TARTU ÜLIKOOL

Arvutiteaduse instituut

Informaatika õppekava

Mariliis Malahhov

Biomeetriapõhise isikutuvastuse tõsikindluse alused sõrmejäljele ja näokujutisele

Bakalaureusetöö (9 EAP)

Juhendajad: Angelika Kärber

Heili Orav

Tartu 2023

Biomeetriapõhise isikutuvastuse tõsikindluse alused sõrmejäljele ja näokujutisele

Lühikokkuvõte

Biomeetria on saanud isikutuvastamise vahendina maailmas üha populaarsemaks ja paljud riigid, sealhulgas ka Eesti, on kasutusele võtnud automaatse biomeetrilise isikutuvastuse süsteemid ehk ABISe. Bakalaureusetöö eesmärk oli soovitada Eesti ABISele juhiseid, mida saaks seal näotuvastuse ja sõrmejäljevõrdluse algoritmidele lävendite seadmisel arvesse võtta. Lisaks oli eesmärk uurida seda, kuidas maailma riikide praktikas on biomeetrilisi andmeid kasutatud ja kuidas andmete kasutust on seadusega reguleeritud. Töö raames tehakse lühiülevaade sõrmejälje ja näotuvastuse ajaloost, varasemast sõrmejäljetuvastussüsteemist, näotuvastussüsteemi tööpõhimõttest ja sõrmejäljevõrdluse metoodikatest. Seejärel tutvustatakse Eesti ABISt. Siis analüüsitakse ülevaatlikult, kuidas sõrmejälge ja näotuvastust on maailma riikides seni kasutatud ja kuidas seda kasutust reguleeritakse. Viimaks tehakse organisatsiooni National Institute of Standards and Technology koostatud kahe raporti tulemuste analüüsi põhjal ABISe jaoks soovitusi ja tähelepanekuid.

Võtmesõnad: biomeetria, sõrmejälje tuvastus, näotuvastus

CERCS: P170

The bases for certainty of biometric identification for fingerprint and facial image

Abstract:

Biometrics has become more popular in the world and many countries, including Estonia, have started using an automated biometric identification system aka ABIS. The aim of this Bachelor's thesis was to recommend guidelines for Estonia's ABIS so they could be taken into account when setting thresholds for the fingerprint and face recognition algorithms. An additional aim was to do an overview of how countries of the world have used biometric data and how the usage of such data is regulated by law. The paper gives an overview of the history of fingerprint and face recognition, previous fingerprint identification system, how a facial recognition system works and the methodologies of fingerprint comparison. Then a description of Estonia's ABIS is given. An analysis of how fingerprint and face recognition have been used in different countries and how such usage is regulated in the world is given. Lastly, two reports

prepared by National Institute of Standards and Technology are analysed and recommendations and observations are given for ABIS based on the results of the analysis.

Keywords: biometrics, fingerprint recognitation, face recognition

CERCS: P170

Sisukord

Sissejuhatus

Biomeetriat kasutatakse maailmas isikutuvastamise ja –samasuse kontrolliks üha rohkem. Igapäevaelus on tavalised näited telefoni lahti lukustamine sõrmejälje või näokujutise abil ja internetipanga mobiilirakendusse sisse logimine sõrmejäljega.

Eesti riik on loonud automaatse biomeetrilise isikutuvastuse süsteemi ehk ABISe, mida haldab siseministeerium. Süsteem sai valmis ja võeti osaliselt kasutusele 2021. aastal, täies ulatuses hakatakse seda kasutama 2023. aasta teises pooles. ABISt hakatakse kasutama isikutuvastuseks ja -kontrolliks erinevates olukordades, peamisteks kasutusaladeks saavad olema õiguskaitse, haldusmenetlus ja piirikontroll. ABISes säilitatakse inimeste näokujutised, sõrmejäljed ja peopesajäljed. Süsteem hakkab oma tööd tegema tehisintellekti abil ja selles kasutatakse ühte algoritmi näotuvastuse ja teist sõrmejäljevõrdluse jaoks. Biomeetriavõrdluse algoritmides kasutatakse täpsuse hindamiseks mõõdikutena väärtuvastuse ja väärnegatiivsuse määra. Hetkel veel puuduvad Eesti ABISes kindlad standardid lävenditele, millest need mõõdikud sõltuvad.

Selle bakalaureusetöö eesmärk oli alguses nende mõõdikute numbriline määramine ABISe jaoks, aga töö käigus sai selgeks, et seda pole olemasolevate andmete ja teadmiste põhjal võimalik teha. Uueks eesmärgiks seati üldisemate soovituste tegemine, mida saaks lävendite seadistamisel arvesse võtta. Lisaks, kuna ABIS säilitab ja kasutab biomeetrilisi andmeid, on eesmärk analüüsida, kuidas maailma riikides on selliseid andmeid kasutatud ja seda kasutust seadusega reguleeritud.

Lõputöö käigus antakse esmalt teoreetiline ülevaade sõrmejälje ja näotuvastuse ajaloost, varasematest tuvastussüsteemidest ja sõrmejäljevõrdluse metoodikatest. Seejärel tutvustatakse lühidalt Eesti ABISt. Järgnevalt analüüsitakse biomeetriliste andmete kasutamist viies valdkonnas ja kasutuse reguleeritust maailmajagude järgi. Viimaks võetakse kokku kaks Ameerika Ühendriikide organisatsiooni National Institute of Standards and Technology ehk NIST koostatud raportit, mis võrdlesid sõrmejälje- ja näotuvastusalgoritme, ja tehakse raporti tulemuste analüüsist lähtuvalt ABISe jaoks soovitusi.

1. Biomeetria ja selle kasutamine

Küllap on tänapäeval enamikul inimestest olnud mingisugune kokkupuude biomeetriaga. Kuigi üldises tähenduses mõistetakse biomeetria all bioloogiliste andmete mõõtmist ja statistilist analüüsi, on käesoleva töö raames kasutusel Andmekaitse ja infoturbe leksikoni (edaspidi AKIT) definitsioon, mis määratleb biomeetria kui „indiviidide automaatne tuvastamine bioloogiliste ja käitumislike karakteristikute põhjal“ [1]. Biomeetrilise tuvastuse saab jagada kaheks: biomeetriline isikutuvastus (ingl *identification)* ja biomeetriline kontroll (ingl *verification*) [2]. Biomeetrilise isikutuvastuse eelduseks on olemasolev biomeetriline andmebaas. Isikutuvastuse käigus võetakse isikult mingisugused biomeetrilised andmed ja võrreldakse neid andmebaasis olemasolevatega, et isiku identiteeti leida [3]. Biomeetrilise kontrolli all mõistetakse seda, kui isik peab mingile süsteemile või teenusele ligi pääsemiseks tõestama biomeetrilise tunnuse abil oma identiteeti [2].

Kuigi käesolevas töös käsitletakse sõrmejälge ja näokujutist, on biomeetrilisi tunnuseid veel mitmeid erinevaid, näiteks silmaiiris või võrkkest, peopesa, allkiri, DNA, hääl. Eestis kasutusele võetavas automaatse biomeetrilise isikutuvastuse süsteemis (edaspidi ABIS, vt 3. ptk.) hakatakse lisaks sõrmejälgedele ja näokujutistele talletama ka peopesajälgi [4].

Biomeetriat on võimalik kasutada paljudes erinevates valdkondades, nagu näiteks [5]:

- õiguskaitse ja avalik julgeolek (kriminaalne/kahtlustatav isik)
- sõjaline (vaenlase/liitlase tuvastamine)
- piiri-, reisi- ja rändekontroll (reisija/rändaja tuvastamine)
- identiteedihaldus (kodaniku/elaniku/valija andmed)
- tervishoid ja toetused (patsiendi/abisaaja/tervishoiutöötaja tuvastamine)
- füüsiline (hooned/ruumid) ja loogiline (arvutisüsteemid/võrgud) juurdepääs (omaniku/kasutaja/töötaja/töövõtja/partneri tuvastamine)
- kommertsrakendused (tarbija/kliendi tuvastamine).

Seoses biomeetria üha laialdasema kasutamisega on tekkinud ka mure inimeste privaatsuse ja isikuandmete kasutamise pärast. Kuna andmekaitse on oluline ka ABISes, antaksegi viiendas peatükis ülevaade sõrmejälgede ja näokujutise kasutuse reguleerimisest maailma riikides, et teiste eeskujul saaks oma riigi süsteemi täiendada.

Probleemi olemusest arusaamiseks on vaja teatud tausta. Selleks tutvustataksegi järgnevalt sõrmejälje ja näotuvastuse ajalugu ja seda, kuidas on võimalik sõrmejälge klassifitseerida. Kirjeldatakse ka ABISe eelkäijat, automaatset sõrmejälgede tuvastussüsteemi (AFIS) ja tehakse ülevaade peamistest metoodikatest, mida sõrmejäljevõrdluse eksperdid kasutavad.

2. Sõrmejälje ja näotuvastuse ajalugu ning sõrmejäljevõrdluse metoodikad

Taustast ja uurimisprobleemist arusaamiseks on oluline teada ka ajalugu ning meetodeid, kuidas automaatne tuvastus töötab. Selles peatükis antakse ülevaade sõrmejäljest ja näotuvastuse ajaloost, tutvustatakse sõrmejälgede klassifitseerimissüsteemi ja kirjeldatakse automaatset sõrmejälgede tuvastussüsteemi (AFIS). Lisaks tutvustatakse peamisi sõrmejäljevõrdluse metoodikaid.

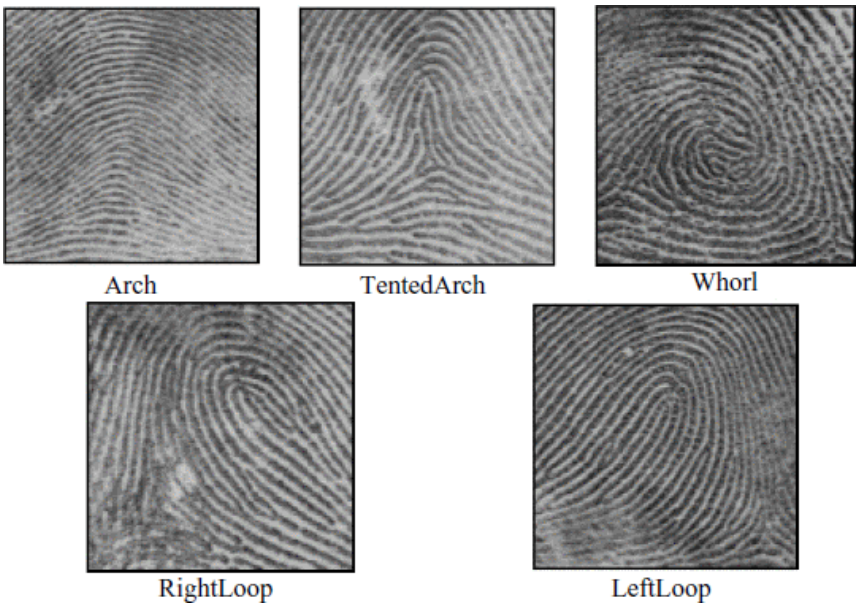
2.1 Sõrmejälje lühiajalugu

Sõrmejälje all mõistetakse sõrmeotsa papillaarjoontest võetud või jäänud jälge [6]. Sõrmejälge on identifitseerimiseks kasutatud juba aastatuhandeid, aga esimese teadusliku uuringu sõrmejälgede kohta avaldas 1684. aastal botaanik Nehemiah Grew [7]. Pärast seda hakati sõrmejälgede uurimisega tõsisemalt tegelema. Cummins ja Midlo [8] kirjutavad, et 1788. aastal avaldas Mayer sõrmejälgede anatoomia detailse kirjelduse. Tema oli ka esimene, kes pani tähele, et sõrmejälgedel on teatud sarnasused [8]. Sellele järgnesid katsed sõrmejälgi kategoriseerida. Lee [7] kirjutab, et esimese klassifitseerimissüsteemi, kus eristati üheksat mustrit, pakkus välja Purkinje 1823. aastal. Faulds viis 1870-ndatel läbi eksperimendi, mille tulemused kinnitasid sõrmejälgede muutumatust [7]. See tulemus oli oluline, kuna sellega saab osaliselt põhjendada sõrmejälgede kasutamise teaduslikku alust. Galton lisas sõrmejälgede klassifitseerimisse sõrmejälje eritunnused (ingl *minutiae*) 1888. aastal [9]. Ta hakkas koostööd tegema *Sir* Edward Henryga, et arendada välja uus klassifitseerimissüsteem, mis avaldati 1899. aastal. See sai tuntuks Henry süsteemina ja võeti kasutusele enamikus inglise keelt kõnelevatest riikidest [10].

20. sajandi alguses hakati sõrmejäljepõhist isikutuvastust laialdaselt kasutama ja loodi esimesed kriminaalide sõrmejälgede andmebaasid [7]. 1980-ndatel valmisid esimesed automaatsed sõrmejäljetuvastuse süsteemid (ingl *automated fingerprint identification system,* tuntud lühendi AFIS all) [11]. AFISe arendamine sai võimalikuks tänu tehnoloogia arengule, samas oli sellega seotud mitmeid väljakutseid. Neid väljakutseid ja AFISe tööd järgnevalt tutvustataksegi.

2.2 Sõrmejälgede klassifitseerimine ja AFIS

Kuigi sõrmejäljed on unikaalsed, on võimalik neid teatud tunnuste järgi kategooriatesse jagada. Henry süsteemi järgi saab kõige üldisemalt eristada viit mustrit [12], need on näidatud joonisel 1. Hiljem arendati välja veel palju erinevaid klassifitseerimise süsteeme, näiteks oli Ameerika Ühendriikides politseil vaja süsteemi, mille abil tuvastada kuriteopaigale jäetud üksikuid sõrmejälgi [10]. Ühe näitena tänapäevani kasutatavast süsteemist saab välja tuua Ameerika Ühendriikide Föderaalse Juurdlusbüroo klassifikatsiooni, kus eristatakse kaheksat peamist mustrit [13].



Joonis 1. Peamised sõrmejäljed [14].

Vastavalt AKITile on sõrmejälgede mustritüübid tõlgitud järgnevalt: *arch* – kaarkurrustik, *whorl* – keerdkurrustik, *loop* – silmuskurrustik [1]. Terminit *tented arch* pole seal tõlgitud.

Sõrmejäljekujutised saab võtmisviisi järgi jagada kahe kategooria vahel: vaalitud, mille puhul sõrmejälje võtmisel rullitakse sõrm küljelt küljele nii, et tekkiv pilt on küüneservast teise küüne-servani ja vajutatud, mille puhul tekib pilt pinnale vajutatud sõrmelt, rullimist ei kasutata [10].

Moses [10] kirjutab, et enne kui leiutati automaatsed tuvastussüsteemid, toimus sõrmejälgede käsitsi tuvastamine sel viisil, et ekspert võrdles sõrmejälgede eritunnusi (papillaarkurrulõpud ja

papillaarkurruhargmikud) sõrmejälgede papillaarjoontel. Kaks sõrmejälge sai kuulutada identseks, kui nende eritunnused olid topoloogiliselt samadel kohtadel. Automaatse tuvastussüsteemi arendamisel võeti see tuvastamisviis aluseks [10].

Automaatset sõrmejäljetuvastajat (ingl *automated fingerprint identification system*, AFIS) hakati esimesena välja töötama Ameerika Ühendriikides 1960. aastatel. Peamised väljakutsed süsteemi arendamisel olid paberil oleva sõrmejälje arvutisse kandmine, pildilt sõrmejälje eritunnuste eraldamine ja ühe sõrmejälje võrdlemine kõikide teiste andmebaasis olevatega. Esimesed süsteemid valmisid 1980-ndatel [11]. Kiiresti sai selgeks, kui kasulik on selline süsteem, kuna see vähendas kõvasti töövaeva. 1990-ndateks võeti kasutusele AFISe variante paljudes riikides [11].

AFISe töö põhineb täpsete algoritmide kasutusel ja selle peamised osad ongi pildi suurendamine, tunnuste eraldamine, indekseerimine ja vastete leidmine [10]. Pidevalt käib töö uute ja paremate algoritmide leidmiseks, et vastete täpsus oleks veelgi kõrgem. Kuna biomeetriliseks isikutuvastuseks kasutatakse tänapäeval ka teisi tunnuseid, on paljud AFISed muudetud automaatse biomeetrilise isikutuvastuse süsteemiks ehk ABISeks [11]. Eestis kasutas AFISt oma töös Kohtuekspertiisi Instituut kuni 2021. aastani, siis mindi üle ABISele [15].

Kuna sõrmejäljetuvastussüsteemide töö põhineb sellel, kuidas sõrmejälgi käsitsi tuvastatakse, tutvustatakse järgnevalt peamisi metoodikaid, mida eksperdid oma töös kasutavad.

2.3 Sõrmejäljevõrdluse metoodilised ja tehnilised alused

Sõrmejälgede võrdlusel on kasutusel kaks peamist metoodikat: ACE-V ja IEEGFI metoodika.

ACE-V metoodikat kasutatakse Ameerika Ühendriikides, Kanadas, Austraalias ja Uus-Meremaal. Selle nimi on akronüüm, mis tuleb sõnadest *analysis* (analüüs), *comparison* (võrdlemine), *evaluation* (hindamine) ja *verification* (kinnitamine) ja selle metoodika etappe saab lühidalt iseloomustada järgnevalt [10]:

- analüüs – papillaarkurdude kvantiteedi ja kvaliteedi hinnang sõrmejäljepildil
- võrdlemine – kahe pildi kõrvuti võrdlemine
- hindamine – otsus, kas saab tuvastada või välistada isiku
- kinnitamine – otsuse kinnitamine teise kompetentse eksperdi poolt.

IEEGFI metoodika on palju kasutusel Euroopa riikides ja selle töötas välja INTERPOLi sõrmejälgede tuvastamise ekspertide grupp [10]. See sarnaneb palju ACE-V metoodikale, aga peamine erinevus on see, et nõutud on sõrmejälje eritunnuste olemasolu. Sõrmejälje eritunnuste all mõistetakse peamiselt papillaarkurrulõppe ja papillaarhargmikke. ACE-V metoodika lubab isikutuvastust ka teiste tunnuste põhjal nagu kortsud, armid ja algavad harjad (ingl *incipient ridge*) [10].

Mõlema metoodika puhul on hindamise etapis kasutusel kas empiiriline või terviklik lähenemine. Empiiriline lähenemine nõuab, et identsuse tuvastamiseks oleks kahel sõrmejäljel mingi minimaalne arv samasuguseid eritunnuseid; terviklik lähenemine seob omavahel vastavuses olevate joonte kvantitatiivsete ja kvalitatiivsete omaduste hindamise [16]. Empiirilises lähenemises on tuntuim ilmselt nn 12 punkti reegel, mis pärineb dr. Locardi 1914. aasta statistilise analüüsi uuringust [17]. Selle reegli järgi saab kaks sõrmejälge tuvastada kui identsed, kui neil on vähemalt 12 samasugust iseloomulikku eritunnust. Ajalooliselt on kasutusel olnud erinevad tunnuste arvud ja rahvusvahelised standardid ühtse hindamise osas puuduvad. Ka tänapäeval on riigiti nõutud tunnuste arv erinev ning ühe riigi sees võivad eri organid kasutada erinevaid arve. 1970-ndatel asutas organisatsioon *International Association for Identification* (IAI) ekspertide komisjoni, mis leidis 1973. aastal, et kindlal tunnuste arvul ei ole otsest teaduslikku alust [16]. 1995. aastal korraldatud konverentsil kinnitati seda otsust. Seetõttu loobusid mitmed riigid kindlast standardist [16]. Tabelis 1 on välja toodud eri riikides kasutusel olevad standardid tunnuste arvule. Ülevaatlikkuse huvides on toodud ära ka riigid, kus standard puudub ehk kasutusel on terviklik lähenemine. Enamik sellistest riikidest on selle vastu võtnud IAI otsuse põhjal [16].

Tabel 1. Standardid sõrmejälgede tunnuste arvule eri riikides [16].

Riik	**Numbriline standard**
Ameerika Ühendriigid	puudub
Kanada	puudub
Ühendkuningriik	puudub
Austraalia	puudub
Itaalia	16-17
Saksamaa	8-12
Holland	10-12
Lõuna-Aafrika Vabariik	7

Venemaa	7
Lõuna-Ameerika riigid	12
Belgia, Prantsusmaa, Iisrael, Kreeka, Poola, Portugal, Rumeenia, Sloveenia, Hispaania, Türgi	12
Šveits	puudub
Soome, Rootsi, Norra, Taani, Island	puudub

Tabelist on näha, kui erinevad võivad olla nõutud sõrmejälje eritunnuste arvud. See on üks põhjuseid, miks rahvusvaheliste standardite seadmine kohtuekspertiisiteaduses on osutunud keeruliseks [16]. Kuna paljud riigid kasutavad oma praktikas eritunnuste arvu, siis võib rahvusvahelise standardi puudumine viia näiteks olukorrani, kus ühes riigis arreteeritakse ja tuvastatakse kahtlusalune 12 eritunnuse põhjal ja seejärel on vaja tema üle mõista kohut teises riigis, kus see arv on 16 [16].

Lisaks sõrmejäljele keskendub käesolev töö näokujutisele, mis on biomeetrilises isikutuvastuses samuti oluline. Järgnevalt kirjeldatakse näotuvastuse ajalugu ja seda, kuidas töötavad kaasaegsed tuvastussüsteemid.

2.4 Näotuvastuse lühiajalugu ja kaasaegsete süsteemide tööpõhimõtted

Vastavalt Andmekaitse ja infoturbe leksikonile on näotuvastus defineeritud kui „biomeetriline isikutuvastus näo individuaaltunnuste põhjal“ [1]. Esimesed katsed panna arvutit inimeste nägusid ära tundma tegi Woodrow W Bledsoe juhitud meeskond aastatel 1964-65 Californias [18]. Takeo Kanade arendas 1970-ndate alguses välja esimese automaatse näotuvastussüsteemi [19]. 1980-ndatel proovisid Sirovich ja Kirby näotuvastust teha lineaarse algebra abil [20, 21]. Turk ja Pentland jätkasid 1990-ndatel nende tööd ja see meetod sai tuntuks nimega Eigenface [22]. 2001. aastal avaldasid Jones ja Viola algoritmi, mille abil sai videol reaalajas nägusid tuvastada [23]. See oli näotuvastuse jaoks oluline areng. 2010ndatel aastatel hakati kasutama süvaõppel põhinevaid lähenemisi, mis on osutunud väga edukaks [24, 25]. Peamine põhjus on see, et kui varasemate meetodite puhul pidi õppimiseks vajalikud tunnused käsitsi sisestama, siis süvaõppe algoritmid suudavad sisendandmetest ise sellised tunnused eraldada [24].

Tänapäevased näotuvastussüsteemid kasutavad nii 2D- kui 3D-tehnoloogiat. 2D-tehnoloogia puhul antakse süsteemile ette teadaoleva isiku pilt. Süsteem mõõdab ära näo karakteristikud, mida nimetatakse sõlmpunktideks (ingl *nodal point*), nagu näiteks silmade vahekaugus ja silmakoopa sügavus [26]. Algoritmid muudavad selle informatsiooni koodiks ja see salvestatakse andmebaasis hoitavasse unikaalsesse faili, et seda saaks tulevikus uute hõivetega võrrelda [26]. Bonsor ja Johnson [27] kirjutavad, et 3D-tehnoloogia puhul on võimalik lisaks olemasoleva pildi skaneerimisele kasutada ka videolt saadud hõivet. Selle eelis on, et seda saab kasutada ka pimedas ja juhtudel, kui isiku nägu ei ole pööratud otse kaamera poole. Süsteem mõõdab ära näo unikaalsed osad nagu silmakoopa, nina ja lõua kurv ning loob biomeetrilise malli. Kui andmebaasis on ainult 3D formaadis pildid, on võrdlemine lihtne; vastasel juhul tuleb võetavale 3D formaadis pildile teha täiendav eeltöötlus, mille abil muudetakse see 2D formaadis pildiks, et seda andmebaasis olemasolevate piltidega võrrelda [27].

Peatükis tutvustati taustainfona sõrmejälje ja näotuvastuse ajalugu ning anti ülevaade levinumatest sõrmejäljevõrdluse metoodikatest. Kuna töö puudutab ABISt, selgitati ka varasemate automaatsete tuvastussüsteemide tööpõhimõtteid. Järgmises peatükis tutvustatakse lähemalt ABISt ja selle Eesti varianti.

3. Automaatse biomeetrilise isikutuvastuse süsteem ehk ABIS

Automaatse biomeetrilise isikutuvastuse süsteem ehk ABIS on andmekogu, kus on võimalik hoida erinevaid biomeetrilisi isikuandmeid, et neid kasutada isikutuvastuseks ja isikusamasuse kontrolliks [4]. Eesti ABIS loodi, et oleks tagatud selliste andmete parem kaitse, saaks tõhusamalt võidelda kuritegevuse vastu ja paremini rakendada kehtivat õigust [4]. ABISes hoitakse näokujutisi, sõrme- ja peopesajälgi. Need andmed asuvad eraldi inimeste eluloolistest andmetest (nt nimi ja isikukood), seega ei saa neid omavahel siduda, kui puudub ligipääs mõlemale andmekogule [4]. ABISe peamised kasutusalad on õiguskaitse, piirikontroll ja haldusmenetlus. ABIS kasutab oma töös tehisintellekti. See võimaldab teha nii üks-ühele võrdlust ehk isikusamasuse kontrolli ja üks-mitmele võrdlust ehk isiku identifitseerimist; mõlemal juhul teeb lõpliku otsuse alati inimene [4].

ABISe õiguslik alus biomeetriliste andmete kogumiseks põhineb Euroopa Liidu isikuandmete kaitse üldmääruse artikli 9 lõike 2 punktile g [28] (vt 4.2.1). Biomeetriliste andmete hõive oli Eestis lubatud ka enne ABISe tulekut, näiteks koguti sõrmejälgi, mida võis kasutada süütegude avastamiseks. Samuti koguti biomeetrilisi andmeid ka varem isikut tõendavate dokumentide jaoks [4].

Kõigil andmetel on teatavasti välja kujunenud teatud aeg, mil neid säilitatakse. ABISe puhul sõltub see andmete hoidmise aeg eesmärgist, milleks need on kogutud, näiteks isikutunnistuse jaoks võetud foto ja sõrmejäljekujutised säilitatakse aktiivselt 15 aastat, pärast mida need arhiveeritakse veel 50 aastaks [29].

Eestis on biomeetriliste andmete kasutamine määratletud lisaks isikuandmete kaitse üldmäärusele ka isikuandmete kaitse seadusega [30]. Selleks, et tulevikus saaks kasutusviise veelgi paremini seadusega sätestada, analüüsitakse järgnevalt seda, kuidas maailma riigid on kasutanud sõrmejälge ja näotuvastust ja seda, kuidas biomeetriliste andmete kasutamine riikides on reguleeritud.

4. Sõrmejälje ja näotuvastuse kasutamine ja selle reguleeritus maailma riikide praktikas

Selles peatükis analüüsitakse sõrmejälgede ja näotuvastuse kasutust ja biomeetriliste andmete kasutuse reguleeritust maailma riikides. Tulenevalt töö eesmärgist on regulatsiooni osas rohkem analüüsitud seda, kuidas riik biomeetrilisi andmeid võib kasutada ja töödelda, erasektoriga seotu on kohati lühidalt mainitud. Kui seaduses on sõrmejälgede ja näokujutise kasutus määratletud erinevalt, on see välja toodud.

4.1 Biomeetriliste andmete kasutamine maailma riikides

Käesolevas alapeatükis kirjeldatakse valdkondade kaupa, kuidas maailma riikides on biomeetrilisi andmeid kasutatud. Ülevaade antakse Ameerika Ühendriikide, Euroopa, Austraalia ja mõnede Aasia, Lõuna-Ameerika ning Aafrika riikide näidete varal.

4.1.1 Õiguskaitse ja avalik julgeolek

Tuntuim sõrmejälgede kasutusala on ilmselt õiguskaitse ja avalik julgeolek. Sõrmejäljepõhist tuvastust hakati kasutama kurjategijate leidmiseks 19. sajandi lõpus ja see kasutusviis on siiani kõige levinum ja tuntum; maailma riikide õiguskaitseorganite jaoks on see olnud põhiline viis, kuidas kriminaale leida [31]. Eestis näiteks kogutakse õiguskaitse raames kuritegudes kahtlustatavatelt isikutelt kõik kümme sõrmejälge [15].

Ka näotuvastust kasutatakse õiguskaitse ja avaliku julgeoleku kategoorias üha rohkem. P. Bischoff on uurinud 100 suurima rahvaarvuga riiki näotuvastustehnoloogia kasutamises. Nende andmete järgi selgus, et peaaegu 80% nende riikide valitsustest ja 70% politseijõududest kasutavad näotuvastust [32]. INTERPOL kasutab alates 2016. aastast isikutuvastuseks ja -kontrolliks globaalset näotuvastussüsteemi (INTERPOL Face Recognition System ehk IFRS); selles süsteemis on rohkem kui 179 riigilt saadud näopildid [33]. Ameerika Ühendriikides on selliseks isikutuvastussüsteemi näiteks FBI arendatud Facial Analysis, Comparison and Evaluation (FACE) Services [34]. Ühendkuningriigis kasutab politsei mõnel pool, nt Londonis, näotuvastust teatud kohtades avaliku videovalve peal, et leida tagaotsitavaid isikuid [35]. Euroopa Liidus on vähemalt 11 riigi õiguskaitseorganid kasutanud näotuvastustehnoloogiat isikute tuvastamiseks näopiltide andmebaasidest ja/või massiliseks jälgimiseks [36]. Eestis pole siiani riik õiguskaitse jaoks näotuvastust kasutanud. 2023. aasta teises pooles jõustub uus

kohtuekspertiisiseadus, mille järgi hakatakse kahtlustatavate isikute näokujutisi säilitama ABISes [15].

4.1.2 Sõjaline kategooria

Teave selle kohta, kuidas sõjaväed välisriikides opereerides biomeetriat kasutavad, on tihti salastatud. On teada, et sõrmejälgi ja näotuvastust kasutatakse Ameerika Ühendriikide armees vaenlaste, sõjavangide ja hukkunute tuvastamiseks. Lisaks saab biomeetriat kasutada ka ligipääsu kontrolliks sõjaväelistele rajatistele [37]. Andmehoiust saab näiteks tuua Ameerika Ühendriikide andmebaasi, kuhu on sõrmejälgi kogutud alates 2004. aastast ja näopilte alates 2009. aastast. Peamiselt on selles andmebaasis olevad identiteedid pärit Iraagis ja Afganistanis toimunud sõjalistest operatsioonidest [38]. NATO on samuti valmis ehitanud oma biomeetrilise andmebaasi, kus hoitakse muuhulgas näokujutisi ja sõrmejälgi. Selles süsteemis on liikmesriikidel võimalik isikutuvastuseks päringuid teha ja üksteisega informatsiooni jagada [39, 40].

Ameerika Ühendriikides võetakse sõjaväkke astujatelt kõik kümme sõrmejälge [41]. Eestis kogutakse sõrmejäljed nendelt tegevväelastelt, kes on seotud kaitseväes demineerimistöödega [29].

4.1.3 Reisimine, piirikontroll ja ränne

Reisimisel on sõrmejälgi ja näopilte võimalik kasutada biomeetrilises passis, et selle abil kiirendada isikutuvastust, samuti on sellega võimalik läbida e-väravaid. E-värav ehk automatiseeritud piirikontroll kasutab biomeetrilises passis sisalduvas mikrokiibis olevaid andmeid, et neid võrrelda inimese sõrmejälgede ja/või näopildiga [42]. Eestis on biomeetriline pass kasutusel olnud alates 2007. aastast ja see sisaldab infot nii näokujutise kui sõrmejälje kohta [43]. Rände kontrolli jaoks on paljudes riikides olemas ka vastavad taristud, mis koguvad riiki sisenejate kohta teavet. Veebisaidil Comparitech toodud reisijate andmete kasutamise uuringu järgi, mis võrdles 50 riiki, nõuab enamik neist viisataotlejatelt sõrmejälgi [44]. Ameerika Ühendriigid kasutab selleks süsteemi IDENT [5]. Euroopa Liidus on selliseks taristuks arendatav European Entry/Exit System (EES), mis registreerib kolmandatest riikidest sisenejate isikuandmeid, sh näopilte ja sõrmejälgi; eelduste kohaselt peaks süsteem tööle hakkama 2023. aasta mai lõpuks [45]. Lisaks koguti kuni aastani 2023 sõrmejälgi ka EURODAC süsteemi, mis on mõeldud asüülitaotlejate andmete hoidmiseks [46]. 2023. aastast hakati neid andmeid ABISesse koguma [29].

Julgeoleku kategoorias mainitud süsteemi IFRS on võimalik kasutada ka piirikontrollis otsingu tegemiseks [33]. Eelnevalt mainitud 100 riigi näotuvastuse uuringust selgus ka, et 60% riikidest kasutas selleks ajaks näotuvastust vähemalt mõnes lennujaamas; sellised riigid on näiteks Venemaa, Ameerika Ühendriigid, Kanada, Hiina, Austraalia ja Brasiilia [32]. Näiteks Ameerika Ühendriigid kasutas 2022. aastal näotuvastust isikukontrolliks riiki sisenemisel kõikides rahvusvahelistes lennujaamades ja riigist väljumisel 36 lennujaamas [47].

4.1.4 Tervishoid ja toetused

Enamikus maailma riikides on kasutusel isikutunnistus kodanike tuvastamiseks ja paljud riigid on sinna lisanud biomeetrilised funktsioonid. Enamasti hoitakse kaardil infot omaniku sõrmejälgede kohta. Sellist isikutunnistust on võimalik kasutada selleks, et tagada ligipääs riiklikele teenustele, nt toetustele või tervishoiule. Esimest võimalust on kasutanud Pakistan, teist näiteks Gabon ja India [48].

4.1.5 Identiteedihaldus

Valdavalt on kodanike tuvastuseks ja valijate registreerimiseks olnud kasutusel eelnevalt mainitud isikutunnistuste süsteem, mida on võimalik siduda ka olemasoleva AFISega [5]. Samas on sel eesmärgil üha rohkem riike hakanud implementeerima biomeetrilisi tuvastussüsteeme. Suurim selline süsteem on India Aadhaari projekt, kuhu on kantud u 1,3 miljardi inimese andmed, sh sõrmejäljed ja foto [49, 50]. Paljud madalama või keskmise sissetulekuga riigid on kasutanud neid süsteeme valijate registreerimiseks, nt Bolivia, Pakistan, Nigeeria ja Ghana [51]. Organisatsiooni The Collaboration on International ICT Policy for East and Southern Africa (CIPESA) koostatud raporti põhjal kogutakse 23 Aafrika riigis biomeetrilisi andmeid, peamiselt selleks, et välja anda isikutunnistusi, juhilube ja passe ning registreerida SIM-kaarte [52].

Peatükis anti ülevaade sellest, kuidas maailma riigid on kasutanud biomeetrilisi andmeid eri valdkondades. Nagu näha, on neid kasutusvõimalusi mitmeid ja võib eeldada, et tulevikus nende arv pigem kasvab.

4.2 Biomeetriliste andmete kasutuse reguleeritus maailma riikides

Peatükis analüüsitakse, kuidas maailma riikide seadusandluses on reguleeritud biomeetriliste andmete kasutus riigi tasandil. Kuna kõikide maailma riikide analüüs jääb selle töö mahu jaoks liiga suureks, on kasutust vaadeldud maailmajagude järgi.

4.2.1 Euroopa

Vastavalt Euroopa Liidus kehtivale isikuandmete kaitse üldmäärusele (General Data Protection Regulation ehk GDPR) [53] kuuluvad biomeetrilised andmed eriliigiliste isikuandmete hulka. Eriliigiliste isikuandmete töötlemine on lubatud teatud põhjustel, millest üks on andmesubjekti antud nõusolek [53]. Nõusolek peab olema antud vabalt, informeeritud ja üheselt mõistetav, samuti on andmesubjektil õigus nõusolekut igal ajal tagasi võtta [53]. Teisteks põhjusteks on teatud olukorrad, näiteks isiku eluliste huvide kaitse või andmete töötlemine kohtu poolt õigusemõistmise raames [53]. Kuna Eesti kuulub Euroopa Liitu, kehtib ka siin GDPR. Mõnedel juhtudel on Eesti riigil otsene kohustus töödelda biomeetrilisi andmeid; sellisteks juhtudeks on dokumendimenetlus, viisamenetlus, piiriületusega seotud menetlus ja varjupaiga ja rahvusvahelise kaitse menetlus [54]. Automaatse biomeetrilise isikutuvastuse süsteemi ehk ABISe põhimääruses on loetletud, kellelt võib riik biomeetrilisi andmeid koguda [29]. Ühendkuningriigis kehtib GDPR-ile sarnane seadus, mis määratleb biomeetriliste andmete töötlemist ja kasutamist [28]. Ühendkuningriigi GDPR erineb Euroopa Liidu omast ainult selle poolest, et seal arvestatakse Ühendkuningriigi kohalike seadustega.

4.2.2 Ameerika

Ameerika Ühendriikides puudub ühtne föderaalseadus, mis reguleeriks biomeetriliste andmete kogumist ja kasutamist, seega jääb see osariikide ja kohalike omavalitsuste tasandile. Kaheksas osariigis on vastu võetud seadused, mis puudutavad biomeetrilisi andmeid [55]. Samuti kehtivad mõnes osariigis ja mitmes linnas piirangud ja nõuded sellele, kuidas politsei ja/või teised valitsusagentuurid võivad näotuvastustehnoloogiat kasutada; mõnes linnas nagu San Francisco ja Oakland on see täiesti keelatud [56]. Erasektori vaates on 2021.a. seisuga 45 osariigis endiselt seaduslik teha isikust pilte ja teda selle alusel tuvastada ilma nõusolekut küsimata [57].

Enamikus Lõuna-Ameerika riikides on olemas isikuandmete kaitset puudutavad seadused ja paljude puhul on ära määratud see, millal riik võib isikuandmeid töödelda. Näiteks Brasiilias kehtiva andmekaitseseaduse järgi võib isikuandmeid, sh biomeetrilisi andmeid töödelda ainult omaniku nõusolekul ja teatud tingimustel. Sarnaselt GPDR-ile on kehtestatud erandid olukordades, kui riigil/avalikul asutusel on vaja sellised andmeid kasutada [58]. Sarnane olukord on Kolumbias ja seal on erasektorile kehtestatud kõige põhjalikumad andmekaitseseadused [59].

4.2.3 Austraalia ja Aasia

Austraalias kehtib 1988. aastast föderaalne seadus, mis puudutab isikuandmeid, sh biomeetrilisi andmeid. Selliste andmete kogumiseks peab olema tagatud indiviidi nõusolek ja andmed peavad olema piisavalt vajalikud neid koguva organisatsiooni mõne tegevuse või funktsiooni jaoks; määratud on ära olukorrad, millal riik võib biomeetrilisi andmeid kasutada [60].

Hiinas kasutab riik biomeetrilisi andmeid elanikkonna massiliseks jälgimiseks ja see tegevus pole piiratud. Samas on vastu võetud seadused, mis määravad ära selle, kuidas erasektor ja kolmandad osapooled võivad isikuandmeid, sh biomeetrilisi andmeid kasutada [57]. Indias puudub üldine seadus, mis kaitseks andmete privaatsust. 2000. aastal võeti seal vastu dokument „Information Technology Act", mis määrab ära selle, kuidas biomeetrilisi andmeid võib koguda ja töödelda [61]. Lisaks on lubatud 2019. aasta otsusega Aadhaari koodi kasutamine isikukontrolliks erasektoris [61]. 2022. aastal võeti vastu seadus, mis lubab politseil arreteeritud või ennetava kinnipidamise all viibivatelt isikutelt koguda biomeetrilisi andmeid. Avalikkuse seas on see tekitanud muret, kuna Indias puudub ühtne süsteem politsei väärkäitumise uurimiseks [62]. Jaapanis kehtib andmekaitseseadus, mis määrab selle, kuidas erasektor võib isikuandmeid, sh biomeetrilisi andmeid kasutada ja töödelda; need piirangud ei kehti samas riigile ja kohalikele omavalitsustele [63].

4.2.4 Aafrika

Aafrikas on 2022.a. seisuga 30 riiki vastu võtnud andmekaitseseadusi; üks esimesi oli Lesotho 2011. aastal [64]. Samas on CIPESA raportis toodud välja, et need seadused ei ole piisavad selleks, et kaitsta isikute privaatsust [52]. Samuti pole tihti täpselt ära määratletud järelevalve selle üle, kuidas riik biomeetrilisi andmeid võib koguda ja töödelda ja ka see, kuidas tegeleda biomeetriliste andmebaaside võimalike lekete tagajärgedega [52].

On näha, et mõnel pool suhtutakse andmekaitsesse piisavalt tõsiselt. Teisalt jälle on riike, kus selliseid seadusi pole kas veel vastu võetud või ei taga need piisaval määral andmete kaitset.

Järgmises peatükis antakse ülevaade biomeetriavõrdluse tuvastusalgoritmide peamistest mõõdikutest ja analüüsitakse kahte Ameerika Ühendriikide organisatsiooni National Institute of Standards and Technology ehk NIST raportit, millest üks puudutab sõrmejälje- ja teine näotuvastust. Analüüsi põhjal tehakse Eesti ABISe jaoks mõõdikute osas soovitusi.

5. Biomeetriavõrdluse mõõdikud ja soovitused nende osas ABISele

Siin tutvustatakse tuvastusalgoritmide täpsuse hindamiseks kasutatavaid mõõdikuid ja kahte Ameerika Ühendriikide organisatsiooni National Institute of Standards and Technology ehk NIST raportit. Esimene neist, „Fingerprint Vendor Technology Evaluation“ [65], võrdles sõrmejäljetuvastusalgoritme. Peatükkides 5.1 ja 5.2 tehakse ülevaade sellest raportist, analüüsitakse tulemusi ja tehakse ABISe jaoks soovitusi. Teine raport, „Face Recognition Vendor Test“ [66], võrdles näotuvastuse algoritme. Ülevaade raportist, tulemuste analüüs ja soovitused ABISele antakse peatükkides 5.3 kuni 5.5.

5.1 Mõõdikute tutvustus ja sõrmejäljetuvastuse raporti ülevaade

Tuvastusalgoritmid töötavad nii, et arvutavad välja sarnasusskoori kahe biomeetriku vahel. Algoritmile on ette antud teatud lävend T. Kõrgeimate skooridega biomeetrikud pannakse võimalike kandidaatide nimekirja, mille pikkus on L. Kandidaadid on järjestatud skoori alusel kõrgemast alates. See nimekiri on algoritmi väljund ja selle põhjal saab ekspert tuvastamisprotsessi jätkata ning lõpliku otsuse teha. Ekspert võib uurida kõiki L kandidaati või ainult esimest $R \leq L$ identiteeti või neid kandidaate, mille skoor on kõrgem kui T [66].

Vastavalt esimeses peatükis defineeritud mõistetele saab otsingud jagada kaheks: isikutuvastus, kus andmebaasis ei pruugi otsitavale biomeetrikule paarilist olla ja isikusamasuse kontroll, kus andmebaasis on otsitavale biomeetrikule paariline olemas. Lisaks on otsinguid võimalik jagada ka selle järgi, kas andmebaasis on otsitavale paariline olemas: raportis kasutatakse mõisteid „paarilisega otsing“ ja „paariliseta otsing“ [65].

Isikutuvastuse puhul on täpsuse tuvastamisel kasutatavad mõõdikud väärtuvastuse määr ja väärnegatiivsuse määr. NISTi raportis on väärtuvastuse määr ehk esimest tüüpi viga defineeritud kui see osa paariliseta otsingutest, kus üks või enam andmebaasis olevatest identiteetidest tagastatakse lävendiga T kas sama või kõrgema sarnasusskooriga. Väärnegatiivsuse määr ehk teist tüüpi viga on defineeritud kui see osa paarilisega otsingutest, kus otsitav paariline ei kuulu tagastatavate kandidaatide nimekirja tipu hulka või sarnasusskoor on allpool lävendit [65].

Pea kõik maailma ABISed, sh Eesti oma, on seadistatud nii, et isiku tuvastamisel tagastab süsteem etteantud arvu pikkuse kandidaatide nimekirja, kus kandidaadid on seatud skoori järgi ritta [4]. Tuvastuseks loetakse olukorda, kus otsitav paariline ületab määratud lävendi. ABISes on väärnegatiivsuse ja väärtuvastuse esinemine defineeritud olukordade järgi [4, 65]:

- otsingul on paariline olemas, aga sarnasusskoor ei ületa lävendit = väärnegatiivne
- otsingul pole paarilist ja lävendi ületab mittepaariline = väärtuvastus
- otsingul on paariline, mis ületab lävendi, lisaks ületab lävendi mittepaariline = tõene tuvastus + väärtuvastus
- otsingul on paariline, mis ei ületa lävendit, samas ületab lävendi mittepaariline = väärnegatiivne + väärtuvastus.

NISTi korraldatud uuringus kasutati andmestikes pilte, mis saadi elushõive ja tindi skaneerimise abil. Elushõive puhul kasutatakse sensorit, mis salvestab papillaarkurrud elektrilise või optilise anduri abil. Skaneeritud tindi tehnika puhul tehakse olemasolevatest paberil sõrmejälgedest digitaalsed pildid. Andmestikud olid erineva suurusega, vahemikus 10 000 kuni 5 000 000 subjekti. Neist eraldati testimise tarbeks otsinguhulgad, mille seas oli paarilisega otsinguhulk suurusega 200 000 ja paariliseta otsinguhulk suurusega 400 000. Testimisel valiti nende otsinguhulkade seast välja juhuslikult valimid suurusega vastavalt 10 000 ja 20 000 [65].

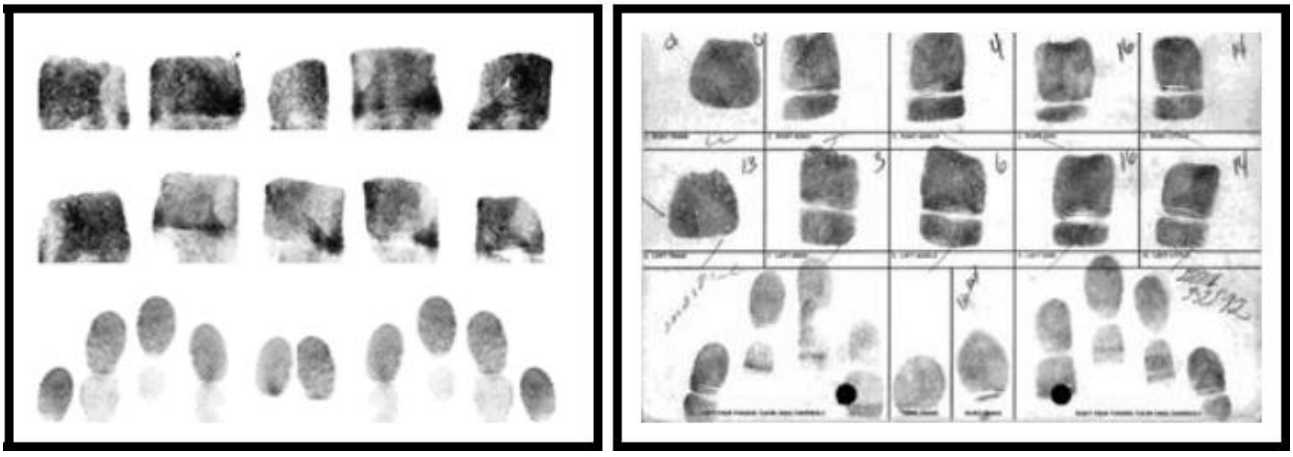
NISTi uuringus võrreldi testimisel omavahel 18 erinevat algoritmi kolmes erinevas hindamisskeemis, mis jagunesid omakorda alamklassideks. Need klassid olid [65]:

- A klass – nimetissõrmed
  - Üks tavaline nimetissõrm, mida otsiti tavaliste nimetissõrmede seast. Pildid pärinesid ühe sõrme elushõivetest.
  - Kaks tavalist nimetissõrme, mida otsiti paaride seast. Pildid pärinesid vasaku ja parema nimetissõrme elushõivetest.
- B klass – vajutatud sõrmejäljed
  - 4, 8 ja 10 sõrme vajutatud jäljed (4-4-2 põhimõttel), mida otsiti 10 sõrme komplektide seast. S.t pildil oli korraga vastav arv sõrmejälgi.
- C klass – 10 sõrme vaalitud/vajutatud
  - 10 sõrme vaalitud, otsiti vaalitud 10 sõrme piltide seast.
  - 10 sõrme vajutatud, otsiti vajutatud piltide seast. Pildid olid 4-4-1-1 põhimõttel.
  - 10 sõrme vajutatud, mida otsiti vaalitud 10 sõrme piltide seast.

Joonistel 2, 3 ja 4 on toodud näited iga klassi kohta.

Joonis 2. Näide vasaku ja parema nimetissõrme elushõivest, A klass [65].

Joonis 3. Näide vajutatud sõrmejälgede elushõivest 4-4-2 põhimõttel, B klass [65].



Joonis 4. Näide C klassist, 10 sõrme vajutatud ja vaalitud elushõive meetodil ning skaneeritud tindi meetodil [65].

Tutvustati tuvastusalgoritmides kasutatavaid mõõdikuid ja anti ülevaade raporti andmestikest ja hindamisskeemidest. Joonistega illustreeriti hindamisskeemide sõrmejälgede tüüpe. Järgnevalt võetakse kokku raporti tulemused, mille põhjal tehakse ABISele soovitusi.

5.2 Raporti tulemuste analüüs ja soovitused ABISele

NISTi raportis fikseeriti väärtuvastuse määr 10^{-3}, kuna see oli väikseim määr, mis oli uuringus kasutatud otsinguhulkade suuruste juures statistiliselt usaldusväärne. Uuriti algoritmide väärnegatiivsuse määrasid selle väärtuvastuse määra juures. Igas alamklassi testis oli kolm vooru, millest kahe viimase tulemused on uuringus ära toodud [65].

ABISe jaoks soovituste tegemisel võetakse aluseks NISTi uuringu lisas E toodud tulemused, kus otsinguajaks oli kuni 20 sekundit [65]. Põhjus on selles, et ABISes on sõrmejäljevõrdluses lubatud maksimaalne otsinguaeg kuni 20 sekundit[1].

Tulemuste põhjal on koostatud tabel 2. Selles tabelis tuuakse ära olukorrad, kus ABISt kasutatakse ja nendes rakendatavad otsingukäigud. Iga otsingukäigu juures on kirjas sõrmejälgede arv ja lubatud otsinguaeg[2]. Kuna ABISe otsingukäigud sarnanevad raportis hinnatud alamklassidega, esitatakse seejärel raporti lisast E võetud tulemused vastava sõrmede arvuga testides. Esimesena tuuakse tulemused, mis on saadud ABISe vastava otsingukäigu lubatud otsinguajaga, teisena esitatakse maksimaalse lubatud otsinguajaga (20 sekundit) saadud tulemused. Tulemused on võetud testimise kolmandast voorust. A klassi puhul tuuakse kolm parimat ja teiste klasside puhul kõik tulemused, kuna neid ei olnud enamasti rohkem kui neli. Siis esitatakse tulemuste keskmine ja uuringus tehtud tähelepanekud.

Tabelis 2 näidatud ABISe otsingukäigud, otsinguajad ja raportist võetud tulemused on isikutuvastamise (1:N otsing) puhul. Isikusamasuse kontrolli (1:1 otsing) jaoks tulemusi eraldi ei esitata, kuna see on sisuliselt isikutuvastamise alamtüüp.

Tabeli viimase otsingutüübi kohta on vaja lisada, et see puudutab süsteemi EES (vt. ptk. 4.1.3) ja kolmandate riikide kodanikke. Eestis hetkel piiril sõrmejälgi ei kontrollita.

Tabelis kasutatud termin „latentne sõrmejälg“ tähendab sõrmejälje kujutise jäljendit [1].

[1] Info on pärit juhendajalt.
[2] Info otsinguaegade kohta pärineb juhendajalt.

Tabel 2. ABISe otsingukäigud ja NISTi raporti osalised tulemused.

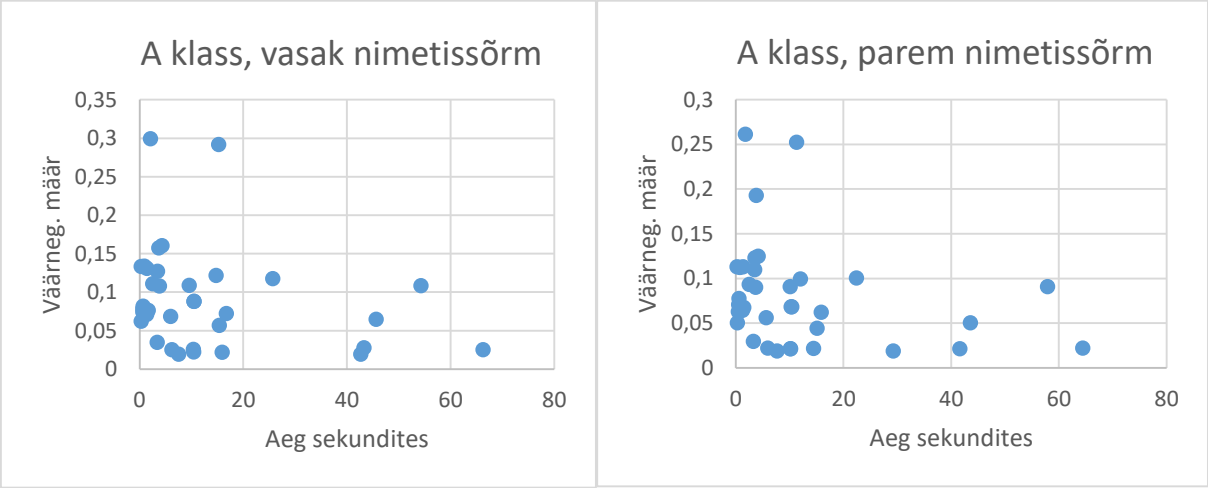
Olukord	Otsingukäigu sõrmejälgede arv, võtmise viis, lubatud otsinguaeg	Parimad tulemused lubatud otsinguajaga, valimi suurus	Parimad tulemused maksimaalse otsinguajaga	Parimate tulemuste keskmine	Uuringus tehtud tähelepanekud, mis võivad olla kasulikud
Haldusmenet-lus, viisataotlus	10, vajutatud, 10 sekundit	B klass 10 sõrme, 3 000 000: 0,0043; 0,0062	0,0031; 0,0043; 0,0062	0,00525 ja 0,0045	
Õiguskaitse	1, latentne, 20 sekundit	A klass vasak nimetissõrm, 100 000: 0,0197; 0,0222; 0,0226	Sama kui lubatud otsinguajaga	0,0215	
		A klass parem nimetissõrm, 100 000: 0,0190; 0,0214; 0,0215	Sama kui lubatud otsinguajaga	0,021	Parem nimetissõrm oli täpsem kui vasak
	10, vajutatud, 10 sekundit	C klass 10 vajutatud vs 10 vajutatud, 5 000 000: puuduvad	0,0088; 0,0102; 0,0368; 0,0711	0,0317	Üldiselt ei ol-nud vajutatud vs vajutatud ja vaalitud vs vaalitud võrdluste tulemuste

					vahel suurt erinevust
	10, vaalitud, 10 sekundit	C klass 10 vaalitud vs 10 vaalitud. 5 000 000: 0,0106;	0,0083; 0,0106; 0,0447	0,0212	
		C klass 10 vajutatud vs 10 vaalitud, 5 000 000: puuduvad	0,0129; 0,0137	0,0133	
Piirikontroll Euroopa Liidu välispiiril, tulevikus kasutatav	4, vajutatud, 3 sekundit	B klass vasaku käe 4 sõrme, 3 000 000: puuduvad	0,0259; 0,0276 0,0288	0,0274	Parema käe testis olid tulemused paremad kui vasaku käe testis
		B klass parema käe 4 sõrme, 3 000 000: puuduvad	0,0151; 0,0167; 0,0202	0,0173	

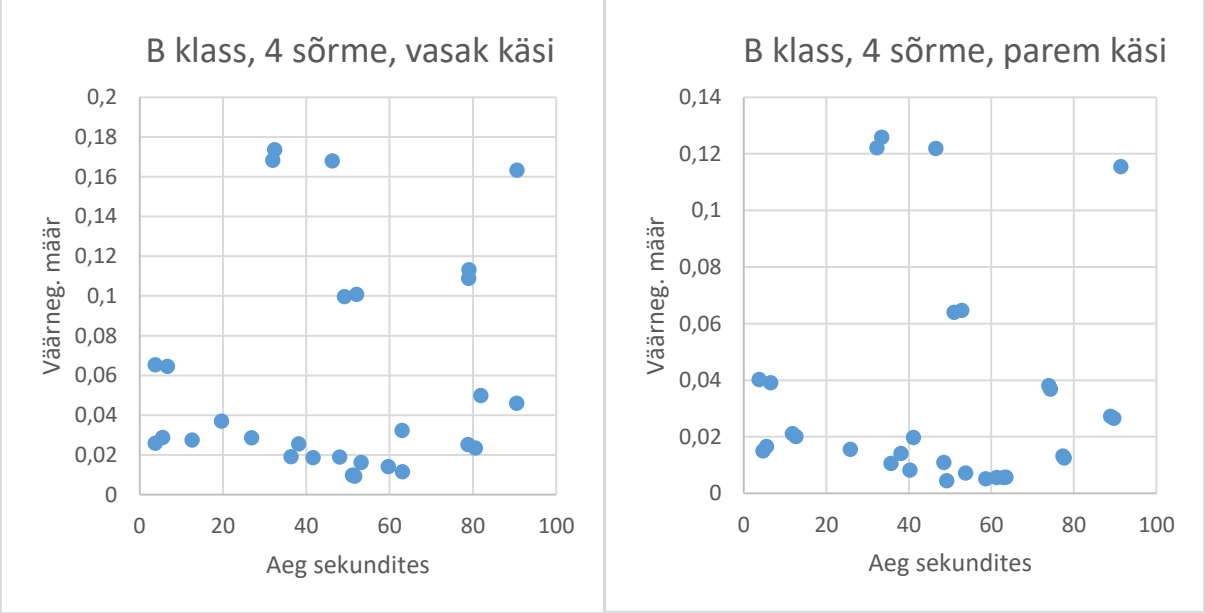
Tabelis 2 toodud keskmisi määrasid saaks ABISe kontekstis väärnegatiivsuse määra piiridena arvesse võtta siis, kui väärtuvastuse määr oleks fikseeritud 0,001 juures ja see oleks statistiliselt usaldusväärne. Nii väärtuvastuse kui väärnegatiivsuse määr sõltuvad etteantud lävendist, millega sarnasusskoore võrreldakse: kui lävendit tõsta, siis väärtuvastuse määr väheneb ja väärnegatiivsuse määr suureneb ning vastupidi.

Tabelis 2 on uuringu tulemuste lahtrites (kolmas veerg) välja toodud ka valimi suurus, mida testis kasutati. Üldiselt kehtib, et mida suurem on andmebaas, seda kauem võtab otsing aega. Tõenäoliselt jäävad ABISe andmekogud väiksemaks kui näiteks B ja C klassi valimid.

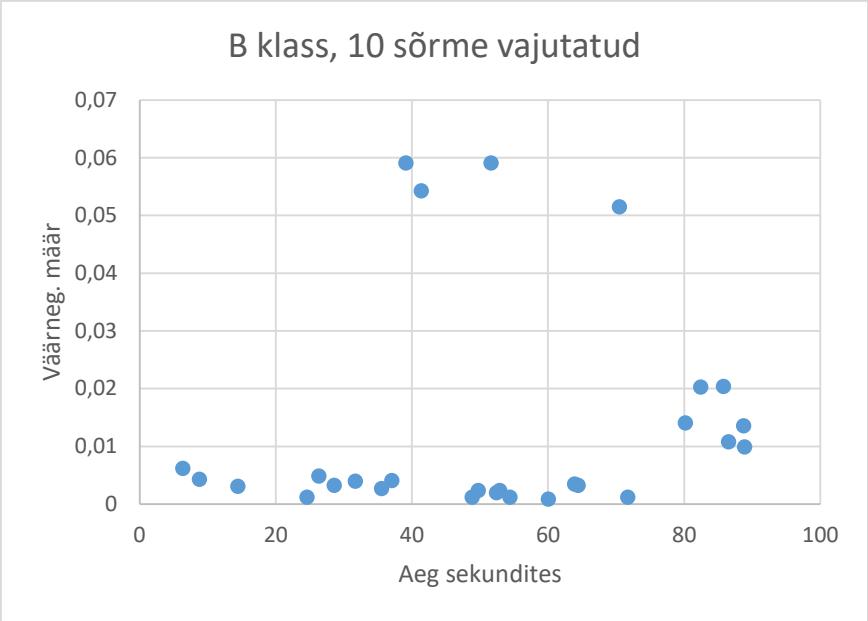
Kui otsinguaja ja väärnegatiivsuse määra vahel on seos, saaks teha oletuse, et ABISele võiks ette anda pikemaid otsinguaegu. Selle kontrolliks koostas töö autor iga tabelis 2 toodud alamklassi tulemuste jaoks graafikud, kuhu on kantud kõik uuringu lisast E võetud otsinguajad ja väärnegatiivsuse määrad. Graafikud on näidatud joonistel 5 kuni 10.



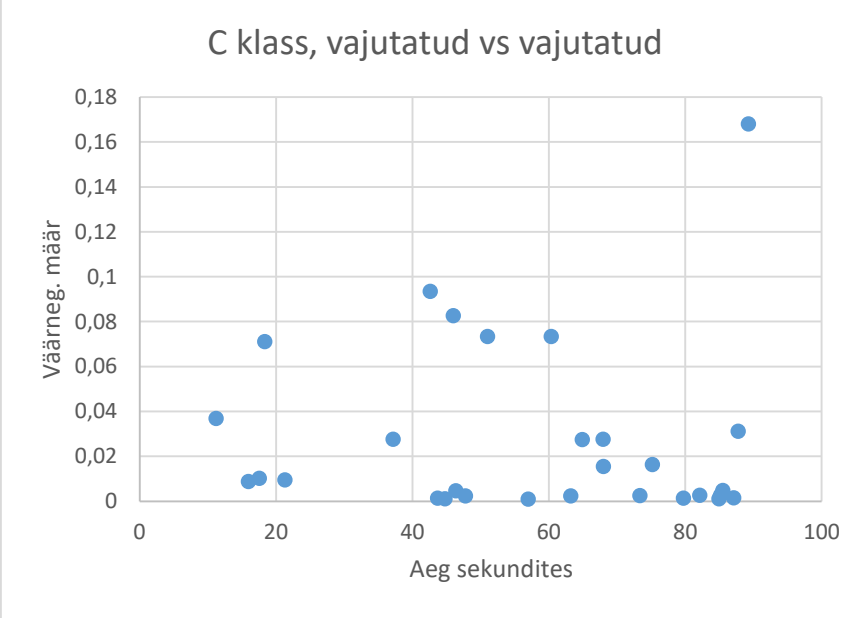
Joonis 5. Punktgraafikud A klassi stsenaariumite jaoks.



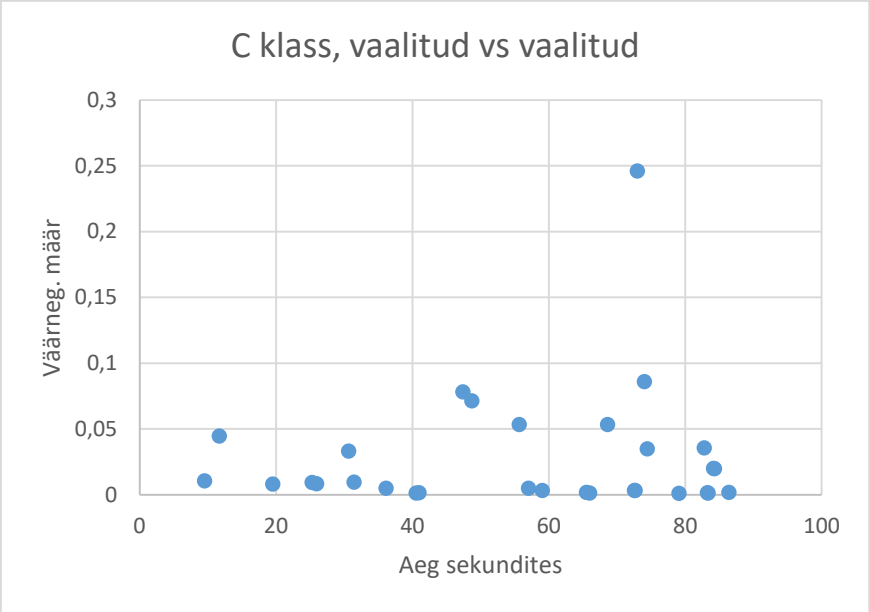
Joonis 6. Punktgraafikud B klassi jaoks, 4 sõrme.



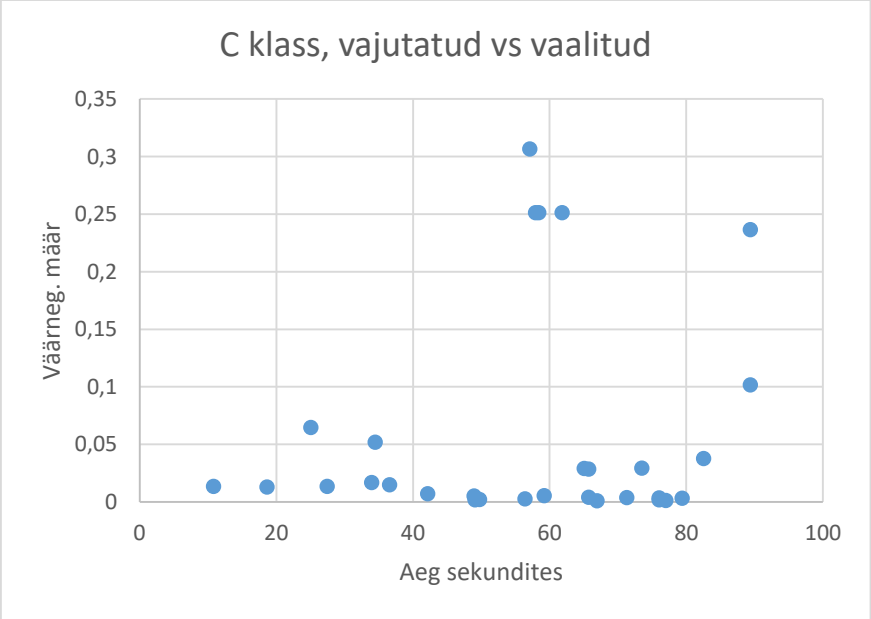
Joonis 7. Punktgraafik B klassi jaoks, 10 sõrme.



Joonis 8. Punktgraafik C klassi jaoks, vajutatud vs vajutatud.



Joonis 9. Punktgraafik C klassi jaoks, vaalitud vs vaalitud.



Joonis 10. Punktgraafik C klassi jaoks, vajutatud vs vaalitud.

Graafikute põhjal saab teha tähelepanekuid, mis võivad olla ABISe jaoks kasulikud:

- A klassis ehk ühe sõrme otsingul ei ole näha seost otsinguaja ja väärnegatiivsuse määra vahel ehk hetkel ei saa väita, et ühe latentse sõrmejälje puhul annab pikem otsinguaeg parema tulemuse.

- B klassi 4 sõrme otsingul võib täheldada, et kui otsinguaeg jääb vahemikku 35-65 sekundit, siis on väärnegatiivsuse määrad väiksemad. Trend ei ole siiski üldine. ABISe vastavas otsingukäigus võib proovida seada pikem otsinguaeg.
- B klassi 10 sõrme otsingul võib täheldada mõnevõrra madalamaid väärnegatiivsuse määrasid, kui otsinguaeg on üle 45 sekundi. Samas ei ole see langus väga suur ja selles testis on otsinguaja kuni 80 sekundit juures üldiselt madalad määrad, enamasti alla 0,005. ABISe vastavas otsingukäigus (viisataotluse olukord) võib vajadusel otsinguaega pikendada.
- C klassis ei ole esimese otsingut puhul näha seost pikema otsinguaja ja madalama väärnegatiivsuse määra vahel, madalamate (alla 0,01) ja kõrgemate tulemustega algoritme on umbes võrdsel määral. Kahe teise otsingukäigu puhul on tulemused sarnased. Siiski võib ära märkida, et otsinguaja > 40 sekundit juures võis kõigis kolmes testis näha madalamaid määrasid. ABISe vastavates otsingukäikudes (õiguskaitse) võib proovida otsinguaegu pikendada.

Kokkuvõtvalt saab öelda, et ABISe jaoks ei ole ainult sellise uuringu põhjal võimalik väärnegatiivsuse määrade osas numbrilisi soovitusi anda, kuna need määrad on seotud kasutatava algoritmi, lävendite ja sellega, millisena fikseeritakse väärtuvastuse määrad. Samuti kehtib sellistes süsteemides üldiselt, et lävend sõltub olukorrast, kus otsingut teostatakse. Mõnel juhul on madalam väärtuvastuse määr olulisem kui teisel [67]. Siiski sai teha tähelepanekuid ja soovitusi, mida on võimalik ABISes kasutada.

5.3 Näotuvastuse uuringu raporti ülevaade

Näotuvastusalgoritme võrrelnud raportis kasutati testimiseks järgnevaid piltide tüüpe [66]:

- Õiguskaitse (ingl *law enforcement* ehk LEO) andmebaas:
    - Arestipildid (ingl *mugshots*): u 86% LEO andmebaasist. Need vastavad piisaval määral ANSI/NIST ITL 1-2011 standardile, peamine erinevus on otsevaatelise poosi kerge varieeruvus. Pildid erinevad suuruselt, enamasti on see 480x600 pikslit. Kasutatud on JPEG tihendust, saadud failisuurused on 18 kuni 36KB. Paljude piltide puhul on tulemuseks teistsugused failisuurused, mis viitab sellele, et ühe värvipiksli kohta on kodeeritud umbes 1,25 bitti.
    - Veebikaamera pildid: 14% LEO andmebaasist; suurus on 240x240 pikslit, mis ei vasta enamikele näotuvastusega seotud standarditele. Peamised defektid olid mitte otsevaateline poos, madal kontrast ja halb resolutsioon. JPEG tihendus oli

liiga suur, mis tähendas seda, et ühe värvipiksli kohta on kodeeritud 0,5 kuni 1 bitti.

- Viisapildid. Need on standarditele vastavad. Osal piltidest on siiski väiksem optiline resolutsioon, kuna nad on skaneeritud paberfotodelt. Lisaks on piltide tihendatud suurus 9,2KB ja neid iseloomustab ka madal silmade vaheline kaugus ehk IOD (ingl lühend sõnadest *interocular distance*), 67 pikslit. See on allapoole ISO/IEC 19794-5:2005 standardis määratud miinimumide (120 pikslit IOD, failisuurus 15KB, pildisuurus 480x460 pikslit).
- Sketšid (selle andmehulga testitulemusi käesolevas töös ei analüüsita).

Raporti järgi võib tihti ette tulla, et ühelt isikult kogutakse ja liikmestatakse[3] biomeetrilisi andmeid rohkem kui ühel korral, nt dokumentide uuesti väljastamisel [66].

Liikmestuse saab jagada kaheks [66]:

- Hiljutine – liikmestatakse ainult teine kõige uuem pilt
- Eluaegne – liikmestatakse kõik pildid, v.a. viimane.

Varasemas, 2010. aasta NISTi raportis leiti, et täpsus paraneb, kui kasutada ühe isiku kõiki pilte [68]. Seetõttu oli töös analüüsitava raporti API dokumendis antud liikmestuse tarkvarale isikust $K \geq 1$ pilti ja tarkvara pidi tegema nende piltide põhjal ühe malli. Testis oli mall see, millega otsitavat pilti võrreldi. Läbiviidud uuringus oli kõikidel juhtudel kõige uuem pilt see, millega otsingut teostati [66].

Hindamisskeemid olid järgmised [66]:

- Arestipiltide otsing LEO andmebaasist, paariliseta ja paarilisega
- Veebikaamera piltide otsing LEO andmebaasist, paariliseta ja paarilisega
- Viisapiltide otsing viisapiltide andmebaasist, paariliseta ja paarilisega.

Testides kasutati hiljutist ja eluaegset liikmestust ja andmehulki suurustega 20 000, 160 000, 640 000 ja 1 600 000 isikut. Hiljutise liikmestuse puhul oli piltide arv võrdne isikute arvuga. Eluaegse liikmestuse puhul olid piltide arvud vastavalt andmehulkadele: 32948, 225585, 856934, 2117750.

[3] Liikmestamine tähendab biomeetriahõivesubjekti biomeetrialiikmekirje loomist ja salvestamist [1].

Otsinguks kasutati kahte paariliseta valimit. Esimene neist oli suurusega 10660 pilti ja sisaldas veebikaamera pilte, teine sisaldas arestipilte, suurus oli 171066 pilti.

NISTi uuringus osalesid 16 näotuvastusalgoritmide tootjat, kes võisid esitada maksimaalselt 7 algoritmi. Testimisel oli raportis ära toodud kuni 42 algoritmi tulemus, see arv esines 160 000 isiku suuruse andmehulga juures. Tulemustest selgus, et ühe tootja algoritmid saavutasid pigem sarnaseid tulemusi ja tootjate vahelised tulemused erinesid omavahel rohkem.

Raportis tuuakse välja näotuvastussüsteemide kaks töörežiimi: ühes on madal lävend, mis nõuab eksperdi tööd, et valepositiivseid vasteid välja praakida; teises on kõrge lävend, mis ei nõua nii suurt sekkumist. Sel puhul on madala väärtuvastuse määraga kaasnev kõrgem väär-negatiivsuse määr [66].

5.4 Näotuvastuse raporti tulemuste analüüs

Eestis hakatakse arestipilte tegema 2023. aasta teises pooles [15]. Hetkel veel ABISes näotuvastust ei rakendata, aga algoritmile, mida kasutama hakatakse, on ette antud maksimaalne otsinguaeg 10 sekundit[4]. Tulevikus plaanitakse kasutada näotuvastust õiguskaitse- ja haldusmenetlustes.

ABISesse kantavad ametlikud fotod peavad vastama ISO/IEC 29794-5 standardile [69]. Näiteks kontrollitakse standardile vastavust ka internetis tehtud dokumenditaotlusel üles laetavate fotode puhul.

Uuringu hindamisskeemide tulemuste põhjal koostati tabelid 3, 4 ja 5, millest lähtudes tehakse tähelepanekuid, mis võiksid olla ABISe jaoks kasulikud.

Tabelis 3 (koostatud raporti tabelite nr 4, 5 ja 6 põhjal) esitatakse raportis saadud väärnegatiivsuse määrad testis, kus LEO andmebaasist otsiti arestipilte, hiljutise ja eluaegse liikmestuse juures. Esitatakse 10 parimat tulemust, mis on saadud otsinguaja kuni 10 sekundit juures. Tulemused on toodud kahe erineva väärtuvastuse määra kohta. Esimene neist on väärtusega 0,002, mida võiks eeldatavasti kasutada rakenduses või ABISe puhul režiimis, kus on kõrge lävend ja ekspert ei vaata tulemusi üle. Teine neist on väärtusega 0,02, mida võidakse kasutada rakenduses/režiimis, kus puudub lävend ja ekspert vaatab kandidaadid üle. Tabelis on toodud ära need tulemused, mis on saadud kandidaatide nimekirja pikkusega 10 puhul, kuna see on tõenäoliselt kõige lähedasem ABISes tagastatavate vastete arvule.

[4] Info on pärit juhendajalt.

Tabel 3. Arestipiltide testide parimad tulemused ja nende keskmised [66].

Andmevalimi suurus	Eluaegne liikmestus, kõrge lävend, väärtuv. määr = 0,002	Eluaegne liikmestus, lävend puudub, väärtuv. määr = 0,02	Eluaegne liikmestus, lävend puudub, vastete arv = 10	Hiljutine liikmestus, lävend puudub, väärtuv. määr = 0,02
160 000	0,052; 0,054; 0,066; 0,073; 0,122; 0,122; 0,128; 0,142; 0,144; 0,171; keskmine: 0,107	0,040; 0,042; 0,048; 0,052; 0,091; 0,094; 0,095; 0,095; 0,100; 0,114; keskmine: 0,077	0,022; 0,023; 0,023; 0,023; 0,043; 0,044; 0,046; 0,048; 0,048; 0,048; keskmine: 0,0368	0,047; 0,047; 0,057; 0,060; 0,106; 0,106; 0,107; 0,109; 0,114; 0,133; keskmine: 0,0886
640 000	0,059; 0,062; 0,076; 0,090; 0,127; 0,129; 0,131; 0,153; 0,156; 0,208; keskmine: 0,119	0,044; 0,046; 0,057; 0,062; 0,096; 0,100; 0,101; 0,101; 0,106; 0,135; keskmine: 0,085	0,024; 0,026; 0,027; 0,027; 0,053; 0,053; 0,055; 0,055; 0,056; 0,056; keskmine: 0,043	0,053; 0,053; 0,067; 0,074; 0,112; 0,114; 0,115; 0,116; 0,119; 0,159; keskmine: 0,098
1 600 000	0,068; 0,070; 0,089; 0,105; 0,134; 0,136; 0,137; 0,161; 0,167; 0,231; keskmine: 0,1298	0,049; 0,050; 0,064; 0,071; 0,102; 0,104; 0,107; 0,107; 0,111; 0,153; keskmine: 0,092	0,026; 0,029; 0,030; 0,030; 0,059; 0,061; 0,063; 0,063; 0,063; 0,063; keskmine: 0,049	0,057; 0,058; 0,075; 0,084; 0,119; 0,120; 0,121; 0,123; 0,124; 0,179; keskmine: 0,106

Tabelis arvutatud keskmiste tulemuste põhjal on näha, et kõrge lävendi seadmisel, kus väärtuvastuse määr on madal, on väärnegatiivsuse määrad minimaalselt 0,1. Kui lävendit mitte rakendada ja kasutada kandidaatide nimekirja pikkusega 10, siis on keskmised määrad vähemalt 0,07 võrra väiksemad. Võrreldes eluaegse liikmestuse (kus kõikidest piltidest tehti kokku üks mall) ja hiljutise liikmestuse määrasid, on näha, et eluaegse liikmestuse korral olid keskmised väärnegatiivsuse määrad madalamad.

Peab küll arvestama, et parimad tulemused on pärit kuni kolmelt näotuvastusalgoritmide tootjalt. Seetõttu oletatakse, et ABISes kasutatav algoritm on omadustelt rohkem nende sarnane.

Tabelis 4 tuuakse ära tulemused selle kohta, kui LEO andmebaasist otsiti veebikaamera pilte, hiljutise ja eluaegse liikmestuse juures. Tulemused on võetud raporti tabelitest 4, 5, 6, 10 ja 11. Hiljutise liikmestuse kohta on välja toodud tulemused, mis on saadud väärtuvastuse määra 0,02 juures ja tulemused juhul kui määrata tagastatavate vastete arvuks 1. Eluaegse liikmestuse kohta on välja toodud tulemused juhtudel, kus tagastatavate vastete arvuks on 1 või 50. Eluaegse liikmestuse kohta käivas raporti tabelis pole eraldi väärtuvastuse määra välja toodud, aga võib oletada, et see on fikseeritud 0,02 juures.

Raportis olevas eluaegse liikmestuse tulemuste tabelites puuduvad keskmised otsinguajad. Sellest hoolimata otsustati tulemused siin esitada, kuna uuringu tabelites, kus otsinguajad olid näidatud, jäid need peaaegu alati alla 10 sekundi. Alles valimi suuruse 1 600 000 korral võisid need suuremaks kasvada.

Tabel 4. Veebikaamera piltide testide tulemused ja nende keskmised [66].

Andmevalimi suurus	Eluaegne liikmestus, lävend puudub, vastete arv = 1	Eluaegne liikmestus, lävend puudub, vastete arv = 50	Hiljutine liikmestus, lävend puudub, väärtuv. määr = 0,02	Hiljutine liikmestus, lävend puudub, vastete arv = 1
160 000	0,077; 0,077; 0,079; 0,079; 0,173; 0,174; 0,194; 0,199; 0,239; 0,240; keskmine: 0,153	0,032; 0,032; 0,032; 0,039; 0,066; 0,067; 0,08; 0,08; 0,107; 0,121; keskmine: 0,0656	0,135; 0,136; 0,145; 0,169; 0,305; 0,314; 0,339; 0,347; 0,369; 0,369; keskmine: 0,2628	0,081; 0,081; 0,082; 0,084; 0,181; 0,184; 0,203; 0,207; 0,25; 0,252; keskmine: 0,1605
640 000	0,094; 0,094; 0,095; 0,097; 0,204; 0,207; 0,231; 0,237; 0,267; 0,273;	0,042; 0,042; 0,043; 0,05; 0,094; 0,096; 0,11; 0,111; 0,134; 0,151;	0,157; 0,160; 0,173; 0,204; 0,352; 0,359; 0,389; 0,391; 0,397; 0,400;	0,098; 0,100; 0,100; 0,100; 0,214; 0,219; 0,241; 0,247; 0,278; 0,282;

	keskmine: 0,1799	keskmine: 0,0873	keskmine: 0,2982	keskmine: 0,1879
1 600 000	0,106; 0,108; 0,108; 0,108; 0,229; 0,229; 0,253; 0,265; 0,287; 0,290; keskmine: 0,1983	0,048; 0,049; 0,049; 0,058; 0,117; 0,117; 0,135; 0,135; 0,16; 0,174; keskmine: 0,1042	0,176; 0,176; 0,192; 0,229; 0,382; 0,394; 0,408; 0,418; 0,418; 0,422; keskmine: 0,3215	0,113; 0,113; 0,115; 0,115; 0,237; 0,246; 0,270; 0,274; 0,298; 0,302; keskmine: 0,2083

Tabeli põhjal on näha, et kui eluaegse liikmestuse stsenaariumis seada tagastatavate vastete arv suuremaks, siis on väärnegatiivsuse määr madalam, seda kõikide valimisuuruste juures. Võrreldes eluaegset ja hiljutist liikmestust, kui tagastatakse üks vaste, on ka siin näha, et eluaegse liikmestuse juures on määrad madalamad. Vahe ei ole küll märgatavalt suur ja üleüldiselt võib teha tähelepaneku, et nende testide väärnegatiivsuse määrad on küllaltki kõrged. See on eelkõige seotud ebastandardsete piltidega.

Viisapiltide uuringus oli ainult üks stsenaarium: hiljutine liikmestus ja üks valimisuurus, 20 000. Tabelis 5 on näha tulemused kahe juhu jaoks: tagastatavate vastete arv 1 ja 50, väärtuvastuse määr on eeldatavasti fikseeritud 0,02 juures. Tabeli 4 juures otsinguaja kohta tehtud märkused kehtivad ka siin. Tabel on koostatud raporti tabelite 10 ja 11 põhjal.

Tabel 5. Viisapiltide testi tulemused ja keskmised [66].

Andmevalimi suurus	Hiljutine liikmestus, lävend puudub, vastete arv = 1	Hiljutine liikmestus, lävend puudub, vastete arv = 50
20 000	0,023; 0,017; 0,026; 0,026; 0,061; 0,062; 0,064; 0,064; 0,066; 0,082; keskmine: 0,0491	0,006; 0,007; 0,007; 0,007; 0,019; 0,019; 0,020; 0,020; 0,020; 0,020; keskmine: 0,0145

Tabelist 5 on näha, et suurema tagastatavate vastete arvu puhul on väärnegatiivsuse määr madalam. See on sarnane eelnevate tabelite vastavate tulemustega.

5.5 Soovitused ABISele

NISTi uuringus tehti tulemuste põhjal mitmeid tähelepanekuid, mis tuuakse siin kokkuvõtvalt ära, kuna nad võiksid olla ABISe jaoks kasulikud. Tähelepanekud ja soovitused on järgnevad [66]:

- Paarilisega otsingu väärnegatiivsuse määrad kasvavad koos liikmestatud subjektide arvu kasvuga. Kui rakendada kõrget lävendit, et väärtuvastuse määr oleks madal, siis väheneb väärnegatiivsuse määra tundlikkus andmebaasi suuruse suhtes.
- Veebikaamera pildid olid teatavasti ebastandardsed ja nende otsingu tulemused olid seetõttu kõige halvemad. Siiski selgus, et halvim tulemus saadi siis, kui otsiti veebikaamera pilti arestipiltide seast, mitte siis, kui otsiti veebikaamera pilti veebikaamera piltide seast. Põhjusena toodi välja, et tuvastustäpsus on parem, kui mõlemad pildid on kas otsevaates või pole kumbki otsevaates. Sellest lähtuvalt saab soovitada, et ABISes peaks tulevikus seda arvesse võtma.
- Režiimis, kus lävendit ei rakendata ja ekspert vaatab tulemusi üle, on väärnegatiivsuse määrade vahel märgatav erinevus sõltuvalt sellest, kas tagastatakse 1 vaste või 50 vastet. Raportis selgus näiteks, et ühe algoritmi puhul kahanes see määr lausa kaks korda. Samas toodi välja, et paremad algoritmid asetasid õige paarilise esimesele kohale suurema sagedusega ja seetõttu oli neil ka väiksem väärnegatiivsuse määra kahanemine. Sellest tulenevalt tehti tähelepanek, et ei ole mõtet väga pikki nimekirju kontrollida. Ka see on soovitus ABISe jaoks.
- Selgus, et väärtuvastuse määr sõltub andmebaasi subjektide arvust kahel viisil: osadel algoritmidel oli lineaarne sõltuvus, teistel jäi see määr peaaegu konstantseks. Sellest tulenevalt rõhutati raportis, et süsteemide puhul, kus kasutatakse nullist suuremaid lävendeid, on tähtis aru saada väärtuvastuse määra sõltuvusest andmebaasi suurusest. Eesmärk oleks saavutada ennustatav väärtuvastuse määr.
- Mida rohkem identiteete süsteemi lisatakse, seda suuremaks muutub väärtuvastuse võimalus. Samas olid uuringus need muutused siiski piisavalt väikesed ja seal järeldati, et näotuvastussüsteemid saavad olla kasulikud riiklikes andmebaasides, kuhu on kantud kogu rahvastiku andmed.
- Viisapiltide otsingu testis selgus, et mida vanem on inimene, seda täpsem on tuvastus: lihtsam on inimesi eristada ja ka isikusamasust kontrollida. Toodi välja, et väikelaste ja eelteismeliste (uuringus kuni 13 aasta vanune isik) puhul olid väärnegatiivsuse väga

kõrged. Siit ka soovitus, et ABISes tuleks sellega arvestada. Võimalusel peaks eristama vanusegruppe ja vastavalt rakendama erinevaid lävendeid.

- Raportis toodi välja kõikide vanemate piltide liikmestuse efekt: see parandas üldiselt tuvastustäpsust. Seal soovitati, et süsteeme peaks disainima nii, et säilitatakse ja liikmestatakse isiku kõik pildid. Pole aga selge, kui vana peaks olema pilt, et seda süsteemist eemaldada. See vajaks edasisi uuringuid (uuring peaks kvantifitseerima väärtuvastuse määra seoses liiga paljude piltide olemasoluga).
- Uuringus rõhutati, et näotuvastuse parandamisel on oluline jälgida võrdlusalusena kasutatava pildi kõrget kvaliteeti olukorras, kus ekspert kandidaate üle vaatab. Pildil peaks olema silmade vaheline kaugus umbes 800 pikslit. Selliseid pilte ei kasutata otse algoritmides, seega on soovitav need pildid koguda ja ümber töödelda vastavalt ISO standardile (IOD 120 pikslit) automaatse näotuvastuse tarvis. Soovitus on seda tähelepanekut ABISe vastavas režiimis rakendada.

Peatükkides 5.3 kuni 5.5 anti ülevaade NISTi näotuvastuse algoritmide võrdluse raportist ja analüüsiti tulemusi. Üldiselt saab järeldada, et väärnegatiivsuse määrad sõltuvad näotuvastuses küllaltki palju konkreetsest algoritmist ja sellest, kuivõrd pildid vastavad kehtestatud standarditele. Seetõttu pole ka siin võimalik ABISele konkreetseid numbrilisi soovitusi teha. Siiski sai uuringu tulemuste ja seal tehtud tähelepanekute põhjal teha järeldusi ja ettepanekuid, mida ABISes tulevikus saaks kasutada.

Kokkuvõte

Töö eesmärk oli analüüsida biomeetriliste andmete kasutust ja kasutuse reguleeritust maailma riikides ja anda Eesti automaatse biomeetrilise isikutuvastuse süsteemi ehk ABISe jaoks soovitusi, mida saaks tuvastusalgoritmidele lävendite seadmisel arvesse võtta. Andmete kasutuse ülevaatest tuli välja, millistel eesmärkidel on seni neid andmeid kasutatud ja millised on võimalikud tulevikusuunad. Biomeetriliste andmete kasutuse reguleerituse osas selgus, et kohati on andmekaitse hästi paika pandud, teisalt jälle on riike, kus sellised seadused on puudulikud või pea olematud.

Biomeetriavõrdluse mõõdikud, millega tuvastusalgoritmide täpsust hinnatakse, sõltuvad lävendist. ABISele soovitamise aluseks võetud raportite tulemuste analüüsist selgus, et ei ole piisavalt empiirilist alust selleks, et teha numbrilisi soovitusi lävendite ja mõõdikute osas. Need lävendid ja mõõdikud sõltuvad süsteemi ehitusest, kasutatavast algoritmist, andmebaasi suurusest ja olukorrast, kus otsingut tehakse. Siiski sai teha tähelepanekuid ja soovitusi nii sõrmejälje- kui näotuvastuse osas, mida saaks süsteemis kasutada. Sõrmejäljetuvastuse osas olid soovitused peamiselt seotud otsinguaegade võimaliku muutmisega. Näotuvastuse osas puudutasid need andmebaasis hoitavate piltide arvu ja standarditele vastavust ja otsingul tagastatavate vastete nimekirja pikkust.

Teema vajab veel kindlasti uurimist. Organisatsioonil National Institute of Standards and Technology on käimas järjepidevad uuringud nii sõrmejälje kui näotuvastuse võrdluse osas ja nende põhjal valmivad tulevikus uued raportid. Kuigi ABIS on selleks ajaks täies mahus kasutusel, saaks tulevikus neid raporteid standardite võimalikuks hindamiseks ja ehk ka parandamiseks analüüsida.

Viidatud kirjandus

[1] Cybernetica AS. Andmekaitse ja infoturbe leksikon. https://akit.cyber.ee

[2] Goode A. Biometric identification or biometric authentication?. 2018. https://veridiumid.com/biometric-identification-and-biometric-authentication/ (19.11.2022)

[3] Ghorbani M., Alizadeh M., Omran A. E., Asem M. M. An Investigative Review of Human Authentication Based on Fingerprint. *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 2018, 1359-1366. https://doi.org/10.1109/IEMCON.2018.8614910.

[4] Siseministeerium. Automaatse biomeetrilise isikutuvastuse süsteemi andmekogu ABIS. https://www.siseministeerium.ee/abis (04.12.2022)

[5] Thales. Biometrics: definition, use cases, latest news. 2022. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics (19.11.2022)

[6] Eesti Keele Instituut. Eesti keele seletav sõnaraamat. https://www.eki.ee/dict/ekss

[7] Lee H. C., Gaensslen R. E., Eds. Advances in Fingerprint Technology. New York: Elsevier. 1991.

[8] Cummins H., Midlo C. Finger Prints, Palms and Soles. New York: Dover. 1961.

[9] Jain A. K., Lin Hong, Pankanti S., Bolle R. An identity-authentication system using fingerprints. *Proceedings of the IEEE*, 1997, vol. 85, no. 9, 1365-1388. https://doi.org/10.1109/5.628674.

[10] Holder E. H., Robinson L. O., Laub J. H. The fingerprint sourcebook. U.S. Dept. of Justice, Office of Justice Programs, National Institute of Justice. 2011.

[11] Thales. Automated Fingerprint Identification System (AFIS) overview - A short history. 2022. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/afis-history (05.12.2022)

[12] Henry E. R. Classification and uses of finger prints. HM Stationery Office [printed by Harrison and sons, Limited]. 1922.

[13] Davis A. 8 most common fingerprint patterns. 2017. https://www.touchngoid.com/8-common-fingerprint-patterns/ (24.11.2022)

[14] Aguilar G., Sanchez G., Toscano K., Salinas M., Nakano M., Perez H. Fingerprint Recognition. *Second International Conference on Internet Monitoring and Protection (ICIMP 2007)*, 2007, 32-32. https://doi.org/10.1109/ICIMP.2007.18.

[15] Kohtuekspertiisiseadus. - RT I, 03.02.2023, 1. https://www.riigiteataja.ee/akt/103022023001 (14.04.2023)

[16] Champod C., Lennard C. J., Margot P., Stoilovic, M. Fingerprints and Other Ridge Skin Impressions. Boca Raton, CRC Press. 2004. https://doi.org/10.1201/9780203485040.

[17] Kingston C. R., Kirk P. L. Historical development and evaluation of the "12 point rule" in fingerprint identification. School of Criminology. University of California, Berkeley, United States.

[18] Norman J. Woodrow Bledsoe Originates of Automated Facial Recognition. https://www.historyofinformation.com/detail.php?entryid=2495 (16.04.2023)

[19] Kanade T. Picture Processing System by Computer Complex and Recognition of Human Faces. Doctoral dissertation, Department of Information Science, Kyoto University. 1973.

[20] Sirovich L., Kirby M. Low-dimensional procedure for the characterization of human faces. *Journal of the Optical Society of America A*, 1987, vol. 4, 519-524. https://doi.org/10.1364/JOSAA.4.000519.

[21] Kirby M., Sirovich L. Application of the Karhunen-Loeve procedure for the characterization of human faces. *IEEE Trans. Pattern Analysis and Machine Intelligence*, 1990, vol. 12, 103-108. https://doi.org/10.1109/34.41390.

[22] Turk M., Pentland A. Eigenfaces for recognition. *Journal of cognitive neuroscience*, 1991, vol. 3, 71-86. https://doi.org/10.1162/jocn.1991.3.1.71.

[23] Viola P., Jones M. J. Robust Real-Time Face Detection. *International Journal of Computer Vision*, 2004, vol. 57, 137–154. https://doi.org/10.1023/B:VISI.0000013087.49260.fb.

[24] Campillo R. Facial Recognition History. 2020. https://www.mobbeel.com/en/blog/facial-recognition-history/ (16.01.2023)

[25] Galbally J., Ferrara P., Haraksim R., Psyllos A., Beslay L. Study on Face Identification Technology for its Implementation in the Schengen Information System. EUR 29808 EN, Publication Office of the European Union, Luxemburg, 2019. https://doi.org/10.2760/661464.

[26] Frederick B. Facial Recognition. 2022. https://www.techopedia.com/definition/32071/facial-recognition (16.01.2023)

[27] Bonsor K., Johnson R. How Facial Recognition Systems Work. https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm (17.01.2023)

[28] Information Commissioner's Office. Guide to the UK General Data Protection Regulation (UK GDPR). https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ (23.01.2023)

[29] Automaatse biomeetrilise isikutuvastuse süsteemi andmekogu põhimäärus. - RT I, 21.12.2022, 18. https://www.riigiteataja.ee/akt/131122021018?leiaKehtiv (04.05.2023)

[30] Isikuandmete kaitse seadus. - RT I, 04.01.2019, 11. https://www.riigiteataja.ee/akt/104012019011 (29.04.2023)

[31] Ashbaugh D. R. Ridgeology. http://onin.com/fp/ridgeology.pdf (24.11.2022)

[32] Bischoff P. Facial recognition technology (FRT): 100 countries analyzed. 2021. https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/ (22.01.2023)

[33] INTERPOL. Facial Recognition. https://www.interpol.int/How-we-work/Forensics/Facial-Recognition (20.01.2023)

[34] Brandom R. Most US government agencies are using facial recognition. 2021. https://www.theverge.com/2021/8/25/22641216/facial-recognition-gao-report-agency-dhs-cbp-fbi (05.05.2023)

[35] Metropolitan Police. Facial Recognition. https://www.met.police.uk/advice/advice-and-information/fr/facial-recognition/ (20.01.2023)

[36] Kayser-Bril N. At least 11 police forces use face recognition in the EU, AlgorithmWatch reveals. 2020. https://algorithmwatch.org/en/face-recognition-police-europe/ (20.01.2023)

[37] Zwanenburg M. Know Thy Enemy: The Use of Biometrics in Military Operations and International Humanitarian Law. *International Law Studies*, 2021, vol. 97, 1405-1431.

[38] Gershgorn D. EXCLUSIVE: This Is How the U.S. Military's Massive Facial Recognition System Works. 2019. https://onezero.medium.com/exclusive-this-is-how-the-u-s-militarys-massive-facial-recognition-system-works-bb764291b96d (24.11.2022)

[39] Monroy M. NATO establishes biometric database, US military has it already. 2019. https://digit.site36.net/2019/11/08/nato-establishes-biometric-database-us-military-has-it-already/ (20.04.2023)

[40] NATO Communications and Information Agency. Countering terrorism: NATO Agency aids in the development of biometrics capabilities. https://www.ncia.nato.int/about-us/newsroom/countering-terrorism-nato-agency-aids-in-the-development-of-biometrics-capabilities.html (20.042023)

[41] Today's Military. Enlisting in the Military. https://www.todaysmilitary.com/joining-eligibility/enlisting-military (17.04.2023)

[42] Negri N. A. R., Borillea G. M. R., Falcãob V. A. Acceptance of biometric technology in airport check-in. *Journal of Air Transport Management*, 2019, Volume 81, 101720. https://doi.org/10.1016/j.jairtraman.2019.101720.

[43] Eesti Rahvusringhääling. Eesti võtab 22. maist kasutusele biomeetrilise passi. 2007. https://www.err.ee/457894/eesti-votab-22-maist-kasutusele-biomeetrilise-passi (02.12.2022)

[44] Bischoff P. 50 countries ranked on how they use, store, and share traveler data. 2022. https://www.comparitech.com/blog/information-security/travel-data/ (04.12.2022)

[45] European Commission. Entry/Exit System (EES). https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/smart-borders/entry-exit-system_en (02.12.2022)

[46] Thales. What is EURODAC. 2022. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/eurodac (02.12.2022)

[47] U.S. Customs and Border Protection. CBP Biometrics - Customs and Border Protection. https://biometrics.cbp.gov/ (20.01.2023)

[48] Gelb A., Clark J. Identification for Development: The Biometrics Revolution. Working Paper, Center for Global Development. 2013. http://www.cgdev.org/content/publications/detail/1426862 (04.12.2022)

[49] Perrigo B. India Has Been Collecting Eye Scans and Fingerprint Records From Every Citizen. Here's What to Know. 2018. https://time.com/5409604/india-aadhaar-supreme-court/ (04.12.2022)

[50] Government of India. Unique Identification Authority of India. https://uidai.gov.in/aadhaar_dashboard/ (04.12.2022)

[51] Gelb A., Diaofasi A. Biometric Elections in Poor Countries: Wasteful or a Worthwhile Investment?. Working Paper, Center for Global Development. 2016. https://www.cgdev.org/sites/default/files/biometric-elections-poor-countries-wasteful-or-worthwhile-investment.pdf (04.12.2022)

[52] CIPESA. Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa. 2022. https://www.ictworks.org/wp-content/uploads/2022/10/Surveillance-Data-Laws-in-Africa.pdf (12.04.2023)

[53] Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679. https://eur-lex.europa.eu/legal-content/et/ALL/?uri=CELEX:32016R0679 (03.05.2023)

[54] Sorainen AS. Euroopa Liidu ja rahvusvaheliste õigusaktide analüüs identiteedihalduse valdkonnas. 2018.

[55] Bryan Cave Leighton Paisner LLP. U.S. Biometric Laws & Pending Legislation Tracker. 2021. https://www.bclplaw.com/en-US/insights/us-biometric-laws-and-pending-legislation-tracker.html (23.01.2023)

[56] Lively T. K. Facial Recognition in the United States: Privacy Concerns and Legal Developments. 2021. https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2021/december/facial-recognition-in-the-us-privacy-concerns-and-legal-developments/ (23.01.2023)

[57] Thales. Biometric data and privacy laws (GDPR, CCPA/CPRA). 2021. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data (23.01.2023)

[58] Soares, E. Brazil: Personal Data Protection Law Enacted. 2018. https://www.loc.gov/item/global-legal-monitor/2018-08-28/brazil-personal-data-protection-law-enacted/ (25.01.2023)

[59] DLA Piper. Collection & Processing in Colombia. 2022. https://www.dlapiperdataprotection.com/index.html?t=collection-and-processing&c=CO (25.01.2023)

[60] Commins I. Using Biometrics: What's the status in Australia. 2021. https://privacy108.com.au/insights/using-biometrics-in-australia/ (24.01.2023)

[61] Uppal A. India: Biometric Data: Regime In India. 2019. https://www.azbpartners.com/bank/biometric-data-regime-in-india/ (24.01.2023)

[62] Krishnan M. India: Is biometric data privacy at risk? 2022. https://www.dw.com/en/concerns-rise-over-a-new-law-that-lets-indian-police-record-prisoners-dna/a-63044478 (25.01.2023)

[63] Coos, A. Data Protection in Japan: All You Need to Know about APPI. 2022. https://www.endpointprotector.com/blog/data-protection-in-japan-appi (25.01.2023)

[64] Kapiyo V. Towards Effective Biometrics and Digital Identity Systems in Africa. 2022. https://cipesa.org/2022/12/towards-an-effective-biometrics-and-digital-identity-system-in-africa/ (12.04.2023)

[65] Watson C. I., Fiumara G. P., Tabassi E., Salamon W. J., Flanagan P. A. Fingerprint Vendor Technology Evaluation. NIST IR 8034. National Institute of Standards and Technology. 2014. https://doi.org/10.6028/NIST.IR.8034.

[66] Grother P., Ngan M. Face Recognition Vendor Test (FRVT), Performance of Face Identification Algorithms. NIST IR 8009. National Institute of Standards and Technology. Gaithersburg, MD. 2014. https://doi.org/10.6028/NIST.IR.8009.

[67] Fiumara G. A Tale of Two Errors: Measuring Biometric Algorithms. 2022. https://www.nist.gov/blogs/taking-measure/tale-two-errors-measuring-biometric-algorithms (25.04.2023)

[68] Grother P., Quinn G., Phillips P. Report on the Evaluation of 2D Still-Image Face Recognition Algorithms. NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD. 2010. https://doi.org/10.6028/NIST.IR.7709.

[69] Sang J., Lei Z., Li S. Face image quality evaluation for ISO/IEC standards 19794-5 and 29794-5. *Proceedings of the Third International Conference on Advances in Biometrics (ICB)*, 2009, 229–238. https://doi.org/10.1007/978-3-642-01793-3_24.

Lisad

I. Lihtlitsents

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Mariliis Malahhov,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose **Biomeetriapõhise isikutuvastuse tõsikindluse alused sõrmejäljele ja näokujutisele**, mille juhendajad on Angelika Kärber ja Heili Orav, reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.
2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 4.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, alates ***09.05.2023*** kuni autoriõiguse kehtivuse lõppemiseni.
3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.
4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Mariliis Malahhov,
09.05.2023