Heidi Kuusisto

BIOMETRINEN TUNNISTUS

Tietojenkäsittelyn koulutusohjelma

2014

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

BIOMETRINEN TUNNISTUS

Kuusisto, Heidi
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Marraskuu 2014
Ohjaaja: Grönholm, Jukka
Sivumäärä: 29

Asiasanat: biometrinen, tunnistus, biotunniste, sormenjälki

Opinnäytetyössä käsitellään biometrista tunnistautumista mahdollisimman monipuolisesti. Selvennetään, mitä biometrisella tunnistuksella tarkoitetaan ja perehdytään hieman aiheen historiaan sekä maassamme viranomaiskäytössä oleviin järjestelmiin. Käsitellään biometrisen tunnistuksen etuja ja haittoja, sekä yleisesti jo käytössä olevia palveluita ja sovelluksia, sekä tutustutaan eri menetelmien käyttöön ja ominaisuuksiin.

Tutkimuksen perusteella voidaan todeta, että biometrinen tunnistautuminen on melko yleistä nykypäivänä ja ihmiset suhtautuvat hyväksyvästi tunnisteiden keräämiseen. Erilaisia menetelmiä on useita ja uusia tutkitaan koko ajan lisää. Järjestelmien tietoturvaa ja helppokäyttöisyyttä kehitetään käyttäjäystävällisimmiksi.
Opinnäytetyö on teoreettinen, joten se perustuu kirjallisuuteen ja tutkimuksiin, joissa aihetta on käsitelty

BIOMETRIC IDENTIFICATION

Kuusisto, Heidi
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Information and Communication Technology
November 2014
Supervisor: Grönholm, Jukka
Number of pages: 29

Keywords: biometric, identification, bio-id, fingerprint

Purpose of the thesis is to deal with biometric authentication as versatile as possible. Clarifies, what biometric identification means and get to know a little history of the subject. Examine the advantages and disadvantages of biometric identification, as well as existing services. Learn about the different methods and their properties.

The study shows, that the biometric authentication is quite common these days and the people accept the use of biometrics. There are several different methods and new ones are constantly studied more. Systems will be developed safer and user-friendly to use. The thesis is a theoretical, so that it is based on the literature and studies, in which the topic has been discussed.

SISÄLLYS

1 JOHDANTO

Ihminen määritellään ja muistetaan hänen ulkonäöstään, äänestään, mielipiteistään tai henkilötunnuksestaan. Lähes kaikki ihmisen ruumiinosat ja tavat toimia, kuten sormenjäljet, silmät, ääni, kävelytyyli tai käsiala on yksilöllisiä, ja näin ollen erilaisilla menetelmillä mitattavia tietoja.

Yhteiskunnan kehittyessä ja globalisoituessa olemme tulleet tilanteeseen, jossa ihmisen on tunnistauduttava jollakin menetelmällä useita kertoja päivässä; kirjautuessaan niin omalle kuin työpaikan tietokoneelle, ja sitten vielä yleensä useampaan kuin yhteen järjestelmään ja palveluun. Töihin tai kotiin mennessä sähköiset lukot pyytävät tunnistusta omalla henkilökohtaisella avaimella ja kaikesta tästä jää merkintä tietokantoihin.

Salasanojen ja älykorttien lisäksi ovat tulleet biotunnisteet. Näiden kolmen yhdistelmä on turvallisin ja varmin tapa todeta ihmisen henkilöllisyys. Yhdysvalloissa 2001 tapahtuneiden terroristitekojen jälkeen Yhdysvallat kiristivät rajojaan ja vaativat biotunnisteet matkustusasiakirjoihin, jotka tätä myöden tulivat myös EU:ssa käyttöön.

Suomessa käyttöönotettiin 2006 passi, johon tallennetaan kasvokuva digitaalisessa muodossa sirulle sekä 2009 sirulle tallennettiin myös sormenjäljet. Biometrinen tunnistautuminen on siis jo kauan ollut mukana viranomaisvalvonnassa, ja pikku hiljaa myös tulossa enemmän joka käyttäjän arkipäiväiseen elämään. Joissakin maissa on jo mahdollista maksaa ostoksensa biotunnistetta käyttämällä. Suomessa tunnistetta tarvitaan esimerkiksi useilla kuntosaleilla.

Tämän työn tarkoitus on perehtyä yleisesti biometriaan. Tarkoituksena on selventää eri menetelmiä, jotka jo ovat käytössä, ja joita vasta tutkitaan. Sen lisäksi selvennetään biotunnisteiden hyötyjä ja uhkia, sekä tutustutaan palveluihin, joissa biotunnisteet ovat käytössä tai kokeilussa.

2 BIOMETRINEN TUNNISTAUTUMINEN

Biometriikka on yksilön tunnistamista fyysisten ominaisuuksien tai käyttäytymisen perusteella. Yksilöllisiä fysiologisia piirteitä ovat muun muassa silmän iiris ja retina, kasvot sekä sormenjäljet. Käytökseen perustuvia mitattavia ominaisuuksia ovat muun muassa käsiala ja kävelytyyli. (Suomen Standardisoimisliiton www-sivut.)

Tunnistukseen tarkoitetut sovellukset perustuvat joko verifiointiin tai identifiointiin. Verifiointi on todentamista, jossa esimerkiksi henkilön sormenjälkeä verrataan vain siihen sormenjälkeen, kuka hänen uskotaan olevan. Identifiointi on tunnistamista, joka taas tarkoittaa, että sormenjälkeä verrataan kaikkiin tietokannan sormenjälkiin, jotta varmistutaan henkilön henkilöllisyydestä. (Jain, Ross & Nandakumar 2011, 10 & 11.)

Tutkimusmenetelmiä on useita, ja niiden käyttöä eri tilanteissa määrittelee niiden erilaiset ominaisuudet, joita selventää taulukko1, jossa menetelmän sopivuutta vertaillaan termeillä:

- Yleisyys tarkoittaa, kuinka todennäköisesti ominaisuus löytyy kaikilta
- Yksilöllisyys tarkoittaa, että ominaisuus on mahdollisimman uniikki
- Pysyvyys tarkoittaa, että ominaisuus ei muutu ajan kuluessa
- Kerättävyys tarkoittaa, että ominaisuus on mitattavissa
- Suoritusteho tarkoittaa tarkkuutta ja nopeutta järjestelmän käytössä
- Hyväksyntä, miten käyttäjät reagoivat ominaisuuden antamiseksi järjestelmän käyttöön
- Luotettavuudella, kuinka helppoa väärentäminen on.

Biometria	Yleisyys	Yksilöllinen	Pysyvyys	Kerättävyys	Suoritusteho	Hyväksyntä	Luotettavuus
Kasvot	korkea	matala	medium	korkea	matala	korkea	matala
Sormenjälki	medium	korkea	korkea	medium	korkea	medium	korkea
Käden geometria	medium	medium	medium	korkea	medium	medium	medium
Iiris	korkea	korkea	korkea	medium	korkea	matala	korkea
Retina	korkea	korkea	medium	matala	korkea	matala	korkea
Allekirjoitus	matala	matala	matala	korkea	matala	korkea	matala
Ääni	medium	matala	matala	medium	matala	korkea	matala

Taulukko1. Eri menetelmien ominaisuuksien vertailu. (Griaule Biometricsin www-sivut 2014a.)

2.1 Historia

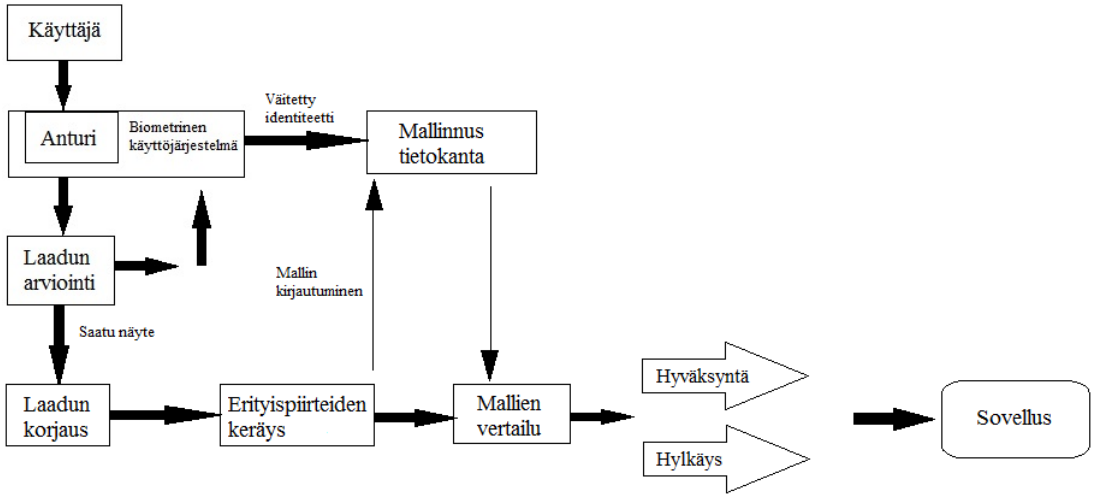
Alphonso M. Bertillo oli ranskalainen kriminologi, joka kehitti ensimmäisen antropologisen järjestelmän 1879. Se mittasi kehon osia erityisesti päätä ja kasvoja. Järjestelmän käyttö levisi nopeasti Euroopassa, ja se oli käytössä lähes kolmekymmentä vuotta. Bertillon järjestelmään kirjattiin myös sormenjäljet, mutta niiden merkitys oli vähäinen. Vasta 1892 Sir Francis Galton kehitti sormenjälkitunnistusta, koska uskoi, ettei kahdella ihmisellä voi olla samanlainen sormenjälki. Menetelmään kuuluneita yksityiskohtia käytetään yhä edelleen. (National Law Enforcement Museum Insiderin www-sivut; Griaule Biometricsin www-sivut 2014b.)

Vuonna 1985 silmälääkärit tohtori Leonard Flom ja Aran Safir esittivät, ettei kahta samanlaista iiristä ole olemassa. Käsitteelle myönnettiin patentti 1987. Vasta 2005 laajan 1995 John Daugmanille myönnetyn patentin vanhennuttua saivat muutkin yritykset mahdollisuuden kaupallistaa omia algoritmejaan. (FBI:n www-sivut a, 114-115.)

2.2 Biometrisen tunnistusjärjestelmän toimintamalli

Biometrinen tunnistusjärjestelmä perustuu siihen, että se mittaa yhtä tai useampaa fyysistä tai käyttäytymiseen perustuvaa ominaisuutta. Itse tunnistusprosessi koostuu kahdesta eri vaiheesta, kirjautumisesta ja tunnistautumisesta. Ensimmäisessä vaiheessa eli kirjautumisessa saadaan käyttäjältä biometrinen näyte, joka tallennetaan

tietokantaan yhdessä henkilötietojen kanssa. Näytettä ei tallenneta suoraan kuvana vaan siitä poimitaan erityispiirteet, jotka sitten tallennetaan tietokantaan. Tunnistusvaiheessa tarvitaan uusi näyte, jota verrataan aikaisemmin tallennettuun malliin. Loppujen lopuksi voidaan todeta, että biometrinen järjestelmä on vain mallin tunnistusjärjestelmä. Järjestelmä sisältää neljä perusosaa (Kuva 1.) eli anturin, ominaisuuksien keräyksen, tietokannan ja näytteiden vertailun (hyväksyntä vai hylkäys).
(Jain, Ross & Nandakumar 2011, 3-4 & 6.)



Kuva1. Yksinkertaisen biometrisen tunnistusjärjestelmän toimintamalli. (Jain, Ross & Nandakumar 2011, 6)

2.3 Biometrinen tunnistautuminen Suomen viranomaiskäytössä

Sormenjälkien kirjaaminen tietokoneille alkoi yleistyä 1980-luvulla. Järjestelmiä kutsutaan yleisesti AFIS-järjstelmiksi (Automated Fingerprint Identification System). Ensimmäiset rikoksesta epäillyn sormenjäljet otettiin Suomessa vuonna 1908, ja 1926 korkein oikeus hyväksyi asiantuntijalausunnon näyttönä. Vuonna 1989 Suomi siirtyi käyttämään AFIS-järjestelmää. Järjestelmä koostuu rekisteriohjelmistosta sekä niin sanotusta vertailualgoritmista. (Kari & Suuripää 2010, 13 & 34.)

Biotunniste otettiin käyttöön Suomen passeissa elokuussa 2006, kun passissa olevalle sirulle tallennettiin kasvokuva. Kesäkuussa 2009 sirulle lisättiin kaksi sormenjälkeä. Tavallisesti sormenjäljet kirjataan kummankin käden etusormista, mutta mikäli näitä ei saada sairaudesta tai vammasta johtuen otetaan näyte keskisormesta, nimettömästä

tai peukalosta. Mikäli henkilö on alle 12-vuotias, ei sormenjälkiä saa ottaa, ja tällöin myönnetään normaali viiden vuoden passi, jossa sormenjälkien lukumääräksi merkitään nolla. Oleellisin asia 2009 tulleessa passilain muutoksessa oli sormenjälkinäytteiden tallennus passin koneellisesti luettavalle sirulle sekä passirekisteriin (Poliisin hallintoasiain tietojärjestelmä). Sormenjälkitiedot tallennetaan passin hakijasta riippuen joko henkilökortti ja passijärjestelmään (Heko-Passi) tai Maahanmuuttoviraston ylläpitämään ulkomaalaisrekisteriin. Oleskelulupakortit biometrisilla tunnisteilla otettiin Suomessa käyttöön tammikuussa 2012, jolloin samanaikaisesti kirjattiin molemmat tunnisteet; kasvokuva ja sormenjäljet. (Kari & Suuripää 2010, 5-6, 10 & 17.)

Poliisilla on mahdollisuus käyttää passirekisteriin tallennettuja sormenjälkiä muuhun kuin keräämis- ja tallettamistarkoitukseen, mikäli on tapahtunut joku luonnononnettomuus, suuronnettomuus tai muunlainen katastrofi, taikka kyseessä on rikoksen uhri tai tunnistamattomaksi jäänyt uhri. Rikoksesta epäillyltä poliisi saa ottaa rikoksen selvittämiseksi ja rikollisen rekisteröimiseksi sormen-, käden- ja jalanjäljet, käsiala-, ääni- ja hajunäytteen, valokuvan sekä tuntomerkit. Vuonna 2007 Suomi sitoutui Prüm-sopimukseen, joka perustettiin 2005. Sen tarkoituksena on säännellä tietojenvaihtoa jäsenmaiden välillä estääkseen terrorismia, valtioiden rajojen ylittävää rikollisuutta sekä laitonta rajojen ylitystä. Tiedonvaihtoon kuuluu muun muassa DNA-, sormenjälki- ja ajoneuvorekisteritiedot. (Kari & Suuripää 2010, 7,15 & 30.)

Lokakuussa 2014 sisäministeriö asetti työryhmän, jonka tehtävänä on tutkia mahdollisuutta sormenjälkien liittämisestä henkilökortteihin. Tarkoituksena on muun muassa selvittää millaisia muutoksia lainsäädäntöön sekä hakukäytäntöön on tehtävä. Nykyään käytössä oleva henkilökorttilaki on vuodelta 1999. (Aaltonen & Laitinen 2014.)

3 BIOMETRINEN TUNNISTAUTUMINEN ARJESSAMME

Biotunnisteita on nykyään kaikkialla ja kaikki ovat niitä varmasti käyttäneet. Postipakettia postista noudettaessa jätämme sähköisen allekirjoituksen, passin saamiseksi

vaaditaan kasvokuva ja sormenjäljet järjestelmään. Useimmat matkapuhelinvalmistajat ovat liittäneet tuotteisiinsa sormenjälkitunnistimen, joita kannettavissa on jo ollut aiemmin. Älyaseita on kehitelty jo pitkään, joissa liipaisimesta pystyy vetämään vain siihen rekisteröity sormenjälki.

Tamperelainen Deltabit Oy ja porilainen Idolo tuottavat molemmat sormenjälkitunnistimella varustettuja lukkoja jokaisen kotioveen. Deltabit Oy:n lukkoihin eivät väärennökset kelpaa, koska sensori aistii ihmisen kehonlämmön eikä näin ollen hyväksy kumisormia. Liian kylmällä on myös syytä lämmitellä käsiään, jottei järjestelmä luule ”sormea kuolleeksi”. Deltabit Oy:n tuotteista löytyy myös Gatekeeper Medi, joka takaa sädehoitopotilaalle varmasti oikean hoidon. Potilas kirjautuu hoitoon sormenjäljellään, johon lääkäri on liittänyt hoitosuunnitelman. (Seppälä 2009; Deltabitin www-sivut a.)

Vuoden 2015 alkupuolella alkaa helsinkiläinen yritys Uniqul kokeilla kasvotunnistuksella tapahtuvaa maksamista muutamissa paikallisissa kahviloissa. Järjestelmä perustuu siihen, että se mittailee henkilön kasvojen mittasuhteita. Maksutapahtumaa suoritettaessa hyväksytään maksu painikkeella, jonka jälkeen järjestelmä tunnistaa kasvot ja maksu on suoritettu. (Krautsuk 2014.)

Fujitsun PalmSecure-kämmentunnistin on ensimmäinen kämmenen verisuoniston (Kuva 5.) tunnistukseen suunniteltu järjestelmä. Se on saanut tietoturvallisuuden sertifikaatin, ja on näin ollen kolmas biometriseen tunnistukseen perustuva järjestelmä, jolle sertifikaatti on myönnetty. Ruotsalainen Fredrik Leifland kehitti maksupäätteen, joka hyödyntää kämmenen verisuonistoa. Laite pohjautuu Fujitsun PalmSesure-tekniikkaan. Lundin kaupungissa Ruotsissa laite on jo käytössä 15 eri yrityksessä ja rekisteröityneitä käyttäjiä on noin 1600. Japanin pankeissa on siirrytty myös käyttämään Fujitsun-tekniikkaa. Pankkiautomaateilta on mahdollista nostaa ja tallettaa rahaa skannaamalla kämmenensä tunnistuslaitteessa. Yhtenä syynä siirtymisessä biotunnisteen käyttöön ovat Japanissa olleet maanjäristykset, joiden vuoksi ihmisille tuli ongelmia, koska henkilötunnukset hävisivät muun omaisuuden mukana. (Fujitsun www-sivut a; Brohlin 2014; Fujitsun www-sivut b.)

Samsung Galaxy S5 -puhelimella on mahdollista maksaa ostoksensa PayPal-maksupalvelussa sormenjäljellä, joka toimii allekirjoituksena. Samsungin on myös tarkoitus liittää vuoden 2014 loppuun mennessä silmän iiristunnistus kyseiseen puhelimeen. Se tunnistaa silmänliikkeet, joka helpottaa esimerkiksi verkkoselaamista. (Belic 2014; Talouselämän www-sivut 2014.) Sormenjälkitunnistimia löytyy myös Applen ja Huawein puhelimista. Windows Phone puhelimissa sormenjälkitunnistusta ei vielä ole otettu käyttöön.

Suomalaiset kuntosaliyrittäjät ovat siirtyneet jäsenkorteista sormenjälkitunnistuksen käyttöön jo vuosia sitten. Perusteluna sormenjäljen käytölle sanotaan, jäsenkorttien väärinkäyttö sekä asiakkaan mahdollisuus tulla kuntosalille, koska vain vaikka henkilökuntaa ei olisikaan paikalla. Asiakkaille sormenjäljen käyttö sopii eivätkä he pelkää tunnisteiden joutumista vääriin käsiin. (Åström-Kupsanen 2007.)

Opioidikorvaushoitoa tarvitseville tehdyssä suomalais-brittiläisessä hankkeessa tutkitaan mahdollisuutta tehdä huumeseula sormenjäljestä. Pienellä kannettavalla laitteella analysoidaan hikeä potilaan sormenpäästä, jonka avulla saadaan selville henkilöllisyys sekä mahdollinen huumeidenkäyttö. (Tacke 2013.)

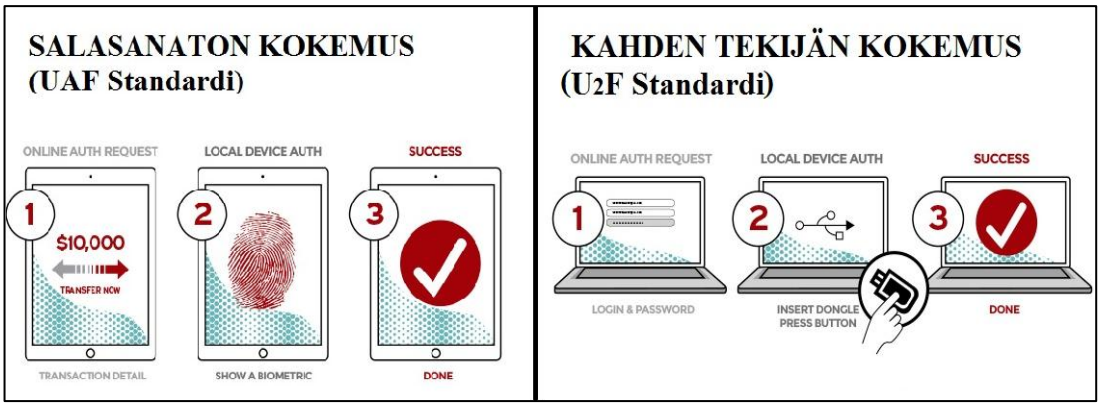
Useat yritykset ovat jo siirtyneet käyttämään kulunvalvonnassa sormenjälkitunnistusta. Deltabit Oy tekee myös kulunvalvontaan sormenjälkitunnistimia. Järjestelmiä käytetään niin työntekijöiden kulunseurantaan, mutta myös hoitolaitoksissa potilaiden kulkemisen seuraamisen. Järjestelmällä voidaan rajoittaa esimerkiksi muistisairaiden potilaiden pääsyä ulkotiloihin. (Deltabitin www-sivut b.)

3.1 Maailma ilman salasanoja

Fido Alliance on organisaatio, joka koostuu yli sadasta teknologiayrityksestä, joiden tarkoituksena on ollut suunnitella vahvaan tunnistukseen ja helppokäyttöisyyteen perustuva menetelmä, jota nämä yritykset käyttävät palveluissaan. Ryhmään kuuluvia yrityksiä ovat muun muassa Google, Lenovo, PayPal, Mastercard ja Microsoft. Organisaation nimi tulee sen englantilaisesta kokonimestä Fast Identity Online Alliance eli nopea verkkotunnistusallianssi. Tarkoituksena on luopua salasanoista ja käyttäjä-

tunnuksista kokonaan. Menetelmän perusajatuksena on, että käyttäjällä on jokin pieni henkilökohtainen laite, jota käyttämällä käyttäjä tunnistautuu laitteeseensa, kuten tietokoneelle tai puhelimeen. Tämä vaatii sen, että laitteessa on fidon suunnittelema protokollapino, joka ohjaa tunnistautumisen fido-palvelimelle. (Secure Linkin www-sivut 2014; Digitodayn www-sivut 2013.)

Fido on kehittänyt kaksi eri tapaa toimia erilaisissa käyttökohteissa ja -tilanteissa. Protokollat perustuvat julkisen avaimen salaukseen, ja ovat erittäin vahvoja menetelmiä verkkourkintaa ajatellen. Vaihtoehdot ovat salasanaton tai kahden tekijän kokemus (Kuva 2.). Salasanattomassa kokemuksessa käyttäjä rekisteröityy verkkopalveluun laitteellaan ja tunnistautuu järjestelmään valitsemallaan todennusmenetelmällä, kuten esimerkiksi sormenjäljellä, katsomalla kameraan tai puhumalla mikkiin. UAF-protokolla antaa palvelulle mahdollisuuden valita, mitkä toiminnot esitetään käyttäjälle. Rekisteröinnin jälkeen käyttäjä vain suorittaa aina todennuksen halutessaan kirjautua järjestelmään eikä salasanoja enää tarvita. Protokollassa on myös mahdollisuus yhdistää useampia tunnistusmekanismeja, esimerkiksi sormenjälki ja PIN-koodi Kahden tekijän kokemuksessa eli U2F-protokollaa käytettäessä voidaan hyödyntää olemassa olevia käyttäjätunnuksia ja salasanoja. Käyttäjä kirjautuu rekisteröityessään laitteeseen tunnuksillaan ja esittää laitteensa eli toisen tekijän, joko asettamalla laitteen usb-porttiin tai käyttämällä NFC-tekniikkaa. Vahva toinen tekijä antaa palvelulle mahdollisuuden yksinkertaistaa salasanan vaikka neljä kirjaimiseksi PIN-koodiksi vaarantamatta turvallisuutta millään lailla. Google julkaisi lokakuussa tiedotteen, että nyt google-tiliin on mahdollista liittää suojausavain. Palvelu on ilmainen, mutta U2F-laite pitää hankkia itse. Laitteen liittämisen jälkeen ei kirjautumisessa tarvita enää salasanaa. (Jordan 2014; Fido Alliancen www-sivut 2014.)



Kuva 2. Käyttäjäntunnistus ilman salasanaa, tai salasanan ja toisen tekijän yhdistelmällä. (Jordan 2014.)

4 BIOMETRISEN TUNNISTAUTUMISEN HYÖDYT JA UHAT

Biometrinen tunnistautuminen on eittämättä turvallinen ja luotettava tapa todentaa henkilön henkilöllisyys. Salasanojen muistaminen nyky-yhteiskunnassa, jossa kirjautumisia tietokonetta käynnistettäessä saattaa olla useita, on melko haastavaa. Kirjaudumme tietokoneelle, sähköpostiin, eri sovelluksiin sekä yrityksen sisäisiin järjestelmiin usein eri tunnuksilla ja salasanoilla. Tietoturvaa ajatellen ei samaa salasanaa saisi käyttää eri järjestelmissä, vaan joka järjestelmään pitäisi kirjautua eri salasanalla minimoidakseen tietoturvariskin. Biometrisessa tunnistuksessa ei tarvitse muistaa erillisiä salasanoja, vaan rekisteröidä oma yksilöllinen tunniste esimerkiksi sormenjälki järjestelmään, joka todennetaan järjestelmään kirjautuessa.

Biotunnistetta ei myöskään voi hukata, ja sen varastaminen on haastavaa, muttei mahdotonta. Biometrisellä tunnistuksella voidaan seurata tarkasti kuka tekee ja mitä. Salasana saatetaan kertoa muillekin, jolloin varmaa loppukäyttäjää ei voida tietää.

Biometrisen tunnistautumisen käytön leviäminen herättää myös kysymykset järjestelmien luotettavuudesta ja tietojen riittävästä salauksesta. Eniten keskustelua herättäneet uhkakuvat ovat kysymykset yhteiskunnan liiallisesta yksilön valvonnasta eli niin kutsutusta ’Big Brother-ilmiöstä’, identiteettivarkauksista ja biometrisesta huijaamisesta. (Ailisto, Ahonen & Lindholm 2005, 7-8.)

Yhtenä uhkaesimerkkinä voidaan mainita Facebook, joka halutessaan voisi pitää maailman suurinta kasvojentunnistus tietokantaa yllä, koska lakeihin ei ole vielä säädetty biometrista tunnistusta koskevia tarkempia kohtia. Toisena esimerkkinä mainittakoon Samsungin ja Applen puhelimissa olevat sormenjälkitunnistimet, joita on helppo huijata. Kun sormenjälki on tallennettu järjestelmään pystyy väärennetyllä sormenjäljellä kirjautumaan sisään. Tunnistin ei aisti sormenlämpöä, koska huijauksessa voi käyttää paksua kalvoa sormen päällä. (Peterson 2014; Tuppi 2014.)

On tärkeää huomioida biotunnisteita käytettäessä, että ne ovat pysyviä, muuttumattomia ja määrittävät järjestelmään päätyessään yksilön henkilöllisyyden ikuisesti. Tämän vuoksi on äärimmäisen tärkeää, että tiedot eivät missään tapauksessa joudu vääriin käsiin. Järjestelmää suunniteltaessa on siis huomioitava tarkasti tiedon säilytyspaikka, henkilöt jotka järjestelmään pääsevät ja tarkka selvitys ketkä kaikki tahot voivat tietoja käyttää. Suomen henkilötietolaissa on määritelty tarkasti käsitteet henkilötiedot ja arkaluonteiset tiedot. Biotunnisteet luokitellaan arkaluonteisiksi tiedoiksi, jonka vuoksi perustuslakivaliokunta totesi passilain muutoksen osalta kesäkuussa 2014, ettei passisormenjälkiä voida käyttää vakavampien rikosten torjunnassa. (Kari & Suuripää 2010, 36 & 38.)

Accenture teetti heinäkuussa 2014 tutkimuksen, jossa selvitettiin eri maissa kansalaisten halukkuutta luovuttaa biotunnisteensa rajavalvonnassa. Tutkimukseen osallistui 3001 vastaajaa ja tulos oli, että yli puolet vastaajista oli valmiita luovuttamaan biotunnisteensa turvatakseen maiden rajoja. Kuitenkin 68 prosenttia haluaisi tietää etukäteen kuinka tiedot pidetään suojassa, ja 67 prosenttia mihin kaikkeen tietoja voidaan käyttää. (Huittinen 2014.) Tutkimuksen pohjalta voisi todeta, että kansalaiset tuntuvat olevan melko tietoisia, kuinka henkilökohtaisista tiedoista puhutaan, kun kyse on biotunnisteesta.

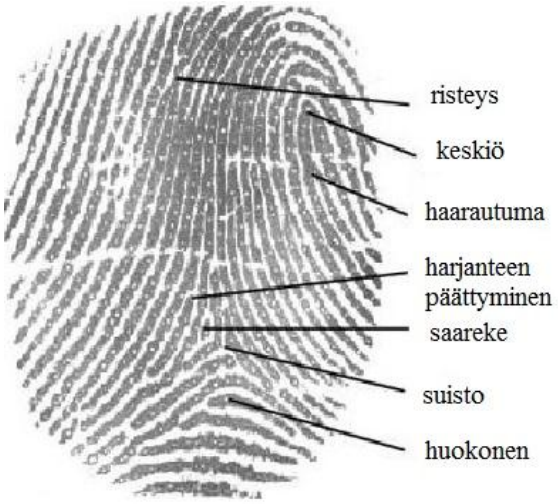
Väärinkäytökset pystytään välttämään parhaiten käyttämällä vähintään kahta eri tunnistusmenetelmää, eli käyttämällä biotunnistetta ja salasanaa tai älykorttia. Vahvin turvallisuus saavutetaan käyttämällä kaikkia kolmea samaan aikaan. (Ailisto, Ahonen & Lindholm 2005, 10.) Vaikka sormenjälkitunnistimiakin voidaan huijata, voidaan

kuitenkin todeta, että salasanan väärinkäyttö on kuitenkin paljon helpompaa kuin sormenjäljen kopion tekeminen.

5 BIOMETRISET TUNNISTUSMENETELMÄT

5.1 Sormenjälkitunnistus

Sormenjälkientunnistus on vanhin biometrinen tunnistustapa, jota henkilön tunnistuksessa on käytetty ja käytetään yhä edelleen. On kuitenkin huomioitava, että sormenjälkien järjestelmällinen käyttö on alkanut vasta 2000-luvun alussa. Menetelmä perustuu useiden erilaisten yksityiskohtien (Kuva 3.) tunnistukseen sormenpään kuvioista. Sormenpään niin sanottuja päätyyppejä on kahdeksan erilaista (Kuva 4.). Keskimääräisesti tyypillisellä nuorella miehellä harjanteita on 20,7 ja naisella 23,4 senttimetriä kohti. Sormenpään kuviointi on joka ainoalla ihmisellä erilainen ja muuttumaton, jopa identtiset kaksoset voidaan erottaa sormenjälkien perusteella. Pienet vammat sormen pintakerroksissa kuten haavat ja mustelmat eivät muuta sormenkuviointia, vaan ruhjeen parannuttua sormenpään harjut ovat taas ennallaan. Syvemmälle kudoksiin ulottuvat vammat taasen jättävät jälkeensä arven, jonka vuoksi sormenpään harjut eivät enää palaudu ennalleen. (Jain, Ross & Nandakumar 2011, 51-52.)



Kuva 3. Sormenpään kuviot. (Mainguet 2014.)

Kuva 4. Sormenjälkimallien päätyypit. (FBI:n www-sivut b.)

Sormenjälkien yksityiskohdat voidaan luokitella kolmelle eri tasolle karkeuden mukaan. Ensimmäisellä tasolla huomioidaan vain harjujen suunnat ja taajuudet. Toisella tasolla harjujen tarkat sijainnit merkitään, mutta geometria ja harjujen mitat jätetään huomioimatta. Kolmannella tasolla huomioidaan jo aivan kaikki pisteet, saarekkeet, hikihuokoset sekä tarkat harjujen mitat ja paikat. (Jain, Ross & Nandakumar 2011, 54-55, 57 & 58.)

Sormenjälkien kerääminen digitaaliseen muotoon voidaan jakaa kahteen eri kategoriaan off-line- ja on-line –menetelmiin. Tunnetuin off-line –menetelmä on paperille painettu mustesormenjälki, joka ei automaattisesti ole digitaalinen, mutta tämä onkin yleinen piirre off-line –menetelmissä. Rikospaikoilta kerättävät sormenjäljet jonkin esineen pinnasta valokuvaamalla, pölyttämällä tai kemiallisella keinolla on toinen mainittava off-line –menetelmä. (Jain, Ross & Nandakumar 2011, 60.)

On-line –mentelmät tuottavat heti skannauksen jälkeen digitaalisen kuvan sormenjäljestä. Tällaisia menetelmiä ovat muun muassa FTIR-tekniikkaan, kapasitanssiin, pietsosähköiseen ilmiöön, ultraääniheijastukseen tai lämpötilaeroihin perustuvat sensorit. Yleisin näistä käytössä oleva on kapasitanssiin perustuva tekniikka, koska ne ovat kooltaan pieniä, ja helposti sulautettavissa kannettaviin tietokoneisiin sekä mat-

kapuhelimiin. Menetelmän heikkous on sen herkkyys sähköstaattisille purkauksille, joka pystytään minimoimaan hyvällä maadoituksella. (Jain, Ross & Nandakumar 2011, 60-62.)

FTIR-tekniikan toiminta perustuu siihen, kun käyttäjä asettaa sormensa lasilevylle ja levyn reunoilla olevat ledit valaisevat sormenpään. Valo imeytyy sormeen ja heijastuu ihosta kameraan, joka lähettää kuvan järjestelmään. Menetelmää kutsutaan valon kokonaisheijastumiseksi. (Giddings 2012.)

Kun sormi painetaan kiinni sensoriin, syntyy näiden välille sähköinen jännite jota kutsutaan pietsosähköiseksi ilmiöksi. Sormenpään harjujen ja laaksojen kohdille syntyy erisuuruinen jännite, koska harjut painautuvat tiukemmin sensoriin kuin laaksot. Ultraääni-menetelmässä äänisignaaleja kohdistetaan sormenpäähän, ja palautuvat kaikusignaalit tallennetaan ja niistä saadaan muodostettua sormenjälki, jota voidaan verrata järjestelmässä oleviin jälkiin. (Jain, Ross & Nandakumar 2011, 62.)

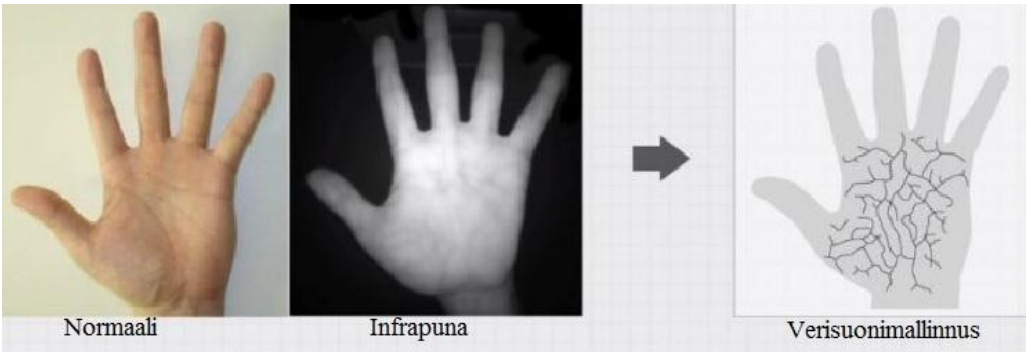
Sormenjälkikuvan on oltava laadullisesti hyvä, jotta saavutettaisiin oikea vastaavuus. Laatuun vaikuttaa useat tekijät, kuten resoluutio ja sormenpään kuvioinnin selkeys. Yleisesti ottaen skannatut sormenjäljet ovat huomattavasti tarkempia, kuin off-line –menetelmillä kerätyt näytteet. Kuluttajille myytävissä tuotteissa olevat sensorit ovat usein kapeita pyyhkäisysensoreita, jotka muodostavat viipaleista kokoamalla kokonaisen sormenjäljen käyttäjän pyyhkäistessä sormensa sensorin yli. (Jain, Ross & Nandakumar 2011, 62-64.)

Sormenjälki skannataan lukijalla, jonka jälkeen itse tunnistaminen eli vertaaminen tietokannassa oleviin sormenjälkiin voidaan tehdä kahdella eri tavalla. Tunnistus tehdään vertaamalla sormenjälkeä joko koko tietokannan näytteisiin tai kohdistamalla haku suoraan tiettyyn henkilöön. Kyseessä on siis joko verifiointi tai identifiointi.

5.2 Kämmentunnistus

Vuosisatoja ovat ennustajat ennustaneet kämmenistä tulevaisuutta ihmisille. Kämmenjäljentunnistusta biometrisena tunnistusmenetelmänä on tutkittu enemmän ja enemmän viime vuosien aikana. Tutkijat ovat pystyneet ratkomaan useita ongelmia, joiden vuoksi kämmenjälkitunnistusta ei ole voitu pitää luotettavana menetelmänä. Kämmenen linjat liittyvät myös eräisiin sairauksiin, kuten down- ja cohen-syndroomaan. Kämmenjälki koostuu tavallisesti uurteista, linjoista, rakenteesta, harjuista, deltapisteistä ja pienistä yksityiskohdista. (Jain 2012, 1007-1009.)

Kämmenestä tunnistaminen on jaettu kahteen eri kategoriaan; korkean ja matalan resoluution kuviin. Korkean resoluution kuvia käytetään esimerkiksi tunnistettaessa rikollisia, ja matalan resoluution kuvia niin sanotuissa kuluttajatuotteissa, kuten kulunvalvonnassa. Kämmenjäljen väärentäminen on huomattavasti hankalampaa kuin esimerkiksi sormenjäljen, koska kämmenen rakenne on monimutkaisempi. On myös epätodennäköisempää, että kenenkään kämmenjälki jää kokonaisuudessaan johonkin pintaan, josta sen voisi helposti kopioida. (Jain 2012, 1007-1009.)



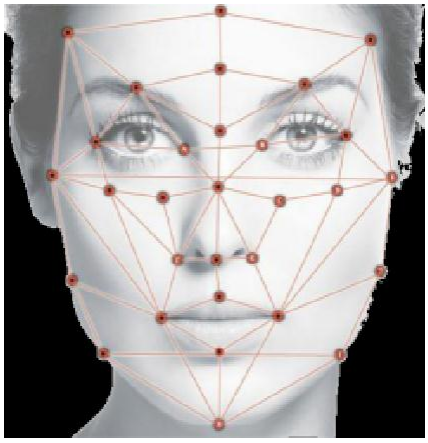
Kuva 5. Kämmenen verisuonisto (Japantodayn www-sivut 2013.)

5.3 Kasvotunnistus

Kasvot kertovat ihmisestä yhdellä vilkaisulla useita asioita, kuten iän, etnisen taustan, sukupuolen ja sen hetkisen tunnetilan. Kasvojen tunnistus on ollut tutkinnan kohteena jo vuosikymmeniä, mutta sen kohtaamat haasteet eivät ole vieläkään selätetty. Tieto siitä, miten tunnistamme tutut kasvot ruuhkassa ei ole selvää, joten sen opettaminen koneille on melko haastavaa. (Jain, Ross & Nandakumar 2011, 97.)

Yksinkertaisimmillaan kasvojentunnistus perustuu siihen, että kasvot kuvataan ja eri osien kohdat merkitään pisteillä (Kuva 6.), kuten leuka, otsa, silmät, poskipäät sekä muut selvästi erottuvat kohdat. Vertailu tapahtuu tutkimalla pisteiden välisiä mittasuhteita. Ihmisen kasvoissa on lukuisia erotettavia ominaisuuksia, näiden risteyksistä syntyy solmukohtia, joita kasvoissa on keskimäärin 80. Kasvojentunnistuksessa järjestelmä tunnistaa kasvot, tekee kohdistamalla verkkomallinnuksen, suorittaa mittaukset, etsii kuvalle vastaavuuden ja suorittaa todentamisen tai tunnistamisen. (Bonsor & Johnson 2013.)

Kasvojen ominaisuudet voidaan luokitella kolmeen eri luokkaan. Ensimmäiseen luokkaan kuuluvat karkeat helposti havaittavat ominaisuudet, kuten sukupuoli, kasvojen malli ja rotu. Tällaiset ominaisuudet pystytään tulkitsemaan myös matalan resoluution kuvista. Toisessa luokassa kasvojen komponentteja kuvataan geometrisesti ja rakenteellisesti. On tärkeää määritellä komponenttien tarkat sijainnit ja näiden mittaerot toisiinsa nähden. Kolmannessa luokassa kuvataan kasvojen mikropiirteitä, joita ovat esimerkiksi luomet, arvet ja pisamat. (Jain, Ross & Nandakumar 2011, 100-103.)



Kuva 6. Erään sovellusalgoritmin merkitsemät pisteet kasvojen komponenteille. (Heyce Technologiesin www-sivut 2014.)

Kasvojen tunnistuksessa käytettyjä kuvatyyppejä on pääasiassa kolmea erilaista: 2D, 3D sekä video. 2D-kuvista tunnistaminen on ongelmallisinta, koska kuvan pitäisi olla melko täsmällisesti samanlainen kuin alkuperäinen tallennettu otos. Pienetkin valon muutokset tai taustan sekavuus laskevat todennäköisyyttä löytää oikea henkilöllisyys. Näitä ongelmia voidaan välttää käyttämällä korkean resoluution kameroita, lämpö-

kameroita sekä PTZ-kameroita, eli kääntyvällä päällä ja motorisoidulla zoomilla varustettuja kameroita. Tällä hetkellä kuitenkin PTZ-kameran zoomin käyttö heikentää kuvan laatua huomattavasti, mutta tekniikka kehittyy koko ajan. NIR-kameralla voidaan kasvokuva ottaa myös pimeään aikaan. 2D-järjestelmien perusedellytys on, että käyttäjä on melko lähellä sensoria (1-2 metrin päässä) kuvaa otettaessa. Kohteen ollessa kauempana tuottaa järjestelmä epätarkkoja matalan resoluution kuvia. Ratkaisuna tähän on käyttää super-resoluutiota, jossa matalan resoluution kuva muunnetaan korkean resoluution kuvaksi. (Jain, Ross & Nandakumar 2011, 104-106.)

3D-järjestelmiä on kahteen eri tekniikkaan perustuvia: laserskannaukseen tai stereografiseen rekonstruktioon. Laserskannausta pidetään yleisesti ottaen tarkempana, mutta stereografinen rekonstruktio tarjoaa lähes ajantasaista ja virheetöntä kuvaa. 3D-skannauksessa ihmisen pää kuvataan 120^{o} alueelta ja tätä kutsutaan 2.5D-skannaukseksi. Täydellinen 3D-malli kasvoista saadaan yhdistämällä 3-5 kappaletta 2.5D-kasvokuvaa. 3D-kasvomalli näytetään monikulmaisena verkkorakenteena, jota järjestelmän on vaivatonta käsitellä. Kuvankäsittely muuntaa verkkorakennetta esimerkiksi tasoittamalla sitä, mutta muutokset ovat niin pieniä, että kuva pysyy lähes muuttumattomana. Myöskään valaistus ei vaikuta kuvan tunnistukseen. On kuitenkin asioita, kuten ihmisen ilmeet, ikääntyminen ja purenta, eli onko suu auki, kiinni vai raollaan, jotka vaikuttavat kuvan tunnistettavuuteen. Muita mainittavia ongelmia, jotka estävät tekniikan etenemisen toistaiseksi laajemmalti on sensorien kallis hinta sekä kuvien suuri koko. (Jain, Ross & Nandakumar 2011, 106-107.)

Videokuvaus on myös yleistymässä enemmän kasvojentunnistus järjestelmissä, koska laitteiden hinnat ovat laskeneet. Esimerkiksi viranomaisten mielenkiinto on herännyt, koska mahdollisuus hyödyntää jo valmiita valvontakamerajärjestelmiä ihmisten nopeaan tunnistamiseen reaaliajassa kuulostaa helpolta ja kustannustehokkaalta. Videokuvauksella saadaan luotettavia tuloksia johtuen suuresta materiaalin määrästä, joka tosin heikentää kuvien laatua. Koska tietoa kertyy niin paljon, että kuvat ovat yleensä resoluutioltaan verrattavissa 2D-kuviin. (Jain, Ross & Nandakumar 2011, 107-109.)

Kasvojentunnistuksen hyötyjä verrattaessa muihin biometrisiin järjestelmiin on, ettei siinä tarvita fyysistä kosketusta, se on luotettava ja turvallinen sekä voidaan toteuttaa

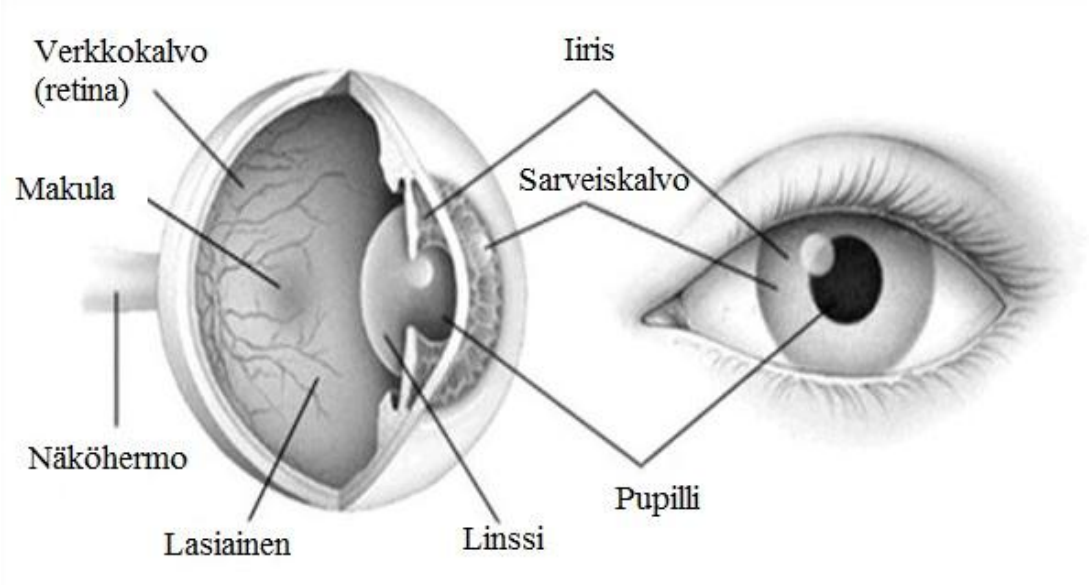
millä tahansa kameralla tai videokameralla. Järjestelmän käyttöönotto ei siis vaadi suuria investointeja. (Al-Ghamdi, B. A. S., Allaam, S. R. & Soomro, S. 2010, 28.)

5.4 Iiris-tunnistus

Iiris-tunnistus on melko uusi menetelmä yksilön tunnistamisessa. Sille haettiin ensimmäisen kerran patenttia vasta vuonna 1994. Se on kuitenkin luotettava biometrinen tunnistusmenetelmä, sillä silmän värikalvo on jokaisella uniikki ja rakenteellisesti erilainen. Iiristunnistuksen luotettavuuteen vaikuttaa kuitenkin muutama asia, kuten pupillin koko, huumeiden tai lääkkeiden käyttö sekä ikä. Silmän käyttöä biometrisena tunnisteena on tutkittu paljon, mutta iiris on kuitenkin osa johon suurin osa tutkimuksista ja käytössä olevista järjestelmistä perustuu. (FBI:n www-sivut, 114; Dunker 2003, 9; Jain, Ross & Nandakumar 2011, 141.)

Iiris on kehittynyt täydellisesti ollessamme kahdeksan kuukautta vanha, eikä sitä voida kirurgisesti muuttaa vahingoittamatta näkökykyä. Järjestelmää ei myöskään voi huijata käyttämällä ’keinotekoista iiristä’, koska sen reagointi valoon paljastaa väärennöksen. Iiriksen monimutkainen rakenne mahdollistaa algoritmit, joiden avulla järjestelmien tekeminen yksilön tunnistamiseksi on mahdollista. Iiris sijaitsee silmässä sarveiskalvon alla, mutta kuitenkin linssin edessä (Kuva 7.). (Dunker 2003, 4.)

Iiristunnistukseen perustuvista järjestelmistä voidaan erotella neljä eri vaihetta. Ensimmäinen vaihe on saada kuva silmästä. Kuvien ottamisessa käytetään erittäin valoherkkää CCD-kameraa, jolla otetut otokset ovat mustavalkoisia. Kuvia otetaan yleensä useita sarjassa ja laatuun perustuen vain muutama tallennetaan, joista saadaan riittävästi tietoa iiriksestä. Toinen vaihe on segmentointi, jossa iiris erotetaan muista silmän osista, eli sen sisempi ja ulompi raja tunnistetaan, ja kaikki häiriöt poistetaan kuvasta, kuten silmäluomet ja –ripset. Tämä on tärkeä vaihe iiriksen tunnistamisen onnistumiseksi. Kolmannessa vaiheessa suoritetaan normalisointi. Useimmiten se tehdään muuttamalla iiris napakoordinaateiksi, josta tulokseksi saadaan suorakaiteen muotoinen kokonaisuus, joka kulmasuunnassa vastaa alkuperäistä iiristä ja palstat vastaavat säteen suuntaa. Viimeisessä eli neljännessä vaiheessa koodataan ja sovitetaan kahta iirismallia keskenään. (Jain, Ross & Nandakumar 2011, 144-145.)



Kuva 7. Silmän anatomia (Unsortedinfon www-sivut.)

Kuva-alueesta riippuen kuvassa yleensä näkyvät myös silmäluomet ja ripset, sekä joissain tapauksissa kulmakarvat. Tärkeintä kuitenkin on saada iiriksestä selvä kuva, jota pystytään käsittelemään ja näin ollen vertailemaan. Kuvan huonoon laatuun vaikuttavia tekijöitä ovat liian sulkeutuneet luomet, epäonnistunut keskitys, liikesumentuma, epätasainen valaistus, matalan resoluution sensori ja liian pitkä kuvausmatka, laajentunut pupilli, sivusta otettu kuva tai piilolinssit. Kuvattavan kohteen etäisyys sensoriin saa maksimissaan olla kaksi metriä. Järjestelmään olisi myöskin syytä päivittää uusi kuva noin kahden vuoden välein, koska silmän värikalvo ikääntyy ja näin ollen silmä muuttuu. Notre Damen-yliopistossa tehdyssä tutkimuksessa osoitettiin, että kolme vuotta vanha kuva ei päästänyt käyttäjää kirjautumaan järjestelmään useissa tapauksissa. Tutkimukseen osallistui 644 ihmistä. (Jain, Ross & Nandakumar 2011, 164-165; Dunker 2003, 9; Graham-Rowe 2012.)

5.5 Retinatunnistus

Verkkokalvo eli retina sijaitsee silmän takaosassa (Kuva 7.), itse tunnistus perustuu verisuonistoon, joka verkkokalvolla on. Tätä menetelmää voidaan pitää vieläkin tarkempana ja luotettavampana kuin iiristunnistusta. Verkkokalvo säilyy muuttamattomana koko iän läpi paitsi sairastettaessa glaukoomaa tai diabetesta. Silmää kuvatta-

essa on oltava täysin liikkumatta ja maksimissaan seitsemän senttimetrin päässä sensorista. Laitteistojen korkea hinta sekä menetelmän epämukavuus ovat toistaiseksi estäneet sen laajemman käyttöönoton. (Dunker 2003, 9.)

5.6 Äänitunnistus

Biometrisia tunnistusmenetelmiä on kahdenlaisia, kuten jo aiemmin totesimme. Ääneen perustuva tunnistusmenetelmä on näitä molempia, eli siihen kuuluu fysiologisia ja käyttäytymiseen perustuvia tarkkailtavia ominaisuuksia. Fyysisiin ominaisuuksiin kuuluvat kaikki elimet, joita äänen tuottamiseen tarvitaan. Näitä ovat muun muassa ääniväylä, suu- ja nenäontelot sekä huulet. Nämä ominaisuudet pysyvät muuttumattomina ihmisen koko elämän ajan. Käyttäytyminen sen sijaan muuttuu ajan kuluessa. Siihen vaikuttavia tekijöitä ovat ikääntyminen, murteet, tunteet sekä sairaudet, kuten flunssa. (Jain, Ross & Nandakumar 2011, 33.)

Puheentunnistamiseksi on pääasiallisesti kaksi eri tekniikkaa. Tekstiin perustuvassa järjestelmässä käyttäjä toistaa ennalta määrättyä lausetta, jota verrataan aikaisemmin annettuun ääninäytteeseen. Järjestelmä hyödyntää ”Hidden Markov mallia” (HMM), jossa satunnaiset mallit tuottavat tilastollisen mallin yksilön äänestä. Teksti riippumattomassa järjestelmässä ei ole määritetty mitä käyttäjä puhuu. Hyvä pituus ääninäytteelle on 2-8 sekuntia. (Jain, Ross & Nandakumar 2011, 33; Biometrics.govin www-sivut; Myers, L 2004, 4.)

Äänitunnistus on myös edullinen vaihtoehto muihin biometrisiin tunnistusmenetelmiin verrattuna. Siinä ei tarvita kalliita erillisiä skannereita tai muita laitteita, vaan yksinkertaisimmillaan käyttäjän puhelin riittää. Äänijäljet ovat kooltaan melko pieniä, joten tallennustilaankaan ei tarvitse suuria summia investoida. Menetelmä ei kuitenkaan sovi korkeaa turvallisuutta vaativiin kohteisiin ainakaan yksinään käytettäväksi. Monibiometriikkaa käytettäessä eli yhdistettäessä äänijälki salasanaan tai avainkorttiin on turvallisuus jo melko riittävä. (Myers, L 2004, 5)

5.7 Muut tunnistusmenetelmät

Biometrisiä tunnistusmenetelmiä on lukuisia ja lähes kaikkea on tutkittu, mutta vain muutamaa voidaan käyttää korkean turvaluokituksen kohteissa. Seuraavaksi on esiteltynä muutamia pehmeän biometrian tunnistusmenetelmiä. Pehmeä biometria tarkoittaa, että tunnistettava kohde tai käytös ei ole täysin muuttumatonta yksilökohtaisesti.

5.7.1 Korvamallin tunnistus

Korvan käyttöä biometrisena tunnisteena on tutkittu jo useita vuosia. Sitä pidetään toisaalta luotettavana, koska ihmisen korva kehittyy vasta neljän kuukauden ikäisenä. Korvan kehitys pysyy muuttumattomana koko elämän, mutta tutkimuksissa on myös selvinnyt, että korva saattaa venyä painovoimasta johtuen iän aikana. Yksistään korvan tunnistus ei ole riittävän tietoturvallista, mutta yhdistettynä kasvojentunnistukseen paranee turvaluokitus huomattavasti. Tunnistus voidaan myös toteuttaa samoilla laitteilla kuin kasvojentunnistus. (Griaule Biometricsin www-sivut 2014c.)

5.7.2 Kävelytyylin tunnistus

Kävelytyylin käyttö yksilön tunnistuksessa on käytännöllistä, koska se ei vaadi minkäänlaista vuorovaikutusta käyttäjän kanssa. Näyte voidaan ottaa vaikka turvakameran videotallenteesta. Kävelytyylin tunnistaminen perustuu ajatukselle, että jokaisella ihmisellä on oma uniikki tapansa kävellä. (Abdullah ym. 2011, 358.) Menetelmää ei kuitenkaan voida pitää kovinkaan luotettavana tunnistusmenetelmänä, koska kävelytyyli muuttuu lähes jatkuvasti johtuen eri jalkineista, vammoista, kantamuksista tai jopa mielialasta.

5.7.3 Käsialan tunnistus

Käsialaan perustuvat tunnistusjärjestelmät on jaettu kahteen eri ryhmään on-line- ja off-line -allekirjoituksiin. Off-line -menetelmä perustuu staattisiin eli muuttumatto-

miin piirteisiin allekirjoituksessa. Allekirjoitus tehdään paperille, joka saadaan kameran tai skannerin avulla siirrettyä tunnistusjärjestelmään. Online-menetelmässä kiinnitetään huomiota dynaamisiin eli muuttuviin ominaisuuksiin. Allekirjoitus suoritetaan kosketusnäytölle, joka huomioi jokaisen sipaisun ja painalluksen tehdessään tunnistusta. Käsialan on todettu olevan jokaisella sen verran erilainen, että se on todettu olevan luotettava menetelmä ja tämän vuoksi laajalti maailmalla käytössä. Allekirjoituksen väärentäminenkin on kuitenkin täysin mahdollista useilla eri tavoilla, kuten esimerkiksi mallintamalla tai jäljittelemällä. Väärennöksien vuoksi onkin järjestelmiä kehitettävä koko ajan tarkemmiksi ja luotettavimmiksi. (Khan & Dhole 2014, 6879.)

6 YHTEENVETO

Biometriset tunnistusmenetelmät ovat tulleet käyttöömme, ja pelkkä salasanojen käyttö on vanhentunutta käytäntöä. Menetelmät toki ovat vanhoja ja kauan käytössä olleita, mutta vasta viimeisen kymmenen vuoden aikana ovat ne rantautuneet kannettaviin tietokoneisiimme ja puhelimiimme. Palveluita kehitellään hurjalla vauhdilla lisää ja pian huomaamme maksavamme ostoksemme vain kävelemällä kassan ohi. Useita kehonosia ja tapoja toimia on tutkitta, mutta vain muutamia voidaan pitää tarpeeksi luotettavina tunnistusmenetelminä. On kuitenkin muistettava biotunnisteiden ainutlaatuisuus ja pysyvyys antaessamme jotain niin henkilökohtaista itsestämme.

Kehitys on kuitenkin selvä, biometrinen tunnistautuminen on tullut jäädäkseen ja suurin osa väestöstä on jo antanut sormenjälkensä ja kasvokuvansa viranomaisten käyttöön hakiessaan passia tai muita matkustusasiakirjoja. Sosiaalisessa mediassa jaamme kasvokuvamme sovellusten käyttöön sen kummemmin miettimättä. Siispä voimme todeta, että suurin osa on jo biometrisen jälkensä järjestelmiin jättänyt, vielä kun lait ja tietoturva saadaan ajan tasalle tilanteen kanssa.

LÄHTEET

Aaltonen, K. & Laitinen, K. Henkilökorttilain muutostarpeita selvittävä työryhmä. Sisäministeriö. Viitattu 20.11.2014. http://www.intermin.fi/download/56100_henkilokorttilaki_esiselvitys_asettamispaatos_161014.pdf?309345544bb7d188

Abdullah, J., Chong, P-F., Ng, H., Tong, H-L., Tan, W-H. & Yap, T. T-V. 2011. Human identification based on extracted gait features. International journal on new computer architectures and their applications. The society of digital information and wireless communications. Viitattu 11.11.2014. http://sdiwc.net/digital-library/web-admin/upload-pdf/00000032.pdf

Ailisto, H., Ahonen, P. & Lindholm, M. 2005. Biometrisen tunnistamisen tietoturvallisuus ja yksityisyyden suoja. Liikenne- ja viestintäministeriö. Helsinki: Edita publishing oy.

Al-Ghamdi, B. A. S., Allaam, S. R. & Soomro, S. 2010. Recognition of human face by face recognition system using 3D. Journal of Information & Communication Technology. Viitattu 15.10.2014. http://www.biztek.edu.pk/4%20Recognition%20of%20Human.pdf

Belic, D. 2014. PayPal launches fingerprint-based payments for Galaxy S5, Galaxy Gear smart watch apps. Intomobile. Viitattu 20.11.2014. http://www.intomobile.com/2014/04/13/paypal-launches-fingerprintbased-payments-galaxy-s5-galaxy-gear-smart-watch-apps/

Biometrics.govin www-sivut. Biometrics technology and standards overview. Viitattu 22.10.2014. http://www.biometrics.gov/documents/biotechstandard.pdf

Brohlin, M. Studentens affärside: Betala med handen. Aftonbladet. Viitattu 20.11.2014. http://www.aftonbladet.se/temautbildning/article18619505.ab

Deltabitin www-sivut a. Deltabit medi – luotettavaa potilastunnistusta. Viitattu 13.11.2014. http://www.deltabit.fi/potilastunnistus/

Deltabitin www-sivut b. Referenssit. Viitattu 14.11.2014. http://www.deltabit.fi/kulunvalvonta/referenssit/

Digitodayn www-sivut 2013. Salasanat joutavat tunkiolle. Viitattu 25.11.2014. http://www.digitoday.fi/tietoturva/2013/05/13/salasanat-joutavat-tunkiolle/20136731/66

Dunker, M. 2003. Don't blink: Iris recognition for biometric identification. SANS Institute. Viitattu 17.10.2014. http://www.sans.org/reading-room/whitepapers/authentication/dont-blink-iris-recognition-biometric-identification-1341

FBI:n www-sivut a. Biometric center of excellence. Iris recognition. Viitattu: 2.9.2014. http://www.fbi.gov//about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/files/iris-recognition.pdf

FBI:n www-sivut b. Fingerprints & other biometrics. Fingerprint identification. Viitattu 15.9.2014. http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/fingerprint-overview

Fido Alliancen www-sivut. Google launches security key, world's first deployment of fast identity online universal second factor (FIDO U2F) authentication. Viitattu 25.11.2014. https://fidoalliance.org/news/item/google-launches-security-key

Fujitsun www-sivut a. PalmSecure-kämmentunnistin. Viitattu 2.10.2014. http://www.fujitsu.com/fi/solutions/high-tech/tietoturva/biometrics/

Fujitsun www-sivut b. Fujitsu builds Japan's first palm vein authentication system for ATMs. Viitattu 20.11.2014. http://www.fujitsu.com/global/about/resources/news/press-releases/2012/0926-01.html

Giddings, J. 2012. Multi-touch keyboard and mouse. Kickstarter. Viitattu 7.10.2014. https://www.kickstarter.com/projects/1116966310/multi-touch-keyboard-and-mouse

Graham-Rowe, D. 2012. Ageing eyes hinder biometric scans. Nature. Viitattu 21.11.2014. http://www.nature.com/news/ageing-eyes-hinder-biometric-scans-1.10722

Griaule Biometricsin www-sivut. 2014a. Comparison of biometrics. Viitattu 11.11.2014. http://www.griaulebiometrics.com/en-us/book/understanding-biometrics/introduction/types/comparison-of-biometrics

Griaule Biometricsin www-sivut. 2014b. History of biometrics. Viitattu 15.9.2014. http://www.griaulebiometrics.com/en-us/book/understanding-biometrics/introduction/history

Griaule Biometricinsin www-sivut 2014c. Ear. Viitattu 22.10.2014. http://www.griaulebiometrics.com/en-us/book/understanding-biometrics/introduction/types/behavioral/ear

Bonsor, K. & Johnson, R. 2013. How facial recognition systems work. HowStuffWorks. Viitattu 14.10.2014. http://electronics.howstuffworks.com/gadgets/

Heyce Technologiesin www-sivut. 2014. Biometric face recognition systems – a new world of touch free authentication. Viitattu 21.9.2014. http://www.heyce.com/face_recognition_systems.html

Huittinen, H. 2014. Kansalaiset valmiita biotunnisteiden käyttöönottoon rajavalvonnassa. Accenture. Viitattu 11.11.2014. http://www.accenture.com/fi-en/company/newsroom-finland/Pages/citizens-willing-introduction-biometrics-border-control.aspx

Jain, A. K., Ross, A. A. & Nandakumar, K. 2011. Introduction to biometrics. Springer.

Jain, V.K. 2012. International journal of engineering research and applications. A technique to ROI of palmprint for palmline matching. IJERA.

Japantodayn www-sivut. 2013. Fujitsu boosts security for multi-service palm-vein authentication system. Viitattu 21.9.2014. http://www.japantoday.com/category/technology/view/fujitsu-boosts-security-for-multi-service-palm-vein-authentication-system

Jordan, G. 2014. FIDO Alliance members demonstrate new authentication standards. SecureIDNews. Viitattu 25.11.2014. http://secureidnews.com/news-item/fido-alliance-members-demonstrate-new-authentication-standards/

Kari, J. & Suuripää, K. 2010. Selvitys passisormenjälkitietojen käyttämisestä vakavimpien rikosten torjunnassa. Sisäasiainministeriö. Viitattu 2.9.2014. http://www.intermin.fi/julkaisu/202014?docID=54166

Khan, S. & Dhole, A. 2014. A review on offline signature recognition and verification techniques. International journal of advanced research in computer and communication engineering. Viitattu 11.11. 2014. http://www.ijarcce.com/upload/2014/june/IJARCCE2F%20a%20sameera%20A%20Review%20on%20Offline.pdf

Krautsuk, S. 2014. Ulkonäöllä on väliä – pian voit maksaa ostokset naamallasi. YLE. Viitattu 13.11.2014. http://yle.fi/uutiset/ulkonaolla_on_valia__pian_voit_maksaa_ostokset_naamallasi/7613475?

Mainguet, J-F. 2014. Fingerprint, palmprint, pores. Viitattu 23.9.2014. http://fingerchip.pagesperso-orange.fr/biometrics/types/fingerprint.htm

Myers, L. 2004. An exploration of voice biometrics. SANS Institute. Viitattu 22.10.2014. http://www.sans.org/reading-room/whitepapers/authentication/exploration-voice-biometrics-1436

National Law Enforcement Museum Insiderin www-sivut. Bertillon system of criminal identification. Viitattu 7.10.2014. http://www.nleomf.org/museum/news/newsletters/online-insider/november-2011/bertillon-system-criminal-identification.html

Peterson, Andrea. 2014. . ‘The biometrics revolution is already here – and you may not be ready for it ’. The Washington Post. Viitattu 14.11.2014. http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/17/the-biometrics-revolution-is-already-here-and-you-may-not-be-ready-for-it/

Secure Linkin www-sivut 2014. Ajankohtaista. Viitattu 25.11.2014. http://www.securelink.fi/ajankohtaista/

Seppälä, P. 2009. Avain, jota et hukkaa. Asunto & Kiinteistö. Viitattu 13.11.2014. http://www.asuntokiinteisto.fi/lehti.php?sub=artikkeli&jid=31

Suomen Standardisoimisliiton www-sivut. Biometriikka. Viitattu 23.9.2014. http://www.sfs.fi/standardien_laadinta/sfs_n_tekniset_komiteat_ja_seurantaryhmat/it-standardisointi/it_-_aihealueet/biometriikka

Tacke, U. 2013. Opioidikorvaushoidossa testataan sormenjälkeen perustuvaa huumeseulontaa ja lääkekelloa. Itä-Suomen yliopisto. Viitattu 13.11.2014. http://www.uef.fi/fi/uef/-/opioidikorvaushoidossa-testataan-sormenjalkeen-perustuvaa-huumeseulontaa-ja-laakekelloa

Talouselämän www-sivut 2014. Samsungin seuraava lippulaiva lukee iiriksiä? Viitattu 20.11.2014. http://www.talouselama.fi/uutiset/samsungin+seuraava+lippulaiva+lukee+iiriksia/a2225354

Tuppi, J. 2014. Näin Samsung Galaxy S5:n sormenjälkilukijaa huijataan. Puhelinvertailu. Viitattu 21.11.2014. http://www.puhelinvertailu.com/uutiset/2014/04/15/nain_samsung_galaxy_s5_n_sormenjalkilukijaa_huijataan

Unsortedinfon www-sivut. Introduction of biomatrics. Iris recognition. Viitattu 22.10.2014. http://www.unsortedinfo.com/introduction-of-biomatrics

Åström-Kupsanen, M. 2007. Sormenjälkitunnistaminen yleistyy – miten käy tietoturvan? YLE. Viitattu 20.11.2014. http://yle.fi/aihe/artikkeli/2007/01/25/sormenjalkitunnistaminen-yleistyy-miten-kay-tietoturvan