Elollisuuden tunnistus sormenjälki- ja kasvojentunnistuksessa

Turun yliopisto
Tietotekniikan laitos
TkK-tutkielma
Tietotekniikka
Helmikuu 2024
Topi Haatainen

TURUN YLIOPISTO
Tietotekniikan laitos

Topi Haatainen: Elollisuuden tunnistus sormenjälki- ja kasvojentunnistuksessa

TkK-tutkielma, 25 s.
Tietotekniikka
Helmikuu 2024

Tässä tutkielmassa tutustutaan biometrisistä tunnistautumismuodoista kahteen yleisimpään eli sormenjälki- ja kasvojentunnistukseen. Tutkielmassa perehdytään näiden tunnistautumistapojen toimintaan, haavoittuvuuksiin ja siihen, kuinka näitä haavoittuvuuksia on yritetty ratkaista. Elollisuudentunnistuksessa käytettävien algoritmien suorituskyvyn vertailua varten on kehitetty matemaattiset yhtälöt. Näistä yhtälöistä tärkeimmät ovat virheellinen hyväksyntä ja virheellinen hylkäys. Tutkielman keskiössä on elottomien kopioiden hyödyntäminen hyökkäyksissä sekä se, kuinka näitä elottomia kopioita hyödyntäviä hyökkäyksiä pyritään torjumaan.
Sekä sormenjälkitunnistus että kasvojentunnistus on mahdollista murtaa elottomilla kopioilla. Elottomia kopioita, joilla sormenjälkitunnistimen pystyy murtamaan, on muun muassa muovailuvahasta tai paperista tehdyt kopiot. Kasvojentunnistuksen murtamisessa on useampi vaihtoehto, jotka riippuvat tunnistuksessa käytettävästä sensorista ja algoritmista. 2D- ja 3D-teknologian erot tuottavat suurimman merkityksen kasvojentunnistusalgoritmiin. Yleisimpiä elottomia kopioita, joilla kasvojentunnistus voidaan murtaa, ovat valokuvat, videot ja maskit.
Näiden haavoittuvuuksien torjumiseen on kehitetty useita eri metodeja, joihin kuuluvat erilaiset ohjelmistopohjaiset ratkaisut sekä laitteistopohjaiset ratkaisut. Konvoluutioneuroverkot ovat suuressa keskiössä uusia keinoja pohdittaessa.

Asiasanat: biometrinen, tunnistautuminen, sormenjälki, kasvot, elollisuus, tunnistus

Sisällys

1 Johdanto **1**

1.1 Menetelmät ja tiedonhaku 2

1.2 Rakenne 2

2 Biometrinen tunnistautuminen **4**

2.1 Suorituskyvyn vertailu 5

2.2 Biometrisen tunnisteen murtaminen 6

3 Sormenjälkitunnistus **8**

3.1 Näytteenotto ja todentaminen 9

3.2 Haavoittuvuudet 10

3.3 Haavoittuvuuksien torjunta 11

4 Kasvojentunnistus **14**

4.1 Näytteenotto ja todentaminen 15

4.2 Haavoittuvuudet 16

4.3 Haavoittuvuuksien torjunta 18

5 Pohdinta **21**

6 Yhteenveto **24**

Lähdeluettelo **26**

1 Johdanto

Nykyaikana erilaista tietoa liikkuu enemmän kuin koskaan aiemmin. On itsestään selvää, että osa tästä tiedosta on erittäin arkaluonteista ja se on pidettävä salassa ulkoisilta osapuolilta. Salasanojen käyttäminen on ollut hyvä tapa suojata arkaluonteista tietoa, mutta teknologian kehittyessä yksinkertaisten salasanojen murtamisesta on tullut helppoa. Yleinen ohje on, että samaa salasanaa ei kannata käyttää useammassa paikassa samaan aikaan. Toinen ohje salasanoihin on, että niistä pitää tehdä pitkiä ja monimutkaisia. Ihmisen on kuitenkin vaikea muistaa useita monimutkaisia salasanoja.

Kaikkia tietoturvaratkaisuja koskettaa sama taistelu käytettävyyden ja turvallisuuden välillä. Mitä enemmän ratkaisu sisältää tietoturvaominaisuuksia, kuten pitkiä salasanoja tai fyysisiä avaimia, sitä vaikeampi järjestelmä on murtaa. Tämä kuitenkin aiheuttaa ongelman, jossa luvallisen käyttäjän vaiva käyttää haluttua järjestelmää kasvaa. Tämä aiheuttaa usein tietoturvallisuuden laiminlyöntejä, esimerkiksi salasanaa valittaessa valitaan lyhyt ja helposti muistettava salasana. Tämä ikuinen taistelu on luonut tarpeen luotettavalle ja helppokäyttöiselle tunnistautumiselle.

Biometrisiä tunnistautumismenetelmiä voidaan pitää luotettavana ja helppokäyttöisenä vaihtoehtona salasanoille. Näitä tunnistautumismenetelmiä on useita, joista sormenjälki ja kasvojentunnistus ovat tällä hetkellä yleisimmin käytössä. Vaikka nämä menetelmät tarjoavat turvallisen tunnistautumistavan, kaikki järjestelmät voi jollain tapaa murtaa.

Biometrisien tunnistautumistapojen suurin haavoittuvuus on elollisuuden tunnistus. Tämän tutkielman tavoitteena on perehtyä sormenjälki- ja kasvojentunnistusteknologioiden elollisuuden tunnistuksen toimintaan. Tutkielmassa on pyrkimys saada selville elottomien kopioiden toimintaa molemmissa teknologioissa. Tutkielman tutkimuskysymykset ovat:

1. Minkälaisilla elottomilla kopioilla voi ohittaa sormenjälkitunnistimen?
2. Minkälaisilla elottomilla kopioilla voi ohittaa kasvojentunnistimen?

1.1 Menetelmät ja tiedonhaku

Tutkielma on toteutettu kirjallisuuskatsauksena. Kirjallisuutta on haettu IEEE:n (Institute of Electrical and Electronics Engineers) tietokannasta käyttämällä hakulausekkeita ”fingerprint” AND ”liveness detection” ja ”face” AND (”recog*” OR ”ident*”) AND ”liveness detection”. Hakutulokset on rajattu vuoteen 2020 ja uudemmat.

Sormenjälkitunnistusta koskeva haku tuotti 42 hakutulosta ja kasvojentunnistusta koskeva haku tuotti 72 hakutulosta. Tuloksia rajattiin ensin otsikoiden perusteella ja myöhemmässä vaiheessa abstraktin osuuden perusteella. Lopullinen aineisto koostuu viidestä sormenjälkitunnistukseen ja neljästä kasvojentunnistukseen liittyvästä vertaisarvioidusta artikkelista sekä useasta näitä päälähteitä tukevista artikkeleista aihealueittain. Näiden lähteiden lisäksi hakusanalla ”biometric authe*” on haettu yleistä tietoa biometrisestä tunnistautumisesta.

1.2 Rakenne

Tämän tutkielman alussa käydään läpi, mitä biometrinen tunnistautuminen on. Luvussa kolme käsitellään tarkemmin sormenjälkitunnistuksen toimintaa ja sen haavoittuvuuksia elollisuuden tunnistuksessa sekä näiden torjuntaa. Luku neljä käsitte-

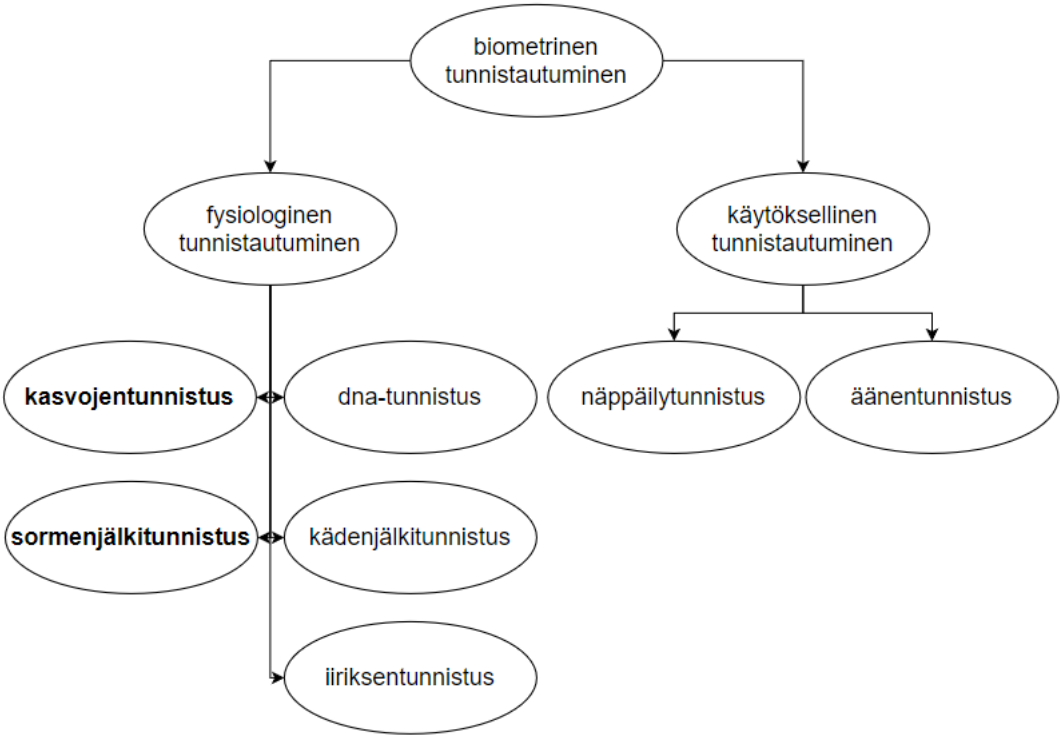
lee kasvojentunnistuksen osalta samoin sen toimintaa ja haavoittuvuuksia elollisuuden tunnistuksessa sekä näiden torjuntaa. Luku viisi kokoaa päätelmiä tutkielman aikana kerätyistä tiedoista ja siitä, kuinka todennäköisiä uhkia eri käyttäjäryhmille haavoittuvuudet ovat. Lopuksi luvussa kuusi kootaan yhteen edellisissä luvuissa käsitellyt asiat ja kerrataan merkittävimmät erot sormenjälki- ja kasvojentunnistuksen välillä.

2 Biometrinen tunnistautuminen

Biometrisessä järjestelmässä käyttäjä tallentaa itsestään fyysisen jäljen järjestelmään. Biometrinen tunnistautuminen tarjoaa nopean ja luotettavan tavan tunnistautua. Biometrisen tunnistautumisen etuna on käytännöllisyys, sillä Käyttäjän ei tarvitse muistaa monimutkaisia salasanoja. Käyttäjä ei myöskään voi unohtaa tai hävittää biometristä tunnistetta. [1]

Biometrisiä tunnistautumismuotoja on kahdenlaisia (kuva 2.1). Nämä ovat biologinen tunnistautuminen ja käytöksellinen tunnistautuminen. Käytöksellisiä tunnistautumismuotoja on esimerkiksi äänentunnistus ja näppäilytunnistus, jossa algoritmi tunnistaa käyttäjän näppäilyrytmin avulla käyttäjän. Biologisissa tunnistautumismuodoissa sensorit ottavat fyysisen näytteen halutusta henkilöstä. Erilaisia tunnistautumisia ovat muun muassa sormenjälki-, kasvojen-, kädenjälki- ja iiriksentunnistus sekä dna-näyte. [2] Nämä henkilöä yksilöivät piirteet tallennetaan biometrisen tunnistuksen suorittavaan laitteeseen, jotta henkilön identiteetti voidaan varmistaa. [3]

Biometrisen tunnisteen tulee täyttää seitsemän kriittistä ominaisuutta, jotta se toimii toivotulla tavalla. Nämä seitsemän ominaisuutta ovat uniikkius, kokonaisvaltaisuus, muuttumattomuus, keräiltävyys, toteutus, arvoisuus ja välttäminen. Näistä seitsemästä tärkein on uniikkius. Jos jokainen käyttäjä halutaan tunnistaa, on tärkeää, että käyttäjät pystytään erottamaan toisistaan [3].



Kuva 2.1: Biometristen tunnisteiden puukaavio

2.1 Suorituskyvyn vertailu

Erilaisia biometrisiä tunnistautumistapoja on lukuisa määrä, ja jatkuvasti tutkitaan mahdollisia uusia ominaisuuksia, joita voitaisiin hyödyntää biometrisessa tunnistautumisessa. Esimerkiksi aivoaaltojen hyödyntämistä biometrisessä tunnistautumisessa on tutkittu usean vuoden ajan [4][5], mutta se ei ole vielä päässyt yleiseen käyttöön. Selvittääksemme mitkä näistä useasta eri tunnistautumistavoista on toimivimpia ja luotettavimpia, on pitänyt kehittää menetelmiä, joilla suorituskykyä voidaan vertailla.

Biometristen tunnistautumismenetelmien suorituskykyä pystyy vertailemaan matemaattisilla funktioilla. Virheellisen hyväksynnän aste (engl. false acceptance rate, FAR) mittaa, kuinka usein luvaton käyttäjä pääsee järjestelmän tunnistautumisvaiheen ohi. Tämä voidaan laskea jakamalla väärä positiivinen näyte väärän positiivisen näytteen ja oikean negatiivisen näytteen summalla (yhtälö 2.1). Virheellinen

hylkäysaste (engl. False rejection rate, FRR) mittaa, kuinka usein järjestelmä hylkää luvallisen henkilön. Tämä voidaan laskea jakamalla virheellinen negatiivinen virheellisen negatiivisen ja oikean positiivisen summalla (yhtälö 2.2). Näiden kahden avulla voidaan laskea virhe ja tunnistusaste. Virhe on FAR ja FRR summa (yhtälö 2.3). Tunnistusaste lasketaan vähentämällä luvusta yksi sata kertaa virhe (yhtälö 2.4). [2]

$$FAR = \frac{vPos}{oNeg + vPos} \tag{2.1}$$

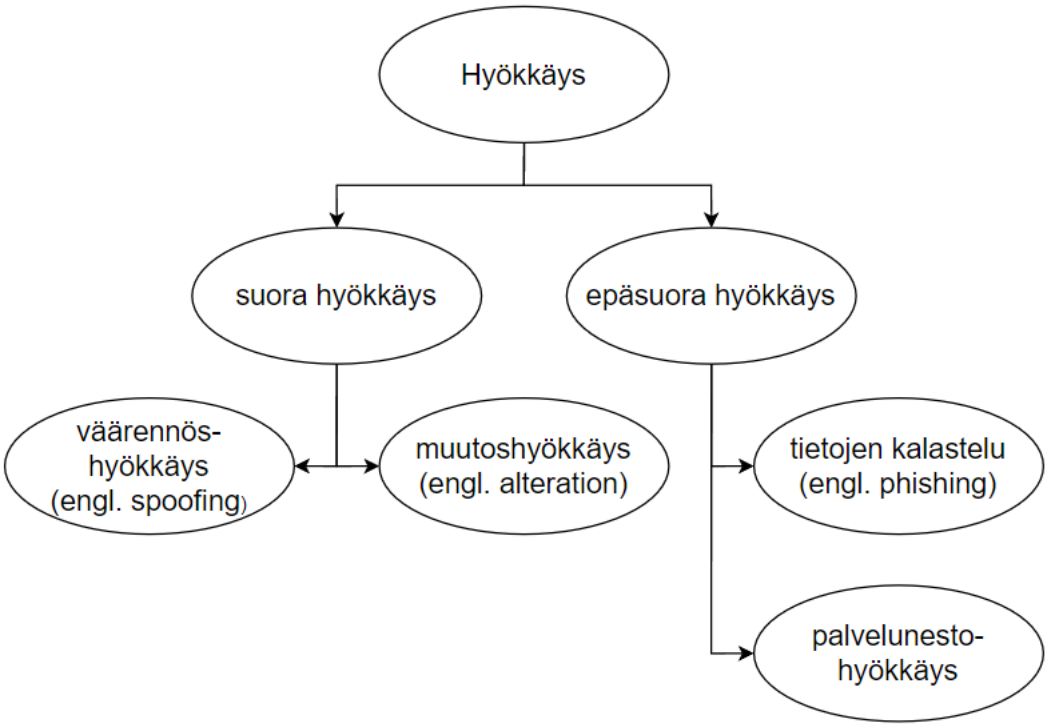
$$FRR = \frac{vNeg}{vNeg + oPos} \tag{2.2}$$

$$virhe = FRR + FAR \tag{2.3}$$

$$tunnisteaste = 1 - 100 * virhe \tag{2.4}$$

2.2 Biometrisen tunnisteen murtaminen

On olemassa kahdenlaisia keinoja, joilla voidaan yrittää murtaa biometrinen tunnistusjärjestelmä. Nämä ovat suorat ja epäsuorat hyökkäykset (kuva 2.2). Epäsuora hyökkäys voidaan toteuttaa ohjelmiston moduuliin tai moduulien väliseen rajapintaan, esimerkiksi tietojen kalastelulla (engl. phishing). Suorien hyökkäysten tavoitteena on huijata järjestelmän sensoria esittämällä sille väärennetty tunniste. Tämän vuoksi suoria hyökkäyksiä voidaan kutsua myös sensorihyökkäyksiksi. Suorat hyökkäykset voidaan jakaa kahteen kategoriaan: väärennös- (engl. spoofing) ja muutoshyökkäyksiin (engl. alteration). [6] Elottoman objektin esittäminen sensorille on yksi tapa toteuttaa suora hyökkäys. Elottomat objektit voidaan luokitella keinotekoisiin ja ihmisperäisiin. [7] Gelatiinista tehty sormi on esimerkki keinotekoisesta objektista ja irronnut sormi ihmisperäisestä objektista. Nämä elottomia objekteja hyödyntävät hyökkäykset kuuluvat väärennöshyökkäys kategoriaan. Väärennöshyökkäykset ovat



Kuva 2.2: Esimerkkejä eri hyökkäysten luokittelusta puukaaviossa

eniten käytetty tapa, jolla yritetään murtaa biometrisiä tunnisteita. Muunnoshyökkäyksissä hyökkääjä käyttää omaa biometristä jälkeään, jota on muokattu erilaisilla keinoilla, esimerkiksi imitoimalla hyökkäyksen kohdetta, ja yrittää näin onnistua murtamaan biometrisen tunnisteen. [6] Suorat hyökkäykset ovat huomattavasti yleisempiä kuin epäsuorat hyökkäykset, sillä niiden toteuttamiseen ei tarvita suurta määrää tietoa. [8]

Näiden hyökkäysten seurauksena on mahdollista, että biometrinen tunniste murretaan ja siitä saadaan mallinnettua kopio. Tämän seurauksena tunnistetta ei voi enää luotettavasti käyttää. Ihmisen biometrisiä ominaisuuksia on todella hankala muokata, joten uuden vastaavan tunnisteen luominen kopion uhrille on hankalaa. On myös mahdollista, että hyökkääjä murtaa tietopankin, johon usean henkilön biometrisen tunnisteen data on tallennettu, ja näin hyökkääjä murtaa usean henkilön biometrisen tunnisteen samanaikaisesti. [9]

3 Sormenjälkitunnistus

Sormenjälkitunnistautuminen on yleisin biometrinen tunnistautumistapa. [10] Sormenjälkitunnistautumisen suosio perustuu siihen, että se on kustannustehokasta ja se takaa todella suuren tunnistautumistarkkuuden. Sormenjälkitunnistautumisen käyttäminen on suosittua älypuhelimissa, rikostekniikassa ja lääketieteessä. [8]

Jokaisella ihmisellä on uniikki sormenjälki, jota voidaan hyödyntää yksilöidessä ihmisiä. Sormenjälki on pysyvä ja se ei muutu ihmisen vanhetessa. Vain harvoissa tapauksissa ihmisen sormi joudutaan amputoimaan, joten suurin osa ihmisistä pystyy hyödyntämään sormenjälkitunnistautumista niin kauan kuin haluaa.

Sormenjälkitunnistusta tutkittaessa yhdeksi tärkeimmäksi lähteeksi muodostui Omolewan ja muiden tutkimus [11], joka esittää selkeästi, miten sormenjälki saadaan mallinnettua sormesta muotoon, jota koneet ymmärtävät. Jeong ja Jeong [10] taas esittävät ongelmia älypuhelimissa runsaasti käytettyjen pienikokoisten tunnistimien osalta. Casula ja muut [12] avaavat tämänhetkistä tilannetta sormenjälkitunnistimien elollisuuden tunnistuksen tehokkuudessa. Spinoulas ja muut [13] tuovat esiin sormenjälkitunnistukseen kohdistuvien hyökkäysten torjuntaan hyödynnettäviä ratkaisuja. Zhang ja muut [14] puolestaan esittävät samoihin ongelmiin vaihtoehtoisia ratkaisuja. Näiden lisäksi mukana on muita lähteitä, joiden avulla tärkeimpien lähteiden väitteitä on voitu tukea ja mahdollisesti laajentaa.

3.1 Näytteenotto ja todentaminen

Jotta sormenjälkeä voidaan hyödyntää tunnistautumisessa, se täytyy ensin tallentaa järjestelmään. Sormenjälki voidaan tallentaa sensorin avulla. Yksi tapa tallentaa sormenjälki on muokata se binaarimuotoon. Tallennetun sormenjäljen mustille pikseleille voidaan asettaa arvo 1 ja vaaleille pikseleille arvo 0. Kun pikselin tummuutta arvioidaan se voi saada 256 eri intensiteettitasoa. Saatua intensiteettiarvoa verrataan kynnysarvoon ja tämän perusteella suoritetaan jako mustiin ja vaaleisiin pikseleihin. Tallennettua sormenjälkikuvaa useasti ohennetaan, jotta sormenjäljen harjanteet saadaan yhden pikselin paksuiseksi. Tämä helpottaa yksityiskohtien erottamista sormenjäljestä ilman, että se muuttaa yksityiskohtien paikkaa. Kuvan reunoille lisätään vaaleita pikselirivejä, jotta kaikkein reunimmaiset yksityiskohdat säilyvät varmasti kuvaa ohennettaessa. [11]

Sormenjäljen todentamiseen on erilaisia tapoja. Yksi tapa on hyödyntää sormenjäljestä saatujen yksityiskohtien paikkoja. Huonolaatuinen sormenjälki tuottaa ongelmia tälle tavalle. Toinen tapa on hyödyntää korrelaatiota. [11]

Pienikokoiset sormenjälkitunnistimet ovat saaneet suosiota puhelimien ja muiden käsikäyttöisten laitteiden käytössä, sillä pienempi tunnistin on halvempi tuottaa kuin iso tunnistin. Pienen koon vuoksi tunnistimen ottama sormenjälki on vain pieni osa sormenjäljestä. Tästä näytteestä käytetään nimitystä osittainen sormenjälki. Osittaista sormenjälkinäytettä otettaessa sormenjälkisensori tallentaa kuvan sormesta. Tämän jälkeen kuvasta saadun jäljen yksityiskohtia verrataan tietokannan sormenjälkiin. Tietokannan jäljet antavat tuloksen, kuinka samankaltainen jälki on. Parhaan tuloksen saanut jälki valitaan, ja jos tämän jäljen kynnysarvo ylittyy, tunnistautuminen hyväksytään. [10]

3.2 Haavoittuvuudet

Sormenjälkitunnistimien koko aiheuttaa merkittävän haavoittuvuuden tunnistautumismenetelmässä. Pienten tunnistimien käyttämät osittaiset sormenjäljet mahdollistavat niin sanotun ”masterprintin” luomisen. Tällainen masterprint kykenee huijaamaan järjestelmää ja esiintymään mahdollisesti useana eri sormenjälkenä. Mitä pienenemmän osan sormenjäljestä tunnistin käyttää, sitä helpompi on luoda masterprint. Osittaisen sormenjäljen tunnistuksessa kynnysarvon ylittävän sormenjäljen ei täydy olla täysin identtinen, sillä kynnysarvon ylittävät sormenjäljet hyväksytään. Mitä vähemmän yksityiskohtia osittaisessa sormenjäljessä on, sitä helpommin hyökkääjän käyttämä sormenjälki hyväksytään [10].

Älypuhelimissa käytettyjen sormenjälkitunnistimien ottama näyte on noin 9 - 48% koko sormenjäljestä. Mitä pienempi näyte sormenjäljestä otetaan, sitä vähemmän se sisältää yksityiskohtia. Tutkimus on osoittanut, että mitä pienemmän osan sormenjälkeä tunnistin käyttää yhdessä korkean FAR:n kanssa, sitä suuremmalla todennäköisyydellä hyökkääjä pääsee virheellisesti läpi tunnistautumisesta. Jotta sallittujen käyttäjien sormenjälkien onnistuneen hyväksyminen saadaan korkeaksi, täytyy myös FAR nostaa korkeammalle. [10]

Nykyisten mobiililaitteiden sormenjälkisensorit eivät tunnista onko niille esitetty sormenjälki elollinen vai onko se valmistettu jostain eri materiaalista, kuten paperista tai muovailuvahasta. Yksi yleisimmistä elottoman sormenjäljen torjumiseen käytetyistä tavoista on konvoluutioneuroverkot (engl. Convolutional Neural Network, CNN). Tällaiset neuroverkot ovat yleensä todella hyviä ja tarkkoja tunnistamaan sormenjäljet. Lähiaikoina on saatu selville, että nämä neuroverkot ovat haavoittuvaisia koulutusvaiheessa. Jos koulutusmateriaalin sekaan joutuu vääriä kuvia, algoritmi, jonka avulla sormenjälki tunnistetaan, ei toimi kunnolla. [15] CNN:n suureksi haasteeksi on muodostunut koulutusmateriaalin vähäisyys. Mitä enemmän eri parametreja CNN hyödyntää, sitä suuremman koulutusmateriaalin se tarvitsee toimiakseen

kunnolla. [16]

Sormenjäljen voi kopioida käyttämällä magneettista pulveria ja teippiä pintaan, jota haluttu sormi on koskenut. Helpompi tapa kopioida sormenjälki on ottaa siitä valokuva. Valokuvatusta sormenjäljestä tehty kopio kykenee läpäisemään muutamien modernien puhelimien sormenjälkitunnistuksen. Valokuvasta kopioidun sormenjälkihyökkäyksen toimivuutta on tutkittu vuoden 2019 kansainvälisen sormenjäljen elollisuuden tunnistus kilpailun voittaneita algoritmeja vastaan. Tutkimus osoitti, että hyökkääjillä on realistinen mahdollisuus huijata parhaita moderneja elollisuuden tunnistuksen algoritmeja. [12]

3.3 Haavoittuvuuksien torjunta

Esitelmähyökkäyksien tunnistus (engl. presentation attack detection, PAD) on tärkeä osa-alue sensoreihin kohdistuvia hyökkäyksiä torjuttaessa. Toinen nimi, jota esitelmähyökkäyksille voidaan käyttää, on väärennöshyökkäys (engl. spoofing). Tähän tunnistukseen käytettävät tavat voidaan jakaa kahteen osaan, jotka ovat ohjelmistopohjaiset ratkaisut ja hybridiratkaisut. Ohjelmistopohjaiset ratkaisut nimensä mukaan lisäävät pelkästään uuden ohjelmisto-osan, jonka avulla hyökkäys tunnistetaan. Hybridiratkaisuissa käytetään ohjelmisto-osan lisäksi uutta laitteistoa hyökkäyksen tunnistamiseen. Hybridiratkaisuista voidaan puhua myös laitteistopohjaisena ratkaisuna, mutta näissä laitteistopohjaisissa ratkaisuissa on aina mukana myös jonkinlainen ohjelmisto, joten kuvaavampi nimi on hybridiratkaisut. [13]

Ohjelmistopohjaisissa ratkaisuissa sormenjäljen elollisuus pystytään varmentamaan eristämällä sormenjäljestä halutut ominaisuudet. Esimerkkejä näistä halutuista ominaisuuksista ovat hikirauhaset, hiki, ihon elastisuus ja tekstuuri. [14] Hikirauhaset ovat nähtävissä sormenjäljen harjanteilla, kun sormenjälkeä tarkastellaan mikroskoopilla. Kun kehonlämpötila on korkeampi kuin ympäristö, nämä rauhaset erittävät runsaasti hikeä. Tämä ilmiö esiintyy aidoissa sormenjäljissä, mutta keino-

tekoisissa sormenjäljissä sitä ei esiinny. [16] Ohjelmistopohjaiset ratkaisut voidaan jakaa edelleen kahteen osaan, jotka ovat CNN:t sekä luokittelut, joissa hyödynnetään käsin tehtyjä ratkaisuja [17]. Useimmat viimeisintä tekniikkaa edustavat ratkaisut hyödyntävät CNN:iä. Jo olemassa olevia neuroverkkoja, kuten VGG-19, hyödynnetään sormenjäljen elollisuuden tunnistukseen lisäämällä niiden koulutukseen hienosäädettyä koulutusmateriaalia. [14]

Ohjelmistopohjaiset ratkaisut ovat kustannustehokkuutensa ja päivitysmahdollisuuksiensa myötä huomattavasti suositumpi ratkaisu, mutta hybridiratkaisuilla pystytään ratkaisemaan ohjelmistopohjaisissa ratkaisuissa olevia ongelmia. Tunnistautuminen ja hyökkäysten tunnistus ovat kaksi täysin erilaista toimenpidettä. Tämä rajoittaa yhden laitteen mahdollisuuksia suoriutua molemmista tehtävistä. Kaikki sormenjälkeä aistivat tekniikat ovat haavoittuvaisia vähintään yhdelle esitelmähyökkäyksessä käytettävälle materiaalille. Hybridimallissa on kaksi erilaista sormenjälkeä aistivaa tekniikkaa, jolloin onnistuneen hyökkäyksen on huijattava samanaikaisesti niitä molempia. [13] Keskeisimmät erot ohjelmistopohjaisten- ja hybridiratkaisuiden välillä on esitetty taulukossa 3.1.

Taulukko 3.1: Ohjelmistopohjaisten ja hybridiratkaisujen vertailu

	Ohjelmistopohjainen	Hybridi
kustannustehokas	x	
halvempi päivittää	x	
monimutkaisempi murtaa		x
pienempi fyysinen koko	x	

Tutkimus on osoittanut, että hybridiratkaisuista luotettavimmin suoriutuivat erilaiset sensorin suunnasta näkyvällä valolla tai infrapunalla valaistut ratkaisut. Näkyvän valon ja infrapunan läheisen valon (engl. near infrared, NIR) monispektriset kuvat antavat laajan kuvan esitetyn sormen spektristä ja tekstuurista. Lyhyen aallon infrapunalla saadaan ihmisen ihosta tyypillinen vaste, johon ihonväri ei vaikuta. [13]

Eräs tapa, jolla sormenjäljen elollisuutta voidaan tarkastaa tunnistautumisvaiheessa, on monisäteinen paikallinen binaarikuvio (engl. multi-radius local binary pattern, Multi-radius LBP). Tämä tapa käyttää paikallisen vaiheen kvantisointia (engl. local phase quantization, LPQ) paikallisten tekstuurien deskriptoreina ja aallokemuunnoksia (engl. wavelet transform) poistamaan kohinaa. [18]

Kun sormenjälkeä tunnistetaan tällä tavalla, ensimmäisenä sormenjäljestä poistetaan aallokemuunnoksella kohina. Tämän jälkeen multi-radius LBP muuttaa sormenjäljen binaarimuotoon. Lopuksi sumennettu tekstuuri luokitellaan LPQ:n avulla. Tutkimuksessa tämän tavan suoritusta mitattiin virhekeskiarvolla. Virhekeskiarvon voi laskea jakamalla FFR:n ja FAR:n summa kahdella (yhtälö 3.1). Tutkimukset ovat osoittaneet, että tämän tavan virhekeskiarvo on 6.73%. [18]

$$virhekeskiarvo = \frac{FRR + FAR}{2} \tag{3.1}$$

4 Kasvojentunnistus

Ihmiset ovat kautta aikojen erottaneet ihmiset toisistaan kasvojen avulla. Teknologian kehittyessä kasvojentunnistus on voitu toteuttaa tietokoneiden avulla ja nykyään tietokoneen tekemään kasvojentunnistusta voidaan hyödyntää arkisissa tunnistautumistilanteissa.

Kasvojentunnistusta hyödynnetään erilaisissa käyttöympäristöissä. Kasvojentunnistusta voidaan hyödyntää esimerkiksi valvontakameroissa, rajavartiossa ja muissa yhteiskunnallisissa tunnistusta vaativissa toimissa. Rikolliset on mahdollista jäljittää valvontakameroista saatujen kasvojen avulla. Nämä kasvot voidaan tunnistaa erilaisilla ohjelmistoilla, jotka esimerkiksi etsivät kaikki sosiaalisen median sivut, joilla samat kasvot ovat esiintyneet. Kasvojentunnistusta hyödynnetään myös yksilötasolla. Esimerkiksi usean älypuhelimen tai tietokoneen lukituksen voi avata käyttämällä kasvojentunnistusta. Myös sovellukset hyödyntävät kasvojentunnistusta tunnistautumisprosessissaan, esimerkiksi verkkopankkiin pystyy kirjautumaan kasvojentunnistuksella.

Kasvojentunnistukseen perehtyvässä luvussa lähteisiin on valikoitunut Kollin ja muiden tutkimus [19], jossa käydään selkeästi läpi, kuinka kasvoista saadaan muodostettua digitaalinen näyte sekä erilaisia tähän operaatioon käytettäviä algoritmeja. Mohzary ja muut [20] esittävät erilaisia uhkamalleja kasvojentunnistukseen ja tarjoavat yhden vaihtoehdon, jolla torjua nämä mahdolliset uhat. Hadiprakoso, Setiawan ja Girinoto [21] kuvailevat useita yleisiä tapoja torjua näitä haavoittu-

vuuksia ja syventyvät CNN:n pariin. Grinchuk, Parkin ja Glazistova [22] kertovat haastavimman haavoittuvuuden eli maskien käytön torjumisesta. Nämä lähteet valikoituivat tutkielmaan sopivan otsikoinnin ja abstraktin osuuden perusteella. Näiden lisäksi lukuun on valikoitunut muutama artikkeli tukemaan väitteitä ja tarjoamaan kattavampaa tutkimusta aiheesta.

4.1 Näytteenotto ja todentaminen

Ennen kuin kasvojentunnistusohjelma pystyy suorittamaan kasvojentunnistuksen siihen syötetystä kuvasta, on sen ensin tunnistettava, missä kohdassa kuvaa kasvot sijaitsevat. Jos tunnistusohjelmaan syötetään video, ohjelman täytyy myös osata valita sopiva kuva videosta. Tällainen sopiva kuva ei ole sumea ja siinä on selkeästi näkyvissä kasvot. Jotta tunnistusohjelma tietää onko kuva sumea, sen on ensin suoritettava sumeuden tunnistus. Näistä tunnistuksista tunnetuin on Laplacen operaattori, joka on määritetty alla esitettynä gradienttifunktiona (yhtälö 4.1). Kun Laplaceen lisätään kaksi Kerneliä, saadaan muodostettua Laplacen Kernel, joka on 3x3 matriisi. Jos tämä matriisi ei ylitä raja-arvoa, ohjelma toteaa, että kyseinen kuva on sumea. [19]

$$\Delta f(x, y) = div(grad(x, y)) \tag{4.1}$$

Kasvojen tunnistuksessa käytettävään datan keräämiseen on erilaisia tapoja. Kasvoista voidaan kerätä 2D- tai 3D-malli. Näissä tavoissa kamera kerää kasvoista yksityiskohtia, esimerkiksi kasvojen muodosta, nenästä, kulmakarvoista, huulista ja silmistä. Näiden etäisyydet toisistaan lasketaan ja niiden avulla saadaan luotua kasvoista tunniste. [23] Tämän tunnisteen avulla kasvoista saadaan koodattua tietokoneen tietokantaan yksilöivä tunniste. Ihmisen kasvoissa on noin 80–90 eri solmukohtaa, joista saadaan muodostettua kasvojentunnistukseen käytettäviä yksityiskohtia.

[19]

Muita algoritmeja, joita hyödynnetään kasvojentunnistuksessa ovat esimerkiksi histogrammitasaus, jota voidaan käyttää, jos tunnistusohjelmassa on esiintynyt kontrastiltaan heikko kuva. Histogrammitasaus yrittää tasoittaa pikseleiden kontrasti eroja. Haar Cascade -luokittelu on nopea algoritmi, jossa hyödynnetään suurta näytemäärää koulutuksessa sekä Haarin Kerneleitä, jotta saadaan erotettua kuvasta parhaat kasvojen piirteet. Myös k-lähimmän naapurin algoritmia voidaan hyödyntää kasvojentunnistuksessa. Sen yleisin käyttötarkoitus on kasvojen luokittelu. [19]

Myös kasvojentunnistuksessa voidaan hyödyntää paikallista binaarikuviota (engl. Local Binary Pattern, LBP). LBP algoritmissa pikseleistä luodaan 3x3 matriiseja, joissa reunimmaisia pikseleitä verrataan keskimmäiseen ja tämän perusteella annetaan pikseleille joko arvo 1 tai arvo 0. [24]

4.2 Haavoittuvuudet

Kasvojentunnistukseen kohdistuvien hyökkäysten määrä kasvaa kasvojentunnistusta käyttävien laitteiden yleistyessä [25]. Ihmisen kasvot ovat kuitenkin helpommin varastettavissa kuin esimerkiksi sormenjälki. Kohteen kasvot voidaan hankkia esimerkiksi kameralla tai sosiaalisesta mediasta. [21]

Kasvojentunnistus sensoreita voidaan yrittää murtaa kahdella tavalla. Nämä tavat ovat 2D- ja 3D-hyökkäykset. 2D-hyökkäysmalleja ovat valokuvan tai videon esittäminen hyökkäyksen uhrista sensorille. 3D-hyökkäyksissä käytetään usein maskeja. [26][24] Sekä 2D- että 3D-hyökkäykset voidaan jakaa staattisiin ja dynaamisiin hyökkäyksiin. Staattinen 2D-hyökkäys voi olla esimerkiksi valokuvan esittäminen sensorille. Yleinen esimerkki dynaamisesta 2D-hyökkäyksestä on videon esittäminen sensorille. 3D-hyökkäyksissä staattinen hyökkäys voi olla esimerkiksi kasvoista mallinnetun patsaan esittäminen sensorille ja dynaaminen 3D-hyökkäys voi olla toteutettu kosmetiikkaa hyödyntävällä robotilla. [21] 2D-tunnistimiin kohdistuvia hyökkäyk-

siä on tutkittu runsaasti. 3D-tunnistimiin kohdistuvia hyökkäyksiä on puolestaan tutkittu liian vähän. [27]

Valaistusta voidaan hyödyntää kasvojentunnistus sensoriin kohdistuvissa hyökkäyksissä [27]. Yleisessä käytössä olevat elektroniikkalaiteet, kuten älypuhelimet käyttävät muihinkin tarkoituksiin näkyvää valoa käyttäviä kameroita. Näiden kameroiden avulla pystytään suorittamaan myös kasvojentunnistus [28]. Useat algoritmit, joita käytetään 3D-kasvojentunnistuksessa hyödyntävät valoa [27].

Hyökkäykset voidaan luokitella kolmeen eri tasoon, joita voidaan nimetä kirjaimin A, B ja C. Tason A hyökkäyksiä on helppo toteuttaa. Esimerkki tason A hyökkäyksestä on valokuvan esittäminen sensorille. Tason B hyökkäykset ovat hieman monimutkaisempia hyökkäyksiä ja ne tarvitsevat avukseen hieman osaamista ja yksinkertaisia välineitä. Paperinen naamio, jossa naamion silmiin on puhkaistu pienet reiät, on esimerkki tason B hyökkäyksestä. Tason C hyökkäykset ovat haastavia toteuttaa ja vaativat asiantuntijatason osaamista. Niiden valmisteluun kuluu huomattavasti kauemmin kuin tason B hyökkäyksiin. Esimerkiksi virtuaalinen 3D-malli kasvoista on tason C hyökkäys. Näistä hyökkäyksistä tason A ja tason B hyökkäyksien tunnistaminen on standardi tunnistuslaitteissa, jos algoritmilla on nopea tunnuksenvarmistus verkossa (engl. Fast Identity Online, FIDO) -sertifikaatti, mutta tason C hyökkäyksien tunnistaminen on todella hankalaa. [20]

Elollisuuden tunnistaminen nykyisillä tekniikoilla on haastavaa, sillä esitelmähyökkäyksissä käytettävien välineiden laatu paranee ja näiden välineiden valmistamisprosessi helpottuu. [20] 3D-tulostimien yleistyminen ja niiden tuottaman tulosteen tarkkuuden parantumisen myötä 3D-maskien käyttö hyökkäyksissä on yleistynyt ja niiden tehokkuus kasvanut. Tätä ongelmaa kasvattaa nykyisten hyökkäysten tunnistuskeinojen huono yleistettävyys. Nykyiset tietokannat sisältävät todella vähän vaihtelua esimerkiksi ihon värin, valaistuksen tai mallihenkilöiden välillä. Tästä seuraa algoritmien huono suoriutuminen uusissa olosuhteissa. [22]

4.3 Haavoittuvuuksien torjunta

Kasvojentunnistuksessa esiintyviä haavoittuvuuksia voidaan torjua ohjelmisto-, laitteisto- tai silmäpohjaisilla ratkaisuilla. Laitteistopohjaiset ratkaisut ovat laskennallisesti kalliita, sillä kuvaaminen on kallista ja ne vaativat valosensoreita, jotta elollisuuden tunnistus onnistuu. Ohjelmistopohjaiset ratkaisut vaativat paljon muistia ja monimutkaiset hyökkäykset tuottavat merkittäviä haasteita. Silmäpohjaiset ratkaisut tarvitsevat käyttäjän yhteistyötä ja erityisvälineitä. [20]

Kasvojentunnistuksessa käytettävässä elollisuuden tunnistuksessa usein tarkastellaan silmien tai huulien liikkeitä. Silmänräpäytystä hyödyntämällä saadaan todella tarkasti tunnistettua, onko sensorille esitetyt kasvot esimerkiksi valokuva tai patsas. Tällainen piirteiden tarkkailu toimii tehokkaasti valokuvahyökkäyksiä vastaan, mutta kun hyökkääjä hyödyntää videota tai maskia, tämä keino ei ole enää riittävä. Näitä muita hyökkäysmalleja vastaan on täytynyt kehittää uusia tapoja. [21]

Haaste ja vastaus -todennus (engl. challenge-response authentication) on tapa, jolla pystytään torjumaan esitelmähyökkäyksiä. Tässä tavassa tunnistettavalta henkilöltä odotetaan tiettyä toimintoa, jota kutsutaan haasteeksi. Tämän jälkeen laite tunnistaa haasteen ja suorittaa henkilön todentamisen. Tässä tavassa suurimmaksi haasteeksi on muodostunut käytettävyys, sillä jatkuva haasteen tekeminen aiheuttaa suurta ylimääräistä työmäärää tunnistettavalle henkilölle. [21]

3D-kamerat ovat todella tehokas tapa estää esitelmähyökkäyksiä. Näiden kameroiden tarjoama erityistarkkuus pikseleiden syvyyteen mahdollistaa 3D-objektin, kuten kasvojen, erottamisen litteästä kuvasta. Näitä kameroita ei olla vielä pystytty hyödyntämään puhelimien sovelluksissa. [21]

Kuvan tekstuurissa on havaittavissa selkeitä eroja, kun verrataan oikeita ja väärennettyjä kasvokuvia. Tämä ero johtuu kasvojen uudelleenrakentamisen aikana tapahtuvasta kasvojen ilmeiden ja heijastavuuden laadun heikkenemisestä. Tätä teks-

tuurieroa on yritetty havaita hyödyntämällä esimerkiksi LBP:tä tai lähimmän naapurin algoritmia. Tekstuuritunnistuksen heikkoutena on kuitenkin sen riippuvuus valaistuksesta. [21]

Tutkimusten keskittyminen alkuaikoina näkyvään valoon kasvojentunnistukseen kohdistuvan esitelmähyökkäyksen tunnistuksessa johtuu näkyvää valoa hyödyntävien kameroiden suosiosta päivittäin käytetyissä elektroniikkalaitteissa. [28]

Videolla tehtyjä kasvojentunnistukseen kohdistuvia hyökkäyksiä vastaan elollisuutta voidaan tarkastaa CNN:n avulla [21]. Kasvojentunnistukseen voidaan hyödyntää sekä 2D- ja 3D-CNN-malleja. 2D-mallissa CNN-matriisi koostuu korkeus- ja leveysakseleista. 3D-mallissa mukana on myös syvyysakseli. [29] Näiden CNN:n kehityksen ja sensoriteknologian kehityksen myötä monimodaliteetti suosio esimerkiksi älypuhelimissa on kasvanut. Monimodaliteettia on tutkittu todella vähän verrattuna aiemmin suosittuihin yksittäisiin kameroihin. [28] Myös CNN:n ongelmaksi on havaittu se, kuinka ei ole olemassa vain yksiselitteistä piirrettä, jota niiden tulisi etsiä. Tällä hetkellä luotamme, että nämä CNN:t löytävät jotain mitä ihmissilmät eivät huomaa. [21]

3D-tunnistuksen tietokantojen vaihtelevuuden puutetta on lähdetty ratkomaan ja esimerkiksi CASIA-SURF HifiMask -tietokanta on huomattavasti enemmän vaihtelua sisältävä tietokanta kuin moni muu vaihtoehto. Osa tunnistusalgoritmeista on suunniteltu niin, että ne tarkastelevat kasvoja kokonaisuutena. Tästä seuraa ongelma, jossa algoritmi ei huomaa hyökkääjän paljastavia yksityiskohtia, kuten epäluonnollista silmän kimallusta tai epänormaalia ihon tekstuuria. Toinen osa tunnistusalgoritmeja hajottaa kasvot useaan osaan ja tarkastelee näitä erikseen. Tämän tavan ongelmaksi muodostuu se, kuinka kasvojen osa saattaa olla liian pieni tarkasteluun tai algoritmi keskittyy liikaa paikallisiin yksityiskohtiin ja unohtaa kokonaisuuden. [22]

Grinchuk ja muut esittivät tutkimuksessaan, että kasvojentunnistuksen voisi to-

teuttaa useassa korkeamman resoluution erässä, joissa keskitytään eri osiin kasvoja, esimerkiksi yksi tunnistus tarkastelisi korvia ja toinen silmiä. Korkean resoluution avulla kuvista saataisiin erotettua yksityiskohdat tarkemmin. Tämän lisäksi tarkasteltaisiin myös kasvojen kokonaisuutta, jotta voidaan hyödyntää molempien tapojen parhaat puolet. Tämän tekniikan avulla virhekeskiarvoksi saatiin 3%. [22]

Yksi tyyppiesimerkki, joka hyödyntää CNN:iä on Apple in My Eyes (AIME). AIME on ohjelmistopohjainen torjuntakeino, joka hyödyntää sarveiskalvoja elollisuuden tunnistuksessa. AIME tunnistaa sarveiskalvoista tulevan heijastuksen. AIME hyödyntää syviä CNN:iä ja sen funktio myötäkytkentää saadakseen CNN:ltä kuvan ominaisuudet. Käyttämällä VGG-16:ta AIME onnistuu 99,99% tarkkuudella ominaisuuksien erottelussa ja luokittelussa. [20]

5 Pohdinta

Kuten kaikki muutkin tietoturvallisuuteen liittyvät suojaustavat, myös biometriset tunnisteet ovat käytettävyyden ja turvallisuuden välisen jatkuvan taistelun uhreja. Ovi, jossa on tuhat eri lukkoa, on vaikea tiirikoida ja näin se pitää luvattomat käyttäjät hyvin poissa, mutta nämä tuhat lukkoa aiheuttavat myös luvalliselle käyttäjälle suuren vaivan päästä ovesta läpi. Tämä sama ilmiö esiintyy myös biometristen tunnisteiden kohdalla, esimerkiksi sensorin hyväksymistarkkuudessa. Jos sensorilla on matala FAR, se estää hyvin luvattomien käyttäjien pääsyn tunnistuksen läpi, mutta usein nämä sensorit hylkäävät myös luvallisen käyttäjän helpommin, sillä niiden vaatimassa näytteessä saa olla vähemmän poikkeamia näytekappaleeseen verrattuna. Turvallisimmin toimivat laitteet tarvitsevat usein paljon osia ja näin niiden koko saattaa kasvaa suureksi. Tästä seuraa ongelmia käytettävyyteen, jos laite, joka käyttää biometristä tunnistetta on tarkoitettu liikuteltavaksi. Edellä mainittujen asioiden seurauksena täydellistä biometristä tunnistautumisjärjestelmää on lähes mahdoton luoda. Taulukossa 5.1 on vertailtu kasvojentunnistusta ja sormenjälkitunnistusta, jotta saadaan parempi kuva niiden keskeisistä eroista.

Taulukko 5.1: Sormenjälki- ja kasvojentunnistuksen suorituskyvyn vertailu taulukko

	Sormenjälki	Kasvot
Enemmän tutkittu	x	
Murtamistapa on tiedossa	x	x
Näytteen varastaminen yksinkertaista	x	x
Varastamaninen somesta		x
Vähemmän uhkamalleja	x	

Käyttäjän kasvot on huomattavasti helpompi varastaa julkisella paikalla kuin sormenjälki ilman, että herättää suurta huomiota. Tämä tapahtuu yksinkertaisesti ottamalla valokuva kohteesta tai käyttämällä niiden sosiaaliseen mediaan julkaisemaa kuvaa hyödyksi. Toisaalta, jos hyökkäyksen tekijä todella haluaa sormenjäljestä näytteen, voi hyökkääjä käydä leikkaamassa kohteelta halutun sormen irti. Tämän jälkeen hyökkääjä on käytännössä jo murtanut sormenjälkitunnisteen. Henkilöt, jotka todennäköisemmin valikoituvat tällaisten hyökkäysten kohteiksi, ovat todennäköisesti joitain muita henkilöitä kuin normaalia rauhallista elämää eläviä henkilöitä, joten tämä ei kovin suurella todennäköisyydellä koske suurta osaa ihmisistä. Monet hyökkäystavat vaativat usein ammattitaitoisia menetelmiä ja tämän seurauksena hyökkäyksen kohteet todennäköisesti valitaan muulla tavalla kuin sattumalla.

Tutkielmassa tarkastellun kirjallisuuden perusteella esitelmähyökkäyksen toteuttamisessa kasvojentunnistukseen on useampi vaihtoehto kuin sormenjälkitunnistukseen kohdistuvassa hyökkäyksessä. Vaikka sormenjälkitunnistus voidaan ohittaa elottomalla kopiolla, joka on tehty esimerkiksi muovailuvahasta tai paperista, kaikki sormenjälkitunnistimeen kohdistuvat esitelmähyökkäykset ovat samankaltaisia. Kasvojentunnistukseen voidaan puolestaan esittää 2D- tai 3D-hyökkäyksiä ja nämä hyökkäykset kykenevät olemaan staattisia tai dynaamisia. Näissä hyökkäyksissä voidaan hyödyntää esimerkiksi valokuvia, patsaita, videoita tai maskeja. Kaikkiin näihin tilanteisiin vaaditaan erilaisia algoritmeja erottamaan luvallinen käyttäjä luvattomasta. Tästä seuraa se, kuinka kasvojentunnistusalgoritmeja kehitettäessä pitää ottaa huomioon useampi eri vaihtoehto, mikä johtaa hakalampaan kehitykseen.

Näiltä hyökkäyksiltä suojautuminen vaatii puolustajilta paljon ponnisteluja, sillä hyökkäykset kehittyvät jatkuvasti ja puolustajat ovat aina askeleen jäljessä, ja tämän lisäksi puolustajien on toimittava lain sallimilla tavoilla. Tekoälyn kehittyessä hyökkääjät saavat lisää välineitä, joiden avulla he voivat pyrkiä murtamaan biometrisiä tunnisteita. Generatiivisen tekoälyn hyödyntämisestä biometristen tunnisteiden

murtamisessa ei ole vielä julkaistu monia tutkimuksia, ja sen tutkiminen voisikin olla mahdollinen jatkokehitys tämän tutkielman aiheelle.

6 Yhteenveto

Tutkielmassa selvitettiin sormenjälkitunnistuksen ja kasvojentunnistuksen elollisuuden tunnistuksen tämänhetkisiä eroja kirjallisuuskatsauksena. Tutkielma eteni laajasta systemaattisesti aina rajatumpaan aiheeseen kohti tutkimuskysymyksiä:

1. Minkälaisilla elottomilla kopioilla voi ohittaa sormenjälkitunnistimen?
2. Minkälaisilla elottomilla kopioilla voi ohittaa kasvojentunnistimen?

Tutkimuksen aikana saatiin selville, että elottomia kopioita, joilla sormejälkitunnistimen voi ohittaa, ovat esimerkiksi muovailuvahasta tai paperista tehdyt kopiot. Elottomia kopioita, joilla voi puolestaan ohittaa kasvojentunnistuksen, ovat esimerkiksi kuvat, videot, patsaat ja maskit.

Tutkielmassa ensimmäisenä käsiteltiin biometristä tunnistautumista yleisellä tasolla. Biometrisentunnistautumisen voi jakaa kahteen alakategoriaan, fysiologinen tunnistautuminen ja käytöksellinen tunnistautuminen. Näitä tunnistautumistapoja voidaan yrittää murtaa kahdella erilaisella hyökkäystavalla. Nämä tavat ovat suorat ja epäsuorat hyökkäykset. Jotta tiedetään, kuinka hyvin nämä biometriset tunnisteet toimivat, on kehitetty matemaattiset mallit, joiden avulla näitä tunnistautumistapoja voidaan vertailla keskenään. FAR:ia ja FRR:ia pystytään hyödyntämään erilaisilla keinoilla, jotta saadaan laskettua esimerkiksi tunnistautumistavan virhekeskiarvo.

Kolmas luku käsitteli sormenjälkitunnista ja vastasi ensimmäiseen tutkimuskysymykseen. Sormenjälkitunnistuksessa verrataan sensorille esitettyä sormenjälkeä

järjestelmään tallennettuihin malleihin. Sormenjälki täytyy muuttaa muotoon, jota koneet ymmärtävät, jotta sitä voidaan vertailla järjestelmään tallennettuihin sormenjälkiin. Tämä tapahtuu muuttamalla se binaarimuotoon. Sormenjälkitunnistus voidaan ohittaa esimerkiksi muovailuvahasta tehdyllä elottomalla kopiolla sormenjäljestä. Tätä ongelmaa on yritetty ratkaista usealla eri tavalla hyödyntäen esimerkiksi erilaisia ohjelmistoja, kuten CNN:iä tai hyödyntämällä hybridiratkaisuja.

Tämän jälkeen käsiteltiin kasvojentunnistusta ja vastattiin toiseen tutkimuskysymykseen. Kasvojentunnistuksessa kasvojen yksityiskohtia, kuten silmien etäisyyttä toisistaan, verrataan järjestelmään tallennettuihin kasvoihin. Kasvojentunnistuksen voi murtaa 2D- tai 3D-hyökkäyksillä, joissa hyödynnetään esimerkiksi valokuvia tai maskeja. Hyökkäysten toimivuus riippuu algoritmista, jota tunnistusjärjestelmä käyttää. Myös kasvojentunnistuksessa hyökkäyksiä torjuttaessa voidaan hyödyntää esimerkiksi CNN:iä.

Lopussa suoritettiin lähteistä saatujen tietojen perusteella kokoava vertailu sormenjälki- ja kasvojentunnistuksen murtamisesta. Viimeisenä ajatuksena esitettiin, kuinka generatiivinen tekoäly saattaa mullistaa sormenjälki- ja kasvojentunnistuksen sekä niissä käytettävään elollisuuden tunnistuksen.

Lähdeluettelo

[1] J. Anand Babu, H. P. Neha, K. S. Babu ja R. N. Pinto, "Secure Data Retrieval System using Biometric Identification", teoksessa *2022 IEEE International Conference on Data Science and Information System (ICDSIS)*, 2022, s. 1–4. DOI: 10.1109/ICDSIS55133.2022.9915968.

[2] Vandana ja N. Kaur, "A Study of Biometric Identification and Verification System", teoksessa *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 2021, s. 60–64. DOI: 10.1109/ICACITE51222.2021.9404735.

[3] P. Johri ja M. S. Arora, "Review of the issues and a thorough investigation of biometric authentication systems", teoksessa *2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC)*, 2022, s. 892–897. DOI: 10.1109/IIHC55949.2022.10060335.

[4] L. Zhou, C. Su, W. Chiu ja K.-H. Yeh, "You Think, Therefore You Are: Transparent Authentication System with Brainwave-Oriented Bio-Features for IoT Networks", *IEEE Transactions on Emerging Topics in Computing*, vol. 8, nro 2, s. 303–312, 2020. DOI: 10.1109/TETC.2017.2759306.

[5] M. Fallahi, T. Strufe ja P. Arias-Cabarcos, "BrainNet: Improving Brainwave-based Biometric Recognition with Siamese Networks", teoksessa *2023 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 2023, s. 53–60. DOI: 10.1109/PERCOM56429.2023.10099367.

[6] M. R. Zafar ja M. Ali Shah, "Fingerprint authentication and security risks in smart devices", teoksessa *2016 22nd International Conference on Automation and Computing (ICAC)*, 2016, s. 548–553. DOI: 10.1109/IConAC.2016.7604977.

[7] "IEEE Standard for Biometric Liveness Detection", *IEEE Std 2790-2020*, s. 1–24, 2020. DOI: 10.1109/IEEESTD.2020.9080669.

[8] F. Alqahtani ja R. Zagrouba, "Fingerprint Spoofing Detection Using Machine Learning", teoksessa *2020 International Conference on Computing and Information Technology (ICCIT-1441)*, 2020, s. 1–7. DOI: 10.1109/ICCIT-144147971.2020.9213710.

[9] Y. Wang, B. Li, Y. Zhang, J. Wu, P. Yuan ja G. Liu, "A Biometric Key Generation Mechanism for Authentication Based on Face Image", teoksessa *2020 IEEE 5th International Conference on Signal and Image Processing (ICSIP)*, 2020, s. 231–235. DOI: 10.1109/ICSIP49896.2020.9339252.

[10] J. Y. Jeong ja I. R. Jeong, "Effect of Smaller Fingerprint Sensors on the Security of Fingerprint Authentication", *IEEE Access*, vol. 11, s. 97 944–97 951, 2023. DOI: 10.1109/ACCESS.2023.3312176.

[11] O. T. Omolewa, E. J. Adeioke, O. O. Titilope, A. K. Sakarivan ja A. J. Kehinde, "Border Control via Passport Verification using Fingerprint Authentication Technique", teoksessa *2023 International Conference on Science, Engineering and Business for Sustainable Development Goals (SEB-SDG)*, vol. 1, 2023, s. 1–7. DOI: 10.1109/SEB-SDG57117.2023.10124584.

[12] R. Casula, G. Orrù, D. Angioni, X. Feng, G. L. Marcialis ja F. Roli, "Are spoofs from latent fingerprints a real threat for the best state-of-art liveness detectors?", teoksessa *2020 25th International Conference on Pattern Recognition (ICPR)*, 2021, s. 3412–3418. DOI: 10.1109/ICPR48806.2021.9413301.

[13] L. Spinoulas, H. Mirzaalian, M. E. Hussein ja W. AbdAlmageed, "Multi-Modal Fingerprint Presentation Attack Detection: Evaluation on a New Dataset", *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 3, nro 3, s. 347–364, 2021. DOI: 10.1109/TBIOM.2021.3072325.

[14] Y. Zhang, S. Pan, X. Zhan, Z. Li, M. Gao ja C. Gao, "FLDNet: Light Dense CNN for Fingerprint Liveness Detection", *IEEE Access*, vol. 8, s. 84 141–84 152, 2020. DOI: 10.1109/ACCESS.2020.2990909.

[15] H. w. Kwon, J.-W. Nam, J. Kim ja Y. K. Lee, "Generative Adversarial Attacks on Fingerprint Recognition Systems", teoksessa *2021 International Conference on Information Networking (ICOIN)*, 2021, s. 483–485. DOI: 10.1109/ICOIN50884.2021.9333904.

[16] C. Yuan, S. Jiao, X. Sun ja Q. M. J. Wu, "MFFFLD: A Multimodal-Feature-Fusion-Based Fingerprint Liveness Detection", *IEEE Transactions on Cognitive and Developmental Systems*, vol. 14, nro 2, s. 648–661, 2022. DOI: 10.1109/TCDS.2021.3062624.

[17] R. C. Contreras, L. G. Nonato, M. Boaventura et al., "A New Multi-Filter Framework for Texture Image Representation Improvement Using Set of Pattern Descriptors to Fingerprint Liveness Detection", *IEEE Access*, vol. 10, s. 117 681–117 706, 2022. DOI: 10.1109/ACCESS.2022.3218335.

[18] Z.-S. Chen, R. Pulungan, Y.-H. Li et al., "Fingerprint Liveness Detection Using Handcrafted Feature Descriptors and Neural Network", teoksessa *2022 IEEE 11th Global Conference on Consumer Electronics (GCCE)*, 2022, s. 619–621. DOI: 10.1109/GCCE56475.2022.10014245.

[19] J. Kolli, S. Chaluvadi, V. M. Manikandan ja Y.-C. Hu, "An Efficient Face Recognition System for Person Authentication with Blur Detection and Image Enhancement", teoksessa *2022 1st International Conference on Sustainable*

Technology for Power and Energy Systems (STPES), 2022, s. 1–6. DOI: 10.1109/STPES54845.2022.10006633.

[20] M. Mohzary, K. J. Almalki, B.-Y. Choi ja S. Song, "Apple in My Eyes (AIME): Liveness Detection for Mobile Security Using Corneal Specular Reflections", *IEEE Internet of Things Journal*, vol. 10, nro 4, s. 3356–3367, 2023. DOI: 10.1109/JIOT.2022.3215916.

[21] R. B. Hadiprakoso, H. Setiawan ja Girinoto, "Face Anti-Spoofing Using CNN Classifier & Face liveness Detection", teoksessa *2020 3rd International Conference on Information and Communications Technology (ICOIACT)*, 2020, s. 143–147. DOI: 10.1109/ICOIACT50329.2020.9331977.

[22] O. Grinchuk, A. Parkin ja E. Glazistova, "3D mask presentation attack detection via high resolution face parts", teoksessa *2021 IEEE/CVF International Conference on Computer Vision Workshops (ICCVW)*, 2021, s. 846–853. DOI: 10.1109/ICCVW54120.2021.00100.

[23] K. Yliana, A. Arina ja P. Anastasia, "Vulnerability of Biometric Protection", teoksessa *2023 International Russian Smart Industry Conference (SmartIndustryCon)*, 2023, s. 275–280. DOI: 10.1109/SmartIndustryCon57312.2023.10110772.

[24] B. Wahyudono ja D. Ogi, "Implementation of Two Factor Authentication based on RFID and Face Recognition using LBP Algorithm on Access Control System", teoksessa *2020 International Conference on ICT for Smart Society (ICISS)*, 2020, s. 1–6. DOI: 10.1109/ICISS50791.2020.9307564.

[25] R. Padnevych, D. Semedo, D. Carmo ja J. Magalhães, "Improving Face Liveness Detection Robustness with Deep Convolutional Generative Adversarial Networks", teoksessa *2022 30th European Signal Processing Conference (EUSIPCO)*, 2022, s. 1866–1870. DOI: 10.23919/EUSIPCO55093.2022.9909693.

[26] A. A. Mohamed, M. M. Nagah, M. G. Abdelmonem, M. Y. Ahmed, M. El-Sahhar ja F. H. Ismail, "Face Liveness Detection Using a sequential CNN technique", teoksessa *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, 2021, s. 1483–1488. DOI: 10.1109/CCWC51732.2021.9376030.

[27] Y. Li, Y. Li, X. Dai, S. Guo ja B. Xiao, "Physical-World Optical Adversarial Attacks on 3D Face Recognition", teoksessa *2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2023, s. 24 699–24 708. DOI: 10.1109/CVPR52729.2023.02366.

[28] Z. Li, H. Li, X. Luo, Y. Hu, K.-Y. Lam ja A. C. Kot, "Asymmetric Modality Translation for Face Presentation Attack Detection", *IEEE Transactions on Multimedia*, vol. 25, s. 62–76, 2023. DOI: 10.1109/TMM.2021.3121140.

[29] N. Nanthini, N. Puviarasan ja P. Aruna, "A novel Deep CNN based LDnet model with the combination of 2D and 3D CNN for Face Liveness Detection", teoksessa *2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)*, 2022, s. 1–7. DOI: 10.1109/ICSES55317.2022.9914362.