Tallinna Ülikool

Digitehnoloogiate instituut

SÕRMEJÄLJE TUVASTUSSÜSTEEMID

Seminaritöö

Autor: Neyl Kaskmaa

Juhendaja: Andrus Rinde

Tallinn 2016

Autorideklaratsioon

Deklareerin, et käesolev seminaritöö on minu töö tulemus ja seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

.....	.....
(kuupäev)	(autor)

SISUKORD

SISSEJUHATUS

Enne 2011. aastat kui välja tuli esimene nutitelefon sõrmejälje lugejaga olid sõrmejäljed kasutusel peaaegu ainult kriminalistikas ning suurfirmades sissepääsu tagamiseks, kuid kui 2013. aastal tuli Apple välja oma *Touch ID'ga* siis muutus sõrmejäljelugeja tähtsus ja kättesaadavus kõigi jaoks. Teema kohta on olemas väga vähe eesti keelset materjali, seega on töö koostatud peaaegu ainult võõrkeelsetele allikatele toetudes.

Käesoleva töö eesmärgiks on lugejale tutvustada erinevaid sõrmejäljelugejate süsteeme. Töös seletatakse, kuidas toimivad erinevad süsteemid, ning mis on nende erinevused ja tugevused. Lisaks antakse töös lühike ülevaade ka teistes biomeetrilistest võimalustest, ning ülevaade biomeetria turvalisusest ja inimeste arvamusest biomeetria kohta.

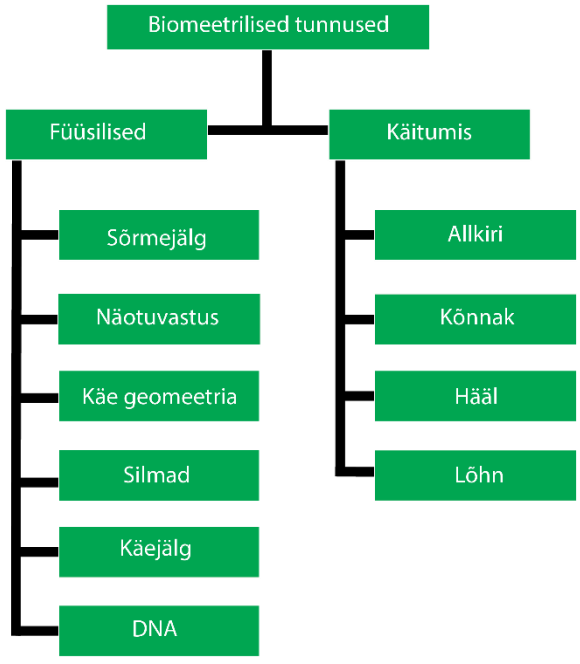
Käesoleva töö teema sai valitud, kuna autorile pakuvad huvi biomeetra ning sealhulgas sõrmejäljelugejad. Tänapäeva ühiskonnas levivad biomeetrilised isikutuvastussüsteemid aina laiemat, seega on hea anda ülevaade kasutusel olevatest tehnoloogiates.

Eesmärkide saavutamiseks annab autor kirjanduse põhjal ülevaate sõrmejäljest, kui ühest olulisemast biomeetrilisest isiku tuvastamise süsteemist.

1 BIOMEETRIA TUNNUS SÕRMEJÄLG

Biomeetriaks nimetatakse teadust, kus inimesi tuvastatakse tema füüsiliste-, keemiliste- ning käitumisomaduste järgi. Kaasaegses maailmas on biomeetria tähtsus kasvanud, kuna on vajadus suuremahuliste lahenduste järgi, mis suudaks inimesi tuvastada üle võrgu ning olla kindel, et tegemist on kindlasti õige inimesega. Lisaks kasvab biomeetria vajadus kuna vajatakse väga turvalist ja usaldusväärset moodust inimese isiku kindlaks tegemisel, praegused näiteks parooliga lahendused ei ole turvalised, kuna neid on väga lihtne ära unustada, jagada, arvata ning varastada. (Jain, Flynn,& Ross, 2008, 1)

Hetkel on maailmas kasutusel mitmeid erinevaid lahendusi inimeste tuvastamiseks. Biomeetrilised süsteemid kasutavad eelkõige sõrmejälgi, näotuvastust, käe/sõrme geomeetriat, silma vikerkesta ja võrkkesta, allkirja, kõnnakut, käejälge, häält, kõrva, käel olevaid veene, lõhna ning DNA-d. Need tunnused jagatakse omakorda kaheks, füüsilised omadused ning käitumisomadused (**Tõrge! Ei leia viiteallikat.**). Selliseid tunnuseid k asutatakse eelkõige sellepärast, et neid ei saa varastada ning üldjuhul ka kopeerida. (Jain et al., 2008, 3)



Joonis 1 Biomeetria tunnused

Enim kasutatakse praegusel ajal sõrmejälgi, kuna neid on väga mugav kasutajal kasutada ning sõrmejälje lugejad on üldiselt väga turvalised.

1.1 Biomeetria turvalisus

Biomeetriat on hakatud kasutama eelkõige, kuna see on teistest lahendustest turvalisem. Visa Euroopa (2015) poolt viidi läbi küsitlus, kus üritati leida erinevusi generatsioonide vahelisest netiturvalisusest. Noorem generatsioon on 16 kuni 24 aastased ning ülejäänud 25 või vanemad.

Küsitlusest selgus, et noorem generatsioon jagab oma paroole palju kergekäelisemalt, näiteks pangakaardi PIN koodi on jaganud 34% noorema generatsiooni vastanutest, kuigi kõikidest vastanutest on jaganud vaid 23%. Sama on ka mobiili parooliga, kuid seal on erinevus veel suurem. 32% noorematest on jaganud oma telefoni parooli, kuid vaid 10% kõikidest vastanutest. (Visa Europe, 2015)

Lisaks tuli uurimusest välja, et 32% noortest kasutab igal pool sama PIN koodi, ning 10% kasutab igal pool ka sama parooli. See näitab, et paroolid on väga ebaturvalised, ning lihtsalt varastatavad. (Visa Europe, 2015)

Vastanutest 76% kinnitas, et nad oleksid nõus kasutama biomeetrilisi turvakontrolle, näiteks sõrmejäljed ja näotuvastus. Küsitlusest selgus veel, et kõige turvalisemaks ja kindlamaks peetakse DNA analüüsi, seejärel sõrmejälge ja võrkkesta skanneerimist. (Visa Europe, 2015)

Levinud on arvamus, et biomeetria kasutamine ei ole turvaline, kuna sellega jagad sa oma privaatsust eraettevõtetele, vahel ka riigiasutustele. Kardetakse identiteedivargust ning andmete valedesse kätesse sattumust. Tänapäeval on riigiasutustel olemas andmebaas inimeste biomeetriliste omadustega, ning isikudokumentide saamiseks tuleb igal juhul oma sõrmejäljed riigile jätta. (Trader, 2011)

Näiteks Eestis kantakse sõrmejälg igasse isikut tõendavasse dokumenti peale ID-kaardi. Eelkõige on see loodud dokumentide võltsimise vältimiseks. Sõrmejälg loob seose dokumendi ning omaniku vahel. (Politsei- ja Piirivalveamet, 2016)

Tegelikkuses on peaaegu võimatu erafirmadelt sõrmejälgi varastada, kuna need on krüpteeritud nii, et sellest ei ole võimalik üldse pilti vaadata, ning algoritmi abil suudab pildi luua vaid süsteem. Muidugi on väga väike võimalus, et keegi sellega ka hakkama saaks, kuid see on väga minimaalne. Seega on sõrmejäljed üks turvalisemaid viise isikute tuvastamiseks. Samas, kui sõrmejälg kuidagi kopeeritakse siis seda nii lihtsalt vahetada ei saa nagu parooli. (Trader, 2011)

1.2 Sõrmejälje tunnused

Kõik inimesed on eristatavad oma sõrmejälgede poolest. Igal sõrmejäljel on mustrid, mille abil tuvastatakse, kelle sõrmega on tegemist. Üldiselt tuvastatakse sõrmejälgi kolme tunnuse abil: papillaarkurrud, papillaarmustrid ning eritunnused. (Kisand, 2013, 14)

Papillaarkurrud: pärisnaha peal asuv marrasnahk, mis on moodustanud joonja kurru. Papillaarkurrud on sõrmedel, varvastel, peopesal ja jalatallal. (Lall, 2010, 9)

Papillaarmustrid: papillaarliinid, mis paiknevad joonjalt ja kühmudena, need on papilaarkurdudest tekkinud mustrid ja vormid. (Lall, 2010, 9)

Papilaarkurrud ning papilaarmustrid võib jagada kolmeks. Sõrmedel on need kaarkurrustik, silmuskurrustik ning keerdkurrustik (Joonis 2). Keerdkurrustike leidub ligikaudu 30% inimestel, kaarkurrustikke 5% ja silmuskurrustikke umbes 65%. (Kisand, 2013, 16)

Joonis 2 Papillaarmustrid Allikas: A. Lall, Kuritegude jälgede kriminalistikaline uurimine, Sisekaitseakadeemia 2010.

Sõrmejälge vaadeldes tehakse kõigepealt kindlaks sõrmejälje kurrustik. Seejärel uuritakse kindla kurrustiku eripärasid, näiteks kurru keskosa, papillaarliinide hulk keskosa ja delta vahel, deltade omavaheline paiknemine jne. Kõigi nende tunnuste alusel saab teha ülevaate sõrmejäljest, kuid lõplik otsus tehakse eritunnuste järgi. Eritunnused jagatakse omakorda neljateistkümneks. (Lall, 2010, 10)

1-2. Papillaarotsik on papillaarkurru algus või lõpp (Joonis 3). (Lall, 2010, 10)

Joonis 3 Papillaarotsik on papillaarkurru algus või lõpp Allikas: A. Lall, Kuritegude jälgede kriminalistikaline uurimine, Sisekaitseakadeemia 2010.

3. Papillaarlooke all mõeldakse aga detaili, milles papillaarkurru lookelise iseärasuse järel ei esine kõrvalekaldumist kurru esialgsest suunast (Joonis 4**Tõrge! Ei leia viiteallikat.**). (Lall, 2010, 10)

Joonis 4 Papillaarlooke Allikas: A. Lall, Kuritegude jälgede kriminalistikaline uurimine, Sisekaitseakadeemia 2010.

4. Papillaarkurru kumerus, reljeefsus (Joonis 5). (Lall, 2010, 10)

Joonis 5 Papillaarkurru kumerus Allikas: A. Lall, Kuritegude jälgede kriminalistikaline uurimine, Sisekaitseakadeemia 2010.

5. Papillaarkurru nõgusus (Joonis 6). (Lall, 2010, 10)

Joonis 6 Papillaarkurru nõgusus Allikas: A. Lall, Kuritegude jälgede kriminalistikaline uurimine, Sisekaitseakadeemia 2010.

6. Papillaarsilla moodustab kahte kõrvuti asetsevat papillaarkurdu ühendav papillaarlõik (Joonis 7). (Lall, 2010, 10)

Joonis 7 Papillaarkurde ühendav papillaarlõik Allikas: A. Lall, Kuritegude jälgede kriminalistikaline uurimine, Sisekaitseakadeemia 2010.

7. Papillaarkäänd on papillaarkurru järsult või sujuvalt toimuv suunamuutus, kusjuures pärast seda ei asetse papillaarkurd endisel tasapinnal (Joonis 8). (Lall, 2010, 10)

Joonis 8 Papillaarkäänd Allikas: A. Lall, Kuritegude jälgede kriminalistikaline uurimine, Sisekaitseakadeemia 2010.

8. Papillaarhaak, konks (Joonis 9). (Lall, 2010, 10)

Joonis 9 Papillaarhaak Allikas: A. Lall, Kuritegude jälgede kriminalistikaline uurimine, Sisekaitseakadeemia 2010.

9. Papillaarlõigul ületab pikkus selle laiuse (Joonis 10). (Lall, 2010, 10)

Joonis 10 Papillaarlõigul ületab pikkus selle laiuse Allikas: A. Lall, Kuritegude jälgede kriminalistikaline uurimine, Sisekaitseakadeemia 2010.

10. Papillaarsilm (Joonis 11). (Lall, 2010, 10)

Joonis 11 Papillaarsilm Allikas: A. Lall, Kuritegude jälgede kriminalistikaline uurimine, Sisekaitseakadeemia 2010.

11. Papillaarsaar kujuneb papillaar-kurru lahknemisel ja kurdude taasliitumisel, kusjuures moodustub saaretaoline detail (Joonis 12). (Lall, 2010, 10)

Joonis 12 Papillaarsaar Allikas: A. Lall, Kuritegude jälgede kriminalistikaline uurimine, Sisekaitseakadeemia 2010.

12. Papillaarpunkt -punktijas moodustis (Joonis 13). (Lall, 2010, 10)

Joonis 13 Papillaarpunkt Allikas: A. Lall, Kuritegude jälgede kriminalistikaline uurimine, Sisekaitseakadeemia 2010.

13.Papillaarlahknemine, hargnemine (Joonis 14). (Lall, 2010, 10)

Joonis 14 Papillaarlahknemine Allikas: A. Lall, Kuritegude jälgede kriminalistikaline uurimine, Sisekaitseakadeemia 2010.

14.Papillaarühinemine (Joonis 15). (Lall, 2010, 10)

Joonis 15 Papillaarühinemine Allikas: A. Lall, Kuritegude jälgede kriminalistikaline uurimine, Sisekaitseakadeemia 2010.

Kuna sõrme papillaarkurrustike vahale on higinäärmed, siis on inimese sõrmed peaaegu alati natukene niisked. Papillaarkurrustikes puuduvad rasunäärmed, kuid see satub sinna muudelt kehaosadelt, näiteks sügades, lisaks esineb papillaarkurrustikes surnud

marrasnaha rakke. Tänu higile ning rasule jätab inimene alati midagi puudutades maha endast jälje. (Kisand, 2013, 15)

Sõrmejäljed jäävad pinnasele erinevalt (Joonis 16), see oleneb sõrme niiskusest ja sõrmejälje füüsilisest kvaliteedist. (Maltoni, Maio, Jain,& Prabhakar, 2009, 74)

Joonis 16 Erineva niiskusega sõrmejäljed: a) hea sõrmejälg b) kuiv sõrmejälg c) märg sõrmejälg d) füüsiliselt halvas seisus sõrmejälg. Allikas: Davide Maltoni Handbook of Fingerprint Recognition 2009.

Seega sõrmejälje lugemiseks eristatakse inimestel papillaarkurrustikke, nende mustrit, mustrite omadusi ning papillaarkurrustikke eripäraseid jooni, lisaks peab sõrmejälg olema piisavalt niiske ja terve, et see oleks loetav. Lisaks sõrmejälgedele on igal inimesel ka erinev peopesa, jalatald ning varbad, mille järgi saaks samuti inimest tuvastada. (Kisand, 2013, 13)

1.3 Sõrmejälje lugemise tehnoloogia ajalugu

Sõrmejälgi on hakatud lugema alates 19nda sajandi lõpust, kui Sir Francis Galeton, kes oli muuseas Charles Darwini nõbu, defineeris sõrmel punktid, mille järgi saab sõrmejälgede järgi inimesi tuvastada. Neid sõrmel asetsevaid punke nimetati algselt „Galtoni punktideks“ ning neist punktidest sai alguse sõrmejälgede järgi inimeste tuvastamine. Neid üksikuid punkte on viimase sajandi jooksul edasi arendatud ning nii on loodud süsteem sõrmejälgede tuvastamiseks. (National Science and Technology Council [NIST], kuupäev puudub)

1960ndate lõpus, kui arenesid arvutid ning kogu tehnoloogia tekkis ka võimalus automatiseeritud sõrmejälgede tuvastamiseks. 1969 aastal otsustas Föderaalne Juurdlusbüroo ehk FBI, et on vaja automatiseeritud süsteemi, kuna inimene tuvastab sõrmejälgi liiga kaua. Nad pöördusid oma vajadusega National Institute of Standards and Technology (NIST) poole, et nad uuriksid kuidas oleks võimalik sellist süsteemi luua. (NIST, kuupäev puudub)

NIST tõi suurimate katsumustena välja sõrmejälgede skaneerimise ning suure hulga sõrmejälgede seast õige otsimise ja võrdlemise. (NIST, kuupäev puudub)

1975ndal aastal rahastas FBI sõrmejälje skannerite tehnoloogiat, mis viis lõpuks prototüübi valmimiseni. See seade salvestas vaid isikuandmed, sõrmejälje klassi ning eritunnused, kuna sellel ajal oli maksis mälu digitaalsete piltide salvestamiseks liiga palju, see süsteem töötas vaid ette antud piltidega. (NIST, kuupäev puudub)

Järgmiste aastate jooksul arendas NIST välja algoritmi, mille abil suutis süsteem kõik andmed kokku pakkida, ning said sellest väiksemahulise faili, mille nimeks sai M40 algoritm, see on esimene FBI poolt kasutatud süsteem inimeste tuvastamiseks sõrmejälgede abil. Selle süsteemi abil pidid töötajad ise muutma võrreldavate piltide hulga võimalikult väikseks, et arvuti suudaks väiksest valimist leida õige sõrmejälje. (NIST, kuupäev puudub)

1981. aastaks oli loodud juba viis automaatset sõrmejälje tuvastus süsteemi. Kõik süsteemid olid välja arendatud erinevate riikide poolt, ning seetõttu olid süsteemid erinevate tehnoloogiatega, ning omavahel süsteemis olnud sõrmejälgi võrrelda ei saanud.

See viis aga ühtse sõrmejälje lugemise standardini, mis kehtib tänapäevalgi. (NIST, kuupäev puudub)

Järgmise sammuna oli vaja reaalajas toimivat süsteemi. Selleks korraldati konkurss, kus oli eesmärgiks: 1. digitaalne sõrmejälje lugemine 2. kohapeal sõrmejälje tunnuste välja lugemine 3.tunnuste võrdlemine andmebaasis olevatega. Konkursi võitis 1994. aastal ettevõte Lockheed Martin, mis tegeleb lennundus-ja kosmosetööstuses, ning relva-ja kaitsetööstuses. Suurem osa süsteemist saadi tööle aastaks 1999. Selle ajavahemiku sees arendati sõrmejäljelugejaid ka erafirmade poolt. Süsteemid olid arendatud ligipääsu tagamiseks ning sisse logimiseks. Sellega oligi loodud automaatselt kohapeal sõrmejälgi tuvastav süsteem. (NIST, kuupäev puudub)

Lihtinimeste jaoks muutus sõrmejäljelugeja igapäevaseks 19. oktoobril 2004, kui IBM andis välja sülearvuti ThinkPad T42 (Joonis 17), millel oli sõrmejäljelugeja sisse logimiseks (Germain, 2004). Peale seda lõid ka paljud teised tootjad enda arvutitele sõrmejäljelugejad.

Joonis 17 Esimene sõrmejälje lugeja sülearvutil. Allikas: IBM kodulehekülg, http://www-01.ibm.com/common/ssi/rep_ca/6/897/ENUS105-006/index.html

Esimene telefon, millele on sisse ehitatud sõrmejälje lugeja on Toshiba G500 (Joonis 18), mis anti välja 2007. aasta veebruaris. Nagu ka esimesel arvutil, oli ka G500 sõrmejälje lugeja vaid telefoni lukust avamiseks, ning muud funktsionaalsust sellel polnud. (Chakrabarty, 2016)

Joonis 18 Toshiba G500. Allikas: Phonesdata koduleheküIg, http://phonesdata.com/en/smartphones/toshiba/g500-1810/

Esimene sõrmejälje lugeja tänapäevasel nutitelefonil oli Motorola Atrix, mis oli selleks ajaks Google poolt ära ostetud. Kui esimese nutitelefoni sõrmejälje lugejaga tegi tegelikult Motorola, siis suurt kasutajate huvi sõrmejälje lugejate vastu tõmbas siiski alles Apple iPhone 5s. Peale iPhone 5s'i lisasid enamus mobiilitootjaid oma lipulaevadele sõrmejälje lugejad, sealhulgas Samsung ning HTC. (Greenberg, 2013)

2 TEHNOLOOGIAD SÕRMEJÄLGEDE LUGEMISEKS

Sõrmejäljelugejaid kasutatakse tänapäeval väga erinevates kohtades, näiteks kriminalistikas, telefonides, ukselukkudes ja auto avamiseks.

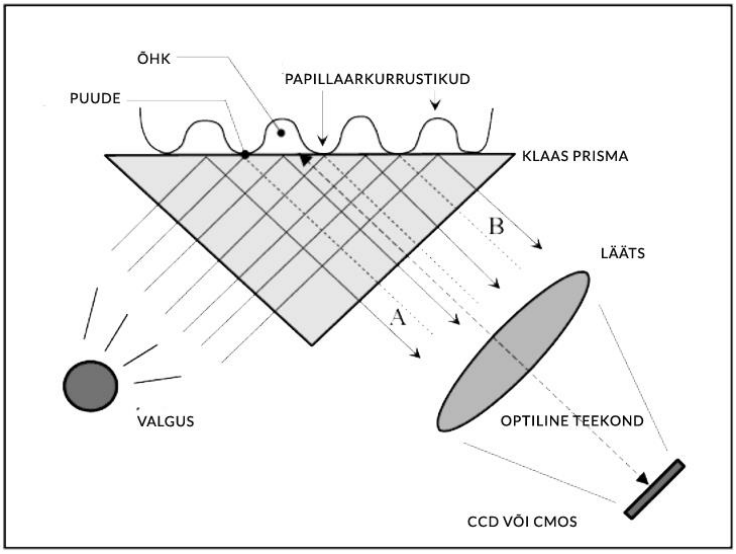
Sõrmejälje lugemiseks kasutatavates skannerites on kõige tähtsamaks komponendiks sensor, mis loob sõrmejäljest pildi. Peaaegu kõiki olemasolevaid sensoreid saab jagada kolmeks: optilised-, pooljuht- ning ultraheliskannerid. (Maltoni et al., 2009, 63)

2.1 Optilised skannerid

Reaalajas töötavatest skanneritest vanimad on just optilised skannerid ning neid kasutatakse väga palju siiani. (Maltoni et al., 2009, 63)

Optilised skannerid kasutavad peegeldumise efekti (Joonis 19). Kõige kasutatavam optilise skanneri tüüp on FTIR, mis peegeldab valguse abil papillaarkurrustikke. Kui papillaarkurrustiku tipud puutuvad kokku klaas/plastik pinnaga skanneri peal, siis on nad optilises ühenduses prisma pinnaga, kuid kurrud jäävad kindlale kaugusele. Prisma vasakut külge valgustatakse nii, et valgus hajub sõrmele. Valgus peegeldub vastavalt kurdudele ja kurrustike tippudele. Kuna pinnasega ühenduses olevad kurrustiku tipud jäävad peegeldades heledaks, ning kurrud tumedaks, siis joonistub välja sõrmejäljest muster. Tekkinud muster peegeldatakse skanneri paremasse külge, kus lääts muudab peegelduse CCD või CMOS sensorile sobivaks, ning seejärel koostab sensor sellest omakorda pildi. Kuna selline skaneerimine on kolmemõõtmeline, siis ei ole võimalik seda foto, ega prinditud paberi abil kopeerida. (Maltoni et al., 2009, 63)

Optilisi skannereid kasutatakse eelkõige kohtades, kus täpsus on oluline, kuid skanner ei pea olema väga väike. Suur osa uksi ja hooneid avavatest skanneritest, mis on kinnitatud näiteks uste kõrvale, töötavad just optiliselt. Optilised skannerid on väga turvalised, ning vastupidavad, kuid eelkõige täpsed. (Maltoni et al., 2009, 63)



Joonis 19 Optilise skanneri töö. Allikas: Maltoni et al. (2009) Handbook of Fingerprint Recogniton, 63.

Lisaks FTIR süsteemile on ka teisi optilisi skannereid, näiteks FTIR prisma lehtedega, kus ühe suure prisma asemel on terve leht väiksemaid, kuid see süsteem töötab väga sarnaselt. Peale selle on erinevaid lahendusi veel, kuid need kõik töötavad sama põhimõttega, seega ei ole vajalik neid eraldi lahti seletada. (Maltoni et al., 2009, 64)

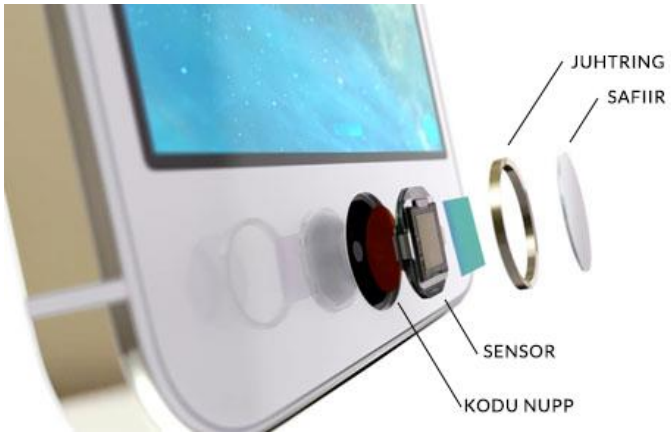
2.2 Pooljuhtskannerid

Kuigi pooljuhtskannerid patenteeriti juba 1980ndatel, siis kättesaadavaks muutusid need alles 1990ndate aastate keskel. Pooljuhtskannerid loodi, kuna teised tehnoloogiad olid liiga kulukad ja suured ning seetõttu ei saanud paljud kasutajad endale seda lubada. Pooljuhtskannerid on süsteemid, mille pinnal on õhuke kiht elektrit juhtivat materjali. Pooljuhtskannerid jagatakse nelja kategooriasse: mahtuvusskanner, termoskanner, pieso-elekterskanner ja elektriväljakannerid. (Maltoni et al., 2009, 67)

2.2.1 Mahtuvusskanner

Mahtuvusskanneri pind on jagatud pikslitest, mis moodustavadki tegelikult sensori. Sõrme ja pinnase vahel lastakse ringlema elektrilaengud, ning süsteem mõõdab, kui pikk vahemaa on sõrmel asetseva punkti, ning sensori vahel. Iga piksli kohta saadetakse laeng. Seega kurdude ning kurrustike tippude vahemaa pinnasega on erinev, ning selle abil joonistatakse välja muster. Nagu ka optilisi skannereid, ei ole võimalik lihtsa pildi abil seda skannerit petta. (Maltoni et al., 2009, 67)

Sellist lahendust kasutab näiteks ka Apple (Joonis 20). (Moldrich, 2014)



Joonis 20 iPhone sõrmejäljelugeja. Allikas. Macworld koduleheküIg, http://www.macworld.co.uk/news/apple/inside-iphone-5s-touch-id-scanner-how-does-iphone-fingerprint-scanner-work-3468255/

Apple kasutab juhtringina roostevaba terast, see peab tuvastama, kas inimene on sõrme nupule pannud. (Moldrich, 2014)

Pinnase materjalina kasutab Apple safiiri, eelkõige kuna see on hea juht. Lisaks ei teki kristallidele kriimustusi, seega ei mõjuta lugeja pind sõrmejälje kvaliteeti. (Moldrich, 2014)

Apple skanneri tihedus on 500 pikslit ühe tolli kohta, ehk sensor suudab luua väga selge pildi sõrmejäljest. (Moldrich, 2014)

2.2.2 Termoskanner

Termoskannerite puhul mõõdetakse sõrme mustrite temperatuure. (Maltoni et al., 2009, 68)

Asetades sõrme pinnale, hakkab skanner sõrme soojendama ning sõrme kurrustikud puutuvad kokku lugeja pinnaga. Selle tagajärjel on kurdude vahele jääva õhu temperatuur on kontaktis oleva osaga erinev. Selle abil koostatakse sõrmest pilt, mille sensor suudab tuvastada. (Maltoni et al., 2009, 68)

Termoskannereid kasutatakse kõige vähem, kuna nad võivad olla ebatäpsed, sellegipoolest on nad väga väiksed ning neid saab igale poole paigutada. Näiteks kasutatakse termoskannereid tulirelvadel, ning relvast saab lasta vaid see kelle sõrmega see klapib. (Homeland Security, 2016)

2.2.3 Piesoelekterskanner

Piesoelekterskanner ehk rõhuskanner, annab sõrmele elektrilaengu, kui skanneri pinnale on avaldatud survet. Skanneri pind on tehtud elektrit mittejuhtivast materjalist ning peale surve avaldamist tekib sõrme ja pinna vahel elektrivool. Sõrmemustri erinevad osad avaldavad elementidele erinevalt survet ja selle järgi mõõdab sensor kurrustike kauguse, ning loob pildi. Paraku ei ole see aga hea lahendus, kuna üldiselt pole need sensorid väga täpsed. Piesoelekterskanner oli üks esimesi pooljuht skannereid, mis leiutati, kuid tänapäeval seda enam ei kasutata. (Maltoni et al., 2009, 69)

2.2.4 Elektriväljaskannerid

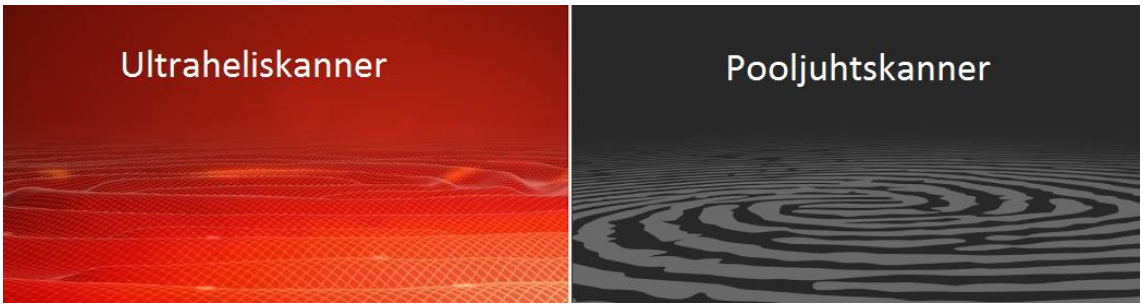
Elektriväljaskannerid koosnevad kahest osast: juhtring, mis koostab siinuselise signaali ning maatriksi antennidest, mis suudavad elektri signaali vastu võtta, antenniks ongi sõrm. Ringi sees asetsev pind peab olema materjal, mis juhiks elektrit. Ring annab sõrmele elektrilaengu ning sensor mõõdab signaali kauguse ning koostab selle abil sõrmejäljest pildi. Pildi õnnestumiseks peab sõrm olema kogu aeg ühenduses nii ringiga kui ka sensoriga. Elektrivälja skannerit kasutati rohkem eelmise kümnendi alguses, kus peamiseks kasutus kohaks olid sissepääsud, ning ka mõned arvutite küljes olevad skannerid. (Maltoni et al., 2009, 68)

2.3 Ultraheliskannerid

Ultraheliskannerite puhul kasutatakse helilaineid. Skanner saadab välja akustilised signaalid, ning jäädvustab tagasi peegeldatud signaali pikkused. Signaali abil mõõdetakse sõrmejälge osade kaugust ning kurrustiku struktuuri. Ultraheliskanner koosneb kahest osast: saatja, mis genereerib akustilised helid ning vastuvõtja, mis võtab vastu tagasi tulnud lained. See meetod loob pildi sõrme pinnast isegi läbi õhukese kinda, kuid sõrm peab lugemiseks olema väga puhas, ning tehnoloogia oli veel paar aastat tagasi väga kallis. Ühe skanneri hinnaks oli kuni 5000 dollarit. (Maltoni et al., 2009, 69)

Esimese ultraheliskanneri paigaldas telefonile Hiina firma Qualcomm, kes suutis ultraheliskanneri teha väga väikseks ning paigutada see telefoni sisse. Skanner on saadaval nende 2016. aasta lipulaeval Le Max Pro. Skanner asub telefoni tagumisel küljel, ning asetades sõrm skannerile, saadab skanner välja lained, mille järgi sõrmejälg

tuvastatakse. Võrreldes teiste skanneritega on ultraheliskanneri eeliseks kolmemõõtmeline pilt, mis on tunduvalt turvalisem, kui näiteks pooljuhtskannerite kahemõõtmeline pilt (Joonis 21). (Triggs, 2016)



Joonis 21 Ultraheliskanner ja pooljuhtskannri loodud pilt. Allikas http://www.androidauthority.com/how-do-ultrasonic-fingerprint-scanners-work-666053/

2.4 Skannerite kvaliteet

Skannerite kvaliteeti mõõdetakse mitmete parameetrite abil, nendeks on pindala, resolutsioon, halli tase, geomeetria täpsus, signaali täpsus. Lugeja testimiseks kasutatakse erinevaid algoritme ning leitakse erinevused saadud piltide vahel, üldjuhul kehtib reegel: mida suurem on parameeter seda parem on tulemus. (Maltoni et al., 2009, 76)

Skannereid jagatakse kaheks, mitme sõrme lugejad ning ühe sõrme lugejad. Mitme sõrme lugejaid kasutatakse eelkõige näiteks piiriületusel, isikudokumentides. Ühe sõrmejälje lugejaid kasutatakse näiteks arvutisse või telefonisse sisse logimiseks. Mitme sõrme lugejad on peaaegu 10 korda kallimad, seega ei tasu nende paigaldamine näiteks arvutile lihtsalt ära, kuigi mitme sõrme lugeja on palju turvalisem. (Maltoni et al., 2009, 83-84)

Sõrmejälje lugejatest ei saa välja tuua parimat, neil kõigil on omad plussid ja miinused. Optilised skannerid on väga täpsed ja turvalised, kuid nad on ka aeglasemad ning süsteem on kulukas ning suurem kui teised. (Maltoni et al., 2009, 71)

Kõige odavam lahendus on pooljuht skannerid, kuna nüüdseks on sensorite hinnad läinud väga madalaks ning sensorite täpsus väga suureks, siis võib pooljuhtskannereid pidada kõige paremaks variandiks, kuid pooljuht skannerid ei ole nii täpsed kui optilised skannerid.

Kõige täpsemad ja turvalisemad skannerid on ultraheliskannerid, kuid neid ei toodeta väga palju kuna nende hind on teistest kordades kõrgem. (Maltoni et al., 2009, 69)

2.5 Sõrmejälje lugemine mobiilseadmetes

Kui Apple tuli esimese sõrmejäljelugejaga välja aastal 2013, siis Androidil oli see võimalus juba aastal 2011, kui välja tuli Motorola Atrix, kuid Windows Phone'il veel sõrmejäljelugejaid pole.

Apple andis arendajatele ligipääsu oma sõrmejäljelugejatele aastal 2014, kui välja tuli operatsioonisüsteem IOS 8.0. Sellest ajast saati saab kõikidesse rakendustesse lisada sõrmejäljega isikutuvastuse. (Apple, kuupäev puudub)

Androidi arendajad saavad sõrmejäljelugejat kasutada 2015. aasta oktoobrist, kui Android avalikustas uue operatsioonisüsteemi Marshmallow. Samuti saab sõrmejälje tuvastuse lisada igale rakendusele, mis arendatakse. (Android, kuupäev puudub)

Kuigi Windowsi telefone sõrmejälje lugejaga veel pole, siis Windows andis arendajatele ligipääsu juba aastal 2014, kui välja tuli Windows 8.1, Windowsi operatsiooni süsteemi puhul saab seda kasutada ka arvuti rakenduste loomiseks. Esimene Windowsi operatsioonisüsteemiga, ning sõrmejäljelugejaga telefon tuleb välja 2016 aasta lõpus HTC poolt. (Microsoft, 2015)

Kõikide süsteemide puhul toimib sõrmejälje tuvastamine telefonis, kuna üksi seadmetest ei salvesta sõrmejälgi kuskile mujale. Lisaks sellele ei avalda üksi firma salvestatud sõrmejälgi kolmandatele osapooltele, vaid kontrollib oma süsteemis, kas sõrmejälg on õige, ning siis saadab vastuse kolmandale osapoolele. (Microsoft, 2015) (Android, kuupäev puudub) (Apple, kuupäev puudub)

KOKKUVÕTE

Käesoleva seminaritöö eesmärgiks oli tutvustada lugejatele erinevaid sõrmejäljelugejate süsteeme.

Sõrmejäljelugejate tehnoloogiaid on palju erinevaid, ning neil kõigil on omad plussid ja miinused. Nagu töös selgub, siis kõige rohkem kasutatakse pooljuhtskannereid. Tõenäoliselt, kuna see on üks odavamaid ning suhteliselt täpne variant. Pooljuhtskannerite suurimaks plussiks võib lugeda selle kompaktsuse.

Teised skannerid on liiga suured ning kulukad, et neid paigutada väikestesse igapäeva seadmetesse, kuid sõrmejäljelugejad arenevad edasi ning varsti on ka teised süsteemid muudetud kompaktsemaks.

Teiste biomeetriliste süsteemide arendus on väga kallis ja tehnoloogia noor, kuid tulevikus kasutatakse neid rohkem, kuna osad neist on veel turvalisemad kui sõrmejäljed.

Antud valdkond on maailmas veel väga noor, kuid areneb iga päevaga aina edasi. Edasi tuleks uurida ka teisi biomeetrilisi võimalusi ning anda neist ülevaade. Kuna kasutusel on väga palju erinevaid biomeetrilisi lahendusi, siis oleks uurimus väga mahukas, kuid väga vajalik ning huvitav.

Eelkõige tuleks uurida näotuvastust ning häältuvastust, kuna nende areng on kõige kiirem ning aktuaalsem. Lisaks tuleks uurida biomeetria üldist turvalisust, ning teiste tehnoloogiate turvalisust võrreldes sõrmejälgedega, sest näiteks allkirjad, mis kuuluvad samuti biomeetria alla, ei ole enam turvalised lahendused.

KASUTATUD KIRJADUS

Android (kuupäev puudub) *Android 6.0 APIs* Loetud aadressil https://developer.android.com/about/versions/marshmallow/android-6.0.html

Apple (kuupäev puudub) *Local Authentication.* Loetud aadressil https://developer.apple.com/reference/localauthentication

Chakrabarty, J. (2016, 17. aprill). *Fingerprint Scanner On Phones: History & Evolution, But Do We Really Need That?* [ajaveebipostitus]. Loetud aadressil https://www.igadgetsworld.com/fingerprint-scanner-history-evolution-but-do-we-really-need-that/

Germain, J. M. (2004, 4. oktoober). IBM Introducing Fingerprint Reader into Laptop. *TechNewsWorld.* Loetud aadressil http://www.technewsworld.com/story/37017.html

Greenberg, A. (2013, 11. september). Motorola Bashes Apple's iPhone Fingerprint Reader, Forgets It Sold One First. *Forbes.* Loetud aadressil http://www.forbes.com/sites/andygreenberg/2013/09/11/motorola-bashes-apples-iphone-fingerprint-reader-forgets-it-sold-one-first/#2329197493be

Homeland Security (2016) *Smart Gun Technology Patents.* Loetud aadressil https://www.dhs.gov/sites/default/files/publications/R-Tech%20Smart%20Gun%20Technology%20Patents%20for%20Micro%20Site%20DELIV%20160719.pdf

Jain, A., Flynn, P., & Ross, A.(2008). *Handbook of Biometrics.* New York: Springer.

Kisand, E. (2013). *Sõrmejäljed ja daktüloskoopiaekspertiisid* (magistritöö). Loetud aadressil http://dspace.ut.ee/bitstream/handle/10062/31635/kisand_evelin.pdf

Lall, A. (2010). *Kuritegude jälgede kriminalistikaline uurimine.* Loetud aadressil https://digiriiul.sisekaitse.ee/handle/123456789/301?locale-attribute=et

Maltoni, D., Maio, D., Jain, A., & Prabhakar, S.(2009). *Handbook of Fingerprint Recognition.* London: Springer.

Microsoft (2015, 29. aprill) *Windows Software Development Kit for Windows 8.1* Loetud aadressil https://developer.microsoft.com/en-us/windows/downloads/windows-8-1-sdk

Moldrich, C. (2013, 16. oktoober). What is Apple's Touch ID and how does it work? *The Telegraph.* Loetud aadressil http://www.telegraph.co.uk/technology/apple/11167454/What-is-Apples-Touch-ID-and-how-does-it-work.html

National Science and Technology Council (kuupäev puudub) *Fingerprint Recognition.* Loetud aadressil https://www.fbi.gov/file-repository/about-us-cjis-fingerprints_biometrics-biometric-center-of-excellences-fingerprint-recognition.pdf

Politsei- ja Piirivalveamet (2016). *Sõrmejäljed isikut tõendavates dokumentides.* Loetud aadressil https://www.politsei.ee/et/teenused/lingid/sormejaljed/index.dot

Trader, J. (2011, 24, jaanuar). *Biometrics, Privacy and Identity Theft – What Are You Risking?* [ajaveebipostitus]. Loetud aadressil http://blog.m2sys.com/privacy-2/biometrics-privacy-and-identity-theft-%E2%80%93-what-are-you-risking/

Triggs, E. (2016, 6. jaanuar). Ultrasonic fingerprint scanners: how do they work? *Android Authority.* Loetud aadressil http://www.androidauthority.com/how-do-ultrasonic-fingerprint-scanners-work-666053/

Visa (2015). *Generation Z ready for biometric security to replace passwords.* Loetud aadressil https://www.visaeurope.com/newsroom/news/generation-z-ready-for-biometric-security-to-replace-passwords