Liljander Akseli

# BIOMETRISTEN TODENNUSMENETELMIEN TIETOTURVA JA KÄYTETTÄVYYS – SORMENJÄLKI JA SILMÄN IIRIS BIOMETRISINÄ TUNNISTEINA

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2016

# TIIVISTELMÄ

Liljander, Akseli
Biometristen todennusmenetelmien tietoturva ja käytettävyys – sormenjälki ja silmän iiris biometrisinä tunnisteina
Jyväskylä: Jyväskylän yliopisto, 2016, 33 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja: Koskelainen, Tiina

Ihmiset joutuvat päivittäin todentamaan identiteettinsä erilaisin keinon saadakseen pääsyn esimerkiksi johonkin palveluun tai laitteeseen. Perinteisten, esimerkiksi käyttäjänimeen ja salasanaan tai ulkoisesti generoitavaan koodiin perustuvien todennusmenetelmien lisäksi erilaiset käyttäjän luonnollisiin piirteisiin perustuvat biometriset todennusmenetelmät ovat kasvattaneet suosiotaan viime vuosina. Biometriaa hyödynnetään esimerkiksi korkean turvatason kulunvalvonnassa, valtioiden rajavalvonnassa ja yksityishenkilöiden matkapuhelimissa. Tietoturvan ja käytettävyyden näkökulmat ovat tärkeitä, jotta voidaan luoda biometrisia todennusjärjestelmiä, joissa saavutetaan tyydyttävä turvataso ja säilytetään kuitenkin palvelun käytön ja todentamistilanteen käyttäjäystävällisyys sekä mielekkyys. Puutteellinen tietoturva voi aiheuttaa arkaluontoisten tietojen ja toimintojen päätymisen vääriin käsiin. Tietoturvan taso voi kuitenkin olla joillekin käyttäjille näkymätön ja tuntematon aihe, kun taas käytettävyys on suoraan vaikutuksessa käyttäjän tyytyväisyyteen ja vaikuttaa myös suuresti ostopäätökseen. Tässä tutkielmassa käsitellään tietoturvaa ja käytettävyyttä biometrisissä sormenjäljen ja iiriksen tunnistuksen menetelmissä. Tutkielman tavoitteena on selvittää näiden todennusmenetelmien tietoturvan ja käytettävyyden suurimpia ongelmia, sekä pyrkimyksiä niiden ratkaisemiseen. Lisäksi pyritään selvittämään, miten tietoturvaa ja käytettävyyttä mitataan biometrisessa käyttäjäntodentamisessa. Tutkielma on kirjallisuuskatsaus, jonka pääasiallisia lähteitä ovat alan konferenssi- ja lehtiartikkelit. Tutkielmassa havaitaan biometrisessä todennuksessa esiintyvän käytettävyyden ongelmia, jotka johtuvat esimerkiksi käyttäjän syntyperästä, ikääntymisestä, työhistoriasta, onnettomuudesta tai ympäristöolosuhteista. Pyrkimyksiä näiden ongelmien ratkaisemiseksi löydetään menetelmien tunnistuksen algoritmien, käyttöliittymien, laitteiden ja kuvaustekniikoiden kehittämisen saralta. Tietoturvan suurimmaksi ongelmaksi taas havaitaan ihmisen biometristen, yksilöivien tunnisteiden rajallinen määrä, sekä niiden vaihdettavuuden ja korvattavuuden puute. Ongelman korjaamiseksi havaitaan olevan kehitetty erilaisia kumottavissa olevan biometrian menetelmiä ja algoritmeja.

Asiasanat: biometria, todentaminen, tietoturva, käytettävyys, sormenjäljet

# ABSTRACT

Liljander, Akseli
Data security and usability in biometric user authentication methods – fingerprint and iris as biometric samples
Jyväskylä: University of Jyväskylä, 2016, 33 p.
Information Systems, Bachelor's Thesis
Supervisor: Koskelainen, Tiina

People run into different kinds of identity-claim scenarios in their daily lives. Traditional means of user authentication include usernames and passwords or externally generated codes. However, lately biometric methods, which are based on user's natural features, have gained popularity as well. Biometry is utilized, for an example, in high-security access control, national border control and personal mobile phones.The aspects of data security and usability are crucial for creating biometric systems, which achieve the required security level, while maintaining the user-friendliness and reasonableness of using the service. Lack of proper security might cause sensitive data to end up in the wrong hands. However, data security might be an invisible and unknown area for some users, while usability is tightly connected to user satisfaction and also affects buying decisions greatly. This thesis studies data security and usability in biometric user authentication technologies, emphasizing the methods of user authentication via fingerprint and iris recognition. The thesis aims to identify the main problems of data security and usability in these methods, and the steps, which have been taken to adjust them. The meters of evaluating data security and usability on biometry was also researched. The thesis was conducted as a literary review mainly based on conference and journal articles on the field of information systems. It was perceived, that biometric authentication includes usability problems which are caused by innate features, aging, working history, accidents or environmental effects. To adjust these problems, methods of improving the algorithms, user interfaces, devices and imaging have been suggested. The greatest problem in the area of data security was found to be the lack of different, unique biometric samples in a human being, and the absence of possibilities in changing and replacing those samples. To overcome this problem, many methods and algorithms of cancelable biometrics have been created.

Keywords: biometry, authentication, data security, usability

# KUVIOT



# TAULUKOT

**SISÄLLYS**

# 1 JOHDANTO

Todentamisella tarkoitetaan prosessia, jossa käyttäjän identiteetin vastaavuus väitettyyn identiteettiin varmistetaan (SANS™ Institute, s.a.). Perinteisiä todennusmenetelmiä ovat muun muassa käyttäjänimeen ja salasanaan perustuvat teknologiat. Salasanaan perustuvan todennuksen vahvuutta voidaan parantaa esimerkiksi puhelimeen tai sähköpostiin lähetettävällä, tai ulkoisesta laitteesta generoitavalla uniikilla koodilla, joka täytyy identiteettiä todentaessa syöttää palveluun käyttäjänimen ja salasanan lisäksi. Nykyään myös biometria tarjoaa monenlaisia keinoja identiteetin todentamiseen. Biometrinen todentaminen tarkoittaa henkilön tunnistamista fysiologisten ja käytökseen perustuvien ominaispiirteiden avulla (Adamsson, Hakkala, & Hyrynsalmi, 2015). Biometrisiä todentamiskeinoja ovat muun muassa äänentunnistus, sormenjälkitunnistus, kasvojentunnistus ja erilaisten silmän piirteiden tunnistaminen. Tässä tutkielmassa käsitellään pääasiassa sormenjälkeen ja silmän iirikseen perustuvia käyttäjän todentamisen menetelmiä.

Kansainvälisen standardisoimisjärjestö The International Organization of Standardsin (ISO) ISO 13407 -standardi määrittelee käytettävyyden tiettyjen käyttäjien kykynä käyttää tuotetta saavuttaakseen määritellyt päämäärät tietyssä käyttökontekstissa tehokkaasti ja tyydyttävästi (Theofanos, Micheals, & Stanton, 2009). Tässä tutkielmassa päämäärällä ja käyttökontekstilla tarkoitetaan käyttäjän identiteetin todentamista johonkin laitteeseen, palveluun tai järjestelmään pääsyn saamiseksi. Käyttäjän todentamisessa on tärkeää, että onnistutaan valitsemaan menetelmä, joka on tarpeeksi turvallinen palvelun ja sen sisältämän informaation kannalta. Käyttäjän näkökulmasta tärkeää on kuitenkin myös todennuksen käytettävyys. Tietoturvaltaan parhaimmat menetelmät saattavat aiheuttaa käyttäjälle ylimääräistä vaivaa, ja toisaalta kaikista helppokäyttöisimmät todennusmenetelmät saattavat olla liian helppoja murtaa tai kopioida. Etenkin jotkut biometriset menetelmät saattavat myös olla hankalia tai epämukavia käyttää esimerkiksi julkisella paikalla. Käytettävyys tulee ottaa huomioon myös suunnitellessa tuotteen markkinointia ja käyttäjätyytyväisyyttä. Tietoturva voi olla näkymätön elementti, jota asiakas ei välttämättä ymmär-

rä. Käytettävyys puolestaan vaikuttaa suoraan asiakkaaseen ja asiakkaan käyttökokemukseen, ja voi olla yhteydessä ostopäätökseen.

Tutkielman aiheeksi todennusmenetelmien joukosta on valikoitujuuri biometriset menetelmät, koska biometria on jatkuvasti kehittyvä ja yleistyvä ala. Biometriaa on vasta viime aikoina alettua tutkia enemmän, erityisesti käytettävyyden näkökulmasta. Se on myös muita käyttäjäntodentamisen kategorioita laajempi ja monipuolisempi. Tutkielma käsittelee käytössä olevia biometrisia todentamismenetelmiä sekä niiden käytettävyyttä ja tietoturvaa, keskittyen pääasiassa sormenjäljen ja silmän iiriksen tunnistamisen menetelmiin. Nämä menetelmät on valikoitu käsiteltäviksi, sillä niistä löytyy tutkielman kirjoittamisen hetkellä eniten aikaisempaa tutkimusta. Lisäksi ne edustavat kahta biometrisen tunnistamisen pääasiallista kategoriaa, eli kosketukseen perustuvaa ja kontaktitonta tunnistamista. Tutkielmassa tarkastellaan menetelmien käytettävyyttä ja tietoturvaa sekä perinteisten numeroarvoisten mittareiden avulla, että konkreettisten tietoturvan ja käytettävyyden ongelmien kautta.

Pääasiallinen tutkimuskysymys on, mitkä ovat biometrian, sormenjälkitunnistuksen ja silmän iiriksen tunnistamisen tietoturvan ja käytettävyyden suurimmat ongelmat? Toinen tutkimuskysymys kuuluu, millä tavoin menetelmien tietoturvaa ja käytettävyyttä on ehdotettu parannettaviksi? Lisäksi luodaan yleiskatsaus biometrian tietoturvan ja käytettävyyden mittareihin. Tutkielma on toteutettu kirjallisuuskatsauksena, jossa pääasiallisina kirjallisuuden lähteinä toimivat Institute of Electrical and Electronics Engineers- (IEEE) ja Association for Computing Machinery (ACM) -julkaisukirjastot. Aiheen rajauksen apuna toimivat pääasiallisten lähdemateriaalien lisäksi aiemmat kandidaatin tutkielman tasoiset kirjallisuuskatsaukset, erityisesti Jyväskylän Yliopiston julkaisukirjastossa.

Tutkielmassa selvitetään aiheeseen liittyvän kirjallisuuden perusteella yleisesti biometrisen käyttäjäntodennuksen, sekä sormenjälkitunnistuksen ja iiriksentunnistuksen käytettävyyden ja tietoturvan tunnuslukuja. Tutkielmassa nostetaan esille myös teknologioiden suurimpia tietoturvariskejä ja käytettävyyden ongelmia. Lisäksi selvitetään ympäristöolosuhteita ja ihmisten fyysisiä ominaisuuksia, jotka heikentävät menetelmien tietoturvaa merkittävimmin. Suurimpiin ongelmiin liittyen tarkastellaan myös niihin ehdotettuja konkreettisia ratkaisuja. Tutkielman perusteella saa yleiskuvan biometristen käyttäjäntodennusmenetelmien tietoturvan ja käytettävyyden lähihistoriasta ja nykytilasta, sekä ongelmakohdista, joihin biometrian tietoturvan ja käytettävyyden kehityksen ja tutkimuksen huomiota tulisi tulevaisuudessa kiinnittää.

Seuraavassa sisältöluvussa käydään läpi käyttäjän todentamisen käsitteistöä ja kategorioita, sekä esitellään sormenjälkeen ja silmän iiriksen perustuvat biometrisen todentamisen menetelmät. Luvussa kolme tarkastellaan käytettävyyden ja tietoturvan mittareita ja käsitteistöä, sekä niiden toteutumista biometriassa yleisesti. Luvussa neljä jatketaan käytettävyyden ja tietoturvan tarkastelua mittaustulosten ja käytännön ongelmia kautta, keskittyen sormenjäljen ja iiriksen tunnistuksen teknologioihin. Tämän jälkeen siirrytään yhteenvetoon ja pohdintaan.

# 2 KÄYTTÄJÄN TODENTAMINEN

Käyttäjän todentamisella saavutetaan pääsy tietoverkkoon tai laitteistoon, jossa määritellyt palvelut on räätälöity käyttäjälle tai jossa kyetään suorittamaan määrättyjä tehtäviä. Todentamisen jälkeen käyttäjälle annetaan pääsy esimerkiksi yrityksen sisäiseen verkkoon, tietokantoihin, rakennuksiin, ajoneuvoihin ja niin edelleen. (Braz & Robert, 2006.) Eräs tapa luokitella todentamismenetelmät on jakaa ne kolmeen ryhmään: Jotain, mitä sinulla on, jotain, mitä tiedät ja jotain, mitä luontaisesti olet (Gorman, 2003). Tässä tutkielmassa keskitytään fyysisiin piirteisiin perustuviin biometrisiin teknologioihin. Tässä luvussa esitellään käyttäjän todentamisen menetelmien kolme kategoriaa, sekä tarkemmin sormenjälkeä ja silmän iiristä hyödyntävät todentamismenetelmät, jotka kuuluvat luontaisiin ominaisuuksiin perustuvaan kategoriaan, eli biometriseen todentamiseen.

## 2.1 Todentamismenetelmät

Gormanin (2003) luettelemissa kolmessa todentamismenetelmien luokassa omistuksella tarkoitetaan jotakin, ulkoista, fyysistä esinettä, jolla käyttäjä voidaan tunnistaa. Se voi olla esimerkiksi avain, älykortti tai sormus. Tällainen todentamisen tapa on helppokäyttöinen, mutta epäkäytännöllinen, sillä esinettä joutuu kantamaan mukanaan. Myös turvallisuus on melko huono, sillä joku toinenkin henkilö voi käyttää kyseistä esinettä. (Gorman, 2003.)

Tietoon perustuvat todennusmenetelmät taas voidaan pitää muistissa ja jäljentää sieltä. Esimerkkejä ovat PIN-koodi tai pyyhkäisykuvio. Ne ovat suhteellisen helppoja käyttää ja käytännöllisiä. Ne ovat kuitenkin kognitiivisesti rasittavia, sillä ne täytyy pitää muistissa, ja tarjoavat ainoastaan keskiverron turvallisuustason. (Gorman, 2003.) Heikkoutena niillä on myös todennäköisyys tulla kadotetuksi, varastetuksi tai helposti väärennetyiksi (Leo, Marco & Distante, 2014).

Viimeisellä ryhmällä tarkoitetaan menetelmiä, jotka perustuvat ihmisen luonnollisiin biometrisiin ominaisuuksiin (Gorman, 2003). Biometriset teknologiat todentamisessa ovat erittäin helppokäyttöisiä ja melko käytännöllisiä, mutta voivat olla kalliita laskennallisessa tai vaadittavan laitteiston mielessä. Lisäksi ne vaativat paljon ylläpitoa ja voivat kärsiä luotettavuusongelmista. (Liang, Fleming, & Wang, 2014). Biometriset teknologiat voidaan jakaa fyysisiin ominaisuuksiin perustuviin menetelmiin ja käytökseen perustuviin menetelmiin. Käytökseen perustuvia menetelmiä ovat esimerkiksi puheeseen, allekirjoitukseen tai näppäinten painalluksiin perustuva todentaminen. Fyysisiin piirteisiin perustuvat menetelmät voivat olla esimerkiksi silmän värikalvon eli iiriksen tai verkkokalvon kuvaus, sormenjälki tai kasvojen tunnistus. (Rodrigues & Santos, 2013.) Faundez-Zanuy (2006) kuitenkin huomauttaa, että jako fyysisiin ominaisuuksiin perustuviin ja käytökseen perustuviin menetelmiin on melko keinotekoinen. Hänen perustelee väitettään sillä, että esimerkiksi äänen muodostumiseen vaikuttavat ääntöväylän fyysiset ominaisuudet ja toisaalta opittu käytös vaikuttaa esimerkiksi tapaan painaa sormi tunnistimeen tai tapaan katsoa kameraan.

Clarken (1994) mukaan hyvän biometrisen piirteen tulee sisältää seitsemän ominaisuutta. Ensimmäinen ominaisuus on universaalisuus, eli jokaisella ihmisellä täytyy olla kyseinen piirre. Toinen vaatimus on yksilöllisyys, eli ominaisuuden perusteella pitäisi kyetä erottamaan kaksi ihmistä toisistaan. Kolmanneksi, ominaisuuden tulisi olla pysyvä, eli riippumaton esimerkiksi ajan kulumisesta tai vaihtuvista ilmasto-oloista. Neljänneksi, ominaisuuden pitäisi olla kerättävissä ja kvantitatiivisesti mitattavissa. Viidenneksi, ominaisuuden tulisi olla yleisesti hyväksytty, eli ihmisten tulisi kyetä käyttämään teknologiaa tuntematta sitä esimerkiksi ärsyttäväksi tai tunkeilevaksi. Kuudenneksi, piirteen tulee kyetä hyvään suorituskykyyn tunnistuksen tarkkuudessa ja tunnistuksen kestossa. Viimeiseksi, vilpillisten ihmisten ja tekniikoiden kyvyn huijata biometristä järjestelmää tulisi olla hyvin vähäpätöinen.

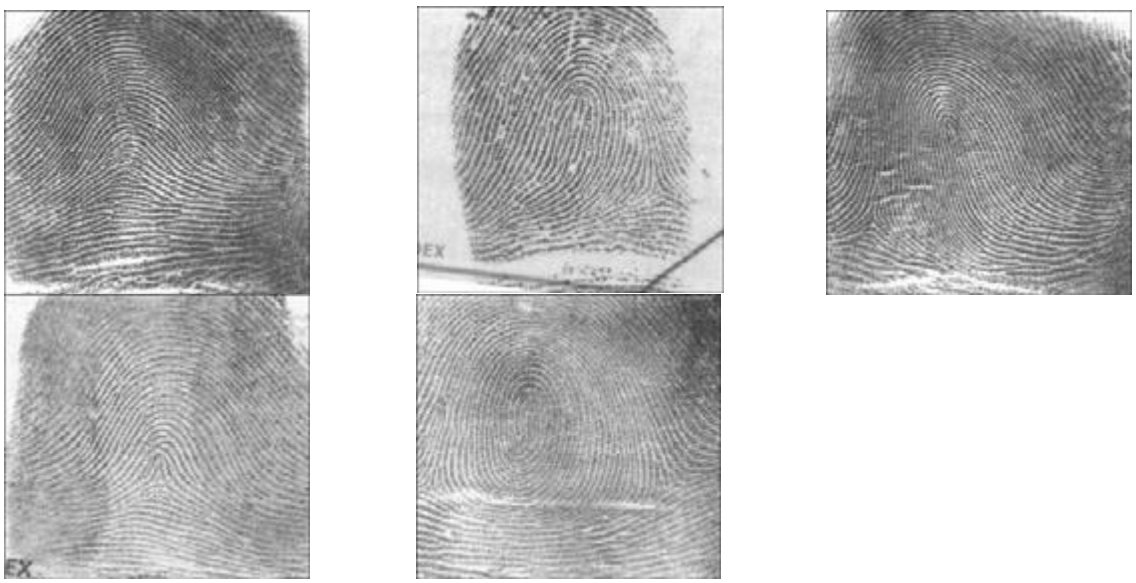
Biometriaa on jo käytössä tai suunnitteilla käyttöönotettavaksi monilla toimialoilla. Elliott, O'connor, Bartlow, Robertson ja Guest (2015) mainitsevat muun muassa automaattisen rajanvalvonnan, pankkitoiminnan ja terveydenhoidon alan hyödyntävän toiminnassaan biometrisiä teknologioita. Myös korkean turvatason kulunvalvonnassa on päädytty käyttämään biometriaa (Meenakshi & Padmavathi, 2009). Coventry, De Angeli, Johnson & McCabe (2003) tarkastelevat biometrian soveltamista pankkiautomaattien käyttäjän todentamisen käytännöksi. Heidän mukaansa pankin tai pankkijärjestelmän käyttäjien määrä on niin suuri, että jo pelkän prosessointiajan vuoksi järjestelmä, jossa käyttäjä tunnistettaisiin esimerkiksi sormenjäljen avulla, olisi mahdoton. Tämän vuoksi turvaudutaan menetelmään, jossa pyritään todentamaan käyttäjän väitetty henkilöllisyys vertaamalla kahta näytettä toisiinsa.

Jain (2007) ja Kowtkon (2014) mukaan viime vuosina eniten huomiota saaneet ja eniten käytössä olevat biometriset teknologiat ovat sormenjäljen, iiriksen ja kasvojen tunnistamisen menetelmät. Tähän tutkielmaan on valittu tarkasteltavaksi sormenjäljestä ja silmän iiriksestä saataviin näytteisiin perustuvat bio-

metriset käyttäjän todentamisen menetelmät. Sormenjäljen tunnistus on valittu tutkielmaan esimerkiksi fyysistä kosketusta vaativasta menetelmästä. Silmän iiris taas on valittu esimerkiksi kontaktittomasta biometrisen tunnistamisen menetelmästä. Seuraavaksi käsitellään tarkemmin tämän tutkielman pääasiallisen mielenkiinnon kohteena oleviin sormenjäljen ja iiriksen tunnistamiseen liittyviä ominaisuuksia ja käyttökohteita.

## 2.2 Sormenjälki

Perinteisesti sormenjälkitunnistuksella tarkoitetaan automaattista biometristä menetelmää, jossa pyritään todentamaan kaksi vertailtavaa sormenjälkeä samaksi. Tunnistaminen voi perustua erimerkiksi niin sanotun Henryn menetelmän mukaan sormenjäljen kaarteisiin, pyörteisiin tai silmukkoihin (kuvio 1) (Bundesamt für Sicherheit in der Informationstechnik, 2004). Sormenjäljen tunnistava laite voi kuvata jäljen optisella kameralla, ultraäänellä tai kapasitanssisilla, eli sähkövarausta hyödyntävillä sensoreilla (Maeva & Severin, 2009). Perinteisen sormenjäljen kuvioihin perustuvan tunnistamisen lisäksi sormea voidaan hyödyntää biometrisessä tunnistamisessa esimerkiksi kuvaamalla sen verisuonien muodostamaa kuviota (Kathuria, 2010) tai pyyhkäisemällä sormi lämpötunnistimen yli (Coventry ym., 2003).



KUVIO 1 Sormenjäljen matala kaari, vasemmanpuoleinen silmukka, oikeanpuoleinen silmukka, korkea kaari ja pyörre (Bundesamt für Sicherheit in der Informationstechnik, 2004)

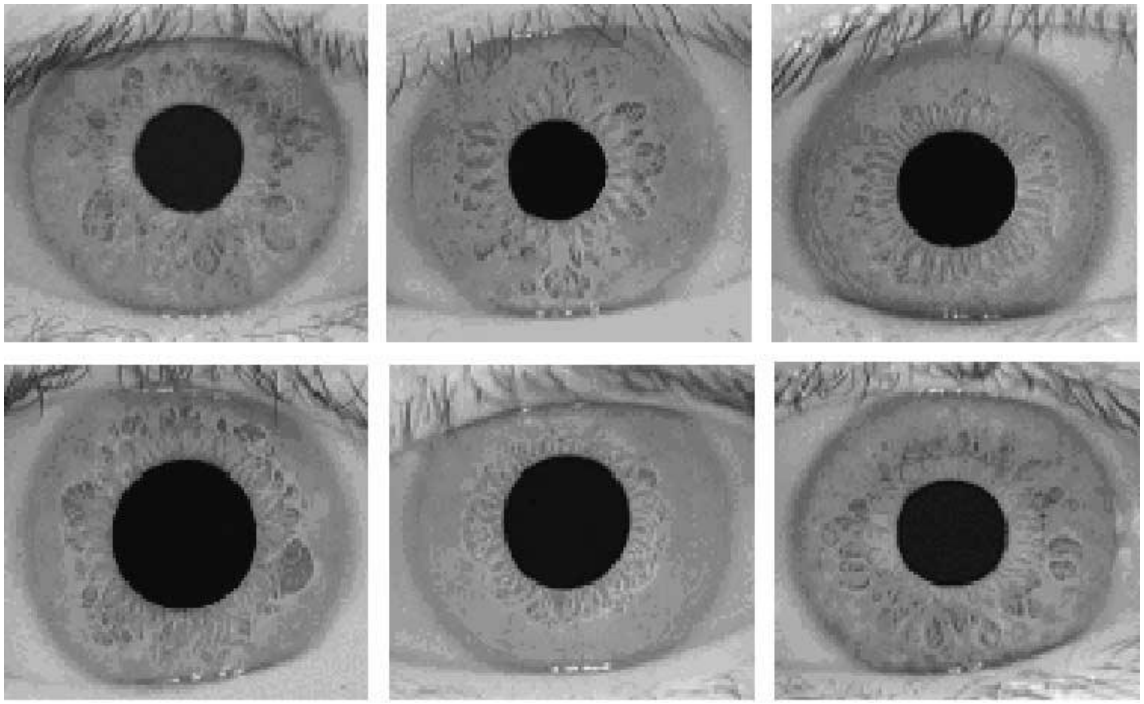
Sormenjäljen käyttö biometrinä on vanhin tietokoneavusteinen tunnistusmenetelmä, ja se on menetelmistä laajimmin käytössä tänä päivänä (Faundez-Zanuy, 2006). Sormenjälki on yleisin rikospaikalle jätetty todiste, jolla rikoksen tekijä jäljitetään. Tämän vuoksi sormenjälkitunnistuksella on kaikista automaattisista biometrisistä todennusmenetelmistä parhaat lähtökohdat, erityisesti viran-

omaistyön saralla. Nykyisellään onkin jo olemassa kattavia sormenjälkitietokantoja. (Maeva & Severin, 2009.) Sormenjälkitunnistusta käytetään yleisesti mm. passeissa kasvattamassa todennusprosessin luotettavuutta (Maple & Norrington, 2006). Sormenjälki on sisältynyt myös uusiin suomalaisiin passeihin vuodesta 2009 alkaen. Sormenjälkitunnistusta on lisäksi ehdotettu yhdeksi vaihtoehdoksi PIN-koodin korvaajaksi pankkiautomaateissa (Ashokarajanl, Angelinjosphia, Gayathd, Rajendran, & Anandhakumar, 2013).

Sormenjäljen tunnistamisen teknologia on läsnä myös ihmisten arjessa jopa päivittäin. Kosketuksella toimivien älylaitteiden määrän kasvu on lisännyt tarvetta yhteensopiville todennusmenetelmille (Koundinya ym., 2014) ja useat matkapuhelimien, tablettien ja muiden älylaitteiden valmistajat ovatkin lisänneet laitteisiinsa mahdollisuuden sormenjäljen tunnistamiseen perustuvaan kirjautumiseen. Myös vähemmän kriittisissä, matalamman tietoturvan vaativissa kohteissa on otettu sormenjälkitunnistusteknologiaa käyttöön. Esimerkiksi Yhdysvaltojen Disney World -huvipuistoissa käytetään automaattista sormenjälkitunnistusta todentamaan kausilippujen omistajat (Ailisto, Ahonen, & Lindholm, 2005).

## 2.3 Silmän iiris

Silmästä voidaan ottaa biometrinen tunniste usealla tavalla. Verkkokalvoon perustuvassa tunnistuksessa skannataan käyttäjän verkkokalvon verisuonten muodostamia kuvioita (Ashrafil Amin & Yan, 2009). Verkkokalvon ohella toinen yleisesti käytetty silmän ominaisuuksin perustuva biometri on silmän iiris. Iiriksen tunnistuksessa hyödynnetään yhden tai molempien silmien yksilöllisiä, silmän sisällä suojassa olevia vakaita kuvioita (kuvio 2). Ne ovat selvästi näkyvissä, mutta hyvin suojassa ajan ja ympäristön kuluttavalta vaikutukselta. Lisäksi ne voidaan nähdä hieman pidemmänkin matkan päästä. (Daugman, 2009.) Kuten sormenjälki, iiriksen tekstuurit ovat vakaita ja yksilöiviä, jopa identtisten kaksosten tapauksissa, ja niitä on hyvin vaikea väärentää kirurgisesti (Leo ym., 2014). Connell ja Ratha (2013) kertovat iiriksentunnistuksen suosion kasvaneen, koska se on tarkka, siinä tarvitut sensorit ovat halpoja ja sen käytettävyys on parempi kuin kosketusta vaativat biometriset menetelmät kuten sormenjäljen tunnistus.



KUVIO 2 Esimerkkejä kuvatuista iirisnäytteistä (Ma, Tan, Wang, & Zhang, 2004)

Harvinaisempia silmän ominaisuuksiin perustuvia biometrisen todentamisen menetelmiä ovat esimerkiksi silmän liikkeiden seuraaminen (Narcizo, Queiroz & Gomes, 2013) tai silmänräpäytyksien aivoaaltoja mittaava teknologia (Bertram, Sattel, Hohmann & Wiegert, 2008). Silmän ominaisuuksiin perustuva biometrinen todentaminen sopii sormenjälkeä paremmin ihmisille, jotka eivät kulttuurillisista, hygienia- tai muista syistä tahdo fyysistä kosketusta sensorin kanssa. Toisaalta silmänkuvaustekniikkaan pohjautuvat menetelmät herättävät huolta silmään kohdistuvista terveyshaitoista, vaikka tällaisista vaikutuksista ei ole julkaistu tieteellistä näyttöä (El-Abed, Giot, Hemery & Rosenberger, 2010). Tässä tutkielmassa silmän ominaisuuksiin perustuvista biometrisistä menetelmistä keskitytään silmän iiriksen tunnistamiseen.

Monet valtiolliset identiteettijärjestelmät hyödyntävät iiriksentunnistusteknologiaa ja laajat tutkimusyhteisöt selvittävät tapoja tehdä menetelmästä vielä tarkempi, laajamittaisemmissakin sovellutuksissa (M. J. Burge & Bowyer, 2013). Esimerkiksi Yhdistyneissä Kuningaskunnissa on mahdollista ylittää valtion raja käyttämällä todistuksena henkilöllisyydestä ainoastaan silmän iiristä (Palmer & Hurrey, 2012). Muissakin kansallisissa henkilökorttijärjestelmissä iiriksen käyttö on osoitettu luotettavaksi keinoksi kansalaisen todentamiseksi (Daugman, 2005). Myös M. J. Burge ja Bowyer (2013) kertovat iiriksentunnistuksen olevan käytöissä useissa kansallisissa identiteettijärjestelmissä. Silmän iiriksen käyttöä PIN-koodin sijaan pankkiautomaatilla identiteetin todentamiseksi on ehdotettu, ja aiheesta on tehty tutkimusta sekä kenttätestejä (Lynne Coventry, Angeli & Johnson, 2003).

Iiriksen tunnistaminen on yksi suosituimmista ja tutkituimmista biometrisen todentamisen teknologioista, mutta ihmisten arjessa se ei vielä näy samalla ta-

valla, kuin esimerkiksi sormenjälkitunnistus, jota ihmiset saattavat käyttää useita kertoja päivässä avatakseen mobiililaitteensa lukituksen. Alan Goode (2014) kertoo iiriksen tunnistuksen olevan yksi parhaista biometrisen käyttäjäntodentamisen menetelmistä, mutta tällä hetkellä hän havaitsee siinä ongelmia liittyen matkapuhelinsovellutuksiin. Hänen mukaansa iiriksen tunnistuksen kehitys matkapuhelin-alalla on hyvin rajoittunutta, koska onnistunut iiriksen skannaus vaatii toimiakseen infrapunateknologiaa. Muita iiriksen tunnistuksen käytettävyyden ja tietoturvan ongelmia käydään tarkemmin läpi luvussa neljä.

# 3 KÄYTETTÄVYYS JA TIETOTURVA BIOMETRIASSA

Biometrian käyttö turvallisuussovellutuksissa on lisääntynyt, mikä on saanut niiden tarjoajat ja tutkijat analysoimaan biometristen algoritmien tehokkuutta ja heikkouksia. Kuitenkin biometrian käyttökelpoisuuteen ja suorituskykyyn liittyvät myös monet muut seikat, kuten käytettävyys ja käyttäjien hyväksyntä, joiden vaikutus voi olla huomattava. (Fernandez-Saavedra, Alonso-Moreno, Uriarte-Antonio & Sanchez-Reillo, 2009.) Perinteisesti käyttäjä on nähty biometriassa vain passiivisena näytteenantaja, eikä interaktiivisena ja integroituna osana biometristä järjestelmää (Theofanos, Micheals & Stanton, 2009). Biometristen teknologioiden suunnittelussa, kehityksessä ja arvioinnissa onkin aiemmin keskitytty laitteiston ja ohjelmiston suorituskykyyn, funktionaalisuuteen, luotettavuuteen ja tarkkuuteen. Tämä johtuu siitä, että teknologioiden ollessa uusia ja vasta kehittymässä, oli välttämätöntä keskittyä pääasiassa näiden osa-alueiden tehtäviin (Theofanos ym., 2009). Tässä luvussa käsitellään biometrian perinteisiä mittareita, biometrian käytettävyyttä ja sen käytettävyyden arviointiin kehitettyjä menetelmiä, sekä biometrian tietoturvaa.

## 3.1 Biometrian mittaamisen perinteiset mittarit

Perinteisesti biometrisiä teknologioita on arvioitu järjestelmävirheiden arvojen mukaan. Niitä ovat esimerkiksi tunnisteen kirjaamisen epäonnistuminen (FTE), kirjautumistilanteessa näytteen hankkimisen epäonnistuminen (FTA), virheellisen hyväksynnän arvo (FAR) sekä virheellisen hylkäyksen arvo (FRR) (Elliott ym., 2015). Virheellisen hyväksynnän arvo kuvastaa siis todennäköisyyttä sille, että väärä henkilö pääsee sisälle järjestelmään ja virheellisen hylkäyksen arvo sille, että oikea henkilö ei pääse sisälle järjestelmään. Tunnisteen kirjaamisen epäonnistumisen arvo kuvastaa niiden käyttäjien määrää, jotka eivät saa lainkaan tarpeeksi laadukasta biometristä tunnistetta syötetyksi järjestelmään. Näytteen hankkimisen epäonnistumisen arvo taas niitä henkilöitä, jotka ovat

syöttäneet järjestelmään hyväksytyn tunnisteen, mutta eivät kykene tuottamaan tarpeeksi laadukasta tunnistetta todentamistilanteessa. (Coventry, 2005.) Näitä biometrian perinteisiä mittareita, mittauskohteita, sekä vaihtoehtoisia mittareita on vertailtu alla olevassa taulukossa (taulukko 1), joka on koottu tätä tutkielmaa varten lähdekirjallisuuden perusteella.

TAULUKKO 1 Biometrian käytettävyyden ja tietoturvan mittarit

| Mittauksen kohde | Perinteinen mittari | Vaihtoehtoinen mittari | Mittaa käytettävyyttä/tietoturvaa |
|---|---|---|---|
| Tunnisteen kirjaamisen epäonnistuminen | Failure To Enroll, (FTE) | False Enrollment Rate (FER) | Käytettävyys |
| Näytteen hankkimisen epäonnistuminen | Failure To Acquire (FTA) | | Käytettävyys |
| Virheellisen hyväksynnän arvo | False Accept Rate (FAR) | Equal Error Rate (EER), False Match rate, (FMR) | Tietoturva |
| Virheellisen hylkäyksen arvo | False Reject Rate (FRR) | Equal Error Rate (EER), False Non-match Rate, (FNMR) | Tietoturva |

Biometrian perinteisistä mittareista tunnisteen kirjaamisen epäonnistumisen ja näytteen hankkimisen epäonnistumisen voidaan siis katsoa kuvastavan enemmän käytettävyyden näkökulmaa. Virheellisen hyväksynnän arvon ja virheellisen hylkäyksen arvon taas voidaan nähdä koskevan enemmän tietoturvaa. Ne ovat kuitenkin kaikki läheisesti toisiinsa kytköksissä ja usein yhtä ominaisuutta parannettaessa joudutaan toisesta tinkimään. Kowtko (2014) huomauttaakin, että esimerkiksi virheellisen hylkäyksen arvo ja virheellisen hyväksynnän arvo ovat suoraan yhteydessä toisiinsa ja kun toista kasvatetaan, toinen laskee, sekä toisin päin. Hän ehdottaakin yhdeksi biometrian mittariksi yhtä suurten virhemäärien arvoa (EER), joka tarkoittaa virheellisen hyväksynnän ja virheellisen hylkäyksien arvojen leikkauspistettä. Hänen mukaansa biometrisiä järjestelmiä arvioidessa on tärkeää löytää matala raja-arvo, jossa virheelliset hylkäykset ja virheelliset hyväksynnät kohtaavat.

Lassmann (2002) käyttää kirjaamisten epäonnistumisesta termiä False Enrollment Rate (FER). Hän mainitsee siihen liittyvänä biometrian dilemmana, että voidaan valita joko laaja huonolaatuisten biometristen näytteiden tietokanta, tai suurempi määrä henkilöitä, jotka eivät voi käyttää biometristä ominaisuutta. Mansfield ja Wayman (2002) pitävät virheellisen hyväksynnän ja virheellisen hylkäyksen arvoja käytännöllisinä mittareina potentiaalista järjestelmän käyttäjää ajatellen. He näkevät niissä kuitenkin hieman monitulkintaisuuden mahdollisuutta, sillä ne vaihtelevat, jos järjestelmä hyväksyy useamman yrityksen tai sisältää useita malleja. Tämän vuoksi he käyttävätkin tunnistusalgoritmien virheiden arvoina virheellisen yhteensopivuuden arvoa ja virheelli-

sen epäyhteensopivuuden arvoa. Virheellisen yhteensopivuuden arvo tarkoittaa heidän mallissaan oletettua todennäköisyyttä sille, että näyte julistetaan virheellisesti samankaltaiseksi yhden satunnaisesti valitun, geneettisesti erilaisen (esimerkiksi toinen silmä tai identtisen kaksosen silmä) mallin kanssa. Virheellisen epäyhteensopivuuden arvo taas tarkoittaa heidän mallissaan oletettua todennäköisyyttä sille, että näyte julistetaan virheellisesti poikkeavaksi saman käyttäjän antaessa kyseisen näytteen. Kyseiset arvot siis lasketaan usean vertailun perusteella. Myöhemmin tutkielmassa käytetään tässä luvussa esitellyistä mittareista niiden englanninkielisiä lyhenteitä, jotka ovat nähtävissä taulukossa 1.

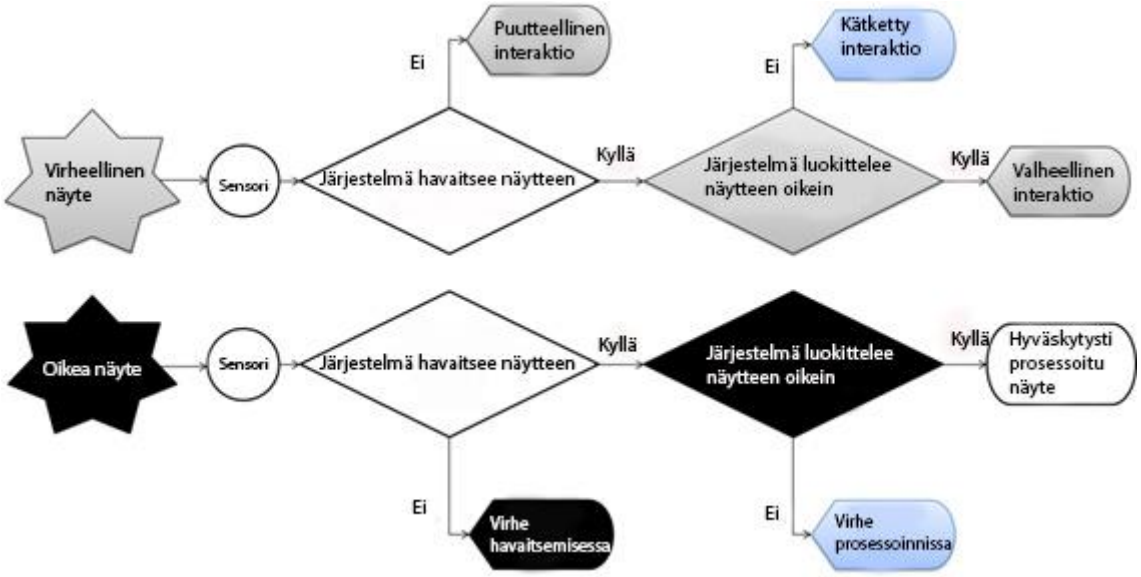
## 3.2 Käytettävyys

Nielsenin (1993) mukaan käytettävyydessä on kyse siitä, kuinka hyvin käyttäjä pystyy toteuttamaan kyseessä olevan tuotteen toiminnon. Nielsen on siis samaa mieltä johdannossa esitellyn kansainvälisen käytettävyyden standardin kanssa. Näkökulmien ero on siinä, että ISO-standardi määrittelee käytettävyyden ominaisuutena, joka toteutuu kun toiminto voidaan suorittaa tehokkaasti ja tyydyttävästi. Nielsenin mukaan käytettävyys taas on muuttuva arvo, eli käytettävyydellä voi olla eri tasoja. Nielsenin näkökulma tukee paremmin tätä tutkielmaa ja sen havaintoja, sillä tutkielmassa tarkastellaan biometrian käytettävyyden muuttuvia mittareita. Tämän tutkielman tapauksessa Nielsenin mainitsema toiminto siis tarkoittaa käyttäjän identiteetin varmistamista. Käyttäjän kokemuksen kannalta identiteetin varmistamisen käytettävyys on tärkeää, sillä jotkin biometriset menetelmät saattavat olla hankalia tai epämukavia käyttää esimerkiksi julkisella paikalla. Myös käyttäjän fyysiset ominaisuudet tai esimerkiksi kirjautumisympäristön sääolosuhteet voivat aiheuttaa käyttäjälle kohtuutonta vaivaa.

Biometriassa havaitaankin väistämättömiä käytettävyyden ongelmia. Esimerkiksi jokaisen biometrisen menetelmän tapauksessa on ihmisiä, jotka eivät kykene käyttämään kyseistä menetelmää, sillä heidän näytteensä on liian huonotasoinen biometrisille sensoreille tai heiltä puuttuu vaadittu biometrinen ominaisuus täysin (Lassmann, 2002). Tämä rikkoo selvästi aiemmin tässä tutkielmassa tarkasteltuja Clarken (1994) hyvän biometrisen piirteen ominaisuusvaatimuksia. Biometristä käyttäjäntodennusta on ehdotettu vaihtoehdoksi myös esimerkiksi ikääntyville ihmisille, jotka eivät kykene enää muistamaan riittävän turvallisuuden takaavia salasanoja yhtä hyvin kuin ennen. Ikääntyvillä käyttäjillä voi kuitenkin olla terveysongelmia, jotka rajoittavat biometrian käytettävyyttä (Kowtko, 2014). Liang, Fleming ja Wang (2014) taas ovat tutkineet kirjautumismenetelmiä matkapuhelimissa ja huomauttavat, että matkapuhelimien tapauksessa kirjautumismenetelmän käytettävyys on tärkeä tekijä, sillä käyttäjät voivat pitää tärkeämpänä ohjelman tai ominaisuuden käytettävyyttä kuin sen turvallisuutta. He pitävät turvallisuutta tärkeänä, mutta toivovat

suunnittelijoiden ottavan myös käytettävyysasiat huomioon, sillä yksi ilman toista ei ole tarpeeksi.

Tämän luvun alussa mainitut neljä yleisintä mittaria, eli FTE, FTA, FAR ja FRR, ovat toimineet hyvin uusien teknologioiden, biometristen modaliteettien ja uusien algoritmien arvioinnissa. Tällainen järjestelmätason arviointi on kuitenkin johtanut käytettävyyden tutkimuksen rajoittumiseen biometristen teknologioiden saralla. (Elliott ym., 2015.) Elliott ja kumppanit esittelevätkin Human-Biometric Sensor Interaction-mallin, eli HBSI-mallin (kuvio 3), jossa esitellään kuusi uutta, fyysiseen ja kognitiiviseen ergonomiaan sekä käytettävyyteen enemmän kantaaottavaa mittaria. Niissä muun muassa eritellään, johtuuko väärä hyväksyntä tai hylkäys kirjautumistilanteessa tai näytteenkirjaamistilanteessa käyttäjästä vai biometrisestä sensorista. Puutteellinen interaktio (Defective interaction, DI), kätketty interaktio (Concealed interaction, CI), ja valheellinen interaktio (False interaction, FI) perustuvat HBSI-mallissa vääränlaisen näytteen esittämiseen. Virhe havaitsemisessa (Failure to detect, FTD) on mittari tilanteille, jossa oikeanlainen näyte on annettu, mutta sensorit eivät havaitse sitä. Virhe prosessoinnissa (Failure to Process, FTP) taas tarkoittaa tilannetta, jossa oikeanlainen näyte on annettu, mutta se ei etene järjestelmään asti huonon laadun tai virheellisen piirteiden erittelyn vuoksi. Viimeiseksi, hyväksytysti prosessoitu näyte (Succesfully Processed Sample, SPS) on näyte, joka on havaittu ilman esiin tulleita virheitä, ja joka hyväksytään järjestelmään.




KUVIO 3 HBSI-mallin näytteen esittämisen viitekehys (Elliot ym., 2015, 3)

HBSI-mallia on hyödynnetty esimerkiksi käden geometriaan (Elliott, Senjaya, Kukula, Werner & Wade, 2010) ja allekirjoitukseen perustuvien biometristen teknologioiden kehittämisessä (Brockly, Guest, Elliott & Scott, 2011). Koska tässä tutkielmassa keskitytään kyseisten teknologioiden sijaan sormenjäljen ja silmän iiriksen tunnistamiseen käyttäjän todentamisessa, HBSI-mallin sovellutuksia ei tarkastella tässä katsauksessa syvemmin. HBSI-malli on kuitenkin tut-

kielman kannalta tärkeä, sillä se on tuore malli, joka pyrkii ottamaan käytettävyyden paremmin huomioon biometrian arvioinnissa. Biometrian käytettävyyden mittaamisesta kiinnostuneille lukijoille suositellaan tutustumista kyseisiin HBSI-mallin sovellutuksia käsitteleviin artikkeleihin.

Omalla tavallaan biometristen teknologioiden käytettävyyttä ovat arvioineet myös Braz & Robert (2006). He arvioivat artikkelissaan biometristen teknologioiden käytettävyyttä suhteellisella arvosanalla yhdestä viiteen. Arvosanat on laadittu heidän tarkastelemansa kirjallisuuden, sekä kuhunkin menetelmään liittyvien käytettävyyden ongelmien vakavuuden mukaan. He ovat ottaneet antamissaan arvosanoissa huomioon muun muassa ongelmat, jotka aiheutuvat menetelmän käyttöä rajoittavista, käyttäjän fyysisistä piirteistä ja menetelmän sosiaalisesta hyväksynnästä, sekä käyttäjien kyvystä rekisteröidä onnistunut näyte järjestelmään.

Biometristen käyttäjäntodennusteknologioiden käytettävyyden parantamiseksi on esitelty useita yleisiä toimintaperiaatteita. Esimerkiksi Takahashi ja Hirata (2011) esittelevät kolme tilannetta, joissa on hyödynnetty käytettävyyttä heikentäviä naiiveja ratkaisuja, tallennettujen biometristen parametrien säilyttämiseksi. Ne ovat parametrien säilyttäminen päätelaitteessa, parametrien säilyttäminen asiakkaan hallussa olevassa laitteessa ja salasanaan perustuvan parametrigeneraattorin käyttäminen. He kertovat, että jos parametreja säilytetään päätelaitteessa, kuten tietokoneella, mobiiliterminaalissa tai sensoreissa, joudutaan karsimaan käyttäjien määrää tallennustilan rajallisuuden vuoksi. Tällöin käytettävyys heikkenee. Jos parametreja säilytetään asiakkaan hallussa olevassa laitteessa, käyttäjää joutuu kantamaan ylimääräistä laitetta mukanaan. Tällöin käytettävyys heikkenee myös, koska laite on helppo unohtaa esimerkiksi töihin tai kotiin. Jos taas käytetään salasanaan perustuvaa parametrigeneraattoria, joutuu käyttäjä muistamaan hankalan, tietoturvatasoltaan korkean salasanan. Kun turvaudutaan ulkoiseen laitteeseen tai salasanaan, joudutaan luopumaan pyrkimyksestä korvata perinteisen käyttäjätodennusmetodit ja helppokäyttöisyydestä, jota biometrian käytöllä tavoitellaan. Takahashi ja Hirata ehdottavatkin käyttävyydeltään parhaan parametrienhallintajärjestelmän olevan sellainen, että tallennetut parametrit säilytetään parametrienhallintaserverillä, joka on erillään serveristä, jolla käyttäjän todentaminen tapahtuu.

## 3.3 Tietoturva

Biometriset teknologiat voivat parantaa tietoturvaa joiltakin osin, mutta niiden käyttö synnyttää myös uusia tietoturvauhkia. Biometriseen sensoriin voi joissakin tapauksissa syöttää valheellisen näytteen, biometrinen näyte ei ole korvattavissa tai salainen, eikä varastettua biometristä ominaisuutta voida vaihtaa. (Faundez-Zanuy, 2006.) Joitakin biometrisiä tuotteita voidaan huijata hyvin pienellä vaivalla, kuten hyödyntämällä keinotekoisen silikonisormen sormenjälkeä, kasvojen valokuvaa tai ääninauhoitetta (Lassmann, 2002). Tällaisia hyökkäyksiä voidaan torjua esimerkiksi valvomalla paikkaa, jossa todentamis-

prosessi tapahtuu, tai kehittämällä teknologioita, joilla näytteenantajan voidaan havaita olevan oikea, elävä ihminen. Biometrialla suojattuja kohteita vastaan tapahtuu kuitenkin muita menetelmiä vähemmän perinteisiä kyberhyökkäyksiä (Kowtko, 2014). Lisäksi biometristen näytteiden korvattavuuden ja salattavuuden ongelmia on pyritty eri tavoin ratkaisemaan.

Tehtäessä parannuksia biometrisen todentamisteknologian käytettävyyteen, saatetaan synnyttää uusia tietoturvariskejä. Esimerkiksi edellisessä alaluvussa esitellyssä Takahashin ja Hiratan (2011) ehdottamassa parametrienhallintajärjestelmässä parametrit ovat helposti vaarassa joutua vääriin käsiin käyttäjän todentavan laitteen kautta. He ehdottavatkin yhtä aikaa käytettävyydeltään korkeatasoisen ja turvallisen biometrisen käyttäjäntodennuksen kehittämisen tueksi useaa kumottavissa olevaan biometriaan perustuvaa protokollaa, joilla luodaan kertakäyttöinen malli biometrisestä ominaisuudesta.

Kumottavissa oleva biometria (cancelable biometrics) tarkoittaa järjestelmiä biometristen näytteiden turvaamiseksi näytetietokannan tietoturvan murtuessa (Jenisch & Uhl, 2011). Käsite pitää sisällään useita algoritmeja, joilla pyritään vaikuttamaan biometrisen todentamisen turvallisuuteen ja yksityisyyteen liittyviin ongelmiin, jotka johtuvat siitä, että ihmisellä on vain yhdet kasvot, kaksi silmää ja kymmenen sormea (Adler, 2009). Ongelma on siis se, että ihmisen biologisten ominaisuuksien vuoksi voidaan yhdestä henkilöstä saada vain rajallinen määrä biometrisiä tunnisteita. Kumottavissa olevan biometrian tarkoituksena on luoda biometrisestä näytteestä useita, peruutettavissa olevia biometrisiä malleja, jotta tunnisteen joutuessa vääriin käsiin, sen voisi vaihtaa samalla tavoin kuin salasanan tai luottokorttinumeron (Ratha, Connell, Bolle & Chikkerur, 2006).

Edellisessä luvussa tarkasteltiin Brazin ja Robertin (2006) käytettävyydelle antamia suhteellisia arvosanoja. Braz ja Robert ovat artikkelissaan arvioineet suhteellisella arvosanalla yhdestä viiteen myös kunkin tarkastelemansa biometrisen menetelmän tietoturvan. Arvosanat perustuvat menetelmiä koskevan kirjallisuuden havaintoihin, ja kunkin menetelmän tietoturvaongelmien vakavuuteen. Arvosteluperusteena on käytetty myös kustakin menetelmästä havaittuja FRR- ja FAR-arvoja.

# 4 SORMENJÄLKITUNNISTUKSEN JA IIRIKSEN-TUNNISTUKSEN KÄYTETTÄVYYDEN JA TIETO-TURVAN ONGELMAT

Edellisessä luvussa käsiteltiin perinteisiä biometrian mittareita, käytettävyyden ja tietoturvan käsitteitä, sekä biometrisen käyttäjäntodennuksen käytettävyyttä ja tietoturvaa. Lisäksi esiteltiin ehdotuksia ja ratkaisuja niiden parantamiseen. Tässä luvussa perehdytään tarkemmin biometrian käytettävyyteen, tietoturvaan ja niiden mittaamiseen sormenjäljen ja silmän iiriksen tunnistamiseen perustuvissa biometrisissä teknologioissa. Vaikka aiemmin mainitut mittarit (FTE-, FTA-, FAR- ja FRR -arvot) ovat saaneet kritiikkiä osakseen, ne ovat yleisesti käytössä tutkitussa lähdeaineistossa koskien tämän tutkielman käsittelemiä biometrisiä teknologioita. Kyseiset mittarit soveltuvat selkeinä numeroarvoina erinomaisiksi vertailukohdiksi tutkielmassa käsiteltyjen biometristen teknologioiden välillä. Lisäksi tässä luvussa tarkastellaan kyseisten todennusmenetelmien käytettävyyden ja tietoturvan ongelmia, sekä keinoja, joilla näitä ongelmia on pyritty korjaamaan ja käsiteltyjä tunnuslukuja parantamaan.

## 4.1 Mittaustuloksia

Braz ja Robert (2006) kertovat todentamismenetelmien vertailussa sormenjäljen, käden ja kasvojen tunnistuksen saaneen käytettävyydestä suhteellisen arvosanan kolme asteikolla yhdestä viiteen. Myös iiriksen ja verkkokalvon tunnistuksen kategorialle on annettu arvosana kolme. Heidän asteikollaan sormenjälkitunnistus ja iiriksentunnistus ovat siis kohtalaisen käytettäviä, mutta niissä on silti paljon kehitettävää. Perinteisten käytettävyyden mittareiden saralla pienimmät sormenjälkitunnistuksen FTE- ja FTA-arvot on kirjallisuudessa tuonut esille Faundez-Zanuy (2006). Hän on havainnut sormenjälkitunnistuksen FTE-arvon olevan n. 1-2 % ja FTA-arvon n. 0.4-2.8 %. Nämä arvot ovat kuitenkin peräisin verrattain suppeasta, 200 koehenkilön testistä. Lynne, Coventry, Angeli ja Johnson (2003) puolestaan uskovat sormenjälkitunnistuksen FTE-arvon olevan

jopa 10 %. Iiriksen skannauksen FTE-arvoksi taas on saatu alimmillaan 0.005 % (Lynne Coventry ym., 2003). Faundez-Zanuyn (2006) esittelemissä testeissä iiriksen skannaukselle on puolestaan ilmoitettu FTE-arvo 0.5 % ja FTA-arvo 0.0 %.

Tietoturvan näkökulmasta Braz ja Robert (2006) ovat tutkimuksessaan antaneet sormenjälkeen perustuvalle biometriselle todentamiselle suhteellisen arvosanan neljä asteikolla yhdestä viiteen. Silmän tunnistamisen menetelmille heidän antamansa arvosanansa on viisi. Brazin ja Robertin arviointimenetelmän mukaan sormenjälkitunnistus ja iiriksentunnistus ovat siis tietoturvaltaan korkealla tasolla, mutta sormenjälkitunnistus vaatii kuitenkin enemmän tietoturvan kehittämistä kuin silmään perustuvat teknologiat. Faundez-Zanuy (2006) on tutkimuksessaan havainnut pienimmän perinteisen tunnusluvun myös sormenjälkitunnistuksen FAR-arvolle. Hän on saanut FAR-arvoksi sadan henkilön kokeella 0.02 % ja kahden sadan henkilön kokeella 0.01 %. Molemmissa testeissä FRR-arvoksi saatiin 2 %. Bhattacharyya, Ranjan, Das, Kim ja Bandyopadhyay (2009) taas ovat selvittäneet 25000 koehenkilön testissä sormenjälkitunnistuksen FAR- ja FRR-arvoksi 2 %. Braz ja Robert (2006) kertovat FRR-arvon olevan välillä 1 - 20 % ja FAR-arvon välillä 0.001 - 5 %. Iiriksentunnistukselle Faundez-Zanuy (2006) on ilmoittanut FRR-arvoiksi yhdellä yrityksellä 2 % ja kolmella yrityksellä 0,25 %. FAR-arvoiksi molemmissa tapauksissa saatiin 0,0001 %. Bhattacharyya ym. (2009) ovat havainneet 1224 henkilön testillä iiriksentunnistuksen FAR-arvon olevan 0.94 % ja FRR-arvon 0.99 %. Braz ja Robert (2006) arvioivat FRR-arvon olevan iiriksen tai verkkokalvon tunnistuksessa välillä 2 – 10 % ja FAR-arvon yhtä suuri tai pienempi kuin 0,001 %. Seuraavaan taulukkoon (taulukko 2) on kerätty tutkielmassa esiintyneet pienimmät mittaustulokset sormenjäljen ja iiriksen tunnistamisen perinteisistä tunnusluvuista.

TAULUKKO 2 Sormenjäljen ja iiriksen tunnistamisen pienimmät tunnusluvut

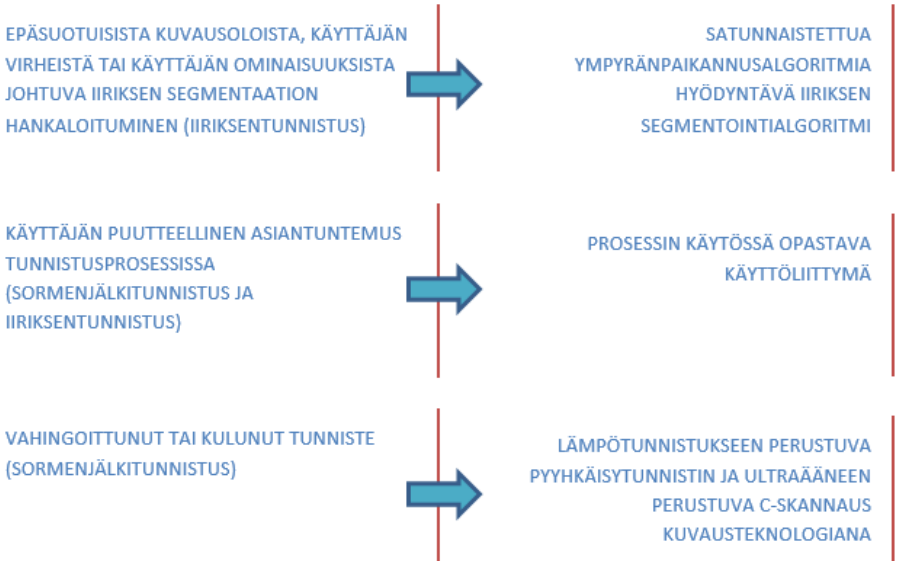
| | FTE | FTA | FAR | FRR |
|---|---|---|---|---|
| Sormenjälki | 1 % | 0.4 % | 0.01 % | 2 % |
| Iiris | 0.005 % | 0 % | 0.0001 % | 0.25 % |

Tässä tutkielmassa tarkasteltujen lähteiden perusteella sormenjälkitunnistuksen FRR-arvo näyttäisi asettuvan lähelle kahta prosenttia, mutta FAR-arvoa tarkastellessa havaitaan suhteellisen suurta eriävyyttä välillä 0.01 % - 2 %. Erot voivat johtua suuresta vaihtelusta koehenkilöiden määrissä tutkimuksesta toiseen, mutta joka tapauksessa tutkimustulokset osoittavat, että sormenjälkitunnistus ei ole tietoturvansakaan puolesta täydellinen, vaan käyttäjä voi jopa kaksi kertaa sadasta todentaa itsensä järjestelmään väärällä identiteetillä. Iiriksentunnistuksen tapauksessa taas huomataan FAR-arvon sijoittuvan alle prosenttiin ja FRR-arvon alle kahteen prosenttiin. Iiriksentunnistuksen FRR-arvo on siis korkeimmillaan samaa luokkaa kuin sormenjälkitunnistuksen, mutta FAR-arvon kannalta se on tietoturvaltaan parempi kuin sormenjälkeen perustuvat teknologiat.

Taulukossa esiteltyjen, pienimpien mitattujen tulosten perusteella, iiriksentunnistus on jokaisessa luokassa sormenjälkitunnistusta korkeatasoisempi. Kirjallisuudesta löytyvien korkeimpien lukujen perusteella on kuitenkin selvää, että molempien menetelmien tietoturvan tunnuslukujen alentamiselle on tarvetta. Ainakin tiettyjen sormenjälkitunnistusmetodien kohdalla on tarvetta myös käytettävyyden arvojen alentamiseksi. Iiriksen tunnistamisen käytettävyyden taas voitaisiin mittareiden perusteella olettaa olevan erinomaista tasoa. Kuitenkin, kuten edellisessä luvussa mainittiin, käytettävyyttä tai tietoturvaa ei voida mitata ainoastaan näiden numeroarvojen perusteella. Sen vuoksi seuraavissa alaluvuissa keskitytään sormenjälkitunnistuksen ja iiriksentunnistuksen käytettävyyden ja tietoturvan käytännön ongelmien tarkasteluun. Myös ehdotuksia käytettävyyden ja tietoturvan parantamiseksi näissä menetelmissä käydään läpi.

## 4.2 Käytettävyys

Koska sormenjälkitunnistusta käytetään usein esimerkiksi viranomaistyössä, sen tietoturvan vaatimukset on asetettu korkealle. Sormenjälkitunnistusta käytetään myös arjessa, kuten matkapuhelinten lukituksessa, jolloin käyttäjä voi joutua todentamaan itsensä lukuisia kertoja päivässä. Tällöin käytettävyyskin nousee erityisen tärkeäksi tekijäksi tietoturvan rinnalle. Myös silmän iirikseen perustuvien biometristen teknologioiden käyttötarkoitukset, kuten automaattinen kontrolli valtioiden rajanylityksissä, vaativat korkean tietoturvan tason. Käytettävyys nousee kuitenkin myös iiriksentunnistuksen kohdalla toiseksi tärkeäksi tekijäksi. Huono käytettävyys rajanylityksessä voi aiheuttaa viivästyksiä, ongelmatilanteita ja heikentää ihmisten halukkuutta käyttää teknologiaa todentamisen vaihtoehtona. Tässä tutkielmassa esiin nousseita biometrian käytettävyyden ongelmia ratkaisu- ja parannusehdotuksineen on havainnollistettu seuraavassa kuviossa (kuvio 4).




KUVIO 4 Biometrian käytettävyyden ongelmia, sekä ratkaisu- ja parannusehdotuksia

Braz ja Robert (2006) huomauttavat, että iiriksenkuvauksen piirissä on henkilöitä, jotka eivät voi kokonaisvaltaisesti tai lainkaan käyttää menetelmää kirjautuakseen palveluun. Esimerkiksi tietyt silmäsairaudet vaikuttavat iiriksentunnistuslaitteiden kykyyn saada silmästä hyväksyttävää kuvaa. Myös sormenjälkitunnistuksen käytettävyys voi heiketä huomattavasti, tai koko teknologia voi muuttua jopa täysin käyttökelvottomaksi, jos käyttäjän sormenjälki on kulunut tai sormenjälkeä ei ole laisinkaan. Faundez-Zanuyn (2006) mukaan tällaisia tapauksia voivat olla muun muassa ikääntyneet henkilöt, jotkut aasialaiset kansat tai esimerkiksi happojen tai sementin parissa työskentelevät ruumiillisen työn tekijät. Hänen mukaansa käytettävyys voi heiketä myös sään tai ympäristön vuoksi, sillä jotkut sormenjälkilukijat eivät kykene poimimaan sormenjälkeä, joka on esimerkiksi liian öljyinen, kuiva, kostea, lämmin ja niin edelleen. Hän huomauttaa, että sormenjäljen osittainen tai täydellinen vaurioituminen voi tehdä todentamisesta mahdotonta.

Iiriksentunnistuksen olennaiset komponentit ovat iiriksen biometrisen näytteen hankinta, iiriksen segmentaatio, iiriksen piirteiden erottelu, iiriksen mallin luominen, iiriksen mallin yhteensovitus ja lopuksi iiriksen tunnistaminen. Iiriksen segmentointi tarkoittaa pupillien rajojen ja limbisten rajojen havaitsemista, sekä silmäluomien ja kulmakarvojen rajaamista pois mallista. (Leo ym., 2014.) Iiriksen tunnistuksen olennaisista komponenteista erityisesti segmentaatio voi aiheuttaa käytettävyyden ongelmia. Proenca ja Alexandre (2011) kertovat perinteisten iiriksen segmentointialgoritmien tarkkuuden vähenevän huomattavasti, jos näkyvällä aaltopituudella otetussa iiriksen kuvassa on kohinaa ja se on otettu epäsuotuisissa kuvausoloissa. Heidän mukaansa segmentaatio voi tällöin hankaloitua esimerkiksi silmän anatomisten ominaisuuksien, kuten silmäripsien tai kulmakarvojen okkluusioiden vuoksi. Myös valaistus, käyttäjän toimet, kuten väärään kulmaan asettuminen, sekä esimerkiksi käyttäjän päässä olevat silmälasit tai piilolinssit voivat hankaloittaa segmentaatiota.

Leo ym. (2014) esittelevätkin iiriksen segmentointialgoritmin, jolla pyritään ohittamaan näitä käytettävyyttä heikentäviä seikkoja satunnaistetun ympyränpaikannusalgoritmin avulla. Se käyttää usean todistusaineiston strategiaa määritelläkseen oikeaoppiset ympyrät. Lisäksi algoritmia hyödynnetään löytämään limbisiä rajoja, sekä pupillin ja silmäluomen rajoja myös luonnollisissa ympäristöissä ja heikoissa valaistusoloissa. Se ei myöskään vaadi interaktiota erilaisiin operointiolosuhteisiin sopeutumiseksi. Heiden esittelemänsä algoritmi kasvatti iiriksen segmentaation käytettävyyttä vaikuttamatta negatiivisesti segmentaation tarkkuuteen. Sen kyky erotella iirikseen sisemmät ja ulommat rajat oli tehokkaampi kuin aiemmassa kirjallisuudessa pääasiassa esiintyvän lähestymistavan.

Lisäksi iiriksentunnistuksen käytettävyyttä on pyritty parantamaan uudenlaisen käyttöliittymän avulla. He, Sun, Tan ja Qiu (2008) näkevät iiriksen tunnistuksen käytettävyyden ongelmana selkeän tunnisteen kuvaamisen vaikeuden. Osasyynä sille he näkevät epäkäyttäjäystävällisen käyttöliittymän ja toisaalta sen, että kuvista saattaa tulla epätarkkoja. He tarkastelevatkin mahdollisuutta iiriksentunnistuksen käytettävyyden parantamiseen iiriksen kuvien spekulaaristen pisteiden tarkkailun avulla. Heidän menetelmässään spekulaaristen pisteiden avulla arvioidaan käyttäjän ja kameran välinen etäisyys. Etäisyyden parantamiseksi luodaan käyttäjäystävällinen käyttöliittymä, joka avustaa käyttäjää löytämään sopivan käyttöetäisyyden. Lisäksi etäisyyden arvioinnin ansiosta voidaan palauttaa epäselvästä iiriksen kuvasta tarkempi versio. Heidän tuloksensa osoittavat, että tällä tavoin kyetään parantamaan käytettävyyttä ilman huomattavia laskennallisia kuluja. Heidän menetelmänsä ei myöskään vaadi ylimääräistä laitteistoa eikä kasvata tunnistamiseen kuluvaa aikaa, kuten heidän käsittelemässään aiemmassa kirjallisuudessa esiin tuodut vaihtoehdot. Heidän kokeessaan käytettiin 190 iiriksen kuvaa, 19 eri asennosta kuvattuna ja 19 eri henkilöltä. Yrityksissä ottaa kuva käyttäjän iiriksestä havaittiin virhe noin viidessä prosentissa tapauksia. Palautustoimien ansiosta tunnistamisen tehokkuus lisääntyi epätarkan kuvan tapauksissa ja palautus vei tietokoneelta aikaa vain viisi millisekuntia.

Myös sormenjälkitunnistuksen käytettävyyttä on pyritty parantamaan käyttöjärjestelmän muutoksilla. Esimerkiksi Conti ym (2009) ehdottavat FTE-arvon alentamiseksi käyttöliittymää, jolla kyetään käyttämään kaikkia sormenjälkitunnistusjärjestelmän funktioita luonnollisen kielen avulla, vaatimatta käyttäjältä asiantuntemusta kyseisenlaisten järjestelmien käytöstä. Sormenjälkitunnisteen kirjaamisen epäonnistumiset vähenevät, sillä käyttöliittymä toimii järjestelmässä kuin asiantunteva avustaja, opastaen oikean tavan syöttää tunniste järjestelmään.

Coventry ym. (2003) taas ovat pyrkineet parantamaan sormenjälkitunnistuksen käytettävyyttä kehittämällä ohjelmiston sijaan todennuksessa käytettävää laitteistoa. He tekivät käyttäjätutkimuksen sormenjäljentunnistusteknologialla, jossa käyttäjä pyyhkäisee sormensa lämpötunnistimen päältä todistaakseen identiteettinsä pankkiautomaatilla. Tämän teknologian ansiosta prosessista ei jää sensorin pintaan sormenjälkeä ja se poistaa osan ikääntyneen tai vahingoit-

tuneen ihon tunnistamiseen liittyvistä ongelmista. Kokeen FTE-arvoksi saatiin 8.5 %, kun koehenkilöt jaettiin kolmeen ryhmään sen mukaan, paljonko ohjeita heille annettiin. Epäonnistumisten havaittiin johtuvan henkilökohtaisista syistä, joita ei voitu edesauttaa ohjeistuksella, harjoittelulla tai palautteella.

Maeva ja Severin (2009) puolestaan ovat pyrkineet sormenjälkitunnistuksen käytettävyyden parantamiseen kehittämällä sormenjäljen kuvaamisen teknologiaa. He esittelevät uudenlaisen, ultraääneen perustuvan sormenjäljen kuvaustekniikan, niin sanotun C-skannauksen, jolla luodaan horisontaalinen kuva sormenpään hikirauhasista halutulta syvyydeltä. Tämän kuvan perusteella voidaan rakentaa uudelleen perinteiset ultraääniskannauksen niin sanotut A- ja B-kuvat sormenpäästä. Tekniikan ansiosta tunnistettavasti tarvitsee ottaa vain yksi ultraäänikuva, jonka pitäisi olla jokaisella ihmisellä yksilöllinen. Myöskään minkäänlaisen sormen pintaan kohdistuvan tahallisen tai tahattoman kuuluman ei pitäisi hankaloittaa C-skannauskuvan perusteella tunnistamista.

## 4.3 Tietoturva

On arvioitu, että todennäköisyys löytää kaksi henkilöä, joilla on sama sormenjälki, on yksi miljardissa (Faundez-Zanuy, 2006). Myös käyttäjät luottavat sormenjäljen tunnistuksen turvallisuuteen, sillä esimerkiksi Coventryn ym. (2003) pankkiautomaatilla tapahtuvan sormenjälkitodennuksen kokeessa koehenkilöille laaditussa kyselyssä sormenjälkitodennus nähtiin PIN-koodiin perustuvaa todentamista turvallisempana. Yhdistyneiden Arabiemiraattien sisäministeriön iiriksentunnistusta käsittelevässä kokeessa taas 200 miljardin silmäparin iiristen ristitestauksessa virheellisiä tunnistuksia havaittiin alle yksi kahdesta sadasta miljardista (Daugman, 2005). Erään arvion mukaan taas todennäköisyys, että kaksi eri satunnaista iiristä olisivat identtiset, on noin $10^{35}$ (Hallinan, 1991). Iiriksentunnistuksessa kyetään tehokkaasti erottamaan eri henkilöt ja jopa saman henkilön oikea ja vasen silmä toisistaan (Faundez-Zanuy, 2006). Sormenjälki ja silmän iiris ovat molemmat siis lähes uniikkeja tunnisteita. Näihin tunnisteisiin perustuvien teknologioiden tietoturvassa on kuitenkin havaittu muista syistä johtuvia ongelmia. Tässä tutkielmassa esiin nousseita biometrian tietoturvan ongelmia ratkaisu- ja parannusehdotuksineen on havainnollistettu seuraavassa kuviossa (kuvio 5).


KUVIO 5 Biometrian tietoturvan ongelmia, sekä ratkaisu- ja parannusehdotuksia

Connell, Ratha, Gentile ja Bolle (2013) näkevät iiriksentunnistuksen kaltaisten kontaktittomien biometrisen todentamisen menetelmien olevan uhattuna eri tyyppisille hyökkäyksille kuin ilman kontaktia toimivat. Yhtenä tällaisena uhkana he näkevät yksilöidyt piilolinssit, joilla voidaan huijata iirikseen perustuvia tunnistusmenetelmiä. He esittelevätkin uudenlaisen, rakennettuun valoon perustuvan menetelmän, joka tunnistaa oikean iiriksen peittävän keinotekoisen esineen.

Kunnil, Pillai ja Milshtein (2011) pitävät salasana-tyyppistä todentamismenetelmää haavoittuvaisena, sillä salasanan ja PIN-koodin voi hävittää tai se voi tulla varastetuksi, ja lisäksi hyvät salasanat ovat tavallisille yksilöille liian hankalia muistaa. He ovat päätyneet kontaktittomasti kuvattavaan sormenjälkitunnisteeseen perustuvaan todentamiseen ehdotuksessaan salasanatodentamista turvallisemmasta menetelmästä. Tutkielman edellisessä luvussa kerrottiin kumottavissa olevan biometrian olevan yksi merkittävimmistä biometrian tietoturvan parantamiseen käytetyistä järjestelmistä. Kunnil ym. (2011) ehdottavatkin esittelemänsä kontaktittoman sormenjälkitunnistuksen tietoturvaratkaisuksi kumottavissa olevan biometrian algoritmia, jossa sormenjäljen datasta luodaan pitkä pseudosatunnainen salasana yhtä sessiota varten. Lisäturvana heidän menetelmänsä tarkastelee myös sormen verisuonten kuvioita varmistuakseen sormenjälkinäytteen tulevan oikealta, elävältä ihmiseltä. Jotkut kuluttajat suhtautuvat pelokkaasti biometrisiin todentamismenetelmiin ja uskovat rikollisten voivan varastaa esimerkiksi heidän sormensa (L Coventry ym., 2003). Verisuonten kuviot varmistavana menetelmänä voi olla tehokas keino torjumaan tätä pelkoa.

Myös iiriksen tunnistamiseen perustuviin biometrisiin käyttäjäntodentamisteknologioihin on kehitetty kumottavissa olevan biometrian tietoturvaratkaisuja. Esimerkiksi Jenisch ja Uhl (2011) esittelevät kumottavan tunnisteen iiriksentunnistusjärjestelmän, joka perustuu Man, Tanin, Wangin ja Zhangin (2004) piirteidenerottelualgoritmiin, sekä biometrisen datan permutaatioon ja uudelleenkartoitusalgoritmiin. Heidän esittelemänsä menetelmä koostuu piirteiden erottelusta, näytteen rakenteen kuutioinnista ja permutaatiosta sekä kuutioiden uudelleenjärjestelystä.

# 5 YHTEENVETO JA POHDINTA

Tämän tutkielman tarkoitus oli perehtyä biometriseen käyttäjäntodentamiseen käyttäen esimerkkeinä sormenjälkeen ja silmän iirikseen perustuvia teknologioita. Tutkielmassa tarkasteltiin biometrian yleisiä, sekä määritellyille kahdelle teknologialle tyypillisiä käytettävyyden ja tietoturvan ongelmia, ja niiden ratkaisuehdotuksia. Ongelmia tarkastelemalla pyrittiin nostamaan esille kehityssuuntia tulevaa biometrisen teknologian kehittämistä ja siihen liittyvää tutkimusta varten. Tutkimuskysymyksissä haluttiin selvittää, mitkä ovat biometrian, sormenjälkitunnistuksen ja silmän iiriksen tunnistuksen käytettävyyden ja tietoturvan suurimman heikkoudet. Lisäksi haluttiin selvittää, miten menetelmien käytettävyyttä ja tietoturvaa on pyritty parantamaan.

Sormenjälkitunnistuksen ja iiriksentunnistuksen tunnuslukujen tarkastelun perusteella voitiin päätellä iiriksentunnistuksen olevan käytettävyydeltään ja tietoturvaltaan paremmalla tasolla kuin sormenjälkitunnistuksen. Vaikka tunnusluvut olivat iiriksentunnistuksen kohdalla parempia, huomattiin sormenjälkitunnistuksen olevan laajemmin käytössä. Sormenjälkitunnistuksen suosion syiksi selvisi ainakin sen pitkä historia erityisesti viranomaistyössä. Iiriksentunnistuksen huomattiin myös olevan erityisesti laitteistovaatimuksiensa puolesta hankala ottaa käyttöön esimeriksi mobiilisovellutuksissa. Toisaalta kaikkien tunnuslukujen vertailuissa havaittiin suuriakin eroavaisuuksia tutkimuksesta ja kokeesta toiseen. Tulosten eroavaisuudet ovat voineet johtua esimerkiksi kokeiden suoritustavoissa, koehenkilöiden määristä ja kummankin todennusteknologian kategorian sisällä sovelletusta metodista. Lisäksi tässä tutkielmassa todettiin, etteivät biometrian perinteiset tunnusluvut anna kokonaisvaltaista kuvaa menetelmien käytettävyyden ja tietoturvan tilasta. Siksi tutkielmassa perehdyttiin myös menetelmien käytännön ongelmiin ja ratkaisuehdotuksiin käytettävyyden ja tietoturvan näkökulmasta.

Yhdeksi merkittäväksi biometrian käytettävyyden ongelmaksi havaittiin kirjallisuuden perusteella lähes poikkeuksetta haasteellisuus tai jopa kykenemättömyys teknologioiden käyttöön tiettyjen käyttäjäryhmien kohdalla. Biometrisen tunnisteen puuttuminen synnynnäisten syiden tai tapaturman seurauksena on mahdollista kaikkien biometristen todentamismenetelmien koh-

dalla. Sormenjäljen tapauksessa nousi esille sen mahdollisuus kulua esimerkiksi ikääntymisen tai ruumiillisen työn seurauksena. Myös joidenkin etnisten ryhmien kyvyn onnistuneen sormenjälkitunnisteen antamiseen havaittiin olevan rajoittunut. Silmän iiriksen tapauksessa taas nousivat esille ikääntymisen lisäksi erilaiset silmäsairaudet ja silmäripsien tai kulmakarvojen okkluusiot, jotka voivat heikentää iiriksen tunnistamisen todennäköisyyttä. Sormenjäljen tunnistuksen havaittiin hankaloituvan sormenjäljen ollessa esimerkiksi liian öljyinen, kuiva, kostea tai lämmin. Iiriksentunnistuksen kohdalla taas ympäristöolosuhteiden negatiivisia vaikutuksia nousi esille vähemmän ja ne rajoittuivat tutkitussa kirjallisuudessa lähinnä heikon valaistuksen vaikutukseen. Iiriksentunnistuksen piirissä käytettävyyden ongelmien havaittiin johtuvan enemmän käyttäjän toimista, kuten väärästä asennosta ja silmälasien tai piilolinssien käytöstä.

Ehdotuksissa käytettävyyden parantamiseksi oli sormenjälkitunnistuksen ja iiriksentunnistuksen välillä yhtäläistä pyrkimys vaikuttaa käytettävyyteen kehittämällä tunnistusjärjestelmän käyttöliittymää. Molemmissa ehdotuksissa käyttöliittymän parantamiseksi pyrittiin lisäämään käyttöliittymän kykyä avustaa käyttäjää toimimaan oikein tunnistusprosessissa. Lisäksi sormenjälkitunnistuksen tapauksessa käyttöliittymää ehdotettiin käytettäväksi luonnollisen kielen avulla, jotta asiantuntemuksen tarve vähenisi. Sormenjälkitunnistuksen käytettävyyden kehityksen ehdotukset sisälsivät myös parannuksia tunnistuslaitteistoon, sekä kuvausteknologiaan. Iiriksentunnistukseen keskittyvä ehdotus taas pyrki kohentamaan käytettävyyttä uudenlaisella iiriksen segmentointi- ja ympyränpaikannusalgoritmilla. Molempien tutkielmassa käsiteltyjen biometristen teknologioiden käytettävyyttä voidaan siis kehittää keskittymällä teknologian luonteenomaisiin piirteisiin. On kuitenkin olemassa ominaisuuksia, kuten käyttöliittymä, joihin kehitetyt käytettävyyden parannukset ovat sovellettavissa muihinkin biometrisiin teknologioihin. Käytettävyyden jatkotutkimuksessa tulisi jatkossakin sekä ratkaista teknologioiden ominaisia käytettävyyden ongelmia, että kehittää edelleen biometrian yleiseen käytettävyyteen vaikuttavia ominaisuuksia.

Tutkielman lähdekirjallisuudessa todettiin, että biometrialla suojattuja kohteita vastaan tapahtuu perinteisiä kohteita vähemmän hyökkäyksiä. Lisäksi havaittiin olevan epätodennäköistä löytää kaksi samanlaista sormenjälkeä tai silmän iiristä. Biometrian tietoturvariskien huomattiinkin piilevän aivan uusissa, biometrialle uniikeissa uhkissa. Biometrian tietoturvan ongelmiksi havaittiin esimerkiksi valheellisen syötön mahdollisuus ja joidenkin järjestelmien heikko suojaus erilaisia huijausyrityksiä vastaan. Jotkut järjestelmät saattavat esimerkiksi hyväksyä silikonisormen sormenjäljen tunnisteena tai tunnistaa silmän iiriksen sijaan piilolinssin kuvion. Näitä ongelmia oli pyritty ratkaisemaan esimerkiksi todentamalla näytteenantaja eläväksi verisuonien kuvioiden tunnistuksen avulla. Iiriksentunnistuksessa taas hyödynnettiin menetelmää, joka tunnistaa iiriksen olevan keinotekoisesti peitetty. Biometrian yleisimmäksi ja kaikkien biometristen teknologioiden välillä universaaliksi tietoturvan ongelmaksi havaittiin kuitenkin se, että ihmisellä on rajattu määrä biometrisia tunnisteita, eivätkä ne ole korvattavissa. Tämän ongelman ratkaisemiseksi oli kuitenkin

esitetty useita erilaisia, kumottavissa olevaan biometriaan perustuvia kehitysehdotuksia ja algoritmeja, joissa biometrisestä tunnisteesta luodaan useita kumottavissa olevia malleja. Myös biometrian tietoturvaa on siis kehitetty sekä torjumalla tietylle teknologialle ominaisia uhkia, että keskittymällä koko biometrialle yhteiseen tietoturvariskiin. Tulevaisuudessa on tärkeää jatkaa yksittäisissä teknologioissa havaittujen heikkouksien paikkaamista, mutta tärkeintä on kuitenkin keskittyä kumottavissa olevan biometrian tutkimukseen ja kehitykseen. Jos biometria yleistyy ilman toimivia kumottavissa olevan biometrian ratkaisuja, voi henkilö menettää kaikki biometriset tunnisteensa väärien tahojen tietoon. Tällainen tapaus vaarantaisi käyttäjän jokaisen biometrisellä tunnisteella suojatun laitteen ja palvelun.

Tutkielmassa havaittiin siis, että osittain jopa virheettömistä tunnuslukujen arvoista huolimatta käytettävyyden ja tietoturvan ongelmia esiintyy laajasti biometrisessä todentamisessa ja esimerkkeinä tarkastelluissa teknologioissa. Useimpiin havaittuihin ongelmiin on kehitetty ratkaisuja, mutta ne parantavat usein vain yhtä ongelmaa, eivätkä aina ratkaise sitä kokonaan. Ratkaisut ongelmiin saattavat myös tuoda mukanaan uusia ongelmia. Esimerkiksi käytettävyyden parantuessa tietoturva voi heikentyä, ja toisinpäin. Tutkielman avulla saa hyvän yleiskuvan biometrisen todentamisen käytettävyyden ja tietoturvan tilasta, sekä niiden parantamisen kehityssuunnista. Tutkielman avulla voi saada suuntaviivoja biometrisen teknologian valitsemisen avuksi, sekä teknologian käytettävyyttä ja tietoturvaa parantaviin toimenpiteisiin. Jatkotutkimuksessa olisi hyödyllistä keskittyä löytämään kokonaisratkaisuja, joilla biometristen menetelmien käytettävyys ja tietoturva saataisiin asetettua optimaaliseen tasapainoon. Lisäksi olisi tärkeää keskittyä kehittämään HBSI-mallin kaltaisia uusia järjestelmiä biometrian mittaamiseen ja pyrkiä uudenlaisiin biometrian mittauksen standardeihin, joissa tietoturvaa ja käytettävyyttä, sekä niiden suhdetta voitaisiin tehokkaammin arvioida.

# LÄHTEET


Adamsson, A., Hakkala, A., & Hyrynsalmi, S. (2015). Biometristen järjestelmien yksityisyys – haasteet ja mahdollisuudet.

Adler, A., & Cappelli, R. (2009). Encyclopedia of Biometrics Springer Science+ Business Media, LLC 2009.

Ailisto, H., Ahonen, P., & Lindholm, M. (2005). *Biometrisen tunnistamisen tietoturvallisuus ja yksityisyyden suoja*.

AshokaRajan, R., Angelinjosphia, R., Gayathri, P., Rajendran, T., & Anandhakumar, P. (2013). A novel approach for secure ATM transactions using fingerprint watermarking. Teoksessa *Advanced Computing (ICoAC), 2013 Fifth International Conference on* (s. 547-552). IEEE.

Amin, M. A., & Yan, H. (2009). Phase congruency based retinal vessel segmentation. Teoksessa *Machine Learning and Cybernetics, 2009 International Conference on* (s. 2458-2462). IEEE.

Abo-Zahhad, M., Ahmed, S. M., & Abbas, S. N. (2014). A new biometric modality for human authentication using eye blinking. Teoksessa *Biomedical Engineering Conference (CIBEC), 2014 Cairo International* (s. 174-177). IEEE.

Bhattacharyya, D., Ranjan, R., Das, P., Kim, T. H., & Bandyopadhyay, S. K. (2009). Biometric authentication techniques and its future possibilities. Teoksessa *Computer and Electrical Engineering, 2009. ICCEE'09. Second International Conference on* (s. 652-655). IEEE.

Braz, C., & Robert, J. M. (2006). Security and usability: the case of the user authentication methods. Teoksessa *Proceedings of the 18th International Conferenceof the Association Francophone d'Interaction Homme-Machine* (s. 199-203). ACM.

Brockly, M., Guest, R., Elliott, S., & Scott, J. (2011). Dynamic signature verification and the human biometric sensor interaction model. Teoksessa *Security Technology (ICCST), 2011 IEEE International Carnahan Conference on* (s. 1-6). IEEE.

Burge, M. J., & Bowyer, K. (2013). *Handbook of iris recognition*. Springer Science & Business Media.

Bundesamt für Sicherheit in der Informationstechnik. (2004). Study : " Evaluation of Fingerprint Recognition Technologies – BioFinger ", 1–122.

Clarke, R. (1994). Human identification in information systems: Management challenges and public policy issues. *Information Technology & People*, *7*(4), 6-37.

Connell, J., Ratha, N., Gentile, J., & Bolle, R. (2013). Fake iris detection using structured light. Teoksessa *Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on* (s. 8692-8696). IEEE.

Coventry, L., De Angeli, A., & Johnson, G. (2003). Usability and biometric verification at the ATM interface. Teoksessa *Proceedings of the SIGCHI conference on Human factors in computing systems* (s. 153-160). ACM.

Coventry, L., De Angeli, A., & Johnson, G. (2003). Biometric verification at a self service interface. *Contemporary ergonomics*, 247-252.

Daugman, J. (2005). Results from 200 billion iris cross-comparisons. *University of Cambridge Technical Report UCAM-CL-TR-635*.

Daugman, J. (2004). How iris recognition works. *Circuits and Systems for Video Technology, IEEE Transactions on*, *14*(1), 21-30.

El-Abed, M., Giot, R., Hemery, B., & Rosenberger, C. (2010). A study of users' acceptance and satisfaction of biometric systems. Teoksessa *Security Technology (ICCST), 2010 IEEE International Carnahan Conference on* (s. 170-178). IEEE.

Elliott, S. J., O'Connor, K., Bartlow, E., Robertson, J. J., & Guest, R. M. (2015,). Expanding the human-biometric sensor interaction model to identity claim scenarios. Teoksessa *Identity, Security and Behavior Analysis (ISBA), 2015 IEEE International Conference on* (s. 1-6). IEEE.

Elliott, S. J., Senjaya, B., Kukula, E. P., Werner, J. M., & Wade, M. (2010). An evaluation of the Human Biometric Sensor Interaction using hand geometry. Teoksessa *Security Technology (ICCST), 2010 IEEE International Carnahan Conference on* (s. 259-265). IEEE.

Faundez-Zanuy, M. (2006). Biometric security technology. *Aerospace and Electronic Systems Magazine, IEEE*, *21*(6), 15-26.

Fernandez-Saavedra, B., Alonso-Moreno, R., Uriarte-Antonio, J., & Sanchez-Reillo, R. (2010). Evaluation methodology for analyzing usability factors in biometrics. *Aerospace and Electronic Systems Magazine, IEEE*, *25*(8), 20-31.

Goode, A. (2014). Bring your own finger–how mobile is bringing biometrics to consumers. *Biometric Technology Today*, *2014*(5), 5-9.

Gorman, L. O. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, *91*(12), 2021-2040.

He, Z., Sun, Z., Tan, T., & Qiu, X. (2008). Enhanced usability of iris recognition via efficient user interface and iris image restoration. Teoksessa *Image Processing, 2008. ICIP 2008. 15th IEEE International Conference on* (s. 261-264). IEEE.

Jain, A. K. (2007). Biometric recognition: overview and recent advances. Teoksessa *Progress in Pattern Recognition, Image Analysis and Applications* (s. 13-19). Springer Berlin Heidelberg.

Jenisch, S., & Uhl, A. (2011). Security analysis of a cancelable iris recognition system based on block remapping. Teoksessa *Image Processing (ICIP), 2011 18th IEEE International Conference on* (s. 3213-3216). IEEE.

Kathuria, M. (2010). Design of a Vein Based Personal Identification System. Teoksessa *Advances in Recent Technologies in Communication and Computing (ARTCom), 2010 International Conference on* (s. 284-286). IEEE.

Koundinya, P., Theril, S., Feng, T., Prakash, V., Bao, J., & Shi, W. (2014). Multi resolution touch panel with built-in fingerprint sensing support. Teoksessa *Design, Automation and Test in Europe Conference and Exhibition (DATE), 2014* (s. 1-6). IEEE.

Kowtko, M. A. (2014). Biometric authentication for older adults. Teoksessa *Sys-*

*tems, Applications and Technology Conference (LISAT), 2014 IEEE Long Island* (s. 1-6). IEEE.

Kunnil, V. O., Pillai, A., & Milshtein, S. (2011). Biometrics assisted secure network transactions. Teoksessa *Technologies for Homeland Security (HST), 2011 IEEE International Conference on* (s. 69-74). IEEE.

Lassmann, G. (2002). Some results on robustness, security and usability of biometric systems. Teoksessa *Multimedia and Expo, 2002. ICME'02. Proceedings. 2002 IEEE International Conference on* (s. 577-579). IEEE.

Leo, M., De Marco, T., & Distante, C. (2014). Highly usable and accurate iris segmentation. Teoksessa *2014 22nd International Conference on Pattern Recognition (ICPR)* (s. 2489-2494). IEEE.

Liang, H. N., Fleming, C., & Wang, W. (2014). User Authentication Interfaces in Mobile Devices: Some Design Considerations. Teoksessa *Computational Science and Engineering (CSE), 2014 IEEE 17th International Conference on* (s. 754-757). IEEE.

Ma, L., Tan, T., Wang, Y., & Zhang, D. (2004). Efficient iris recognition by characterizing key local variations. *Image Processing, IEEE Transactions on*, *13*(6), 739-750.

Maev, R. G., Bakulin, E. Y., Maeva, E. Y., & Severin, F. M. (2008). High resolution ultrasonic method for 3D fingerprint representation in biometrics. Teoksessa *Acoustical Imaging* (s. 279-285). Springer Netherlands.

Mansfield, A. J., & Wayman, J. L. (2002). *Best practices in testing and reporting performance of biometric devices* (s. 1-36). Teddington, Middlesex, UK: Centre for Mathematics and Scientific Computing, National Physical Laboratory.

Maple, C., & Norrington, P. (2006). The usability and practicality of biometric authentication in the workplace. Teoksessa *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on* (s. 958-964). IEEE.

Meenakshi, V. S., & Padmavathi, G. (2009). Security analysis of hardened retina based fuzzy vault. Teoksessa *Advances in Recent Technologies in Communication and Computing, 2009. ARTCom'09. International Conference on* (s. 926-930). IEEE.

Narcizo, F. B., Rangel de Queiroz, J. E., & Gomes, H. M. (2013). Remote Eye Tracking Systems: Technologies and Applications. Teoksessa *Graphics, Patterns and Images Tutorials (SIBGRAPI-T), 2013 26th Conference on* (s. 15-22). IEEE.

Palmer, A. J., & Hurrey, C. (2012). Ten reasons why IRIS needed 20: 20 foresight: Some lessons for introducing biometric border control systems. Teoksessa *Intelligence and Security Informatics Conference (EISIC), 2012 European* (s. 311-316). IEEE.

Ratha, N., Connell, J., Bolle, R. M., & Chikkerur, S. (2006). Cancelable biometrics: A case study in fingerprints. Teoksessa *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on* (s. 370-373). IEEE.

Rodrigues, P., & Santos, H. (2013). Health users' perception of biometric authentication technologies. Teoksessa *Computer-Based Medical Systems (CBMS), 2013 IEEE 26th International Symposium on* (s. 320-325). IEEE.

Takahashi, K., & Hirata, S. (2011). Parameter management schemes for cance-

lable biometrics. Teoksessa *Computational Intelligence in Biometrics and Identity Management (CIBIM), 2011 IEEE Workshop on* (s. 145-151). IEEE.

Theofanos, M. F., Micheals, R. J., & Stanton, B. C. (2009). Biometrics systems include users. *Systems Journal, IEEE*, *3*(4), 461-468.