VAASAN YLIOPISTO
TEKNILLINEN TIEDEKUNTA
TIETOTEKNIIKAN LAITOS

Juha-Pekka Ikäläinen

MONIBIOMETRISET TUNNISTEJÄRJESTELMÄT

Tietotekniikan
Pro gradu -tutkielma

VAASA 2008

SISÄLLYSLUETTELO

LYHENTEET

BMF	bi-modal fusion – audiovisuaalinen fuusiomenetelmä
CAESAR	civilian american and european surface anthropometry resource – tietokanta
CMC	cumulative match characteristic – kumulatiivinen osumakäyrä
CMF	cross-modal fusion – fuusiometodi
COST	state of the art commercial off the shell – eräs kaupallinen biometrinen järjestelmä
DET	detection error tradeoff – virheiden kompromissi
EER	equal error rate – yhtä suuri virheluku
FaceIt	kaupallinen kasvotunnistealgoritmi
FAR	false accept rate – väärä positiivinen tunnistus
FER	failure to enroll rate – epäonnistunuiden kirjautumisien määrä
FMR	false match rate – väärien hyväksymien määrä
FNMR	false non-match rate – väärien hylkäysten määrä
FRR	false reject rate – väärä negatiivinen tunnistus
GAR	genuine acceptance ratio – todellisten hyväksymien määrä
IR	infrared - infrapuna
JMD	joint multibiometric database – West Virginian yliopiston henkilötietokanta
LSA	latent semantic analysis – puheen tunnistamisessa käytettävä menetelmä
MAS	max-score – fuusiometodi
MCYT	espanjalainen sormenjälkitietokanta
MIS	min-score – fuusiometodi

MM	min-max normalization – minimi-maksimi normalisointi menetelmä
MW	matcher weighting – fuusiometodi
PCA	PCA algoritmi – Coloradon yliopiston kehittämä algoritmi henkilön tunnistamiseen
QLQ	quadric line quadric – normalisointimenetelmä
ROC	receiver operating characteristic
SecurePhone	projekti, jonka tarkoituksena kehittää biometriseen tunnistamiseen sopiva matkapuhelin
SS	simple-sum - fuusiometodi
SVM	metodi monibiometriseen fuusioon
TER	total error rate – kokonaisvirheluku
TH	tanh - normalisointimenetelmä
UW	user weighting – fuusiometodi
XM2VTS	biometriseen tunnistamiseen suunniteltu audio-visuaalinen tietokanta
ZS	Z-score - normalisointimenetelmä

VAASAN YLIOPISTO
Teknillinen tiedekunta
Tekijä: Juha-Pekka Ikäläinen
Tutkielman nimi: Monibiometriset tunnistejärjestelmät
Ohjaajan nimi: Jari Töyli
Tutkinto: Kauppatieteiden maisteri
Laitos: Tietotekniikan laitos
Oppiaine: Tietotekniikka
Opintojen aloitusvuosi: 2002
Tutkielman valmistumisvuosi: 2008 **Sivumäärä:** 66

TIIVISTELMÄ:

Biometriikalla tarkoitetaan yleensä automatisoitua tekniikkaa, jonka avulla mitataan ja analysoidaan henkilön fyysisiä tai käytöksellisiä ominaisuuksia. Näitä ominaisuuksia ovat esimerkiksi sormenjäljet, iirikset, ääni- ja kasvokuvat ja kävely. Näiden tietojen analyysiä käytetään sitten tarpeen mukaan joko henkilön tunnistamiseen tai identiteetin varmentamiseen. Monibiometriikka, tai biometrinen fuusio, on prosessi, jossa yhdistetään tietoja useista biometrisista lähteistä. Tietoja voidaan yhdistää ennen, samanaikaisesti tai tunnistamisen tai varmentamisen jälkeen.

Monibiometrisiä järjestelmiä pidetään yksibiometrisiä luotettavampina, johtuen tunnistuksen tapahtumisesta monista riippumattomista näytteistä. Nämä järjestelmät vastaavat paremmin tiukkoihin tehokkuusvaatimuksiin, joita eri sovellukset asettavat. Ne helpottavat ei yleispäteviä ongelmia koska useat näytteet takaavat populaatiolle riittävän katteen. Ne myös estävät huijauksia koska huijarin on vaikeampaa huijata useita sensoreita tai väärentää useita biometrisiä näytteitä samanaikaisesti. Sen lisäksi ne voivat helpottaa haaste-vaste tyyppistä mekanismia vaatimalla käyttäjää esittämään satunnainen joukko biometrisia näytteitä ja siten varmistaa, että ”live” käyttäjä on todellakin nykyinen käyttäjä.

Monibiometriikassa voi olla myös joitakin ongelmia. Esimerkiksi monibiometriikka tarkoittaa monia kirjautumisen ongelmia. Tuotekehityksessä ei ole yksinkertaista määrittää oikeita yhdistelmiä fuusiolle (esimerkiksi iiris ja sormenjälki). Lisäksi monimutkaisemman järjestelmän vaatima prosessointiaika kasvaa, mikä lisää asiakkaan tunnistamiseen tai todentamiseen kuluvaa aikaa.

AVAINSANAT: monibiometriikka, biometrinen fuusio,

UNIVERSITY OF VAASA
Faculty of technology
Author: Juha-Pekka Ikäläinen
Topic of the Master's Thesis: Multibiometric systems
Instructor: Jari Töyli
Degree: Master of Science in Economics and Business Administration
Department: Department of Computer Science
Major subject: Computer Science
Year of Entering the University: 2002
Year of Completing the Master's Thesis: 2008 **Pages:** 66

ABSTRACT:

Biometrics usually refers to automated technologies for measuring and analyzing an individual's physical and behavioural characteristics; such as fingerprints, irises, voice patterns, facial patterns and gait. The analysis of such data is then used for identification or verification purposes, depending on need. Multi-modal biometrics, or *biometric fusion*, is the process of combining information from multiple biometric readings, either before, during or after a decision has been made regarding identification or authentication from a single biometric.

Multimodal biometric systems are expected to be more reliable due to the presence of multiple, independent pieces of evidence. These systems are able to meet the stringent performance requirements imposed by various applications. They address the problem of non-universality, since multiple traits ensure sufficient population coverage. They also deter spoofing since it would be difficult for an impostor to spoof multiple biometric traits of a genuine user simultaneously. Furthermore, they can facilitate a challenge-response type of mechanism by requesting the user to present a random subset of biometric traits thereby ensuring that a 'live' user is indeed present at the point of data acquisition.

In multimodal biometrics there are also some disadvantages like multiple biometrics means multiple enrolment difficulties. The process of determining the correct feature vector combinations required to fuse, *e.g.*, iris and fingerprint data, is not simplistic and adds to a systems R&D overhead. System processing times are increased due to the complex computations required.

KEYWORDS: multi-modal biometrics, biometric fusion,

1. JOHDANTO

Tässä työssä käsitellään henkilön tunnistamista ja identiteetin varmentamista monibiometristen järjestelmien avulla. Biometrisessa tunnistamisessa käytetään hyväksi henkilön fyysisiä ja käytökseen perustuvia ominaisuuksia. Yksibiometrinen tunnistaminen perustuu nimensä mukaisesti yhteen biometriseen tunnisteeseen. Tunniste voi olla esimerkiksi sormenjälki, kasvokuva tai silmän iiris. Monibiometrinen tunnistaminen perustuu vähintään kahden tunnisteen yhdistämiseen. Yhdistämiseen on olemassa useita menetelmiä ja tekniikoita

1.1 Tutkimuksen tausta

Biometrisen tunnistamisen käyttö ja suosio kasvaa kovaa vauhtia. Esimerkiksi International Biometric Group (2007) on raportissaan todennut, että vuonna 2007 biometriset sovellukset olivat noin kolmen miljardin dollarin liiketoimintaa. Vuonna 2012 summa olisi jo 7,4 miljardia dollaria. Vuonna 2007 monibiometristen järjestelmien osuus oli vain 2,9 prosenttia kaikista biometrisistä menetelmistä.

Euroopan unioni on antanut biometrista passia koskevan asetuksen (N:o 2252/2004), joka on kaikkia jäsenmaita sitova. Asetuksen mukaan matkustusasiakirjassa tulee olla tekninen osa, siru, johon biometriset tunnisteet tallennetaan. Biometriset tunnisteet ovat kasvokuva ja sormenjäljet. Biometristen tunnisteiden käyttöönotto passeissa tapahtuu Suomessa kaksivaiheisesti. Ensimmäisessä vaiheessa otetaan käyttöön kasvokuva, joka tallennetaan digitaalisessa muodossa passin sirulle. Toisessa vaiheessa sirulle tallennetaan sormenjäljet. Sirullinen passi otettiin Suomessa käyttöön 21.8.2006. Toiseen vaiheeseen siirrytään vuonna 2009. Biometrisella passilla tulee olemaan tärkeä rooli kansainvälisen terrorismin, laittoman maahantulon ja kansainvälisen rikollisuuden torjunnassa. Biometrian avulla rajavalvonta voidaan kohdistaa entistä paremmin: suurista matkustajavirroista voidaan tunnistaa ne ihmiset, jotka tulee ottaa tarkempaan tarkasteluun. Biometrinen passi on sirun turvaratkaisujen takia selvästi vaikeampi väärentää kuin perinteinen passi. Väärennettyjä perinteisiä passeja liikkuu maailmalla suuria määriä. (Sisäasiainministeriö 2008)

EU:n komissio haluaa, että unionin alueelle tulevilta kolmansien maiden kansalaisilta ruvetaan keräämään biometriset tunnisteet eli muun muassa sormenjäljet. Tietojen keruu alkaa vuonna 2015, jos jäsenmaat ja Euroopan parlamentti hyväksyvät ehdotuksen. (Sipilä 2008)

Suomessa on jo nyt, esimerkiksi lukuisia kuntosaleja, joissa magneettikortit on korvattu sormenjälkitunnistimilla. Tietosuojavaltuutettu Reijo Aarnio on huolissaan sormenjälkitunnisteiden turvallisesta säilytyksestä kuntosaleilla. Tietosuojavaltuutetun näkökulmasta ongelma on se, jos biometrinen tunniste joutuu vääriin käsiin. Silloin tunnisteen omistaja ei enää itse pysty kontrolloimaan tiedon käyttöä. (Åström-Kupsanen 2007)

1.2 Tutkielman tarkoitus

Tässä tutkielmassa tutustutaan monibiometrisiin tunnistejärjestelmiin. Tutkimusmenetelmä on teoreettinen eli tutkimus perustuu kirjallisuuteen sekä aiheesta julkaistuihin tutkimuksiin. Monibiometriikkaan liittyy tiettyjä olettamuksia, joiden oikeellisuutta pyrin selvittämään, alan uusimpien tutkimusten avulla.

Kappaleessa kaksi esittelen ensin biometriaan liitettyjä olettamuksia. Olettamukset liittyvät yksi- ja monibiometristen järjestelmien hyviin ja huonoihin puoliin. Sitten kerron monibiometrisista järjestelmistä rakenteen, tekniikan ja arkkitehtuurin osalta. Kappaleen lopussa kerron siitä, miten erilaisia järjestelmiä voidaan vertailla keskenään. Miten niiden virheet määritellään ja miten ne ilmoitetaan.

Kappaleessa kolme esittelen tutkimuksia, joissa on tutkittu henkilön tunnistamista useiden erilaisten biometristen menetelmien yhdisteinä. Mielenkiintoisin on ehkä ensimmäisenä esiteltävä kasvo- ja sormenjälkikuvaan keskittyvä tutkimus. Kasvo- ja sormenjälkitunnistehan tulee myös uusiin biometrisiin passeihin, jotka meilläkin otetaan käyttöön. Toisessa tutkimuksessa on yhdistetty sormenjälki, kasvo ja käden geometria.

Kolmannessa kuvataan kasvokuvan ja iiriksen yhdistelmä ja neljännessä kasvojen ja useiden sormenjälkien yhdistelmä..

Kappaleessa neljä esitellään muutamia tutkimuksia, joissa on tutkittu henkilön tunnistamista ja henkilön identiteetin varmentamista yhdestä biometrisesta kohteesta johdettujen erilaisten yhdisteiden avulla. Tutkimuksina on kasvotunnistaminen kaksi- ja kolmiulotteisesti. Käden geometria ja kämmenen jälki sekä infrapunavalo ja näkyvävalo kasvotunnistamisessa Lopuksi esitellään monibiometriikan uusimman menetelmän prototyyppi. Siinä on kehitetty sensori, joka kuvaa kaikki tunnetut käden biometriset tunnisteet yhtäaikaisesti.

Kappaleessa viisi esittelen audiovisuaalisista monibiometrisista menetelmistä tehtyjä tutkimuksia. Tutkimuskohteina on videokuvaan perustuva tunnistaminen, äänen ja sormenjäljen yhdistäminen, mobiililaitteille suunniteltu ääni-, kasvo- ja käsialatunnistaminen sekä käyttäjän elävyyteen perustuva tutkimus.

Kappaleessa kuusi esittelen ensin kevyttä biometriikkaa yleisellä tasolla. Tutkimuksina esittelen ensin sormenjäljen ja kolmen erilaisen kevyen biometrisen tunnisteen yhdistelmän. Sitten esittelen kevyeen biometriaan perustuvan monibiometrisen tunnistemenetelmän, joka sopisi paremmin käyttäjien tunnistamisessa kuntosalilla kuin tietosuojavaltuutetun kammoama sormenjälkitunnistaminen.

1.3 Aikaisempi tutkimus

Vaasan yliopiston tietotekniikan laitokselle on Jarmo Johannes Pimperi kirjoittanut vuonna 2005 pro gradu – tutkimuksen: Johdatus biometriikan perusteisiin, käytettävyyteen ja tietoturvaan. Se antaa melko kattavan kuvan muun muassa erilaisten yksibiometristen tunnistemenetelmien tekniikoista. Monibiometrisistä järjestelmistä ei suomenkielistä tutkimusta löytynyt, vaikka ainakin VTT on niitä tutkinut. Oikeastaan lähes kaikki tässä työssä käyttämäni lähteet olivatkin englanninkielisiä ja ulkomaisten tutkijoiden tekemiä.

2. MONIBIOMETRIIKAN PERUSTEET

Biometriikka voidaan määritellä automatisoiduksi, koneen avulla tapahtuvaksi henkilön identiteetin tunnistamiseksi (identification) tai todentamiseksi (verification). Prosessissa hyödynnetään henkilön ainutlaatuisia fysiologisia (physiological) tai käyttäytymiseen (behavioral) perustuvia ominaisuuksia, joiden perusteella tunnistaminen tai todentaminen suoritetaan (Pimperi 2005: 11). Biometriset järjestelmät ovat nykyään käytössä useissa kaupallisissa sekä siviili- ja rikosteknisissä sovelluksissa henkilöiden identiteetin tunnistamiseksi ja vahvistamiseksi. Nämä järjestelmät perustuvat sormenjäljen, käden geometrian, iiriksen, verkkokalvon, kasvojen äänen tai muun vastaavan todistusvoimaan hyväksyttäessä tai hylättäessä henkilön identiteetti. (Ross & Anil 2004: 1)

2.1 Monibiometriikkaan liitetyt olettamukset

Enemmistö biometrisista järjestelmistä perustuu yksibiometriikkaan (unimodal). Ne siis perustuvat yksittäiseen biometriseen näytteeseen henkilön tunnistamisessa, esimerkiksi sormenjälki- tai kasvotunnisteeseen. Näillä järjestelmillä on useita ongelmia, jotka voivat vaikuttaa tunnistamiseen. Ross ym. (2004: 1) mukaan näitä ongelmia ovat: Kerätyn tiedon häiriö (noisy data). Arpi sormenjäljessä tai ääninäyte vilustuneelta ovat esimerkkejä tietohäiriöstä. Vialliset tai huoltamattomat sensorit voivat myös aiheuttaa tietohäiriöitä (esimerkiksi lika sormenjälkisensorissa) tai epäedullinen ympäristö (huono valaistus kasvotunnistuksessa). Sisäinen häiriö (intra-class variations). Tällaista vaihtelua aiheuttaa yleensä käyttäjä, joka toimii väärin suhteessa sensoriin (esimerkiksi väärä asento kasvotunnistuksessa) tai kun sensorin arvoja muokataan kesken tunnistuksen. Ulkoiset häiriöt (inter-class similarities), joita esiintyy biometrisessä järjestelmässä, joka koostuu suuresta määrästä käyttäjiä. Tällaisessa järjestelmässä voi olla samankaltaisia näytteitä useilla käyttäjillä. Ei universaali (non-universality), jolloin osalta ihmisistä ei voida saada sopivaa biometristä näytettä. Väärennökset (spoof-attacs), jonka kaltaiset hyökkäykset ovat vaarana erityisesti silloin kun, käytetään

käyttäytymiseen perustuvia biometrisiä tunnisteita, kuten käsiala tai ääni. Myös fyysisiin ominaisuuksiin perustuvia näytteitä on pystytty väärentämään.

Ulkoisia häiriöitä voidaan kutsua myös yksilöllisyyden puutteeksi (lack of individuality). Se tarkoittaa, että eri henkilöiden biometriset näytteet voivat olla liian samanlaisia. Esimerkiksi kasvotunnistemenetelmät, jotka ovat yleisesti käytössä nykyisissä järjestelmissä, eivät pysty aina erottamaan esimerkiksi identtisiä kaksosia tai isää ja poikaa. Tämä yksilöllisyyden puute lisää järjestelmän FMR–virheitä (false match rate). (Nandakumar 2005: 9)

Jotkut yksibiometristen järjestelmien rajoitukset identiteetin tunnistamisessa voidaan voittaa keräämällä informaatiota monista lähteistä. Tällaiset järjestelmät tunnetaan monibiometrisina järjestelminä (multimodal biometric systems). Niitä voidaan pitää luotettavampina, johtuen tunnistuksen tapahtumisesta monista riippumattomista näytteistä. Nämä järjestelmät vastaavat paremmin tiukkoihin tehokkuusvaatimuksiin, joita eri sovellukset asettavat. Ne helpottavat ei yleispäteviä ongelmia koska useat näytteet takaavat populaatiolle riittävän katteen. Ne myös estävät huijauksia koska huijarin on vaikeampaa huijata useita sensoreita tai väärentää useita biometrisiä näytteitä samanaikaisesti. Sen lisäksi ne voivat helpottaa haaste-vaste (challenge-response) tyyppistä mekanismia vaatimalla käyttäjää esittämään satunnainen joukko biometrisia näytteitä, ja siten varmistaa, että ”live” käyttäjä on todellakin nykyinen käyttäjä. (Ross ym. 2004: 1)

Nandakumarin (2005: 9) mukaan monibiometriset järjestelmät voivat parantaa järjestelmän kykyä tutkia suuria tietokantoja tehokkaasti ja nopeasti. Järjestelmä voidaan ohjelmoida tutkimaan ensin helpommat ja vähemmän tarkat tunnistemenetelmät. Jäljelle jäänyt ”karsittu” tietokanta sitten tutkitaan monimutkaisemmalla ja tarkemmalla tunnistemenetelmällä.

Howells (2005: 9) on luetellut joitakin monibiometriikan huonoja puolia. Hänen mukaansa esimerkiksi monibiometriikka voi tarkoittaa monia ongelmia. Tuotekehityksessä ei ole yksinkertaista määrittää oikeita yhdistelmiä fuusiolle

(esimerkiksi iiris ja sormenjälki). Lisäksi monimutkaisemman järjestelmän vaatima prosessointiaika kasvaa, mikä lisää asiakkaan tunnistamiseen tai todentamiseen kuluvaa aikaa.

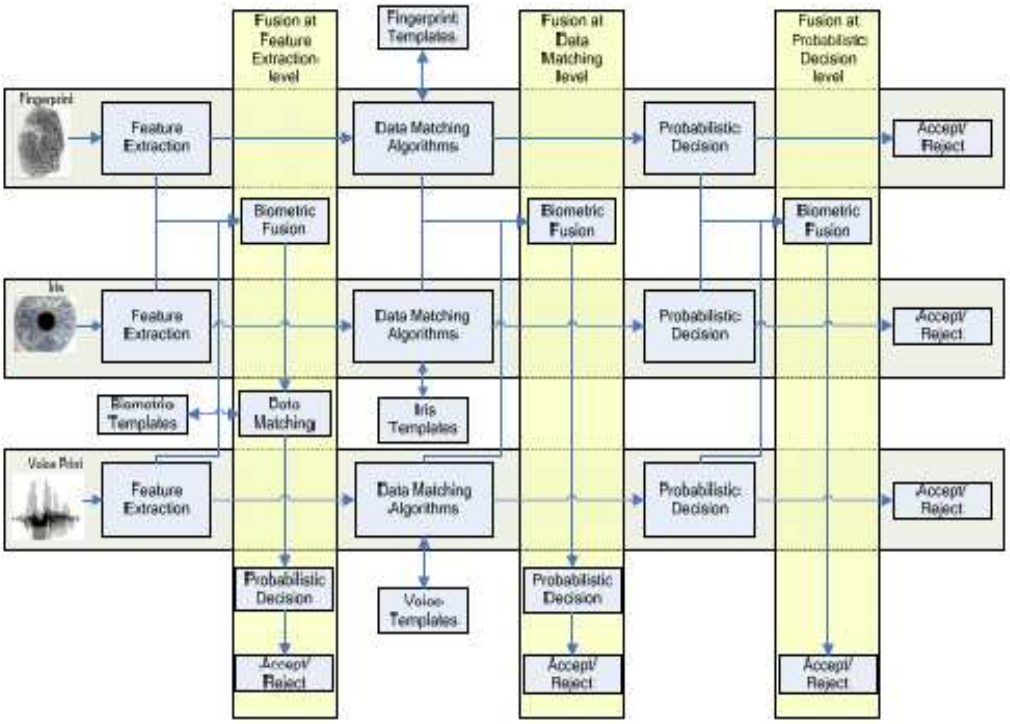
Dessimoz, Richiardi, Champod & Drygajlo (2006: 112) ovat todenneet, että monibiometriikan käyttö tunnistedokumenteissa (passi) ei ole ongelmatonta. Riippumatta siitä, onko passien informaatio raakadataa tai biometrinen mallinne, niin varastoitavan informaation koko kasvaa. Tämä aiheuttaa haasteita ainakin yksilö- ja tietosuojalle. Monibiometriikan käyttö tunnistedokumenteissa lisää maiden rajoilla ja tarkastuspisteissä tarvittavien laitteiden ja sensoreiden määrää. Tämä myös vaatii lisää koulutettua henkilöstöä ja vaatii siten myös lisää henkilöstön koulutusta. Nämä seikat lisäävät monibiometristen järjestelmien käyttökustannuksia.

2.2 Monibiometrinen järjestelmä

Monibiometrisen järjestelmän rakenne riippuu voimakkaasti sovelluksen tarkoituksesta. Kirjallisuudessa on esitelty useita monibiometrisiä järjestelmiä, jotka eroavat toisistaan arkkitehtuurin, biometristen menetelmien määrän ja valikoimien, tietojen keräämisen tason sekä tiedon yhdistämismenetelmien suhteen. (Nandakumarin 2005: 12)

Monibiometrinen järjestelmä kerää kahta tai useampaa biometristä näytettä. Se käyttää fuusiota yhdistämään niiden analyysit ja tuottaa tällä tavalla parempia ratkaisuja FAR- (false accept rate) ja FRR (false reject rate) -arvojen alentamiseksi. Monibiometrinen järjestelmä voidaan toteuttaa viidellä tavalla. Voidaan käyttää useita sensoreita keräämään samaa biometriaa. Voidaan kerätä useita eri biometrisiä näytteitä. Samaa biometriaa voidaan tutkia useita kertoja, jotta saavutettaisi optimaalinen lukema. Samasta biometriasta voidaan ottaa kaksi tai useampia näytteitä, esimerkiksi kahden eri sormen sormenjäljet tai molemmat iirikset. Eri algoritmeja voidaan käyttää samaan biometriaan, jotta saavutetaan riippumattomat tulokset. Epäkorreloivien yhdistelmien, kuten esimerkiksi sormenjäljen ja kasvojen tai kahden eri sormenjäljen, odotetaan

antavan parempia tuloksia kuin korreloivien yhdistelmien, joita ovat esimerkiksi useat sormenjälkinäytteet samasta sormesta. (Howells 2005: 9)



Kuva 1. Biometrisen fuusion vaihtoehdot. (Howells 2005: 6)

Kuvasta 1 nähdään, että fuusio voi tapahtua missä tahansa tunnisteprosessin vaiheessa kolmella eri fuusio metodologialla. Ensimmäinen on näytteenottofuusio (Feature-Extraction level fusion). Toinen on datan vertailu fuusio (Data-Matching level fusion) ja kolmas on todennäköisin ratkaisu fuusio (Probabilistic-Decision level fusion). Näiden lisäksi voidaan mainita harvinainen sensoritason fuusio (sensor level fusion).

Näytteenottofuusio

Tietoja, jotka on kerätty jokaisesta sensorista, käytetään ominaisvektorin luomiseen. Sormenjälkien tapauksessa vektori voi sisältää kolme ulottuvuutta: sijainti, muoto ja harjanteiden suunta. Ihanteellisessa tapauksessa tämä vektori tunnistaa ainutlaatuisesti henkilön. Todennäköisemmin vektori tunnistaa koko kirjautuneesta joukosta osajoukon.

Kaikkien biometrioiden ominaisvektorien yhdistelmä luo vektorin, jolla on korkeampi ulottuvuus ja korkeampi todennäköisyys yksilöllisesti tunnistaa henkilö. (Howells 2005: 6).

Datan vertailu fuusio

Kun jokaisesta biometriasta on luotu ominaisvektorit, ne ohjataan niiden yksilöllisille yhteensovitus algoritmeille, jotka yrittävät sovittaa niitä viimeksi saatuihin näytteisiin. Yksilöllisesti yhteensopivat todennäköisyydet yhdistetään ja saadaan tulos, jonka perusteella päätös voidaan tehdä. Tämän fuusion suorittamiseksi on olemassa monia erilaisia metodeja. Niistä suosituimmat ovat summasääntö (sum rule), päätöspuu määritys (decision tree determination) ja lineaarinen syrjintä analyysi (linear discriminate analysis).

Summasääntömetodilla voidaan ottaa painotettu keskiarvo algoritmien tuottamista pisteistä niin, että esimerkiksi sormenjälkien ja iiriksen fuusion yhteispisteet voidaan laskea kaavalla:

$$s = \frac{1}{2}\left(\beta s^{(fp)} + (1-\beta)s^{(i)}\right) \qquad (1)$$

Kaavassa $s_{(fp)}$ ja $s_{(i)}$ ovat sormenjäljen ja iiriksen biometristen näytteiden keskinäiset pisteet. β on painotus, joka voidaan laskea käyttäen koulutusdataa tai vahvasti kerätyn näytteen laadusta riippuvaa dataa. Komponenttien pisteet täytyy normalisoida, jotta varmistetaan laskettujen pisteiden merkityksellisyys. Päätöspuumäärityksessä kerättyä biometristä näytettä verrataan talletettuun näytteeseen ja se hyväksytään aidoksi jos sen määrittämä arvo on asetetun kynnysarvon tai kohdearvon yläpuolella. Lineaarista syrjintäanalyysiä (LDA) käytetään määrittelemään binäärinen tulos vektorien joukosta. (Howells 2005: 6).

Todennäköisin ratkaisu fuusio

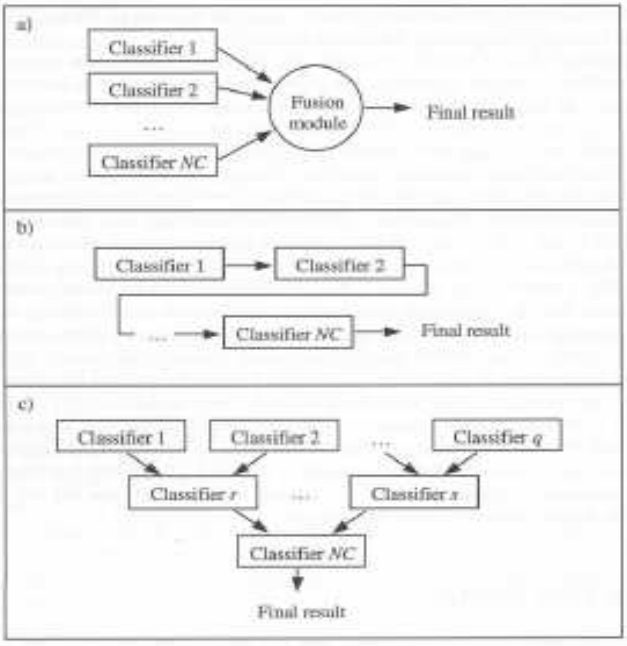
Todennäköisin ratkaisu fuusio ei ole oikeastaan fuusio ollenkaan, vaikka sitä niin kutsutaankin. Tämän metodin periaate on se, että jokainen biometrinen järjestelmä tutkii yhteensopivuutta vain keräämällään biometrisellä näytteellä. Tämän se lähettää sitten binääriseen sopii / ei sovi – vektorin päätöksenteko moduuliin. Ratkaisu perustuu siihen, kumpia on enempi. Jotkut järjestelmät pitävät sisällään metodin, jolla päätöstä voidaan painottaa tärkeämmäksi katsottua biometriaa kohden. Esimerkiksi iiris voidaan painottaa tärkeämmäksi kuin retina. (Howells 2005: 6)

Sensoritason fuusio

Sensoritason fuusio on melko harvinainen koska fuusio tällä tasolla vaatii sen, että datan, jota on saatu erilaisilla biometrisillä sensoreilla, pitäisi olla keskenään vertailukelpoista. Tämä on käytännössä hyvin harvoin mahdollista. Esimerkiksi kasvokuvia, jotka on otettu eri resoluutioilla, ei voida vertailla. Sen sijaan samoilla resoluutioilla otettuja kuvia voitaisiin sensoritason fuusion avulla yhdistää kolmiulotteiseksi kasvokuvaksi. (Nandakumar 2005: 12)

Järjestelmän arkkitehtuuri

Monibiometrinen järjestelmä voi toimia kolmella eri tavalla. Ne ovat sarja- (serial), rinnakkais- (parallel) tai hierarkkinen malli (hierarchical mode). Mallit on esitelty kuvassa 2. Sarjamallissa yhden vaiheen ulostuloa (output) käytetään vähentämään mahdollisten tunnistettavien henkilöiden määrää ennen seuraavaa vaihetta. Siksi esimerkiksi useita eri näytteitä ei tarvitse hankkia samanaikaisesti. Järjestelmä voi myös tehdä päätöksen henkilön tunnistamisesta ennen kuin kaikki näytteet on kerätty. Tällöin järjestelmän käyttämä aika henkilön tunnistamiseen voi laskea. Rinnakkaismallissa tunnistuksen saamiseksi kerätään tietoa useista vaiheista samanaikaisesti. Hierarkiamallissa yksilöllisiä luokittelijoita (classifier) yhdistetään puumaiseen rakenteeseen. Tämä malli on hyvä silloin kun luokittelijoita on paljon. (Ross ym. 2004: 3)



Kuva 2. a) rinnakkainen b) sarja ja c) hierarkinen arkkitehtuuri. (Dessimoz ym. 2006: 38)

Tulosten normalisointi

Seuraavat asiat tulee ottaa huomioon ennen yksittäisten tulosten yhdistämistä. Yksittäiset tulokset eivät välttämättä ole homogeenisia. Yksi menetelmä voi esimerkiksi mitata näytteiden samankaltaisuutta ja toinen näytteiden erilaisuutta. Eri menetelmien tulokset eivät ole välttämättä samalla numeerisella asteikolla. Tulokset voivat myös sijoittua eri tilastolliseen jakaumaan. Näiden syiden johdosta tulosten normalisointi (score normalization) samankaltaisiksi on tärkeää ennen niiden yhdistämistä. (Nandakumar 2005: 33)

Tulosten normalisointi tarkoittaa yksittäisten tulosten sijainti- ja asteikkoparametrien muuttamista samankaltaisiksi. Kun normalisointiparametrit on määritelty määrittelyjoukon avulla, puhutaan määritellystä tulosten normalisoinnista (fixed score normalization). Tällaisessa tapauksessa tutkitaan tulosten jakaumaa ja jakauman perusteella valitaan sitten sopiva kaava. Kaavan perusteella sitten määritellään

normalisointiparametrit. Joustavassa tulosten normalisoinnissa (adaptive score normalization) normalisointiparametrit arvioidaan ominaisvektorin perusteella. Tämän menetelmän hyvä puoli on se, että se pystyy joustamaan esimerkiksi äänisignaalin pituuden suhteen. Hyvässä normalisointimenetelmässä tulosten jakauman sijainti- ja asteikkoparametrien arviointi tulee olla tehokasta ja vahvaa. Vahvuus tarkoittaa immuunisuutta ulkopuolisille vaikutteille. Tehokkuus tarkoittaa hankitun arvion ja optimaalisen arvion läheisyyttä, kun datan jakauma tunnetaan. (Nandakumar 2005: 33, 35)

Yksinkertaisin normalisointimenetelmä on minimi - maksimi normalisointi (min – max normalization). Se sopii parhaiten tapauksiin, joissa tulosten maksimi ja minimi raja-arvot tunnetaan. Tällöin minimi- ja maksimiarvoiksi voidaan asettaa nolla ja yksi. Vaikka raja-arvoja ei tunnettaisi, voidaan tulosten minimi- ja maksimiarvot arvioida ja näin soveltaa tätä normalisointimenetelmää. (Nandakumar 2005: 36)

Yleisimmin käytetty normalisointimenetelmä on Z-score, joka käyttää annetun datan aritmeettista keskiarvoa ja normaalihajontaa. Tämän menetelmän voi olettaa toimivan hyvin jos tiedetään ennalta keskimääräinen tulos ja tulosten vaihtelu. Mikäli vertailualgoritmin luonteesta ei ole ennakkotietoa, tulosten keskiarvo ja normaalihajonta tulee arvioida. Keskiarvo ja normaalihajonta ovat herkkiä ulkoisille häiriöille. Tämä menetelmä ei siis ole vahva. Z-score normalisointi ei aina takaa yhteistä numeerista valikoimaa eri vertailujen normalisoiduille tuloksille. Muita normalisointimenetelmiä ovat muun muassa desimaaliskaalaus (desimal scaling) ja mediaani ja mediaanin absoluuttinen hajonta MAD (median absolute deviation), (Nandakumar 2005: 38, 48)

Painotus (weight)

Monibiometrisesa järjestelmässä tärkeä ominaisuus on mahdollisuus valita jokaiselle biometriselle näytteelle sellainen luottamuksen taso, että järjestelmä säilyttää käyttäjiä ja järjestelmän operaattoria koskevan hyväksyttävän tasapainon luotettavuuden ja kirjautumisajan välillä. Lisäksi painotuksen etu on se, että sitä voidaan soveltaa populaatiotasolla, yksilötasolla tai kaikkialla niiden välillä. Kun yhdistetään erilaiset

painotukset eri biometriikoihin, voidaan varmistaa, että esimerkiksi huonot sormenjäljet omaavan henkilön tunnistamiseen käytetään enemmän jotakin muuta biometriikkaa. Näin voidaan parantaa aidon tunnistamisen todennäköisyyttä. Operaattori voi esimerkiksi painottaa voimakkaammin käsillään työtä tekevien ja huonot sormenjäljet omaavan joukon kasvotunnistamista. (Howells 2005: 9)

2.3 Biometrisen järjestelmän virheettömyys ja järjestelmän arviointi

Biometrisen järjestelmän virheettömyydellä tarkoitetaan täydellistä ja aukotonta tunnistamis- tai todentamisprosessia. Tämä on ihannetilanne, jossa käyttäjä on toiminut laitteen kanssa siten, että järjestelmä on tulkinnut tilanteen oikeaksi ja virheitä ei ole päässyt tulemaan. Tämä ihannetilanne on kuitenkin käytännössä mahdoton ja arkielämän tilanteet eivät aina vastaa laboratoriossa suoritettuja testejä.

Tunnistamis- ja todentamisprosessista voidaan erottaa kolme vaikuttavaa tekijää. Nämä ovat käyttäjä, järjestelmän suorituskyky ja käyttöliittymä. Vaikka käyttäjä on toiminut oikein ja operoinut järjestelmän käyttöliittymää selkeällä ja oikealla tavalla, voi järjestelmä silti tehdä virheen tunnistamalla tai todentamalla käyttäjän täysin väärin.

Biometriikkaan perustuvassa järjestelmässä käytetään virheistä termejä FRR (false reject rate) ja FAR (false accept rate). Nämä kaksi tuottavat lukuarvon, joka ilmoitetaan prosentteina. FRR ja FAR ovat tärkeimmät suorituskykymittarit arvioitaessa biometrisen järjestelmän tekemiä virheitä käyttäjän tunnistamis- tai todentamisprosessissa. (Pimperi 2005: 42)

FAR (false accept rate)

Väärä positiivinen tunnistus, joka tarkoittaa Biometrics FAQ (2007) mukaan arvoa, jolla järjestelmään kuulumaton henkilö hyväksytään järjestelmään. Koska väärästä hyväksymisestä voi usein seurata vahinkoja voidaan FAR luokitella turvallisuutta mittaavaksi arvoksi. FAR on muuttuva tilastollinen arvo, joka ei vain osoita henkilön vastaavuutta vaan voi olla myös määritetty yksilöllisille arvoille (personal FAR).

FAR-määrittelyssä on otettava huomioon seuraavat asiat: FAR on tilastollinen arvo, jonka mittaamisen tarkkuus riippuu mittauskertojen määrästä. Tämän perusteella FAR ei ole ainoastaan biometrisestä järjestelmästä riippuvainen vaan myös käyttäjästä. On siis olemassa myös henkilökohtainen FAR (personal FAR). Jos ollaan tekemisissä suurien käyttäjätietokantojen kanssa on huomioitava, että yksilön FAR-tulos ei saa vaikuttaa muiden FAR-arvoihin. Tämä ongelma voidaan välttää tutkimalla kaikkien henkilöiden FAR-tilastoja ja laskemalla niistä keskiarvo, jonka perusteella järjestelmää säädetään uudelleen. FAR-arvoa määriteltäessä olisi hyvä rajoittaa henkilöiden tunnistus- ja todentamisyritys yhteen kertaan.

FAR-arvoa voidaan kuvata kaavalla (2). Kaavan osoittajassa on kaikkien onnistuneitten vilpillisten yritysten määrä rekisteröityä käyttäjää (enrolled user) kohden. Vilpillinen käyttäjä saa onnistuneesti käyttöön rekisteröityneen käyttäjän identiteetin (väärä positiivinen tunnistus). Nimittäjässä on vastaavasti kaikki vilpilliset onnistuneet ja epäonnistuneet yritykset rekisteröityä käyttäjää kohden. (Pimperi 2005: 44)

$$FAR(n) = \frac{\text{Kaikkien onnistuneiden yritysten määrä rek. Käyttäjää kohden}}{\text{Kaikkien vilpillisten yritysten määrä rek.käyttäjää kohden}} \quad (2)$$

Kaava (2) FAR-arvon laskeminen (Biometrics FAQ 2007)

FRR (false reject rate)

Väärä negatiivinen tunnistus, joka Biometrics FAQ (2007) mukaan tarkoittaa arvoa, jolla järjestelmään kuuluva henkilö hylätään tunnistamis- tai todentamistilanteessa. FRR:ta ajatellaan yleensä mukavuuskriteereinä, koska väärä tunnistaminen on ennen kaikkea kiusallinen. FRR on ei-paikallaan oleva tilastollinen määrä, joka ei vain näytä vahvaa henkilökohtaista korrelaatiota vaan se voidaan jopa määrätä kutakin yksittäistä biometrista ominaispiirrettä varten. (Biometrics FAQ 2007)

FRR on tilastollinen arvo, jonka mittaamisen tarkkuus riippuu mittauskertojen määrästä. Tämän perusteella FRR ei ole ainoastaan biometrisesta järjestelmästä riippuvainen vaan

myös käyttäjästä. Toisin sanoen on olemassa myös henkilökohtainen FRR. Suurien käyttäjätietokantojen kanssa on syytä ottaa huomioon, että yksilön FRR-tulos ei saa vaikuttaa muiden FRR-arvoihin. Tällainen tilanne voi syntyä, kun jokainen henkilö yrittää todentaa itseään biometriseen järjestelmään monta kertaa. Tämä ongelma voidaan välttää tutkimalla kaikkien henkilöiden FRR-tilastoja ja laskemalla niistä keskiarvo, jonka perusteella järjestelmää säädetään uudelleen. (Pimperi 2005: 43)

Biometrics FAQ (2007) mukaan henkilökohtainen FRR voi muuttua ajan kuluessa ja se voi vähentyä käytettäessä järjestelmää, joka oppii tunnistamaan käyttäjän tavan operoida laitteen kanssa. Koska FRR on tilastollinen tunnusluku, on tehtävä suuri määrä todentamisyrityksiä, jotta saataisiin tilastollisesti luotettavia tuloksia. Yksinkertaisuudessaan FRR-arvoa voidaan kuvata kaavalla

$$FRR(n) = \frac{\text{Henkilön epäonnistuneet todentamisyritykset}}{\text{Henkilön kaikki epäonnistuneet todentamisyritykset}} \quad (3)$$

Kaava (3) FRR-arvon laskeminen (Biometrics FAQ 2007)

Kun lasketaan FAR ja FRR arvoja, kynnysarvo (laatuhylkäys arvo QPR) pitää ottaa huomioon.

$$FAR(th) = (1 - QRR)\, FMR(th) \quad (4)$$

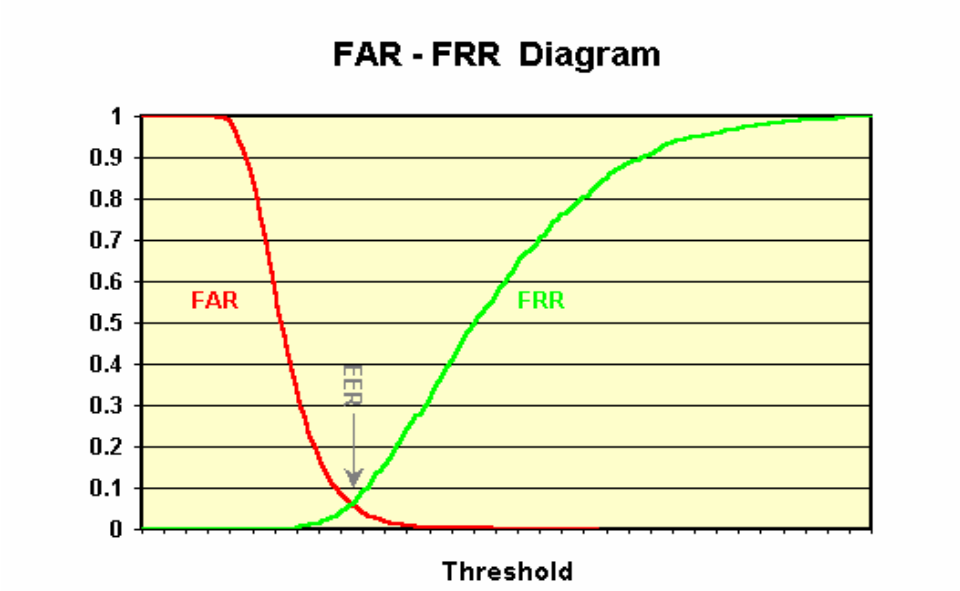
$$FRR(th) = QRR + (1 - QRR)\, FNMR(th) \quad (5)$$

Tällöin raja-arvoiksi saadaan:

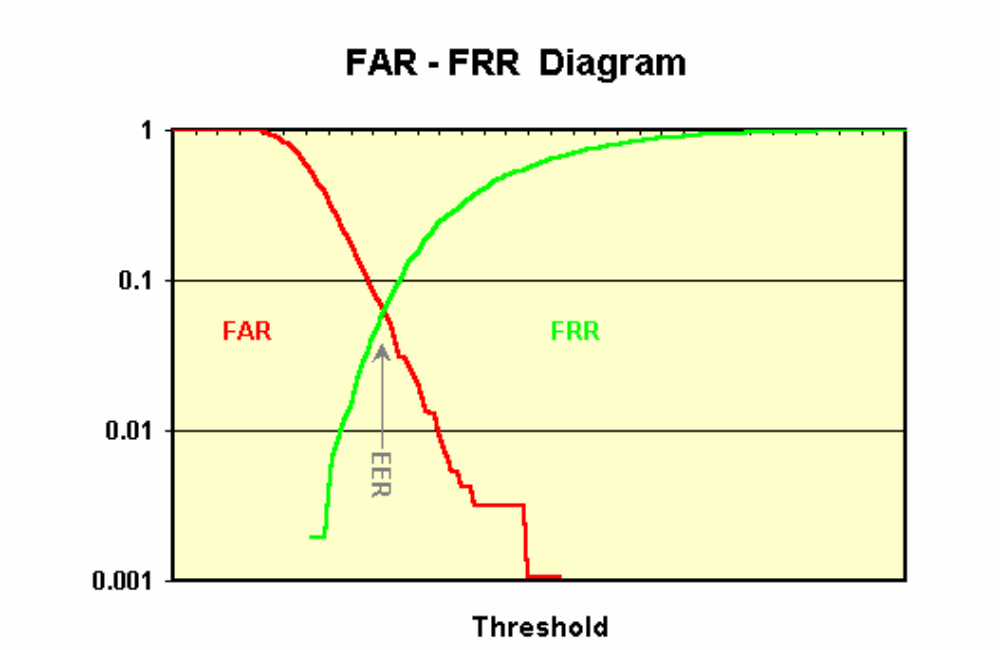
$$FAR(0) = 1 - QRR \qquad FAR(K) = 0 \quad (6)$$

$$FRR(0) = QRR \qquad FRR(K) = 1 \quad (7)$$

Kynnysarvo määräytyy FRR- ja FAR-arvojen mukaan. Arvoa löysentämällä tai kiristämällä voidaan vaikuttaa mallinteeseen kohdistuvaan vertailuun. Seuraavat diagrammit osoittavat tyypilliset tulokset lineaarisella ja logaritmisella asteikolla



Kuva 3. FAR- ja FRR-arvojen tyypillinen tilanne lineaarisesti. (Biometrics FAQ 2007)



Kuva 4. FAR- ja FRR-arvojen tyypillinen tilanne logaritmisesti. (Biometrics FAQ 2007)

Kuvista 3 ja 4 voidaan päätellä, että kumman tahansa arvon muuttaminen vaikuttaa aina toiseenkin arvoon. FAR-virheiden väheneminen lisää FRR–virheitä ja päinvastoin. Näiden kahden suhde ja arvo vaikuttavat biometrisen järjestelmän käytettävyyteen ja etenkin siihen, kuinka järjestelmä toimii virheettömästi. Täydellistä virheettömyyden

tilaa ei voida saavuttaa, mutta virheiden mahdollisuutta voidaan pienentää siedettävälle tasolle ilman, että järjestelmän käytettävyys häiriintyy. (Biometrics FAQ 2007)

EER (equal error rate)

Kahden biometrisen järjestelmän vertailu FAR- tai FRR–arvojen perusteella voi olla vaikeaa. Jos järjestelmän toimittaja ilmoittaa vain oman FAR–arvon ilman FRR–arvoa, voikin olla niin, että alhaisen FAR–arvon omaavalla järjestelmällä onkin kelvottoman korkea FRR–arvo. Myös silloin, kun molemmat arvot on annettu, on ongelmana se, että ne molemmat ovat kynnysarvosta riippuvaisia. Mikäli kynnysarvo on vaihtuva tai säädettävä, ei ole järkevää tapaa päättää onko järjestelmässä parempi olla korkea FAR ja matala FRR vai päinvastoin. Järjestelmän EER–arvoa voidaan käyttää esittämään kynnysarvosta riippumaton mittaus arvo. Mitä pienempi EER on, sitä parempi on järjestelmän suorituskyky. EER on FAR- ja FRR–arvojen summa eli se kohta, jossa nämä arvot ovat yhtä suuret. Teoriassa tämä toimii hyvin jos EER lasketaan käyttäen ääretöntä ja edustavaa testiryhmää. Tämä ei tietenkään ole mahdollista käytännössä. Siksi onkin tärkeää, että EER–arvoja vertailtaessa käytetään samaa testidataa ja samaa testiprotokollaa. (BioID 2004)

ROC (receiver operating characteristic)

Jotta eri järjestelmien tehokkuutta voitaisiin vertailla menestyksellä pitää siis käyttää kynnysarvosta riippumatonta menetelmää. Eräs tällainen menetelmä on tutkatekniikasta saatu ROC–käyrä, joka kuvaa FRR–arvoja suoraan FAR–arvoja vastaan. Näin se eliminoi kynnysarvon vaikutuksen. ROC, samoin kuin FRR, voi saada vain arvoja nollan ja yhden väliltä. Ihanteellinen ROC saa arvoja jotka ovat joko x–akselilla (FAR) tai y–akselilla (FRR). Siis kun FRR ei ole nolla FAR on yksi ja päinvastoin. ROC ei voi kasvaa. Joskus käytetään ROC–käyrän sijasta termiä DET (detection error tradeoff). (Biometrics FAQ 2007)

CMC (cumulative match characteristic)

CMC–käyrä osoittaa tunnistamisen todennäköisyyttä useilla arvoilla. Yksi sen tärkeimmistä piirteistä on se, että graafissa, joka sisältää kaikki mahdolliset arvot, siis jos tietokannassa on esimerkiksi 140 henkilöä ja CMC–käyrä menee arvon 140 läpi, tunnistamisen todennäköisyys on sata prosenttia. On tärkeää määrittää tietokannan suuruus kun todennäköisyyttä kuvataan CMC–käyrällä. Oikean tunnistamisen todennäköisyys on huomattavasti parempi arvolle 10 sadan henkilön tietokannalle kuin 10000 henkilön tietokannalle. (NSTC Subcommittee on biometrics 2006: 19)

FER, FIR, FMR ja FNMR

FER tai FTE (failure to enrol rate) kuvaa niitä ihmisiä, jotka eivät onnistu kirjautumaan järjestelmään. Voi olla myös henkilökohtainen (personal FER). FIR (false identification rate) on todennäköisyys tunnistamiselle, jossa biometrinen näyte tunnistetaan väärin perustein. FMR (false match rate) on arvo, jolla järjestelmään kuulumaton henkilö hyväksytään ja FNMR (false non-match rate) arvo, jolla järjestelmään kuuluva hylätään väärin perustein. (Biometrics FAQ 2007)

Arviointi

Biometrisen järjestelmän tarkkuutta ja suoritustehoa voidaan arvioida luotettavasti vain silloin kun järjestelmää testataan riittävän laajalla ja kattavalla tietokannalla. Tietokannan henkilötietojen tulisi olla kerätty monipuoliselta populaatiolta vaihtelevissa ympäristöolosuhteissa. Ihanne olisi tietokanta, jossa olisi yli 25000 henkilön biometriset näytteet, mutta käytännössä nykyiset järjestelmät testataan yleensä alle tuhannen henkilön näytteillä. Monibiometrinen tietokanta voi olla joko todellinen tai virtuaalinen. Todellisessa tietokannassa erilaiset näytteet on kerätty samalta henkilöltä. Virtuaalisessa tietokannassa on yhdistetty yhden tietokannan henkilön näytteet toisen tietokannan henkilön näytteiden kanssa ja luotu näin yksi virtuaalinen henkilö. Virtuaalisen henkilön luominen perustuu olettamukseen, että saman henkilön eri biometriset näytteet ovat toisistaan riippumattomia. (Nandakumar 2005: 40)

3. ERILAISISTA BIOMETRIIKOISTA KOOSTUVAT JÄRJESTELMÄT

Tässä kappaleessa esitellään muutamia tutkimuksia, joissa on tutkittu henkilön tunnistamista useiden erilaisten biometristen menetelmien yhdisteinä. Yksi henkilö on siis antanut useita biometrisiä näytteitä eri sensoreille, jotka on sitten fuusioitu jollakin menetelmällä yhdeksi biometriseksi malliksi. Mielenkiintoisin on ehkä ensimmäisenä esiteltävä kasvo- ja sormenjälkikuvaan keskittyvä tutkimus. Kasvo- ja sormenjälkitunnistehan tulee myös uusiin biometrisiin passeihin, jotka meilläkin otetaan käyttöön.

Useiden erilaisten biometristen näytteiden yhdistelmien odotetaan olevan häiriön kestäviä. Niiden odotetaan helpottavan, ei universaalisuuden ongelmia eli tilanteita, joissa kaikilta käyttäjiltä ei saada kunnollista näytettä. Menetelmällä saavutettavien tulosten odotetaan olevan tarkempia, ja yhdistelmien arvellaan vaikeuttavan huijausyritysten onnistumismahdollisuuksia verrattuna yksibiometrisiin menetelmiin. (Nandakumar 2005: 19)

3.1 Sormenjälki ja kasvo

Snelick, Uludag, Mink, Indovina & Jain (2005) ovat tutkineet monibiometrista tunnistejärjestelmää käyttäen kaupallista *State of the art comersial off the shell* (COST) järjestelmää. Tutkimuksessa on käytetty noin tuhannen henkilön kasvo- ja sormenjälkitunnisteita. Kasvotunnisteina käytettiin FERET-kuvatietokantaa. Sormenjälkitietokantana oli suojattu tietokanta, josta tekijät eivät voi antaa tarkempia tietoja. He käyttivät kahta sormenjälkeä ja kahta kasvokuvaa jokaiselta 972:ta käyttäjältä. Tutkijat yhdistivät yksilöiden kasvokuvat ja sormenjäljet niin, että he saivat virtuaalisen tietokannan, joka koostui 972:ta kohteesta. Kaikilla kohteilla oli tietokannassa kaksi kasvo- ja kaksi sormenjälkikuvaa. Jokaiselta kohteelta määriteltiin yksi kasvo- ja yksi sormenjälkikuva kohdekuvaksi ja yksi kasvo- ja yksi sormenjälkikuva vertailukuvaksi. Normalisointi ja fuusion parametrien määrittämiseksi tutkijat käyttivät koko tietokantaa.

Vertailuarvot luotiin neljästä COTS järjestelmästä, kolmesta sormenjälkijärjestelmästä ja yhdestä kasvokuvajärjestelmästä. Jokaisesta neljästä järjestelmästä kaikkia vertailukuvia verrattiin kohdekuviin. Näin saatiin 972 oikeaa tulosta, joissa kuvat ovat samalta kohteelta, sekä 943,812 (972x971) väärää tulosta. Tutkijat käyttivät tulosten normalisointiin MM (min-max), ZS (Z-score), TH (tanh) ja QLQ (Quadric line quadric) metodeja. Fuusiometodeina tutkijat käyttivät SS (simple-sum), MIS (min-score), MAS (max-score), MW (matcher weighting) ja UW (user weighting) metodeja. Tutkijat kävivät läpi kaikki mahdolliset normalisointi ja fuusio vaihtoehdot tietokannan kaikille kohteille. Tutkijat selvittivät menetelmien EER- (equal error rate) ja FRR- (false reject rate) virhearvot (ks. kappale 2.3). Menetelmä on sitä parempi mitä pienempi on sen EER-arvo. Tutkijat saivat kolmelle yksittäiselle sormenjäljelle EER-arvot 3,96, 3,72 ja 2,16. Kasvokuvan tulos oli 3,76.

Taulukko 1. EER-arvot normalisointi- ja fuusio vaihtoehdoilla(%). (Snelick ym. 2005: 10)

Normalization Method	*Fusion Method*				
	SS	MIS	MAS	MW	UW
MM	0.99	5.43	0.86	**1.16**	***0.63**
ZS	*1.71	5.28	1.79	1.72	1.86
TH	1.73	**4.65**	1.82	*1.50	1.62
QLQ	**0.94**	5.43	***0.63**	**1.16**	***0.63**

Taulukossa 1 on sormenjälkien ja kasvokuvan yhdistelmän tulokset. Paras eli alhaisin EER-arvo on merkitty vaakarivillä *-merkillä ja pystyrivillä tummennettuna. Taulukosta nähdäänkin, että kaikkien muiden kuin MIS fuusion arvot ovat yksittäisien sormenjälkien ja kasvokuvan arvoja pienemmät. Tämä tarkoittaa sitä, että muilla kuin MIS fuusiolla yhdistetyillä sormenjälki- ja kasvokuvanäytteillä saadaan virheettömämpiä järjestelmiä. Tekijät tutkivat järjestelmän käyttäytymistä myös FRR -arvoilla. FRR–virhe tarkoittaa arvoa, jolla järjestelmään kuuluva henkilö hylätään tunnistamis- tai todentamistilanteessa. Mitä pienempi FRR–arvo on, sitä parempi on järjestelmä.

Taulukko 2. Väärien negatiivisten tunnistusten määrä toimittaessa välillä 1% - 0,1% FAR. (Snelick ym. 2005: 11)

Matcher	*FAR*	
	1%	0.1%
Fingerprint (Vendor 1)	62	85
Fingerprint (Vendor 2)	48	72
Fingerprint (Vendor 3)	25	32
Face	59	100
QLQ/SS Multimodal System	9	21

Taulukkoon 2 on merkitty kolmen yksittäisen sormenjäljen (fingerprint) ja yhden kasvokuvan (face) sekä QLQ/SS monibiometrisen järjestelmän FRR-arvot. Taulukosta nähdään, että väärien negatiivisten tunnistusten määrä on selvästi alhaisempi monibiometrisen järjestelmän kohdalla kuin yksibiometrisillä näytteillä.

Tutkimuksessa käytettiin tuhannen henkilön joukkoa ja se on huomattavasti suurempi kuin aikaisemmat tutkimukset. Tutkimus osoitti, että COTS tyyppinen monibiometrinen järjestelmä kasvo- ja sormenjälkikuville antaa paremman tuloksen kuin yksibiometrinen järjestelmä. Tulokset eivät olleet kuitenkaan yhtä hyviä kuin joissakin aiemmissa tutkimuksissa. Tämä oli odotettua ja johtui tutkijoiden mukaan siitä, että käytetty tarkempi COTS järjestelmä tasoitti fuusion etuja. Kun käytössä on tarkka järjestelmä, EER-arvon paraneminen yhdellä prosentilla puolittaa järjestelmän FAR ja FRR virheet. Vähemmän tarkan järjestelmän EER-arvon paraneminen yhdellä prosentilla vähentää FAR ja FRR virheitä vain 20 prosenttia.

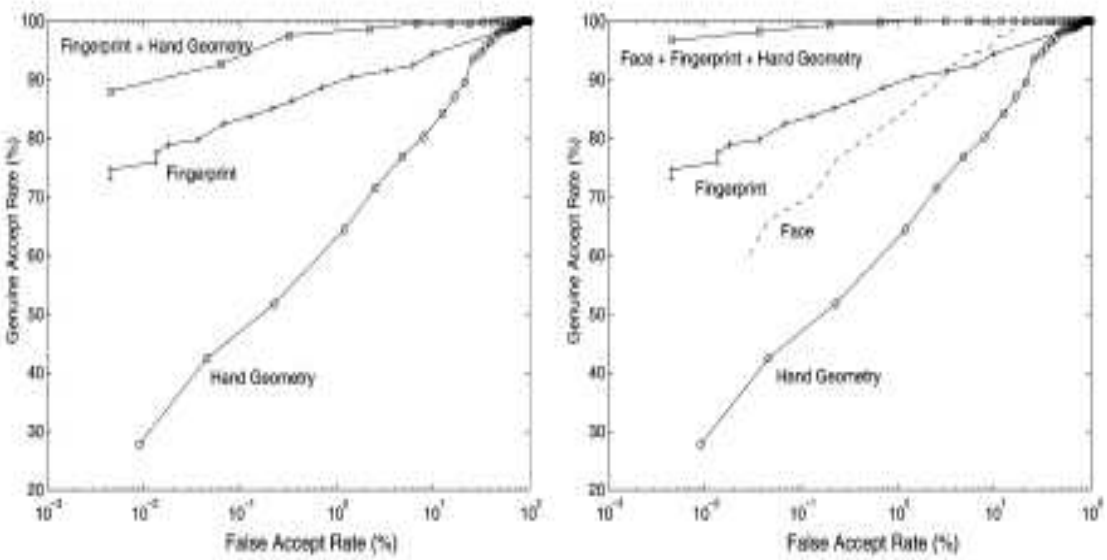
Tutkijoiden johtopäätös normalisointi- ja fuusiometodeista kasvo- ja sormenjälkikuville on se, että avoimissa populaatioissa, joissa henkilöiden tarkat ominaisuudet eivät ole tiedossa, kannattaisi käyttää MM normalisointia ja SS fuusiota. Tämä sopisi siis parhaiten juuri lentokentän kaltaiseen paikkaan. Määrätyissä suljetuissa populaatioissa, kuten jonkin toimiston henkilökunnalle, kannattaisi käyttää QLQ ja UW fuusiometodeita.

3.2 Sormenjälki, kasvo ja käden geometria

Ross ym. (2003) ovat tutkineet kasvo, sormenjälki ja käden geometriaa yhdistävää monibiometriikkaa. Heidän tutkimustietokantansa koostui 50 henkilöstä. Ensimmäisessä vaiheessa kaikki henkilöt antoivat viisi kasvo- ja sormenjälkinäytettä. Tätä dataa käytettiin luomaan 500 (50 x 10) aitoa tulosta ja 12250 (50 x 5 x 49) väärää tulosta. Toisessa vaiheessa kerättiin käden geometria tiedot erikseen viideltäkymmeneltä henkilöltä. Näistä saatiin myös 500 aitoa tulosta ja 12250 väärää tulosta. Jokainen ensimmäisen vaiheen henkilö sai satunnaisen parin toisen vaiheen henkilöstä. Näin saatiin vastaavat aidot ja väärät tulokset kaikille menetelmille.

Tutkijat kertoivat, että tässä tutkimuksessa summasääntö (sum rule) tuottaa parempia tuloksia kuin muut fuusio metodit. Tutkijoiden saamia tuloksia esitellään Kuvassa 5. Menetelmien toimivuutta on kuvattu GAR-arvon (genuine acceptance ratio) ja väärän hyväksynnän, eli FAR–arvon suhteella. GAR on kuvattu y-akselilla ja FAR x-akselilla. GAR ilmoitetaan prosentteina. Mitä lähempänä sataa prosenttia GAR on, sitä parempana järjestelmää voidaan pitää. Kuvassa vasemmalla on sormenjäljen, käden geometrian (hand geometry) ja näiden yhdistelmän käyrät.

Kuvasta 5 nähdään, että sormenjäljen ja käden geometrian fuusio antaa paremman tuloksen kuin kummatkin menetelmät yksinään. Esimerkiksi 0,01 FAR (kuvassa 10 potenssiin -2), osoittaa käden geometrialle GAR–arvoksi noin 40, sormenjäljelle noin 80 ja näiden yhdistelmälle noin 90 prosenttia. Oikealla on käden geometrian, kasvojen, sormenjäljen ja näiden kaikkien yhdistelmän käyrät. FAR–arvolla 0,01, käden geometrian GAR on noin 40, kasvojen noin 65, sormenjäljen noin 80 ja kaikkien yhdistelmän arvo on lähellä sataa prosenttia.



Threshold	Genuine Accept Rate (%)	False Accept Rate (%)
41	100.00	49.19
43	99.77	33.28
46	99.55	6.77
47	98.66	2.20
48	97.55	0.32
51	84.00	0.00

Threshold	Genuine Accept Rate (%)	False Accept Rate (%)
57	100.00	1.59
58	99.77	0.65
59	99.33	0.19
60	98.22	0.03
62	95.55	0.00

Kuva 5. Tulosten paraneminen käytettäessä summasääntöä. (Ross ym. 2003: 11)

3.3 Sormenjälki ja iiris

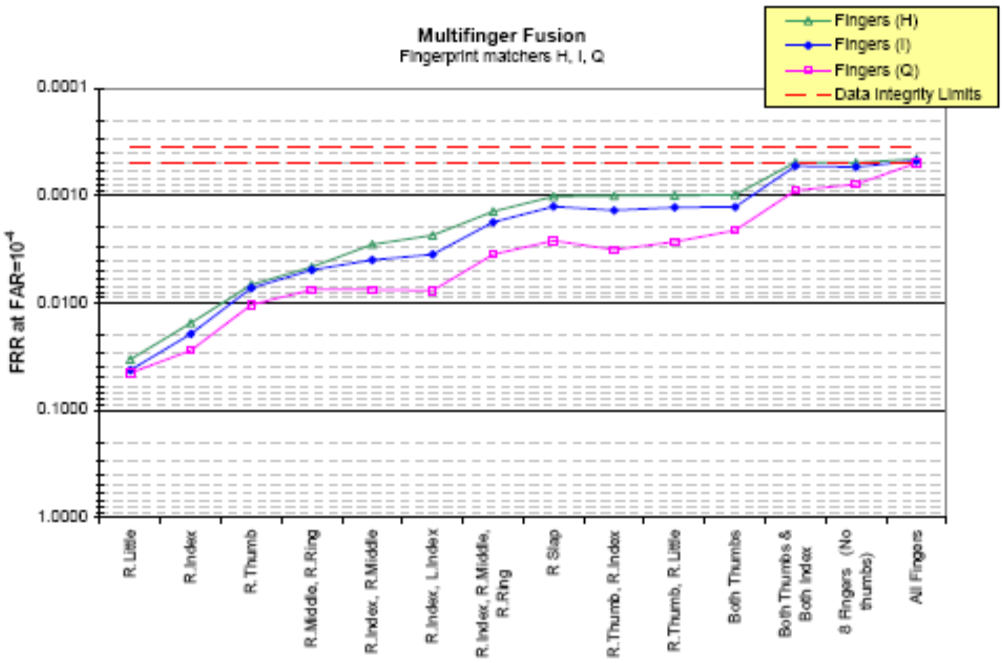
Nandakumar, Chen, Jain & Dass (2006) tutkivat sormenjäljen ja silmän iiriksen käyttöä henkilön tunnistamisessa. He käyttivät monibiometristä tietokantaa, joka on kerätty West Virginian yliopistossa. Se sisältää 320:tä henkilöltä kultakin viisi sormenjälki- ja iirisnäytettä. Tutkijat esittelevät todennäköisyys suhteeseen (likelihood ratio) perustuvan menetelmän, jolla saavutetaan laaturiippuva (quality-dependent) tulosten vertailufuusio. Tämä metodi ei vaadi järjestelmää asettamaan painotusta eri menetelmille, vaan se arvioi sekä aitojen että väärien tulosten laadun ja tuottaa todennäköisyys arvot, joiden mukaan menetelmät painottuvat.

Tutkijoiden mukaan sormenjäljen ja iiriksen fuusio parantaa järjestelmän todellista hyväksyntä eli GAR-arvoa (genuine acceptance ratio) huomattavasti verrattuna molempien menetelmien yksittäisiin tuloksiin. GAR ilmoitetaan prosentteina. Paras mahdollinen GAR olisi sata prosenttia, minkä saavuttaminen on kuitenkin lähinnä teoreettinen mahdollisuus. Laatupohjainen (quality-based) fuusio parantaa tuloksia kaikkein parhaiten. Esimerkiksi FAR –arvon ollessa 0,01 iiriksen GAR–arvo on 75,2 prosenttia. Sormenjäljen GAR –arvoa tutkijat eivät ilmoittaneet, mutta totesivat sen olleen iiristä huonompi. Sormenjäljen ja iiriksen, tuote- ja laatupohjaisen fuusion, GAR –arvot ovat 89,5 ja 94,8 prosenttia. Laatupohjainen fuusio on tulosten suhteen verrannollinen painotettuun summametodiin Tutkijat kuitenkin painottavat, että painotettu summasääntö vaatii tulosten normalisoinnin ja sopivien painotusten löytämisen paremman tarkkuuden saavuttamiseksi (ks. kappale 2.3). Tutkijoiden ehdottama laatupohjainen fuusiomalli parantaa merkittävästi sormenjäljen ja iiriksen monibiometrisen yhdistelmän tuloksia

3.4 Kasvot ja useiden sormenjälkien yhdistelmä

Ulery, Hicklin, Hallinan, Watson & Fellner (2006) ovat tutkineet kasvojen ja useiden sormenjälkien yhdistelmät toimivuutta biometrisessa tunnistamisessa. He käyttivät vertailuun laajaa NBDF06 tietokantaa, josta he käyttivät kolmea kasvokuvaa (A, B ja C) ja kolmea sormenjälkikuvaa (H, I ja Q). Vertailtavat tulokset yhdistettiin Likelihood ratios metodilla. Tämä metodi arvioi Neyman-Pearson optimoinnin FRR:n minimoimiseksi tietyllä FAR-arvolla. Se on tutkijoiden mukaan ollut tehokkain menetelmä useissa tutkimuksissa. Testihenkilöillä oli n-kappaletta sormenjälkiä tai n-kappaletta sormenjälkiä sekä kasvokuva. Tutkijat käyttivät neljäätoista eri sormenjälkiyhdistelmää ja yhdeksää erilaista vertailua (kolme sormenjälkeä * kolme kasvokuvaa) Koesarjat koostuivat neljästä testistä. Ensimmäisessä testisarjassa oli oikean henkilön yksi sormenjälkikuva. Toisessa oli oikean henkilön sormenjälki- ja kasvokuva. Kolmannessa oli virtuaalihenkilön sormenjälki- ja kasvokuva ja neljännessä yksi vertauskohde (kasvokuva). Jokaiseen testisarjaan tutkijat saivat yli 64000 aitoa ja

122000 huijausnäytettä. Tulosten tarkkuutta heikensivät tietokannan epätarkkuudet. NBD06 tietokannassa oli 33 henkilöä (0,051%), joiden yksi tai useampi sormenjälki tunnistettiin väärin sekä 24 henkilöä (0,037%), joiden kasvokuva tunnistettiin väärin. On huomioitava, että FRR voi läpäistä 0,051 prosenttisen rajan joidenkin sormenjälkiyhdisteiden osalta, muttei 0,037 prosentin rajaa. Tämän tutkimusten tuloksia esitellään kuvissa 6 ja 7.

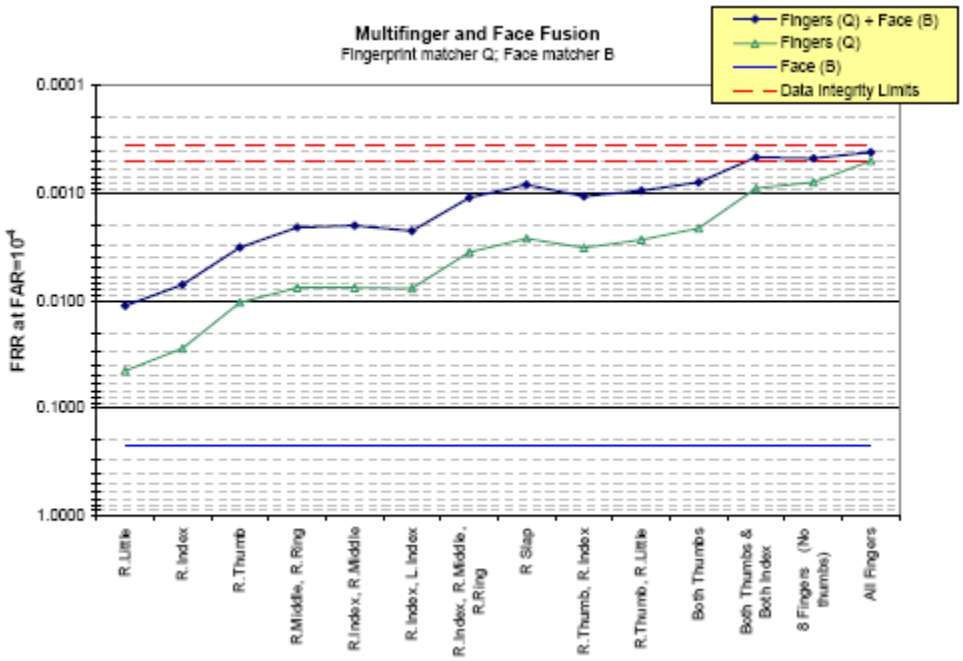


Kuva 6. Useiden sormenjälkien fuusio. (Ulery ym. 2006: 13)

Kuvassa 6 on kuvattu sormenjälkien tarkkuutta väärien negatiivisten tunnistusten (FRR) kohdalla. FRR-arvot on merkitty y-akselille ja sormenjäljet x-akselille. Yksittäisten sormenjälkien ja sormenjälkien yhdistelmien, tulokset on merkitty pisteinä, joiden läpi on vedetty käyrät. Mitä korkeammalle pisteet ja käyrät sijoittuvat sitä pienempi on menetelmän FRR–virhe. Nyt nähdään, että useiden sormien yhdistelmä parantaa järjestelmän tarkkuutta. Samoin nähdään se, että mitä sormia käytetään, on vähintään yhtä tärkeää kuin se montako sormea yhdistelmässä käytetään. Peukalot (thumb) ovat

selvästi tarkemmat kuin muut sormet. Peukalot ovat yhtä paljon etusormia (index) tarkemmat kuin nimettömät pikkurillejä (little) tarkemmat. Kahden peukalon yhdistelmä on paljon tarkempi kuin kahden keskisormen yhdistelmä. Neljän sormen yhdistelmä on yhtä tehokas kuin peukalon ja jonkin toisen sormen yhdistelmä.

Kuvassa 7 on tulokset kokeista, joissa tutkijat tutkivat useiden sormenjälkien ja kasvokuvien yhdistelmiä. Tulokset on kuvattu samalla tavalla kuin kuvassa 6. Kuvasta näkee, että kasvojen ja sormenjälkien yhdistelmä on kaikissa tapauksissa hyödyllinen. Kun lisätään kasvokuva yhteen tai kahteen sormenjälkeen, laskee FRR melkein suurusluokan verran. Nimettömän, keskisormen (middle) ja kasvojen yhdistäminen on tehokkaampi kuin neljän sormen yhdistelmä.



Kuva 7. Useiden sormenjälkien ja kasvojen yhdistelmä. (Ulery ym. 2006: 14)

Tutkijoiden mukaan sormenjälkien yhdistelmät ovat hyvin tehokkaita, samoin sormenjälkien ja kasvojen yhdistelmät. Kun yhdistetään kaksi sormenjälkeä tai yksi sormenjälki ja kasvokuva FRR-arvot laskevat 50 – 90 prosenttia. Kahden sormenjäljen

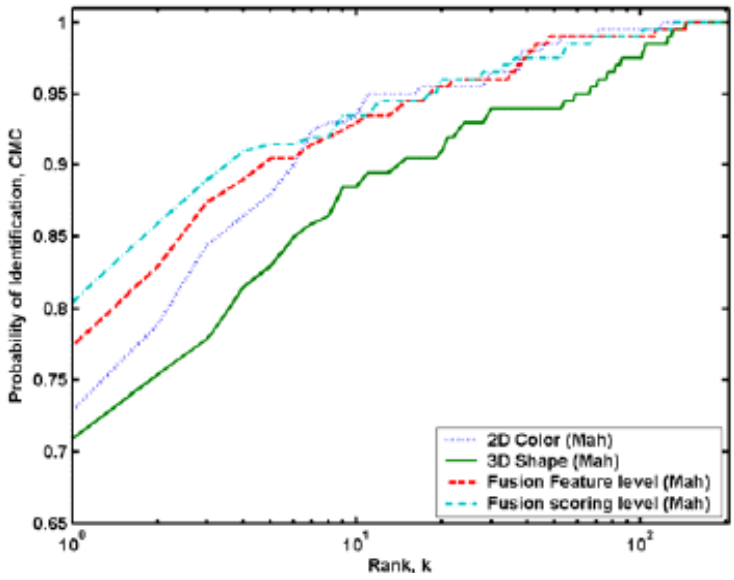
ja kasvojen yhdistelmä oli tehokkaampi kuin neljän sormenjäljen. Eri sormenjälki yhdistelmien tulosten määrittäminen oli tutkijoiden mielestä vaikeaa, koska tulosten tarkkuus riippui sormien sijainnista ja järjestyksestä. Peukalonjäljet olivat suuremman kokonsa ansiosta tarkemmat kuin muiden sormien jäljet. Kaikissa tapauksissa tulosten korrelointi rajoitti sormenjälkiyhdistelmien hyötyjä. Vahvin korrelaatio oli vierekkäisillä sormilla. Pikkurilli oli yllättäen kuitenkin suhteellisen tehokas yhdistelmissä. Tämä johtui varmaankin sen erilaisesta käyttäytymisestä laatuvirheiden suhteen. (Ulery ym. 2006: 1-17)

4. MONTA SENSORIA SAMALLE BIOMETRIIKALLE

Tässä kappaleessa esitellään muutamia tutkimuksia, joissa on tutkittu henkilön tunnistamista ja henkilön identiteetin varmentamista yhdestä biometrisesta kohteesta johdettujen erilaisten yhdisteiden avulla. Henkilöstä on siis otettu esimerkiksi kasvokuva kahdella erilaisella kameralla ja nämä näytteet on sitten fuusioitu yhdeksi biometriseksi tunnisteeksi. On myös tutkittu, voidaanko yhdestä kuvasta vetää kaksi erilaista biometrista mallinetta ja fuusioida ne yhdeksi biometriseksi tunnisteeksi. Lopuksi esitellään monibiometriikan uusimman menetelmän prototyyppi. Siinä on kehitetty sensori, joka kuvaa kaikki tunnetut käden biometriset tunnisteet yhtäaikaisesti.

4.1 Kasvotunnistaminen kaksi- ja kolmiulotteisesti

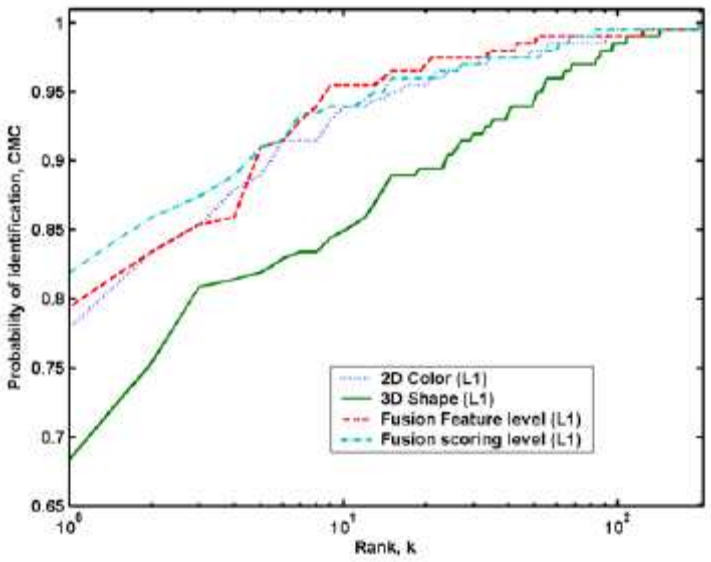
Godil, Ressler & Grother (2004) ovat tutkineet kolmiulotteista kasvotunnistamista, henkilön tunnistamiseksi ja identiteetin varmistamiseksi, kasvojen eri asennoissa ja erilaisissa valaistusolosuhteissa. Sitten he vertasivat tuloksia kaksiulotteisiin värikuvien tuloksiin ja lopuksi he tutkivat näiden kahden menetelmän yhdistämistä. He käyttivät CAESAR (civilian american and european surface anthropometry resource) tietokantaa. Siihen kuuluu 5000 ihmistä. Tämä tutkimus koostui kahdesta sadasta kohteesta, joilta kaikilta tuli kuvat seisoessa ja istuessa. Kolmiulotteisten kuvien ottamiseksi tutkijat käyttivät kolmeulotteista laserskanneria ja kaksiulotteisten kuvien ottamissa he käyttivät digitaalista kameraa. Yhdistämisessä tutkittiin fuusioita kuva- ja tulostasolla. Kuvatasolla kolmiulotteisten- ja värikuvien tiedot yhdistettiin. Tulostasolla tutkijat tutkivat fuusiota minimi- (min), keskiarvo- (mean), maksimi- (max) ja tulo- (product) säännöillä. Tuloksia esitellään kuvissa 8 ja 9.



Kuva 8. CMC-käyrät 2D ja 3D kuvalle, sekä kuvataso- ja tulostasofuusioille. (Godil ym. 2004: 8)

Tutkijoiden tulosten mukaan CMC (cumulative match characteristic) (ks. kappale 2.3) 2D kuvalle on 0,728, ja 3D:lle 0,708. Kuvatason fuusiolle arvo on 0,7738 ja tulostason fuusiolle 0,81. Kuvassa 8 on tulosten mukaan piirretty CMC-käyrät kaksiulotteiselle ja kolmeulotteiselle kuvalle, kuvafuusiolle ja tulosfuusiolle. Y-akselilla on identiteetin varmentamista kuvaavat arvot ja x-akselilla tietokannan kokoa kuvaavat arvot (rank). Mitä korkeampi y-akselin CMC –arvo on, sitä varmempi on järjestelmä. Käyrässä, joka sisältää kaikki mahdolliset arvot, tunnistamisen todennäköisyys on sata prosenttia.

Tutkijat tutkivat myös L1 luokittelua kuvien yhdistämisessä. Tulosten mukaan, CMC 2D kuvalle on 0,778, ja 3D:lle 0,683. Kuvatason fuusiolle arvo on 0,794 ja tulostason fuusiolle 0,82. Kuvassa 9 on näiden tulosten mukaan piirretty CMC (cumulative match characteristic) kaksiulotteiselle ja kolmeulotteiselle kuvalle, kuvafuusiolle ja tulosfuusiolle L1 luokiteltuna.



Kuva 9. CMC-käyrät 2D ja 3D kuville, sekä kuvataso- ja tulostasofuusioille L1 luokiteltuina. (Godil ym. 2004: 8)

Tulokset osoittavat, että kaksiulotteiset tunnisteet antavat parempia tuloksia kuin kolmiulotteiset. Samoin nähdään, että fuusio antaa parempia tuloksia kuin yksittäiset biometriikat. Fuusio tulostasolla antaa myös parempia tuloksia kuin fuusio kuvatasolla. Tuloksiin vaikuttaa varmasti se, että kolmiulotteiset laserskanneri kuvat eivät ole yhtä tarkkoja kuin digitaalisella kameralla otetut kuvat. Kolmiulotteiset skannerit ovat myös paljon kalliimpia kuin tavalliset digikamerat.

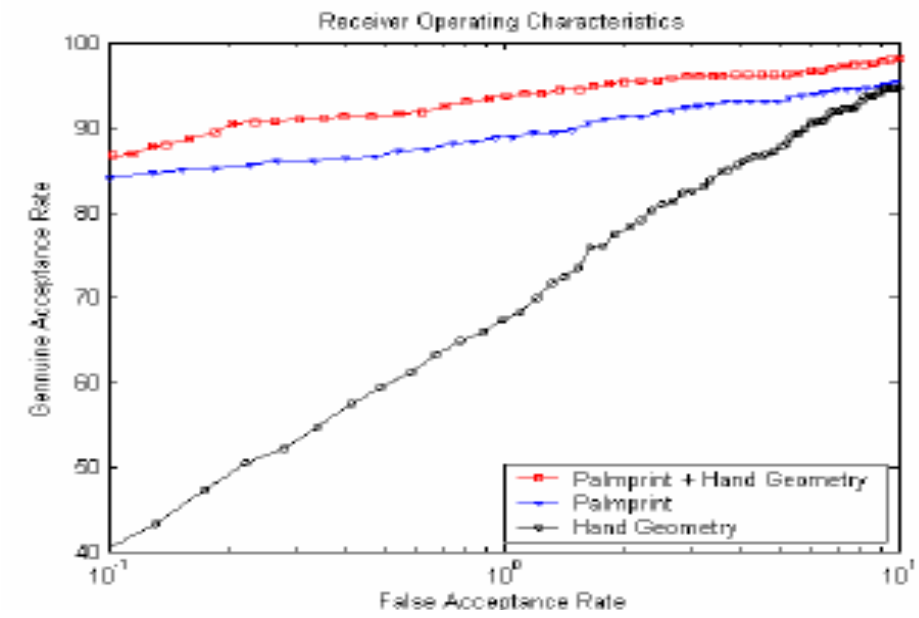
4.2 Käden geometria ja kämmenen jälki

Kumar, Wong, Shen & Jain (2003) ovat tutkineet käden geometrian ja kämmenen jäljen (palmprint) yhdistämistä. He ovat käyttäneet yhtä digitaalista kameraa, jonka kuvasta on vedetty molemmat biometriset näytteet. He keräsivät tuhat käden kuvaa. Testihenkilöitä oli mukana sata ja he kaikki antoivat kymmenen kuvaa. Ensimmäisiä viittä kuvaa jokaiselta käytettiin harjoittelemiseen ja loppuja viittä kuvaa tutkimukseen. Tutkimuksen tuloksia esitellään taulukossa 3.

Taulukko 3. Kämmenen jäljen, käden geometrian sekä kahden fuusion, virhearvot. (Kumar ym. 2003: 6)

	FAR	FRR	Decision Threshold
Palmprint	4.49 %	2.04 %	0.9830
Hand Geometry	5.29 %	8.34 %	0.9314
Fusion at Representation	5.08 %	2.25 %	0.9869
Fusion at Decision	0 %	1.41 %	0.9840

Taulukossa 3 on 472:den testikuvan tuloksista saadut väärät positiiviset tunnistamiset (FAR), väärät negatiiviset tunnistamiset (FRR) sekä käytetty kynnysarvo (decision threshold). Kaikki käyttäjät eivät onnistuneet antamaan kelvollista näytettä. Testin laadun varmistamiseksi 28 tällaista kuvaa poistettiin. Taulukosta nähdään, että kämmenen jäljen (palmprint) virhearvot ovat matalampia kuin käden geometrialla (hand geometry). Tämä tarkoittaa sitä, että kämmenen jälkeen perustuva tunnistaminen on tarkempaa kuin käden geometriaan. Tuloksista nähdään myös, että yhdistelmistä päätöksentekotason fuusiolla (decision level) on kaikkein pienimmät virheluvut. Esiteltyjä tuloksia on kuvattu GAR arvoilla kuvassa 10.



Kuva 10. Käden geometrian ja kämmenen jäljen tulokset. (Kumar ym. 2003: 6)

Kuvassa 10 menetelmien toimivuutta on kuvattu GAR-arvon (genuine acceptance ratio) ja väärän hyväksynnän eli FAR–arvon suhteella. GAR on kuvattu y-akselilla ja FAR x-akselilla. Mitä lähempänä sataa prosenttia GAR on, sitä parempana järjestelmää voidaan pitää. FAR arvon ollessa 0,01, käden geometrian GAR on noin 40, kämmenen jäljen 85 ja näiden yhdistelmän noin 87 prosenttia. Tämä tarkoittaa, että kämmenen jälkeen perustuva tunnistaminen on tarkempaa kuin käden geometriaan. Samoin voidaan sanoa, että yhdistäminen antaa paremman tuloksen kuin kumpikaan biometriikka erikseen. Fuusiomenetelmänä tutkijat ovat käyttäneet päätöksentekotasoa (decision level).

Saavutettuja tuloksia voidaan pitää merkittävinä siksi, että tässä järjestelmässä käytettiin vain yhtä kameraa eli sensoria. Tämän voidaan olettaa säästävän kirjautumisaikaa ja järjestelmän vaatimia kustannuksia. Tutkijat toteavat myös, että fuusio päätöksentekotasolla, käyttäen maksimisääntöä, tuottaa parhaat tulokset. (Kumar ym. 2003)

4.3 Infrapunavalo ja näkyvävalo kasvotunnistamisessa

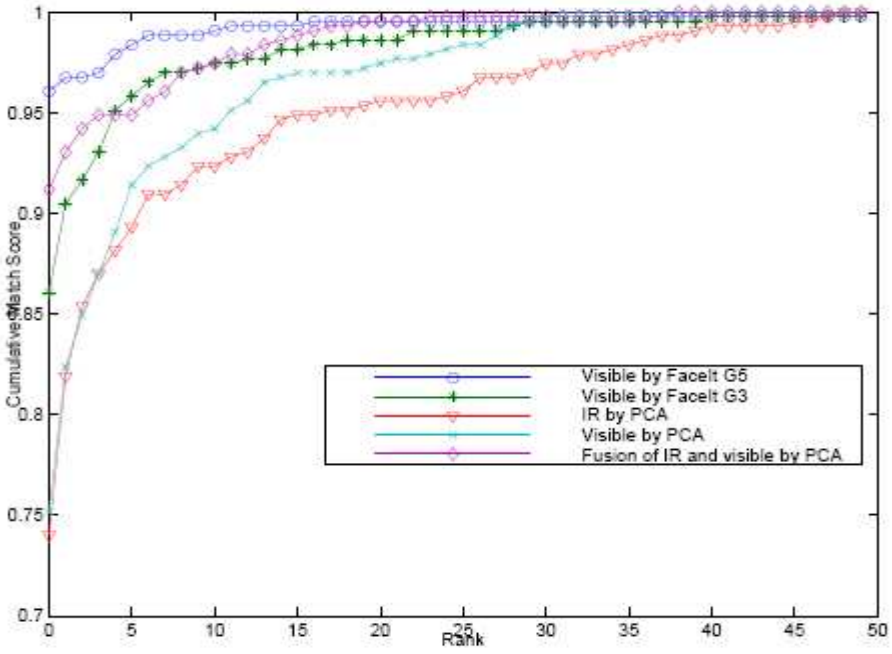
Chen, Flynn & Bowyer (2005) ovat tutkineet infrapunavalon (IR) ja näkyvän valon (visible light) käyttöä kasvokuvien biometrisessä tunnistamisessa. Heidän tietokantansa koostui 10916 kuvasta kumpaakin biometristä menetelmää kohden. Kuvat olivat 488:a eri ihmiseltä. Suurin osa kuvista oli kerätty Notre Damen yliopistossa vuosina 2002 ja 2003. Kuvia otettiin viikoittain ja useimmat henkilöt osallistuivat kuvauksiin eri aikoihin eri viikoilla. Näin saatiin aikaväli (time-lapse) mukaan testiin. Kuvauksissa käytettiin erilaisia valaistusolosuhteita. Yksi oli sellainen, jossa kuvattavaan nähden keskeltä osoittava valo oli pois päältä. Tätä olosuhdetta tutkijat kutsuvat ”LF” -valaistukseksi. Toisessa valaistusvaihtoehdossa oli kaikki valot päällä. Tätä he kutsuvat ”LM” -valaistukseksi. Jokaista henkilöä ja jokaista valaistus olosuhdetta kohden otettiin kaksi kuvaa. Ensimmäisessä kuvassa henkilöllä oli luonnollinen ilme ja sitä kutsutaan ”FA” -kuvaksi. Toisessa henkilö hymyili ja sitä kutsutaan ”FB” -kuvaksi. Tunnistamisessa tutkijat käyttivät PCA algoritmia ja kaupallista FaceIt algoritmia. Tutkijoiden tuloksia on esitelty seuraavassa.

Taulukko 4. Parhaat tulokset yhdestä aikavälisestä kokeesta infrapuna- ja näkyvällä valolla. (Chen ym. 2005: 30)

Modality \ Condition	FA|LM	FB|LF	FA|LF	FA|LM + FB|LF	FA|LM FA|LF
IR	0.92	0.73	0.92	0.90	0.93
Visible	0.81	0.73	0.82	0.85	0.85
IR + Visible	0.95	0.97	0.90	N/A	N/A

Taulukossa 4 on infrapuna ja näkyvän valon testin parhaat tulokset. Tulokset ilmoitetaan CMC –arvoina. Tunnistaminen on sitä todennäköisempää mitä lähempänä yhtä CMC –arvo on. Testissä käytetyt kuvat ovat joko kahdesta eri menetelmästä (IR ja Visible) tai samalta menetelmästä, mutta kahdesta eri olosuhteesta (FA|LM + FB|LF ja FA|LM + FA|LF). Tulokset ovat huonommat yhdistettäessä FA|LM ja FB|LF kuin FA|LM. Infrapunalla paras tulos yhdistettäessä FA|LM ja FB|LF on 0,85 ja yhdistettäessä FA|LM ja FA|LF samoin 0,85. FA|LM, FB|LF ja FA|LF antaa yksinään tulokset 0,81, 0,73 ja 0,82. Yhdistettäessä infrapunan ja näkyvän valon FA|LM, FA|LF ja FB|LF saadaan tuloksiksi 0,95, 0,97 ja 0,90. Nämä ovat selvästi parempia kuin saman menetelmän yhdistelmillä.

Kuvasta 11 nähdään aikavälillisen (time-lapse) tunnistamisen CMC–käyrät infrapunavalolle ja näkyvälle valolle, käytettäessä PCA algoritmia ja FaceIt algoritmia. CMC –arvot on kuvattu y-akselilla. Mitä korkeammat luvut menetelmä antaa y-akselilla sitä tarkempi se on. Käyristä nähdään, että näkyvällä valolla (visible) FaceIt G3 ja G5 voittaa sekä näkyvän valon, että infrapunavalon (IR) PCA:n. Samoin nähdään, että infrapunan ja näkyvän valon fuusio voittaa kaikki muut vaihtoehdot paitsi näkyvän valon G5:n.



Kuva 11. Infrapuna ja näkyvän valon kuvien CMC –käyrät. (Chen ym. 2005: 32)

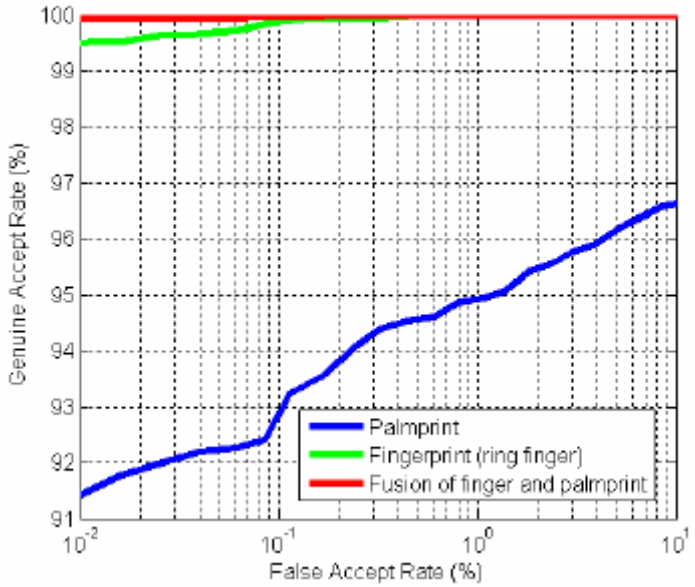
Tutkijoiden mukaan samanaikaisessa tunnistamisessa kumpikaan menetelmä ei ole selkeästi toista parempi. Aikavälisessä tunnistamisessa infrapunavalon ja näkyvän valon menetelmien osumatarkkuus aleni. Yli viikon viive kuvien otosta tunnistamiseen heikensi tuloksia enemmän kuin pelkkä viikon viive. Selvää näyttöä siitä, että tulokset olisivat heikentyneet samassa tahdissa ajan kasvaessa ei tutkijat kuitenkaan löytäneet. Infrapunakuvien tason vaihtelu ajan kuluessa tulisi kuitenkin ottaa tutkijoiden mielestä huomioon siihen perustuvia biometrisiä järjestelmiä suunniteltaessa.

4.4 Koko käden monibiometrinen tunnitemenetelmä

Rowe, Uludag, Demirikus, Parthasaradhi & Jain (2007) ovat suunnitelleet ja kehittänet prototyypin järjestelmälle, joka käyttää koko käden biometrisiä tietoja yhtäaikaisesti. Järjestelmä perustuu monispektriseen tekniikkaan, joka antaa samalla kertaa tiedot käyttäjän sormenjäljistä, käden geometriasta ja kämmenen jäljestä, käyttäjän kirjautuessa järjestelmään. Tämän järjestelmän etuja aikaisempiin järjestelmiin

verrattuna on nopeampi kirjautumisaika, parempi kuvien laatu ja parempi suoja huijauksia vastaan. Järjestelmän avulla kädestä saadaan monipuolisia biometrisia tietoja. Niitä ovat neljän sormen sormenjäljet sekä osa peukalon jälkea Kämmenen jäljen tärkeimmät osat, kuten pääviivat (principal lines), rypyt (wrinkles), harjanteet (ridges) ja muut yksityiskohdat. Kämmenen muoto (shape) sekä ihon rakenne (texture).

Tutkijat keräsivät tietokannan viideltäkymmeneltä vapaaehtoiselta henkilöltä kahtena eri päivänä. Vapaaehtoisilta kerättiin kumpanakin kertana kolme MSI dataotosta sekä oikeasta että vasemmasta kädestä. Näin saatiin 600 MSI dataotosta sadasta yksilöllisestä kädestä. Monibiometriseen fuusioon tutkijat kokeilivat yhden sormen (nimetön) tulosten yhdistämistä kämmenenjälkikuvaan. Fuusiossa käytettiin painotettua summasääntöä. Kämmenkuvalle painotus 0,15 ja sormenjäljelle 0,85. Tämän yhdistelmän tuloksia on esitelty kuvassa 12.



Kuva 12. Nimettömän ja kämmenenjäljen fuusion ROC-käyrä. (Rowe ym. 2007: 6)

Kuvasta 12 tutkimuksen tuloksia on kuvattu ROC–käyrän (receiver operating characteristic) avulla. Se eliminoi kynnysarvon vaikutuksen (ks. kappale 2.3). Y-akselilla on GAR-arvot ja x-akselilla FAR-arvot. Nyt nähdään, että kämmenen jäljen GAR on noin 91, sormenjäljen noin 99,5 ja fuusion sata prosenttia. Voidaankin sanoa,

että yksittäisen sormenjäljen ja kämmenenjäljen yhdistelmä peittoaa kummankin menetelmän yksinään saaman tuloksen. Tämä oli odotettavaakin aikaisempien tutkimusten perusteella. Tutkijoiden kehittämän, koko käden samanaikaiseen monibiometriseen tunnistamiseen perustuvan järjestelmän, etuja aikaisempiin järjestelmiin verrattuna on se, että se vaatii käyttäjältä vain yhden näytteenannon. Sillä saadaan samalla kertaa monibiometrinen data, joka koostuu sormenjäljestä, kämmenestä ja käden geometriasta. Tässä järjestelmässä siis yksi sensori voi kerätä useita erilaisia biometrisia näytteitä. Tämä vähentää järjestelmän käyttämää kokonaisaikaa ja tekee siitä yksinkertaisemman verrattuna useiden sensoreiden järjestelmiin. Yksi pieni haitta on se, että järjestelmä vaatii hieman enemmän laskentakapasiteettia. Se on kuitenkin varsin merkityksetön haitta varsinkin kun tiedetään, että uutta tekniikkaa ja tehokkaampia mikroprosessoreja kehitetään.

5. AUDIOVISUALINEN FUUSIO JA NÄYTTEEN ELÄVYYS

Fuusioimalla useita biometrisiä näytteitä järjestelmästä saadaan entistä immuunimpi tunkeutumisyrityksille. Esimerkiksi audiovisuaalisessa tunnistejärjestelmässä tunkeutujan pitäisi pystyä “imitoimaan” henkilöä samanaikaisesti sekä audio- että visuaalisesti. Audiovisuaalisuus lisää myös järjestelmän luotettavuutta ja käytettävyyttä. Esimerkiksi kasvo- ja äänitunnisteiden käytössä valaistusolosuhteet voivat heikentää kasvotunnisteen toimivuutta, mutta äänitunnisteeseen ne ei vaikuta. Samoin melun heikentäessä äänitunnistetta voi kasvotunniste toimia luotettavasti. Nykyiset audio-visuaaliset biometriset tunnistejärjestelmät toimivat yleensä kasvotunnisteiden osalta staattisesti. Tämä voi heikentää järjestelmän luotettavuutta tunkeutujia vastaan. Luotettavuuden parantamiseksi järjestelmän pitäisi pystyä hoitamaan henkilön tunnistaminen niin, että varmistuisi henkilön olevan elävä ihminen eikä esimerkiksi pelkkä kuva tai muu vastaava väärennös. Tällaista menetelmää kutsutaan elävyyden (liveness) tunnistamiseksi. (Chetty ym. 2005: 1)

Elävyyden kytkemisellä monibiometriseen järjestelmään voidaan parantaa järjestelmän turvallisuutta, luotettavuutta ja tehokkuutta. Biometrinen järjestelmä voi olla altis erilaisille huijauksille. Sormenjälkikuvia on voitu valmistaa ja jopa väärennettyjä sormia on kehitetty onnistuneesti. Pahin vaihtoehto olisi kuolleen henkilön sormen käyttäminen järjestelmän huijaamisessa. Lähes kaikkia yksittäisiä tunnistemenetelmiä voidaan periaatteessa yrittää huijata ja kehittämällä erilaisia estomenetelmiä näiden huijausten toteuttaminen voidaan tehdä huomattavasti vaikeammaksi. (Schuckers, Hornak, Norman, Derakhshani & Parthasaradhi 2002: 10, 14, 25)

5.1 Videokuvaan perustuva tunnistaminen

Ouyang & Lee (2006) ovat tutkineet videokuvan käyttöä audiovisuaalissa tunnistamisessa. Heidän tutkimuksessaan oli staattinen ja dynaaminen näytteenotto puhuvista huulista, yhdistettynä lausuntaan perustuvaa tunnistamiseen. He esittelevät uuden menetelmän, jossa yhdistyy puhuvien huulten staattinen ilme ja liikekuviot.

Tutkimus perustuu XM2VTS tietokantaan. Se on yksi laajimmista biometriseen tunnistamiseen suunnitelluista audiovisuaalisista tietokannoista. Sen kuvasarjat ja puhedata on synkronisesti äänitetty. Äänitys koostui neljästä tapahtumasta, joissa 295 henkilöä lausui englannin kieliset numerot nollasta yhdeksään. Kahden tapahtuman aikaväli oli kuukausi. Videokuva tallennettiin sinistä taustaa vasten. Testien tulokset on esitelty taulukossa 5.

Taulukko 5. Videokuvaan perustuvan audiovisuaalisen tutkimuksen tulokset. (Ouyang ym. 2006: 4)

Session		Identification Rate			
Train	Test	Geometric	Behavioral	Combined	1st Frame
s_1, s_2	s_4	97.00%	89.50%	98.00%	84.00%
s_1, s_2, s_3	s_4	99.25%	94.00%	99.50%	93.75%
s_1, s_2	s_3	96.75%	89.75%	97.25%	78.25%
s_1, s_2, s_4	s_3	98.75%	94.75%	99.25%	91.25%
s_1, s_3	s_2	96.25%	88.25%	96.75%	83.50%
s_1, s_3, s_4	s_2	98.50%	93.25%	98.75%	92.00%
s_2, s_3	s_1	96.25%	88.75%	97.00%	80.75%
s_2, s_3, s_4	s_1	98.50%	94.00%	98.75%	88.25%

Taulukossa 5 on esitelty neljä ryhmää. Niistä S1 esittää geometrista (geometric) ja S2 käytökseen (behavioral) perustuvaa näytettä. S3 esittää näiden lineaariyhdistettä. Ryhmässä S4 on vain jokaisen kuvasarjan ensimmäinen kuva. Tulokset on esitelty GAR -arvon (genuine acceptance ratio) avulla. Mitä korkeampi GAR–arvo sitä parempi tunnistemenetelmä. Taulukosta nähdään, että pelkästään geometriaan perustuvat näytteet saavat korkeammat tulokset kuin käytökseen perustuvat. Ne siis peittoavat pelkästään käytökseen perustuvat näytteet. Yhdistettyjen näytteiden paremmuus pelkästään geometrisiin nähden on 0,25 – 1 prosenttia. Käytökseen perustuvat näytteet siis korreloivat geometristen näytteiden kanssa ja niitä voisi pitää vähintäänkin täydentävänä informaationa. Kun edellisten näytteiden tuloksia verrataan pysäytyskuvan tuloksiin on parannukset vieläkin suurempia.

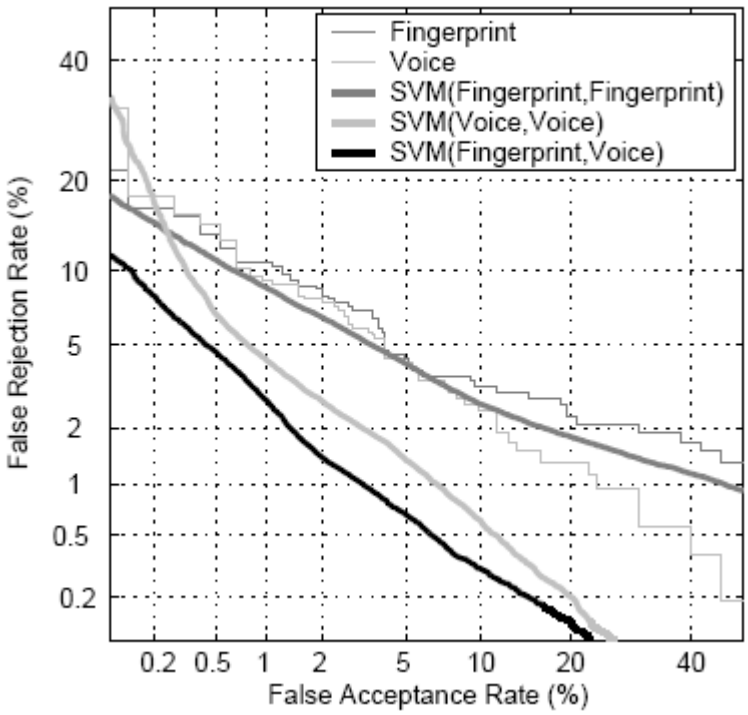
Tässä tutkimuksessa on siis esitelty uusi huulten ominaisuuteen ja geometriaan perustuvan audio-visualisen tunnistejärjestelmä. Tutkimuksen tulosten mukaan staattinen ja dynaaminen menetelmä antaa paremmat tulokset kuin pysäytyskuvaan perustuva tunnistaminen. Käytökseen perustuva menetelmä voi täydentää geometrista menetelmää. Yhdistämällä nämä monibiometriseksi järjestelmäksi saadaan parhaat tulokset.

5.2 Äänen ja sormenjäljen yhdistäminen

Fierrez-Aquilar, Ortega-Garcia, Gonzales-Rodriquez & Bigun (2004) tutkivat ääninäytteen ja sormenjälkikuvan yhdistämistä biometriseksi tunnisteeksi. Tutkijoiden käyttämä äänidata koostui testiryhmän jäsenten lyhyistä lausahduksista, tässä tapauksessa käyttäjän puhelinnumerosta. Ryhmä koostui 75:tä käyttäjästä, jotka kaikki antoivat kymmenen ääninäytettä kuukauden väliajoin. Kolmea ensimmäistä tutkijat käyttivät harjoitusdatan muodostamiseen ja loput seitsemän päätyi varsinaiseksi testidataksi. Lisäksi suoritettiin kymmenen huijausyritystä jokaista käyttäjää kohti. Sormenjälkidatana tutkijat käyttivät MCYT tietokantaa. Se koostuu 330 henkilöstä, jotka oli valittu neljästä espanjalaisesta akateemisesta järjestelmästä. Jokainen käyttäjä antoi 240 sormenjälkikuvaa tietokantaan, mutta testissä on käytetty vain 75:den ensimmäisen käyttäjän nimettömän sormen kuvia. Tutkijat eivät tutkineet ainoastaan menetelmien monibiometristä fuusiota. He selvittivät myös, parantaako saman menetelmän yhdistäminen järjestelmän luotettavuutta.

Kuvassa 13 on esitelty sormenjäki- ja äänitunnistemenetelmien, yksi- ja monibiometristen, SVM fuusioiden tulokset. Niiden esittelemiseen tutkijat käyttävät DET (detection error tradeoff) käyriä. Tällaiset käyrät kuvaavat tietynlaista kompromissia FRR- ja FAR-virheiden välillä. Mitä vähemmän virheitä menetelmä tuottaa, sitä lähempänä origoa käyrän päät sijaitsevat. Kuvasta 13 nähdään, että moni-anturiset (multi-probe) menetelmät vähentävät virheitä, ja siten parantavat identiteetin varmentamisen tuloksia, verrattuna menetelmien yksibiometrisiin tuloksiin. Lähimpänä

origoa sijaitsee sormenjäljen ja ääninäytteen yhdistelmä. Se siis tuottaa tutkituista menetelmistä vähiten virheitä.



Kuva 13. Sormenjäki- ja äänimenetelmien yksi- ja monibiometrinen fuusio.(Fierrez-Aquilar ym. 2004: 7)

Tutkijat tutkivat myös menetelmien EER (equal error rate) arvoja. Mitä pienempi EER on, sitä parempi on menetelmän suorituskyky. Näistä tuloksista voidaan mainita, että sormenjälkitunnisteeseen perustuva menetelmä antoi EER tulokseksi 4,40 prosenttia. Äänitunnisteen vastaava EER tulos oli 2,70 prosenttia. Monibiometristen järjestelmien EER oli 1,65 prosenttia. Parhaan tuloksen antoi monibiometrinen sormenjälkikuvan ja ääninäytteen yhdistelmä.

5.3 Ääni-, kasvo- ja käsialatunnistaminen

Allano, Morris, Sellahewa, Garcia-Salicetti, Koreman, Jassim, Ly-Van, Wu & Dorizzi (2006) ovat tutkineet tulosten fuusiometodien käyttöä monibiometrisessä

tunnistamisessa. Nämä testit kuuluivat SecurePhone – projektiin, jonka tavoitteena oli kehittää biometriseen tunnistamiseen perustuva mobilinen kommunikointijärjestelmä. Ääni-, kasvo- ja allekirjoitusmenetelmät valittiin koska ne ovat helppokäyttöisiä ja käyttäjän kannalta vaivattomia. Järjestelmän liikuteltavuus aiheuttaa sen, että järjestelmän tarkkuus heikkenee koska olosuhteet vaihtelevat. Voidaan joutua toimimaan metelin keskellä tai heikentyneissä valaistusolosuhteissa. Signaalin heikkeneminen voidaan korvata fuusioimalla kolme biometristä näytettä.

Tutkijat käyttivät Qtek2020 älypuhelinta ja Smartphonen omia sensoreita eli mikrofoonia, kameraa ja kosketusnäyttöä, joilla on rajoitetut tiedon keruu mahdollisuudet Tietokannan audiovisuaalinen data on englanninkielinen. Tietokanta koostuu 60:tä puhujasta, joista puolet miehiä ja puolet naisia. Näistä 80 prosenttia puhui englantia äidinkielenään. Heidät jaettiin kolmeen ikäryhmään: alle 30 -vuotiaat, 30 – 45 -vuotiaat ja yli 45 -vuotiaat. Kolmen tyyppisiä kehotteita (prompt) talletettiin: viisinumeroisia, kymmennumeroisia ja lyhyitä lauseita. Kaikista talletettiin kuusi näytettä. Jokaista käyttäjää talletettiin kahdella eri kerralla, joiden väli oli vähintään viikko. Jokainen talletus sisälsi kaksi sisä- ja ulkotalletusta. Talletukset tehtiin olosuhteiden suhteen erilaisissa olosuhteissa. Allekirjoitukset talletettiin aina hyvissä olosuhteissa. Kaksikymmentä allekirjoitusta talletettiin sekä miehiltä että naisilta. Henkilöt, jotka eivät kuuluneet tietokantaan, tekivät testiä varten kaksikymmentä allekirjoitusväärennöstä.

Tutkijoiden tulosten ja johtopäätösten mukaan yksibiometriset tunnisteet antavat huonommat tulokset kuin monibiometriset yhdisteet. Tämä johtuu muun muassa siitä syystä, että vaihtuvissa olosuhteissa fuusion osat voivat täydentää toisiaan. Fuusiometodeissa oli eroja, mutta huonoinkin fuusiometodi peittosi yksibiometristen tunnisteiden tulokset. Tämä tulee tutkijoiden mielestä lisäämään monibiometriikan käyttöä mobililaitteiden käyttäjien tunnistamisen yhteydessä. Tässä käytetyt menetelmätkin ovat käyttäjien kannalta vaivattomia.

5.4 Näytteen antajan elävyyden todentaminen

Chetty ym. (2005) tutkivat, uutta monibiometristä kasvojen ja äänen fuusiomenetelmää, henkilön biometriseksi tunnistamiseksi ja henkilön elävyyden varmentamiseksi. Elävyyden varmentaminen suojaa järjestelmää huijaus yrityksiltä varmistamalla, että biometrinen näyte on saatu elävältä henkilöltä. Tutkijoiden ehdottama menetelmä perustuu audiovisuaaliseen (bi-modal) näytefuusioon, cross-modal fuusioon sekä 3D muoto- ja rakennetekniikan fuusioon. Tämän avulla, tutkijat saavuttavat merkittäviä parannuksia järjestelmän turvallisuuteen, kehittämiään ykköstyypin (type-1) ja kakkostyypin (type-2) hyökkäyksiä vastaan. Ykköstyypin hyökkäyksissä tutkijat käyttivät väärennettyä pysäytyskuvaa ja ennalta nauhoitettua väärennettyä ääninäytettä. Kakkostyypin hyökkäyksessä käytettiin pysäytyskuvasta tehtyä liikkuvaa videota ja ennalta nauhoitettua ääninäytettä.

BMF (bi-modal) menetelmässä audiovisuaalisten ominaisvektorien fuusio paransi huomattavasti kasvo – ääni menetelmien kykyä varmistaa elävyys ja estää hyökkäykset. BMF malli heikensi myös datan herkkyyttä muutoksille. Tässä tutkittiin tosin vain ykköstyypin hyökkäys yrityksiä. CMF (cross-modal) mallissa, tutkijat tutkivat menetelmän toimivuutta ykkös- ja kakkostyypin hyökkäyksiä vastaa. He esittelivät kaksi uutta menetelmää: LSA (latent semantic analysis) ja CCA (canonical correlation analysis). Ykköstyypin hyökkäyksiä ne estivät peräti 80 prosenttia ja 60 prosenttia paremmin BMF:n verrattuna. Ne ovat tehokkaita myös kakkostyyppisten hyökkäysten estämisessä. CCA:lla noin 42 prosenttinen ja LSA:lla 61 prosenttinen parannus virheiden suhteen, verrattaessa PCA -kuva ja MFCC kasvo – ääni menetelmiin. 3MF (3D multi-modal) menetelmässä tutkittiin myös ykkös- ja kakkostyyppisten hyökkäysten estämistä. Tässä menetelmässä kolmeulotteiset kasvokuvat toimivat parhaiten hyökkäyksiä vastaan. Äänen, 3D muodon ja rakenteen monibiometrinen fuusio antoi 25 – 40 prosenttia paremman tuloksen kuin CMF. Ykköstyypin hyökkäysten EER (equal error rate) oli alle yksi ja huomattavasti vaikeampi kakkostyypin hyökkäysten EER oli alle seitsemän.

6. KEVYT BIOMETRIIKKA

Ensimmäisen biometrisen järjestelmän kehitti Alphonso M. Bertillon vuonna 1883. Se käytti antropologisia näytteitä, kuten pään ja korvan pituus ja leveys. Muita näytteitä, joita järjestelmä käytti, oli esimerkiksi keskisormen ja jalan pituus. Näitä käytettiin yhdessä sellaisten ominaisuuksien, kuten silmien väri, arvet ja tatuoinnit, henkilön identiteetin tunnistamiseen. Kaikkien yksittäisten biotunnistemenetelmien tulokset Bertllonin järjestelmässä voivat vaihdella, mutta yhdessä ne auttoivat henkilön identiteetin tunnistamisessa kohtuullisella tarkkuudella. (Nandakumar 2005: 63)

Nykyiset biometriset järjestelmät eivät ole täydellisiä. Niiden virheluku ei ole nolla. Ongelmia aiheuttaa muun muassa häiriöt datassa, ei-universaalisuus ja biometristen näytteiden epäselvyys. Nämä voivat johtaa ei hyväksyttäviin ongelmiin henkilön tunnistamisessa ja identiteetin varmentamisessa. Kasvo-, sormenjälki- ja iiristunnisteiden monibiometristen yhdistelmien käyttö voi vähentää näitä ongelmia. Useiden fuusiomenetelmien käyttö voi kuitenkin lisätä kirjautumis- ja tunnistamisaikaa. Tämä lisää käyttäjien vaivaa ja kasvattaa järjestelmän kustannuksia. Eräs ratkaisu, jolla järjestelmän virheiden määrää voidaan laskea aiheuttamatta lisää vaivaa käyttäjille, on kevyt (light, soft) biometriikka. Se perustuu keveiden tunnisteiden lisäämiseen biometriseen järjestelmään. Näitä ovat esimerkiksi käyttäjän sukupuoli, etnisyys, pituus, paino ja silmien väri. (Nandakumar 2005: 63)

Eräs uusimmista kevyen biometriikan menetelmistä on henkilön tunnistaminen kävelytyylistä. Asiaa on tutkittu VTT:llä. Tulokset ovat olleet lupaavia, väärä hyväksyminen tapahtui vain kahdessa prosentissa tapauksista ja väärä hylkääminen vajaassa viidessä prosentissa. Tunnistus perustuu kiihtyvyysanturilla mitattuun käyttäjän kävelytyyliin. VTT tutkii menetelmän soveltuvuutta kännyköihin. Idea on, että kännykkä tunnistaa olevansa oikean omistajan matkassa. Muussa tapauksessa se sulkee itsensä. (Nenonen 2007: 16)

Kevyen biometrisen järjestelmän käytettävyyttä voisi kuvata seuraavalla esimerkillä. Kuvitellaan kolme käyttäjää, jotka ovat A (mies, 180 cm), B (nainen, 170 cm) ja C

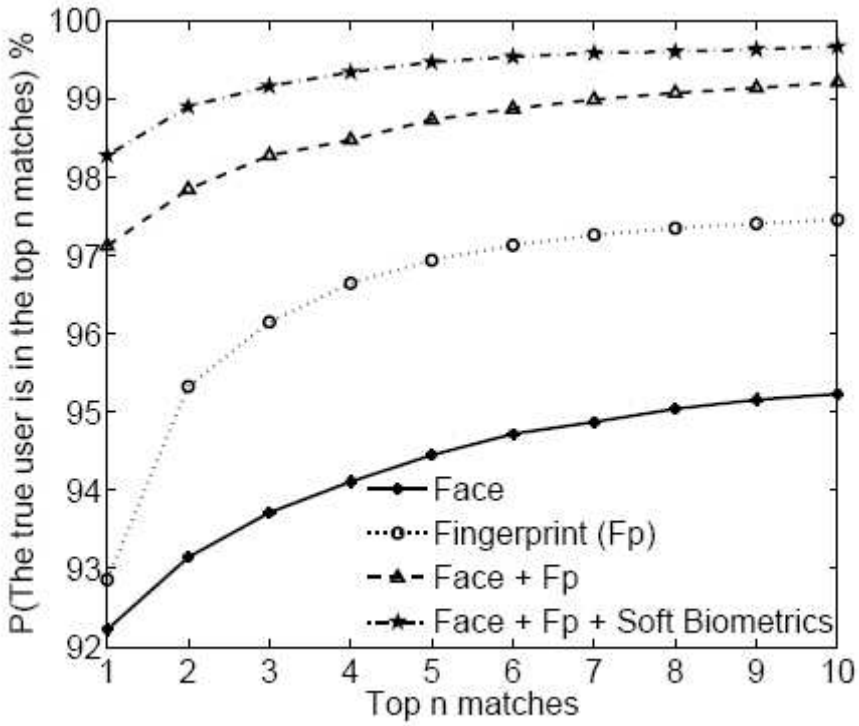
(mies, 160 cm). Tunnistejärjestelmänä on sormenjälkitunniste. Kun käyttäjä A esittää sormenjälkinäytteen X järjestelmälle, sitä verrataan kaikkien kolmen käyttäjän järjestelmään tallennettuihin näytteisiin. Oletetaan, että sormenjälkien vertailu antaisi tulokset P(A|X) = 0,42, P(B|X) = 0,43 ja P(C|X) = 0,15. Tässä tapauksessa käyttäjä A saatettaisiin tunnistaa virheellisesti käyttäjäksi B. Käyttäjä A saatettaisiin myös torjua virheellisesti järjestelmästä B:n kanssa liian samankaltaisen tuloksen johdosta. Toisaalta, jos järjestelmään kuuluisi myös toisarvoinen tunnistejärjestelmä, joka automaattisesti tunnistaisi käyttäjän sukupuolen ja pituuden sormenjäljen antamisen yhteydessä, järjestelmä erottaisi käyttäjän A helposti käyttäjästa B. (Nandakumar 2005: 63-64.)

6.1 Kasvo-, sormenjälki ja kevyen biometriikan yhdistäminen

Nandakumar (2005: 75-83) on tutkinut kevyiden biotunnisteiden yhdistämistä kasvo- ja sormenjälkitunnistamiseen ja henkilön identiteetin varmentamiseen. Kevyitä menetelmiä olivat sukupuolen, etnisyyden ja pituuden tunnistaminen. Tietokantana on ollut West Virginian yliopiston JMD (Joint multibiometric database). Valittu joukko koostui 263 henkilön neljästä kasvokuvasta ja neljästä vasemman käden etusormen sormenjälkikuvasta. Ne otettiin puolen vuoden aikana. Kasvojen vertailuun hän käytti IndentixFaceIt järjestelmää. Etnisyyden tutkimiseen X. Lu:n ja A. K. Jain:n *Ethnicity Identification from Face Images.* Se luokittelee henkilöt aasialaisiin tai ei-aasialaisiin 82.3 prosenttisella tarkkuudella. Sukupuolen määrittelyssä tutkija käytti samaa menetelmää kuin etnisyyden määrittelyssä ja menetelmien tuloksetkin olivat samat. Samalla kun henkilöiden kasvo- ja sormenjälkinäytteet kerättiin, arvioitiin myös henkilön pituus ja talletettiin se tietokantaan. Sukupuoli, etnisyys ja pituus painotettiin tässä tutkimuksessa niin, että ne saivat arvot 0,1, 0,1 ja 0,5 tunnistuksen yhteydessä ja 0,5, 0,5 ja 0,75 henkilön identiteetin varmentamisessa.

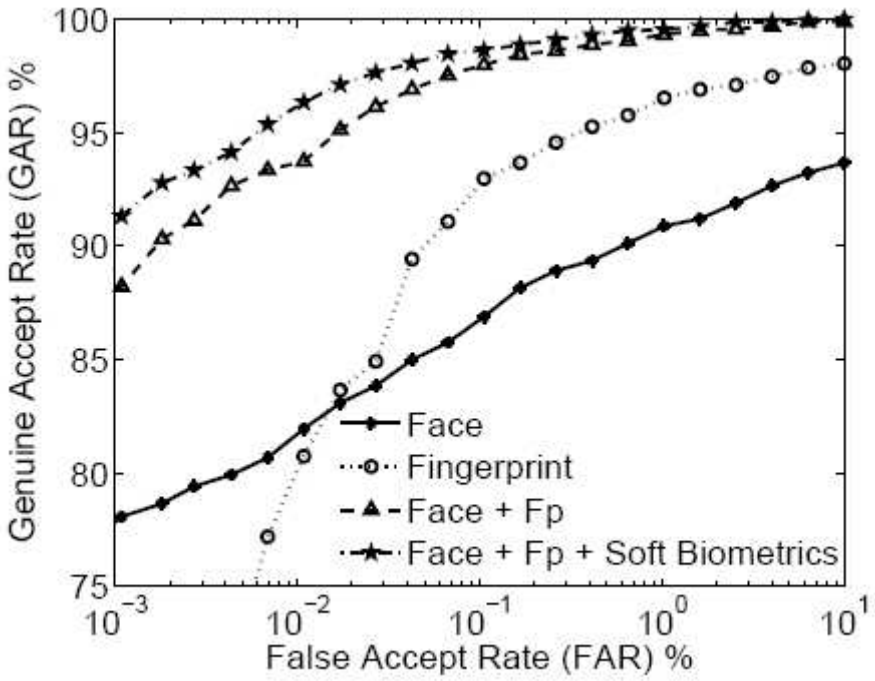
Tutkimuksen tuloksia on esimerkiksi se, että etnisyyden ja sukupuolen lisäys sormenjälkimenetelmään paransi henkilön tunnistamisessa tulosta 1,3 prosenttia. Pituuden lisäys paransi tulosta noin yhden prosentin. Kaikkien kolmen kevyen

menetelmän yhdistelmä paransi tulosta noin 2,5 prosenttia verrattuna pelkkään sormenjälkitunnisteeseen. Etnisyyden ja sukupuolen lisäys ei parantanut mainittavasti kasvotunnistemenetelmän tarkkuutta. Tutkija arvelee tämän johtuvan siitä, että FaceIt algoritmi ottaa itsessään huomioon joitakin etnisyyteen ja sukupuoleen liittyviä tietoja. Tätä tukee se, että 90 prosenttia väärin tunnistetuista kasvoista kuuluu samaan sukupuoleen, etnisyyteen tai molempiin. Pituuden lisäys kasvotunnisteeseen sitä vastoin parantaa järjestelmän tarkkuutta 0,5 – 1 prosenttia. Tämä osoittaa sen, että kevyt biometriikka parantaa tuloksia vain silloin kun se täydentää ensisijaista menetelmää. Kuvasta 14 nähdään, miten kevyen biometriikan lisäys parantaa sormenjälki- ja kasvotunnistamisen tuloksia. Kasvo- ja sormenjälkitunnisteisiin perustuva monibiometrinen järjestelmä on hyvin tarkka. Se tunnistaa henkilön 97 prosenttisella tarkkuudella. Lisäämällä kevyen biometriikan tiedot tarkkuus paranee tästäkin vielä prosentilla



Kuva 14. Tunnistetulosten paraneminen lisättäessä monibiometriseen järjestelmään kevyttä biometriaa. (Nandakumar 2005: 79)

Henkilön identiteetin todentamisessa sormenjälki ja kasvokuva ovat yksinään melko huonoja menetelmiä alhaisilla FAR arvoilla. Tutkija osoittaa tässä tutkimuksessa, että kevyen biometriikan lisääminen järjestelmään helpottaa tätä ongelmaa. FAR arvon ollessa 0,001 prosenttia, parannusta sormenjälkeen saavutetaan yli 20 prosenttia GAR arvossa. Kuvasta 15 nähdään, että henkilön identiteetin varmentamisessa kasvomenetelmällä ja monibiometrisella järjestelmällä, parannus GAR arvossa on noin kaksi prosenttia FAR arvon ollessa 0,001 prosenttia. Tämä on hyvä parannus kun otetaan huomioon, että ensisijaisen monibiometrisen järjestelmän GAR arvo oli jo ennestään korkea.



Kuva 15. Identiteetin varmentamisen tulosten paraneminen lisättäessä kevyen biometriikan menetelmiä monibiometriseen järjestelmään. (Nandakumar 2005: 82)

6.2 Hiiren käyttöön perustuva tunnistaminen

Gamboa, Fred & Jain (2007) ovat kehittäneet ja esitelleet menetelmän, jolla käyttäjän identiteetti voidaan varmistaa hänen hiirenkäyttönsä perusteella. Tutkijat esittelevät tässä kevyen biometriikkaan ja perinteiseen salasanaan perustuvaan kirjautumisen yhdistelmän. He antavat sille nimen WebBiometrics. Se tarkkailee käyttäjän hiiren liikkeitä kun hän klikkaa PIN–koodinsa. Asiakkaiden verkkokäyttäytymisen selvittäminen on yhä tärkeämpi osa useiden IT yritysten toimintaa. Sitä käytetään esimerkiksi markkinoinnissa. Esimerkiksi Googlen ja Yahoon tiedetään tarjoavan palveluita, jotka kohdistavat markkinointia käyttäytymisen perusteella.

Menetelmä perustuu virtuaaliseen näppäimistöön. Käyttäjän tulee hiirellä klikkaamalla syöttää sille käyttäjätunnus ja tunnusluku. Tunnusluku on satunnainen eli se vaihtuu joka kerta. Näin ollen sen jäljentäminen on mahdotonta, vaikka käyttäjän toiminta talletettaisiin. Tunnusluku pyydetään syöttämään kolme kertaa. Menetelmän kehittämisessä oli mukana viidenkymmenen vapaaehtoisen opiskelijan joukko. Opiskelijat testasivat järjestelmää pelaamalla muistipelejä. Tietokantaan tuli yhteensä viisi tuntia toimintaa ja 400 klikkausta käyttäjää kohden. Tutkimuksen tulosten mukaan, mitä pidempi PIN-koodi sitä parempi tulos. Kymmenen numeron PIN-koodi antoi EER arvoksi 12,5 prosenttia ja viidentoista numeron PIN–koodi vain 6,2 prosenttia. Tämän menetelmän ongelmana voidaan pitää ainakin sitä, että kaikki tietokoneen käyttäjät eivät voi käyttää hiirtä.

Tämä hiiren liikkeisiin perustuva tunnistemenetelmä on yksibiometrinen. Siihen voisi helposti yhdistää esimerkiksi sormenjäljen tunnistavan hiiren ja näin saataisiin monibiometrinen menetelmä. Tällainen menetelmä voisi sopia esimerkiksi yritykselle, jonka tietokoneilla on arkaluonteisia tietoja. Sormenjäljen tunnistava hiiri on saatavilla ainakin Siemensin valmistamana. Siemens on kehittänyt sormenjäljen koodaavan ja varastoivan algoritmin sekä ohjelmiston, joka mahdollistaa sormenjälkien keskitetyn hallinnan sekä käyttöoikeuksien tunnistamisen. Hiiri on helppokäyttöinen. Käyttäjä vain asettaa sormensa hiiressä olevaan sormenjälkitunnistimeen. Kirjautuminen kestää alle sekunnin. (Vehkasaari 2007: 7)

Toinen vaihtoehto voisi olla Fujitsun kämmenen tunnistava hiiri. Fujitsun PalmSecure hiiri esiteltiin ensi kertaa jo 2006, jolloin se oli tarkoitettu yritys- ja automaattikäyttöön, mutta nyt laitetta ollaan lähiaikoina tuomassa myös kuluttajamarkkinoille. PalmSecuren teknologia perustuu kämmenen verisuonikuvion kartoittamiseen infrapunasäteilyllä, ja kuvioon vertaamiseen tietokantaan tallennettuihin sallittuihin käyttäjiin. Toisin kuin sormenjälkeen perustuva biometriikka, suonten infrapunakartoitus toimii vain kun kämmenessä kiertää veri. (Verkossa.fi 2008)

6.3 Pituus, paino ja rasvaprosentti tunnistemenetelminä

Allisto, Lindholm, Mäkelä & Vildjiounaite (2004) ovat esitelleet tutkimustaan kevyestä biometriikasta ja sen käytöstä huomaamattomana ja helppona menetelmänä henkilön tunnistamisessa pienen riskin järjestelmässä. Heidän mukaan kevyt biometriikka soveltuu parhaiten järjestelmiin, joissa tarvitsee tunnistaa pieni joukko käyttäjiä. Näitä voi olla esimerkiksi kodit ja pienet toimistot. Tutkijat käyttävät tässä esimerkkinä kuntosalille sopivaa järjestelmää. Järjestelmän tarkoitus voi olla esimerkiksi kuntosalin jäsenten sisään pääsyn varmistaminen niin, etteivät he voisi lainata jäsenkorttia järjestelmään kuulumattomille kavereille. Ovella voisi tietenkin kysyä henkilöllisyystodistuksen tai käyttää sormenjälkitunnisteiden kaltaista vahvaa biometriikkaa. Nämä ovat kuitenkin asiakkaiden kannalta pulmallisia ja joissakin maissa jopa laittomia menetelmiä. Kevyttä biometriikkaa voisi käyttää tällaisessa tapauksessa varmistamaan, että kortin haltija on todellakin se, joka väittää olevansa. Hyöty voidaan saavuttaa käyttämällä henkilöiden fyysisiä ominaisuuksia kuten pituutta, painoa tai rasvaprosenttia varmistamaan, että henkilö on oikeutettu sisäänpääsyyn. Paino voitaisiin mitata lattiaan asetetulla anturilla ja pituus videokameran avulla. Nämä sijoitetaan tietenkin siten, ettei ulkopuoliset näe mittausten tuloksia. Tällaisilla menetelmillä väärästä tunnistamisesta aiheutuvat kustannukset olisivat minimaaliset.

Tutkijoilla oli käytössä tietokanta, johon oli kerätty tiedot 62:den henkilön pituudesta, painosta ja rasvaprosentista. Tämä määrä vastaa keskikokoista toimistoa tai kuntosalia. Henkilöt olivat aikuisia ja heistä 51 oli miehiä ja 11 naisia. Tiedot kerättiin kahdessa tilaisuudessa kahden viikon välein. Paino ja rasvaprosentti kerättiin molemmissa

tilaisuuksissa. Ensimmäisessä tilaisuudessa kysyttiin henkilön pituus ja toisessa se mitattiin lisäämällä siihen satunnaisesti luku väliltä –2,5 – 2,5. Viisi koehenkilöä testasi vielä menetelmää yksityiskohtaisesti, monta kertaa päivässä, ennen ja jälkeen ruokailun, sisä- ja ulkovaatteet päällä. Henkilöiden keskimääräinen painon vaihtelu päivän aikana oli 0,7 prosenttia. Pitkän aikavälin painon vaihtelun voisi kompensoida ottamalla mukaan esimerkiksi kymmenen viimeisen mittauksen keskiarvopainon. Tutkimuksen tuloksia on esitelty taulukossa 6.

Taulukko 6. Tutkimuksen tulokset. (Allisto ym. 2004: 3)

Metodi	TER	FRR	FAR
Paino	11,40 %	1,60 %	9,80 %
Pituus	15 %	0 %	15 %
Rasvapro.	35 %	7 %	28 %
0,5* pituus + 0,5*paino	8 %	5 %	3 %
Pituus JA Paino	2,40 %	0 %	2,40 %
Pituus TAI Paino	12,40 %	1,60 %	10,80 %
Paino JA Rasvapro.	8 %	3 %	5 %

Henkilön identiteetin varmentamisessa painon TER –arvo (total error rate) oli 11 prosenttia. Tämä on selvästi huonompi luku kuin tyypillinen sormenjälkitunnisteen tulos, mutta aika lähellä tyypillisiä kasvo- ja äänituniteiden tuloksia. Pituuden TER –luku oli 15 prosenttia ja rasvaprosentin TER –luku oli 35 prosenttia. Painon ja pituuden fuusio paransi TER –arvoa 2,4 prosenttia. Rasvaprosentti yksinään antoi huonon tuloksen, mutta fuusioimalla sen painon kanssa, putosi TER –arvo kahdeksaan prosenttiin. Päätöstason JA (AND) sääntö antoi parempia tuloksia kuin painotettu summa tai TAI (OR) sääntö. Koska henkilön pituus ja paino eivät ole täysin riippumattomia toisistaan, niiden fuusiolta ei voida odottaa yhtä hyviä tuloksia kuin vaikkapa sormenjäljen ja kasvojen fuusiolta. Tuloksissa on otettava huomioon se, että testiryhmä koostui vain 62:a henkilöstä.

Esimerkiksi kuntosalilla voisi olla käytössä lyhyt lista (short list), jossa olisi tunnistetulokset laskevassa järjestyksessä. Kevytbiometrisen mittauksen jälkeen esimerkiksi viiden sopivimman henkilön nimikirjaimet tai muu vastaava tunniste esitettäisiin. Käyttäjä voisi silloin valita listalta oman tunnuksensa. Painon ja pituuden

fuusio JA säännön avulla antaa tunnistuksen lyhyeltä listalta sataprosenttisesti. Painotetulla summasäännöllä tulos oli 97 prosenttia.

Tulosten mukaan kevyen biometriikan käyttö, henkilön identiteetin varmentamisessa yhdessä vaikkapa jäsenkortin kanssa, voi olla käyttökelpoinen kuntosalin tai pienen toimiston yhteydessä. Painoon perustuvassa tunnistamisessa järjestelmään kuulumattoman henkilön sisään pääsyn todennäköisyys jonkun toisen identiteetillä oli 9,8 prosenttia. Toisin sanoen yhdeksän kymmenestä huijarista jäisi kiinni. Käyttäjien kannalta tunnistamiseen liittyvien epämiellyttävien tilanteiden, kuten virheellisen sisäänpääsyn eston, riski olisi nolla prosenttia. Jos käytettäisiin yhdistettyä painon ja pituuden tunnistemenetelmää huijarin sisäänpääsyn mahdollisuus olisi vain 2,4 prosenttia. (Allisto ym. 2004)

7. JOHTOPÄÄTÖKSET

Biometristen tunnistejärjestelmien suosion kasvu tulee varmasti jatkumaan voimakkaana. Alalle kehitetään yhä edullisempia ja helppokäyttöisimpiä menetelmiä. Tämä on aiheuttanut varmasti aiheellistakin huolta monella taholla. Monibiometriset yhdistelmät ovat toistaiseksi olleet vain pieni tekijä alalla. Ne pystyvät kuitenkin ratkaisemaan monia yksibiometrisiin menetelmiin liittyviä ongelmia. Tämän johdosta, niiden suosio tuleekin varmasti kasvamaan tulevaisuudessa.

Olettamus siitä, että monibiometriset yhdistelmät lisäävät järjestelmän tarkkuutta, osoittautui oikeaksi. Kaikki tässä työssä läpikäydyt tutkimukset tukivat tätä väitettä. Esimerkiksi kasvo- ja sormenjälkitunnisteiden yhdistelmä voi jopa puolittaa järjestelmän FAR ja FRR virheet. Sormenjälkeen ja käden geometriaan perustuva yhdistelmä on selvästi tarkempi kuin kyseiset menetelmät yksinään. Sormenjäljen ja iiriksen fuusio parantaa järjestelmän todellista hyväksyntä eli GAR- arvoa huomattavasti verrattuna molempien yksittäisiin tuloksiin. Useiden sormien yhdistelmä parantaa järjestelmän tarkkuutta. Samoin nähdään se, että mitä sormia käytetään, on vähintään yhtä tärkeää kuin se, montako sormea yhdistelmässä käytetään. Kun lisätään kasvokuva yhteen tai kahteen sormenjälkeen, laskee FRR melkein suurusluokan verran. Sormenjälkien yhdistelmät ovat hyvin tehokkaita. Samoin sormenjälkien ja kasvojen yhdistelmät. Kun yhdistetään kaksi sormenjälkeä tai yksi sormenjälki ja kasvokuva FRR-arvot laskevat 50 – 90 prosenttia

Esittelemieni tutkimusten mukaan monibiometriset järjestelmät helpottavat kerätyn tiedon häiriönä tunnettua ongelmaa. Tällaisia on esimerkiksi likainen sormenjälki tai käheä ääni. Useiden sormenjälkien yhdistelmissä ei yhden sormen huonolla kuvalla ole ratkaisevaa merkitystä, kuten olisi yksibiometrisessa tunnistamisessa. Ulkoisissa häiriöissä on kyse siitä, että järjestelmässä on useita samankaltaisia näytteitä. Tätä ongelmaa voi ehkäistä valitsemalla monibiometriseen järjestelmään toisistaan riippumattomia tunnistemenetelmiä. Ei universaalinen ongelma tarkoittaa sitä, että osalta henkilöistä ei saada biometrista näytettä. Tutkimusten perusteella myös näihin ongelmiin saadaan monibiometrisillä yhdisteillä helpotusta. Tutkimusten perusteella

voidaan olettaa, että monibiometriset yhdistelmät pienentävät tiedon häiriöiden, ulkoisten häiriöiden ja ei universaalisuuden aiheuttamia ongelmia. Tämä vaatii tulosten normalisoinnin ja sopivien painotusten löytämisen. Tilanteita, joissa käyttäjä toimii väärin, kutsutaan sisäisiksi häiriöiksi. Näihin ei tutkimuksista löytynyt niin selkeitä helpotuksia kuin edellisiin. Toisaalta mikään ei kumonnutkaan olettamusta, että monibiometriset järjestelmät helpottaisivat näitä ongelmia.

Olettamus siitä, että monibiometriset yhdisteet vaikeuttaisivat järjestelmän huijausta, osoittautui tutkimusten perusteella oikeaksi. Esimerkiksi kappaleessa 5.4 esittelemäni audiovisuaaliseen (bi-modal) näytefuusioon, cross-modal fuusioon sekä 3D muoto- ja rakennetekniikan fuusioon perustuvan järjestelmän avulla, tutkijat saavuttavat merkittäviä parannuksia järjestelmän turvallisuuteen ykköstyypin ja kakkostyypin hyökkäyksiä vastaan. Kolmeulotteiset kasvokuvat toimivat parhaiten hyökkäyksiä vastaan. Äänen, 3D muodon ja rakenteen monibiometrinen fuusio antoi 25 – 40 prosenttia paremman tuloksen kuin CMF. Ykköstyypin hyökkäysten EER oli alle yksi ja huomattavasti vaikeampi kakkostyypin hyökkäysten EER oli alle seitsemän.

Moniobiometristen järjestelmien ongelmina pidettiin sitä, että ne lisäävät kustannuksia ja käyttäjien kirjautumisaikaa. Näitä ongelmia voitiin kuitenkin pienentää joillakin tutkimuksissa esitellyillä menetelmillä. Esimerkiksi kappaleessa 4.2 esittelin kämmenen jälkeen ja kämmenen geometriaan perustuvan järjestelmän. Tässä järjestelmässä käytettiin vain yhtä kameraa eli sensoria. Tämän voidaan olettaa säästävän kirjautumisaikaa ja järjestelmän vaatimia kustannuksia. Kappaleessa 4.4 esittelin koko käden samanaikaiseen monibiometriseen tunnistamiseen perustuvan järjestelmän. Sen etuja useimpiin järjestelmiin verrattuna on se, että se vaatii käyttäjältä vain yhden näytteenannon. Sillä saadaan samalla kertaa monibiometrinen data, joka koostuu sormenjäljestä, kämmenestä ja käden geometriasta. Tässä järjestelmässä siis yksi sensori voi kerätä useita erilaisia biometrisia näytteitä. Tämä vähentää järjestelmän käyttämää kokonaisaikaa ja tekee siitä yksinkertaisemman verrattuna useiden sensoreiden järjestelmiin. Yksi pieni haitta on se, että järjestelmä vaatii hieman enemmän laskentakapasiteettia. Se on kuitenkin varsin merkityksetön haitta, varsinkin kun tiedetään, että uutta tekniikkaa ja tehokkaampia mikroprosessoreja kehitetään.

Edellä esiteltyihin, biometriseen tunnistamiseen liittyviin ongelmiin, on esitetty ratkaisuksi kevyttä biometriikkaa. Esittelemieni tutkimusten perusteella, se sopiikin hyvin täydentämään monibiometrisiä tunnistejärjestelmiä. Kappaleessa 6.1 esittelemässäni järjestelmässä, etnisyyden ja sukupuolen lisäys sormenjälkimenetelmään, paransi henkilön tunnistamisessa tulosta 1,3 prosenttia. Pituuden lisäys paransi tulosta noin yhden prosentin. Kaikkien kolmen kevyen menetelmän yhdistelmä paransi tulosta noin 2,5 prosenttia verrattuna pelkkään sormenjälkitunnisteeseen. Etnisyyden ja sukupuolen lisäys ei parantanut mainittavasti kasvotunnistemenetelmän tarkkuutta. Kasvo- ja sormenjälkitunnisteisiin perustuva monibiometrinen järjestelmä on hyvin tarkka. Se tunnistaa henkilön 97 prosenttisella tarkkuudella. Lisäämällä kevyen biometriikan tiedot, tarkkuus paranee tästäkin vielä prosentilla

Pienen riskin järjestelmissä kevyen biometriikan yhdistelmät voivat toimia sellaisenaankin. Esimerkiksi kappaleessa 6.3 esiteltiin painoon, pituuteen ja rasvaprosenttiin perustuva järjestelmä. Henkilön identiteetin varmentamisessa painon TER – arvo oli 11 prosenttia. Tämä on selvästi huonompi luku kuin tyypillinen sormenjälkitunnisteen tulos, mutta aika lähellä tyypillisiä kasvo- ja äänituniteiden tuloksia. Pituuden TER – luku oli 15 prosenttia ja rasvaprosentin TER – luku oli 35 prosenttia. Painon ja pituuden fuusio paransi TER – arvoa 2,4 prosenttia. Rasvaprosentti yksinään antoi huonon tuloksen, mutta fuusioimalla sen painon kanssa, putosi TER – arvo kahdeksaan prosenttiin. Päätöstason JA (AND) sääntö antoi parempia tuloksia kuin painotettu summa tai TAI (OR) sääntö. Koska henkilön pituus ja paino eivät ole täysin riippumattomia toisistaan, niiden fuusiolta ei voida odottaa yhtä hyviä tuloksia kuin vaikkapa sormenjäljen ja kasvojen fuusiolta.

Johdannossa kerroin uusista biometrisista passeista, joihin tulee sormenjälki- ja kasvotunnistemenetelmät. Näiden yhdistelmä antaa tarkan tuloksen. Kappaleessa 3.1 esitellyn tutkimuksen johtopäätös normalisointi- ja fuusiometodeista kasvo- ja sormenjälkikuville on se, että avoimissa populaatioissa, joissa henkilöiden tarkat ominaisuudet ei ole tiedossa, kannattaisi käyttää MM normalisointia ja SS fuusiota.

Tämä sopisi siis parhaiten juuri lentokentän kaltaiseen paikkaan. Määrätyissä suljetuissa populaatioissa, kuten jonkin toimiston henkilökunnalle, kannattaisi käyttää QLQ ja UW fuusiometodeita.

Johdannossa kerroin kuntosalista, joka kerää käyttäjiltään sormenjäljet. Tietosuojavaltuutettu paheksui tätä. Kevyen biometriikan käyttö, henkilön identiteetin varmentamisessa yhdessä vaikkapa jäsenkortin kanssa, voisi olla käyttökelpoinen kuntosalin tai pienen toimiston yhteydessä. Painoon perustuvassa tunnistamisessa järjestelmään kuulumattoman henkilön sisään pääsyn todennäköisyys jonkun toisen identiteetillä oli 9,8 prosenttia. Toisin sanoen, yhdeksän kymmenestä huijarista jäisi kiinni. Käyttäjien kannalta tunnistamiseen liittyvien epämiellyttävien tilanteiden, kuten virheellisen sisäänpääsyn eston, riski olisi nolla prosenttia. Jos käytettäisiin yhdistettyä painon ja pituuden tunnistemenetelmää, huijarin sisäänpääsyn mahdollisuus olisi vain 2,4 prosenttia.

Jatkossa eräs kasvava soveltuvuus alue biometriikalle tulee olemaan mobiililaitteet eli kännykät ja kannettavat tietokoneet. Tällaisen mobiilin monibiometrisen järjestelmän esittelin kappaleessa 5.3. Siinä valittiin ääni-, kasvo- ja allekirjoitusmenetelmät koska ne ovat helppokäyttöisiä ja käyttäjän kannalta vaivattomia. Järjestelmän liikuteltavuus aiheuttaa sen, että järjestelmän tarkkuus heikkenee, koska olosuhteet vaihtelevat. Voidaan joutua toimimaan metelin keskellä tai heikentyneissä valaistusolosuhteissa. Signaalin heikkeneminen voidaan korvata fuusioimalla biometrisiä näytteitä. Tulosten mukaan yksibiometriset tunnisteet antavat huonommat tulokset kuin monibiometriset yhdisteet. Tämä johtuu muun muassa siitä syystä, että vaihtuvissa olosuhteissa fuusion osat voivat täydentää toisiaan. Fuusiometodeissa oli eroja, mutta huonoinkin fuusiometodi peittosi yksibiometristen tunnisteiden tulokset. Tämä tulee tutkijoiden mielestä lisäämään monibiometriikan käyttöä mobililaitteiden käyttäjien tunnistamisen yhteydessä. Tässä käytetyt menetelmätkin ovat käyttäjien kannalta vaivattomia.

8. YHTEENVETO

Tässä työssä on tarkoituksena ollut tutustuttaa lukija monibiometristen tunnistejärjestelmien perusteisiin sekä alan uusimpiin tutkimustuloksiin. Selvittää niiden avulla monibiometristen tunnistejärjestelmien hyviä ja huonoja puolia sekä joitakin mahdollisia käytännön vaihtoehtoja. Työhön pyrin valitsemaan mahdollisimman tuoreita tutkimuksia. Useimmat onkin julkaistu vuosien 2004 – 2007 välillä, ulkomaisten yliopistojen tutkijoiden toimesta.

Kappaleessa kaksi esiteltiin ensin biometriseen tunnistamiseen liittyviä olettamuksia. Lähinnä siihen, mitä ongelmia yksibiometrisillä tunnistejärjestelmillä voi olla ja voisiko monibiometriset järjestelmät olla ratkaisu näihin ongelmiin. Kappaleessa myös esiteltiin monibiometrisen järjestelmän toimintaa. Käytiin läpi eri tekniikoita, menetelmiä ja järjestelmien arkkitehtuuria. Lopuksi perehdyttiin siihen, miten biometristen järjestelmien toimivuutta ja tarkkuutta voidaan mitata. Virheettömyyden osalta tarkemmin tutustuttiin väärän hylkäyksen ja väärän hyväksynnän aiheuttaviin virheisiin.

Kappaleessa kolme esittelen tutkimuksia, joissa on tutkittu henkilön tunnistamista useiden erilaisten biometristen menetelmien yhdisteinä. Yksi henkilö on siis antanut useita biometrisiä näytteitä eri sensoreille, jotka on sitten fuusioitu jollakin menetelmällä yhdeksi biometriseksi malliksi. Mielenkiintoisin on ehkä ensimmäisenä esiteltävä kasvo- ja sormenjälkikuvaan keskittyvä tutkimus. Nämä tunnisteethan tulevat myös uusiin biometrisiin passeihin, jotka meilläkin otetaan käyttöön. Kasvo- ja sormenjälkiyhdisteiden todettiin olevan varsin tehokkaita tunnistemenetelmiä. Tutkimuksen tulosten perusteella myös annettiin suosituksia siitä, millä tekniikalla lentokentän kaltaisessa paikassa tunnistaminen kannattaisi suorittaa. Toisessa tutkimuksessa yhdistettiin sormenjälki, kasvo ja käden geometria. Kolmannessa kuvattiin kasvokuvan ja iiriksen yhdistelmä ja neljännessä kasvojen ja useiden sormenjälkien yhdistelmä..

Kappaleessa neljä esiteltiin tutkimuksia, joissa on tutkittu henkilön tunnistamista ja henkilön identiteetin varmentamista, yhdestä biometrisesta kohteesta johdettujen erilaisten yhdisteiden avulla. Henkilöstä on siis otettu, esimerkiksi kasvokuva kahdella erilaisella kameralla, ja nämä näytteet on sitten fuusioitu yhdeksi biometriseksi tunnisteeksi. On myös tutkittu, voidaanko yhdestä kuvasta vetää kaksi erilaista biometrista mallinetta ja fuusioida ne yhdeksi biometriseksi tunnisteeksi. Tutkimuksina on kasvotunnistaminen kaksi- ja kolmiulotteisesti. Käden geometria ja kämmenen jälki sekä infrapunavalo ja näkyvävalo kasvotunnistamisessa Lopuksi esiteltiin monibiometriikan uusimman menetelmän prototyyppi. Siinä on kehitetty sensori, joka kuvaa kaikki tunnetut käden biometriset tunnisteet yhtäaikaisesti. Tässä järjestelmässä, siis yksi sensori voi kerätä useita erilaisia biometrisia näytteitä. Tämän todettiin vähentävän järjestelmän käyttämää kokonaisaikaa ja tekevän siitä yksinkertaisemman verrattuna useiden sensoreiden järjestelmiin.

Kappaleessa viisi esiteltiin audiovisuaalisista monibiometrisista menetelmistä tehtyjä tutkimuksia. Ensimmäisen tutkimuksen kohteena oli videokuvaan perustuva tunnistaminen. Toisessa tutkittiin äänen ja sormenjäljen yhdistämistä. Kolmas ja ehkä mielenkiintoisin tutkimus koski mobiililaitteille suunniteltua ääni-, kasvo- ja käsialatunnistamista. Laitteen liikuteltavuuden todettiin heikentävän järjestelmän tarkkuutta heikentämällä signaalia. Signaalin heikkeneminen voitiin korvata fuusioimalla biometrisiä näytteitä. Tulosten mukaan yksibiometriset tunnisteet antoivat huonommat tulokset kuin monibiometriset yhdisteet. Tämän arveltiin johtuvan muun muassa siitä syystä, että vaihtuvissa olosuhteissa fuusion osat voivat täydentää toisiaan. Fuusiometodeissa todettiin olevan eroja, mutta huonoinkin fuusiometodi peittosi yksibiometristen tunnisteiden tulokset. Viimeisessä tutkimuksessa selvitettiin näytteen elävyyden vaikutusta huijausten torjunnassa. Elävyyden varmistavien ominaisuuksien avulla tutkijat saavuttivat merkittäviä parannuksia järjestelmän turvallisuuteen ykköstyypin ja kakkostyypin hyökkäyksiä vastaan

Kappaleessa kuusi esiteltiin ensin kevyttä biometriikkaa yleisellä tasolla. Kerrottiin, mitä menetelmiä voitaisiin käyttää kevyinä tunnistemenetelminä ja kerrottiin esimerkki kevyen biometriikan teoreettisesta käyttötilanteesta. Tutkimuksina esiteltiin ensin

sormenjäljen ja kolmen erilaisen kevyen biometrisen tunnisteen yhdistelmän. Kevyinä tunnistemenetelminä oli käytetty henkilön pituutta, sukupuolta ja etnisyyttä. Tällaisen järjestelmän todettiin sopivan hyvin täydentämään vahvaa biometrista tunnistamista. Lopuksi esittelin kevyeen biometriaan perustuvan, monibiometrisen tunnistemenetelmän, joka olisi erinomainen vaihtoehto kuntosalin tai pienen toimiston ovella tapahtuvaan henkilöiden tunnistamiseen. Tämä järjestelmä käytti kevyinä biotunnisteina henkilön pituutta, painoa ja rasvaprosenttia. Järjestelmän todettiin olevan käyttäjien kannalta huomaamaton ja pienen riskin tilanteissa myös ylläpitäjälle parempi vaihtoehto kuin esimerkiksi pelkkään sormenjälkitunnisteeseen perustuva järjestelmä.

LÄHDELUETTELO

Allano, Lorene, Andrew C. Morris, Harin Sellahewa, Sonia Garcia-Salicetti, Jacques Koreman, Sabah Jassim Bao Ly-Van, Dalei Wu & Bernadette Dorizzi (2006). *Non intrusive multi-biometrics on a mobile device: a comparison of fusion techniques.* Lainattu 19.1.2008.

Allisto, Heikki, Mikko Lindholm, Satu-Marja Mäkelä & Elena Vildjiounaite (2004). *Unobtrustive user identification with light biometrics.* Lainattu 4.2.2008:

BioID (2004). Lainattu 10.12.2007: http://www.bioid.com/sdk/docs/About_EER.htm

Biometrics FAQ (2007). Lainattu 22.11.2007: http://www.bromba.com/faq/biofaqe.htm

Chen, Xin, Patrick J. Flynn & Kevin W. Bowyer (2005). *IR and visible light face recognition.* Lainattu 25.1.2008: http://www.cse.nd.edu/~kwb/ChenFlynnBowyerCVIU_2005.pdf

Chetty, Girija & Michael Wagner (2005). *Audio-Visual Multimodal Fusion for Biometric Person Authentication and Liveness Verification.* Lainattu 27.1.2008: http://crpit.com/confpapers/CRPITV57Chetty.pdf

Dessimoz, Damien, Jonas Richiardi, Christophe Champod & Andrzej Drygajlo (2006). *Multimodal biometrics for identity documents. Lainattu 14.10.2007:* http://www.europeanbiometrics.info/images/resources/90_264_file.pdf

EY asetus N:o 2252/2004 (2004). *Jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevista vaatimuksista.* Annettu 13.12.2004: http://europa.eu.int/eur-lex/lex/LexUriServ/site/fi/oj/2004/l_385/l_38520041229fi00010006.pdf

Fierrez-Aquilar, Julian, Javier Ortega-Garcia, Joaquin Gonzales-Rodriquez & Josef Bigun (2004). *Kernel-based multimodal biometric verification using quality signals.* Lainattu1.2.2008: http://atvs.ii.uam.es/files/2004_BTHI_KernelFusionQuality_Fierrez.pdf

Gamboa, Hugo, A.L.N. Fred & Anil K. Jain (2007). *Webbiometrics: User verification via web interaction.* Lainattu 10.2.2008: http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/HugoFredJainWebBiometricsBYSM2007.pdf

Godil, Afzal, Sandy Ressler & Patrick Grother (2004). *Face recognition using 3D facial shape and color map information: comparision and combination.* Lainattu 23.1.2008: http://zing.ncsl.nist.gov/godil/3dfacepaper.pdf

Howells, Lee (2005). *Fusion comes in from the cold*. Lainattu 14.10.2007: http://www.europeanbiometrics.info/images/resources/77_922_file.pdf

International Biometric Group (2007). *Biometrics Market and Industry Report 2007-2012.* Lainattu 11.11.2007: http://www.biometricgroup.com/reports/public/market_report.html

Kumar, Ajay, David C. M. Wong, Helen C. Shen & Anil K. Jain (2003). *Personal verification using palmprint and hand geometry biometric.* Lainattu 24.1.2008: http://biometrics.cse.msu.edu/Publications/Multibiometrics/Kumaretal_PalmprintHandFusion_AVBPA2003.pdf

Nandakumar, Karthik, Yi Chen, Anil K. Jain & Sarat C. Dass (2006). *Quality based score level fusion in multibiometric systems.* Lainattu 10.1.2008: http://biometrics.cse.msu.edu/Publications/Multibiometrics/Nandakumaretal_QualityFusion_ICPR2006.pdf

Nandakumar, Karthik (2005). *Integration of multible cues in biometric systems*. Lainattu 3.2.2008: http://biometrics.cse.msu.edu/Publications/Thesis/KarthikNandakumar_BiometricFusion_MS05.pdf

Nenonen, Heikki (2007). Sisäänpääsy kämmenen varassa. *KauppalehtiVip* 7.5.2007

NSTC Subcommittee on biometrics (2006). *Biometrics testing and statistics*. Lainattu 15.12.2007: http://www.biometrics.gov/Documents/BioTestingAndStats.pdf

Ouyang, Hua & Tan Lee (2006). *A new lip feature representation method for video-based bimodal authenticatio.* Lainattu 29.1.2008

Pimperi, Jarno Johannes (2005). *Johdatus biometriikan perusteisiin, käytettävyyteen, hyväksyttävyyteen ja tietoturvaan.* Pro gradu –tutkielma. Vaasan yliopisto.

Ross, Arun & Anil K. Jain (2004). *Multimodal biometrics: an overview*. Lainattu 12.10.2007:http://biometrics.cse.msu.edu/Publications/Multibiometrics/RossJain_MultimodalOverview_EUSIPCO04.pdf

Ross, Arun & Anil Jain (2003). *Information fusion in biometrics.* Lainattu 12.1.2008

Rowe, Robert K., Umut Uludag, Meltem Demirikus, Sujan Parthasaradhi & Anil K. Jain (2007). *A multispectral whole-hand biometric authentication system.* Lainattu 10.2.2008: http://biometrics.cse.msu.edu/Publications/Multibiometrics/RoweEtalMultispectralHandBSYM2007.pdf

Schuckers, Stephanie, Larry Hornak, Tim Norman, Reza Derakhshani & Sujan Parthasaradhi (2002). *Issues for liveness detection in biometrics.* Lainattu 2.2.2008: http://www.biometrics.org/html/bc2002_sept_program/2_bc0130_DerakhshabiBrief.pdf

Sipilä, Annamari (2008). EU:n komissio haluaa kerätä sormenjäljet ulkomaisilta matkailijoilta. *Helsingin Sanomat* 14.2.2008.

Sisäasiainministeriö (2008). *Biometriahanke*. Lainttu 10.1.2008: http://www.intermin.fi/intermin/hankkeet/biometria/home.nsf/pages/indexfin

Snelick, Robert, Umut Uludag, Alan Mink, Michael Indovina & Anil Jain (2005). *Large scale evaluation of multimodal biometric authentication using state of the art systems.* Lainattu 10.1.2008: http://w3.antd.nist.gov/pubs/TPAMI-0373-1103-Final_Reprint.doc

Ulery, Brad, Austin Hicklin, Peter Hallinan, Craig Watson & William Fellner (2006). *Effectiveness of Score-Level Fusion.* Lainattu 23.1.2008: http://www.itl.nist.gov/iad/894.03/pact/ir_7346_B.pdf

Vehkasaari, Mika (2007). *Ei enää salasanoja PC:lle, hiiri tunnistaa sormenjäljen.* Siemens Osakeyhtiön asiakaslehti 1/2007. Lainattu 10.2.2008: http://www.siemens.fi/CMSADfiles.nsf/all/FEB7777B5765148EC22572C10040641D/$file/Partneri0107-netti_2.pdf

Verkossa.fi (2008). *Fujitsun hiiri tunnistaa käyttäjän kämmenestä.* Julkaistu 8.1.2008. Lainattu 10.2.2008: http://www.verkossa.tv/wordpress/?p=1563

Åström-Kupsanen, Maarit (2007). Sormenjälkitunnistaminen yleistyy –miten käy tietoturvan? *TV1 Kuningaskuluttaja* 30.1.2007. Lainattu 10.1.2008: http://kuningaskuluttaja.yle.fi/node/1701