TEKNIIKKA JA LIIKENNE

Sähkötekniikka

Elektroniikka

INSINÖÖRITYÖ

BIOMETRISET TUNNISTUSJÄRJESTELMÄT

Työn tekijä: Pauli Paakkunainen
Työn ohjaajat: Esa Häkkinen

Työ hyväksytty: ___. ___. 2009

Esa Häkkinen
yliopettaja

Metropolia

ALKULAUSE

Tämä insinöörityö tehtiin biometrian alaan kohdistuvan henkilökohtaisen ja yleisen kiinnostuksen vuoksi. Haluan kiittää kaikkia niitä henkilöitä, jotka ovat tukeneet ja kannustaneet minua viime vuosien ajan. Kiitos isä, äiti, veljet ja kaikki minulle rakkaat ystävät. Haluan myös kiittää Esa Häkkistä ja Aira Korkeamäkeä heidän antamistaan neuvoista ja avusta tämän työn laatimisessa.

Helsingissä 9.2.2009

Pauli Paakkunainen

TIIVISTELMÄ

Työn tekijä: Pauli Paakkunainen

Työn nimi: Biometriset tunnistusjärjestelmät

Päivämäärä: 9.2.2008 **Sivumäärä:** 90

Koulutusohjelma: Sähkötekniikka

Suuntautumisvaihtoehto: Elektroniikka

Työn ohjaaja: yliopettaja Esa Häkkinen

Tässä insinöörityössä selvitettiin biometristä tunnistusta seuraavien piirteiden avulla: sormenjälki, kämmen, kasvot, puhe, iiris, retina, käsialadynamiikka ja näppäimistö–dynamiikka. Työssä myös esiteltiin biometrisen järjestelmän toimintaperiaate sekä 12 potententiaalista tulevaisuuden biometristä tunnistusmenetelmää.

Työssä havaittiin että standardien puute ja aitouden varmennus on ongelma biometriikan alalla. Biometristen tunnistejärjestelmien valmistajat käyttävät järjestelmissään omia standardejaan, ja näin mallinteiden vaihdettavuus eri valmistajien järjestelmien välillä on lähes mahdotonta. Aitouden varmennuksen puutteen vuoksi useat tunnistusjärjestelmät ovat alttiina mahdollisille huijauksille.

Kirjallisuustutkimuksen perusteella suositellaan, että identifiointia, verifiointia, kulun–valvontaa ja muita biometrisiä tunnistusjärjestelmäsovelluksia suunniteltaessa ja niitä käyttöön otettaessa tulee huomioida aitouden varmennus, tieto- ja yksityisyydensuoja. Monibiometriset tunnistusjärjestelmät mahdollistavat aitouden varmennuksen käytön sellaisien menetelmien kohdalla, jotka eivät sitä sisällä itsessään.

Avainsanat:
biometria, biometrinen tunnistaminen, henkilöllisyyden varmennus, henkilön tunnistus, sormenjälkitunnistus, kämmentunnistus, kasvotunnistus, puhujatunnistus, iiristunnistus, retinatunnistus, käsialadynamiikkatunnistus, näppäimistödynamiikkatunnistus, verisuoni–kuviotunnistus, kasvojen termografian tunnistus, DNA-profilointi, hikihuokosanalyysi, kädenpuristustunnistus, kynnenaluskuviotunnistus, ominaishajutunnistus, korvan muodon tunnistus, kävelytyylitunnistus, ihon luminesenssin tunnistus, jalanjälkitunnistus, askeldynamiikkatunnistus, aivokäyrätunnistus

Metropolia

ABSTRACT

Name: Pauli Paakkunainen

Title: Biometric Recognition Systems

Date: 9.2.2009 **Number of pages:** 90

Department: Electrical Engineering

Study Programme: Electronics

Instructor and Supervisor: Esa Häkkinen, Tech. Lic., Principal Lecturer

The main purpose of this graduate study was to examine biometric recognition techniques. The aim was also to give a description of the basic operating principle of the biometric recognition system and of 12 potential future biometric recognition techniques. The study was carried out as literature research.

This study of biometric recognition techniques focused primarily on fingerprint, hand, face, voice, iris, retina, signature and keystroke dynamics.

It was found out that, in the field of biometrics, the lack of standards and liveness test capability constitute a problem. The biometric recognition system manufacturers use their own standards and, therefore, the interchangeability of biometric templates between two manufacturers is nearly impossible. Due to the lack of liveness test capability, many biometric recognition systems are vulnerable to possible abuse.

On the basis of the literature research, when designing identification, verification, access control or other biometric recognition system applications, the focus should be especially on the liveness test capability and on data and privacy protection. Multibiometric recognition systems make it possible to add the liveness test capability to the biometric techniques that do not have it naturally.

Keywords:
biometrics, biometric recognition, verification, identification, fingerprint recognition, hand geometry, facial recognition, voice recognition, iris recognition, retina recognition, signature recognition, keystroke dynamics, vein pattern recognition, facial thermography, DNA profiling, sweat pore analysis, hand grip, fingernail bed, body odor, ear shape, gait, skin luminescense, footprint, foot dynamics, brainwave pattern

SISÄLLYS

TÄRKEIMMÄT LYHENTEET

AFIS	*Automatic Fingerprint Identification System*	automaattinen sormenjälkien tunnistusjärjestelmä
CCTV	*Closed-Circuit TV*	suljetun piirin TV
DTW	*Dynamic Time Warp*	dynaaminen aikasovitus
EER	*Equal Error Rate*	keskimääräinen virhealttius
FAR	*False Accept Rate*	väärien hyväksyntöjen määrä
FMR	*False Match Rate*	väärien hyväksyntöjen määrä
FNMR	*False Non Match Rate*	väärien hylkäysten määrä
FRR	*False Rejection Rate*	väärien hylkäysten määrä
FTAR	*Failure to Acquire Rate*	epäonnistuneiden taltiointien määrä
FTER	*Failure to Enroll Rate*	epäonnistuneiden kirjautumisten määrä
IR	*Infra Red*	infrapuna
PCA	*PCA-algorithm*	PCA-algoritmi
VQ	*Vector Quantification*	vektorikvantisointi

1 JOHDANTO

Nyky-yhteiskunnassa toisinaan on tarve varmistaa oma tai toisen henkilön identiteetti tai tunnistaa joku ihminen. Luotettava ja mutkaton tunnistus helpottaa kaikkien elämää ja yleinen turvallisuus paranee, kun rikolliset tunnistetaan nopeasti ja pystytään erottamaan lainkuuliaiset ihmiset rikollisista. Kun automatisoimme tunnistusprosesseja, laajennamme tietokoneiden ja muiden laitteiden tärkeiden tehtävien määrää. Nämä uudet automatisoidut prosessit voivat parantaa turvallisuuttamme, tehokkuuttamme ja käyttömukavuuttamme.

Tämän insinöörityön tarkoituksena oli kerätä tietoa biometrisistä tunnistus–menetelmistä ja käydä läpi niiden perusteita. Työ on kirjallisuustutkielma aiheesta, ja aiheen valintakriteerinä toimi kiinnostus aihetta kohtaan.

Työ koostuu kolmesta osasta. Ensimmäisessä osassa esitellään tunnistus–menetelmät yleisesti ja valitaan tämän tutkimuksen syventymisen kohteeksi biometrinen tunnistus. Toinen osa käsittelee biometriseen tunnistamiseen liittyviä peruskäsitteitä ja periaatteita. Kolmantena osana on biometristen tunnistusmenetelmien esittely ja niiden perusteita.

Työssä mainitaan mm. yksityisyyden suoja ja monibiometriset menetelmät, jotka jätetään vain maininnalle työn rajaamisen vuoksi.

2 TUNNISTUSMENETELMÄT

Automatisoidut tunnistusjärjestelmät voidaan suunnitella toimimaan eri tavoin eri ihmisille ja niin, että ne reagoivat halutulla tavalla eri tilanteissa. Käytännössä tähän liittyy kaksi erillistä toimintoa: henkilöllisyyden varmennus sekä tunnistusmekanismi, joka yhdistää ja toteuttaa halutut toiminnot tuolle henkilölle. Esimerkiksi henkilö X eroaa töistä, jolloin järjestelmän tulee estää häntä käyttämästä mitään yrityksen järjestelmiä ja resursseja. Ei ole ongelma, vaikka tietokoneet yhä tunnistaisivat, kuka tämä henkilö on, kunhan häneltä evätään tietyt oikeudet.

Tunnistusjärjestelmät voidaan jakaa kolmeen ryhmään seuraavasti [4, s. 44.]:

- henkilön tiedossa oleva tunnistustieto (salasana, tunnusluku)
- henkilön mukana kulkeva tunnisteväline (kortti, poletti)
- henkilö itse (biometrinen tunniste)

2.1 Tunnistustieto, salasana tai tunnusluku

Salasanoja ja tunnuslukuja käytetään yritysten, koulujen ja jopa kotien ovissa, tietokoneissa ja monissa muissa lukemattomissa sovelluksissa. Ihmisten tulee muistaa useita eri käyttäjätunnuksia, salasanoja ja erilaisia tunnuslukuja. Teoriassa henkilö säilyttää tunnusluvut, käyttäjätunnukset ja niihin kuuluvat salasanat ulkomuistissa, valitsee salasanan niin, että se on lähes mahdoton arvata, eikä kerro salasanaa muille. Käytäntö on kuitenkin osoittanut useimmiten henkilön toimivan juuri päinvastoin: ihmiset useimmiten kirjoittavat kaiken muistiin, jakavat salasanoja ystävilleen ja valitsevat jonkin helposti arvattavan sanan tai yhdistelmän. Jotkin sovellukset pakottavat henkilön luomaan vaikeasti arvattavia salasanoja, mutta useimmat ihmiset luovat tämän seurauksena salasanamuistilistoja. Listan päätyessä vääriin käsiin salasanat eivät tarjoa enää minkäänlaista suojaa.

Salasanat ovat nykyisin yleisesti käytettyjä ja väärinkäytettyinä helposti uhattuja, mutta kaikesta huolimatta ne ilmentävät olennaisesti tarvetta automaattiselle tunnistukselle ja sen toimintaperiaatetta eli sitä, että käyttäjän tulee välittää jotakin tietoa tai esittää jokin näyte, jota kukaan muu ei voi tietää ja käyttää. Näitä piirteitä ja ominaisuuksia voidaan luokitella esimerkiksi seuraavasti:

- tunniste, tieto jota kukaan muu ei tiedä tai voi esittää
- varmenne, tieto jonka avulla voidaan varmentaa tunniste
- perussalaisuus, henkilön hallussa oleva tieto joka tuottaa tunnisteen
- täsmäys, prosessi jossa tunnistetta verrataan algoritmien avulla varmenteeseen

Yksinkertaisimmat salasana- ja tunnuslukusovellukset luovat kaikkein yksinkertaisimman tunnistusjärjestelmän, jossa henkilön oma muisti toimii tunnisteena, varmenteena ja perussalaisuutena. Käytännössä tämä tarkoittaa

käyttäjätunnusta ja/tai salasanaa, joita verrataan serverille ennalta tallennettuihin tietoihin. Käytännössä kuitenkin salasanoihin perustuvissa järjestelmissä niihin liitetään lukuisia kryptografisia tekniikoita ja hash-salakoodaus suojaamaan salasanoja varkauksilta. [1, s. 5.]

Salasanat toimivat luotettavasti, kunhan ne eivät ole helposti arvattavissa tai kaapattavissa tai päädy vääriin käsiin vahingossa. Esimerkiksi henkilön valitessa lempivärinsä salasanaksi, se on helppo arvata, ja tunkeutujan on mahdollista löytää oikea salasana niin sanotulla sanakirjahyökkäyksellä, koska käytetty sana on yleisesti tunnettu. Jos kyseessä on verkossa tapahtuva tunnistus, niin tunkeutuja voi kaapata salasanan lähetyksen aikana. [1, s. 5.; 4, s. 44.]

Vaikka hyökkäyksiä vastaan on joukko menetelmiä, niin mikään ei niistä ei estä salasanan jakamista. Vaikka yrityksissä ja sovelluksissa yleensä on sääntöjä ja ohjeita, että salasanoja ei saa jakaa muiden kanssa, niin näin ei kuitenkaan aina toimita, vaan ihmiset käyttävät samoja salasanoja ja jopa toistensa tunnuksia. Syynä tälle on yleisesti se, että jokin työ vaatii salasanasuojatun tietokoneen käyttöä eikä uusien tunnusten luonti onnistu helposti tai ei vaivauduta opettelemaan omia tunnuksia ja salasanoja. Käyttäjätunnukset saatetaan myös antaa tilapäisesti tuuraavan henkilön käyttöön, kun varsinainen työntekijä sairastuu, koska ei vaivauduta luomaan uutta käyttäjätiliä tilapäiselle henkilölle muutaman päivän tai viikon vuoksi. Ihmisillä on myös tapa tehdä salasanojen muistaminen itselleen helpoksi käyttämällä samaa salasanaa eri sovelluksissa, jolloin kaikki kyseiset sovellukset ovat tunkeutujan käytettävissä salasanan päätyessä vääriin käsiin.

Ongelma on lopulta se, että tarvittaessa ei voida jäljittää ja erottaa, mitkä olivat alkuperäisen käyttäjän tekemisiä ja mitkä tilapäistyöntekijän tai vuoroparin. Tämä heikentää vastuunalaisuutta, jota suunnitellun järjestelmän on tarkoitus tarjota. Lisäksi salasana ja käyttäjätunnus tulee sitä helpommaksi varastaa, mitä useampi henkilö sen tietää. Kuten vanha sanontakin sanoo: kaksi ihmistä voi pitää salaisuuden vain, jos toinen on kuollut.

2.2 Tunnistusväline, avainkortti tai poletti

Fyysiset tunnistusvälineet, kuten avainkortit ja poletit suunniteltiin alun perin eliminoimaan tiettyjä salasanasuojauksen heikkouksia. Suurin avainkorttien ja polettien hyöty on se, että niitä ei voi jakaa samalla tapaa kuin salasanoja. Jos henkilö lainaa avainkorttiaan tai polettiaan, niin toinen henkilö voi kirjautua muttei alkuperäinen omistaja. [1, s. 6.]

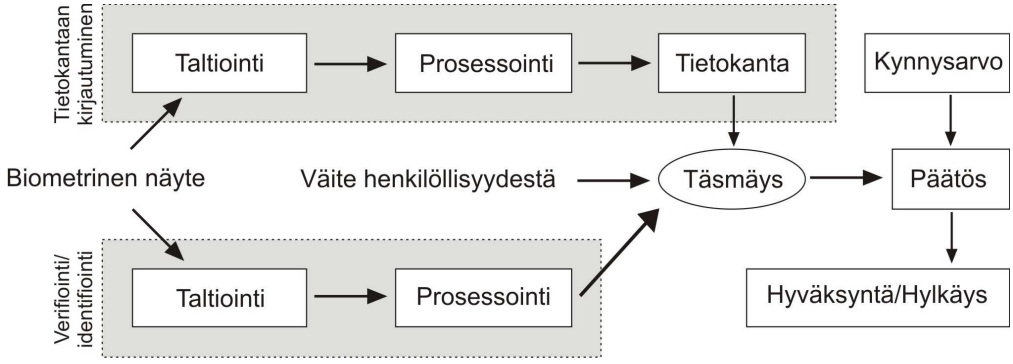
Yleensä nämä avainkortit ja poletit sisältävät perussalaisuuden, joten henkilön itse ei tarvitse sitä opetella. Henkilön tarvitsee vain muistaa kantaa avainkorttia tai polettia mukanaan, jotta se on lähettyvillä, kun hän tarvitsee sitä. Yleensä tämän kaltaiset järjestelmät käyttävät perussalaisuutta luodakseen vaikeasti ennakoitavan arvon. Kun henkilö haluaa kirjautua sisään, hänen välineensä luo oikean tunnisteen, jonka hän joko näppäilee sisään kuten normaalin salasanan tai sitten laite lukee tiedon automaattisesti. Yleensä nämä järjestelmät eivät hyväksy samaa salasanaa kahdesti. Tämä kasvattaa turvallisuutta, koska salasanan kaappaaminen ja uudelleenkäyttö ei ole mahdollista. Tämän kaltaisten järjestelmien huono puoli on se, että käyttäjä pystyy kirjautumaan vain paikoissa, joissa on kortin tai poletin lukijalaite. [1, s. 6.; 4, s. 44.]

2.3 Tunnistusominaisuus, biometrinen tunniste

Biometrinen tunnistus perustuu mitattavissa oleviin ihmisen fyysisiin tai henkilökohtaisiin piirteisiin, jotka ovat henkilölle yksilöllisiä. Yleisimmät ja tunnetuimmat biometriset tunnistuksen menetelmät yrittävät tunnistaa henkilön sormenjälkien, kämmengeometrian, silmän, kasvojen tai puheen kautta. Tunnistaminen tapahtuu vertaamalla juuri suoritettuja mittauksia aiemmin tietokantaan tallennettuihin. Biometrisellä tunnistuksella on kaksi käyttökohdetta: identifiointi ja verifiointi.

Identifiointiprosessissa pyritään määrittämään henkilön identiteetti. Tunnistusjärjestelmä lukee näytteen, käsittelee sen ja vertaa sitä jokaiseen näytteeseen tietokannassa. Tämän kaltaista toimenpidettä kutsutaan ”one to many” -hauksi (1:N). Riippuen järjestelmästä se esittää parhaimman osuman ja/tai joukon mahdollisia osumia luokitellen ne todennäköisyyksien mukaisesti. [1, s. 8.; 4, s. 44.]

Verifiointiprosessissa pyritään varmentamaan henkilön identiteetti. Verifiointijärjestelmä yleisesti vaatii henkilöltä kortin, poletin, asiakirjan tai jonkin muun syötteen kuten käyttäjätunnuksen, jolla tämä esittää olevansa kyseinen henkilö. Tämä liittää henkilön tietokantaan tallennettuun mallinteeseen. Biometrisen näytteen annettuaan järjestelmä vertaa sitä tietokantassa olevaan. Tämän kaltaista toimenpidettä kutsutaan ”one to one” -hauksi (1:1). Lopuksi järjestelmä joko tunnistaa tai ei tunnista henkilöä verrattuaan juuri annettua näytettä tietokannassa olevaan mallinteeseen. Kuvassa 1 on tyypillisen biometrisen järjestelmän perusrakenne. [1, s. 8.; 4, s. 44.]



Kuva 1. Biometrinen järjestelmä prosessikaaviona. *Rekisteröintiprosessissa biometrinen näyte luetaan sensorilla digitaaliseen muotoon, josta algoritmit muuntavat sen mallinteeksi (template), minkä jälkeen se tallennetaan tietokantaan. Verifiointi- ja identifiointiprosessi on samanlainen täsmäykseen asti, jossa luotua mallinnetta verrataan tietokannassa oleviin mallinteisiin, minkä jälkeen tulos ilmoitetaan asetettujen kynnysarvojen mukaisesti muodossa ”hylkäys”, ”hyväksytty”, ”vastaavuus löydetty” tai ”vastaavuutta ei löydetty”.*

Tunnistusprosessi alkaa biometrisestä lukijalaitteesta, jolle henkilö esittää biometrisen näytteen. Lukijan sensorit tallentavat biometriset arvot ja luovat mallinteen niiden pohjalta. Mallinne toimii henkilön tunnisteena. Varmenne on luotu yhdestä tai useammasta biometrisestä näytteestä, jotka on tallennettu tietokantaan henkilön rekisteröityessä järjestelmään. Seuraavaksi järjestelmä vertaa, kuinka paljon tunnistusprosessissa luotu mallinne vastaa tietokannassa olevaa mallinnetta. Jos tunniste vastaa varmennetta asetettujen raja-arvojen puitteissa, niin järjestelmä tunnistaa henkilön tai hyväksyy käyttäjän sisäänkirjautumisen. Jos tunniste ei vastaa mallinnetta riittävästi, niin järjestelmä hylkää käyttäjän sisäänkirjautumisen tai ”one to many” -haun ollessa kyseessä

ei joko tunnista henkilöä tai lukee tämän mahdollisten osumien joukkoon. [1, s. 8; 4, s. 44.]

Ihmiselle yksilölliset biometriset piirteet tai ominaisuudet toimivat perussalaisuutena ja näin ihminen on aina valmis varmentamaan itsensä, jos sille on tarvetta. Biometriset tunnisteet eivät ole kuitenkaan niin salaisia kuin luulemme. Ihmiset jättävät jälkeensä tunnistettavia jälkiä kuten sormenjälkiä, puhettamme voidaan nauhoittaa, käsiämme ja kasvojamme kuvata. Kaikkia näitä voidaan käyttää väärennetyn tunnisteen luomiseksi, jonka avulla tunnistusjärjestelmiä voidaan huijata. Huijausten estämiseksi onkin olemassa useita menetelmiä, joista tärkeimpiä ovat monibiometriset menetelmät ja aitouden varmennus.

3. BIOMETRINEN TUNNISTUS

Kykenemme ihmisinä tunnistamaan muita ihmisiä heidän puheensa, kasvojensa tai muiden heille ominaisten piirteiden perusteella. Laitteet täytyy suunnitella niin, että ne kykenevät tunnistamaan ihmiselle yksilölliset piirteet ja ohjelmoida niin, että ne pystyvät tekemään eron kahden henkilön välillä. Tekniikan ja algoritmien kehittyessä ero inhimillisen erotuskyvyn ja koneellisen tunnistuksen välillä pienenee. Biometriikan tarkoitus on tarjota luotettava ja varma tapa tunnistaa henkilö ja varmentaa tämän henkilöllisyys luotettavasti, nopeasti ja mahdollisimman vaivattomasti.

3.1 Yleistä tietoa

Biometriikka tarkoittaa kirjaimellisesti ihmismittaustiedettä. Sana viittaa henkilötunnistamisen automatisoituihin menetelmiin joko fyysisten tai olemukseen liittyvien piirteiden avulla. Viime vuosien kasvanut kiinnostus biometristä tunnistusta kohtaan johtuu luotettavien ja silti vaivattomien, kustannustehokkaiden ja helposti omaksuttavien universaalien vahvojen tunnistusmenetelmien puutteesta. [1, s. 27.]

Biometristä tunnistusta käytettäessä henkilö ei voi hävittää tai unohtaa avainkorttia tai salasanaa, koska henkilö itse toimii tunnisteena. Useimmat käytetyistä tunnisteista pysyvät muuttumattomina koko ihmisen eliniän.

Biometrisen tunnistuksen käyttö myös vähentää tarvetta vaihtaa hävinneitä avainkortteja tai unohtuneita salasanoja.

Salasanat ja avainkortit ovat helposti varastettavissa. Biometrinen tunnistus vähentää riskiä, että toinen henkilö voisi esittää hyväksytyn tunnisteen ja näin päästä luvatta käsiksi toimintoihin, joihin hänellä ei normaalisti olisi oikeuksia. Näin biometrinen tunnistus mahdollistaa vahvan ja luotettavan tavan henkilön tunnistamiseksi salasanaan tai avainkorttiin verrattuna. [1, s. 27.]

Vuosien laite- ja ohjelmatekniikan kehitys on mahdollistanut nykyisin kaupallisesti kilpailukykyisten biometristen tunnistusjärjestelmien kehityksen. Prosessorien laskentatehon kasvu ja tietokoneiden verkostoituminen on mahdollistanut entistä suurempien tietokantojen käytön biometrisissä järjestelmissä.

Nykyisin lukuisat julkiset ja yksityiset järjestöt hyödyntävät biometriikkaa. Viranomaisten kiinnostus biometrisiin tunnistusjärjestelmiin on kasvanut erityisesti viime vuosina tapahtuneiden terroristihyökkäysten vuoksi. Valmistajat ovat viime vuosina kasvavassa määrin lisänneet erilaisten biometristen järjestelmien tuotantoa ja tutkivat uusia tapoja ja mahdollisuuksia kehittää biometriikkaa entisestään.

3.2 Biometriset tuntomerkit ja ominaisuudet

Biometrisiä tuntomerkkejä ja ominaisuuksia kuvataan termeillä vahva ja yksilöllinen. Vahvuus eli näytteen toistettavuus viittaa tuntomerkin tai ominaisuuden muuttumattomuuteen ihmisen eliniän aikana ja siihen, kuinka onnistuneesti se voidaan tunnistaa automaattisin mittauskeinoin tuona aikana. Vahva biometrinen tunniste on siis funktio, joka kuvaa sen stabiiliutta ja kestävyyttä muutosten suhteen. Yksilöllisyys viittaa biometrisen tuntomerkin tai ominaisuuden eroihin ihmisten välillä ja siihen, että tämä ero voidaan tunnistaa.

Biometriset tuntomerkit ja ominaisuudet voidaan jakaa kolmeen eri ryhmään:

- genotyyppi eli perimätyyppi
- fenotyyppi eli yksilön ilmiasu
- olemus

Genotyyppi eli perimätyyppi on yksilön vanhemmilta perittyjen geenimuotojen kokonaisuus. Geneettisiä piirteitä kuten kasvojen rakennetta ja muotoa on vaikea muokata, ja vaikka se ei teoreettisesti ole täysin mahdotonta, niin kyseisiä ominaisuuksia pidetään yksilöllisinä [12].

Fenotyyppi eli yksilön ilmiasu on yksilön kaikkien havaittavien ominaisuuksien kuten anatomisten, biokemiallisten, fysiologisten ja käyttäytymisen muodostama kokonaisuus. Tämän ryhmän ominaisuudet kehittyvät hyvin aikaisissa sikiön kehitysvaiheissa. Nämä geneettisesti satunnaisesti kehittyvät ominaisuudet ovat yksilöllisiä, ja niitä on käytännössä mahdoton muokata [11].

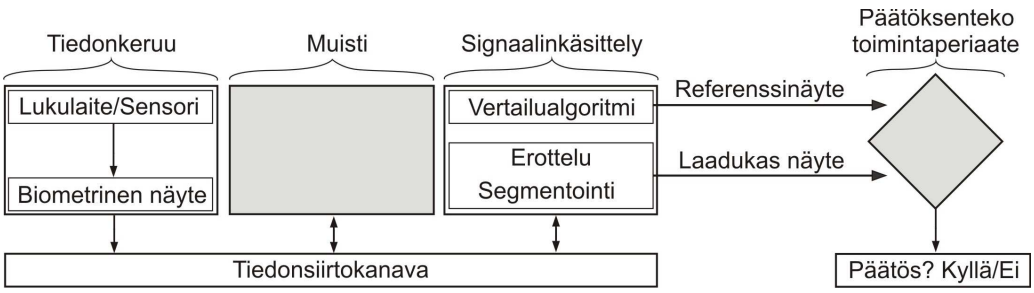
Olemukseen kuuluvat ominaisuudet ovat opittuja tai harjoiteltuja henkilön tekemiseen perustuvia tapoja kuten puhetyyli tai käsiala. Teoriassa henkilö voi muuttaa kävelytyyliään tai opetella uuden käsialan, mutta aikuisikään mennessä henkilö ei pysty juurikaan pääsemään vanhoista tavoistaan eroon [1, s. 28].

Kaikki biometriset tunnisteet sisältävät piirteitä jokaisesta näistä kolmesta ryhmästä, kuten esimerkiksi tapa, jolla henkilö esittää sormenjälkensä biometriselle lukulaitteelle. Kaupalliset saatavilla olevat järjestelmät kuitenkin keskittyvät pääsääntöisesti vain yhden ryhmän biometrisiin mittauksiin kuten sormenjälkiin tai kämmenen geometrisiin mittoihin. [1, s. 29.]

3.3 Biometrisen järjestelmän toimintaperiaate

Biometrisen järjestelmän toimintaperiaate koostuu neljästä vaiheesta (kuva 2):

- tiedonkeruu
- tiedonsiirtokanava
- signaalinkäsittely
- päätöksenteon toimintaperiaate.



Kuva 2. Biometrisen järjestelmän komponentit ja prosessikaavio. *Tiedokeruu–prosessissa biometrinen näyte luetaan, minkä jälkeen saatu informaatio siirretään tiedonsiirtokanavaa pitkin signaalinkäsittelyprosessiin, jossa näytteestä luodaan mallinne, joka voidaan siirtää ja rekisteröidä muistiin tiedonsiirtokanavaa pitkin. Päätöksentekoprosessi vertaa esitettyä laadukasta mallinnetta muistin tietokannassa oleviin referenssimallinteisiin, minkä jälkeen ilmoitetaan tulos muodossa ”hyväksytty” tai ”hylätty”.*

3.3.1 Tiedonkeruu

Tiedonkeruu on vaihe, jossa biometrinen näyte annetaan järjestelmälle. Vaihe sisältää biometrisen näytteen kaappaamisen digitaalisessa muodossa ja näin saadun informaation siirron signaalinkäsittelyyn. Jos biometrinen näyte luetaan etälukulaitteella, niin tieto voidaan pakata ja salata ennen tiedonsiirtoa. [1, s. 29.]

3.3.2 Tiedonsiirtokanava

Tiedonsiirtokanava viittaa tiedonsiirtoreitteihin järjestelmän eri osien ja toimintojen välillä. Osa biometrisistä järjestelmistä toimii itsenäisesti, ja tiedonsiirtokanavat ovat laitteen sisäisiä. Suuremmat hajautetut järjestelmät sisältävät keskustietokannan, johon yhdistyy useita etätiedonkeruupisteitä. Näiden välisenä tiedonsiirtokanavana voidaan käyttää esimerkiksi LAN-verkkoa tai Internet-verkkoa. [1, s. 29; 6, s. 47.]

3.3.3 Signaalinkäsittely

Signaalinkäsittely, josta myös tietyissä asiayhteyksissä käytetään termiä kuvankäsittely, on vaihe jossa biometrinen näyte tai biometriset lähtöarvot käsitellään algoritmien avulla epäoleellisen informaation ja häiriöiden

poistamiseksi ja/tai tärkeiden piirteiden korostamiseksi, minkä jälkeen paikannetaan tunnistusprosessille tärkeä informaatio ja taltioidaan halutut biometriset piirteet muistiin itse tunnistustapahtumaa varten. Vaiheesta yleisesti käytetään termiä mallinteen luominen.

Tietojenkäsittely koostuu näytteen segmentoinnista, tunnistukselle oleellisten piirteiden eristämisestä ja erottelemisesta ja lopulta itse biometrisen mallinteen muodostamisesta (matemaattinen esitysmuoto alkuperäisestä biometrisestä tunnisteesta). Segmentointi on vaihe, jossa erotellaan olennainen biometrinen informaatio muusta taustainformaatiosta, kuten esimerkiksi puhenäytteen alussa ja lopussa mahdollisesti olevien ylimääräisten signaalikomponenttien pois leikkaaminen. Vaiheesta yleisesti käytetään termiä piirreirrotus.

Kun biometrinen mallinne on luotu, voi ydinvertailuprosessi joko rekisteröidä mallinteen tai verrata mallinnetta yhteen tai useampaan referenssimallinteeseen. Vertailuprosessi muodostaa vertailutuloksen, joka ilmaisee kuinka samankaltaisia mallinteet ovat keskenään. Mallinteen luonti ja rekisteröinti muodostaa laatutuloksen, joka ilmaisee kuinka laadukas alkuperäinen näyte on tai kuinka hyvin biometrisen informaation karsiminen haluttuihin tärkeimpiin peruspiirteisiin onnistui. Lopuksi päätöksentekoprosessi käyttää vertailu- ja laatutulosta asetettujen raja-arvojen mukaisesti määrittääkseen, onko kyseessä hyväksytty tunnistus tai mallinteen rekisteröinti. [1, s. 30; 6, s. 47.]

3.3.4 Päätöksenteon toimintaperiaate

Päätöksenteon toimintaperiaate on viimeinen vaihe, jossa sovellus arvioi signaalinkäsittelyn tuloksia annetun näytteen ja tietokannassa olevan referenssimallinteen suhteen, minkä jälkeen prosessi tekee lopullisen päätöksen (hyväksytty tai hylätty) sen suhteen, vastaavatko mallinteet toisiaan asetettujen raja-arvojen puitteissa. Juuri otetun näytteen tulee myös olla riittävän laadukas, ja jos näytteen informaatio ei vastaa sille asetettuja raja-arvoja, niin sen tulkitaan olevan epäkelpo ja käyttäjä joutuu antaamaan uuden näytteen, kunnes saadaan taltioitua tarpeeksi laadukas näyte. [1, s. 30; 6, s. 47.]

Esitelty päätöksenteon toimintaperiaate on vain esimerkki yleisesti käytössä olevasta menettelytavasta. Esimerkistä poikkeavat toimintaperiaatteet ovat siis

mahdollisia, ja lopulta tämä vaihe voidaan räätälöidä asiakkaan ja loppukäyttäjien vaatimusten ja toivomusten mukaiseksi.

3.3.5 Tietokantaan rekisteröityminen

Ensimmäistä kertaa tietokantaan rekisteröityvän henkilön tulee antaa yksi tai useampi biometrinen näyte, jonka pohjalta luodaan biometrinen mallinne. Myöhemmin käyttäjän sisäänkirjautuessa järjestelmään verrataan lukulaitteella otettua biometristä näytettä tietokannassa olevaan referenssimallinteeseen. Tietokantaan luotavaan mallinteeseen tarvittava näytteiden määrä riippuu käytetystä biometrisestä menetelmästä, henkilöstä, käyttö- ja kirjautumisympäristöstä, sekä suorituskyky- ja tunnistustarkkuusvaatimuksista. Kunnollisen mallinteen luomista heikentäviä tekijöitä ovat esimerkiksi sormen huono asemointi lukulaitteessa, likainen lukulaitteen sensori, likainen tai vammautunut sormi. Vertailualgoritmien suorituskyky myös paranee, kun tietokantaan kirjautuessa otetaan useampia näytteitä. Mallinne luodaan useampien näytteiden keskiarvona, minkä jälkeen se taltioidaan tietokantaan. Useampien otettujen näytteiden vuoksi tietokantaan rekisteröityminen kestää kauemmin kuin itse järjestelmään sisäänkirjautuminen.

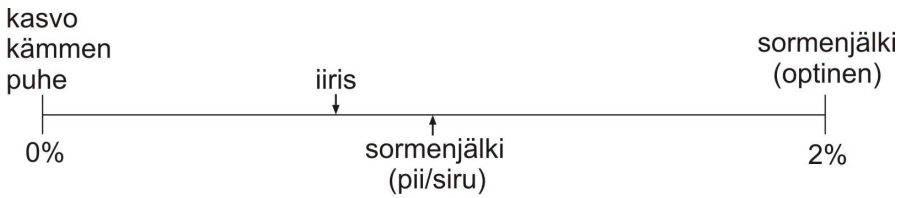
Järjestelmät tyypillisesti antavat näytteiden pohjalta kirjautumisarvon, joka kuvaa tietokantaan kirjautumisen laatua. Etukäteen asetettujen parametrien mukaisesti tuon arvon tulee olla yli tietyn hyväksytyn raja-arvon. Raja-arvoa valitessa tulee huomioida käyttömukavuus ja rekisteröitymisen läpimenoaika. Suuri/pieni arvo merkitsee suurempaa/pienempää vertailutarkkuutta. Tietyissä erikoissovelluksissa mallinne voidaan luoda vain yhden näytteen pohjalta. Tämän kaltaisia järjestelmiä voidaan hyödyntää mm. valvontajärjestelmissä, joissa henkilön kasvokuva taltioidaan, ja sen pohjalta luodaan mallinne, jonka avulla henkilö voidaan myöhemmin tunnistaa ja näin jäljittää hänen liikkeitään valvontakameroiden avustuksella. [1, s. 31.]

Tarkkuus on tärkeä asia referenssimallinnetta luotaessa. Rekisteröitymisessä epäonnistumista mitataan epäonnistuneiden rekisteröitymisten määrällä (FTER). FTER määritetään kaikkien tietokantaan rekisteröityvien henkilöiden ja epäonnistuneiden rekisteröitymisten määrän suhteena. Mitä suurempi FTER on,

sitä suuremmalla todennäköisyydellä kyseinen biometrinen järjestelmä ei sovi käytettäväksi suurille käyttäjämäärille.

$$FTER = \frac{epäonnistuneiden\ rekisteröitymisten\ määrä}{rekisteröityvien\ henkilöiden\ määrä}$$

FTER:ään vaikuttavat useat ympäristölliset tekijät, henkilön syntyperä, työ ja elämäntyyli. Esimerkiksi ihmisen sormenjäljet ovat alttiita vammoille ja kulumille, jos henkilö työskentelee paljon käsillään. Myös sormenjälkipiirteissä on huomattaviakin eroavaisuuksia etnisten ryhmien välillä. Tämän kaltaiset tekijät tulee huomioida ennen kuin biometrinen järjestelmä otetaan käyttöön. Kuvassa 3 on joukko biometrisiä menetelmiä ja niiden sijoittuminen suhteellisesti FTER-vertailussa. [1, s. 32; 3, s. 24.]



Kuva 3. Muutamien biometristen menetelmien sijoittuminen suhteellisesti FTER-vertailussa. *Vertailun tulokset pohjautuvat Tony Mansfieldin biometristen laitteiden testituloksiin maaliskuun 21. päivänä 2001 julkaistussa raportissa:"Biometric product testing: final report".*

3.3.6 Tietokantaan rekisteröitymisen toimintaperiaate

On välttämätöntä määrittää, kuinka tarvittava informaatio mallinteiden luomiseksi kerätään. Menettelytapaa valittaessa tulisi huomioida:

- tarvittava lisäinformaatio
- kirjautumisyritysten maksimi määrä
- kirjautumisinformaation tallennusmedia ja säilytysmuoto
- vaihtoehtoisten tai monibiometristen järjestelmien käyttö
- kirjautumistoimisto ja sen henkilökunta

Lisäinformaatio voi olla tarpeen riippuen biometrisen järjestelmän käyttökohteesta. Joissakin sovellutuksissa henkilökohtaisen informaation sisällyttäminen osaksi biometristä tunnistusjärjestelmää voi olla tarpeen.

Kirjautumisyrityksille on hyvä asettaa maksimi määrä, oli kyse rekisteröitymisestä tai sisäänkirjautumisesta. Nykyiset järjestelmät saattavat vaatia joissakin tilanteissa keskimäärin neljä tai viisi yritystä, ennen kuin järjestelmä saa asetetun raja-arvon ylittävän näytteen taltioitua. Tämä yleensä johtuu käyttäjästä tai ympäristöllisistä tekijöistä. Jos lukijaa käyttävät useat ihmiset, niin on hyvä rajoittaa kirjautumisyritysten määrää ihan vain ruuhkatilanteiden välttämiseksi ja tarvittaessa opastaa käyttäjää hakemaan konsultointiapua järjestelmän ylläpitäjältä. [1, s. 33.]

Kirjautumisinformaation tallennusmedia ja säilytysmuoto voi olla verkoistettu, paikallinen tai kannettava muisti. Osin tämä riippuu valitusta biometrisestä järjestelmästä. Kannettava muisti parantaa henkilön yksityisyydensuojaa, koska hänen biometrinen mallinteensa ja informaatio säilyvät hänen hallussaan, mutta toisaalta heikentää tehokkuutta ja käyttömukavuutta. Kannettavan muistin myötä katoaa myös yksi biometrian tuomista suurista eduista eli se, että henkilön ei tarvitse muistaa ottaa mukaan avainkorttia tai polettia.

Tilanteesta riippuen voi olla tarve käyttää vaihtoehtoista tunnistusjärjestelmää. Kyseinen tilanne voi esimerkiksi johtua pysyvästä/tilapäisestä vammasta tai syntymäviasta, jonka vuoksi suunnitellun biometrisen tunnistusmenetelmän käyttö ei ole mahdollista. Käytettävää biometristä menetelmää valitessa tuleekin huomioida sen käyttöympäristö ja mahdolliset vaihtoehtoiset toimenpiteet.

Monibiometristen järjestelmien avulla on mahdollista tehdä entistä tarkempia ja luotettavampia turvajärjestelmiä. Monibiometristen menetelmien avulla on mahdollista lisätä aitouden varmennus sellaisiin biometrisiin menetelmiin, jotka eivät sisällä sitä luonnostaan. Usean biometrisen ominaisuuden tai piirteen tunnistus yhtäaikaisesti ei vain paranna tunnistustarkkuutta, vaan vaikeuttaa myös keinotekoisten tunnisteiden luontia. [1, s. 33.]

Kirjautumistoimiston ja koulutetun henkilökunnan käyttö on tarpeen silloin, kun halutaan ja katsotaan tarpeelliseksi opastaa ihmisiä järjestelmän käytössä. Näin

myös varmistetaan, että tietokannassa olevat mallinteet ovat tasalaatuisia ja oikeaoppisesti rekisteröity järjestelmään. Kyse ei aina ole pelkästä opastuksesta, vaan tietyissä käyttökohteissa on myös tarve valvoa rekisteröitymisprosessia ja näin estää mahdolliset huijaukset. [1, s. 33.]

3.3.7 Päätöksenteko

Automaattisessa biometrisessa tunnistuksessa tunnistustarkkuus on tärkeä osa päätöksentekoa. On suhteellisen helppo ylläpitää korkea tunnistusaste ja tarkkuustaso one-to-one-tyypin vertailussa eli henkilöllisyyden varmennuksessa, koska näytettä verrataan vain yhteen tietokannassa olevaan mallinteeseen. Tämän tyypin järjestelmät ovat suhteellisen yksinkertaisia hallita ja ylläpitää.

Tunnistus eli one-to-many-tyypin vertailu on vaikeampi ja työläämpi toiminto, koska näytettä verrataan kaikkiin tietokannassa oleviin mallinteisiin. Tietokannan kasvaessa tunnistus vaikeutuu, koska hakujen täytyy käydä läpi entistä suurempia määriä rekisteritietoja ja näin myös hakuajat ja resurssivaatimukset kasvavat. Yhä useampia rekisteritietoja läpikäydessä myös mahdollisten vastineiden määrä kasvaa. Tunnistushaku muodostaa listan mahdollisista vastineista (esim. lista mahdollisista rikollisista, joiden kasvot vastaavat turvakameroiden taltioimaa kuvaa). Tämän tyypin järjestelmät ovat kalliimpia kuin henkilöllisyyden varmennusjärjestelmät niiden laitteisto- ja ohjelmistovaatimusten vuoksi.

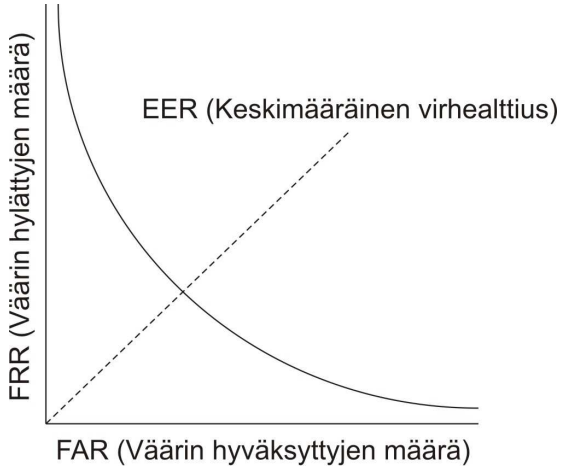
Väärien hyväksyntöjen määrä (FAR) ja väärien hylkäysten määrä (FRR) ovat ensisijaisen tärkeitä tarkkuutta kuvaavia mittoja. FAR, joka tunnetaan myös väärin hyväksyttyjen prosenttina (FMR) tai tyypin II virheenä kuvaa, kuinka monta prosenttia huijareista pääsee keskimäärin järjestelmään sisään. FAR lasketaan kaavan 1 mukaisesti, jossa FA on väärin hyväksyttyjen määrä ja N on näytteiden kokonaismäärä. [5, s. 7.]

$$FAR = \frac{FA}{N} * 100 \qquad (1)$$

FRR, joka tunnetaan myös väärin hylättyjen prosenttina tai tyypin I virheenä, kuvaa kuinka monta prosenttia aidoista käyttäjistä keskimäärin hylätään väärin perustein. FRR lasketaan kaavan 2 mukaisesti, jossa FR on väärin hylättyjen määrä ja N on näytteiden kokonaismäärä. [5, s. 8.]

$$FRR = \frac{FR}{N} * 100 \qquad (2)$$

FAR:n ja FRR:n avulla voimme määrittää, mikä biometrinen menetelmä sopii ja toimii parhaiten kyseisessä käyttöympäristössä ja tilanteessa (kuva 4).



Kuva 4. Keskimääräinen virhealttius (EER). *EER on FAR:n ja FRR:n leikkauspiste. Mitä pienempi EER on, sitä tarkempi kyseinen biometrinen menetelmä tai järjestelmä on. [1, s. 36; 5, s. 8.]*

Tunnistus voidaan suorittaa joko henkilön vapaaehtoisella suostumuksella tai salassa häneltä ilman hänen suostumustaan. Useimmat biometriset menetelmät lukeutuvat ensin mainittuun ryhmään, mutta osa biometrisistä menetelmistä kuitenkin mahdollistaa salattujen tunnistusjärjestelmien käytön kuten esimerkiksi kasvojentunnistuksen valvontakameroiden avustuksella.

Pääsääntöisesti biometriikasta puhuttaessa tarkoitetaan elävien henkilöiden vertailua. Nykyisin biometrisissä järjestelmissä käytetäänkin erilaisia menetelmiä, jotta voidaan havaita mahdolliset keinotekoiset tunnisteet. Biometrisen tunnisteen aitouden varmentamisessa voidaan hyödyntää

esimerkiksi ihmisen ruumiinlämmön tunnistusta tai liikkeentunnistusta. Kaikki biometriset järjestelmät eivät sisällä aitouden varmennusta. Useimmat yritykset eivät ole sisällyttäneet aitouden tunnistusta osaksi järjestelmiään lisääntyvien kustannusten vuoksi.

Tietyissä sovelluksissa on myös ehdottoman tärkeää, että on olemassa turvatoimenpiteitä sellaisille tilanteille, joissa henkilö pyrkii pääsemään käsiksi toimintoihin, joihin hänellä ei normaalisti olisi valtuuksia, esimerkiksi pakottamalla toista valtuutettua henkilöä suorittamaan tunnistuksen hänen puolestaan. Esimerkiksi sormenjälkien tunnistuksessa luvallinen henkilö voidaan tunnistaa kaikista sormista, mutta jos tunnistusta ei suoriteta oikealla sormella, niin järjestelmä käynnistää hiljaisen hälytyksen.

Vertailu on myös altis erilaisille käyttäjään ja käyttöympäristöön liittyville sekä biologisille tekijöille, joiden vaikutukset vaihtelevat eri biometrsisten menetelmien ja käytettyjen laitteiden välillä. Taulukossa 1 on näistä muutamia mainittuna.

Taulukko 1. Tekijöitä jotka vaikuttavat heikentävästi rekisteröintiin ja mallinteiden täsmäykseen *[1, s. 37]*

Menetelmä	**Tekijä joka aiheuttaa virheen**	**Mahdolliset ratkaisut**
Kaikki	Mallinteiden vanheneminen iän myötä ja muiden tekijöiden vuoksi	- Uudelleen rekisteröinti - Mallinteiden päivitys
Sormenjälki	Sormenjälkien rappeutuminen joka aiheutuu mm. työstä, ikääntymisestä tai vammautumisesta.	- Useampien sormien rekisteröinti tietokantaan - Mallinteiden päivitys
Kämmen	Vamma	- Molempien käsien rekisteröinti tietokantaan
Kasvot	Ympäristölliset tekijät kuten valaisu, miljöö, henkilön asento ja liike, silmälasit	- Kontrolloidut skenaariot - Usean kameran ja kamerakulman käyttö
Iiris	Henkilön asento ja liike, väärin kohdistettu katse, silmälasit	- Lukijalaitteen käytölle luonteenomainen sijainti - Käyttäjien kouluttaminen
Puhe	Tauti tai sairaus, henkilön ikä, äänen tallennusjärjestelmien eroavaisuus	- Uudelleen rekisteröinti - Yhdenmukaisten äänen tallennusjärjestelmien käyttö

3.4 Muistinhallinta

Muistinhallinta on hyvin tärkeä osa tunnistusprosessia. Virheitä ja häiriöitä tulee olla mahdollisimman vähän, järjestelmän tulee toimia mahdollisimman tehokkaasti ja suoriutua suoritettavista hakukyselyistä nopeasti, ja tietokannan käytön tulee olla vaivatonta.

Mallinteet eivät ole raakadataa tai skannattuja kuvia biometrisestä näytteestä, vaan lähes poikkeuksetta joukko henkilölle tunnusomaisia piirteitä, jotka biometrinen järjestelmä on erottanut ja taltioinut otetusta näytteestä. Esimerkiksi sormenjälkien kohdalla nämä piirteet voivat sisältää erilaisten yksityiskohtien sijainnin. Hyödyntäen näiden sijaintia algoritmit sallivat tietyn verran poikkeamaa näytteenlukuvaiheessa tapahtuvan hienoisen liikkeen vuoksi ja sellaisten ympäristöllisten tekijöiden vuoksi kuin lika tai rasva. Todellisuudessa biometrisen tunnisteen esittäminen lukulaitteelle ei ikinä tuota täysin identtistä tulosta, mutta ominaiset piirteet kuitenkin pysyvät muuttumattomana.

Mallinteiden käytön ongelma on se, että ne toimivat ikään kuin tilannekuvana tietylle biometriselle tunnisteelle juuri sinä tiettynä taltioinnin ajanhetkenä. Biometrinen tunniste, kuten henkilön puhe, voi muuttua henkilön iän tai epänormaalien olosuhteiden vuoksi. Tämän kaltaisesta muutoksesta puhuttaessa tarkoitetaan mallinteen vanhenemista, ja jotta olisi käytössä ajan tasalla oleva referenssimallinne, tulee sitä päivittää. Mallinteiden vanhenemisesta ei ole testituloksia pitkältä ajanjaksolta, mutta voidaan olettaa, että mallinteiden vanheneminen vain pahenee ajan myötä tietokantojen suuretessa ja sisältäessä ihmisiä kaikista ikäluokista. Osalla biometrisistä järjestelmistä on mahdollisuus päivittää biometristä referenssimallinnetta jokaisen näytteen lukutapahtuman aikana. Näin biometrisen järjestelmän referenssimallinne olisi aina ajan tasalla oleva keskiarvo. Testitulosten puutteen vuoksi on kuitenkin mahdotonta sanoa, kuinka tämän kaltainen keskiarvoinen referenssimallinne vaikuttaisi tunnistustarkkuuteen.

Tietyissä sovelluksissa on tärkeää säilyttää epäonnistuneiden yritysten mallinteet, jotta voidaan välttyä huijausyrityksiltä, ja mahdollisesti myöhemmin suoritettavien selvitysten vuoksi.

Mallinteiden koko on yksi osa niiden hallinnointia. Biometrisestä tunnisteesta riippuen sen koko vaihtelee, ja taulukossa 2 on nykyisin käytettävien mallinteiden keskimääräinen koko. Tietokantaan taltioidaan kuitenkin useampia mallinteita henkilöä kohden, mikä kasvattaa tarvittavaa tilan määrää. Vaihtoehtoisten mallinteiden tilantarve tulee huomioida järjestelmän suunnittelussa. [1, s. 38.]

Taulukko 2. Biometristen tunnistusmenetelmien mallinteiden arvioitu tilantarve *[1, s. 38]*

Biometrinen tunniste	**Mallinteen koko tavuina (B)**
Kämmen	8
Retina	96
Kasvo	84 - 2000
Puhe	70 - 80 per nauhoitettu sekunti
Iiris	256 - 512
Sormenjälki	256 - 1200
Allekirjoitus	500 - 1000

Nykyaikaiset pakkausmenetelmät ovat mahdollistaneet biometristen mallinteiden ja kuvien pakkaamisen entistä pienempään kokoon, jolloin ne vievät vähemmän tilaa ja ovat kustannustehokkaampia. Tiedon pakkaaminen on hyödyllisintä suuren mittakaavan järjestelmissä, kuten esimerkiksi virannoimaisten käyttämissä sormenjälkitietokannoissa.

Mallinteiden taltioinnin kolme oleellisinta menetelmää ovat paikallismuisti, verkkomuisti ja muistikortti.

3.4.1 Paikallismuisti

Paikallismuistissa mallinteet taltioidaan biometriseen laitteeseen. Menetelmä sopii käytettäväksi pienten käyttäjämäärien fyysisen sisäänpääsyn hallinnointiin. Paikallismuistin koko ja sen myötä mallinteiden määrä on riippuvainen kyseisen laitteen rakenteesta. Menetelmä takaa paremman suojan kuin osa muista menetelmistä, koska se ei ole altis verkkohäiriöille tai mahdollisille verkko–hyökkäyksille. Olettaen että itse laite on suojattu, tämän kaltainen ratkaisu on turvallinen eikä ole alttiina tunkeutujille, koska se ei siirrä tietoa verkon kautta.

Menetelmän yksi suurimmista heikkouksista on verkkomuistin hyötyjen täydellinen puute. Mallinteiden hallinnointi on vaikeaa, koska käyttäjien rekisteröinti tietokantaan täytyy suorittaa jokaiselle paikalliselle lukulaitteelle erikseen. Lisäksi tietokannan varmuuskopionti on huomattavasti vaikeampaa. Tiettyjen biometristen menetelmien kohdalla on kuitenkin mahdollista käyttää kannettavia lukulaitteita. Tämä tuo paikallismuistiin menetelmän kaipaamaa joustavuutta. Paikallismuistin käyttö on kuitenkin epäkäytännöllinen ratkaisu suuren mittakaavan järjestelmissä. [1, s. 39.]

3.4.2 Verkkomuisti

Verkkomuistissa mallinteet taltioidaan erilliseen tietokantaan, jossa lukulaitteiden tarvittava informaatio on saatavilla verkkoyhteyden kautta. Verkkomuistin käyttö on lähes välttämätön suuren mittakaavan järjestelmissä, kun järjestelmän on tarkoitus suorittaa one-to-many-tyypin hakuja, jolloin mahdollisesti järjestelmä käy läpi tuhansia tai jopa miljoonia rekisteritietoja. Verkkomuistin yksi hyvä puoli on mahdollisuus ylläpitää erillistä listaa sisäänkirjautumisista, mikä helpottaa mahdollisten luvattomien tunkeutujien tunnistamista. Tämän kaltaisen listan ylläpito voi kuitenkin hidastaa järjestelmän toimintaa, minkä vuoksi laitevalmistajat eivät välttämättä tarjoa kyseistä ominaisuutta kaikissa valmistamissaan laitteissa tai laitemalleissa. Verkkomuistin yksi tärkeimmistä eduista on se, että rekisteröityminen järjestelmään voidaan suorittaa missä tahansa sallitussa rekisteröintipisteessä, minkä jälkeen kaikki järjestelmään liitetyt lukulaitteet voivat verkon kautta suorittaa hakukyselyn verkossa olevasta tietokannasta. Verkkomuistin tietokanta on myös helppo varmuuskopioida mahdollisten häiriöiden tai laiterikkojen varalta. [1, s. 39.]

3.4.3 Muistikortti

Kiinteästi asennettujen mallinnemuistimenetelmien kohdalla tietokannan koko ei ole ongelma, jos tarvittava tilantarve on mitoitettu oikein. Sirukorttien ja muiden kannettavien muistilaitteiden kohdalla tulee käytettävän muistin koko valita järjestelmän käyttämän mallinteen koon pohjalta. Tyypillisessä älykortissa muistin koko on noin 8 K:sta 64 K:oon asti. Pääsääntöisesti älykortteihin sisällytetään muutakin informaatiota kuten esimerkiksi käyttäjätunnus/salasana.

Halvimpien älykorttien eli ns. muistikorttien muistin koko on vain 2 – 4 K. Kannettava muisti on ehkä parhain tapa ylläpitää yksilöllisyydensuojaa, koska henkilön biometristä mallinnetta ei ole taltioitu itse lukulaitteeseen tai verkossa sijaitsevaan tietokantaan. Suurin ero halpojen ja kalliiden muistikorttien välillä on se, että vain kalliimmissa korteissa mallinteet voidaan salakoodata ja näin suojata mahdollisilta väärinkäytöksiltä, jos kortti häviää.

Vaikka kannettavan muistikortin avulla voidaan mahdollistaa korkean tason turvallisuusaste, niin sen käyttö kuitenkin avaa joukon uusia ongelmia. Kortti voi esimerkiksi kadota tai vahingoittua, jolloin täytyy järjestää mahdollisuus kortin uusimiseksi, ja näin henkilön biometrinen mallinne on pakko luoda uudestaan, ellei aiemmin luoduista mallinteista säilytetä varmuuskopioita. Tosin varmuuskopioiden olemassa olo tekisi kannettavan muistinkortin käytön hyödyt lähes olemattomaksi. On myöskin mahdollista, että kortti varastetaan, jolloin väärinkäytön riski on olemassa.

On tärkeää että mallinne on taltioitu muistiin mahdollisimman turvatulla tavalla. Jos mallinnetta on mahdollista muokata tai manipuloida, niin se vaarantaa koko järjestelmän turvallisuuden. Tietosuoja on ehkä biometristen järjestelmien heikoin osa-alue, koska useimmiten kaikki mallinteet on taltioitu yhteen tietokantaan. Tietokantojen täytyy olla erittäin hyvin suojattu ja turvassa kaikilta niitä mahdollisesti uhkaavilta tekijöiltä. Tietosuojan tulee huomioida, käytetäänkö paikkallismuistia, verkkomuistia vai kannettavaa muistilaitetta mallinteiden taltioinnissa. Myös tulee huomioida, taltioidaanko mallinteet erilliseen tietokantaan vai monikäyttöiseen tietokantaan. Monikäyttöinen tietokanta sisältää lisätietoa käyttäjästä, kuten esimerkiksi nimien, puhelinnumeron, osoitteen ja henkilöturvatunnuksen. Identiteettivarkausten riski kasvaa, mitä enemmän informaatiota biometriseen mallinteeseen liitetään. [1, s. 40.]

3.4.4 Muistinhallintaongelmat

Muistinhallinta on tärkeä osa järjestelmästä, joka vaikuttaa biometrisen järjestelmän arkkitehtuuriin ja suunnitteluun. Suuren mittakaavan järjestelmän tulee olla toimiva ja kaikille yhteinen maailmanlaajuinen järjestelmä.

Suuren mittakaavan järjestelmien tulisi sisältää seuraavia asioita:

- yhteinen mallinne standardi
- riittävän suuri kapasiteetti oletetulle maksimi käyttäjämäärälle
- tietokantaan rekisteröityminen useammasta toimipisteestä
- toimiva ja monipuolinen tietokantarakenne (kyselyiden luominen ja manuaaliset haut tietokannasta)
- hajautettu haku ja täsmäysarkkitehtuuri tietojen käsittelyssä (tietojenkäsittelytehojen maksimoimiseksi)
- lujitettu tietoturva, vaikka biometriset järjestelmät sisältävät ominaisuuksia mallinteiden salakoodaamiseksi, niin tietoturvariskit on tunnettava ja otettava huomioon. Useimmiten biometristen järjestelmien heikoin kohta on mallinteiden ja tunnistustietojen siirtovaihe biometrisen lukulaitteen ja verkossa sijaitsevan tietokannan välillä.

3.5 Käyttäjäkoulutus

Käyttäjäkoulutus on tärkeää rekisteröitymisen ja onnistuneiden sisäänkirjautumisten parantamisen vuoksi. Koulutuksen tulisi sisältää tieto siitä, kuinka tunniste tulisi esittää lukulaitteelle ja ohjeistus siitä, kuinka lukulaitteen toimintakunto ylläpidetään korkeana. Esimerkiksi optisen sormenjälkilukulaitteen sensorin linssin tulee olla riittävän puhdas, jotta laite toimisi oikein. Käyttäjien tai huoltohenkilökunnan tulee siis säännöllisesti puhdistaa linssi ja käyttäjien sormensa, jotta saavutetaan hyväksyttävä tunnistus. Tietyissä sormenjälkienlukulaitteissa ei kyseisiä ongelmia ilmene, mutta sormen oikeaoppinen asettelu on kuitenkin yhtä tärkeää kyseisissä laitteissa. On myös tärkeää tuntea varajärjestelmät, jos laite ei toimi kuten sen pitäisi. Esimerkiksi jos pääovien biometrinen lukulaite ei toimi hätätilanteessa, niin mikä on vaihtoehtoinen suunnitelma?

Käyttäjäkoulutuksen tarkoitus on vähentää epäonnistuneiden kirjautumisten määrää ja parantaa oikeiden tunnistusten määrää. Näin kustannukset pysyvät alhaisina ja käyttäjätyytyväisyys korkealla.

4 BIOMETRISET TUNNISTUSMENETELMÄT

Tässä osiossa esitellään nykyiset ja joukko mahdollisia tulevaisuuden biometrisiä tunnistusmenetelmiä sekä käsitellään ongelmia esimerkkien ja kuvien avulla.

4.1 Sormenjälkitunnistus

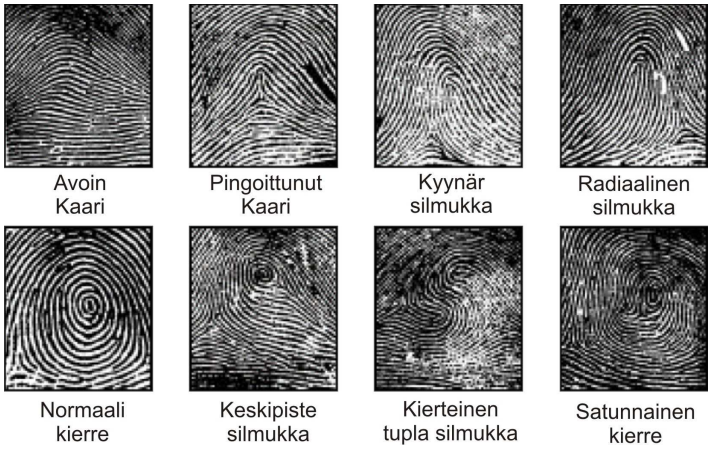
Sormenjäljet ovat vanhin ja yleisesti hyväksytty biometrinen tuntomerkki. Nykyisistä biometrisistä menetelmistä sormenjälkitunnistus on yksi kaikkein luotettavimmista, ja sen vuoksi menetelmää käytetäänkin mm. rikospaikka–tutkimuksissa.

Latentit painojäljet, jotka jäävät kosketettuamme jotain pintaa, koostuvat lukuisten aineiden jäännöksistä, jotka pääsääntöisesti sisältävät orgaanisia aineita kuten aminohappoja ja elottomia aineita kuten suola ja veri. Jäännökset voivat myös sisältää jonkin muun aineen jäänteitä, jota olemme saattaneet koskettaa lähiaikoina. Sormenjälki viittaa harjanteiden ja laaksojen muodostamaan kuvioon sormenpäässä. Harjanteissa on poikkeavuuksia, joiden sijaintia ja orientoitumisinformaatiota sormenpään alueella käytetään sormenjälkien täsmäyksessä. Sormenjäljet ovat yksilöllisiä ja erilaisia saman henkilön muiden sormien sormenjälkien kanssa. Identtisten kaksosten, joiden DNA on hyvin samankaltainen, ei uskota omaavan identtisiä sormenjälkiä. [13.]

Perinteisesti sormenjälkiä on taltioitu käyttäen mustetta ja paperia. Elektroniikan ja algoritmien kehitys on mahdollistanut kompaktit sensorit, jotka taltioivat digitaalisessa muodossa kuvan sormenjäljestä. Nykyiset sensorit ovat niin pieniä, että niitä voidaan esimerkiksi käyttää osana nykyisiä tietokoneen oheislaitteita kuten hiiri tai näppäimistö. Tämä on johtanut mm. siihen, että automaattisten sormenjälkientunnistusjärjestelmien käyttö on lisääntynyt huomattavasti niin siviili- kuin viranomaissovelluksissa.

Sormenjäljen yksilöllisyys määritellään sormenpään harjanteiden muodostamien topografisten pinnanmuotojen ja tiettyjen harjupoikkeavuuksien eli yksityiskohta–pisteiden avulla. Sormenjäljen kategoria tyypillisesti määritellään sen yleisen muodon perusteella (silmukka, kaari, kierre), ja yksityiskohta pisteiden avulla

määritellään kahden sormenjäljen yhtäläisyydet. Automaattisissa sormenjälkien tunnistusjärjestelmissä sormenjälkikyselyissä hyödynnetään sormenjälkien luokittelua (kuva 5) haun rajaamiseksi pienemmälle alueelle, jotta tunnistukseen kuluva aika ja käytetyt resurssit saadaan minimoitua. Sormenjälkiharjanteiden muodostamaa kuviota harvoin käytetään varsinaisessa sormenjälkien täsmäyksessä. [14, s. 8.]



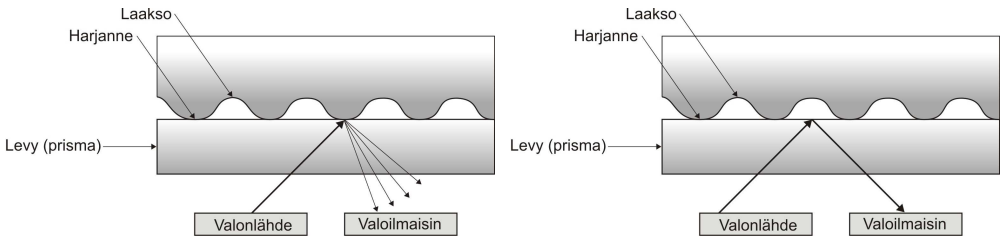
Kuva 5. Erityyppisiä sormenjälkiä*. Sormenjäljen yleisen muodon avulla voidaan rajata suoritettava haku tietyntyyppisiin sormenjälkiin. Kaaren muotoisissa sormenjäljissä harjanteet virtaavat toiselta puolelta kuvaa ja päättyvät kuvan vastakkaiseen laitaan. Kierteen muotoisissa sormenjäljet ovat yleensä pyöreän muotoisia. Silmukan muotoisissa sormenjäljissä harjanteet virtaavat jommaltakummalta puolta kuvaa, kaartuvat ja päättyvät samalle puolelle kuvaa kuin mistä ne saapuivat. [15.]*

4.1.1 Sormenjälkisensorityypit

Yhden sormen latenttien sormenjälkien lukijalaitteiden sensorityypit ovat

- optinen sensori
- painesensori
- terminen sensori
- kapasitiivinen sensori
- ultraäänisensori.

Optisissa sensorilukumenetelmissä tyypillisesti sormi asetetaan lasilevylle, jolla sitä valaistaan sopivalla tavalla. Linssi kerää prisman avulla heijastuneen valon CMOS- tai CCD-kennolle (kuva 6), josta tieto muunnetaan digitaaliseen muotoon harmaasävyiksi. [5, s. 11.]

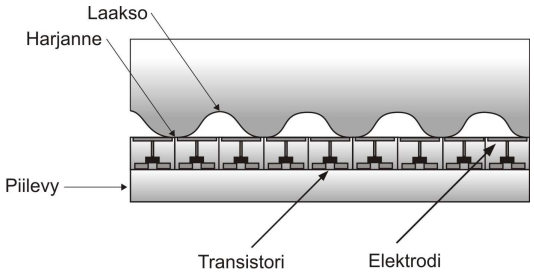


Kuva 6. Optisen sensorin toimintaperiaate. *Ledien avulla valaistaan sormen pintaa, josta harjanteiden ja laaksojen heijastama valo kulkee prisman kautta linssille, josta se fokusoidaan CMOS- tai CCD-kennolle.*

Painesensoreihin perustuvissa järjestelmissä matriisiin asetetut piezosähköiset kiteet mittaavat harjanteiden ja laaksojen muodostamia paine-eroja, kun sormi painetaan sensorilevyä vasten. [16, s. 7.]

Termisiin sensoreihin perustuvissa järjestelmissä käytetään pyrosähköisistä anturielementeistä koostuvia matriiseja, jotka mittaavat harjujen kontakti kohtien ja laaksoissa olevan ilman lämpötilaeroja. Sensorit perustuvat pyrosähköisen materiaalin kykyyn synnyttää tietty jännite lämpötilaerosta. [16, s. 8.]

Kapasitiivisiin sensoreihin perustuvat järjestelmät sisältävät tyypillisesti metallilevyistä koostuvia matriiseja, jotka mittaavat mikrovolttien suuruisia potentiaalieroja harjujen ja laaksojen välillä (kuva 7). Näin saatu kapatanssikuvio voidaan digitoida myöhempää käyttöä varten. [16, s. 6.]



Kuva 7. Periaatekuva kapasitiivisesta sensorista. *Elektrodit muodostavat pikselimatriisin, joka mittaa ihon ja laaksoissa olevan ilman välistä kapasitanssieroa.*

Ultraäänisensoreihin perustuvissa järjestelmissä käytetään menetelmää, joka kolmen eri aallonpituisen ultraäänisen pulssin avulla havaitsee ja mittaa

sormenjälkien harjut yksityiskohtaisesti. Tämä on tällä hetkellä yksi kalleimmista sensorityypeistä. Lika tai muste ei haittaa jäljen taltiointia lainkaan. [17; 5, s. 13.]

4.1.2 Mallinteen taltiointi

Yksityiskohtien ja muiden piirteiden taltioimiseksi järjestelmä käy läpi tyypillisesti useavaiheisen prosessin. Ensin luetaan näyte, minkä jälkeen sormenjälki erotellaan lohkoon taustasta. Tämä vaihe sisältää reunojen tunnistamista ja harjujen tunnistamiseksi kaksiuloitteisten fourier-muunnosten soveltamista vaaka- ja pystymuotoisten reunojen tunnistamiseksi sekä gabor filtereiden käyttöä taajuuden ja suunnan määrittämiseksi.

Tämän jälkeen sormenjäljen harjujen muodostamia viivoja muokataan niin, että ne ovat vain 1 pikselin levyisiä, minkä jälkeen tieto muutetaan binääriseksi. Syy miksi sormenjälkiä alun perin taltioitiin 500 ppi ja 8-bittisenä harmaasävyisenä oli se, että saatiin taltioitua tarpeeksi informaatiota harjujen sijainnista jäljen analysointia varten ja että kuva olisi tarpeeksi tarkka manuaalista tarkastelua varten. [2, s. 4.]

Ohennetusta binäärikuvasta voidaan tämän jälkeen etsiä yksityiskohtia käyttäen gabor filtereitä kuvan eri kohdissa. Laskelmat näyttävät harjanteiden sijainnin, virtaussuunnan, harjanteiden päätepisteet ja suunnanvaihdokset. Eri valmistajien algoritmien eroavaisuudet ovat lähinnä siinä mitä tietoa he käyttävät x-, y- ja theta-arvoissa. Tyypillisesti ne sisältävät joukon seuraavista sormenjäljen ominaisuuksista: kokonaiskuva, lähtökohta, deltasijainti, kuvan kokonaislaatu, sekä osan seuraavista yksityiskohtien ominaisuuksista: yksityiskohdan laatu tai varmuus, lähimmät naapurit, harjujen haaraumat lähellä naapureita, ympyräkehän neljännes, jossa yksityiskohta sijaitsee, harjun pituus ja kaarevuus, jossa yksityiskohta on.

Kun piirteet on taltioitu, tietue vie noin 1000 tavua. Tämän jälkeen tietuetta verrataan tietopankissa oleviin jotta voidaan laskea vastaavuustulos. Vastaavuustulokselle asetetaan raja, jonka mukaan vastaavuudet ja mahdolliset vastaavuudet erotellaan ja järjestellään. Jos kyseessä on väitetyn henkilöllisyyden varmennus, niin kyselymallinnetta verrataan vain yhden tai mahdollisesti muutaman eri tietueen kanssa. Jos kyseessä on tapaus, jossa

henkilö ei ole rekisteröitynyt aiemmin tai ainakin väittää niin, suoritetaan ns. kylmähaku. Tällaisessa tapauksessa hakua voidaan rajata erilaisilla ylimääräisillä tiedoilla kuten henkilön sukupuoli ja asettamalla jokin ikäalue, jolta haku suoritetaan. Hakuja voidaan myös rajata sormenjäljestä saatavilla tiedoilla kuten sormenjäljen yleisen muodon perusteella. [1, s. 63.]

4.1.3 Vankkuus, oletettu tarkkuus

Perinteisesti sormenjälkiyhteisö kuvasi AFIS-järjestelmien suorituskykyä käsitteiden tarkkuus, luotettavuus ja valintatarkkuus avulla.

Tarkkuus-käsite kuvasi sitä todennäköisyyttä, ettei järjestelmä tee vääriä tunnistuksia (toisin sanoen että AFIS järjestelmä ei yhdistä sormenjälkeä väärään tietueeseen tietokannassa). Luotettavuus-käsite kuvasi sitä todennäköisyyttä, jolla AFIS-järjestelmä löytää ja tunnistaa oikean sormenjäljen tietokannasta. Valintatarkkuus käsite kuvasi vaihtoehtoisten tunnistukselle asetetun raja-arvon ylittävien osumien määrää hakua suorittaessa.

Nämä IAI NIST AFIS-määritelmän standardissa olevat käsitteet ovat kuitenkin vaihtumassa uusiin käsitteisiin, joita voidaan käyttää laajemmalti biometriikan allalla. Uudet korvaavat käsitteet ovat epäonnistuneiden kirjautumisten määrä (FER), väärien hylkäysten määrä (FRR), väärien hyväksyntöjen määrä (FMR) ja epäonnistuneiden taltiointien määrä (FTAR). [1, s. 64.]

Useamman sormen AFIS-järjestelmien suorituskyvyssä on suuria eroja verrattuna yhden sormen järjestelmiin, joita käytetään mm. kulunvalvontaan. Viranomaisten kymmenen sormen, rullattujen ja latenttien sormenjälkikuvioiden kohdalla epäonnistunut taltiointi yksittäisessä sormessa voidaan hyväksyä. Näissä kymmensormijärjestelmissä epäonnistuneiden tunnistusten määrä (FTMR) ja väärien hyväksyntöjen määrä on erittäin lähellä nollaa. Uusimmissa siviilikäyttöön suunnatuissa sovelluksissa, joissa käytetään vain sormenpään muodostamaa tasaista kuviota, voi virheiden määrä kasvaa varsin suureksi. [1, s. 64.]

Yhden sormen järjestelmissä, joita esimerkiksi käytetään kirjautuessa sisään tietokoneen käyttöjärjestelmään, on virheiden määrä varsin suuri, koska

käyttäjämäärät saattavat olla varsin suuria, kyseisen lukijan käyttö harvinaista, lukijalaitteen sensori unohdetaan puhdistaa, ja lukuisten muiden syiden vuoksi. Tosin on tärkeää huomioida, että vaikka väärien tunnistusten prosentuaalinen osa tuntuu varsin suurelta, esimerkiksi 5 %, niin tämä ei ole niin suuri uhka kuin aluksi voisi luulla. Oletetaan että 100 henkilöä ohittaa paikan muut turvamekanismit kuten lukitut ovet, avainkortti/polettitarkastukset ja tietää käyttäjänimet ja salasanat. Tämä 5 % tarkoittaa kuitenkin sitä, että vain 5 näistä 100:sta henkilöstä tunnistetaan väärin perustein hyväksytyksi käyttäjäksi. Lukema on niin pieni, että on järkevämpää keskittyä siihen ongelmaan, kuinka näiden henkilöiden sisäänpääsy pysäytetään jo etuovelle.

4.1.4 Manuaalinen sormenjälkien täsmäys

NIST:n oikeusindentifikaatiostandardin määritelmä sormenjäljen yksityiskohdalle tai yksityiskohdille on seuraavanlainen:

”Harjanteiden tuntomerkkejä käytetään jäljen yksilöintiin. Yksityiskohdat ilmenevät paikoissa, jossa yksittäisessä harjanteessa ilmenee poikkeama yhtäjaksoisessa viivassa. Poikkeama voi ilmetä esim. viivan loppumisena, haarautumisena tai uuden erillisen aallon alkuna ja/tai pikaisena loppuna”. [8.]

Nykyisin käytämme näistä tapahtumista termejä päätepiste, haarautuma ja piste.

Sormenjälkitutkijat kuvaavat sormenjälkien yksityiskohtia kolmella tasolla:

- Taso 1: Ns. Galtonin taso, sormenjäljen yleinen ulkonäkö. Kuvio ja yleinen harjujen muoto, luokitus, harjujen määrä, keskeiset alueet ja asento.
- Taso 2: Harjanteiden yksityiskohdat ja niiden muodostaman jäljen muoto: suurten muutosten sijainti yksittäisissä harjuissa kuten päätepisteet, haarautumat, saaret, pisteet, niiden yhdistelmät ja niiden suhteet toisiinsa nähden. Näitä tapahtumia tai yksityiskohtia voidaan kuvailla käyttämällä xyz-koordinaatistoa, jossa x ja y kertovat sijainnin ja käyttämällä kulmaa esimerkiksi theta tai θ harjujen virran suhteessa x akseliin.
- Taso 3: Yksittäisten harjujen yksityiskohdat kuten harjanteiden mittasuhteet. Reunojen muoto ja leveys (riippuvainen musteprosessista ja jäljen tuottamiseen käytetystä voimasta) sekä hikihuokosten sijainnista ja niiden suhteesta toisiinsa.

Jos kaksi sormenjälkeä sisältävät saman informaation tasolla 1 ja tason 2 yksityiskohdat täsmäävät toisiinsa ilman selittämättömiä poikkeavuuksia, niin tutkija voi merkata ja numeroida ne yksityiskohdat jotka täsmäävät. Näin tutkijat voivat todentaa, että kaksi sormenjälkeä vastaavat toisiaan ja näin yhdistää ne johonkin tiettyyn henkilöön. Tämän kaltaista tietoa latenttien sormenjälkien tutkijat joutuvat esittämään oikeudelle, kun he todistavat että kaksi sormenjälkeä kuuluvat jollekkin tietylle henkilölle. [1, s. 49.]

On tärkeää huomata, että kun sormenjälkiä taltioidaan, otetut painojäljet eroavat hieman. Useimmat kahden rullatun ja kahden latentin sormenjäljen erot ovat hyvin pieniä, mutta sormen liika tai ali mustaaminen voi johtaa esimerkiksi harjujen päätepisteiden ilmenemiseen haarautumana tai haarautumien muuttumiseen päätepisteiksi, myös lika ja öljy voi pilata yhtenäisen tasalaatuisen jäljenoton. Jäljenoton yhteydessä käytetty voima voi vaikuttaa yksityiskohtien suhteellisen x- ja y- informaation vääristymiseen painojäljessä.

Sormenjälkiä taltioidessa lukuisat eri syyt aiheuttavat eroja yksittäisissä otoksissa. Syitä voivat olla esimerkiksi:

- jälki saattaa olla asemoitu eri kohtaan taltiointivaiheessa
- kuvattu sormi saattaa olla eri asennossa
- jäljenotossa on käytetty voimaa eri lailla, mikä voi johtaa kaikkien piirteiden mittasuhteiden ja paikanmäärityksen skaalausvirheisiin
- jokin yksityiskohta ei taltioidu oikein tai jää puuttumaan kokonaan
- jäljen epäyhdenmukaisuus huonon kontaktin takia harjujen ja taltiointipinnan välillä aiheutuu esim. kosteudesta, liasta, vammasta tai sairaudesta.

4.1.5 Sormenjälkikortit

Ajan myötä huomattiin tarve standardisoida sormenjälkitiedonkeruukaavakkeet. Korttien täytyi mahtua normaaliin kortistokaappiin ja niissä tuli näkyä selkeästi sormenjälkien kuvat niin, että tiedetään mistä sormesta on kyse. FBI kehitti alun perin nykyisin viranomaisten käyttämän yhteisen standardin, joka sisälsi mm. kortin koon, käytettävän musteen tyypin, sekä tekstikenttien ja sormenjälkien sijainnit.

FBI:n ja poliisien käyttämissä sormenjälkikorteissa on 14 sormenjälkikenttää, joista 10 on varattu jokaiselle 10:lle yksittäiselle sormelle ”rullatussa” formaatissa, 2 kenttää on tarkoitettu 4 sormen yhtäaikaselle latentille tai ns. huitaisuformaatille, joka otetaan molemmista käsistä, ja 2 kenttää on tarkoitettu latentille sormenjälkikuviolle molempien käsien peukalosta.

Kahden ylimmäisen rivin sormenjälkikentät otetaan mustetta käyttämällä ja rullaamalla jokainen sormi kynnen vasemmasta laidasta kynnen oikeaan laitaan. Kynnestä kynteen menetelmällä varmistetaan, että kahdet eri aikaan otetut sormenjäljet limittäytyvät riittävästi, jotta voidaan tehdä luotettava tunnistus ja että koko sormenjäljen pinta on saatavilla sormenjälkitutkimuksissa.

Latentit jäljet sormenjälkikortin alimmaisella rivillä taltiodaan, jotta voidaan varmistua, että rullatut sormenjäljet ovat oikeassa järjestyksessä. Ne myös sisältävät selkeämmän jäljen sormenjäljen keskusosasta, koska rullattujen sormenjälkikuvien laatu kärsii hieman vähäisestä mutta silti huomattavissa olevasta paineesta ja rullaavasta liikkeestä aiheutuvasta vääristymästä. [15.] Kuva 8 on sormenjälkikortista.

Kuva 8. Oikean käden peukalon tai sormen 1 *(kuten tutkijat numeroivat sen)* ***sormenjälki.*** *Kuvaan on merkitty kaksi yksityiskohtapistettä: harjanteen päätekohta ja harjanteen haarautuma. Yksityiskohtapisteitä käytetään sormenjälkien täsmäyksessä.*

4.1.6 Kämmenjälkitunnistus

Arviolta noin 30 prosenttia latenteista jäljistä, joita kerätään rikospaikoilta kuuluu johonkin muuhun osaan kämmentä kuin sormenpäähän, minkä vuoksi on kiinnostuttu myös koko kämmenen jäljen taltioinnista rikollisilta. Ei ole aina selvää, onko latentti jälki syntynyt sormenpään vai kämmenen kosketuksesta. Tämän vuoksi olisi tärkeää kerätä myös koko kämmenen jälki.

4.1.7 Sormenjälkitunnistussovelluksia

Tarve tarkistaa ihmisen taustatiedot on kasvanut. Lapsien hyväksikäyttö- ja kidnappaustapaukset ovat herättäneet mm. kiinnostusta mahdollisuuteen suorittaa taustatietokyselyitä sellaisista ihmisistä, jotka työskentelisivät lasten ja vanhusten kanssa. Toisaalta on kuitenkin kohtuutonta tutkia jokaisen opettajaksi hakevan rikosrekisteriä. Tämän vuoksi voitaisiin kehittää valtiollinen järjestelmä, josta voidaan suorittaa hakuja lähes reaaliajassa. Ensimmäisiä tämän kaltaisia USA:n valtion sovelluksia oli automatisoitu sosiaaliavustus, joka oli aikoinaan uusi sovellus AFIS-tekniikalle. [1, s. 60.]

LA-AFIRM oli osa yritystä kontrolloida sosiaaliturvan kustannuksia, jotta ihmiset eivät voisi hyödyntää sosiaaliturvaa käyttäen useita eri nimiä. Uutta järjestelmää pidettiin menestyksenä. Sen seurauksena sosiaaliturvaa haettiin jopa 20 % vähemmän kuin aiemmin. Mitään varmaa tietoa ei ole siitä, että oliko kavallusten määrä niin suuri vai pelottiko ihmisiä pois tieto siitä että heidän sormenjälkensä taltioidaan. Järjestelmä koostui Printrak AFIS-järjestelmästä ja yhden sormen latentin sormenjäljen lukijasta jokaisessa sosiaalivirastossa. Hakijoiden tuli todistaa henkilöllisyytensä sormenjäljen avulla joka kuukausi lunastaessaan shekkinsä. [1, s. 61.]

INS esitteli IDENT-järjestelmänsä 90-luvun puolivälissä. IDENT käytti ANSI/NIST-standardia tyypin 4 tietueille, jotka pakattiin suhteessa 15:1, mutta taltioi vain latentteja sormenjälkikuvia. Skannereita otettiin käyttöön rajoilla ja järjestelmän idea perustui LA-AFIRM-ratkaisumalliin. Näin voitiin tutkia, oliko henkilö pidätetty aiemmin tai etsittiinkö häntä jostain rikoksesta kuten esim. maahantunkeutumisyrityksestä, kun hänet on jo aiemmin karkotettu. [1, s. 61]

Pidätetyiltä ihmisiltä pääsääntöisesti taltioitiin kaksi etusormenjälkikuvaa ja kasvokuva. Nämä lähetettiin sähköisesti INS:n päämajaan, josta tuli vastaus muutamassa minuutissa raja-asemalle. Vastaus pääsääntöisesti oli joko positiivinen tai negatiivinen ns. uusi laiton rajanylittäjä. Positiivisessa tapauksessa vastaus sisälsi tietoja aiemmasta kohtaamisesta, kasvokuvan, aikaisemmat sormenjälkikuvat. Ottaen huomioon vain kahden sormen käytön sormenjälkiä otettaessa, epäsuopeat olosuhteet (likaiset sormet, henkilön vastustus), suuren työmäärän (jopa yli 1800 henkilöä päivä ja tämä vain yhdellä asemalla), IDENT–järjestelmä ei ollut läheskään yhtä tarkka kuin kymmenen sormen järjestelmä. Järjestelmä oli kuitenkin merkittävä virstanpylväs sormenjälkien käytöstä. [1, s. 61.]

Nykyisin suurin osa yrityksistä käyttää yhden sormen tunnistusta järjestelmissään ja laitevalmistajat käyttävät hyvin samankaltaisia täsmäysalgoritmejä tuotteissaan. Tämän kaltaiset järjestelmät on tyypillisesti suunniteltu muutaman sadan ihmisen käyttöön. Pääsääntöisesti laitteet perustuvat joko yksityiskohtien täsmäytykseen tai kuvavertailumenetelmiin. Täsmäysmenetelmät hyödyntävät joko harjujen muodostaman kuvan vertailua koordinaatistossa tai taajusalueiden yhtäläisyyksiä käyttäen kaksiuloitteisia fouriermuunnoksia.

4.2 Kämmentunnistus

Toiseksi käytetyin biometrinen tunniste on käsi itse. Tämä biometrinen menetelmä hyödyntää vähemmän yksityiskohtaista informaatiota kuin jopa tason 1 sormenjälkitunnistus. Menetelmässä käytetään tyypillisesti binääristä (musta-valko) kuvaa, josta mitataan sellaisia asioita kuin esimerkiksi sormen pituus.

Kämmengeometrialukijat kuten esimerkiksi RSI:n valmistamat mittaavat kämmenen pintapuolen ja neljän sormen pituutta, leveyttä ja paksuutta. Nämä piirteet ovat tarpeeksi tunnusomaisia, jotta voidaan hyväksyä ja tunnistaa esitetty henkilöllisyys. Ne eivät ole kuitenkaan tarpeeksi tunnusomaisia, jotta voitaisiin suorittaa henkilöllisyyshakuja. Kämmengeometriaskannerit käyttävät 32000 pixelin CCD-digitaalikameraa tallentaakseen kämmenen kolmiuloitteisen muodon kämmenen muotojen muodostamien varjokuvien ja niiden ääriviivojen avulla. Kuvassa 9 on tyypillinen kämmengeometrialukija. [1, s. 65.]

Kuva 9. Tyypillinen kämmengeometrialukija näppäimistöllä. *Kuvassa oleva IR security technologies yhtiön handkey II kämmengeometrialukija on tarkoitettu käytettäväksi ovien kulunvalvonta- ja pääsynhallintasovelluksissa. Se on tyypillinen kämmengeometrialukija, jossa on viisi tappia, jotka auttavat käyttäjää asettamaan kämmenen lukijaan oikein. Kyseisessä lukijalaitteessa on myös näppäinlukko, jossa voidaan käyttää henkilökohtaista tai esim. jokaisen työntekijän tuntemaa yhteistä tunnuslukua.*

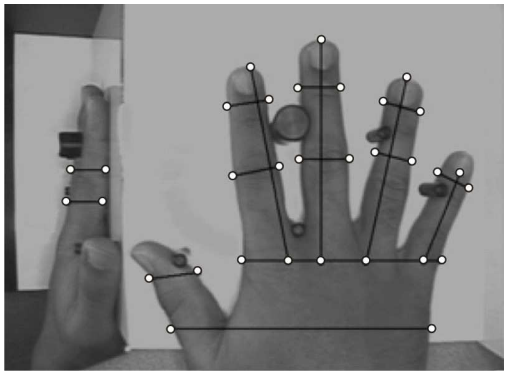
RSI-kuvantaltiointijärjestelmä koostuu valonlähteestä, kamerasta, yhdestä peilistä ja tasaisesta alustasta, jossa on 5 tappia. Käyttäjän tulee asettaa kämmen alaspäin kääntyneenä alustalle. 5 tappia toimii kontrollipisteinä käyttäjän oikean käden asianmukaiselle asemoinnille. Laite on kytketty PC:hen, jossa on ohjelma, joka osaa tulkita reaaliaikaista kuvalähetystä kämmenen yläpuolelta ja sivulta. Käyttöliittymä auttaa kämmenen kuvan taltioinnissa. Yksinäinen peili heijastaa kämmenen sivuprofiilin kameraan. RSI:n laitteet taltioivat kaksi kuvaa kädestä. [1, s. 65.]

Käyttäjä asettaa kätensä erittäin heijastavalle pinnalle. Kuvan taltioinnin jälkeen kämmenen sijainti ja koko määritellään segmentoimalla kämmenen himmentämä tumma alue heijastuneesta valosta. Toinen kuva saadaan käyttämällä samaa kameraa ja peliä. Tämän kuvan tarkoitus on mitata kämmenen paksuutta. Käyttäen vain kämmenen binaarikuvaa ja heijastettua taustakuvaa järjestelmä ei pysty taltioimaan arpia, harjuja, eikä edes mahdollisia tatuointeja. Kuitenkin sormukset, laastarit ja käsineet voivat muuttaa kuvaa ja lopullisia mittauksia niin paljon, että syntyy virheellinen hylkäys. [1, s. 65; 6, s. 58.]

Kuva 9. CCD-kameran taltioima kuva kämmenestä ylhäältä ja sivulta päin

Järjestelmä käyttää varjokuvia laskeakseen pituuksia, leveyksiä ja paksuuksia kämmenen alueelta ja sormista poislukien peukalon. Kuvasta mitataan yli 90 arvoa, joiden avulla kämmenen ja sormien ominaispiirteet taltioidaan lopuksi noin 9 tavun mallipohjaksi (kuva 10). Täsmäys sisältää geometrisen eron laskemista kysytylle henkilölle kuuluvan mallinteen ja esitetystä näytteestä luodun mallinteen välillä. Tuloksen tulee myös läpäistä sille asetettu raja-arvotesti. [1, s. 66.]

Kirjautumisvaihe kestää noin 30 sekuntia, jonka aikana käyttäjä asettaa kätensä lukijaan kolme kertaa. Laitteen sisäinen prosessori ja ohjelma luo noin 9 tavun mallipohjan näiden kolmen mittauksen keskiarvosta. Mielenkiintoisesti meidän kätemme ovat useimmiten peilikuvia toisistaan, joten monet ihmiset voivat kirjautua oikealla kädellään mutta käyttää vasenta kämmentään ylösalaisin käännettynä verifiointiin. [1, s. 66.]



Kuva 10. Joukko suoritettavia kämmengeometriamittauksia tyypillisessä kämmentunnistusjärjestelmässä. *Mittauksien avulla lasketaan mm. sormien pituutta ja leveyttä ja kämmenen paksuutta [9].*

Biomet Partnersin tekniikka on samankaltainen kuin RSI:n, mutta se taltioi muodon ja ominaisuudet etu- ja keskisormesta ihan kummasta kädestä tahansa, eikä se taltioi lainkaan koko kämmenen aluetta. Tiedot taltioidaan 14 – 20 tavun mallipohjaan, joka sallii henkilöllisyyshakuja pienissä väestömäärissä samoin kuin myös henkilöllisyyden verifioinnin. Tässä järjestelmässä on kaksi tappia, jotka erottavat etusormen ja keskisormen niin, että järjestelmä voi suorittaa tarvittavat mittaukset. Sivuprofiilikuvaa ei oteta, koska sormien paksuutta ei mitata.

4.2.1 Kämmentunnistussovelluksia

Kämmengeometriatunnistus mahdollistaa tarkkuudeltaan ja käyttö–mukavuudeltaan hyvien ja lujitettujen turvajärjestelmien käytön useissa eri tarkoituksissa kuten

- pääsynhallinnassa
- kulunvalvonnassa
- käytönvalvonnassa.

Monet ydinvoimalat käyttävät pääsynhallintaskannereita henkilöiden verifiointiin valvotuilla alueilla. Tämän kaltaisissa käyttötarkoituksissa, joissa turvatoimet ovat erittäin tarkkoja, raja-arvot ovat erittäin tiukat verrattuna esimerkiksi kulunvalvonta järjestelmiin.

Yritykset voivat käyttää lukulaitteita verifioidakseen henkilön ja tämän työajan leimaukset. Tämä on kustannustehokas tapa eliminoida niin sanottu ”kaveri leimaus”. Tämän kaltaisissa järjestelmissä raja-arvo useimmiten on keskitasoa, koska pahimmassa tapauksessa väärinleimaukset voidaan korjata jälkikäteen.

Käytönvalvontasovelluksista voidaan mainita esimerkiksi Georgian yliopisto, missä käytetään kämmengeometriatunnistusta ruokalahuijauksien vähentämiseksi. Tällä on estetty oppilaiden välistä lounaskorttien lainausta toisilleen.

Yksi suurimmista kämmengeometrian tunnistusjärjestelmistä on Disney World, Orlando, Floridassa. Järjestelmä asennettiin koska havaittiin väärinkäyttöä

kausikorttien käytössä. Näitä kausikortteja käyttivät väärin esimerkiksi paikalliset ihmiset, jotka lainasivat niitä ystävilleen ja sukulaisilleen näin säästääkseen useamman kausikortin oston hinnan. Ongelma laajeni entisestään, kun turistioppaat alkoivat käyttää näitä vanhoja pahvisia kausikortteja kierroksillaan kaupitellen niitä asiakkailleen päiväksi perien itse päivittäiset maksut. [1, s. 68.]

Oli haasteellista löytää sellainen biometrinen tunniste, jota voitaisiin käyttää nopeasti, ilman sen suurempaa koulutusta ja ennaltakirjautumista. Vanhemmat saattavat ostaa liput koko perheelle, eikä olisi ollut käytännöllistä vaatia, että kaikkien, joille liput ostetaan, tulisi olla paikalla ostosta tehdessä. Disneyn täytyi myös kamppailla sen tosiasian kanssa, että kaikki heidän asiakkaansa eivät välttämättä osaa lukea englanninkielisiä ohjetauluja. [1, s. 68.]

Disney käyttää nykyisin BioMet Partnersin kahden sormen geometriajärjestelmää. Ensimmäinen kerta koostuu järjestelmään kirjautumissessiosta. Jos joukko kortteja myydään perheelle, niin nämä kortit ovat ristiinlinkattuja sisäänkirjautumistietokoneessa siten, että perheenjäsenet voivat käyttää toistensa kortteja ensimmäisen kerran jälkeen. Laitteen käyttötapahtuma kestää keskimäärin noin 11 sekuntia siitä hetkestä, kun kortin asettaa laitteeseen. Järjestelmää on hienosäädetty, käyttömukavuutta paranneltu ja laitteen tarkkuutta hienosäädetty niin, että pitkällä aikavälilläkin olisi mahdollisimman pieni väärien hylkäysten prosentti järjestelmän ollessa kuitenkin mahdollisimman tarkka. [1, s. 68.]

4.2.2 Uhkat ja heikkoudet

Ilmiselvä heikkous on, että jokainen voi ostaa halvan skannerin ja kokeilla kunnes löytää käden, joka on ”tarpeeksi lähellä” ollakseen laitteen mielestä vastaava toisen henkilön mallinteen kanssa. Kyseinen henkilö voisi näin esiintyä jonakin toisena ihmisenä esimerkiksi leimaten kaverinsa töihin, päästä alueille joille hänellä ei olisi muuten pääsyä tai jopa ylittää rajan väärän henkilöllisyyden turvin. Tietysti eri käyttöön olevilla laitteilla on oma tarkkuutensa ja täsmäyksen raja-arvoasetukset vaihtelevat laitteissa, mutta tämä vaara on kuitenkin olemassa. Kuten jokaisen biometrisen tunnistusjärjestelmän kohdalla, raja-arvojen säätäminen käyttökohteen, käyttäjämäärän ja turvaluokituksen mukaisesti on tärkeää.

4.3 Kasvotunnistus

Automaattinen kasvotunnistus on monimutkainen ja kiehtova ohjelmistosaavutus. Kysymys kuuluu kuitenkin: ”Pystyykö kone tunnistamaan kasvot vähintään yhtä tarkasti kuin ihminen itse?” Ongelma juontaa varhaisiin konenäkötutkimuksiin vuodelta 1970. Ongelma yhä kiehtoo ja viehättää tutkijoita. Tiedämme että ihmiset näyttävät erillaisilta ja ihmisinä meillä on kyky erottaa satoja kasvoja: perheenjäseniä, sukulaisia, ystäviä, työkavereita, julkisuuden henkilöitä jne. Ihminen pystyy tunnistamaan kasvot ilman sen suurempia ponnisteluita, vaikka ihmiset näyttävätkin erilaisilta ja heillä on lukemattomia erityispiirteitä. Toisin sanoen mitä piirteitä tietokoneohjelman tulisi käyttää tunnistaakseen tai erottaakseen henkilöt toisistaan pelkästään konenäön avulla?

Vaikka aihetta tutkitaan erittäin aktiivisesti, niin ei ole vielä päädytty mihinkään yhteisymmärrykseen siitä, mikä olisi kaikkein visuaalisesti merkittävin piirre, jolla erotamme yksilöt toisistaan ulkonäön avulla. Useita tietokoneohjelmia ja menetelmiä on tutkittu ja kokeiltu, mutta kaikki menetelmät yrittävät verrata kasvojen oleellisia peruspiirteitä niin, että vertauskuva olisi riippumaton sijainnista, asennosta, kasvonilmeestä, kasvojen karvoituksesta tai silmälaseista, mutta kuitenkin herkkä ydineroavaisuuksille, jotka muodostavat yksilöllisen identiteetin.

Nykyiset kasvotunnistusmenetelmät ovat hyötyneet niin konenäkö- ja tekoälytutkimusten, kuin kuvankäsittely- ja kognitiivisten tieteiden tutkimusten saavutuksista. Vaikka muita biometrisiä menetelmiä pidetään luotettavampina ja yksilöllisempinä tunnistuksen metodeina, niin kasvotunnistus on silti suosittu menetelmä. Vaikka menetelmä on kiistanalainen, niin kyseessä on kuitenkin yksi passiivisimmista ja ei-tunkeilevista biometrisen tunnistamisen menetelmistä. Nykyisin paljon käytettyjen halpojen digitaalikameroiden myötä ja televisiosta näkyvien poliisisarjojen myötä mahdollisten käyttökohteiden tuntemus on tehnyt menetelmästä tutun monille ihmisille.

4.3.1 Kasvotunnistussovelluksia

Pääasiallisesti kasvotunnistusjärjestelmät ovat joko tunnistus- ja varmennussovelluksia tai tarkkailu- ja valvontasovelluksia. Tunnistus- ja varmennusjärjestelmät tarkistavat käyttäjän henkilöllisyyden hänen pyrkiessä joko tietokoneelle tai jollekin alueelle. Tarkkailu- ja valvontasovellukset ovat ehkä osa-alueista kiinnostavin, haastavin, mutta myös kiistellyin. Valvontasovelluksilla voidaan skannata kasvoja julkisilla paikoilla tai vaikka tietyillä tarkastuspisteillä ja näin verrata kasvoja esimerkiksi etsittyjen rikollisten tai epäiltyjen listalla oleviin. Tekniikkaa voitaisiin käyttää myös huijausten estämiseksi järjestelmissä, joissa suoritetaan one-to-many-tyypin vertailuja henkilöllisyystietokannasta yrittäen löytää ja poistaa kaksoiskappaleet tai väärennetyt henkilöllisyydet. Kasvotunnistukselle on löydetty myös syvempiä moderneja käyttösovelluksia, kuten videoiden analysointi ja arkistointi. Esimerkiksi kasvotunnistusohjelma voisi tutkia tuhansia tunteja uutisnauhotteita ja etsiä esimerkiksi poliittisen henkilön esiintymiset ja arkistoida nämä. Kun kasvotunnistus ja muu tekniikka kehittyy, niin uskotaan että tulevaisuuden sovellukset tulevat käyttämään hyväksi kasvojen tunnistusta kännyköissä, videokonferenssi sovelluksissa, roboteissa, interaktiivisissa peleissä ja älytaloissa.

4.3.2 Kasvotunnistustekniikka

Kuten kaikessa kuvapohjaisessa biometriikassa kohteen oikea tunnistus, eristäminen ja kirjaaminen kuva-alalle on tärkeä ja välttämätön vaihe ennen kuin tunnistusprosessi voidaan suorittaa. Kasvojen tunnistus ja taustakuvan poisto ovat osa segmentointivaihetta. Kasvojen segmentointiprosessi nimelliseltä etäisyydeltä ja eritoten ihmisjoukossa on haasteellisempaa kuin muissa biometrisissä järjestelmissä suuremman vaihtelevuuden vuoksi. Kameran sijainti, näkökenttä ja taustakuva voivat aiheuttaa huomattavaa vaihtelevuutta siihen kuinka kasvot näkyvät kuvassa ja kuinka helposti tai vaikeasti ne ovat automaattisesti paikannettavissa ja eroteltavissa muusta kuvasta. Sijainti ja kokoero voidaan korjata, kun kasvot ja silmät on paikannettu, jos erot eivät ole liian suuria. Kasvojen havaitseminen saadaan aikaan tutkien muotoja ja piirteitä kuvassa. Useimmat ohjelmat pyrkivät etsimään kasvojen kaltaisia alueita kuvasta aloittaen keskeltä kuvaa työstäen kuvaa keskeltä ulospäin. Yleisimmin kasvojen havaitsemisprosessin tuloste on sijainti- ja rekisteröintitietoa, sisältäen

kasvot rajaavan suorakulmion, silmien koordinaatit ja mahdollisesti nenän alaosan ja suun keskiosan sijainnin. [1, s. 73.]

Videoissa liikeinformaatiota voidaan käyttää hyödyksi kun yritetään löytää ja tunnistaa henkilön kasvoja. Kasvotunnistus on jo varsin hyvä yksipuolisille ja jopa eri asennoissa oleville kasvoille, jotka voidaan havaita, taltioida ja rekistöröidä koodausta varten. Kuitenkin ongelma on huomattavasti suurempi, kun tämä yleistetään ihmisjoukkoon. Ihmisjoukot voivat sisältää useampia kasvoja ja huomattaviakin eroja etäisyyksissä, asennoissa ja kamerakulmissa. Ylimääräinen taustaliike (häiriö) vain lisää ongelman suuruutta tehden kasvotunnistuksen entistä vaikeammaksi ja epäluotettavaksi suurissa ihmisjoukoissa. Ei-ihanteellisissakin olosuhteissa voidaan kuitenkin saavuttaa varsin hyviä tuloksia, kun ohjelma on oikein kalibroitu ja kamerat on sijoitettu taktisesti oikein kohdealueelle. Tarkempien ohjelmakalibrointien avulla voidaan sisällyttää erilaisia kohdemerkkejä ympäristöön. Nämä merkit antavat tarkempaa syvyysinformaatiota muuten latteaan kuvaan. [1, s. 73.]

Vuosien tutkimustyön ja parannusten jälkeenkin nykypäivän tekniikka toimii parhaiten kontrolloiduissa ympäristöissä, jotta saadaan kaapattua sopivia, yhdenmukaisia, ristiriidattomia kasvokuvia. Vaihtelevat kamerakulmat ja joukko–tilanteet vaikeuttavat kasvotunnistusta ja heikentävät toimintaa huomavasti. Vaikkakin on huomattavasti eri variaatioita ja eroja eri lähestymistavoissa, niin ne kaikki lukeutuvat pääasiallisesti kolmeen eri algoritmien luokkaan: hermo–verkkoihin, ominaiskasvoihin ja paikallisten piirteiden analyysiin. Mallipohjien koot vaihtelevat kaikkien näiden kolmen eri pääluokan välillä ja eri valmistajien välillä, mutta pääsääntöisesti ne vievät alle 100 tavua. Tunnetut teollisuuden laitevalmistajat ilmoittavat mallipohjiensa vievän vain jopa 86 tavua. [1, s. 74.]

Hermoverkkoratkaisut edustavat laajoja kuviolajien tunnistusalgoritmejä joita käytetään kasvojen kuvioihin, joita neuroverkot käyttävät tunnistuspisteinään tavalla tai toisella. Neuroverkot pohjautuvat yksinkertaisiin suoritusyksiköihin tai solmuihin, jotka on aseteltu kerroksiin ja yhdistetty painotetuin liitoksin. Syötteiden määrä vastaa piirteiden lukumäärää, ja hermoverkot tyypillisesti hyödyntävät yhtä tai useampaa välikerrosta ennen kuin tieto siirretään uloimmalle kerrokselle. Uloin kerros vastaa eri luokkien määrää. Kasvotunnistuksessa luokkien määrä vastaa järjestelmään kirjautuneiden

määrää, joita harkitaan tunnistettavan. Tämä mahdollistaa menetelmän, joka sallii tietokoneen oppia suorittamaan luokittelutehtäviä, jotka pohjautuvat suoraan tiedossa oleviin kuvioihin. Vaikka neuroverkkojen perussuoritusyksiköiden funktiot perustuvat biologisten hermosolujen perusominaisuuksiin eivät tietokoneohjelmalliset solut kuitenkaan noudata ja sisällä biologisten hermosolujen toimintoja eivätkä ominaisuuksia. Ne hyväksyvät useita painotettuja syötteitä (luonnonmukainen biologinen vastine hermosolujen kestävyys), suorittavat yksinkertaisia lisäyksiä määrittäkseen aktivointitason ja näin kukin vuorollaan tuottavat tämän tulosteen. Ne eivät taltioi aikaviiveitä eivätkä muita monimutkaisia funktioita kuten biologinen hermoverkko tekee. Kaikesta huolimatta hermoverkot ilmentävät tiettyjä piirteitä, jotka matkivat ihmisälyä. Esimerkiksi ne voivat yleistää hyvin ja näin mahdollistaa tunnistuksen puutteellisesta tiedosta tai tiedosta, jossa esiintyy luonnostaan hajontaa. [1, s. 74.]

Neuroverkot kehitettiin 1950- ja 1960-luvulla. Vaikka hyvin monet osallistuivat niiden kehitykseen, niin Marvin Minskyä pidetään yhtenä huomattavimmista ensimmäisen sukupolven neuroverkkojen kehittäjistä. Muotosarjaa arvioitaessa, on käytössä valtava määrä eri arkkitehtuureita, joita voidaan kutsua neuro–verkoiksi. Monet keskittyvät piirrevalintoihin, painotuksiin ja virheenkorjaus–kaavoihin, jotka ovat johtaneet hajontaan alkuperäisessä sisällössä. Kaikki tämä on johtanut hienoisiin eroihin käytöksessä ja hyödyissä jossain tietyssä tietueessa. Vaikkakin useat erilliset tutkimukset ja kehitysprojektit ovat rikastaneet neuroverkkojen tutkimuksia, niin erilaisuus merkitsee myös, että eri valmistajien sovellukset voivat tuottaa erilaisia tuloksia samasta tiedosta, ja tätä on pidettävä mahdollisena epäkohtana. [1, s. 75.]

Ominaiskasvot on termi, jota käytetään toisen laajan algoritmityypin luokittelussa. Ominaiskasvoalgoritmit vertailevat kasvoja niiden abstraktion eli erotuskuvan paletin pohjalta. Matthew Turk ja Alex Pentland usein mainitaan puhuttaessa menetelmän kehityksestä. He esittelivät prosessin kuinka kasvojen erotuskuvat tai ominaiskasvojen tuntomerkit saadaan kerättyä kuvakokoelmasta ja kuinka kasvot sen jälkeen esitetään painotettuna summana näistä kuvanäytteistä. Haluttu yhtäläisyys tai samankaltaisuus kasvojen välillä voidaan sen jälkeen ilmoittaa numeerisena eroavaisuutena näiden painotettujen summien arvojen pohjalta. On kritisoitu, että tämä luokittelutapa ei vastaa tapaa,

jolla ihminen tunnistaa ja tulkitsee kasvojen piirteitä ja samankaltaisuuksia. Kaikesta huolimatta ominaiskasvoalgoritmien matemaattisten ominaisuuksien ja tunnistusprosessin on demonstroitu saavuttavan riittävän tarkkoja tuloksia jopa tietyissä minimaalisesti kontrolloiduissa ympäristöissä. [1, s. 75.]

Paikallispiirteiden analyysi viittaa termiin, jota käytetään algoritmityyppi luokasta, jossa taltioidaan joukko geometrisiä tietueita ja etäisyyksiä kasvokuvista, joita käytetään kasvojen ilmentämisessä ja vertailussa (huom. paikallisia piirteitä voitaisiin käyttää hermoverkkojen kanssa yhdessä). Varsinaiset piirteet joita käytetään nykypäivän kaupallisissa tuotteissa tunnistuksessa ovat yrityssalaisuuksia ja patentoituja eivätkä ole yleisesti tiedossa. Sen sijaan niitä kuvataan yleisin piirtein: suu, nenä, leuka, kulmakarvat ja posket. Paikallisten piirteiden analyysiin tulee paikallistaa ja taltioida nämä piirteet, kuvata niiden sijainti, koko ja yleinen muoto. Kasvoja voidaan tämän jälkeen verrata niiden piirteiden osien samankaltaisuuksia vertailemalla. Yleisesti paikallisten piirteiden analyysimenetelmä on kiinnostava, koska se esittää kasvot vähemmän abstraktissa muodossa vektoripohjaisina piirteinä. Menetelmän on demonstroitu olevan yksi parhaiten toimivista. Paikallisten piirteiden analyysi ei kuitenkaan toimi yleisessä ympäristössä yhtä hyvin kuin toiset tekniikat, koska se on riippuvainen onnistuneesta tasalaatuisesta kuvankaappauksesta, josta tulee löytyä keskeiset piirteet. Menetelmiä on hienosäädetty mm. optimoimalla niiden toimintaa sisällyttämällä painoarvoa piirteiden tilastollisiin ominaisuuksiin sellaisina kuin ne esiintyvät yleisesti järjestelmään kirjatuilla ihmisillä. [1, s. 75.]

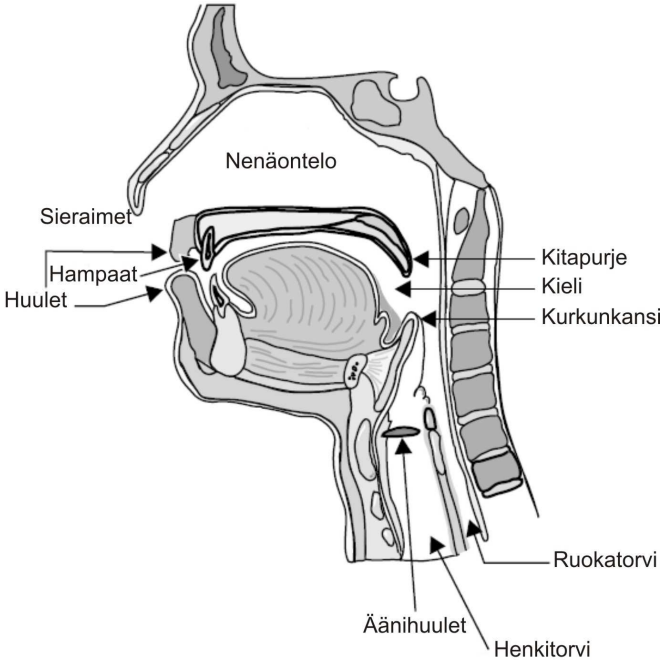
4.3.3 Tutkimus ja muu kasvotunnistustekniikka

Kasvojen termografia ja kasvojen skannaus infrapunasensoreilla tukevat tai laajentavat molemmat kaksiuloitteista kasvotunnistusta. Kasvojen termografia perustuu piilevään verisuonirakenteeseen ja sen lämpöominaisuuksiin. Nämä kiinnostavat siksi, että ne ovat vähemmän alttiita valeasuille. Termografia voidaan suorittaa myös hämärissä olosuhteissa. Termografialla on myös omat selkeät ominaisuudet, joita voidaan käyttää tunnistuksessa. Termografia on myös lupaava hybriditekniikka. Infrapunakameroita voidaan myös käyttää normaalien valvontakameroiden kanssa yhdessä, jolloin voidaan parantaa ihmisten ja kasvojen haivaitsemista valvontajärjestelmissä. Toinen potentiaalinen vaihtoehto on käyttää termografiaa ”tahdosta

riippumattomattoman punastumisreaktion” havainnointiin, joka liitetään usein ahdinkoon. Kasvoalueen verenkiertoa lisäävät myös fysiologiset tilat kuten fyysinen harjoittelu, alkoholi ja jopa ihan normaali pureskelu ja syöminen. Joitakin hybridihavaintotekniikoita on jo testattu sotilaallisissa valvontajärjestelmissä. Erikoistuneen luonteensa ja korkeiden kustannustensa vuoksi niitä ei todennäköisesti tulla hyödyntämään kaupallisissa järjestelmissä lähitulevaisuudessa. [1, s. 77.]

4.4 Puhujatunnistus

Puhujatunnistus on biometrinen menetelmä, joka hyödyntää sekä fysiologisia että käytöksellisiä elementtejä. Äänielinten fyysinen muoto on pääasiallinen fysiologinen komponentti. Äänielimet koostuvat suun ja nenän ilmateistä (kuva 11). Äänemme syntyy varsinaisesti pehmytkudosonteloissa. Ontelot toimivat yhdessä suun, leuan, kielen, nielun ja kurkunpään liikkeiden kanssa kontrolloiden puheenmuodostusta. Näiden ilmateiden fyysiset ominaisuudet luovat mitattavissa olevan akustisen äänen muodon puheellemme. Niiden muoto, pituus ja äänenvoimakkuus toimivat akustisina suodattimina näin vaikuttaen äänensävyyn, äänen korkeuteen ja resonanssiin. Liike, puhetyyli ja sanojen ääntäminen muodostavat perustan käyttäytymispohjaisille piirteille äänibiometriassa. Lisäksi esimerkiksi vapaamuotoinen puheen analysointi, jossa analyysi pohjautuu puhemalleihin ilman asetettua sanastoa, ottaa vertailussa ja analyysissä huomioon myös kieliopin, sanojen esiintymistiheyden tilastona, ilmausten käytön, muut rytmiin ja henkilön aksentille tyypilliset piirteet. [1, s. 78.]



Kuva 11. Puhe-elinten perusanatomia. *Äänielimet koostuvat suun ja nenän ilmateistä, joiden fyysiset ominaisuudet luovat mitattavissa olevan akustisen äänen muodon puheellemme.*

Puheentodentaminen, josta käytetään myös nimeä puhujatunnistus, on yksi monista puhetekniikan perustuvista sovelluksista. Puheenymmärtäminen on toinen eri tarkoitukseen suunnattu tekniikka. Puheenymmärtämisen tarkoitus on ymmärtää puhuttuja sanoja ja lauseita. Alun perin tätä kehitettiin puhekäyttöliittymiin tietokoneisiin. Puheenymmärrystä voidaan käyttää saneluun kirjoitusohjelmissa ja kasvavassa määrin tukemaan ja ymmärtämään puhekomentoja. Puheeymmärtäminen tulee yleistymään huomattavasti sulautetuissa järjestelmissä, jotka vaativat tai hyötyvät hands-free-käyttöliittymästä. Mahdollisia käyttökohteita ovat esimerkiksi tietokoneet, autot, kuluttajaelektroniikka, kodinkoneet ja älytalot. Kuitenkin puhujatunnistamisen ero puheenymmärtämiseen nähden on, että tämän ainoa tavoite on määrittää kuka puhuu ja näin tunnistaa henkilöllisyys pelkän puheen avulla. Käyttäjän henkilöllisyyttä kysytään puhenäytteen avulla (yksi sana tai lyhyt lause). Näyte taltioidaan mikrofonin avulla, minkä jälkeen näytteen akustisia ominaisuuksia verrataan aiemmin taltioituun mallinäytteeseen. Jos ne vastaavat toisiaan raja-arvojen puitteissa, niin käyttäjä hyväksytään ja tunnistetaan. [1, s. 79.]

Identifiointi tai verifiointi suoritetaan joko tekstin sisällöstä riippuvaisena tai riippumattomana järjestelmän luonteesta riippuen. Tekstin sisällöstä riippumaton tunnistus tarkoittaa, että käyttäjän antama puhenäyte ei riipu opetusvaiheessa annetusta puhenäytteestä, vaan voi sisältää muitakin sanoja. Tekstin sisällöstä riippuva tunnistus tarkoittaa, että käyttäjä antaa kirjautumisvaiheessa puhenäytteenään joitakin opetusvaiheessa antamistaan sanoista. [18, s. 6.]

Yleisimmin käytetyllä tekstin sisällöstä riippuvalla tunnistusmenetelmällä saavutetaan alhaisempi virhemarginaali rajoittamalla näytteenotto ennaltamäärättyihin yksittäisiin sanoihin tai lyhyisiin lauseisiin. Menetelmän vapaamuotoisuuden vuoksi tekstistä riippumaton tunnistusmenetelmä käsittelee puhetta pidemmän aikaa. Molempia tiloja voidaan myös käyttää yhtäaikaisesti, mutta käytännöllisistä syistä pitkien lauseiden ja puheen käyttäminen on usein käyttökelvoton ja huono vaihtoehto ko-operatiivisissa tunnistusjärjestelmissä, joissa käyttäjä odottaa pikaista vastausta tunnistuskyselyyn.

Teoria ja tekniikka keskittyy äänenymmärtämisessä ja puhesynteesi–sovelluksissa pääsääntöisesti siihen, kuinka parametrillisesti kaapata, taltioida ja toistaa puhesignaaleja, kun taas puhujatunnistussovelluksissa pääsääntöisesti pyritään luokittelemaan ja ymmärtämään puhesignaaleja.

4.4.1 Puhujatunnistussovelluksia

Puhujantunnistus mahdollistaa käytännöllisen käyttöönliittymän todentamis- ja tunnistusjärjestelmissä. Monet verifiointisovellukset ovat tekstiriippuvaisia, ja vaativat käyttäjää ensin esittämään käyttäjätunnuksensa joko kirjoittamalla sen tai esittämällä laitteelle jonkin älykortin, minkä jälkeen laite pyytää käyttäjää toistamaan ennaltamäärätyn sanan tai lyhyen lauseen. Käyttäjän puhenäyte sen jälkeen käsitellään ja sitä verrataan ennalta taltioituun mallinäytteeseen, joka kuuluu kysyiselle käyttäjätunnukselle. Äänentoistohyökkäysten estämiseksi jotkin sovellukset luovat satunnaisesti syötelauseen sanastosta ja numeroista, jotka on määritelty sovelluksen kirjautumisvaiheessa. Näin luotu lisähaaste auttaa vähentämään satunnaisten huijareiden määrää ja luomaan esteen määrätietoisille ja taitaville huijareille.

On myös hyvä huomioida, että äänentunnistusta ei pidetä yhtenä tarkimmista biometrisistä teknologioista. Kuvauksen mukaisen tekstiriippuvaisen tunnistuksen uskotaan voivan saavuttaa 2 %:n ylimenovirhetaajuuden, tehden siitä näin järkevän turvaratkaisun vain matalan turvaluokan ympäristöihin. Myös puhujatunnistustuksen tarkkuus on hyvin altis ympäristön poikkeavaisuuksille ja usein myös käyttö on harjoittelua vaativaa. Esimerkiksi eri kuulokkeiden ja mikrofonien käyttö tietokantaan kirjautumisvaiheessa ja varmistusvaiheessa saattaa heikentää suorituskykyä usein täysin odottamattomalla ja ennalta tuntemattomalla tavalla.

Puhujatunnistuksen suorituskyky myös heikkenee, kun taustalla on useita puhujia tai taustaääniä ympäristössä. Tekstiriippuvainen tunnistus voidaan kalibroida toimimaan kohtalaisen hyvin hiljaisessa ympäristössä, mutta tekniikka itsessään ei kelpaa kunnolliseksi tunnisteeksi korkean turvaluokan ympäristöissä. Jos puhujantunnistuksen lisäksi käytetään esimerkiksi nelinumeroista PIN-koodia, niin väärien hyväksyntöjen määrä (FAR) vähenee ollen noin yksi miljoonasta sen sijaan että se olisi yksi sadasta.

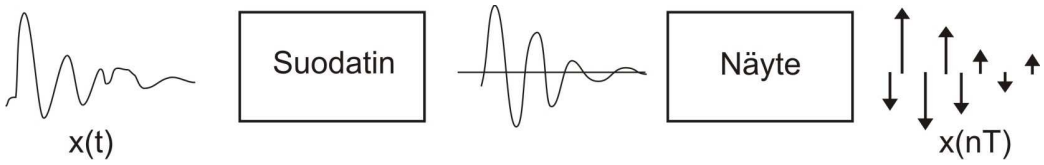
Haastavampi (ei niin tarkka menetelmä) äänentunnistustapa pyrkii tunnistamaan puhujan keskustelun kautta ja on näin tekstistä riippumaton. Näissä sovelluksissa voidaan käyttää analysointiin puhekommunikaatiota tai esimerkiksi käydä läpi ja tutkia erilaisia kommunikaation kanavia. Esimerkiksi pankki voisi suorittaa äänentunnistuksen puhelimessa ennen kuin suostuu puhumaan henkilökohtaisista asioista henkilön kanssa. Eräs potentiaalinen sovellutus on tutkia erilaisia nauhoitteita ja näin etsiä jonkin tietyn henkilön puheita, elokuvia jne. Myös kyky tunnistaa puhujat kiinnostaa erityisesti viranomaisia. Puheen yhdistäminen henkilöllisyyteen salakuuntelunauhotteista on tärkeä työkalu poliisiviranomaisille. [1, s. 82.]

4.4.2 Puhujatunnistuksen toimintaperiaate

Puhesignaalit ovat informaatiorikkaita sisällöltään, ja näin puhenäytteet ovat kooltaan suuria. Toteutuksesta riippuen puhenäytteet ovat noin 70 – 80 tavua jokaista nauhoitettua sekuntia kohden. Näin ääninäytteiden tilavaatimus on huomattavasti suurempi kuin muiden biometristen tunnisteiden. Pienissä sovelluksissa, jotka käyttävät yhden sanan salasanoja, tarvittavan muistin määrä

ei ole suuri ongelma, mutta usean käyttäjän suuremman luokan järjestelmissä se on samoin kuin järjestelmissä joiden toiminta perustuu pitkien puhenäytteiden käyttöön ja niiden analysointiin.

Ääninäytteet ovat aaltomuotoisia, ja niissä aika on vaakatasossa ja äänenvoimakkuus pystytasossa (kuva 12). Aallontaajuus viittaa kokonaisten jaksojen määrään per sekunti, kun aalto värähtää edestakaisin. Perinteinen analoginen puhelin lähettää sähkömagneettisen aallon joka värähtää noin 3000 kertaa per sekunti. Tämän taajuuden ilmaistaan yleisesti olevan 3000 Hz tai 3 kHz. Kun äänen tai puheen aaltomuodot muunnetaan digitaaliseen esitysmuotoon, niin signaali näytteistetään moniin pieniin aikaväleihin (T). Tämä mahdollistaa alkuperäisen signaalin esittämisen kerrannaisnäytejaksona x(nT). Digitaalinen signaali on teknisesti analogista parempi, koska se operoi suuremmilla nopeuksilla ja omaa puhtaamman äänenlaadun ja vähemmän virheitä. Digitaaliset puhelinlinjat toimivat 8kHz, kuitenkin useimmat puhelimeen liittymättömät puhujatunnistussovellukset näytteistävät äänisignaalit taajuudella 12 kHz tai 16 kHz. Vertailuna standardi digitaalinen ääni CD:llä on näytteistetty tajuudelle 44.1 kHz. [1, s. 83.]



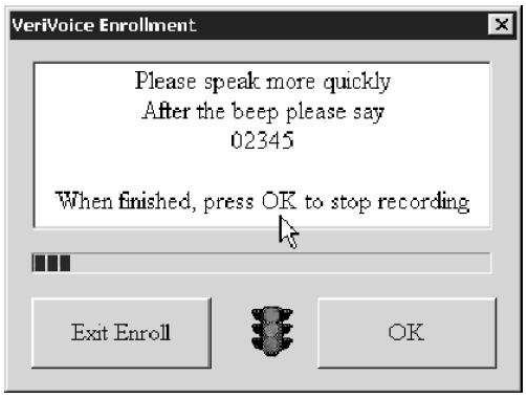
Kuva 12. Puheen aaltomuodon digitalisointi. *Näin alkuperäinen aaltomuoto muunnetaan digitaaliseen muotoon, joka mahdollistaa signaalin esittämisen kerrannais–näytejaksona x(nT)*

Puhujatunnistus arvioi äänensävyä, kestoaikaa, äänen korkeutta ja voimakkuutta signaalissa ja vertaa näitä ominaisuuksia tietokannassa oleviin ääninäytteisiin. Vaikka näytteen foneettinen sisältö ja merkitys eivät ole suoranaisesti oleellisia tunnistuksessa, niin foneettisia piirteitä tai osia voidaan hyödyntää lisäpiirteinä vertailussa. Foneettiset jaksot kielessä kuten vokaalit ja konsonantit ovat tyypillisesti lyhyitä kestoltaan (mitataan millisekunteissa), kuitenkin on olemassa erilaisia menetelmiä tämän informaation merkitsemiseksi ja taltioimiseksi puheesta. [1, s. 83.]

Puhujatunnistuksessa on neljä perusvaihetta, jotka voidaan toteuttaa usein eri tavoin. Ensimmäinen vaihe on puheen taltiointi digitaalisessa muodossa. Toinen vaihe on piirteiden valitseminen ja taltiointi. Kolmas vaihe on piirteiden ryhmitteleminen ja ryhmitetyn esityksen tallennus tietokantaan. Viimeinen vaihe on annetun ääninäytteen täsmäys ja päätöksen teko. On olemassa lukuisia menetelmiä ja akustisia malleja piirteiden määrittelemiseksi ja niiden luokittelemiseksi toisistaan erilaisiksi vastineiksi. Menetelmä, jota kutsutaan vektorikvantisoinniksi (VQ), kartoittaa suuria vektoriesityksiä alueiksi puhesignaaleista, jotka sisältävät monia tuhansia arvoja. Nämä muutamat alueet muodostavat perustan puhujakohtaisten piirteiden määrittelyssä. VQ-hakutaulukko muodostetaan jokaiselle käyttäjälle puhenäytesarjan avulla. Sen jälkeen tunnistusvaiheessa samankaltaisuuksia ja eroja kerätään ajan myötä, jotta voidaan määrittää todennäköisin vastaavuus. Suurin ongelma sanojen tunnistuksessa ja mallinäytteiden täsmäyksessä on sanojen kohdistus ja normalisointi aikatasolla. Dynaaminen aikasovitus (DTW) on eräs hyvin tunnettu menetelmä väliaikaisen rekisteröinnin ja skaalauksen suorittamiseksi. [1, s. 84.]

Puhujamallit voidaan jakaa kahteen eri ryhmään: sapluunamalleihin ja stokastisiin malleihin. Stokastiset mallit ovat suosittu menetelmä puhujantunnistuksessa. Suosituin stokastinen malli on Hidden Markov Model (HHM). Sapluunamallien on tarkoitus mallintaa tiettyä lausahdusta useasta piirrevektorista muodostetun sarjan pohjalta rakennetun keskiarvon perusteella. Stokastisissa malleissa puheentuottamisprosessi oletetaan satunnaisprosessiksi, jonka tarvittavat parametrit voidaan arvioida tarkasti jollain ennalta määritellyllä menetelmällä. Stokastiseen malliin pohjautuvan päätöslogiikan avulla täsmäys on todennäköisyyksien vertailua. Puhuja hyväksytään mikäli aidon puhujan todennäköisyys on suurempi kuin huijarin. [1, s. 84.]

Esimerkkinä voidaan mainita VeriVoice-puhujatunnistusjärjestelmä. Se on tarkoitettu puhelinturvaan, pääsynhallintaan ja PC:lle sisäänkirjautumiseen. Tietokantaan rekisteröityessä puhenäytteen akustisia ominaisuuksia kuvaava malli luodaan käyttäjän ohjelmistolle ääntämien numeroiden pohjalta. Kuvassa 13 on eräs syöte tietokantaan sisäänkirjautumisesta. Koko tapahtuma kestää noin 3 minuutia ja syntyvä puhenäytemalli vie tilaa noin 2 – 6 kilotavua. [1, s. 84.]



Kuva 13. VeriVoice-puhujantunnistusohjelmiston rekisteröitymisikkuna

Kun tietokantaan rekisteröityminen on suoritettu, niin pääsynhallintatapahtumat suoritetaan muutamassa sekunnissa. VeriVoice ilmoittaa järjestelmilleen virheprosentikseen 1.7, jota voidaan säätää niin, että syntyy joko vähemmän vääriä hyväksyntöjä tai vääriä hylkäyksiä.

4.4.3 Muut ohjelmistot ja tekniikka

Tekniikan kehittyessä ja kaupallisen kiinnostuksen kasvaessa puhujatunnistus- ja puheenkäsittelytekniikat ovat ilmiselviä osa-alueita, kun ohjelmistojen työkaluja ja toimintoja aletaan laajentaa ja kehittää. Microsoft Office XP tukeekin jo nykyisin puhekäskykomentoja ja siinä on myös saneluominaisuus. Microsoftin tekniikkaa tukee sen Speech Application Programming Interface (SAPI, puhe ohjelmien ohjelmointikäyttöliittymä), joka on suunniteltu olemaan apuna muille ohjelmistokehittäjille puhesyötön luomiseksi ohjelmistoihinsa. Apple Computers on integroinut puhujatunnistuksen ja tekstistä puheeksi mahdollisuuden nykyisiin käyttöliittymiinsä.

VoiceXML (Voice eXtensible Markup Language) on tiedonsiirtotekniikka, jonka tarkoitus on mahdollistaa puhesovellusten käyttö internetissä. VoiceXML perustuu puhujatunnistukseen, ja ensisijaisesti sen tarkoitus on tiedonsiirto ja puhekomentojen muuntaminen rakenteelliseksi, merkityksi, tekstipohjaiseksi kuvaukseksi. Nämä merkityt kuvaukset voidaan sen jälkeen siirtää ja tulkita. VoiceXML-tekniikkaa käytetäänkin nykyisin esimerkiksi tilauspyyntöjen tekemisessä, ajo-ohjeiden saamiseksi, herätysten tilauksessa, lentoaikojen

seurannassa, sähköpostin lukemisessa ja lukuisissa puhelinsovelluksissa. VoiceXML:n kehityksestä alkuaan vuonna 1999 vastasi telepalveluyritysten yhteistyö, johon kuuluivat IBM, AT&T, Lucent ja Motorola. Nykyisin VoiceXML-standardista vastaa World Wide Web Consortium. [1, s. 85.]

4.5 Iiris- ja retinatunnistus

Ihmisen silmän monimutkainen rakenne mahdollistaa kaksi tarkinta biometrisen tunnistuksen menetelmää. Iiris ja retina sijaitsevat silmän etu- ja takaosassa ja kummallakin on oma tunnusomainen rakenne. Iiris on värillinen kudosrengas, joka ympäröi pupillia. Sen rakenteen runsas kuviointi toimii iiristunnistus–järjestelmien pohjana. Retina sijaitsee silmän takaosassa, joka ei normaalisti ole näkyvissä, mutta silläkin on omat tunnusomaiset piirteensä. Verkokalvon verisuonien geometrinen rakenne toimii retinatunnistusjärjestelmien perustana. Ensimmäiset retinantunnistus järjestelmät tulivat kaupallisesti saataville 1980-luvun alkupuolella ja iiristunnistusjärjestelmät noin 5 vuotta myöhemmin.

4.5.1 Iiristunnistus

Värikalvo eli iiris on silmän etuosassa sijaitseva pyöreän muotoinen osa, joka ympäröi silmän pupillia, ja sen tehtävä on säätää silmään pääsevän valon määrää. Värikalvon keskellä on pupilli eli mustuaisaukko, jonka läpi valo kulkee mykiön kautta verkkokalvolle. Iiris on kerros sarveiskalvon alapuolella, ja se muodostuu suonikkaasta pigmentoituneesta kudoksesta, joka yhdistää säteittäiset pupillia laajentavat lihakset ja sen reunaa kiertävät rengaslihakset. Iiriksen kuvionti on runsas ja monimutkainen sisältäen paljon juovia ja kohoumia. Iiristunnistus tekniikka perustuu näiden kuvioiden taltiointiin, analysointiin ja vertailemiseen.

Ihmisen iiristä kontrolloi kaksi lihasta: laajentajalihas ja rengaslihas, jotka voivat laajentaa tai supistaa värikalvon kokoa ja näin säätää silmään pääsevän valon määrää. Kun iiris on täysin supistunut, niin sen kudosaine menee tiheämmäksi ja näin pupillin koko ja silmään pääsevän valonmäärä kasvaa. Kun iiris laajenee, syntyy päinvastainen tilanne, ja näin silmään pääsevän valonmäärä vähenee. Ympäristön valoisuuteen mukautumisen lisäksi molemmat lihakset ovat yhteydessä autonomiseen hermostoon ja näin toimivat myös sisäisten

fysiologisten reaktioiden vaikuksen alaisina. Sympaattinen reaktio, joka tunnetaan myös ”pako ja pelko”-tilana, stimuloi laajentajalihasta minkä seurauksena iiris puristuu kasaan ja pupilli laajentuu. Parasympaattinen reaktio, joka tunnetaan myös ”lepo ja rentoutumis”-tilana, stimuloi rengaslihasta täten laajentaen iiristä ja näin pienentäen pupillin kokoa. [1, s. 90.]

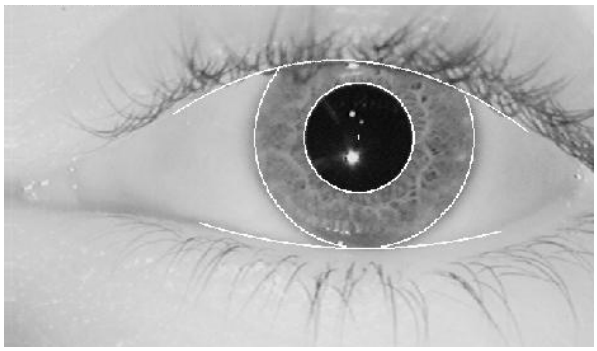
Silmälääkärit huomasivat ensimmäisinä iiriksen tunnusomaiset piirteet ja havaitsivat, että vasemman ja oikean silmän iiriksen kuviot olivat erillaiset. He olettivat, että jokainen iiris on ainutlaatuinen ja että sen muotoon ja kuvioon ei ole mitään havaittua tai tunnettua geneettistä riippuvuutta. Iiris muodostuu satunnaisesti ennen syntymää ja pysyy normaaleissa elinolosuhteissa muuttumattomana syntymästä kuolemaan asti. Yhdessä ominaisuudet erottamiskyky ja muuttumaton tekevät iiriksestä erinomaisen valinnan biometriseksi tunnisteeksi. [1, s. 90.]

Silmälääkäreille Leonard Flomille ja Arin Safirille myönnettiin patentti vuonna 1987 iiristunnistusmetodeille jotka perustuivat näkyvien iiriksen piirteiden tunnistamiseen. Cambridgen yliopiston tohtori John Daugman myöhemmin kehitti algoritmeja, matemaattisia metodeja ja tekniikoita, joilla voitaisiin koodata iiriksen kuviointi ja vertailla niitä keskenään. Nykyiset kaupalliset sovellukset perustuvat Daugmanin patentoituihin menetelmiin. Niitä lisensoi ja markkinoi Iridian Technologies New Jerseyssä ja Genevessä. [1, s. 90.]

Hollywood-elokuvat ovat luoneet unohtumattomia mielikuvia siitä kuinka silmämunia muokataan tai on poistettu ihmisestä pyrkimyksenä tunnistusjärjestelmän huijaaminen. Vaikka tämä ei ole ollut parasta mahdollista mainosta biometrisille tunnisteille, eikä myöskään ole yleisin tapa todellisuudessa laitteiden huijaamiseksi, niin nämä mielikuvat ovat kuitenkin luoneet uusia haasteita turvatoimien suunnittelijoille, jotta ymmärretään ja osataan ottaa huomioon kaikki mahdolliset tavat järjestelmän huijaamiseksi ja ohittamiseksi, vaikka ne olisivatkin kuinka mahdottoman kuuloisia. Vaikka silmä onkin suhteellisen hyvin suojattu elin, niin se ei kuitenkaan ole immuuni vammoille ja taudeille. Esimerkiksi iirismelanooma on iiristä rappeuttava sairaus, joka aiheuttaa iiriksen muuttumisen lähes värittömäksi tai ruskeaksi.

4.5.2 Iiristunnistuksen toimintaperiaate

Iiristunnistus käyttää lähi-infrapunavaloa (0.75-1.4 µm aallonpituudeltaan) ja se on suunniteltu toimimaan yhteistyöhaluisten ihmisten kanssa lähietäisyydellä. Osa yhä tutkimuksen alla olevista projekteista ilmoittavat toimintaetäisyydekseen jopa 5 – 10 metriä. Kyseiset järjestelmät ovat kuitenkin yhä prototyyppejä eikä niitä ole saatavilla kaupallisina tuotteina. Kaupalliset iirisskannauslaitteet toimivat parhaiten noin 8 – 22 cm:n päästä laitteesta. Kuvat skannataan ja käsitellään harmaasävyarvoina ja kuten kuvassa 14, se segmentoidaan niin, että iiris voidaan paikantaa ja eristää muusta kuvasta. Kuvalle tehdään koko- ja kontrastikorjauksia luonnollisesti esiintyvien supistumisten ja laajentumisten vastapainoksi. Tuloksena on kooltaan invariantti esitysmuoto. [1, s. 91.]



Kuva 14. Paikannettu ja eristetty iiris

Tohtori Daugman kuvaili vuonna 1998 tutkimusraportissaan ”How iris recognition works” iirisskannauksen tärkeimpiä toimintoja ja laskelmia suoritettuna 300 MHz:n Sun-työasemalla. Taulukossa 3 on esitettynä iirisskannauksen eri vaiheisiin tuolloin kulunut aika. [1, s. 91.]

Taulukko 3. Iiristunnistuksen eri vaiheisiin kuluva aika [1, s. 92.]

Toimenpide	**Aika (ms)**
Kuvan terävyyden laskeminen	15
Kuvan heijastuksien poisto	56
Silmän ja iiriksen paikannus	90
Mustuaisen reunojen havainnointi ja sijoitus	12
Molempien silmäluomien havainnointi ja sijoitus	93
Silmäripsien ja piilolinssien reunojen poisto	93
Demodulointi ja iiriskoodin luonti	102
XOR-operaatio kahden iiriskoodin välillä	10

Ensikokemuksiinsa optimoidulla kokonaislukupohjaisella koodilla tohtori Daugman arvioi, että yksittäinen hakukoneisto voisi suorittaa noin 100 000 vertailua per sekunti ja totesi:

”Iiristunnistuksen algoritmien matematiikka mahdollistaa sen, että voitaisiin suorittaa valtioiden laajuisia hakuja samanaikaisesti ja näin tehdä luotettava tunnistuspäätös noin 1:ssä sekunnissa käyttäen samanaikaisesti edullisia keskusyksiköitä, jos niin suuri valtiollinen iiristietokanta ikinä luotaisiin.” [1, s. 92.]

Kahden iiriskoodin todellinen vertailu supistuu sarjaksi tehokkaita matalantasoisia XOR-operaatioita. XOR, jota kutsutaan myös exclusive OR:ksi on bittipohjainen operaatio, joka hyväksyy 2 binääristä syötettä ja palauttaa *tosi* (tai 1) kun syötteet eroavat toisistaan ja *väärä* (tai 0) kun syötteet vastaavat toisiaan. Määrä missä laajuudessa kaksi iiriskoodia eroavat toisistaan määräytyy erilaisten bittien määränä tai kahden iiriskoodin merkkivälin etäisyytenä. Tohtori Daugman kuvaa alun perin 256 tavuisen iiriskoodin esityksen ja selittää, kuinka etäisyydet mitataan koodeista. Kuitenkin ajan myötä koodin alkuosaan on lisätty lisäinformaatiota ja muutoksia tehty prosessiin. Iridian ilmoittaakin, että iiris käsitellään nykyisin 512 tavun iiriskoodiksi. Iiriskoodin koosta huolimatta teoria ja menetelmä ovat pysyneet muuttumattomina.

Merkkiväli voidaan myös ilmaista kahden yhtä suuren binäärisen lähteen suhteellisena erona. Tohtori Daugmanin iiriskoodin matemaattinen analyysivertailu osoittaa, että iiristunnistuksen virheprosentti on hyvin pieni. Todennäköisyys, että kaksi eri iiristä tuottaisi riittävän samankaltaisen iiriskoodin, jotta tapahtuisi väärä tunnistus, on teoreettisesti noin 1 kappale 1.2 miljoonasta. Käytännössä iiristunnistusjärjestelmät toimivatkin erittäin hyvin. Muutaman vuoden takainen tehty tekniikkatesti, johon osallistui 200 koeihmistä, osoitti että iiristunnistus toimi lähes virheettömästi. Iiriksentunnistus toimi paremmin kuin sormenjälki-, kämmengeometria-, puhuja- ja kasvotunnistusjärjestelmät, jotka olivat mukana testissä. Testissä iiristunnistuksessa ei tapahtunut yhtään päätösvirheitä (ei vääriä hyväksymisiä eikä hylkäyksiä). Ainoa raportoitu virhe tapahtui tietokantaan rekisteröityessä, kun yhdellä koehenkilöistä oli toinen silmä sokeutunut. [1, s. 93.]

4.5.3 Iiristunnistussovelluksia

Ensimmäiset kaupalliset iiristunnistusjärjestelmät oli pääsääntöisesti suunnattu fyysisen sisäänpääsyn hallintaan. Tällaisille sovelluksille on hyvin tyypillistä, että niitä käyttää suhteellisen pieni määrä ihmisiä ja niitä käytetään suhteellisen harvoin. Näin yksi suhteellisen uusi PC-tietokone selviytyy tietojen käsittelystä ja taltioinnista varsin helposti. Kuvassa 15 on kulunvalvontayksikkö.

Kuva 15. Park Avenue New Jersey:ssä sijaitsevan peruskoulun iirisskanneri

Markkinoiden kasvaessa laitevalmistajat ja turvayritykset ovat alkaneet tutkia uusia käyttömahdollisuuksia ja laajentaa niin identifiointi- kuin verifionti–järjestelmien käyttöä. Esimerkkeinä voidaan mainita työpisteen tietokoneelle sisäänkirjautuminen, turvatut pankkipalvelut, biometriikan yhdistäminen avainkortteihin, matkustajienseulonta (passanger screening) ja jopa televalvonta.

Kuten missä tahansa biometrisessä tunnisteessa, iiristunnistuksen hyödyt ja haitat riippuvat täysin sovelluksesta ja kohdekäyttöympäristöstä. Puhtaasti tekniikan näkökulmasta iiristunnistus- ja iirisvarmennusmenetelmät ovat hienostuneita ja hiottuja, ja järjestelmien toimivuutta on testattu erilaisissa käyttöympäristöissä, niin rauhallisissa toimistotiloissa, kuin sotilaslaivoissa. Iiristunnistus on tarkka menetelmä, jonka käyttötapahtuma tottuneelta käyttäjältä kestää noin 4 – 5 sekuntia, jossa suurin osa ajasta kuluu siihen, kun henkilö kohdistaa katseensa laitetta kohti. Kun kuva on kaapattu ja käsitelty, niin

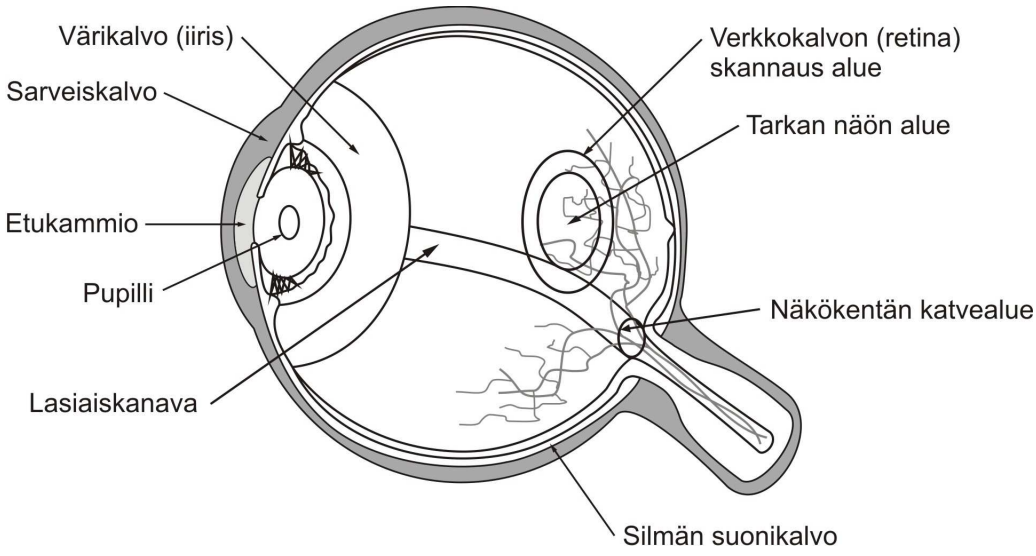
varsinainen varmennusprosessi tietokoneella on nopea ja on noin mikrosekuntien luokkaa. [1, s. 94.]

Pelkästään ominaisuuden näkökulmasta katsoen iiriksen hyvä puoli on, että se on näkyvissä (täten valmiina skannattavaksi) mutta myös luonnossaan suojattu osa silmästä. Vaikka silmäluomet, silmäripset, piilolinssit, silmien erot ja silmälle luonnollinen liike synnyttävät lisähaasteen piirreirrotukselle, näiden ongelmien avuksi on kehitetty menetelmiä, jotka toimivat useimmissa käyttöympäristöissä. Iiriksen luonnollisen liikkeen väitetään toimivan henkilön elollisuuden varmennuksessa, joskin tätä eivät ole puolueettomat testit vielä vahvistaneet. Iiriksen pieni koko ja sen kaareva muoto sopii hyvin ko-operatiivisiin lyhyen matkan pääsyn hallintalaitteiden julkisivuskannauksiin. Kuitenkin iiriksen pieni koko tuottaa ongelmia pitemmillä matkoilla ja ei-vapaaehtoisissa valvonta–järjestelmissä, joissa kuvan resoluutio, kamerakulmat, okkluusio, isolointi ja paikannus muodostuvat kasvavassa määrin tärkeiksi osatekijöiksi.

4.5.4 Retinatunnistus

Verkkokalvo biometrisenä ominaisuutena erottelee yksilöt silmän takana olevien verisuonien muodostamien muotojen avulla. Tohtorit C. Simon ja I. Goldstein tutkielmassaan vuonna 1935 tarkastelivat verkkokalvon verisuonimuotojen toisistaan erottuvia ominaisia piirteitä. Automatisoidut menetelmät retinan kuvioiden kaappaamiseksi ja käsittelemiseksi tunnistus- ja täsmäystarkoituksessa kehitettiin 1970-luvulla. Eyedentify inc. Louisianasta toi markkinoille ensimmäiset verkkokalvon skannaukseen perustuvat pääsynhallintajärjestelmät 1980-luvun alkupuolella.

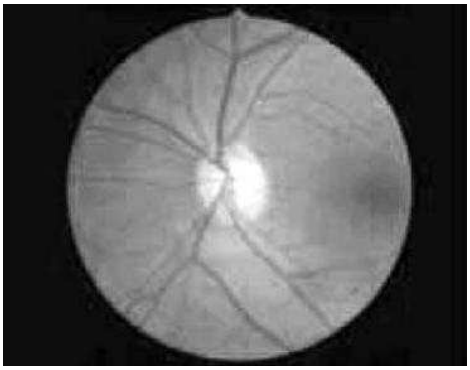
Retinaskannaus suoritetaan valaisemalla verkkokalvoa pienitehoisella infrapunavalolla ja kuvaamalla isompien verisuonten muodostamat kuviot. Koska verkkokalvo sijaitsee silmän takaosassa, niin järjestelmät vaativat toimiakseen vapaaehtoisuutta ja taitoa käyttäjältään, jotta valaisu on riittävä ja kohdistus on kunnollinen. Vaikka silmässä on pieniäkin verisuonia ja muita yksityiskohtaisia piirteitä verkkokalvon alueella niin silti verkkokalvontunnistustekniikka perustuu suurempien verisuonten muodostamiin kuvioihin rengasmaisella alueella kuvan 16 mukaisesti. [1, s. 95.]



Kuva 16. Silmän rakenne ja retinatunnistuksen skannaus alue

Mallikuvat ovat noin 96 tavun kokoisia. Kuvan pyöreä rakenne hajotetaan lineaariseen muotoon, joka muistuttaa viivakoodia. Näin verisuonten muodostama kuvio vie vähemmän tilaa ja sitä voidaan verrata tehokkaasti muihin mallinteisiin.

Esimerkki yhtenevistä verkkokalvon verisuonista näköhermon läheisyydessä on esitetty kuvassa 17. Verisuoniston uskotaan muodostuvan täysin satunnaisesti ja näin sillä ei uskota olevan mikäänlaista geneettistä riippuvuutta. Näiden kuvioiden uskotaan olevan yksi kaikkein eniten yksilöllisesti eroavista piirteistä. Kyseisen piirteen muuttumattomuutta ihmisen vanhetessa ei ole kuitenkaan tiettävästi vielä tutkittu, mutta kuten sormenjälkien ja iiriksen piirteen uskotaan ja oletetaan pysyvän muuttumattomana ihmisen koko eliniän.



Kuva 17. Yhteneviä verkkokalvon verisuonia näköhermon läheisyydessä

Jo terve järki sanoo, että verkkokalvon verisuonikuvioita ei vapaaehtoisesti kukaan muuta tai turmele, mutta kuten kaikissa ihmisen fyysisissä ominaisuuksissa piirteet voivat muuttua jonkin vamman tai sairauden seurauksena. Silmävammat kuten irrallinen verkkokalvo tai isku silmään saattaa johtaa verenvuotoon tai muuten vahingoittaa verisuonistoa. Glaukooma (viherkaihi) ja diabetes ovat yleisiä tauteja, jotka myös voivat vaikuttaa verkkokalvoon. Glaukoomassa kammionesteen ulosvirtauksen heikkenemisen vuoksi paine silmässä ja verkkokalvon alueella kasvaa, minkä seurauksena syntyy epämuodostumia ja verenkierto heikentyy verisuonten puristuessa kasaan näköhermon alueella. Kun diabetes vaikuttaa verkkokalvoon, niin kyseistä tautia kutsutaan nimellä sokeritaudin kaihi. Tauti on vaiheittainen, ja siihen sisältyy epänormaali verenkierto ja vuoto verkkokalvon alueella, joka voi heikentää näkökykyä tai jopa johtaa sokeutumiseen. Vaikka mitään lopullisia tutkimuksia ei ole tehty näiden sairauksien heikentävästä vaikutuksesta tunnistuksen suorituskykyyn, niin molemmat sairaudet vaikuttavat verkkokalvoon ja täten ajan kuluessa niillä on rappeuttava vaikutus niin silmään kuin tunnistukseenkin, varsinkin jos mallikuvia ei koskaan päivitetä. [1, s. 95.]

Koska verkkokalvo on suojattu, sisäinen elin, niin skannaustapahtuma vaatii lyhyen polttovälin ja käyttäjien täytyy olla myöntyväisiä ja yhteistyöhaluisia, jotta tekniikka toimii. Perinteisimmät verkkokalvon skannausjärjestelmät ovat seinä–yksiköitä, joita käytetään ovilla rakennusten ja/tai tietyjen kontrolloitujen alueiden kulunvalvonnassa. Laite toimii siten, että käyttäjä asemoituu 5 – 8 cm:n päähän skannerista, jonka jälkeen hänen tulee kohdistaa katseensa linssiä kohti ja pysyä paikoillaan 1 – 2 sekuntia, joka skannerilla kestää valaisemisessa, kohdistamisessa ja verkkokalvon kuvan taltioinnissa. Vaikka verkkokalvon tunnistus tarjoaa tarkkoja tuloksia, niin osa ihmisistä pitää skannausprosessia epämukavana ja tunkeilevana. Jos sensoriteknologiassa ei tapahdu läpimurtoa tai julkinen mielipide menetelmää kohtaan ei muutu radikaalisti, niin verkkokalvon skannaus todennäköisesti säilyttää maineensa yhtenä kömpelöimmistä biometrisistä menetelmistä.

Nykyisin verkkokalvotunnistuksen markkinat muodostuvat pääsääntöisesti ovien kulunvalvontalaitteista. Näiden järjestelmien suuri tarkkuus tekee niistä ideaalisia sotilaalliseen ja valtiolliseen erikoiskäyttöön. Rajallisten käyttömahdollisuuksien

vuoksi verkkokalvotunnistus on yksi kalleimmista biometrisistä tunnisteista, kun yhdelle laitteelle tulee hintaa noin 2000 – 2500 $. Tosin EyeDentify Inc. on tuonut markkinoille halvempia skannereita, jotka on suunnattu niin työpöytä- kuin yleiskäyttöön. Vuonna 2001 yritys nimeltään Retinal Technologies toi markkinoille omat verkkokalvon tunnistuslaitteet pyrkimyksenään laajentaa verkkokalvotunnistuksen soveltuvuutta tarjoamalla edullisia kannettavia skannereita.

EyeDentify Icam-skannerit käyttävät pientehoista (noin 7 mA) valonlähdettä valaistakseen mahdollisimman lempeällä tavalla verkkokalvoa. Valaistuksen täytyy olla riittävä läpäistäkseen silmän ja tarjotakseen mahdollisimman homogeenisen kuvan, jossa on täysi alue sävykkyyttä, mutta se ei saa olla niin kirkas että valo on vaarallinen tai tuskallinen käyttäjälle. Valonlähde tuottaa jonkin verran näkyvää valoa mutta koostuu pääsääntöisesti lähi-infrapunavalosta (890 nm aallonpituudeltaan). Infrapunavalon käyttö on välttämätöntä, koska verkkokalvo on läpinäkyvä kyseisillä aallonpituuksilla. Skanneri tallentaa koko verkkokalvon ja sen jälkeisen kuvan segmentaation ja eristetyn ja kohdistetun osan kuvasta, joka on välttämätön tunnistamiselle, paikantaa näköhermon ja ottaa näytteen alueen ympäriltä. Tämä menetelmä tuottaa noin 96 tavun kokoisen mallikuvan jokaista tietokantaan sisäänkirjattua henkilöä kohden.

EyeDentify Inc:n itsenäisten tunnistusjärjestelmien mainostetaan pystyvän taltioimaan 3000 henkilön mallikuvat muistiinsa. Kyseinen laite on varustettu Wiegand- ja sarjaliitännällä (RS232). Wiegandliitäntä mahdollistaa yhteensopivuuden ovijärjestelmien kanssa ja sarjaliitäntä mahdollistaa yhteensopivuuden tietokoneiden ja verkkojen kanssa. Nämä perusliitynnät mahdollistavat tehokkaan pääsynhallintajärjestelmän käytön niin yksittäisten ovien kuin laajemman verkoistetun turvajärjestelmän ratkaisuina. [1, s. 97.]

4.5.5 Iiris- ja retinatunnistusmenetelmien tarkkuus

Vuoden 1990 Orkand Corporationin raporttia lukuun ottamatta ei ole saatavilla juurikaan puolueettomia arvioita tai testituloksia verkkokalvotunnistukselle. Siitä huolimatta voidaan kaikella varmuudella sanoa, että verkkokalvon skannaus on hyvä ja tarkka tunnistamisen muoto. Oikeat tunnistukset ovat lähestulkoon kiistattomia ja väärien hyväksyntöjen prosentin on sanottu olevan erittäin lähellä

nollaa. Väärät hylkäykset johtuvat useimmiten käyttäjien tottumattomuudesta ja katseen kohdistusongelmista. Ihmiset suojelevat vaistomaisesti silmiään ja aluksi reagoivat epäröiden ja hämmennyksestä levottomina, kun he käyttävät silmiään biometrisessa tunnistuksessa. Harjoittelun myötä laitteiden käyttö ja katseen kohdistus onnistuu ihmisiltä huomattavasti paremmin.

Verkkokalvon sisäisesti suojassa olevan luonteen vuoksi sen skannaaminen on epämiellyttävää ja hankalaa useissa sovelluksissa, mutta samalla se tarjoaa suuria etuja toisiin biometrisiin tunnisteisiin nähden. Toisin kuin kasvot jotka ovat useimmiten näkyvillä ja sormenjäljet joita jätämme tietämättämme erilaisille pinnoille, verkkokalvo on luettavissa ainoastaan silloin, kun ihminen itse niin päättää ja silloinkin vain tietyissä paikoissa. Tämän ominaisuuden vuoksi verkkokalvontunnistus on ideaalinen ratkaisu erittäin korkean turvaluokituksen vaativiin paikkoihin. Lisäksi verkkokalvo on suojattu ja näin kehon sisäinen kudos on vähemmän altis ympäristön muutoksille, jotka lisäävät vaihtelevuutta ja häiriöitä muissa biometrisissä tunnisteissa. Muut biometriset tunnisteet kuten iiris ja sormenjäljet vaativat toimiakseen lisäksi monimutkaisia ohjelmistomenetelmiä, jotta voidaan taata riittävän hyvä kuvanlaatu ja kompensoida tunnisteen koon vaihtelevuutta tai esimerkiksi sormenjälkien tapauksessa erilaisten ihon tilojen synnyttämien poikkeamien, paineen ja erilaisten sensorien ominaisuuksien huomioimista.

Verkkokalvo on kehonsisäinen elin, jonka on ajankohtaisten ja arkaluontoisten yksityisyyden suojakiistojen lisäksi väärinymmärretty paljastavan tietoa henkilön terveydellisestä tilasta. Tämä on osittain johtanut siihen että osa ihmisistä uskovat että verkkokalvotunnistus on altis henkilön yksityiselämän loukkaamiselle. Tämä ei kuitenkaan pidä paikaansa ja sekaannus todennäköisesti johtuu siitä, että verkkokalvotunnistuslaitteita verrataan väärin perustein eri menetelmään kuvata verkkokalvoa, mitä käytetään lääketieteellisten diagonoosien tekemisessä. Kyseistä lääketieteellistä verkkokalvonskannaus menetelmää kutsutaan angiografiaksi, ja se on hyväksytty lääketieteellinen diagnoosimenetelmä.

Angiografia ja verkkokalvotunnistus kuvaavat molemmat verkkokalvon muotoja mutta siihen yhtäläisyydet loppuvatkin. Angiografia taltioi satoja väriaineen korostamia kuvia tietyn ajan kuluessa ja keskittyy tutkimaan verenkierron

yksityiskohtia koko verkkokalvon alueella. Verkkokalvotunnistusprosessi taltioi vain muutamia kuvia (yksi hyvä kuva on jo riittävä) ja kyseisessä menetelmässä ollaan kiinnostuneita vain suhteellisen pienestä alueesta koko kuvion informaatiosta, joka sijaitsee lähellä näköhermoa. Angiografia käyttää oranssia tai vihreää väriainetta, joka fyysisesti injektoidaan henkilön silmään ennen muita toimenpiteitä. Kyseinen väriaine vahvistaa ja korostaa verenkierron yksityiskohtia paljastaen mahdolliset verenvuodot tai rappeumatilat verkkokalvon kudoksessa. Verkkokalvotunnistus ei sisällä mitään vastaavia injektioita eikä väriaineiden käyttöä, ja käyttötapahtuman aikana otetaan vain nopeasti muutama kuva, joista niistäkin vain hyvin pientä osa-aluetta käytetään tunnistusprosessissa tai taltioidaan tietokantaan rekisteröitymisvaiheessa. Ainoana poikkeuksena verkkokalvon skannaus tunnistustarkoituksessa voi paljastaa vain ihmisen sokeuden, mutta ei mitään muuta ihmisen terveydentilaan liittyvää. Verkkokalvon ja värikalvon skannauksen sisäänkirjautumisvaatimusten vuoksi sokeat ihmiset eivät voisi näitä järjestelmiä käyttää muutenkaan. [1, s. 98.]

4.6 Käsiala- ja näppäimistödynamiikkatunnistus

Käsiala- ja näppäimistödynamiikkatunnistus ovat molemmat niin sanottua käyttäytymistapabiometriikkaa, koska ne mittaavat ja analysoivat sitä, kuinka ihminen tekee asioita – kuinka henkilö kirjoittaa henkilökohtaisen allekirjoituksensa tai kuinka henkilö kirjoittaa. Käsialadynamiikkatunnistus hyödyntää digitointilevyä allekirjoituksen taltioimiseksi elektronisesti niin, että laite samalla jäljittää kuinka allekirjoitus tehtiin. Näppäimistödynamiikka on biometrinen tunniste, joka perustuu ajoitukseen ja näppäinpainallusten välisiin viiveisiin. Tilastolliset ominaisuudet siitä kuinka me kirjoitamme ja erityisesti kuinka kirjoitamme tunnettuja sanoja (erityisesti salasanoja) tai lauseita on mitattavissa ja analysoitavissa. Nämä mitatut mallinteet ovat toistuvia ja niitä voidaan käyttää kohtuullisella tarkkuudella tekemään ero kahden henkilön välillä. Toisin kuin käsialadynamiikkatunnistus, (ja muu biometriikka) näppäimistö–dynamiikkatunnistus ei vaadi sensoreita tai muuta laitteistoa tavanomaisen näppäimistön lisäksi.

4.6.1 Käsialadynamiikkatunnistus

Käsialandynamiikkatunnistus tekniikkaa voidaan käyttää missä tahansa, missä perinteistä allekirjoitusta käytetään, kuten yritysten asiakirjoissa tai vaikka shekkien allekirjoituksissa. Tekniikkaa voidaan käyttää myös esimerkiksi varokeinona henkilöntunnistusmateriaalin kuten henkilökorttien, ajakorttien ja passien myöntämisessä ja niiden käytössä. Lisäksi allekirjoituksen tunnistusta voidaan käyttää vahvistamaan tunnistusprosessia ja näin vähentää petoksien määrää ja väärinkäyttöä elektronisissa kaupankäyntisovelluksissa. Tällaisiä sovelluksia ovat esimerkiksi tietokoneiden sisäänkirjautumiset, tiedostoihin ja erilaisiin dokumentteihin käsiksi pääsy, luottokorttien tilitapahtuman hyväksyminen, ja suuri joukko erilaisia myyntipiste sovelluksia. [1, s. 101.]

Allekirjoituksella on varsin huomattava maine ”sitovana” tunnisteena kulttuurissamme. Tavanomainen musteallekirjoitus sisältää lainmukaisen sitoumuksen henkilön tai yritysten tekemissä sopimuksissa. Henkilökohtaisia allekirjoituksia käytetään yleisimmin asiakirjojen hyväksymiseen tai laillistamiseen, kauppojen hyväksymiseen ja luottokorttien tilitapahtumien hyväksymiseen tai liittämään kyseinen henkilö virallisesti asiakirjaan. Allekirjoitus myös voi ilmaista jonkin asian alkuperän tai sen aitouden. Molemmat tuottavat hämmennystä ja kiistoja ja jopa unohtuvat, kun siirrytään elektronisen median maailmaan. Useat taiteilijat ovatkin huolestuneita digitaalisista ”leikkaa ja liimaa”-työkalujen tuomista mahdollisuuksista ja tämän kautta materiaalin kopioinnista. Kustantajat ovat luonnollisesti huolissaan tekijänoikeudellisen materiaalin kopioinnista ja sen levittämisestä täysin vapaasti. Siirtyminen digitaaliseen mediaan on monimutkainen prosessi ja digitoiduilla allekirjoituksilla saattaa hyvinkin olla tulevaisuudessa tärkeä rooli.

4.6.2 Käsialadynamiikkatunnistuksen toimintaperiaate

Käsialadynamiikkatunnistus toimii niin, että se ottaa huomioon joukon erilaisia osatekijöitä sisältäen allekirjoituksen molemmat peruspiirteet eli itse allekirjoituksen (lopullinen muuttumaton tuotos) ja yksityiskohdat kuinka allekirjoitus tehtiin (dynaaminen tapahtuma). Allekirjoitus itsessään sisältää geometria-, kaarevuus- ja muototietoa niin yksittäistä kirjaimista kuin kokonaisista sanoista. Kuinka allekirjoitus on tehty sisältää lisätietoa viivojen

piirtosuunnista, käytetystä nopeudesta, kynän nosto- ja laskutilanteista ja siitä, kuinka suurta voimaa on käytetty allekirjoituksen tuottamisessa. Turvallisuus–sovellutuksissa allekirjoitusanalyysin dynaamisia näkökohtia voidaan yhdistää tunnettuun salaiseen salasanaan näin tehden allekirjoituksen väärentämisestä entistä vaikeampaa. Käsinkirjoitetut allekirjoitukset taltioidaan elektronisesti digitointialustoilla ja piirtimellä. Monia kaupallisia allekirjoituslevyjä on jo saatavilla nykyisin, ja niitä onkin saatavilla erikokoisina, erilaisilla ominaisuuksilla, suorituskyvyltään erilaisina, ja osassa on lukuisia graafisia sovellutuksia pelkän elektronisen allekirjoituksen taltioimisen lisäksi. [1, s. 102.]

Interlinkin tuotteet vaihtelevat elektronisen allekirjoituksen taltioinnista niiden integroimiseen osaksi suosituimpia asiakirjaformaatteja ja näin osaksi yritysten tunnistusohjelmistoja ja -ratkaisuja.

Halvimpien Interlink electronicsin ePad-digitointilaitteiden kuten esim. kuvassa 18 oikealla olevan ePad II:n kosketusnäyttöjen tallennusresoluutio on 300 x 300 pixeliä per tuuma (ppi) ja näytteenottokyky vaihtelee välillä 100 – 400 kertaa per sekunti mallista riippuen. Keskihintaisten mallien kuten esim. kuvassa 18 vasemmalla olevan ePad I.D. pro II:n kosketusnäyttöjen tallennusresoluutio on 1200 x 1600 ppi ja näytteenottokyky on joko 100, 200 tai 400. Useimmissa ePad digitointilaitteissa on allekirjoituksen graafiselle esittämiselle yksivärinen graafinen näyttö, jonka tarkkuus on 320 x 240. Kalliin hintapään malleissa kuten kuvassa 18 keskellä olevassa ePad XL:ssä on yksi- tai vaihtoehtoisesti 16-värinen graafinen LCD näyttö, jonka tarkkuus on 320 x 240. Uusin ePad-malli ePad LS sisältää täysvärinäytön. Kalleimmat laitteet sisältävät mm. magneettikorttilukijan ja mahdollisuuden käyttää henkilökohtaista PIN-koodia. Epad-tuotteet tukevat 7 bitin (128 arvoa) paineherkkyyttä, joka on tärkeä osa allekirjoituksen toimintadynamiikkaa. Interlink electronicsin ePad-digitointialustojen avulla on mahdollista allekirjoittaa elektronisesti mm. Microsoft Word, Microsoft Excel ja Adobe Acrobat PDF-asiakirjoja.

Kuva 18. Interlink electronicsin ePad- digitointilaitteita

Isompia digitointialustoja, jotka on normaalisti suunnattu graafisiin sovelluksiin kuten luonnoslehtiökäyttöön, digitaalisten valokuvien muokkamiseen ja tietokoneavuisteiseen hahmotteluun, voidaan myöskin hyödyntää käsiala–dynamiikkatunnistusta. Wacom Technology Corporationin myymiä digitointi–levyjä on saatavilla useina eri kokoina ja erilaisin ominaisuuksin.

4.6.3 Käsialadynamiikkatunnistuksen toteutus

Nykyelektroniikka pystyy taltioimaan painetietoa ja näytteistämään 100 – 400 kertaa per sekunti. Perusmittoina allekirjoitusdynaamiikan analyysissä käytetään sijaintia, painetta ja aikaa.

Gupta ja Rick Joyce käyttivät kuutta piirrettä teknisten tutkimusten pohjana:

- kokonaisaika
- nopeuden muutosten määrä x-akselin suunnassa
- nopeuden muutosten määrä y-akselin suunnassa
- kiihtyvyyden muutosten määrä x-akselin suunnassa
- kiihtyvyyden muutosten määrä y-akselin suunnassa
- kynän ylhäällä olon kokonaisaika

Merkittävin päätelmä Guptan ja Joycen tutkimuksissa oli se, että heidän käyttämillään suhteellisen yksinkertaisilla piirteillä (jotka eivät sisältäneet painetta) pystyttiin erottamaan väärennökset. Vaikka heidän testinsä eivät olleet kovin laajoja, niin niihin kuitenkin osallistui vapaaehtoisia kokeneita väärentäjiä. Gupta ja Joyce huomasivat, että väärennettyjen piirteiden arvot erosivat niin

kokonaisajallisesti, kiihtyvyyden muutosten määrän suhteen, jäljen pituuden kuin kynän ylhäällä oloajan suhteen referenssiarvoista (aidosta). Keskihajonnassa oli 20:stä jopa 50:een eroa referenssiarvoon nähden. Toisin sanoen väärentäjät pystyivät väärentämään itse allekirjoituksen varsin tarkasti, mutta he eivät onnistuneet jäljentämään tapaa, jolla alkuperäinen allekirjoitus oli tehty. [1, s. 105.]

Muitakin yksityiskohtaisiin muuttujiin perustuvia menetelmiä on esitetty ja sovellettu käytännössä. Crane ja Ostrem (1983) ehdottivat 44 piirteen sarjaa käytettäväksi, mutta useiden testien jälkeen he vähensivät määrän 23 parhaaseen piirteeseen. He huomasivat että samoihin piirteisiin keskittyminen ei toimisi jokaisen käyttäjän kohdalla, ja he ehdottivat että piirteet voitaisiin kerätä harjoitusnäytteiden avulla ja siten yksilöllistää piirrevalikoima niin, että täsmäyksessä käyttetäisiin vain sopivimpia ja yksilöllisimpiä piirteitä jokaisen henkilön kohdalla. [1, s. 105.]

Automaattiselle käsialan tunnistukselle löytyy omat varsin lupaavat markkinat yritysmaailmassa: Asiakirjojen allekirjoittaminen ja hyväksyminen, laskutuksessa ja kaupankäynnissä. Lisäksi tekniikkaa voidaan käyttää myös esimerkiksi tietokoneissa pääsynhallinassa. Cyber SIGN joka perustettiin vuonna 1977 CADIX:n tytäryhtiöksi markkinoi edullisia pääsynhallintaan tarkoitettuja näytönsäästäjiä, joiden mukana tulee Wacomin digitointilevy. Muita Cyber SIGN:n tuotteita on asiakirjojen allekirjoitusten plug-in-tekniikka ja serveripohjaisia ratkaisuja laajempiin verkkojärjestelmiin.

4.6.4 Näppäimistödynamiikkatunnistus

Toisin kuin muu biometriikka, niin näppäimistödynamiikkatunnistus ei vaadi erikoisilmaisinlaitteistoa tavallisen näppäimistön lisäksi. Käyttäjän näppäinpainallusten dynamiikka taltioidaan täysin ohjelmallisesti ja täten menetelmää voidaan periaatteessa käyttää missä tahansa järjestelmässä, jossa käytetään näppäimistöä.

Näppäimistödynamiikkaa voidaan käyttää yksittäisissä tunnistustilanteissa tai jatkuvassa valvonnassa. Jatkuvaa valvontaa ei käytetä normaaleissa kaupallisissa biometrisissä sovelluksissa, mutta on ehdotettu, että sitä voitaisiin

käyttää tulevaisuudessa valvomattomilla työpisteillä estämään luvatonta käyttöä. Esimerkiksi jos hyväksytty luvallinen käyttäjä lähtee pois työpisteeltään ja toinen käyttäjä yrittää käyttää hänen valvomatonta työpistettään, niin pystyttäisiin huomaamaan muutos näppäimistödynamiikassa. Toisen käyttäjän läsnäolo pystyttäisiin tunnistamaan poikkeavan kirjoitustavan avulla (joka voidaan tulkita luvattomaksi käyttäjäksi tietyissä käyttöympäristöissä ja järjestelmissä) ja järjestelmä voisi lukita järjestelmän ja vaatia uudelleen sisäänkirjautumista.

Näppäimistödynamiikan valvonta on yksinkertainen, mutta helppo tapa kirjata käyttäjän jokainen näppäimen painallus. Menetelmän mahdollinen väärinkäyttö on herättänyt paljon keskustelua, mutta menetelmää kuitenkin käytetään tietoturvainformaation saamiseksi tietyissä ympäristöissä. Kyseiset järjestelmät tulisi merkitä selkeästi, niin että käyttäjä tietää olevansa valvonnan alainen. Rikollinen tapa käyttää hyödyksi näppäimistödynamiikan valvontamenetelmää on niin sanotut spyware-ohjelmat, jotka on suunniteltu toisten käyttäjien salakuuntelua varten. Spyware-ohjelma voi tallentaa tai kaapata tietoa työ-, e-mail- tai keskusteluistunnoista ja tietysti salasanoja. Spyware on halpa, helppokäyttöinen ja toisen käyttäjän koneeseen asennettuna erittäin tunkeileva.

4.6.5 Näppäimistödynamiikkatunnistuksen sovelluksia

Luonteenomaisin käyttösovellus näppäimistödynamiikan tunnistukselle on tehdä salasanoista entistä turvallisempia. Näppäimistödynamiikkaa käytetään jo olemassa olevien salasanojen kanssa niin, että salasana tulee syöttää kyseiselle käyttäjälle tyypillisellä tavalla. Menetelmä on varsin yksinkertainen ja helppo ottaa käyttöön. Kustannuksiltaan kyseessä on myös yksi halvimmista biometrisistä tunnisteista, koska lisälaitteita ei tarvita ja itse ohjelmat ovat suhteellisen halpoja.

Menetelmän heikkous on, että ei ole aina niin helppoa määritellä turvaratkaisun hyötyjä kustannuksiin nähden eikä mahdollisia tilanteita, joissa käyttöoikeudet evätään valtuutetuilta henkilöiltä. Tietty prosentti valtuutetuista käyttäjistä hylätään, koska he ovat väsyneitä, sairaana, stressaantuneita, heillä on jokin vamma tai jokin muu syy, jonka vuoksi he painavat näppäimiä eri tavalla kuin normaalisti. Kaikesta huolimatta näppäimistödynamiikan tunnistus on hyvä lisä perinteisiin turvajärjestelmiin joko käyttäjän itsensä valittavissa olevana

vaihtoehtona tai osana yritysten turvaratkaisuja. Lähitulevaisuudessa käyttöjärjestelmien valmistajat saattavat sisällyttää näppäimistödynamiikan tunnistuksen osaksi käyttöjärjestelmää nykyisten salasanojen lisäksi.

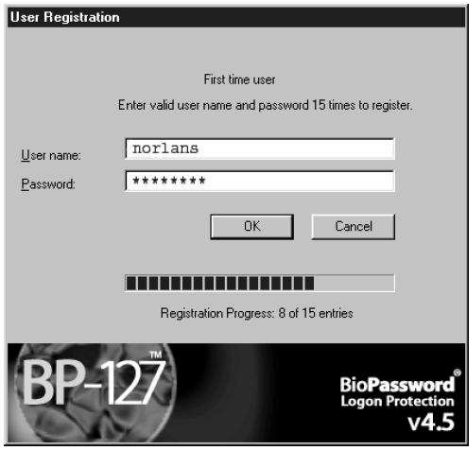
Nykyisin salasanoista pyritään tekemään turvallisempia kehottamalla tai pakottamalla henkilöitä valitsemaan salasanansa seuraavan kaltaisten ehtojen mukaisesti:

- salasanan tulee olla vähintään 6 merkkiä pitkä
- salasanan tulee sisältää vähintään 1 erikoismerkki (ei aakkosellinen)
- salasana ei saa muodostua sanoista tai olla sana
- sanasana tulee vaihtaa säännöllisesti
- salasanaa vaihtaessa tulee uuden salasanan erota aiemmin käytetyistä salasanoista.

Nämä ehdot pakottavat käyttäjät valitsemaan salasanat niin, että niitä olisi mahdollisimman vaikea arvata, mutta samalla kasvaa todennäköisyys, että käyttäjä unohtaa oman salasanansa. Tyypillinen käyttäjä myös reagoi salasanojen vaihtoihin valitsemalla seuraavan salasanansa hyvin samankaltaisin valintaperustein kuin oli valinnut alkuperäisen, koska näin käyttäjän on helpompi muistaa uusi salasana. Perinteinen salasanasuoja on taakkana järjestelmän ylläpitäjälle ja käyttäjille. Joissakin tilanteissa todellisia hyötyjä ja haittoja on vaikea arvioida. Esimerkiksi salasanan päätyessä vääriin käsiin se vaihdetaan uuteen salasanaan, mistä on todellista hyötyä, mutta on vaikea arvioida hyötyjä ja haittoja, kun kaikkien käyttäjien tulee vaihtaa salasanansa tietyin ennalta määrätyin ajanjaksoin. Tämän kaltaiset operaatiot lisäävät järjestelmän ylläpitäjien työmäärää unohtuneiden salasanojen ja lukkiutuneiden käyttäjätilien muodossa. Sen sijaan biometrinen salasanan vahvennus tarjoaa ylimääräisen turvatason perinteisen salasanasuojan lisäksi, ja mikä tärkeintä turvallisuus saavutetaan ilman, että käyttäjille muodostuisi ylimääräistä taakkaa. [1, s. 108.]

Vaikka useita tutkimusprototyyppejä on kehitetty, tutkittu ja testattu, niin BioPassword vaikuttaisi olevan yksi harvoista kaupallisista sovelluksista. BioPasswordin omistaa Net Nanny Inc., ja se on osa Net Nanny Internet-turvaohjelmistoa (suodatus- ja tietoturvaohjelmisto). BioPassword-ohjelmistoa on lisensoinut mm. Musicrypt.com, joka toimii digitaalisen musiikin myyjänä

verkossa. Tietokantaan rekisteröityessään käyttäjän tulee kirjoittaa 15 harjoitusnäytettä haluamastaan salasanasta kuvan 19 mukaisessa ikkunassa.



Kuva 19. BioPassword-ohjelmiston rekisteröintiikkuna. *Käyttäjän tulee antaa ohjelmalle 15 harjoitusnäytettä, joiden pohjalta ohjelmisto luo mallinteen. [1, s. 109]*

BioPasswordin tunnistuksen raja-arvoa voi säätää tiukaksi tai vapaammaksi, jolloin arvo 10 vastaa kaikkein tiukinta asetusta ja arvo 1 vastaa kaikkein anteeksiantavinta asetusta (kuva 20). Näppäimistödynamiikkatunnistus vaatii useita ajoitusnäytteitä, joista se muodostaa tunnistettavan mallinteen. BioPassword-ohjelmisto vaatii myöskin 8 merkkiä pitkän salasanan käytön.

Kuva 20. BioPassword-ohjelmiston konfigurointivalikko. *Valikossa voi mm. poistaa käyttäjätilejä ja muokata tunnistustarkkuuden tasoa. Suurempi tarkkuus lisää epäonnistuneiden kirjautumisten määrää, mutta vähentää väärin hyväksyttyjen määrää.*

Puolueettomia testejä kaupallisten näppäimistödynamiikan tunnistussovelluksien suorituskyvystä ei tiettävästi ole julkaistu, mutta kuten Ordin ja Furnellin tekemässä yhteenvedossa (taulukko 4) on esitetty, sovelluksien suorituskyvyissä on huomattavissa suuria eroja. (Ord & Furnell 1999, 2). [1, s.110.]

Taulukko 4. Ordin ja Furnellin tekemä yhteenveto näppäimistödynamiikan sovelluksien suorituskykyä arvioivissa tutkimuksista

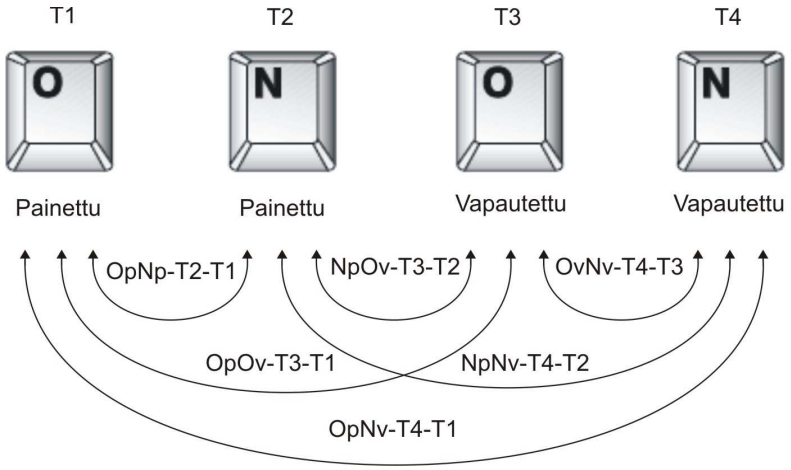
Laatija	**FAR**	**FRR**
Gaines et al. (1980)	0 %	4 %
Legget & Williams (1988)	5 %	5.5 %
Joyce & Gupta (1990)	0.25 %	16.67 %
Bleha et al. (1990)	2.8 %	8.1 %

Virheprosentit kertovat tehtyjen oletusten, käytetyn testidatan ja testimenetelmien eroista eivätkä täten tarkoita, että Gainesin käyttämä menetelmä olisi tarkempi kuin muiden tutkijoiden. Gainesin tutkimus keskittyi itse menetelmään ja sen analysointiin. Hänen testinsä koostui kuudesta ammattikirjurista ja kolmesta valmiista kokosivun tekstistä, joista hän keräsi tietoa samantapaisesti kuin konekirjoitustestissä, kun taas kolme muuta mainittua tutkimusta keskittyivät analysoimaan yksittäisiä salasanoja. [1, s.110.]

Kuten kaikessa käyttäymismalleihin perustuvassa biometriikassa käyttäjän mielentila ja hänen ympäristönsä olosuhteet vaikuttavat tuloksiin. Käyttäjän mielentilaan vaikuttavia tekijöitä ovat esimerkiksi stressi, lepo ja mieltä vaivaavat häiriötekijät. Ympäristöllisiä tekijöitä ovat esimerkiksi käyttäjän asento, kulloinkin käytettävissä oleva laitteisto (kannettava tietokone, pöytätietokone), näppäimistön muoto, kokemus ja tekniikan tuntemus. Näppäimistön muoto ja asento, kuten myös näppäinten koko ja sijoittelu vaikuttavat useimpien henkilöiden kohdalla heidän yksilölliseen mallinteeseensa ja sen toistettavuuteen.

4.6.6 Näppäimistödynamiikan digraafiesitys

Varsinaisia ajoitusjälkiä joita käytetään mallinteiden täsmäyksessä esitetään monin eri tavoin, mutta yleisin tapa on esittää ne digraafisarjoina. Digraafi on kahden peräkkäisen merkin muodostama pari kirjoitusjonossa. Digraafista laskettava viive on ensimmäisen näppäinpainalluksen ja toisen näppäinpainalluksen välinen aika. Vaihtoehtoiset mittaukset ovat mahdollisia, ja kuten kuvasta 21 näkyy, niin digraafille syntyy kuusi vaihtoehtoista mittausta.



Kuva 21. Digraafin viive sanalle ”on”

Digraafien lisäksi merkkijonoja ja sanoja voidaan esittää trigraafeina ja tulevaisuudessa mahdollisesti jopa tetragraafeina. Kaupallisissa näppäimistödynamiikan tunnistussovelluksissa trigraafimenetelmä ei tiettävästi vielä ole käytössä, mutta useita lupaavia tutkimuksia sen käytöstä on tehty. Trigraafi on kolmen peräkkäisen merkin muodostama joukko kirjoitusjonossa. Trigraafista laskettava viive on ensimmäisen ja kolmannen painalluksen välinen aika.

Tieto koostuu aikaleimataulukosta, joka sisältää näppäin alhaalla ja näppäin ylhäällä tapahtumia. Piirteet ilmaistaan painallusviiveenä (aika joka kuluu kun näppäin on painuksissa) ja siirtymäaikana (aika joka kuluu kahden näppäimen painalluksen välillä) eri digraafeille. Vaikka useimmat järjestelmät perustuvat samaan ideaan, niin näppäimistödynamiikan tunnistukselle ei vielä ole kehitetty yhtenäistä standardia. Tämän vuoksi osa järjestelmistä tulkitseekin osan

näppäinpainalluksista hieman eri tavoin. Esimerkiksi osa valmistajista jättää huomioimatta erikoisnäppäimet kuten shift, space ja enter, kun taas toiset eivät.

Näppäimistödynamiikkatunnistusta on myös tutkittu ja testattu käytettäväksi numeerisissa näppäimistöissä. Kyseisillä järjestelmillä olisi huomattavan suuri markkina-alue erilaisten puhelin-, raha-automaatti-, kassakone- ja näppäinlukkojärjestelmien muodossa. Ihmiset usein näppäilevät numeerisia näppäimistöjä käyttäen vain yhtä kättä, eikä se siis sisällä samaa neuromuskulaarista tietoa, jonka ihminen välittää kirjoittaessaan esimerkiksi kahdella kädellä tietokoneen näppäimistöllä.

2000-luvun alkupuolella tehtiin tutkimus näppäimistödynamiikkatunnistuksen käytöstä numeerisissa näppäimistöissä. Tutkimuksessa testattiin 6- ja 11-numeroisen PIN-koodin käyttöä 14 henkilön voimin. Testissä käytettiin kolmea menetelmää tietojen käsittelemiseksi: neuroverkko, pienin etäisyys ja mahalanobisin etäisyys. Testissä neuroverkkojen käyttö tuotti parhaimmat tulokset, mutta väärien hyväksyntöjen määrä oli 9.9 %, kun väärien hylkäysten määräksi oli valittu 30 % (oletettu ihmisen sietokyvyn raja-arvo tulla hylätyksi väärin perustein). 11-numeroisen PIN-koodin testitulokset olivat hiukan paremmat kuin mitä 6-numeroisella PIN-koodilla saavutettiin, mutta numeromäärän kasvaessa koodien muistaminen vaikeutuu ja virheiden määrä kasvaa. [1, s. 112]

Virheprosentit ovat liian suuria, jotta näppäimistötunnistusta voitaisiin käyttää pankkiautomaateissa tai puhelinjärjestelmissä. Oletetun 30 hylkäysprosentin kohdalla väärien hyväksyntöjen määrä oli 9,9 % joka tarkoittaisi sitä, että jos PIN-koodi varastettaisiin, niin järjestelmä hyväksyisi PIN koodin käytön kerran 10:stä yrityksestä. Korkean väärin hylättyjen yritysten prosentin vuoksi täytyisi sallia useampia yrityksiä, mikä olisi vain haitaksi luvallisille käyttäjille, eikä estäisi luvatonta käyttöä.

4.7 Tulevaisuuden biometriset menetelmät

Aiemmin mainitut biometriset tunnisteet ovat yleisesti jo käytössä olevia ratkaisuja tai kaupallisesti toteuttamiskelpoisia ja ovat näin ollen ns. valtavirta–biometriikkaa. On olemassa myös joukko biometrisiä menetelmiä, jotka ovat vielä kokeellisella tasolla ja kehitystyön alla.

Koska kyseiset menetelmät ovat yhä kokeellisia ja niistä on varsin vähän luotettavaa tietoa saatavilla, niin seuraavassa osiossa käydään osa näistä esoteerisen biometriikan tunnetuimmista menetelmistä vain lyhyesti läpi.

4.7.1 Verisuonikuviotunnistus

Pääasiallisesti kyseessä on kämmenselän verisuonikuvion mittaus. Näiden verisuonikuvioiden uskotaan muodostuvan jo ennen syntymää, ja jopa identtisten kaksosten verisuonikuviot eroavat toisistaan. Verisuonikuvio säilyy samanlaisena syntymästä aikuisikään asti sen kokoa lukuun ottamatta.

Infrapunakameraa käyttäen verisuonikuvio voidaan taltioida ja kuva digitoida, minkä jälkeen kuva muunnetaan binääriseksi mallinteeksi joka vie vain noin 300 tavua. Tunnistusmenetelmiä on kahden tyyppisiä: toisessa verrataan keskenään verisuonten solmukohtia suuntavektorien avulla ja toisessa menetelmässä verisuonikuvioiden tärkeimmät alueet esitetään hieman kuten viivakoodi.

Kämmenselän verisuonikuvion hyviä puolia on että se on yleinen, muuttumaton ja luotettava läpi ihmisen eliniän, sitä on lähes mahdoton naamioida ja muuttaa, mittaustapahtuma ei ole tunkeileva ja ruumin sisäisenä ja ihon suojaamana ominaisuutena se ei ole niin altis vahingolle kuin useimmat muut biometriset ominaisuudet. Lisäksi kaupallisia sovelluksia on jo saatavilla. [1, s. 116; 6, s. 76.]

Verisuonikuvioiden tunnistuksen huonoja puolia on, että infrapunakamerat ovat vielä suhteellisen kalliita. Lisäksi päihteet, kuntoilu ja henkilön terveydentila vaikuttavat verenkiertoon näin heikentäen verisuonikuvioiden tunnistamista ja täsmäystä.

Koska kyseinen menetelmä on kilpaileva menetelmä sormenjälkien-, kämmengeometrian- ja muiden tämän kaltaisten biometristen tunnistus–menetelmien kanssa, niin kilpailun sijaan sillä voisi olla parempi tulevaisuus, jos sitä käytettäisiin nykyisten menetelmien kanssa yhdessä. Kämmenselän verisuonikuvion tunnistus voitaisiin liittää osaksi kämmengeometrian tunnistusmenetelmää, jolloin järjestelmä pystyisi myös vahvistamaan kämmenen elollisuuden.

4.7.2 Kasvojen termografia

Kasvojen termografia mittaa kasvojemme lämpöjälkeä, jonka verenkiertomme synnyttää. Infrapunakamerat voivat taltioida tämän lämpöjäljen ja sitä analysoimalla saamme anatomista tietoa, jonka voimme sen jälkeen muuntaa mallinteeksi.

Infrapunakuva on yksilöllinen, koska jokaisen ihmisen kudos ja verisuonirakenne on yksilöllinen. Menetelmän toiminta perustuukin juuri siihen, että vaikka ihmisen kudos- ja verisuonirakenne on muuttumaton niin verenkierron dynaaminen luonne aiheuttaa poikkeamia ja vaihtelua.

Termografian avulla on mahdollista tunnistaa, onko henkilö levännyt vai uupunut, onko hän elossa vai kuollut, hermostunut vai rauhallinen tai esimerkiksi päihteiden vaikutuksen alainen.
Infrapunakuvausta ja kasvojen termografiaa on testattu vielä varsin vähän. Kunnollisten testien tekeminen onkin kallista ja monimutkaista, koska kaupallisia sovelluksia ei juurikaan ole saatavilla ja testeissä tulee ottaa huomioon sellaisia asioita kuin toimintaympäristön lämpötila ja henkilön aineenvaihdunta. [1, s. 117; 6, s. 79.]

Menetelmän suurin ongelma lienee kansan hyväksyntä. Syynä tälle on se että kasvojen termografia voi paljastaa informaatiota henkilön terveydentilasta ja kunnosta, kuten esimerkiksi hengitystiheyden, sydämen lyontitiheyden, mahdolliset tulehdukset, sisäisen verenvuodon, turvotuksen, luun murtumat. Toisinaan kyseisestä informaatiosta on hyötyä ja se on jopa toivottua, mutta useimmat ihmiset kuitenkin voivat pitää tätä liian tunkeilevana, koska termografia voisi paljastaa henkilön yksityisiä asioita tahoille, joille ne eivät

kuulu, ja näin vaikuttaa siihen, miten heihin suhtaudutaan ihmisenä ja työntekijänä.

Toisaalta kasvojen termografian hyvä ja huono puoli verrattuna muuhun biometriikkaan on juuri se, että se paljastaa henkilön terveydentilaan liittyvää informaatiota. Kontrolloiduissa olosuhteissa käytettynä kasvojen termografia voi myös paljastaa henkilön päihteiden käytön. Molemmista ominaisuuksista voisi olla huomattavaakin hyötyä sellaisissa olosuhteissa, joissa on hyvä tietää henkilöllisyyden lisäksi myös terveydentila ja mahdollisten päihteiden käyttö. Näin voitaisiin varmistaa, että esimerkiksi kirurgit, lentäjät ja bussikuskit, poliisiviranomaiset ja palomiehet ovat terveitä ja hyvässä kunnossa ja etteivät he tule töihin päihtyneenä.

Termografian hyvä puoli on myös että infrapunakameroiden toimintaan ei vaikuta näkyvä valo (400 – 700 nanometriä). Näin sitä voidaan käyttää pimeässä ja päivänvalossa, kunhan tietyt ongelmat suunnattujen valonlähteiden suhteen pystytään ratkaisemaan. Termografia sopiikin valvontajärjestelmiin erinomaisesti juuri sen vuoksi, että se toimii erittäin hyvin yöllä tai muuten hämärissä olosuhteissa. Tätä ominaisuutta vahvistaa entisestään se, että naamioinnista ja valeasuista ei ole hyötyä. Kasvojen termografian voisi uskoa kiinnostavan sotilaallisia ja muita korkeaa turvaluokitusta tarvitsevia tahoja osana heidän valvontajärjestelmiään.

4.7.3 DNA-profilointi

DNA eli deoksiribonukleiinihappo sisältää kaikkien eliöiden solujen geneettisen materiaalin, ja geenissä sarja DNA:n nukleotideja muodostaa ohjeen proteiinin valmistamiseen. Henkilön DNA:n kemiallinen rakenne sisältää informaatiota yksilön perinnöllisistä ominaisuuksista.

Toukokuussa 2002 Australian Institute of Criminologyn tekemä julkaisu DNA Identification in the Criminal Justice System kuvaa DNA:ta näin:

"Ihmisen solun DNA on yksilöllinen. Se on seksuaalisen lisääntymisen tuote, jossa yhdistyy puoliksi äidin ja puoliksi isän DNA. Yksilön ruumiissa jokainen solu on solujen jakautumisen tulos, joka kopioi juuri hedelmöitetyn solun DNA:n jokaiseen nukleiinisoluun. Tuloksena tuman DNA on sama kaikkialla ihmisessä mutta erilainen kahden henkilön välillä tehden siitä näin ollen luonnollisen vaihtoehdon yksilön tunnistamiseksi, kuten nimi tai henkilötunnus. Huomattava poikkeavuus on identtiset kaksoset, jotka kehittyvät yhdestä hedelmöittyneestä solusta ja täten omaavat identtisen DNA:n." [1, s. 120.]

Alec Jeffreys ja hänen kollegansa demonstroivat vuonna 1985 DNA:n käyttöä osana rikostutkintaa. Nykyisin DNA on yleisesti hyväksytty ja tunnustettu erittäin luotettava tunniste niin tiedeyhteisöissä, laissa kuin myös kansan keskuudessa. Poliisiviranomaiset käyttävätkin nykyisin DNA:ta säännöllisesti USA:ssa, Iso-Britaniassa ja muualla maailmassa rikostutkimuksissaan, tai vaihtoehtoisesti lapsen isyys tai ihmisen henkilöllisyys voidaan varmistaa DNA-tutkimuksella. DNA-täsmäysprosessista käytetään usein nimitystä ”DNA:n profilointi”. [1, s. 120.]

Nykyisin DNA-tutkimukset ovat suhteellisen kalliita ja aikaa vieviä, mikä tekee niistä varsin epäkelpoja automaattisoituihin tunnistus- ja varmennus sovelluksiin. DNA-tutkimuksilla voidaan myös saada tietoa henkilön mahdollisista sairauksista ja perinnöllisistä ominaisuuksista. Tämä luonnollisesti herättää kysymyksiä ihmisen yksityisyydensuojan kunnioittamisesta ja siitä, miten ihmisen yksityiselämä voidaan turvata mahdollisilta väärinkäytöiltä. Poliisiviranomaisten järjestelmät kuten CODIS (Combined DNA Index System) käyttävätkin tästä syystä DNA:n niin sanottua ”roska DNA”-osaa, joka on se osa DNA:sta, mikä ei sisällä tiettävästi mitään lääketietteellistä tietoa ihmisestä.

DNA ei kuitenkaan ole varsinainen biometrinen tunniste, vaikka sen avulla voidaankin tunnistaa yksilö hyvin suurella tarkkuudella. Tähän syynä on se, että ei ole olemassa automatisoituja menetelmiä tai järjestelmiä, jotka mahdollistaisivat ihmisen tunnistamisen DNA:sta. DNA-tutkimus on epämiellyttävä ja tunkeileva, koska sen tekeminen vaatii kudos-, veri- tai jonkin

muun ruumiillisen näytteen. Kyseisiä näitteitä on lähes mahdoton esittää automatisoiduille tunnistusjärjestelmille ja muutenkin ajatus biometrisestä sylkykuppitunnistimesta on täysin absurdi. Tässä suhteessa DNA-profilointi eroaakin siis kaikista muista biometrisistä tunnisteista, koska siinä verrataan ihmisestä otettuja varsinaisia näytteitä keskenään, kun taas muut menetelmät perustuvat mallinteen käyttöön. [1, s. 120; 6, s. 75.]

Vaikka sivuuttaisimme DNA-profiloinnin nykyiset ongelmat, kuten käyttäjien hyväksynnän, hinnan, tunnistustapahtuman keston, sekä käytännöllisten sensorien, menetelmien ja järjestelmien puutteen, niin DNA-profiloinnin käyttäminen useimmissa arkisissa tapauksissa olisi liioiteltua. Tulevaisuudessa menetelmien ja tekniikan kehittyessä (erityisesti sensorien suhteen) DNA tunnistuksesta kehittyy niin sanotuttu oikea ja erittäin tarkka automaattinen biometrinen tunnistusmenetelmä.

4.7.4 Hikihuokosanalyysi

Sormenjäljet joita jätämme esineisiin ja paikkoihin johtuvat osin jatkuvasta hienerityksestä sormiemme hikihuokosissa ja osin liasta ja rasvasta, jota kertyy kun koskemme sormillamme muita ruuminosia tai erilaisia esineitä ja pintoja. Sormissamme olevasta kosteus- ja rasvakerroksesta siirtyy osa esineisiin näin jättäen papillääriharjanteiden muodostaman kuvion kosketettuun pintaan. Tämän tyypin sormenjälkeä kutsutaan latentiksi sormenjäljeksi.

Hikihuokosten käyttö biometrisenä tunnisteena perustuu oletukseen, että niiden esiintymisalue on yksilöllinen jokaisella ihmisellä ja niiden sijainti pysyy muuttumattomana koko ihmisen eliniän. Kyseessä on kuitenkin oletus, koska hikihuokosten esiintymisalueen yksilöllisyydestä ei ole vielä tehty kunnon tutkimusta, joka todistaisi että tämä oletus on tosi.

Hikihuokosten tunnistus on hyvin samankaltainen tapahtuma kuin sormenjälkien tunnistus. Sormi asetetaan ilmaisimen päälle, jolloin tietokone tallentaa havaittujen hikihuokosten sijainnin sormenmuotoon nähden. Tämän jälkeen erillinen ohjelma muuntaa taltioidun kuvan binääriseen muotoon, minkä jälkeen se digitoidaan ja taltioidaan mallinteeksi. Tätä mallinnetta voidaan myöhemmin käyttää tunnistuksen vertailukohtana.

Tapahtuma ei ole erityisen tunkeileva eikä epämiellyttävä, mutta menetelmä kärsii hyvin samankaltaisista ongelmista kuin sormenjälkitunnistus kuten esimerkiksi siitä, että se on sopimaton likaisissa käyttöympäristöissä. Menetelmän toimivuus ei myöskään ole vielä riittävän hyvä. Hikihuokosten muodostaman kuvion taltiointi ei aina onnistu, koska taltioiduissa kuvissa on liian pieni resoluutio. Kyseinen ongelma johtuu siitä, että skannerit jotka on suunniteltu taltioimaan sormenjälkiä eivät mahdollista suurempien resoluutioden käyttöä, jotta taltioidusta kuvasta voitaisiin paikantaa hikihuokoset. [1, s. 123; 6, s. 80.]

Hikihuokosten tunnistuksen käyttäminen biometrisenä tunnisteena on varsin epätodennäköistä, mutta sen soveltaminen osana muita jo olemassa olevia tunnistusmenetelmiä on lupaava. Hikihuokosten tunnistuksen käyttö osana sormenjälkien tai kämmengeometrian tunnistusta parantaisi molempien menetelmien tunnistustarkkuutta useampien tunnistettavien piirteiden muodossa ja lisäisi molempiin menetelmiin aitouden varmennuksen (liveness test), joka onkin nykyisin polttava kysymys biometriikan alalla.

4.7.5 Kädenpuristustunnistus

Ihmiset tunnetusti kättelevät eri tavoin ja kädenpuristus biometrisenä tunnisteena perustuukin oletukseen, että jokaisella henkilöllä on yksilöllinen kädenpuristus. On olemassa kaksi tapaa lähestyä kyseistä biometristä menetelmää.

Ensimmäinen tapa on käyttää infrapunavaloa ihonalaisen kudoksen ja käden verisuonikuvion valaisemiseksi ja analysoimiseksi, kun se on puristetussa asennossa. Laitevalmistaja Advanced Biometrics Inc:n mukaan noin 3 mm ihon alla sijaitsevat ihonalaiset verisuonikuviot ovat yksilölliset jokaisella henkilöllä. Nämä verisuonikuviot analysoidaan ja tuon informaation avulla luodaan henkilön kädelle yksilöllinen ”allekirjoitus”, jonka jälkeen tuo allekirjoitus muunnetaan mallinteeksi. Kyseistä mallinnetta käytetään tämän jälkeen vertailukuvana aina, kun halutaan varmistaa ihmisen henkilöllisyys. [1, s. 124.]

Toinen tapa on mitata puristusvoimaa ja sitä, kuinka tuo voima jakautuu esinettä puristaessa. Ihmisen kämmenessä on 19 luuta, 19 niveltä ja 20 lihasta, jotka tarjoavat varteenotettavan määrän sormien hermofysiologista kontrollointia ja kämmenen- ja ranteenliikkeitä, joiden avulla on mahdollista tehdä ero eri käyttäjien välillä. Paineanturi taltioi ja digitoi yksilöllisen jäljen ja luo sen avulla mallinteen. [1, s. 124.]

Samoin kuin muissakaan yhä kehitysasteella olevista biometrisistä menetelmistä niin kädenpuristuksen tunnistuksen yksilöllisyydestä ei ole tehty kattavaa tutkimusta, joka tukisi tehtyjä oletuksia. Menetelmän suorituskykyyn kuitenkin voidaan olettaa vaikuttavan ympäristön lämpötila ja käyttäjän yleinen hyvinvointi, jotka molemmat vaikuttavat infrapunailmaisinlaitteiden toimintaan. Voidaan myös varmuudella olettaa, että henkilön ikä ja terveydentila, kuten lihassurkastumat, vaikuttavat olennaisesti siihen, kuinka henkilö tarttuu ja puristaa esineitä. [1, s. 124.]

Toiminnaltaan menetelmä ei ole epämiellyttävä eikä tunkeileva, mutta menetelmää saatetaan vieroksua ja se voi olla epäsuosittu sellaisissa maissa, joissa kättely ei ole yleistä kuten tietyissä Aasian maissa.

Tutkijat ovat kiinnostuneet menetelmästä ja pyrkivät kehittämään niin sanottuja älyesineitä, jotka kykenisivät tunnistamaan omistajan tai luvallisen käyttäjän tämän kädenpuristuksesta. Mahdollisia käyttökohteita voisi olla esimerkiksi lentokoneiden ohjaimet, erilaiset ajoneuvot, tuliaseet ja asejärjestelmät.

New Jersey Institute of Technologylla (NJIT) tutkitaankin kädenpuristuksen tunnistuksen käyttöä osana aseen valmistusta. NJIT:n tutkimus on keskittynyt kolmeen tehtävään parhaiten sopivaan vaihtoehtoon:

- sormenjäljen tunnistus joka taltiodaan normaalista otteesta aseesta
- staattinen kädenpuristus, kämmenen ominaisuuksien mittaus
- dynaaminen puristuksen tunnistus, tapa jolla ampuja puristaa aseen kahvaa juuri ennen laukausta.

Luonnollinen käyttökohde menetelmälle on ovissa, kahvoissa ja muissa kädessä pideltävissä esineissä.

4.7.6 Kynnenaluskuviotunnistus

Kynnen alla olevat yhdensuuntaiset viivat muodostavat yksilöllisen pituussuuntaisen ponttiliitosrakenteen, joka koostuu nystyjen ja ihon rypyistä, jotka ovat asettuneet rinnakkaisiksi riveiksi ikään kuin ne muodostaisivat henkilölle yksilöllisen viivakoodin. Nämä viivat toimivat kynnenalustunnistus–tutkimuksen ja kehitysprojektien pohjana. Menetelmän perusolettamus on, että kyseinen kuvio pysyy muuttumattomana henkilön koko eliniän. Täytyy kuitenkin huomioida se tosiasia, että kynsi ja siten myös kynnenalunen voi altistua kemikaaleille tai vaurioitua näin mahdollisesti vaikuttaen kyseisen kuvion sitkeyteen. Tähän päivään mennessä ei ole olemassa luotettavaa empiiristä tutkimusta, joka tukisi väitteitä että kynnenalusen tunnistus voitaisiin mieltää biometriseksi tunnisteeksi. [1, s. 126; 6, s. 80.]

Valmistajat väittävät menetelmän olevan suhteellisen yksinkertainen ja näin se ei vaatisi runsaasti resursseja tietokoneelta. Jos kyseinen väittämä pitää paikkansa, niin menetelmä voisi olla ideaalinen pieniin kannettaviin laitteisiin kuten PDA, kännykkä tai ase. Tällä hetkellä ei kuitenkaan löydy kaupallisia tuotteita, jotka hyödyntäisivät kyseistä menetelmää.

4.7.7 Ominaishajutunnistus

Vainukoiria on käytetty kautta historian ihmisten jäljittämiseen. Koirien hajuaisti on mahdollistanut henkilön yksilöllisen ominaishajun jättämien jälkien seuraamisen. Jokaisen ihmisen tuoksu koostuu noin 30:stä kemiallisesta aineksesta. Menetelmän perusajatuksena on kehittää elektroninen järjestelmä, jossa ilmaisimet pystyisivät aistimaan joukon erilaisia kemiallisia aineksia, jotka synnyttäisivät ilmaisimissa tietyn jännite-eron tietyn aineen ollessa kyseessä. Tämän jälkeen käyttäen hyväksi neuroverkkoja voitaisiin tehdä ero tiettyjen tuoksujen välillä ja luoda mallikuvio, jonka avulla yksilö tai tietty tuoksu voidaan tunnistaa. [1, s. 126.]

Kemialliset ilmaisimet toimivat molekyylitasolla ja ovat varsin tarkkoja, mutta ne eivät vielä kuitenkaan kykene samaan kuin oikea hajuaisti. Tämän vuoksi näitä ilmaisimia on yhä helppo huijata esimerkiksi peittäen etsitty aines suurilla pitoisuuksilla jotain muuta ainesta. [1, s. 126.]

Ominaishajuun vaikuttaa ruokavalio ja henkinen tila. Myös hormoni- ja tunnetilojen vaihtelu aiheuttaa muutoksia kemiallisessa rakenteessa. Voidaan sanoa, että menetelmässä on yhä omat haasteensa, joiden vaikutuksia tunnistukseen ei vielä täysin tunneta. Ominaishajun yksilöllisyyttä ei ole vielä näytetty toteen, mutta esimerkiksi koirien hajuaistista tehtyjen havaintojen perusteella voimme olettaa tämän olevan totta.

Ominaishajun peittäminen parfyymeilla tai partavedellä ja tietyiltä ei-toivotuilta hajuilta kuten hieltä suojautuminen deodorantilla on eräs menetelmän huolenaiheista. Näillä saattaa olla suorituskykyä huonontava vaikutus biometristen järjestelmien toimivuuteen. Ominaishaju voi myös paljastaa arkaluontoista informaatiota henkilön terveydentilasta tai hygieniasta, mikä voidaan lukea tunkeilevaksi ja epätoivotuksi. [1, s. 126; 6, s. 78.]

Elektronisia tekoneniä on kehitteillä ja saatavilla. Mastiff Electronic Systems Ltd kehitti 1990-luvun lopulla laitteen nimeltään Scentinel. Scentinel on elektroninen tekonenä, jonka ilmaisimet ”haistavat” henkilön käden ja analysoivat henkilön ominaishajua tunnistaakseen tämän. Valmistajan mukaan laitteen suorituskykyyn eivät vaikuta parfyymit tai mikään muukaan voimakas tuoksu, koska ilmaisimet reagoivat vain ihon kemiallisiin yhdisteisiin. Nämä yhdisteet ovat valmistajan mukaan geeniemme muovaamia ja siis yksilöllisiä jokaisella henkilöllä. Laite tunnistaa nämä molekyylit ja tunnistaa henkilön niiden perusteella. [1, s. 126; 6, s. 78.]

Tekniikan mahdollisten sovelluten määrä on niin suuri, että useimmissa julkaisuissa henkilön tunnistus mainitaan niissä vain ohimennen. Potentiaalisia sovelluksia voisi esimerkiksi olla ilmanlaadun tai lääketieteelliset mittaukset. Ruoka-, juoma-, kosmetiikka- tai aseteollisuudessa käyttökohteiden määrä on myös huomattavan suuri. Terroristien torjunnassa kyseistä tekniikkaa voitaisiin hyödyntää tiettyjen vaarallisten kemiallisten aineiden ja räjähteiden havainnointiin. Myös rajaviranomaisten mahdollisuus havaita huumeiden salakuljettajat ja poliisiviranomaisten mahdollisuus tunnistaa myyjät samankaltaisella kannettavalla laitteella olisi huomattava etu tämän kaltaisen rikollisuuden torjunnassa.

4.7.8 Korvan muodon tunnistus

Alfred V. Iannarelli julkaisi 1980-luvun lopulla kirjan ”Ear identification (forensic identification series)” joka käsittelee korvan tunnistamista sen muodon, geometrian ja korvan harjanteiden perusteella. On tärkeää huomata korvanjäljen- ja korvantunnistuksen välinen ero, koska korvan tunnistaminen valokuvasta tarjoaa huomattavasti järkevämpiä mahdollisuuksia kuin korvanjälkien tutkiminen niiden ollessa hyvin harvinaisia ja muutenkin hyvin alttiita vääristymille. Kaikesta huolimatta molempien menetelmien on todettu olevan mahdollisia.

Vuonna 1995 Technical University of Madridissa Espanjassa Carreira-Perpinan tekemän diplomi-insinöörin päättötyön tutkimuksien mukaan korvan automaattisella tunnistuksella on muutamia etuja kasvojen automaattiseen tunnistukseen verrattuna. Carraira-Perpinan mukaan huomattavimmat edut ovat seuraavat:

- Korvan selkeästi pienempi koko kasvoihin verrattuna mahdollistaa pienempien kuvien käytön ja näin kuviin voidaan sisällyttää enemmän ja yksityiskohtaisempaa kuvainformaatiota.
- Korvan värijakauma on tasalaatuisempi kuin kasvoissa, mikä mahdollistaa käytännössä lähes kaiken informaation tallentamisen harmaasävykuvaan.
- Korvan muoto on lähes muuttumaton ja se ei muutu kuten kasvot erilaisten ilmeiden myötä.

Korvien muoto ei muutu juuri lainkaan täysi-ikäisenä, mutta korvien muodon yksilöllisyys on yhä testaamaton oletus. Mikään tutkimus ei vielä tue oletusta, että ihmisten korvat ovat niin erilaisia että täysin samanmuotoista korvaa ei olisi kehittynyt jollekin toiselle ihmiselle. Tutkijoilla National Training Center for Scientific Support to Crime in the United Kingdomilla tai lyhyesti NTCSSCI:lla on kuitenkin kehitteillä tietokanta korvien valokuvia varten.

Korva voi olla piilossa tai jonkin peitossa tai henkilön sen hetkinen liike tekee hyvän ja laadukkaan kuvan taltioimisen mahdottomaksi. Korvan pienen koon vuoksi laadukas kamera on välttämätön, jotta tarvittavat piirteet ja yksityiskohdat

saadaan taltioitua, myös kamerakulma ja valaistus ovat tärkeä osa taltiointiprosessia. Korvalävistykset ovat nykyisin yleisiä ja ne saattavat vaikuttaa korvan muotoon ja näin tunnistustulokseen. [1, s. 128; 6, s. 77.]

Valvontajärjestelmien vaatimusten kasvaessa ja kehittyessä kiinnostus korvan muodon tunnistamiseksi todennäköisimmin kasvaa, koska menetelmä mahdollistaa henkilön tunnistamisen hänen tietämättään. Menetelmästä voi myös tulevaisuudessa olla hyötyä monibiometrisenä järjestelmänä. Näin menetelmän avulla voitaisiin esimerkiksi vahvistaa entisestään kasvojen tunnistusta.

4.7.9 Kävelytyylitunnistus

Teoria kävelytyylin tunnistamisen taustalla pohjautuu siihen, että kuten jokaisella ihmisellä on yksilöllinen ääni ja sormenjälki, niin meillä jokaisella on myös yksilöllinen kävelytyyli. Tunnistus perustuu esimerkiksi kiihtyvyysanturilla mitattuihin vartalon liikkeisiin, jotka muunnetaan numeroiksi, joiden avulla tietokone sitten tunnistaa henkilön. Henkilön kävelytyyli riippuu hänen fyysisestä rakenteestaan ja massasta, mutta siihen vaikuttavat myös kengän tyyppi, vaatetus, vammat, sairaudet, henkinen tila, ympäristö jne.

Menetelmää on lähestytty kahdella eri tapaa. Ensimmäinen tapa on mallintaa kävelytyyliä yksinkertaisesti harmonisena liikkeenä. Tällöin kävelytyylin tunnistus lasketaan ja arvioidaan poikkeamana tuosta liikkeestä. Toinen tapa on koko vartalon mallintaminen, kun se on liikkeessä.

Menetelmän toimivuudessa on yhä haasteita. Mittauksille jotka suoritetaan ohjelmallisesti, kun kuva on taltioitu, ei vielä ole olemassa sovittuja standardimenetelmiä. Videokuvaan perustuvat menetelmät ovat alttiita vaatetuksen suhteen ja näin vaikuttavat osaltaan heikentävästi suorituskykyyn. Henkilön kävelytyyli saattaa myöskin muuttua iän myötä, henkilön laihtuessa tai lihotessa, vammautuessa tai jonkin muun syyn vuoksi. Ihmiset voivat myöskin opetella erillaisia kävelytyylejä. Kävelytyylin tunnistuksesta tuskin koskaan muodostuu vahvaa tunnistusmenetelmää mutta siitä voi olla hyötyä esimerkiksi ihmisen liikkeen tunnistukselle valvontakameroiden videosta tai kun halutaan määrittää ihmisen sen hetkistä liikettä (kävely, juoksu, kantaa painavaa esinettä

jne.) Kävelytyylitunnistus ei ole tunkeileva, mutta se että onko kävelytyyli yksilöllinen on yhä ratkaisematta. [1, s. 130.]

Turvakameroiden käyttö on hyvin yleistä nykyisin (esimerkiksi CCTV), ja niiden hyödyntäminen tulevaisuudessa henkilöiden tunnistamisessa vaatii uusia menetelmiä, ja kävelytyylin tunnistus voisi olla yksi mahdollisuus. Menetelmä sopii erityisesti huomaamattomiin valvontajärjestelmiin, koska tunnistettavan henkilön osallistumista ei tarvita, eikä kuvan tarvitse olla korkeaa resoluutioinen. Kävelytyylitunnistus voisi myös vahvistaa monibiometrisenä järjestelmänä korvan muodon ja kasvojen tunnistusta.

4.7.10 Ihon luminesenssin tunnistus

Ihmisen iho koostuu useista eri paksuisista ihon ja ihonalaisista kerroksista, jotka muodostavat ihon luminesenssin tai yksilöllisen jäljen heijastuksia, kun valo suunnataan ihoa vasten. Lääketieteen tutkijat huomasivat tämän etsiessään vähemmän tunkeilevia menetelmiä potilaiden tarkkailemiseksi. Tämä yksilöllinen heijastusjälki johtuu henkilön ihon ominaisuuksista ja sen useista kerroksista ja erilaisista rakenteista, jotka kukin vaikuttavat valon eri aallonpituuksiin. Tämä yksilöllinen jälki voi mahdollisesti toimia biometrisenä tunnisteena.

Menetelmän kehittäjä Lumidigm väittää menetelmän olevan suhteellisen vakaa. Heidän testiensä mukaan edes raskaana olevien naisten ruumiinkemia ei vaikuttanut tunnistustarkkuuteen. Valmistaja väittää, että tähän päivään mennessä noin 1000 henkilöä on testattu useita kertoja ja tulokset tukevat oletuksia, että ihon luminesenssi on yksilöllinen ja vahva tunniste. Lumidigmin kaupallinen tuote tunnetaan nimellä LightPrint, ja se on noin kolikon kokoinen järjestelmä, joka sisältää kaksi mikropiiriä, joista toinen valaisee ihon valodiodien avulla ja kerää heijastuneet säteet. Toisen mikropiirin tarkoitus on käsitellä vastaanotettu signaali ja luoda henkilölle yksilöllinen valojälki, jota voidaan verrata sitten tietokantaan tallennettuihin mallinteisiin. Toiminnalliselta periaatteeltaan menetelmä ei ole tunkeileva.

Koska Lumidigm on kaupallinen yritys, niin voidaan olettaa että sen tekemät testit tukevat omaa tuotetta ja puolueettomien tutkimusten puutteen vuoksi on mahdoton varmistaa niiden todenperäisyyttä. Kyseessä on muutenkin varsin

uusi menetelmä ja lisätutkimuksia tarvitaan, jotta voidaan määrittää menetelmän todellinen potentiaali. [1, s. 132.]

Menetelmä vaatii hyvin vähän laskentatehoa mikä tekee siitä ideaalisen kannettaviin laitteisiin, kuten älykortit, aseet ja kännykät. Monibiometrisenä tunnisteena ihon luminesenssin tunnistus voisi lisätä aitouden varmennuksen sormenjälkitunnistukseen, kun on tarve erottaa oikea iho eri tyyppisistä jäljennöksistä.

4.7.11 Jalanjälki- ja askeldynamiikkatunnistus

Jalanjälkiä on käytetty jäljittämiseen jo pitkään, mutta se ei ole varsinaisesti biometrinen tunniste. Jalanjälkien käyttö yhtenä tunnistamisen menetelmänä juontaa alkunsa muinaisen Kiinan ajalta, jossa niitä käytettiin lasten tunnistamiseksi. Sairaalassa otettu vastasyntyneen lapsen jalanjälki on yhä nykyisinkin varsin yleinen käytäntö. Jalanjäljen hyödyntämistä biometrisenä tunnisteena on lähestytty kahdella eri tapaa. Yksi tapa on mitata jalan muuttumattomia piirteitä kuten jalanjäljen harjanteita samaan tapaan kuin sormenjälkiä. Toinen lähestymistapa on mitata askelen dynamiikkaa, kun henkilö kävelee.

Jalanjälkien käyttäminen biometrisenä tunnisteena on hankalaa ja tunkeilevaa, koska henkilön on riisuttava kengät ja sukat, jotta jalan harjanteet voidaan skannata. Askeldynamiikka henkilön kävellessä tai juostessa on passiivinen ja helposti mitattavissa. Lisätietoa ja testejä tarvitaan, jotta jalanjälkiä voidaan hyödyntää automaattisessa tunnistuksessa. National Institute of Longevity Sciences (NILS) Japanissa on yksi monista menetelmää tutkivista tahoista. Tutkijat NILS:llä ovat mitanneet painon jakautumista jalassa käyttäen painoherkkiä mattoja. He ovat saavuttaneet menetelmällä 85 %:n tunnistusvarmuuden. Menetelmän yksilöllisyys on kuitenkin yhä testaamaton oletus. [1, s. 134.]

Askeltunnistus (painon jakauma) on huomaamaton menetelmä, ja monibiometrisenä tunnisteena sitä voisi mahdollisesti hyödyntää kävelytyylitunnistuksessa. Ongelmaksi tällöin kuitenkin muodostuisi kuinka kävelytyyli- ja jalanjälkitunnistus suoritettaisiin. [1, s. 134.]

Jalanjälkikuviot ovat kenties yhtä yksilöllisiä kuin sormenjäljet, mutta kattavia tutkimuksia ei ole vielä tehty niiden yksilöllisyyden varmistamiseksi. Voidaan kuitenkin olettaa, että jalanjälkikuvioden ja askeldynamiikan mittausten toistettavuuteen vaikuttavia tekijöitä ovat henkilön paino, kenkien tyyppi, vammat, ikä jne. Huomattavin ongelma on kuitenkin standardien puute.

4.7.12 Aivokäyrätunnistus

Aivokäyrän tunnistamisesta tulee ensimmäisenä mieleen tieteisromaanit ja elokuvat. Kyseisestä tunnistusmenetelmästä olisi kuitenkin hyötyä erityisesti poliisiviranomais- ja anti-terrorismikäytössä. Toimiessaan menetelmä voisi korvata täysin nykyiset valheenpaljastusjärjestelmät ja näin poliisiviranomaiset voisivat esimerkiksi selvittää, onko henkilöllä jotain sellaista tietoa mitä vain syyllinen voisi tietää.

Tiettävästi 1990-luvulla United States Intelligence Community rahoitti psykologi Emanuel Donchinin ja hänen oppilaansa Lawrence Farwellin projektin, jonka tarkoituksena oli laajentaa perinteinen EEG-testi, joka mittaa jännitevaihteluja jota syntyy aivotoiminnan seurauksena. 19.8.2002 biometritechin online-lehdessä julkaistussa artikkelissaan ”Picking your brain in the name of security” lehden päätoimittaja Laura Guevin kuvaili Donchinin projektia näin:

”Donchin keskittyi EEG skannaukselle ominaiseen piirteeseen, jota kutsutaan P300:ksi, joka ilmenee noin sekunnin kolmasosassa, kun koehenkilö tunnistaa jotain asiaankuuluvaa. Farwell jatkoi menetelmän käyttökelpoisuuden testaamista käyttäen P300:aa rikostapauksissa ja lopulta patentoi Farwellin aivojen sormenjälkimenetelmän. Järjestelmän toiminta perustuu siihen, että henkilölle vilautetaan rikokseen liittyviä oleellisia ja epäoleellisia sanoja ja kuvia tietokoneen ruudulla. Aivojen sähköiset reaktiot mitataan käyttäen patentoitua otsanauhaa, jossa on tarvittavat ilmaisimet. Farwell huomasi muistiin ja koodaukseen liittyvän monisärmäisen elektroenkefalografisen reaktion (MERMER), joka esiintyi kun aivot käsittelivät jotain merkittävää informaatiota jonka ne tunnistivat. Näin ollen jos esitetään yksityiskohtia rikoksesta, joita vain syyllinen voisi tietää, niin silloin syyllisen aivot lähettäisivät MERMER:n – mutta syyttömän epäillyn aivot eivät.” [1, s. 133.]

Vastaavasti William Lawson on kuvaillut ihmisen aivokäyrää näin:

”Vaikka on totta että meillä on kyky muokata aivokäyrämme muotoa niin emme kuitenkaan voi muokata aivokäyrämme perusmuotoa.”

Henkilön aivokäyrän perusmuotoa voidaan siis tulevaisuudessa mahdollisesti hyödyntää biometrisenä tunnisteena. *[1, s. 133.]*

Kyseessä on kuitenkin hyvin kokeellisella asteella oleva menetelmä eikä ole olemassa mitään kaupallisia järjestelmiä, jotka mahdollistaisivat aivokäyrätunnistuksen käytön varsinaisena biometrisenä tunnisteena, eikä tutkimuksia jotka tukisivat nykyisten valheenpaljastusmenetelmien soveltamista henkilön yksilöllisyyden määrittämiseksi.

5 POHDINTA

Tässä osiossa esitellään nykyiset ja joukko mahdollisia tulevaisuuden biometrisiä tunnistusmenetelmiä sekä käsitellään ongelmia esimerkkien ja kuvien avulla.

5.1 Biometriasta yleensä

Tulevaisuudessa biometriset tunnistusjärjestelmät yleistyvät ja menetelmät kehittyvät entisestään. Yksibiometristen menetelmien käyttö vähenee monibiometristen menetelmien kehittyessä ja aitouden varmennuksesta tulee välttämätön osa uusia biometrisiäjärjestelmiä. Standardien puute on biometrian alan suurin yksittäinen ja useimpia biometrisiä tunnistusmenetelmiä vaivaava ongelma ,johon tulee puuttua järjestelmien yleistyessä.

Tietoturva ja yksityisyydensuoja ovat molemmat myös erittäin tärkeitä kysymyksiä biometriikan yleistyessä. Työn aihe rajattiin käsittämään biometrisen tunnistusjärjestelmien perusteita, minkä vuoksi tietosuoja ja yksityisyyden suoja jätettiin työssä vain maininnalle. Vaikka biometriset tunnistusjärjestelmät ovat haavoittuvaisia hyökkäyksille ja mahdollisille huijauksille, niin ne kuitenkin edustavat osaa tulevaisuuden lujitetuista turvajärjestelmistä, koska yksi nyky-yhteiskunnan perustarpeista on tarve pystyä tunnistamaan ihminen luotettavasti.

Ihmisten epäluulo biometrisiä tunnistusjärjestelmiä kohtaan johtuu enemmänkin yksityisyydensuojan menettämisen pelosta kuin siitä, että niiden tekniikan toimivuutta epäiltäisiin. Tiettyjen biometrisisten tunnistusjärjestelmien mallinteet voivat sisältää tunnistusinformaation lisäksi tietoa henkilön terveydentilasta, mikä lisää ihmisten epäluuloa biometriaa kohtaan.

5.2 Sormenjälkitunnistus

Sormienjälkitunnistus on kehittynein ja yksi vanhimmista biometrisistä tunnistusmenetelmistä. Järjestelmien käyttämät mallinteet ovat standardoituja. Sormenjälkitunnistuksen selkeä puute on aitouden varmennuksen puute, mutta koska puute tunnetaan voidaan se ottaa huomioon sovelluksia suunnitellessa. Suositeltavaa on kuitenkin, että sormenjälkitunnistusta ei käytetä missään korkean turvaluokituksen kriittisessä tietoturva-, autentikointi- tai kulunvalvonta–sovelluksessa. Menetelmä sopii vähemmän kriittisiin sovelluksiin, joissa on tarve tai hyötyä varmistaa tai tunnistaan käyttäjän henkilöllisyys, kuten esimerkiksi mobiilipuhelin, kannettava mp3 soitin ja kannettava- tai pöytätietokone.

5.3 Kämmentunnistus

Kämmengeometriasovellukset ja -asennukset ovat yksi suosituimmista kalliin hintaluokan AFIS-järjestelmistä. Ne ovat helppoja käyttää ja luotettavia. Vaikka ne ovatkin suhteellisen kalliita ja vievät tilaa, ne kuitenkin voivat käsitellä suuria ihmismääriä ja käyttöä eivätkä vaadi kalibrointia tai taustavalaistusta kuten jotkut biometriset tunnisteet. Yksibiometrisenä järjestelmänä niiden tunnistustarkkuus ja suorituskyky ei kuitenkaan ole riittävä esim. henkilöllisyyden määrittämiseksi. Kämmengeometriajärjestelmissä on usein sen vuoksi myös näppäinlukko, mikä parantaa järjestelmien suorituskykyä. Tulevaisuudessa kämmengeometria–tunnistusjärjestelmien tunnistustarkkuutta ja suorituskykyä voidaan parantaa monibiometrisin keinoin esimerkiksi skannaamalla kämmenen verisuonikuvio, joka lisää kämmentunnistus menetelmään myös aitouden varmennuksen.

5.4 Kasvotunnistus

Nykypäivän tekniikka toimii parhaiten kontrolloiduissa ympäristöissä. Vaihtelevat kamerakulmat ja joukkotilanteet vaikeuttavat kasvotunnistusta ja heikentävät toimintaa huomavasti.

Kasvotunnistustekniikalle ei ole yhtä ainoaa virheprosenttia, koska suorituskyky riippuu pitkälti olosuhteista ja tiedosta, jota sille esitetään. Kuitenkin useat hallitusten teettämät testit osoittavat, että useimmat kaupalliset sovellutukset kykenevät 75 – 80 %:n tunnistustarkkuuteen tietyissä simuloiduissa olosuhteissa ja jopa 90 – 98 %:n tunnistustarkkuuteen ideaaliolosuhteissa. Tekniikasta, sen tehokkuudesta ja hyödyistä todellisuudessa ollaan useaa eri mieltä. Kiireellä suoritetut kenttätestit (esimerkiksi lentokentillä) ovat herättäneet huomiota hyvässä ja pahassa, samoin kuin myös kasvattaneet odotoksia tekniikkaa kohtaan. Hyvin integroiduista ja kalibroiduista järjestelmistä, vaikkakin ne vaativat hieman manuaalista hallintaa ja arvostelua, voidaan mainita kasinot, joilla on huomattu kasvotunnistusjärjestelmien tarkkuus riittäväksi helpottamaan tunnettujen porttikiellon saaneiden pelaajien tunnistamista.

5.5 Puhujatunnistus

Mobiilipuhelinmarkkinoiden kasvu ja massiivinen tietoliikenteen kasvu on luonut joukon puhujatunnistusjärjestelmien valmistajia. Nykypäivän valmistajat tarjoavat tuotteita ja palveluita halvoista PC:n pääsynhallintatuotteista suuriin tietoliikennekokonaisuuksiin asti.

Puheenkäsittelytekniikat ovat jo toimivia, ja nykyisin pyritäänkin lähinnä kehittämään ratkaisuja muutamiin tekniikan osa-alueisiin. Tekniikan toimivuus ja tarkkuus on ongelma. Ongelma voidaan ratkaista kehittämällä uusia menetelmiä taustamelun vaimentamiseksi. Puhujatunnistus on myös laskentatehollisesti yksi vaativimmista biometrisistä teknologioista, joten luonnollisesti tarve kehittää entistä nopeampia ja vähemmän laskentatehoa vaativia käsittelymetodeja on suuri.

Puhujatunnistussovellukset laajentavat sanastojaan ja mahdollisuuksia ymmärtää eri kieliä. Tulevaisuuden puheenkäsittelytekniikat pyrkivät

määrittelemään puhutun kielen, murteen ja jopa puhujan ominaisuuksia, joihin lukeutuu mm. puhujan stressi, asenne ja henkinen tila.

5.6 Iiris- ja retinatunnistus

Iiristunnistus on herättänyt paljon huomiota viime aikoina sen ollessa yksi tarkimmista biometrisistä menetelmistä. Vaikka retina- ja iiristunnistukseen perustuvia tuotteita vielä kehitetään, niin molemmat menetelmät pohjautuvat jo varsin kehittyneisiin ja valmiisiin menetelmiin. Siinä missä tohtori Daugman on julkaissut patentoidut iirisanalysointimenetelmänsä, ei retinantunnistukselle ole saatavilla lainkaan matemaattisia malleja ja kaavoja, jotta voitaisiin arvioida ja vertailla sen vahvuuksia ja heikkouksia muihin menetelmiin nähden. Molemmat menetelmät ovat pääasiallisesti yksittäisten valmistajien sovelluskohtaisia toteutuksia, joiden tiedetään kyllä toimivan hyvin pääsynhallintajärjestelminä. Kumpi on siis parempi? Mikään biometrinen tunniste ei tule todennäköisesti yksinään olemaan se ainoa ja paras ratkaisu jokaiseen mahdolliseen tunnistusjärjelmään. Sisäisten piilossa olevien biometristen tunnisteiden edut verrattuna ulkoisien näkyvien tunnisteiden käyttöön riippuvat täysin sovelluksesta, käyttöympäristöstä, päämäärästä ja käyttäjien mieltymyksistä. Muita tekijöitä jotka vaikuttavat valintaan ovat laitteiden hinta, käyttö- ja huoltokulut, asennus ja laitteiden integrointimahdollisuus osaksi suurempaa järjestelmää.

5.7 Käsialadynamiikkatunnistus

Käsialadynamiikkatunnistusta ja muita siihen perustuvia tekniikoita on tutkittu ja kehitetty aktiivisesti jo melkein kolme vuosikymmentä, ja niiden kohdalla voidaankin jo puhua kehittyneestä teknologiasta. Vaikka puhutaankin suhteellisen kehittyneestä teknologiasta, niin se ei kuitenkaan tarkoita, että käsialadynamiikkatunnistus olisi täydellinen ja toimisi ilman rajoituksia.

Osa valmistajista vertaa allekirjoituksia DNA-tason yksilöllisyyteen, mutta näille väitteille ei kuitenkaan ole minkäänlaisia perusteita. Allekirjoitus on käyttäytymistapoihin perustuva ominaisuus, ja samalta henkilöltä taltioiduissa allekirjoituksissa saattaa olla huomattaviakin eroja. Näin allekirjoitus yksinään ei ole riittävä tunniste erottamaan riittävän luotettavasti yksilöitä keskisuuresta tai

suuresta henkilömäärästä. Kun allekirjoitusta käytetään osana erilaisia anomuksia, niin poikkeuksetta niiden kanssa kysytään muita hallinnollisia tai henkilöhistoriallisia tietoja kuten henkilön osoite ja puhelinnumero.

Tiettyjen olosuhteisiin perustuvien ja käsialadynamiikan tunnistuslaitteille ominaisten tekijöiden tiedetään vaikuttavan tunnistuksen luotettavuuteen ja näin suorituskykyyn. Tunnistuslaitteiden fyysiset ominaisuudet, kuten kynän paino, kynän koko ja pinnan kitka lisäävät vaihtelua prosessiin. Lisäksi väsymys ja psykologiset asiat vaikuttavat oman allekirjoituksen toistettavuuteen. Henkilö voi allekirjoittaa tärkeitä asiakirjoja kuten työ- ja lainahakemuksia huolellisemmin ja hitaammin. Toisaalta hän allekirjoittaa rutiininomaisia asiakirjoja kuten pöytäkirjoja kiireellä sen suuremmin asiaa miettimättä ja ilman minkäänlaista epäröintiä.

5.8 Näppäimistödynamiikkatunnistus

Näppäimistödynamiikkatunnistusta voidaan käyttää inhimillisen kirjoitustavan tunnistuksessa. Nykyajan verkkoyhteiskunnassa on hyvin tärkeää, että voidaan erottaa ohjelman tuottama kirjoitus oikeasta ihmisen tuottamasta kirjoituksesta. Salasanojen arvaus ohjelmallisesti on yksinkertainen, nopea ja hyvinkin todellinen uhka. Näin päästään käsiksi muiden ihmisten salasanoihin luvatta, mikä on tietenkin epätoivottu tilanne ja tämän kaltaiset hyökkäykset pitäisi pystyä tunnistamaan ja estämään. Vaikka ohjelmiinkin voidaan sisällyttää viiveitä, jotta niillä tuotettu kirjoitus tulkittaisiin ihmisen kirjoittamaksi, niin näppäimistödynamiikkatunnistuksesta on kuitenkin selkeää hyötyä monien ohjelmallisten hyökkäysten torjunnassa.

5.9 Tulevaisuuden biometriset menetelmät

Ihminen on yksilöllinen lukemattomin eri tavoin. Vain mielikuvitus ja kykymme mitata näitä piirteitä ja ominaisuuksia on käytännön toteutusten esteenä. On olemassa joukko biometrisiä menetelmiä, jotka ovat vielä kokeellisella tasolla ja kehitystyön alla. Prosessorien hintojen laskiessa, laskentatehon kasvaessa ja algoritmien parantuessa voidaan hyvinkin olettaa, että osa näistä yhä kokeellisista menetelmistä on osa huomisen turvaratkaisuja.

6 YHTEENVETO

Tehdyn kirjallisuustutkimuksen perusteella voidaan sanoa, että biometriikka on tulevaisuuden kehittyvä ala ja biometristen tunnistusjärjestelmien käyttö tulee yleistymään lähitulevaisuudessa.

Tässä insinöörityössä esiteltiin tunnistamisen ja biometrisen tunnistamisen perusteita. Biometriset tunnistusmenetelmät esiteltiin ja niiden perusteita käytiin läpi esimerkkisovelluksien avulla.

Biometristen tunnistusjärjestelmien tunnistusepätarkkuuden voidaan yleistäen sanoa parhaimmillaankin olevan muutaman prosentin tasoa, mitä voidaan pitää liian suurena, kun yleisesti hyväksyttävän väärien tunnistusten määrän tulisi olla yksi miljoonasta.
Kirjallisuustutkimusten perusteella voidaan sanoa, että biometriset tunnistus–järjestelmät ovat tulevaisuuden toimivia ratkaisuja tietoturvaan, autentikointiin ja kulunvalvontaan tarkoitetuissa sovelluksissa. On kuitenkin tärkeää huomioida näiden AFIS-järjestelmien puutteet ja tunnistaa mahdolliset riskit.

Työn lopuksi taulukossa 5 lista yleisesti hyväksytyimpien tunnistusmenetelmien ominaisuuksista ja niiden laadusta.

Taulukko 5. Yleisesti hyväksyttyjen tunnistusmenetelmien ominaisuudet ja niiden laatu

menetelmä	**yleisyys**	**erottelevuus**	**pysyvyys**	**keräiltävyys**	**suorituskyky**	**hyväksyttävyys**
sormenjälki	keskitaso	korkea	korkea	keskitaso	korkea	keskitaso
kämmen	keskitaso	keskitaso	keskitaso	keskitaso	keskitaso	keskitaso
kasvokuva	korkea	matala	keskitaso	korkea	keskitaso	korkea
iiris	korkea	korkea	korkea	keskitaso	korkea	matala
retina	korkea	korkea	keskitaso	matala	korkea	matala
puheääni	keskitaso	matala	matala	korkea	matala	korkea
näppäimistö–dynamiikka	keskitaso	keskitaso	matala	keskitaso	keskitaso	korkea

VIITELUETTELO

[1] Woodward, John D. Jr. – Orlans, Nicholas M. – Higgins, Peter T. Biometrics: Identity Assurance in the information Age. The McGraw-Hill companies,inc. 2003

[2] Spinella, Edmund, Biometric Scanning Technologies: Finger, Facial and Retinal Scanning. Sans Institute. 2003. [Verkkodokumentti, viitattu 9.2.2009] Saatavissa: http://www.sans.org/reading_room/

[3] Ikäläinen, Juha-Pekka, Monibiometriset tunnistejärjestelmät. 2008. [Verkkodokumentti, viitattu 9.2.2009] Saatavissa: http://www.tritonia.fi/fi/kokoelmat/gradu.php

[4] Eloranta, Ville, Silmät Auki! Tietoyhteiskunnan uhat ja mahdollisuudet. Eduskunnan tulevaisuusvaliokunnan julkaisu. 2008. [Verkkodokumentti, viitattu 9.2.2009] Saatavissa: http://www.eduskunta.fi

[5] Zdeněk, Ríha – Václav, Matyáš, Biometric Authentication Systems. 2000. [Verkkodokumentti, viitattu 9.2.2009] Saatavissa: http://www.fi.muni.cz/reports/files/older/FIMU-RS-2000-08.pdf

[6] Makarski, Richard E. – Marrero, Jose A. A Surveillance society and the conflict state: leveraging ubiquitous surveillance and biometrics technology to improve homeland security. 2002. [Verkkodokumentti, viitattu 9.2.2009] Saatavissa: http://stinet.dtic.mil/dticrev/PDFs/ADA407611.pdf

[7] Daugman, John, How iris recognition works. University of Cambridge. [Verkkodokumentti, viitattu 9.2.2009] Saatavissa: http://www.cl.cam.ac.uk/~jgd1000/irisrecog.pdf

[8] ANSI/NIST-ITL 1-2007 revision of ANSI/NIST-ITL 1-2000. American National Standard for Information Systems - Data Format for the Interchange of Fingerprint Facial, & Other Biometric Information – Part 1. National Institute of Standards and Technology. 2007

[9] Veldhuis, Raymond – Bazen, Asker – Booij, Wim, Hendrikse, Anne, A Comparison of Hand-Geometry Recognition Methods Based on Low- and High-Level Features. [Verkkodokumentti, viitattu 9.2.2009] Saatavissa: http://doc.utwente.nl/48121/1/veldhuis.pdf

[10] International Biometric Group. [Verkkodokumentti, 9.2.2009] Saatavissa: http://www.biometricgroup.com/reports/public/reports_and_research.html

[11] Fenotyyppi [Verkkodokumentti, viitattu 9.2.2009] Saatavissa: http://fi.wikipedia.org/wiki/Fenotyyppi

[12] Genotyyppi [verkkodokumentti, viitattu 9.2.2009] Saatavissa: http://fi.wikipedia.org/wiki/Genotyyppi

[13] Fingerprint [verkkodokumentti, viitattu 9.2.2009] Saatavissa: http://en.wikipedia.org/wiki/Fingerprint

[14] Ross, Arun A., Information fusion in fingerprint authentication [Verkkodokumentti, lainattu 2.9.2009] Saatavilla: http://www.csee.wvu.edu/~ross/pubs/RossPhDThesis_03.pdf

[15] Taking legible fingerprints [Verkkodokumentti, viitattu 9.2.2009] Saatavissa: http://www.fbi.gov/hq/cjisd/takingfps.html

[16] Kuusela, Antti, Sormenjälkitunnistimien turvallisuusongelmat. Helsingin ammattikorkeakoulu Stadia. 2006.

[17] Schneider, J.K, Ultrasonic Imaging Systems for Personal Identification. Ultrascan inc. [Verkkodokumentti, viitattu 9.2.2009] Saatavissa: http://www.ultra-scan.com/Default.aspx?tabid=512

[18] Kilpeläinen, Teemu, Automaattisen puhujanvarmennuksen päätöslogiikkaa. 2001. [Verkkodokumentti, viitattu 9.2.2009] Saatavissa: http://cs.joensuu.fi/pages/tkinnu/research/pdf/BSc_Teemu_Kilpelainen.pdf