerar och hur det används i verkligheten idag. En bild av vilka framtida tillämpningar som tekniken kan komma att användas till tas också upp.

1.3. Frågeställning

- Vad innebär irisgenkänning och hur fungerar det?
- Vilka säkerhetsproblem finns?
- Vad finns det för verkliga system och hur fungerar de?
- Vilka framtida användningsområden finns för irisgenkänning?

1.4. Metod

Rapporten baseras på en litteraturstudie då tillgång till ett fysiskt system saknas. Både artiklar med en vetenskaplig grund och artiklar av mer populär-vetenskaplig karaktär har studerats.

2. Introduktion till irisigenkänning

2.1. Historik/bakgrund

Informationsflödet i dagens samhälle ökar ständigt och framförallt sättet som transaktioner mm utförs på förändras. Detta sker inte längre bara med papper och penna eller ansikte mot ansikte utan mer och mer på elektronisk väg, vilket medför att behovet av snabb och säker teknisk identifiering och verifiering av användare ökar. Tidigare har det huvudsakligen funnits två identifieringsgrenar: kunskapsbaserad och attributbaserad ("något du kan", till exempel lösenord och "något du har", till exempel en nyckel eller ett magnetkort). Generellt sett så kan inte dessa system se skillnad på en person som verkligen är berättigad och en bedragare som listat ut lösenordet eller stulit nyckeln. [1]

Biometrisk teknik är metoder som känner igen personer utifrån fysiska och beteendemässiga karaktärstiska. Exempel på sådana är fingeravtryck, talet/rösten, ansiktet, handskrivna signatur, handgeometri, vener (blodflöde) i handleden, näthinnan och iris. Tidigare har biometri nästan uteslutande används för att identifiera brottslingar och för fängelsesäkerhet, men i och med att tekniken utvecklas har det blivit tillräckligt billigt och noggrant för att börja användas på en bredare kommersiell marknad, t.ex. vid ekonomiska transaktioner och inpasseringssystem. [1]

Ett biometriskt system är alltså ett slags mönsterigenkänningssystem. Det finns två huvudsakliga användningsområden. Biometrisk identifiering då man identifierar en människa utifrån en databas med personer som är kända för systemet, svarar på frågan "Vem är jag?". Biometrisk identitetsverifikation verifierar en påstådd identitet, svarar på frågan "Är jag den jag utger mig för att vara?". [1]

Irisigenkänning är den mest lovande av de olika biometriskteknikerna. Det man koncentrerar sig på är den färgade ringen som omger pupillen i det mänskliga ögat. Näst efter DNA är irisen det mest unika kännetecknet på människokroppen. Till och med enäggstvillingar har olika irisar. [1]

Irisigenkänningstekniken kombinerar optiskt datorseende, mönsterigenkänning, och statistisk slutledning. Syftet är att i realtid, med hög säkerhet, identifiera en person med hjälp av analys av det mönster som är synligt inuti ett ögas iris på ett visst avstånd. [2]

De stora användningsområdena av den här tekniken har hittills varit ersättning för pass (automatiserad gränsövervakning), flygplatssäkerhet och tillträdeskontroll till begränsade områden, databastillgång och att logga in på en dator, tillträde till byggnader, sjukhustillämpningar som till exempel mamma-barn matchning på förlossningsavdelningar. [2]

I Storbritannien håller man på att överlägga om irisigenkänningstekniker ska börja användas i samband med ID-kort och pass. Flera flygplatser världen över har installerat dessa system för passagerar- och immigrationskontroll. [2]

2.2. Fördelar/nackdelar

Fördelarna med irisigenkänning är klart många fler än nackdelarna. Om man börjar med att titta på biometrisk teknik i allmänhet så är de mycket säkrare och i vissa avseenden mer användarvänliga än lösenord, nycklar mm. Biometri är mer bundet till en särskild individ, man kan inte ge bort, tappa bort, stjäla, glömma bort eller lätt lista ut den biometrisk datan. Användaren slipper komma ihåg ett svårt lösenord eller komma ihåg att ta med sig ett inpasseringskort. [3]

Fördelarna med att analysera irisen jämfört med andra biometrier är för det första att den är så unik för varje person. Detta gör att tillförlitligheten blir mycket hög. Vid irisigenkänning existerar inte heller problemen med smuts, sår och ärr som när man till exempel använder sig av fingeravtryck. Irisen är ett organ som visserligen är synligt men ändå väldigt skyddat både från smuts och skador. [1]

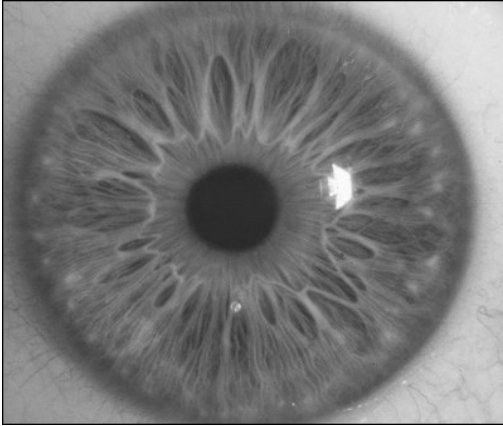
Användarna har inte heller samma associationer till brottslingar som när det gäller fingeravtryck, vissa kan känna sig illa till mods om de måste ge sitt fingeravtryck. Andra problem med till exempel handflateavtryck är att användare inte gillar att sätta sin hand på samma ställe där massor av andra händer varit, är inte heller nåt problem vid irisigenkänning eftersom man använder sig av videokameror som filmar på (i och för sig ofta kort) avstånd. [1]

Andra fördelar med irisigenkänning är att det krävs förhållandevis billig utrustning och mängden data som behöver lagras för varje person är mycket liten, vilket gör att systemen passar bra för storskaliga projekt med många användare. [1]

Exempel på nackdelar är att användare kan vara lite skeptisk till att få nåt som granskar ögat. De är rädda för strålning och att ögat ska bli skadat eftersom det är så känsligt. Ett av de större problemen

med biometri i allmänhet är att om en persons biometriska data skulle bli stulna så är det stulet för resten av livet, eftersom det inte går att byta iris på samma sätt som ett lösenord. [1]

3. Teknisk beskrivning



Figur 1: Iris [4]

3.1. Iris

Iris tillhör den grupp av biometrier som kan uppfattas från distans. Till skillnad från andra biometrier inom samma grupp så är iris den som bäst behåller sina egenskaper över en längre tid. Till exempel ansiktet, som är en populär biometri inom denna grupp, förändras som vi alla vet mycket med åldern. Iris börjar däremot ta sin form från och med två månader efter födseln, och antar sin slutgiltiga form efter cirka ett år. Iris har även en rent statistisk fördel gentemot andra biometrier då den kan variera mer mellan olika personer. Man räknar med att skillnader mellan olika irisar kan uppfattas på upp till en meters avstånd. [5]

3.2. Algoritm

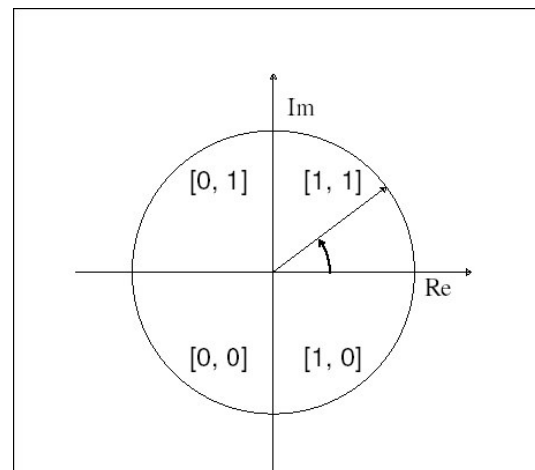
Algoritmen vi valt att ta upp är utvecklad av Johan Daugman som är verksam vid universitet i Cambridge. Hittills har alla kommersiellt använda system med irisigenkänning använt sig av just denna algoritm. Exempel på företag och organisationer är British Telecom, US Sandia Labs, UK National Physics Laboratory, NCR, Oki, IriScan, Iridian, Sensor och Sarnoff. För mer information om dessa försök, se slutet av detta avsnitt. Nedan ges en överblick på hur denna algoritm fungerar. [5]

3.2.1. Fotografering och filtrering

Steg ett innebär att utifrån vad en kamera fångar på bild filtrera ut det intressanta, det vill säga irisen och pupillen. Här används en kamera som fångar monokroma bilder där irisen har minsta diametern 70 pixlar. Ett problem här är att fånga en likadan bild varje gång (subjektet måste befinna sig på samma avstånd från linsen varje gång). Detta kan antagligen lösas genom att ha en kamera som justerar sig själv, men man har i de flesta försök valt att låta subjektet själv, med hjälp av speglar alternativt video, ställa sig i rätt position. När sedan bilden är tagen använder man sig av filter (exakt hur kommer vi inte att gå in på) för att dels få bort skräp som till exempel ögonfransar ur bilden och dels för att få fram endast iris och pupill. [5]

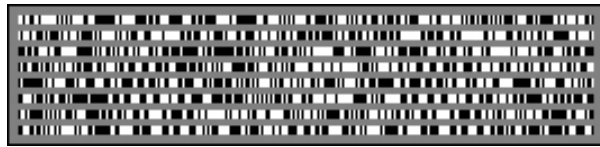
3.2.2. Extraktion av data

Nästa steg är att utifrån den tagna bilden extrahera data som sedan kan lagras i exempelvis en databas. Här använder sig algoritmen av något som kallas "2D Gabor wavelets" för att projicera irisen på det imaginära talplanet. Hur denna projicering går till kommer inte heller gås in på närmre i denna rapport, då det ligger utanför rapportens ramar. Den som är intresserad av hur detta går till kan läsa vidare i [6]. Denna projicering resulterar sedan i ett antal vektorer. Varje vektor kan ses som ett komplext tal, och argumentet på detta tal avgör var (i vilken kvadrant) i det imaginära talplanet vektorn ligger. Beroende på placeringen tilldelas vektorn två stycken statusbitar (se figur 2). Detta upprepas sedan för alla vektorer och vektorernas statusbitar kombineras sedan ihop till en kod om totalt 2048 bitar.



Figur 2: Imaginära talplanet, med respektive kvadrants statusbitar [7]

En grafisk representation (en så kallad "bitström") av denna iriskod återfinns i figur 3. [6]



Figur 3: Iriskod [8]

3.2.3. Jämförelse

När det gäller att jämföra två irisar med varandra är det alltså iriskoden som jämförs. I och med att iriskoden är representerad binärt tillämpas en metod för jämförelse mellan två binära tal, Hammingavstånd. Hammingavståndet mellan två binära tal är skillnaden i bitarna, och med skillnaden menas antalet bitar som skiljer sig mellan talen. Det fås genom att applicera XOR på varje par av bitar från de två iriskoderna. Det leder alltså till en nolla om de två bitarna är lika och en etta om de skiljer sig åt. Sedan summeras antalet bitar som skiljer sig. Ett stort Hammingavstånd fås om irisarna skiljer sig mycket åt, och tvärtom om irisarna är väldigt lika. Hur stort Hammingavstånd som systemet tillåter för att verifiera en iris som korrekt blir alltså systemets så kallade tröskelvärde. [6]

3.3. Prestanda

Med denna algoritm tar varje iris, efter att data extraherats, upp 256 bytes av lagringsutrymme. Som ett exempel nämns att med 300Mhz Sun Workstation kan, med den jämförelseprocess som implementerats, 100 000 jämförelser göras på en sekund. Som nämnt ovan har denna algoritm används i en rad kommersiella system och dessa visar en väldigt imponerande prestanda när det gäller "False Match Rate", alltså irisar som verifierats felaktigt, se Tabell 1. Dock finns ingen information om algoritmens "False Non Match Rate", personer med tillträde som nekats, i den referens vi haft tillgång till. [5]

4. Tillämpningar

När säkerhetskraven ökar börjar fler och fler att titta på biometriska system. Inom flygbranschen har, framförallt efter attacken den 11 september 2001, flera flygplatser testat system baserade på biometri i allmänhet och irisigenkänning i synnerhet. Även inom bankvärlden har tester börjat genomföras med biometriska system för identitetskontroll. Vi har tittat på tre olika försök med irisigenkänning; flygplatsen i Amsterdam som var först i världen med irisigenkänning, SAS i Sverige som fram till och med april i år genomfört tester, och sist har vi tittat på tillämpningar inom bankvärlden där man bland annat i Australien och Storbritannien börjat använda sig av irisigenkänning på uttagsautomaterna.

Organisation	Antal jämförelser	Felaktiga verifieringar
Sandia Labs, USA (1996)	19 701	0
British Telecom, UK (1997)	222 743	0
Sensor Corp, USA (2000)	499 500	0
Joh.Enschedé, NL (2000)	19 900	0
Eye Ticket, USA (2001)	300 000	0
National Physics Lab, USA (2003)	2,73 milj.	0
J. Daugman, UK (2003)	9,1 milj.	0
Iridian Technologies, USA (2003)	984 milj.	0

Tabell 1: Testresultat [9]

4.1. Amsterdams flygplats

Försöken i Amsterdam har pågått sedan oktober 2001, och målen med försöken är dels ökad säkerhet men även minskad betjäningstid i passkontrollerna. Hittills har tjänsten erbjudits till resenärer som innehar ett "European Economic Area passport" (EU-länderna, Norge, Island och Liechtenstein) och som är medlemmar i flygplatsens "privium"-klubb (klubb för de som reser mycket och som värdesätter det lilla extra). I april 2002 var det cirka 2500 personer som var registrerade användare av systemet. [10]

Systemet är uppdelat på två faser. Den första fasen är kvalificering och registrering av användare. Processen involverar passkontroll, bakgrundskontroll och irisskanning. Den skannade irisen krypteras och placeras på ett smartkort. Denna fas tar ungefär 15 minuter att genomföra. Den andra fasen går ut på att identifiera och verifiera resenären när denna ska passera in till området där respektive gate finns. Resenären ställer sig framför irisskannern och sätter sedan i sitt smartkort med irisinformationen i läsaren (se figur 4). [10]



Figur 4: Irisskanner vid Amsterdams flygplats [11]

Om matchningen lyckas, tillåts resenären passera in till det område där resenärens gate finns. Om den misslyckas, vilket antingen beror på att själva verifieringen misslyckas eller att resenären helt enkelt inte finns med i systemet, skickas istället resenären längst fram i kön för den vanliga manuella passkontrollen. Den automatiserade kontrollen tar i vanliga fall ungefär 10-15 sekunder. [10]

I det här systemet har man alltså valt att lagra irisinformationen på smartkort istället för i en central databas. På detta vis slipper resenärerna dela med sig av sin irisinformation och vissa integritetsproblem undanröjs. Det är annars ett av de problem som finns med biometri i allmänhet; om en individs iris till slut finns lagrad i ett stort antal databaser världen över som dessutom använder samma algoritm för igen-

känning, blir det enkelt att göra kopior. Smartkorten använder sig, som nämndes ovan, av kryptering och har plats för information om ytterligare en biometri för framtida bruk. Anledningen till att iris blev den biometrin som används beror dels på att iris är en av de säkraste biometrierna, men en stor anledning var också att det är en teknik som inte kräver någon fysisk kontakt. Frånvaron av fysisk kontakt innebär att vissa hygieniska orosmoment försvinner, och då krävs det heller ingen extra tid till renhållning av systemet. När det gäller prestanda så klarar systemet av ungefär fyra till fem personer per minut och gör det i stort sett utan misstag. Målet, att "möta resenärernas krav på säkerhet och hastighet", anses vara uppnått. [10]

4.2. SAS

SAS (Scandinavian Airlines) har sedan november 2003 genomfört tester av biometriska system vid incheckning och ombordstigning. Anledningarna var två. Den första för att precis som i Amsterdam öka säkerheten och förenkla resan [12]. Den andra för att förbereda sig på framtida säkerhetskrav, som säkerligen inkluderar biometri [12]. Sista delen av testerna inkluderar irisigenkänning, och ska vara klara under april i år (2004). Testerna har genomförts på flygplatsen i Umeå. Systemet som används liknar i stora drag det som använts i Amsterdam, alltså irisskanner och smartkort. [13]

4.3. Uttagsautomater

I Australien har kostnaderna för identitetsstöld uppskattats till 4 miljarder dollar per år. Brott som är kopplat till någon form av identitetsstöld ökar med 50 procent per år. Många av dessa brott är stöld från privatpersoners bankkonton via bankernas uttagsautomater. Förslag till skydd mot detta är att använda biometrisk information som är mycket svårare att förfälska. Om fem år ska bankerna i Australien vara igång med uttagsautomater baserade på irisigenkänning (sagt 2003). [14]

I Storbritannien finns däremot en viss skepsis till dessa uttagsautomater. Försök med denna teknik resulterade i följande; bankerna gillade det, kunderna älskade det, men det blev aldrig ekonomiskt försvarbart:

- Kostnaden att installera tekniken överskred kostnaden för bedrägerierna
- Att registrera varje kund skulle vara tidskrävande, och utrustning skulle behöva finnas på varje bankkontor

- Om en bank börjar använda sig av tekniken, finns problemet fortfarande kvar hos de banker som tillämpar den gamla tekniken med pinkod

[15]

5. Säkerhet

5.1. Attacker och skyddsåtgärder

De attacker vi tar upp här är så kallade ”replay attacks”, vilket är attacker där bedragaren vet hur systemet fungerar och använder den kunskapen i sin attack. Vi antar här att bedragaren dels har tillgång till den biometriska informationen och vet hur indata ska genereras till systemet. Exempel på attacker kan vara ett utskrivet foto av en iris eller bärbar bildskärm med en iris som hålls upp framför skannern. [16]

Skydd mot dessa attacker kan delas in i tre kategorier:

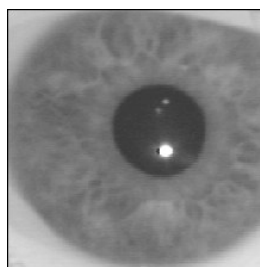
- skydd baserat på passiva egenskaper
- skydd baserat på reaktiva egenskaper
- skydd baserat på aktiv inblandning av användaren

[16]

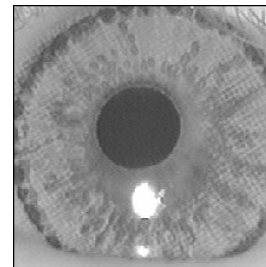
5.1.1. Passiva egenskaper

Dessa skyddsåtgärder bygger på utnyttjande av vetenskapen om hur korrekt indata ska se ut. Många tror att man kan lura en irisskanner genom att imitera en iris med hjälp av en kontaktlins. Dock så visar figur 5 och 6 att en iris på en kontaktlins skiljer sig markant från en äkta iris. [16]

En annan skyddsåtgärd går ut på att identifiera ofrivilliga rörelser i ögat. Även om användaren försöker hålla blicken stilla så rör sig ögat ändå. Detta skyddar mot en bedragare som helt enkelt har skrivit ut en iris på ett papper då den garanterat är helt stilla. [16]



Figur 5: Äkta iris [17]



Figur 6: Imiterad iris på kontaktlins [17]

5.1.2. Reaktiva egenskaper

Här använder man sig av extra hårdvara för att producera stimuli till ögat och då kunna observera ofrivilliga reaktioner. Detta kan till exempel bygga på att ljus skickas mot ögat för att sedan mäta reflektioner på näthinnan alternativt hornhinnan. En annan möjlighet är att mäta pupillens fysiska reaktioner på ljus. [16]

5.1.3. Aktiv inblandning av användaren

Dessa skyddsåtgärder liknar de där man utnyttjar de reaktiva egenskaperna, men skillnaden är att man istället observerar frivilliga reaktioner. Ett alternativ är att be användaren rikta blicken mot förutbestämda eller slumpmässigt utvalda punkter. Ett annat alternativ är att be användaren godtyckligt röra ögat för att sedan mäta de specifika rörelser som uppstår i ett öga i rörelse. [16]

5.2 Kostnader för biometrisk imitation

Att fastställa en exakt kostnad går knappast då det går att spendera hur mycket pengar som helst på att tillverka en kopia. Däremot kan man ställa kostnaderna för kopior av olika typer av biometrier i relation till varandra. Skillnad kan även göras mellan statiska och dynamiska biometrier. Statiske inkluderar händer, ansikte och iris. Exempel på dynamiska biometrier är röst, till viss del signaturer och sättet att skriva på ett tangentbord. En jämförelse av kopieringskostnaden med mera mellan olika statiska biometriska tekniker presenteras i följande tabell (Tabell 2). [16]

Biometri	Sensor/metod	Svårighetsgrad att komma över datan	Kopieringskostnad
Fingeravtryck	Optisk	Väldigt låg, fingeravtryck finns överallt	Väldigt låg
Ansikte	Optisk, infraröd	Låg, kan räcka med foto ur en tidning	Låg
Iris	Optisk, infraröd	Mellan, visst samarbete krävs	Mellan till hög
DNA	Elektrofores	Låg, räcker med t.ex. hårstrå	Hög
Näthinna	Sammanhängande ljus	Hög, samarbete krävs	Hög till väldigt hög

Tabell 2: Kopieringskostnader [18]

6. Diskussion och slutsatser

Biometri är helt klart ett av de säkraste sätten att autentisera användare på. Av alla biometriska tekniker tycker vi att irisigenkänning framstår som en av de, eller kanske den, bästa. Gentemot andra biometriska tekniker har den flera fördelar. Iris är till skillnad mot andra igenkänningsorgan ett internt organ som därmed är skyddat mot yttre påverkningar och behåller därmed sitt utseende och form under hela livet om inget oförutsett inträffar. Irisen går dessutom att registrera på distans, vilket innebär att fysisk kontakt med utrustningen undviks och därmed även eventuella hälsorisker vid dålig renhållning. Den datamängd som krävs vid lagring av en iris är relativt liten (256 byte med Daugmans algoritm) och vilket gör att metoden passar utmärkt för stora populationer. En av de få nackdelar vi kan komma på med irisigenkänning är att användare kan uppleva det som obehagligt när ögat ska registreras av skannern för att de tror att det ska påverka ögat negativt. Detta är dock inte sant och det enda som krävs är information till osäkra användare.

När det gäller säkerhetsaspekter på irisigenkänning tycker vi att de är ganska generella för biometriska tekniker i allmänhet. Ett exempel är att om irisdatan blir stulen går den inte att byta ut på samma sätt som ett lösenord. Många är därför oroliga när deras irisdata sparas i en stor databas. I senare tillämpningar tillämpar man istället smartkort där användarens data sparas för att användaren själv ska ha kontroll över sina irisdata. Andra säkerhetsproblem som till exempel att en bedragare använder sig av en avbildning för att lura systemet finns det skydd emot, men det krävs ofta extra hårdvara vilket i sin tur gör systemet dyrare. Generellt sett är dock systemen väldigt säkra.

I de tillämpningarna av irisigenkänning vi tittat på har systemen generellt sett fungerat mycket bra. Inom flygbranschen har vi sett att systemen mycket väl kan ersätta den vanliga manuella passkontrollen. På bland annat Amsterdams flygplats är man framförallt mycket nöjd med hur systemet ökat effektiviteten. När det gäller tillämpningar inom bankvärlden är man däremot mer skeptisk till resultaten. Ur ren säkerhets-synpunkt har det fungerat förträffligt, men det har visat sig att kostnaden för systemen vida överstigit kostnaden för bedrägerierna. Detta beror på det stora antalet stationer som kräver ny utrustning.

Vi tror att i framtiden kommer biometri i allmänhet och irisigenkänning i synnerhet att tillämpas i fler sammanhang och på fler platser. I informations-samhällets jakt på säkerhet kommer säkerligen iris-

igenkänning att ha betydande roll. Det vi kan se utifrån de tillämpningar vi har tittat på i denna rapport är att det framförallt lämpar sig för system där antalet stationer för igenkänning är relativt få, men däremot får det gärna vara stora mängder användare. Denna grupp av tillämpningar inkluderar till exempel flygplatser. Däremot inser vi att irisigenkänning inte lämpar sig för system där antalet stationer blir stort som till exempel när det gäller uttagsautomater. Än så länge är biometriska system ganska dyra, men om ett biometriskt system ska användas tycker vi att irisigenkänning är det bäst lämpade.

Referenser

- [1] Braghin Chiara, University of Helsinki, Biometric Authentication,
<http://citeseer.ist.psu.edu/cache/papers/cs/21533/http:zSzzSzwww.cs.helsinki.fizSzuzSzasokanzSzdistseczSzdocumentszSzbraghin.pdf/biometric-authentication.pdf/>
- [2] Daugman John, University of Cambridge, Introduction to iris recognition
http://www.cl.cam.ac.uk/users/jgd1000/iris_recognition.html
- [3] Meeting your personal identification challenges, ROFIN,
http://www.rofin.com.au/pr_bssfaq.html
- [4] (Figur) Daugman John, University of Cambridge,
<http://www.cl.cam.ac.uk/users/jgd1000/sampleiris2.jpg>
- [5] Daugman John, University of Cambridge, How iris recognition works, 2004,
<http://www.cl.cam.ac.uk/users/jgd1000/csvt.pdf>
- [6] Daugman John, University of Cambridge, Demodulation by complex-valued wavelets for stochastic pattern recognition,
<http://www.cl.cam.ac.uk/users/jgd1000/complex.pdf>
- [7] (Figur) Daugman John, University of Cambridge,
<http://www.cl.cam.ac.uk/users/jgd1000/math.html>
- [8] (Figur) Daugman John, University of Cambridge,
<http://www.cl.cam.ac.uk/users/jgd1000/iriscode.gif>
- [9] Daugman John, University of Cambridge,
<http://www.cl.cam.ac.uk/users/jgd1000/iristests.pdf>
- [10] IBM looks airline security in the eye, 2002.
<http://www.cl.cam.ac.uk/users/jgd1000/ibm.html>
- [11] (Figur) IBM,
<http://www.ibm.com/press/images1/7-19a.gif>
- [12] Ögat i fokus på SAS-resenärer i Umeå, 2004, Luftfartsverket,
<http://www.lfv.se/site/airports/umea/news.asp?docID=12941>
- [13] Loth Hammar, Nästa steg i SAS biometritest, 2004.
http://biotech.idg.se/ArticlePages/200402/26/20040226112334_BIO/20040226112334_BIO.dbp.asp
- [14] Iris recognition helps to prevent ID fraud, 2003.
<http://www.smh.com.au/articles/2003/02/27/1046064145169.html>
- [15] Forms of access,
<http://www.zdnet.com.au/news/security/0,2000061744,20266478-2,00.htm>
- [16] Ernst Jan, Iris Recognition: Counterfeit and Countermeasures, 2002. <http://www.iris-recognition.org/counterfeit.htm>
- [17] (Figur) Daugman John, University of Cambridge,
<http://www.cl.cam.ac.uk/users/jgd1000/countermeasure.gif>
- [18] Ernst Jan, Iris Recognition: Counterfeit and Countermeasures, 2002. <http://www.iris-recognition.org/counterfeit.htm>