

TDDC03 Projekt, våren 2006

MULTIMODAL BIOMETRI

Petter Olsson, petol880@student.liu.se
Fredric Eliasson, freel252@student.liu.se

Handledare: Viiveke Fåk

Sammanfattning

Denna artikel ger en introduktion till multimodal biometri, vilka fördelar respektive nackdelar som det medför och vilka eventuella tillämpningar multimodala system har. I artikeln undersöks också vilka möjliga attacker som finns mot de multimodala systemen och hur de förhåller sig gentemot system som bara använder sig av ett biometriskt kännetecken.

Två existerande system har undersökts. Ett som framförallt är konstruerat som ett identifikationssystem för den kommersiella marknaden, samt ett verifikationssystem från forskningsvärlden. Detta för att ge känsla för vad det finns för system och hur dessa kan vara utformade.

Resultaten av undersökningen visar att multimodala system är mer flexibla än biometriska system som bara använder ett kännetecken. Det går att öka tillgänglighet, prestanda och säkerhet. De största nackdelarna är att priset och komplexiteten är högre för multimodala system.

1. Inledning

1.1 Bakgrund

Biometri börjar bli mer och mer använt och marknaden växer fort. Enligt International Biometric Group förväntas marknaden för biometri växa med nästan tre gånger till 2010 [13]. Efter terrorattackerna mot World Trade Center 2001 så har krav på säkrare pass kommit framförallt från USA. Biometriska säkerhetslösningar är med andra ord ett aktuellt och intressant ämne idag.

I denna artikel ska multimodal biometri undersökas. Definitionen av multimodal biometri är att två eller fler enskilda biometrier kombineras. Multimodal biometri är

något som är på utvecklingsstadiet och förväntas ge högre tillförlitlighet och säkerhet, men till ett pris av högre kostnader och längre beräkningstider.

1.2 Syfte

Syftet med artikeln är att undersöka multimodala biometriska system och hur de skiljer sig från system där man använder sig av ett enskilt biometriskt kännetecken. Framförallt ska följande frågor behandlas och besvaras:

Vad är multimodal biometri och hur fungerar det? Hur kan system vara utformade och vad skiljer ett system som använder en biometri jämfört med ett multimodalt system? Vilka fördelar respektive nackdelar introduceras med multimodala system? I vilka tillämpningar kan multimodala system vara passande?

1.3 Metod

Metoden som använts för att framställa artikeln är litteraturstudier. På grund av projektets omfattning har det inte varit möjligt att göra några experiment för att generera egna resultat utan den byggs helt på andras studier.

1.4 Avgränsningar

Artikeln kommer inte att beskriva alla typer av biometrier, inte heller alla kombinationer av dessa. Detaljerade förklaringar av algoritmer och matematiska funktioner för matchning och sammanslagning av olika biometrier kommer inte heller behandlas, utan endast enklare förklaringar av vilka metoder som finns.

2. Biometri

Biometri är en fysisk eller beteendemässig egenskap eller kännetecken som skiljer mellan olika individer. Vi använder detta dagligen för att känna igen andra människor genom till exempel röst eller ansikte. Biometri

kan användas för att verifiera eller identifiera individers identiteter med hjälp av datorer. Till de vanligast använda biometrierna för automatisk igenkänning hör fingeravtryck, ansikte, hand, röst och iris. För att kunna jämföra olika biometriska kännetecken för automatiserad igenkänning talar man om fyra egenskaper som är viktiga [1].

- Allmängiltig, alla ska ha det.
- Karaktäristisk, de ska vara tillräckligt olika för att man ska kunna skilja på två individer.
- Beständig, de ska inte ändras så fort med tiden.
- Mätbar, det ska gå att mäta på ett kvalitativt sätt.

Biometri kan användas för att ersätta lösenord och pin-koder. Fördelen är att man slipper många problem med lösenord. Lösenord går att gissa, kan glömmas bort och stjälas om de finns dokumenterade (vilket nästan är en nödvändighet för starka lösenord). Biometri är svårt att förfälska, kan inte glömmas bort och mycket svårt att "stjäla". Anledningen till att använda biometri istället för konventionella metoder som lösenord och passerkort är framförallt ökad säkerhet och smidighet [1].

3. Biometriska system

Ett biometriskt system används för att samla in och känna igen biometriska kännetecken. Man skiljer mellan *verifikationssystem* och *identifikationssystem*. I ett verifikationssystem uppger användaren vem denne är och man matchar mot denna individs sparade mall. I ett identifikationssystem matchar man mot alla sparade mallar i databasen för att försöka fastställa individens identitet [1]. I artikeln kommer termen igenkänning användas när skillnad mellan verifikation och identifikation inte önskas.

3.1 Systemacceptans

I systemet kan man ställa in acceptansen för att ta beslut om en individ ska accepteras eller nekas av systemet. Detta görs med hjälp av ett tröskelvärde som styr hur åtkomligt och säkert systemet blir och beskrivs av följande variabler:

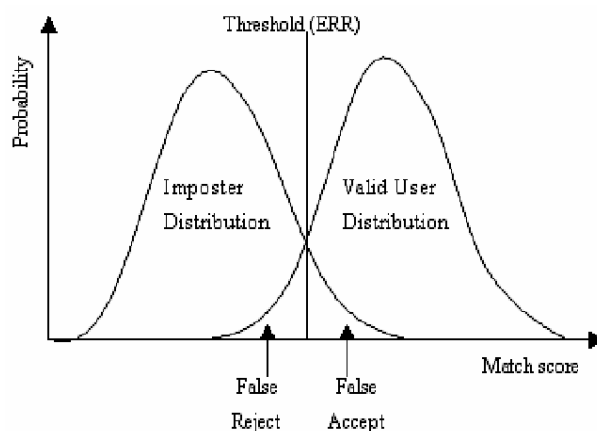
FRR (False Rejection Rate); är andelen behöriga individer systemet avvisar.

FAR (False Acceptance Rate); är andelen obehöriga individer som accepteras av systemet.

GAR (Genuine Acceptance Rate, $1 - FRR$); är andelen individer systemet accepterar.

FER (Failure to Enroll Rate); är andelen mallar som lästs in med för dålig kvalitet för att sparas i databasen.

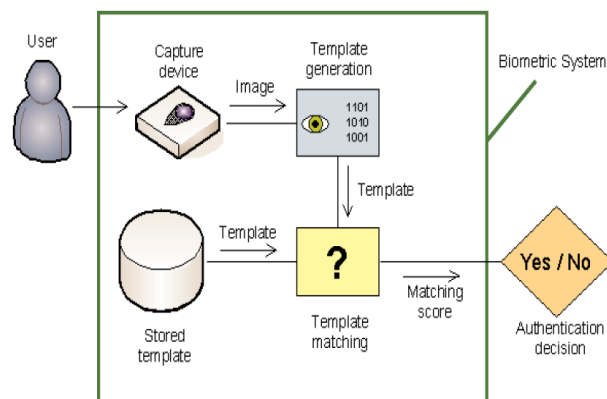
EER (Equal Error Rate); är där FRR och FAR är lika stora.



Figur 1: Relation mellan FAR, FRR och ERR [14]

Ofta vill man att systemet ska ligga nära EER för att få en så bra acceptans som möjligt. Höjer man tröskelvärdet så får man högre säkerhet (lägre FAR), men det ger sämre åtkomlighet (högre FRR). Önskar man en ökad tillgänglighet så sänker man tröskelvärdet, vilket får en motsatt effekt på acceptansvariablerna [1].

3.2 Ett typiskt biometriskt system



Figur 2: Ett biometriskt system [3]

3.2.1 Insamlingsenhet

Insamlingsenheten (fig. 2: capture device) består av en eller flera sensorer för att samla in avtryck, bilder, ljud etc. Utdata från insamlingsenheten är information bestående av biometrisk rådata som sedan skickas till mallgenereringsenheten. I insamlingsenheten finns inga skillnader mellan verifierings- och identifikationssystem [3].

3.2.2 Mallgenereringsenhet

Mallgenereringsenheten (fig. 2: template generation) bearbetar den biometriska datamängden och skapar en representation av den biometriska rådatan. Mallen som genereras innehåller all relevant information systemet behöver, men är mindre än rådatan från sensorerna i inmatningsenheten. Det sker en komprimering av rådatan, som innehåller mycket brus och annan för systemet onödig information. I mallgenereringsenheten finns inga skillnader mellan verifikations- och identifikationssystem.

Innan mallen skickas vidare kontrolleras kvaliteten. Är den för dålig för att matchas eller sparas i databasen (vid enrolling) måste inläsningen göras om [3].

3.2.3 Matchningsenhet

Matchningsenheten (fig. 2: template matching) tar emot mallen från mallgenereringsenheten. I ett verifikations-system kontrolleras mallen mot den sparade på databasen för att se hur väl de stämmer överrens. I ett identifikationssystem matchas den genererade mallen mot alla mallarna i databasen för att hitta tillräckligt bra matchningar [3].

3.2.4 Beslutsenhet

Beslutsenheten (fig. 2: Authentication decision) tar emot ett resultat från matchningsenheten och bestämmer med hjälp av acceptanströskelvärde om systemet ska acceptera individen eller inte [3].

3.2.4 Databas

Ofta sparas alla insamlade mallar i en stor databas (fig. 2: stored template), som ofta är i nära anslutning till systemet, men kan också vara central och nätverksbaserad. I verifikationssystem kan mallarna också vara sparade på ett så kallat smart kort, som individen bär med sig. Matchningen sker då antingen genom att mallen hämtas in i systemet från individens kort eller direkt på kortet [3].

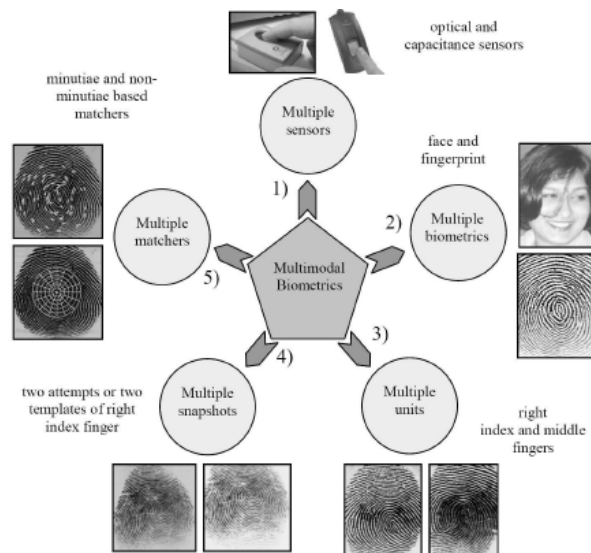
4. Multimodala biometriska system

Med multimodal biometri avses några av följande kombinationer:

- 1) Olika typer av sensorer som samlar data från *en* biometri.
- 2) Flera *olika* biometrier används, till exempel fingeravtryck och röstigenkänning.
- 3) Flera sensorer används, en för varje biometri.
- 4) Flera olika prov tas från en och samma sensor, till exempel både vänster och höger iris.

- 5) Samma karaktärsdrag tas flera gånger från en individ, till exempel att man tar flera fingeravtryck från samma finger.

Man använder sig av flera olika representationer och matchningsstrategier (kombineringsfunktioner) för samma biometri.



Figur 3: Multimodal biometri [5].

Fördelen med att använda flera kännetecken är att man kan få ett mer flexibelt system. Det kan bli säkrare eller smidigare beroende på hur man utformar det. Säkrare genom att FAR minskas utan att påverka FRR allt för mycket. Systemet kan bli smidigare genom att man konstruerar det så att FRR minskar, men också genom att individer som av någon anledning inte kan använda ett visst kännetecken fortfarande kan använda systemet. Detta genom att inte kräva att den individen måste lämna just det kännetecknet. Exempelvis så har man funnit att ca 2 % av befolkningen saknar användbara fingeravtryck och man kan då i dessa fall använda någon annan metod för igenkänning [1] [11].

En annan fördel med multimodala system är att man i identifikationssystem kan öka prestandan eftersom man får en effektivare klassifikation när man använder sig av flera kännetecken och därmed ett mindre antal mallar att söka bland [1].

4.1 Prestanda

Prestanda innebär att man ska uppnå en acceptabel precision, hastighet och robusthet. Den snabba utvecklingen av datorsystem har gjort att det blir lättare att hantera och implementera biometriska system [6][8]. Det finns mycket som kan påverka prestandan, till exempel måste kvalitén på sensorer vara hög för att man

ska kunna göra korrekta beräkningar. Är den avlästa informationen brusig så kan den beräknade matchningspoängen inte vara pålitlig [10].

Det har visat sig att man ökar prestandan på systemet om man tar samma fingeravtryck två gånger [5]. I många fall kan man öka prestandan genom att dra ner på att man kontrollerar att matchningen kommer från en levande individ. En viss nivå av övning och utbildning av det biometriska systemet kan initialt vara avgörande för prestandan.

4.2 Kombinerings av data

Det är viktigt att man har en bra strategi för hur man kombinerar insamlad data i ett multimodalt system. Desto tidigare i processen man slår samman informationen gör att man får bättre resultat, på grund av att information från sensorerna då ännu inte skalats bort. Detta är tillmötesgående att genomföra om karaktärsdragen skiljer sig mycket åt [5].

Tidigt i processen ser biometrisk originaldata från olika biometrier (t.ex. iris och fingeravtryck) mycket olik ut, vilket gör att det blir svårt att kombinera ihop. Däremot kan data från liknande eller samma biometri till exempel fingeravtryck från två fingrar lättare kombineras ihop tidigt i processen [9].

Om kombineringsen sker mot slutet så kan ett multimodalt system bli stelt på grund av att det inte finns så mycket information kvar och det blir då svårt att uppnå en högre säkerhet än det kännetecken som enskilt har högst säkerhet [9].

4.2.1 Arkitektur

Ett multimodalt system kan arbeta på tre sätt: seriellt, parallellt och hierarkiskt. Den seriella modellen används för att minska mängden av biometrisk data, särskilt i stora system med många identiteter. Man kör först en klassificerare som är beräkningsmässigt effektiv för att minska mängden av biometrisk data, som måste sökas igenom. Sedan går man vidare med nästa och så vidare tills man hittar en matchning. Effekten blir att matchningsprocessen går snabbare och därmed även hela systemet. I det parallella systemet kombineras flera kännetecken samtidigt för en matchning. Den hierarkiska modellen lägger ihop olika klassificerare enligt en trädliknande modell. Denna fungerar bäst då man har väldigt många klassificerare [1].

4.2.2 Kombineringsfunktioner

Det finns flera varianter av kombineringsfunktioner så som till exempel bayesianska nätverk eller algoritmer som bygger på linjär algebra. I och med att det finns svårigheter med att kombinera på en låg nivå och man vill uppnå en högre säkerhet än biometriska kännetecknen var

för sig. Nedan följer de tre vanligaste algoritmerna när man kombinerar flera kännetecken:

Summaregel (Sum rule); använder sig av ett viktat medelvärde vars poäng genereras individuellt av modaliteterna.

Exempelvis kan man beräkna medelvärdet för två kännetecken så här:

$$S_{\text{medel}} = \frac{1}{2} (\beta s_1 + (1 - \beta) s_2)$$

s_i är poängen för respektive modalitet. β är en poäng som är viktade, det vill säga poängen kan till exempel beräknas med hjälp av träningsdata som man vet svar till. För att uppnå ett bättre resultat kan man kombinera kännetecknen på flera olika sätt.

Beslutsträd (Decision trees); använder sig av ett binärt träd där de interna noderna innehåller ja/nej frågor medan löven innehåller beslutet. För att systemet ska svara ja så jämför man insamlad biometrisk data med en mall och att den genererade poängen man får fram är över en viss tolerans. Toleransen kan fastställas genom att man tränar sin funktion med träningsdata man redan vet svaret till.

Linjära diskriminant analys; hjälper till att omvandla klassificerarna, genom att fixera de till en linjär som maximerar separationen mellan de olika klassificerarna.

Det man gör är att man projicera samlade originalmängden av biometrisk data från respektive modalitet ner på ett lägre dimensionerat rum, maximerar separationen mellan andelen obehöriga individer som accepteras av systemet (FAR) och andelen individer systemet accepterar (GAR).

Ross och Jain visar med sina experiment att summaregeln var den algoritm som ger bäst prestanda av de tre när de applicerar dem på matchnings data. De visar även att de får ett förbättrat resultat när de kombinerar ansikte och fingeravtryck på mellangenereringsnivå [10].

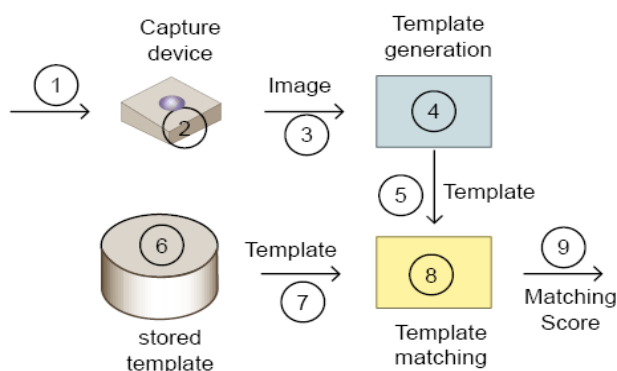
4.2.3 Viktning av olika mallar

Problem kan uppstå när man har många biometriska kännetecken och man har olika kombinationer av dessa för att ge olika säkerhetsnivåer. Detta kan öka FRR när man kräver alla kännetecken medan FAR blir oförändrat om man använder något kännetecken för att bli accepterad. Lösningen på detta är att man viktar de olika modaliteterna individuellt för att anpassa efter vilken säkerhet respektive kännetecken den har, för att hitta en acceptabel kombination mellan förtroende och tillgänglighet för de inblandade individerna [3][9].

5. Säkerhet i multimodala system

Säkerheten i multimodala system blir högre om man kombinerar resultaten från flera kännetecken med en effektiv kombineringsmetod. Attackerna mot multimodala system skiljer sig inte mot biometriska system i allmänhet. Skillnaden är att man måste ta sig förbi fler antal system, vilket ökar komplexiteten för en attack [1].

5.1 Tänkbara attacker



Figur 4: Hot i ett bietriskt system [3]

5.1.1 Imitationsattacker

Vid imitationsattacker (fig. 4: 1) försöker man imitera en individs biometriska kännetecken. Det kan göras till exempel med en inspelning av individens röst eller en kopia av ett fingeravtryck. Multimodala system där flera biometrier krävs för en igenkänning är mycket svårare att imitera, eftersom flera falska kännetecken då måste tillverkas.

För att göra systemet mindre sårbart mot imitationsattacker kan man inkludera funktionalitet för att kontrollera att det är en levande individ som interagerar med systemet. Detta kan exempelvis göras genom att kontrollera temperatur, puls, elektrisk ledbarhet eller att pupillen reagerar normalt på ljus (beror på vilken biometri som används). En annan metod som kan användas är att systemet slumpvis väljer ett kännetecken man ska lämna. Det kan till exempel vara olika röstprov i ett röstigenkänningssystem eller ett slumpvist valt fingeravtryck som ska lämnas. Då blir det mycket svårare för en förövare att attackera systemet eftersom det då inte räcker med att bara göra en kopia av ett fingeravtryck eller spela in en fras som individen säger för att säkert knäcka systemet [1][3][4].

5.1.2 Manipulation av inmatningsenheten

Inmatningsenheten (fig. 4: 2) skulle kunna modifieras så att den skickar en annan bild än den som blir inläst, exempelvis genom att någon lyckas manipulera enhetens mjukvara. Även matchningsenheten (fig. 4: 8) och enheten som genererar mallarna (fig. 4: 4) skulle kunna utsättas för denna attack.

Inmatningsenheten kan också utsättas för DoS attacker. En DoS attack eller "överbelastningsattack" går ut på att skada eller överbelasta ett system så att behöriga användare inte kan använda det.

För att skydda systemet kan man ha hårdvara, vars minne endast går att skriva en gång, för att mjukvaran inte ska kunna manipuleras. Vidare är en varaktig kontroll av systemet och dess delar en användbar metod för att skydda det mot attacker och upptäcka om något har ändrats [3][4].

5.1.3 Falska mallar

En effektiv attack mot ett bietriskt system, som använder en central databas (fig. 4: 6), är om individen som vill attackera systemet lyckas få in sin egen mall i systemet. Då kommer systemet att betrakta denne som en giltig användare. Även redan giltiga mallar skulle kunna ändras så att behöriga individer nekas tillträde.

För att hindra den här typen av attack kan smarta kort användas för att spara de personliga mallarna. Detta fungerar endast i verifikationssystem eftersom mallen då måste kopplas till en specifik individ. I fall där man inte kan använda smarta kort utan måste ha en databas kan säkerheten ökas genom att mallarna som ligger i databasen är krypterade. Andra standardmetoder för att öka säkerheten är också att rekommendera, exempelvis att obehöriga inte har fysisk access till hårdvaran (förutom inläsningsenheten) [3][4].

5.1.4 Manipulation av kommunikation mellan olika enheter

Kommunikationskanalerna (fig. 4: 3,5,7,9) skulle kunna manipuleras så att en tidigare matchning återspelas för att lura systemet. Detta betyder att förövaren måste fånga upp information som skickas mellan enheterna i systemet för att återspela denna.

För att skydda sig mot denna typ av attack måste hårdvaran skyddas så att det blir svårare att fånga upp och sända falska signaler i systemet. Ett annat sätt kan vara att man kontrollerar och avvisar mallen om den är identisk med senast inlästa mall eller den sparade mallen på databasen. Systemet kan också vara konstruerat att begära ett slumpvis kännetecken (se 5.1.1), vilket gör denna attack svårare att genomföra [3][4].

5.1.5 Uttömmande testning

I denna attack skickas mer eller mindre slumpvis data till inmatningsenheten (fig. 4: 1) för att försöka få en lyckad matchning. Denna attack är mest effektiv mot identifikationssystem där matchning sker mot alla mallar i databasen, eftersom sannolikheten för en korrekt matchning då blir större. Det är svårare att utföra denna typ av attack mot ett biometriskt system än mot ett som använder sig av pin-kod eller lösenord, eftersom testfallen är mer komplicerade att skapa. Multimodala system är bättre än system där bara ett kännetecken används, eftersom skapandet av testfall är mer komplicerat.

För att skydda mot uttömmande testning kan traditionella skyddsmekanismer användas. Man låser helt enkelt systemet efter ett visst antal felaktiga försök i rad [4].

6.Existerande multimodala system

Nedan följer en kort beskrivning av två existerande multimodala system. Anledningen till valet av just dessa system är att de skiljer sig ganska mycket åt. Det ena är ett kommersiellt identifikationssystem och det andra är ett forskningssystem som är tänkt att fungera som ett verifikationssystem.

6.1 BioID

BioID är ett kommersiellt multimodalt biometriskt identifikationssystem, (kan även fungera som ett verifikationssystem) tillgängligt sedan 1998, som integrerar tre olika biometriska kännetecken: ansiktsform, röstigenkänning och läpprörelser. Systemet är speciellt eftersom det använder ett dynamiskt kännetecken, läpprörelser. Enligt dem själva så är det de första identifikationssystem som använder denna funktion [2].

6.1.1 Insamling av och klassificering av data

Insamlingen av data är en videoinspelning av en individ som pratar. Videon består av 25 bilder per sekund och från dessa bilder tas ansiktets form och läpparnas position ut när individen talar.

6.1.2 Kombineringsstrategi

Det finns ett par olika val man kan göra vid kombineringsstrategi. Detta är för att man ska kunna välja säkerhetsnivå/smidighetsnivå beroende på tillämpning. Om högsta säkerhetsnivå önskas så kan man kombinera ihop alla tre kännetecken, men det normala är att två av tre ska vara godkända för identifiering. Det finns även ett annat alternativ för kombineringsstrategi. Det är att alla tre kännetecken kombineras med hjälp av summaregeln. Då

kan man välja att vikta kännetecken olika mycket för olika individer, vilket gör att systemet blir mer flexibelt.

Kombinering sker på matchningsnivå efter en klassificering av de enskilda kännetecknen gjorts. Ingen information om vilka algoritmer eller vilka metoder/funktioner som används vid kombineringsstrategi finns.

6.1.3 Prestanda

Systemets skapare har gjort ett test med 150 individer under tre månaders tid. Systemet minskade FAR till under 1 procent lite beroende på säkerhetsnivå. Högre säkerhetsnivå minskade FAR, men resulterade i en ökad FRR.

6.2 A Multimodal System Using Fingerprint, Face and Speech

Detta system är ett forskningssystem som är baserat på tre olika biometrier: fingeravtryck, ansiktsform och röstigenkänning. Motiveringen de har till valet av just dessa tre biometrier är att alla tre har använts inom brottsbekämpningsområdet. Alla har också använts i kommersiella system som enskilda biometrier och så har de tre olika fördelar och nackdelar, vilket gör att de kompletterar varandra. Systemet är tänkt som ett verifikationssystem som ska klara av att hantera flera användare och kunna verifiera identiteten på dessa [12].

6.2.1 Insamling av och klassificering av data

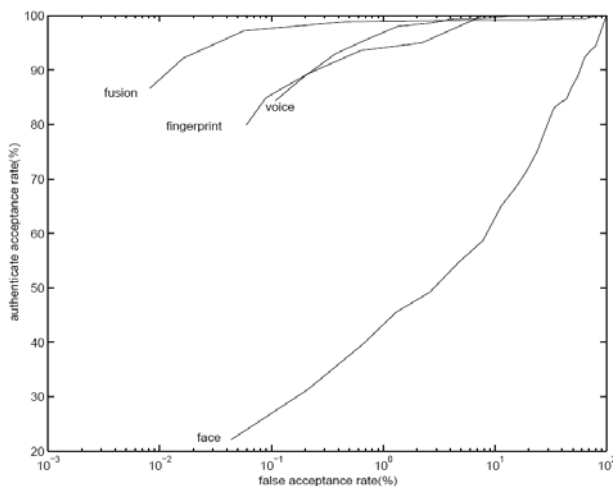
Datamängden samlas in med hjälp av insamlingsenheten och alla användarnas mallar sparas på en databas. Systemet hanterar 50 individer där varje användare har lämnat in 10 fingeravtrycksbilder, 9 ansiktsbilder och 12 röstprov.

6.2.2 Kombineringsstrategi

Biometrierna som används i systemet är väldigt olika varandra både vad gäller karaktären av dem och själva matchningsförfarandet. Därför har man valt att utföra kombinationen av informationen på beslutsnivå. Först beräknas resultatet av matchningen på varje enskild biometri och sedan väger man samman resultatet.

6.2.3 Prestanda

Försöket visar att man med multimodal biometri kan få bättre prestanda. Problemet som de ser är att datamängden är relativt liten och för att kunna dra bättre slutsatser om effektiviseringen måste systemet testas med en större datamängd. Det är också testat i laboratoriemiljö, vilket de anser kan vara en faktor som gör att resultatet blir bättre än vad skulle uppnå i ett verkligt system.



Figur 5: Diagram över de enskilda biometrierna före och efter kombinerad [12].

7. Slutsatser

Fördelarna med multimodala system är att de går att göra säkrare och/eller smidigare än de system som endast använder en typ av biometriskt kännetecken. Vilken effekt man får beror på hur man utformar sitt system. Om man vill ha ett säkrare system så krävs att mer än ett kännetecken måste accepteras för en godkänd igenkänning. Vill man ha ett smidigare system så kan man utforma det så det räcker med att en delmängd av kännetecknen accepteras. Ett annat sätt man kan använda sig av för att nå till ett bättre beslut är att man viktar de olika delarna så att man framhäver fördelarna eller motverkar nackdelarna för respektive biometri.

Det finns nackdelar med multimodala biometriska system. De är dyrare eftersom fler sensorer och mer hårdvara behövs. Det tar längre tid att samla in data och verifikationstiden ökas eftersom det tar längre tid för individen att lämna kännetecknen och för att beräkningen tar längre tid.

Vad avser säkerheten i multimodala system jämfört med ett unimodala system är att attacken blir mer komplex mot de multimodala. Fler system måste knäckas och fler kännetecken måste tillverkas/imiteras för att genomföra en lyckad attack.

Det har också visat sig att man får högre prestanda och tillförlitlighet med multimodala system. I verifikationssystem är de största vinsterna med detta lägre FRR och i identifikationssystem kan det också öka systemets effektivitet.

Tillämpningarna eller användningsområdena för multimodal biometri är alltså antingen system som kräver extra säkerhet, hög tillförlitlighet eller för identifikationssystem med ett stort antal individer.

BioID är väldigt flexibelt i inställningar och hur man vill använda det. Det är ett tydligt tecken på att det är ett kommersiellt system och måste kunna anpassas för flera olika situationer. Vi har inte kunnat få fram information i någon stor omfattning om hur pass bra systemens prestanda är i verklig användning, även om de påstår att prestandan förbättras. Det hade varit trevligt att ha en grundlig utvärdering av det av en oberoende organisation eller individ för att se hur bra det fungerar i verkligheten.

Forskningssystemet visade också på att multimodal biometri ökar systemets prestanda och tillförlitlighet i jämförelse med unimodal biometri. Dock var resultaten även i detta fall osäkra på grund av för liten testgrupp och att systemet inte testats utanför laboratoriemiljö.

8. Referenser

[1] Handbook of Fingerprint Recognition, Springer 2003, Davide Maltoni, Dario Maio, Anil Jain, Salil Prabhakar

[2] BioID: A Multimodal Biometric Identification System, Robert W. Frischholz & Ulrich Diekmann
<http://www.bioid.com/sdk/docs/whitepapers/ieee-computer.pdf>

[3] Biometrics and Security – An Introduction, Kevin Shorter & Ian Nice
http://www.qinetiq.com/home/security/securing_your_business.QuickNavPar.0007.File.pdf

[4] Biometrics – Risks and Controls, 2004, Christos K. Dimitriadis & Despina Polemi
<http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=21329&TEMPLATE=/ContentManagement/ContentDisplay.cfm>

[5] Multimodal Biometrics: An Overview, 2004, Arun Ross & Anil Jain
http://biometrics.cse.msu.edu/RossMultimodalOverview_EUSIPCO04.pdf

[6] Can Multi-biometrics Improve Performance, L. Hong, A. K. Jain, and S. Pankanti
<http://www.research.ibm.com/ecvg/pubs/sharat-int.html>

- [7] Is independence good for combining classifiers?,
Kuncheva, L.I. Whitaker, C.J. Shipp, C.A. Duin,
R.P.W.
http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=906041
- [8] Advances in Robust Multimodal Interface Design,
Sharon Oviatt
<http://portal.acm.org/citation.cfm?id=942597&dl=ACM&coll=ACM>
- [9] Fusion Comes in from the Cold, 2005, Dr Lee
Howells
http://www.europeanbiometrics.info/resources/details.php?Id_taxonomy=138
- [10] Information fusion in biometrics, 2001, Arun Ross &
Anil Jain
http://biometrics.cse.msu.edu/RossFusion_AVBPA01.pdf
- [11] Large Scale Evaluation of Multimodal Biometric
Authentication, Robert Snelick
http://biometrics.cse.msu.edu/NIST_MSU_multimodal_TPAML.pdf
- [12] A Multimodal System Using Fingerprint, Face and
Speech,
AK Jain, L Hong, Y Kulkarni
<http://citeseer.ist.psu.edu/cache/papers/cs/32281/http:zSzzSzwww.cse.msu.edu/zSzpublicationszSztechzSzTRzSzMSU-CPS-98-32.pdf/a-multimodal-biometric-system.pdf>
- [13] International Biometric Group 2006
http://www.biometricgroup.com/reports/public/market_report.html
- [14] Secure Automation Solutions Using Voice
Authentication, 2003, Frost, Sullivan,
http://www.vocent.com/docs/Frost&Sullivan_SecureAutomationSolutionsUsingVoiceAuthenti%85.pdf