INTERNATIONAL UNIVERSITY AUDENTES

Sotsiaal-ja Humanitaarteaduskond

Infotehnoloogia õppetool

Martin Tuude

BIOMEETRILISED AUTENTIMISVAHENDID

Bakalureusetöö

Juhendaja: Jüri Majak

Tallinn 2008

SISUKORD

SISSEJUHATUS

Biomeetriline tuvastamine ja selle täpsus on paelunud paljusid inimesi, samuti ka antud töö autorit. Autoril tekkisid esimesed kokkupuuted biomeetriaga paar aastat tagasi viibides puhkusel Ameerika Ühendriikides, kus tuli tutvuda sõrmejälje tuvastusseadmetega, kõigepealt viisa taotlemisel ja samuti ka piiri ületamisel. Lisaks sõrmejälje šabloonile tehti igast riiki siseneda soovivast isikust eraldi fotoportree. Olles visanud esmapilgu internetis leiduvatele erinevatele biomeetrilistele seadmetele, millest varem aimugi polnud, hakkas antud teema järjest rohkem huvi pakkuma.

Biomeetria on tänapäeval kiiresti arenev uudne ja aktuaalne valdkond, mida on Eestis veel vähe kajastatud. Tänu tehnika kiirele arengule saab biomeetria peatselt igapäevaseks nähtuseks meie elus. Turvalisus muutub järjest olulisemaks ja inimesed puutuvad rohkem kokku biomeetriliste autentimisvahenditega, mis saigi otsustavaks antud bakalaureusetöö teema valikul.

Biomeetrilise tuvastamise puhul kasutatakse isikute kindlakstegemiseks neile ainuomaseid bioloogilisi tunnuseid või käitumuslikke jooni.

Biomeetrial baseeruvat autentsuse kindlakstegemist kasutatakse peamiselt tööjaamades, võrgu- ja domeeni juurdepääsul, üksikisiku sisselogimisel, andmete kaitses, ressurssidele juurde pääsemiseks ja veebi turvalisuse tagamiseks. 2007. aasta maikuust alustas Eesti biomeetriliste identifikaatorite digitaalset lisamist reisidokumentidesse. Biomeetria muudab meie elu tunduvalt mugavamaks ja turvalisemaks. Inimesed ei pea pähe õppima ja meelde jätma juurdepääsukoode, samuti ei saa ka keegi varastada juurdepääsu luba.

Töö eesmärgiks on uurida maailmas enim kasutatavaid biomeetrilisi autentimisvahendeid, nende kasutuskõlblikkust ja efektiivsust, samuti selgitada välja, millised autentimisseadmed vastavad etteantud kriteeriumitele, nõuetele ja võimalustele juhul kui on tegemist uute seadmete soetamisega. Viimane ülesanne osutus esialgu arvatust palju keerukamaks kuna sisaldab mitme vastuolulise kriteeriumi samaaegset täimist. Tulemuste saamiseks tuli püstitada ja lahendada multikriteriaalne optimiseerimise ülesanne.

Uurimisobjektiks on enim levinud biomeetrilised autentimisvahendid nagu silma võrkkest, silmaiiris, sõrme geomeetria, käe geomeetria, allkirja dünaamika, hääle dünaamika ja näokuju.

Enne erinevate autentimisvahendite analüüsimist sai autori poolt püstitatud järgmine hüpotees: kõige optimaalsemaks autentimisviisiks osutub sõrme geomeetria.

Antud bakalaureusetöö koosneb kuuest peatükist, mis omakorda koosnevad alapeatükkidest. Esimeses peatükis käsitletakse tähtsamaid küsimusi biomeetrias ja enim levinud biomeetrilisi tunnuseid. Teises peatükis antakse ülevaade biomeetrilistest seadmetest ja nende positiivsetest ja negatiivsetest omadustest. Kolmandas osas on ära toodud biomeetriliste seadmete töömetoodika, tuvastamistehnika aeg ja maksumus. Neljandas peatükis selgitatakse lahti multimodaalse biomeetria olemust. Viiendas osas kirjeldatakse biomeetriliste seadmetega teostatud teste. Kuuendas peatükis tuuakse välja optimeerimisülesande püstitused, arvutatakse tulemused kahel erineval meetodil ja analüüsitakse saadud tulemusi. Kokkuvõttes tehakse autoripoolsed järeldused analüüsil saadud tulemustest.

Bakalaureusetöö kirjutamisel on aluseks võetud eesti- ja võõrkeelsed ajakirjanduses ilmunud ja internetis olevad artiklid ja uurimused. Töö kirjutamisel esile kerkinud probleemidest võibki välja tuua empiirilise materjali hankimisega seotud probleemid. Antud teema kohta ei ole kättesaadavaid raamatuid. Kuna teema on uudne, on eestikeelset materjali ilmunud väga vähe ja sellel põhjusel on autor kasutanud suures osas võõrkeelset materjali.

1. BIOMEETRIA LÜHIÜLEVAADE

Töö esimeses peatükis kirjeldatakse enimlevinud biomeetrial põhinevaid tunnuseid, nende päritolu ja iseloomulikke jooni. Samuti esitatakse tabeli kujul erinevate kasutusel olevate biomeetriate tugevad ja nõrgad küljed.

1.1. Tähtsamad küsimused biomeetrias

Biomeetria on automatiseeritud meetodid isiku tuvastamiseks, mis baseeruvad füsioloogilistel või käitumislikel tunnustel. Tunnuseid saadakse näost, sõrmejälgedest, käe geomeetriast, käekirjast, silma läätsest, võrkkestast, käeveeni geomeetriast ja häälest. (A. K Jane, A. Ross, S. Prabhakar, An Introdution to Biometric Recognition, 13.03.2008)

Ennem kui hakata tegelema biomeetriaga tuleks vastata algselt järgmistele küsimustele!

Kas rakendus vajab kinnitust või identifitseerimist?

Kui nõutakse subjekti identifitseerimist suurest andmebaasist, siis vajatakse rohkem skalleerimist ja suhteliselt iseloomulikku biomeetriat (N: sõrmejälg, silmaiiris, DNA).

Mis on töökorras rakenduste reziim?

Näiteks: kas rakendused on automaatsed või pool-automaatsed, kas kasutajatel on varem kokkupuuteid olnud biomeetriaga või mitte, kas rakendus on salajane või mitte, kas subjekt on koostöövalmis või mitte ja nii edasi.

Kui tihti esitatakse nõudmisi?

Näiteks suuremat täpsust nõudvate rakenduste korral, vajatakse rohkem iseloomulikku biomeetriat.

Milline biomeetria on vastuvõetav kasutajatele?

Erinevad biomeetriad on erinevalt kohaldatud, olenevalt demograafilisest sõltuvusest, kultuurist, eetilisusest, usust ja hügieeninõuetest kultuuris.

1.2. Enamlevinud biomeetrilised tunnused

Järgnevalt on antud põgus ülevaade enimkasutatavatest biomeetrilistest tunnustest (A. K Jane, A. Ross, S. Prabhakar, An Introdution to Biometric Recognition, 13.03.2008):

- DNA – ühe dimensiooniline ülim unikaalne kood, mis on igal ühel individuaalne, välja arvatud identsetel kaksikutel kellel on identne DNA. Kasutatakse enamasti kohtuliku rakendust isiku tuvastamisel.

- Kõrv – on teada, et kõrva kuju ja kõhrkoe struktuur sisekõrvas on eristatav. Kõrva tunnused ei ole nii unikaalsed indiviidi kohta. Kõrva tuvastamise lähenemisetee baseerub sobiva vahemaa silmatorkavatest punktidest sisekõrva pinnast.

- Nägu – nägu on üks vastuvõetavamaid biomeetriaid, kuna see on üks tavalisemaid meetodeid isiku tuvastamiseks, mida kasutatakse visuaalsel toimel. On väga väljakutsuv arendada näo tuvastamise tehnikat, mis talub vananemise efekti.

- Näo, käe ja käeveeni infrapuna termogrammid - kuumust kiirgava inimkeha kujutis on iseloomulik igal individuaalsel kehal ja seda on võimalik tõestada infrapuna kaameraga märkamatul teel, just nagu tavalise kaameraga. Seda tehnoloogiat kasutatakse salajaseks tuvastamiseks ja selle abil on võimlik vahet teha identsetel kaksikutel. Infrapuna sensorid on aga väga kallid, mis takistavad termogrammide laiemat levikut.

- Sõrmejälg - on muster lainetustest ja orgudest sõrmeotsta pinnal, mis areneb välja inimesel esimese seitsme kuu jooksul loote arengu staadiumis. Isegi identsetel kaksikutel on sõrmejäljed erinevad ja samuti on erinevad ka sama isiku sõrmed. Mitmekordsed sõrmejäljed samast isikust annavad informatsiooni laiaulatuslikeks tuvastamisteks , mis sisaldavad millioneid identsuse tunnuseid.

- Liikumisviis – liikumisviis ei ole väga iseloomulik, kuid see on piisavalt omane võimaldades isiku tuvastamist mõnes madalalt turvatud alas. Liikumisviis on käitumuslik biomeetria ja võib muutuda seoses vanusega, kehakaalu muutustega, vigastustega ja ebakaines olekus. Kuna liikumisele baseeruvad süsteemid kasutavad video salvestamise võtmist liikuvast inimesest, et mõõta mitmeid erinevaid liikumisviise on see arvestatav ja intensiivne.

- Käe- ja sõrme geomeetria – käe geomeetrial süsteemid baseeruvad mitmetel mõõtmistel inimkäest sisaldades endas kujundit, peo suurust ja sõrmede suurust ja pikkust. Mõningaid tunnuseid seoses inimkäega (sõrmede pikkus) on suhteliselt muutumatud ja individuaalsed. Pilditehnikale omane süsteem nõuab koostööd subjektiga ja võtab frontaalse- ja külgvaate pildid peopesast, mis on asetatud paneelile laialisirutatud sõrmedega. Selle tulemusena valmib käest tehtud pilt, mis tundub väga väike, kuid on atraktiivne tunnus piiratud ülekandekiiruse ja mäluga süsteemidel.Oma piiratud eristatuses on käegeomeetrial baseeruvad süsteemid tüüpiliselt kasutatavad kinnitused. Sõrme geomeetria süsteemid (milles saab geomeetrilisust mõõta ainult ühe või kahe sõrmega) võivad olla rohkem eelistatud oma kompaktsele suurusele.

- Silmaiiris – süsteem põhineb kaameral, mis loeb sisse silmavikerkesta kujutise, seejuures ei toimu füüsilist kontakti kasutaja ja seadme vahel, kuigi meetod eeldab õiget silma asetust. Iga silmaiiris on eristatav ja nagu sõrmejälg on ka iiris identsetel kaksikutel erinev.

- Klahvivajutuse dünaamika – on mõttetu oletada, et iga isik trükib klaviatuuril endale iseloomulikul moel. Selline käitumuslik biomeetria ei ole unikaalne igaühele individuaalselt, kuid pakub piisavalt eristatavat informatsiooni, et võimaldada isiksuse tuvastamist.

- Lõhn – on teada, et iga objekt eritab lõhna, mis on iseloomulik tema keemilisele koostisele ja mis on erinevalt tajutav erinevate objektidega. Tuulehoogudest ümbritsetud objektist eraldub hulga lõhnu, mis puhutakse keemilistesse sensoritesse ja jaotatakse eraldi gruppideks. Lõhnade erinevad komponendid, mida inimkeha eritab on igal ühel individuaalselt erinevad.

- Peopesa jälg – Inimese peopesa koosneb samuti mustritest ja orgudest nagu ka sõrmejäljed. Peopesa ala on palju suurem kui sõrmejälgedel ja seega on nad isegi rohkem eristatavamad. Kuid kuna peopesa salvestamiseks vajatakse suuremat ala on need seadmed aga kogukamad ja kallimad.

- Allkiri – see kuidas inimene kirjutab oma nime, on temale iseloomulikuks iseloomujooneks. Kuigi allkirjad nõuavad kokkupuuteid ja saavutusi kirjutamise instrumentidega, paistavad nad olevat vastuvõetavad paljudes institutsioonides ja kommertstehingutes, kui isiku tõestamise meetodid. Allkirjad on käitumusliku

biomeetria osa, mis muutub aja jooksul ja mida mõjutab isiku füüsiline ja emotsionaalne seisund. Mõne inimese allkirjad muutuvad palju, isegi iga järgnev allkiri, mida üritatakse jäljendada, erineb eelmisest oluliselt. Kuigi professionaalne võltsija võib järgi teha allkirja, mis võib tunduda ehtne.

- Hääl – hääl võib olla ainus biomeetria isiku tuvastamiseks telefoni teel. Häält võivad mõjutada isiku tervislik seisund, stress, emotsioonid jne, samuti võib efektiivsust mõjutada ka tausta helid.

Nagu eelnevatest loeteludest näha on isikuid võimalik tuvastada mitmete erinevate biomeetriliste tunnuste abil. Erinevatel elualadel kasutatakse erinevaid biomeetrilisi meetodeid ja tihti mitut meetodit korraga. Igal biomeetrilisel tunnusel on oma tugevused ja nõrkused.

Tabel 1. Hinnang erinevatest kasutusel olevatest biomeetrilisest identifikaatoritele. Tugev, keskmine, ja madal on tähistatud lühenditega T, K ja M.

Biomeetriline identifikaator	**Universaalsus**	**Iseloomulikkus**	**Püsivus**	**Nähtavus**	**Toimimine**	**Vastuvõetavus**
DNA	T	T	T	M	T	M
Kõrv	K	K	T	K	K	T
Nägu	T	M	K	T	M	T
Näo termogramm	T	T	M	T	K	T
Sõrmejälg	K	T	T	K	T	K
Liikumisviis	K	M	M	T	M	T
Käegeomeetria	K	K	K	T	K	K
Käeveeni geomeetria	K	K	K	K	K	K
Silmaiiris	T	T	T	K	T	M
Klahvivajutus	M	M	M	K	M	K
Lõhn	T	T	T	M	M	K
Võrkkest	T	T	K	M	T	M
Allkiri	M	M	M	T	M	T
Hääl	K	M	M	K	M	T

Allikas: Winkpedia The Free Encyclopedia, Biometrics 2008

Küsimusele, milline biomeetria on parim, üheselt vastata ilmselt ei saa, sõltuvalt vajadusest kasutatakse erinevaid kriteeriume (Biometrics, Winkpedia The Free Encyclopedia 12.03.2008):

- **Unikaalne** (erinevad väärtused, erinevatelt isikutelt)
- **Püsiv** (peab olema muutumatu aja jooksul)
- **Välistatav** (saab mõõta koguseliselt)
- **Kasutuskõlblik** (saavutatakse tuvastamise täpsus, ressursid on nõutavad, töökorras/ keskkonna faktorid)
- **Vastuvõetav** (kas inimesed on võimelised seda vastu võtma?)
- **Möödahiilimisvastane** (kui lihtne on ära petta süsteeme)

2. BIOMEETRILISED TUVASTUSSEADMED

Järgnevas peatükis kirjeldatakse enimkasutatavaid biomeetrilisi seadmeid. Alustatakse lühiülevaatega biomeetria ajaloost ning analüüsitakse seadmete positiivseid ja negatiivseid omadusi.

2.1. Sõrmejäljed

Alates 19-ndast sajandist leiti, et inimesi oleks vaja kirjeldada mingit unikaalset tegurit kasutades, eelkõige oli see mõeldud kurjategijate kindlaksmääramisel. Aja möödudes sai sõrmejälgede võtmine rahvusvaheliseks meetodiks politseitöös ja on kuni tänapäevani peamiselt kasutatav meetod isiku tuvastamiseks, nüüd küll juba automatiseeritult. Nüüdne teadus on arenenud nii kaugele, et mõningate masinate abil on võimalik kindlaks teha, kas tegemist on elava inimese sõrmejäljega või mitte. (Mets Olav, Biomeetria, sõrmejälgede tuvastus ja nende tuvastusseadmed, 05.01.2008)

Ainuüksi FBI-l on rohkem kui üle 70 miljoni sõrmejälje faili, nendest enamus on saadud, vanu templipadja ja paberi meetodeid kasutades. See aga nõuab inimestelt kannatlikkust, istuda ja võrrelda sõrmejälgi tunde, isegi kui mitte päevi.

Kõiki sõrmejälgi saab tuvastada kahel põhilisel tunnusel, mida kutsutakse lainetusteks ja orgudeks. Uurides neid tunnuseid on võimalik välja võtta andmeid värskest sõrmejäljest ja salvestada need arvuti andmebaasidesse tulevasteks vajaminevateks võrdlusteks.

Praegusel ajal on olemas kaks põhilist ja aktsepteeritud meetodit andmete väljavõtmiseks, milleks on: üksikasjalisel põhinev ja seostel põhinev meetod. Üksikasjalisel põhinev meetod on enam mikroskoopiline kui teine, alustades sõrme lainetuse hargnemisest ja lõppemisest ja nende määratlemisest XY-koordinaatidesse, mis hiljem salvestatakse faili. Seostel põhinev meetod vaatleb rohkem üldist mustrit lainetustest ja orgudest. Mõlemal meetodil on siiski olemas ka puudused. Üksikasjaline meetod nõuab, et sõrmejälje pilt oleks kõrge kvaliteediga, mustus, vesi, armid ja haavad mõjutavad oluliselt identifitseerimist. Seostel põhineva meetodi korral ei saa aga sõrme liigutada. (Fingerprint, Rosistem Build Your Business, 12.03.2008)

Suhteliselt madal hind on andnud seadmele mitmeid uusi rakendusi näiteks arvutil, mis loeb omaniku sõrmejälgi. Näiteks IBM tõi 2004 aasta sügisel turule uuendatud sülearvuti T42. Kus on kasutajale mõeldud väike skanner (joonis 1), kust tuleb näpuga üle libistada. Selliste

seadmete toomine sülearvutitesse on vajalik kahel eesmärgil. Kõigepealt turvalisus, kuna arvutit saab kasutada vaid isik, kelle näpujälg on eelnevalt arvutisse skaneeritud. Kui tegemist oleks tavapärase näpujälje lugejaga, kuhu sõrm lihtsalt peale suruda oleks kurjategijatel lihtsam arvutisse järgitehtud jälgi kasutades sisse murda. Teine hea omadus on veel, et skanneri mõõtmed on hämmastavalt väikesed, mis on sülearvuti puhul väga oluline aspekt ja väikeseid skannereid on lihtsam hooldada ja puhtana hoida, kuna suured kipuvad kiiremini määrduma ja seega on neilt raske isikuid autentida. Ja samas ei saa mainimata jätta ka kiirust, kuna palju lihtsam on kerge näpuliigutusega ennast arvutisse sisse logida, selle asemel et pikka salasõna sisse toksida.

Pärast esmast käivitamist avaneb automaatselt IBM Fingerprint Software programm, mis juhib kasutajad läbi biomeetria tihniku, kus tuleb salvestada enda näpujäljed, milleks on vaja valida üks sõrm ja sellega kolm korda üle lugeja tõmamta. Pärast kolme edukalt läbitud katset ühitab arvuti need omanikuga ja salvestab need. Ja seejuures ei salvestata sõrmejälge tervikfaili või –pildina, vaid iga andme jaoks luuakse tilluke andmekogum, millest piisab õige jälje ära tundmiseks, seega on süsteem üsnagi turvaline. (Vare 2004, lk 24-25)

Joonis 1. IBM-i sõrmejäljeskanner
Allikas: Vare 2004, lk.24

Tänapäeval on võimalik hankida üsnagi suure täpsusega seadmeid ainult 100 dollari eest, mis on umbes postmargi suurused. Sony FIU optilise tuvastusseadme näitajateks on 1% mitte äratundmisi ja 0,1 % valesid äratundmisi.

Üks levinumaid sõrmejälje tuvastamise meetodeid on mahtuvuslikul sensoril põhinev, kus andur detekteerib elektrivälja sõrme joonte ja süvendite ning anduri pinna vahel. Võrreldes mitmete teiste tuvastamise vahenditega võimaldab selline andur kõrgemat turvalisust ja kasutamise lihtsust. Selline ühe kiibiga lahendus on väiksem ja võtab vähem voolu, 1mW 5V

toite korral, kui teised sõrmejälje andurid. (Mets Olav, Biomeetria, sõrmejälgede tuvastus ja nende tuvastusseadmed, 05.01.2008)

2.2. Silmaiiris

Silmaiiris on ajalooliselt omaks võetud unikaalse tunnusena, olles igale indiviidile ainulaadne. 1980-ndal leidsid kaks arsti Dr. Leonard Folm ja Aran Safir, et pole olemas kahte sarnast silmaiirist. Nad tõestasid seda 1987 aastal, identifitseerides inimesi silmaiirise põhjal. (Iris Scan, National Centre Of State Court, 11.03.2008)

Silmaiiris kaudu isiku autentimine(joonis 2) on tänapäeval üks täpsemaid biomeetrilisuse vahendeid. Silmaiirise skaneerimine arvutisse käib lihtsalt, kusjuures puudub igasugune füüsiline kontakt. Vikerkesta kujutis digitaliseeritakse ja konverditakse see numbriliseks koodiks, mis toimib vaid ühtepidi. Kujutis, mille salvestab tavapärane digitaalkaamera, skaneeritakse põhiliste karakteristikute saamiseks ja salvestatakse 512-baidisele šabloonile. (Iris Recognition Frequently Asked Questions, Rycom, 28.02.2008)

Silmaiirise kaudu tuvastamise esimeses faasis toimub registreerimine. Kus tuvastatav isik astub masina ette ja ootab protsessi lõppu. Kui tuvastamine on lõpetatud, toimub ühe või mõlema silmaiirise salvestamine, sõltuvalt süsteemist, mida kasutatakse. Kujundi omandamise etapil salvestatakse iirised, kasutades must-valgeid kaameraid. Salvestatud pildist võetakse iirise asukoht. Selles staadiumis võtab arvuti salvestatud kujutise ja filtreerib välja kõik peale silmaiirise. Asukoha määramise protsess läbib keerulise algoritmi, mis elimineerib: kulmud, ripsmed ja silma kõvakesta (valge osa silmadel). Kui kujutis on kindlaks määratud, salvestatakse see kahendformaati. Viimane staadium iirise äratundmisel hõlmab pärast registreerimise protsessi. Kui silmaiiris on juba kord registreeritud, siis saab jätkata silmaiirise äratundmise protsessi. Järgnev faas on silma mustri sobivuse aste, mis nõuab äratundmist. Mustri sobivusastmes võetakse asukoht silmaiirise kujutisest ja seda võrreldakse teiste silmaiiristega, mis on salvestatud andmebaasi. Kui sobiv tulemus leitakse, siis kas avatakse uks või ligipääs arvutile aktiveeritakse. (Iris and retinal identification, Western Carolina Univeristy, 12.03.2008)

Vikerkesta numbriline vastavus saadakse silma vikerkesta jagamisel kaheksaks erinevaks piirkonnaks, mille kõiki tulemusi võetakse arvesse koondtulemusena. Kahe vikerkesta erinevus seisneb mittekattuvates bittides, mida nimetatakse Hammingi kauguseks (Hamming

Distance - HD). Identsete koodide puhul võrdub Hammingi kaugus 0-ga, täiesti erinevate puhul aga 100%. Tavaliselt on kahe erineva silma HD ligikaudu 50%. Sama vikerkesta kaks erinevat kujutist võivad erineda teineteisest viie kuni kümne protsendi võrra. Kuna sinna juurde võivad lisanduda mitmesugused mürad, pannakse seadme tuvastmaise piiriks tavaliselt 32%. (Mets Olav, Biomeetria, sõrmejälgede tuvastus ja nende tuvastusseadmed, 20.02.2008)

Heathrow lennujaamas hakati 2002 aastal katsetama silmaiirisel põhinevaid autentimissüsteeme, mis kontrollisid inimese silma, tavapärase passi asemel, kui nad läbisid passikontrolli. Heathrow oli Inglismaa esimene lennujaam, mis tõi välja silmaiirisel põhineva tehnoloogia. Selle eesmärgiks on kiirendada liikumist ja avastada illegaalseid immigrante. Igast reisijast tehti pilt ühest oma silmaiirisest, mis salvestati arvutisse. Selle asemel, et näidata oma passi, liikusid nad kioskisse, kus sekundilise kaamerasse vaatamise järel, sobitati silmaiirise šabloon arvutis olevate andmetega, mille sobivusel avanes tõke automaatselt. Katses hinnati tehnoloogiat ja reisijate reaktsiooni. Selline protseduur pärineb Ameerika Ühendriikidest ja seda peetakse kõrgeimaks tehnoloogiaks üksikisiku identifitseermilsel kogu maailmas. (Airport tests passenger eye Ids, BBC News, 22.12.2007)

Joonis 2. Silmaiirisepõhine autentimine
Allikas: BBC News, Airport tests passenger eye IDs 2007

On olemas mitmeid erinevaid firmasid, mis on seotud silmaiirise äratundmise tehnoloogiaga. LG Electronics on üks suurimaid tootjaid silmaiirise tuvastamise tehnoloogias, paigutades üle 1000 süsteemi, kuuel erineval mandril. Neid süsteeme kutsutakse IrisAccessiks. LG süsteemid on varustatud audio-visuaalsete vihjetega, et aidata isikul kasutada süsteeme. Täiendava tunnusena nendel masinatel on see, et silmaiirise kujutis salvestatakse juhtpaneelile, mitte silmaiirise lugejasse. (LG Irisacess 4000, Sourcesecurity.com, 10.03.2008)

Oki Electronic Industries toodab kahte erinevat mudelit silmaiirise äratundmiseks. IRISPASS-H on väike kätte-mahtuv seade, mida kasutatakse personaalarvuti juures, et identifitseerida kasutajat. Oki laialdasem seade on IRISPASS-WG. See on seinale kinnitatav ja seda saab kasutada samaaegselt koos 126 teise seadeldisega, et kontrollida turvalisust. IRISPASS-WG sisaldab endas tunnuseid, mis automaatselt avastavad silmaiirise asukoha, see tähendab, et kasutajal tuleb ainult seista seadeldise ette, et ennast identifeerida. (Oki introduces the irispass-WG, Oki, 10.03.2008)

EyeTicket Corporation keskendub reisimise töötlemisele ja juurdepääsu kontrollimisele, kasutades silmaiirsie äratundmist. EyeTicketil on kahte erinevat tüüpi seadmeid EyePass ja JetStream. Esimene neist seadmetest on välja töötatud nii, et mitte keegi teine ei pääse juurdepääsu punktist enne läbi, kui on tuvastatud skaneeritud isik. See saavutatakse kahe ukselisel süsteemil, mille vahel on survetundlik põrand. See seadeldis identifitseerib isiku avades alguses esimese ukse, lubades seejärel kasutajal sisse kõndida keset kambrit, järgnevalt kasutab kamber survetundlikku põrandat, veendudes, et ainult üks isik on ruumis. Kui see protsess on läbitud avaneb teine uks, mis juhatab kasutaja välja. EyeTicketi teine toode on JetStream. JetStream on süsteem, mille kasutajad saavad tõestada oma identsust, kiire protsessiga rakendustel, nagu näiteks lennuliinidel, hotellides, raudteedel ja passikontrollides . (Transportation security, The Eyes Have It, 10.03.2008)

Irdian Technologies on juhtiv tootja silmaiirise äratundmise tehnoloogias. Nad uurivad ja toodavad silmaiirise tuvastamise tehnoloogiat, ning hoiavad enda käes rahvusvahelist patenti põhiideest ja tehnoloogiast iirisel tuvastamisest. Irdiani tehnoloogia on realiseeritud kahel moodulil. Esimene neist on PrivaatID tarkvara, mida kasutavad iirisel äratundvad kaamerad, mis on tehtud firamde poolt nagu Oki ja Panasonic. Teine moodul Irdiani tehnoloogias on, et nende tehnoloogia on läbinud spetsiaalse sertifikaadi, mis tõestab, et iirisel tuvastamisel tooted vastavad esitatud nõuetele. (Products, Irdian Technologies, 09.03.2008)

2.3. Näokuju

Inimese näo tuvastamine on olnud suure tähelepanu all viimasel aastakümmnel. On uuritud mitmeid näo äratundmise algoritme ja saadaval on mitmeid kommerts näo tuvastamisel põhinevaid tooteid: rakendused, mis määravad ära rassi, soo ja mitmeid näo tuvastamise ülesandeid, mis vajavad lahendust. (Blackburn Duane M., Face Recognition 101: A Brief Primer, 14.03.2008)

Võrreldes näo tuvastamist teiste biomeetriliste meetoditega on see meetod äärmiselt kliendisõbralik ja üsnagi laialt rakendatav. Kliendisõbralikkuse tagab tuvastamise meetod, mille käigus ei pea tuvastatav astuma vahetusse kontakti kontrollseadmega. Kasutatavuse seisukohalt on mitmeid perspektiivseid rakendusi nagu isikute äratundmine rahvamassist, keskkonnad mis häälestavad end automaatselt konkreetsele kasutajale, ning seadmed, mis abistavad isikute meelespidamist jne. Tehnoloogilisest küljest näo tuvastamise kasutusevõtul takistusi ei ole, kuna kaameraid saab paigutada oma suuruse tõttu sinna kuhu vaja. (Mets Olav, Biomeetria, sõrmejälgede tuvastus ja nende tuvastusseadmed, 08.01.2008)

Näo tuvastamine tehnoloogias kasutakse enamasti tavalisi PC kaameraid, mis üldiselt töötavad 320 X 240 resolutsioonil, sealjuures 3-5 kaadrit sekundis. Kuid samas on ka olemas kallimaid kaameraid, mis on parema resolutsiooniga ja samuti on need võimelised eraldama rohkem kaadreid sekundis, mis annavad ka parema pildi kvaliteedi. Näo tuvastamise tarkvara maksab 59 dollarist, kuni 1000 dollarini, mis tõttu on see üks odavamaid biomeetrilisi tehnoloogiaid. (Biometrics: Face Recognition Technology; GIAC Certified Professionals; 03.01.2008)

Näo tuvastamisel kasutatakse peamiselt järgmiseid tehnikaid (Jean-Francois Mainguet, Face Recognition/ Reconnaissance du visage, 05.02.2008):

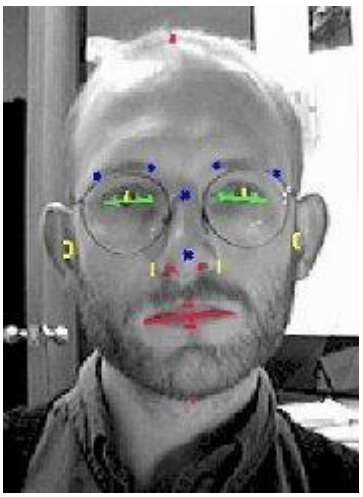
- näo geomeetria: kasutatakse geomeetrilisi tunnuseid näost. Võib kasutada mitmeid erinevaid kaameraid, et saavutada paremat täpsust (2D,3D...);
- naha mustri ära tundmine;
- näo termogramm: kasutatakse infrapuna kaameraid, et märgistada näo temperatuuri;
- naeratus: äratundmisel näo kuju muutub naeratades.

Kuid probleeme tekitab hoopis isiku tuvastamise meetod. Tuvastusseadme probleemide hulka kuuluvad aga inimeste vananemine, meik- upi kasutamine, prillide kandmine jne. (Mets Olav, Biomeetria, sõrmejälgede tuvastus ja nende tuvastusseadmed, 08.01.2008)

Kuid samas on olemas ka mitmeid meetodeid, mille järgi isikuid identifitseerida näo kuju järgi ja mis kunagi ei muutu, nendeks on (Putting an End to Account-Hijacking Identity Theft, Federal Deposit Insurance Corporation, 13.02.2008):

- ülemine osa silmakoopast;
- ala, mis ümbritseb põseluud;
- suu küljed;
- silmade vaheline distants.

Tunnuseid mille järgi saab nägu tuvastada on toodud välja joonisel 3.



Joonis 3. Näo tuvastamine
Allikas: Mainguet, J.F. 2008

2.3.1. Kolmedimensionaalne mudelile baseeruv näo äratundmine

Süsteemid, mis kasutavad näo ära tundmiseks kahedimensioonilist(2D) pilti on sõltuvad sellistest asjaoludest nagu valgus, poseerimise- ja näoilme. Kolmedimensionaalsel (3D) autentimisel need probleemid aga kaovad. Selge 3D pildi saamiseks kasutatakse 3D sensoreid, mis kuvavad näo pinnavormilt informatsiooni. 3D vorm näopinnast, esindab informatsiooni näo struktuurist, mis on seotud näo sisemise anatoomilise struktuuriga selle asemel, et uurida välispinda ja keskkonda. 3D mudeli äratundmiseks kasutatakse 2,5D pilti, mis skaneeritakse sisse erinevate nurkade alt. 2,5D on lihtsustatud 3D (x, y, z), pinna ära tundmine, mis koosneb ühe sügavuse väärtusest (z), igal punktil (x, y) tasapinnal. Viimistletult sarnane meetrilisus defineeritakse sobitamisel. (Matching 2,5D face scans to 3D models, Ieee Xplore, 12.03.2008)

2.4. Käekuju

Käegeomeetria on vanaisa võrreldes teiste tänapäeval kasutusel olevate biomeetriatega, mis loodi 1986- ndal aastal. On olnud kuus erinevat käe skaneerimise toodet, mida on selle aja jooksul arendatud, kusjuures mõned on kommertskasutuses edukad kuni tänapäevani.

Käegeomeetria sisaldab endas mõõtmist ja analüüsimist ühe käe vormist. See on küllaltki lihtne protseduur ja samas ka üllatavalt täpne. Kuigi see nõuab spetsiaalset riistvara, saab seda lihtsalt integreerida teistesse seadmetesse ja süsteemidesse. Tihti lisatakse seadmele, aja ja kohaloleku salvestamise võimalus, mis teeb seadme üsnagi populaarseks. Erinevalt näpujäljest ei ole inimkäsi unikaalne. Individuaalsed käetunnused ei ole identifitseerimisel piisavalt iseloomulikud. Siiski on võimalik välja mõelda meetod, ühendades mitmeid erinevaid individuaalseid tunnuseid, mõõtes sõrmede ja käe pikkust, laiust, paksust ja pinnastruktuuri, tõestamaks eesmärki. (Hand Geometry, National Center for State Courts, 12.12.2007)

Skaneerimisel kasutatakse kõrge resolutsiooniga digitaalseid kujutisi, mis salvestatakse üheksa baidi suuruste andmeühikutena. See on seni loodud väikseim biomeetriline šabloon. Kasutaja asetab oma peopesa metallist pinnale, mis juhitakse nagade taha. Kui käsi on korralikult nagade taga kinni, saab seadeldis lugeda käelt atribuute. Seejärel kontrollib seadeldis andmebaasist isiku vastavust. Kogu see protsess võtab tavaliselt vähem aega kui viis sekundit. Kui tundub, et kätt saab lisada süsteemi, siis praegustel käegeomeetria skanneritel puudub igasugune äratundmine, kas käsi on elavalt inimeselt või mitte ja järelikult saab seda ära petta vale käega, kui surve on rakendatud metallplaadile korrektselt.

Hinnang – käegeomeetrial on mitmeid tugevaid külgi. Kasutajatel on väga lihtne seda kasutada, piisab ainult käe asetamisest seadeldisele (joonis 4). Isikul ei ole vaja kellegagi suhelda, et saada ametlikku juurdepääsu. See on väga kiire ja see säästab raha kaardile baseeruvatelt süsteemidelt.

Samas on sellel biomeetrial ka mõningad puudused, milleks on riistvara kallis hind ja suurus. Samuti võivad mõjutada ka vigastused käel, mis muudavad raskeks lugeja efektiivsuse. Täpsuse puudumine peamistes nõuetes vajab omaette kinnitamist. Väikese hulga informatsiooni mõõtmisel on võimalik et korratakse lugemist, kui liiga palju inimesi on süsteemi andmebaasis, seepärast pole käegeomeetria küllalt tõhus identifitseerimis süsteem. (Hand Geometry, National Center for State Courts, 12.12.2007)

Joonis 4. Käegeomeetrial põhinev tuvastusseade
Allikas: Nationaltime systems 2008

2.5. Liikumisviis

Järjest enam kasvab huvi automatiseeritud tuvastusseadmete vastu, mis põhinevad liikumisviisil, tänu oma unikaalsetele võimalustele tuvastada isikuid kaugustest, kus teised biomeetriad pole võimelised. Selle tuvastamisvõimalusi toetavad õpinguid teistes valdkondades, nagu meditsiin (biomehaanika), matemaatika ja psühholoogia, mis vihjavad liikumisviisi unikaalsusele.

Tuvastamine põhineb (staatilisel) inimese vormil, milleks on liikumine (joonis 5), pakkudes rikkalikke tuvastamisvihjeid. Tihti saab liikumisviisi kasutada ainukese biomeetriana – kriminaalsetel kavatsustel võib motivatsioone varjata näoga, kuid on raske peita ja/või maskeerida oma liikumist loomulikule kaasneva liikumise reaktsiooniga.

Meditsiinilistest õpingutest tehti kindlaks paljud põhilised uskumused liikumisviisi analüüsimiseks. Need õpingud pakuvad välja, et liikumisviis on unikaalne subjekt. Psühholoogias õpetatakse, kuidas tuvastada inimeste liikumisviisi, ära tundmaks sõpru.

Varajased lähenemised kasutasid tunnustel-baseeruvat tehnoloogiat, kuid hiljem võeti kasutusele video kujutlus, samuti vaadeldi eristatuse võimalusi halbade valgustatud tingimustega. Siiski oli see piisavalt võimalik, et mõista liikumisviisi kui biomeetriat.

Varajastes lähenemistes puututi tuvastamisel kokku väheste inimestega, koos hulga piiratud andmetega, arvutamaks toimimist, mis oli siis saadaval. Paljusid tagaotsitavaid tuletati inimese siluetina kuvandist, millele otsiti kirjeldusi, ning seostati identifitseeritava subjektiga. See võis olla üks varasemaid lähenemisi automatiseeritud tuvastamisel liikumisviisist. Liikumisviisi signatuur tuletati ajalise mustrina liikuvast inimesest. Seda nimetati XT dimensiooniks (muundamine ja aeg), liikumisel on pea ja jalad erinevas asendis. Nende asendite kaudu otsustati keha liikumine hüplevatel kontuuridel ja siis see sobitati mudeliga. Liikumise omapära tuletati normaliseerides kohaldatud mudel kiirusega ja siis kasutati lineaarset interpolatsiooni, et tuletada normaliseeritud liikumisviisi vektor. Seda rakendati andmebaasis 26 erineval viisil viielt erinevalt subjektilt, erinevatel aegadel päeva jooksul. Sõltuvalt väärtustest kasutati kaalutletud faktoreid Eukleidese vahemaameetril, õige klassifikatsiooni hinnang piirdus 60%-lt protsendilt, kuni üle 80 protsendi, mis oli algus-aegadel üsna paljulubav. (Mark S. Nixon, John N. Carter, On Gait As a Biometric: Progress And Prosspects, 15.03.2008)

Tänapäeval kasutatakse uuenenud tehnikat inimkujundi liikumise analüüsimisel. See tehnika kasutab katmise funktsioone, et mõõta alasid, ajaliselt muutuvatel signaalidel silueti jadal, liikuvast subjektist. Põhiliselt see kombineerib endas lihtsuse, alusjooneliste alade mõõtmisest koos spetsiifiliselt valitud (kaetud) aladega. Dünaamiliselt ajalisi signaale kasutatakse signatuurina automaatse liikumisviisi tuvastamisel. Seda lähenemist on testitud seni suurimal liikumisviisi andmebaasil. Sisaldades endas 114 subjekti (filmitud laboratoorsetes tingimustes). Siiski individuaalsel maskeerimisel on piiratud osaliselt rakenduvad võimed, nagu õige klassifikatsiooni hinnang, üle 75% informatsiooni saadi kombineerimisel, erinevate alade maskeeringutelt. Teadmised jalast koos subjektiga, algab liikumisviisi tsükkel, mida näidatakse, et täiustada tuvastamise hinnangut individuaalsetel maskeeringutel, kuid omab väikest mõju tuvastamis hinnangule, mis teostatakse maskeeringu kombineerimisel. See tehnika sisaldab endas elementaarsust: tulevikku saab parandada, rakendades faktoreid, mis kasutavad paremat andmete kokkusobitamist ja klassifitseerimist, koos potensiaalsusega kasvavast eristamisvõimalustest. (Automatic gait recognition using area-based metrics, ScienceDirect, 13.03.2008)

Joonis 5. Liikumisviisil põhinev tuvastamine
Allikas: Andrew Blake 2008

2.6. Hääle tuvastamine

Hääle äratundmine on tehnoloogia, mis võimaldab kasutada enda häält sisendseadmes. Hääle äratundmist võib kasutada, et dikteerida teksti arvutisse või anda käsklusi arvutile (N. avada rakenduslikke programme, tõmmata alla menüüsi ja salvestada töid).

Vanemad hääletuvastusseadmed nõudsid, et iga sõna oleks eraldatud täiendava vaba ruumiga. See võimaldas masinal määratleda, kus üks sõna algas ja teine lõppes. Sellised hääletuvastamise seadmed on siiani kasutusel, et navigeerida arvuti süsteeme ja opereerida rakendusi nagu näiteks veebibrauseril.

Uuemad hääletuvastamise seadmed võimaldavad kasutajal dikteerida teksti soravalt arvutisse. Sellised uued rakendused võimaldavad kõnes ära tuua kuni 160 sõna ühes minutis. Rakendused, mis võimaldavad meil pidevat kõnet esitada on disainitud, et meelde jätta teksti ja formaliseerida see, ülejäänud töö teeb arvuti. (Voice Recognition, Rosistem Build Your Business, 11.03.2008)

Kuigi täpsus hääle äratundmise tehnoloogias on küll edasi arenenud viimase paari aastaga, kogevad mõned kasutajad siiani probleeme täpsusega, kas siis rääkimise stiilist või siis nende iseloomulikust häälest. (Understanding Voice Recognition, FindBiometrics.com, 10.01.2008)

Hääle äratundmise tehnoloogia kasutab iseloomulike aspekte hääle identsuse kinnitamiseks individuaalselt. Hääle äratundmine on aeg-ajalt häiritud kõne tuvastamisel tehnoloogia tõttu, mis tõlgib kasutaja poolt öeldut (see protsess ei ole seotud autentimisega).

Hääle äratundmisel saab kasutada igasuguseid audio edastusseadmeid, kaasa arvatud mobiil- ja lauatelefoni ja samuti ka lihtsat PC mikrofoni. Hääle äratundmissüsteemide kasutamine võib muutuda vastavalt audio signaali kvaliteedile ja samuti ka muutlikkusele registreerimisel tõstmisseadmete vahel ja seega tulevikus võib sealt autentimine olla keerulisem. Enne individuaalset registreerimist viidatakse, et kasutaja väljendaks järjestikust numbritejada, et kontrollida signaali kvaliteeti.

Hääle äratundmine kasutab närvivõrgustikku, et "õppida" ära tundma isiku häält. Kui isik räägib, siis hääle äratundmise tarkvara mäletab, nii nagu antud isik ütleb igat sõna. Selline kohaldamine nõuab hääle äratundmist, isegi kui kõik räägivad erineva aktsendiga ja erinevas käändes. Lisaks õppimisele kuidas hääldada sõnu, kasutab hääle äratundmise seade grammatilist konteksti ja sagedust, mida kasutatakse sõnade ennustamiseks. Need jõulised statistilised tööriistad võimaldavad tarkvaral välja lõigata massiivsest keelest andmeid, enne kui inimene suudab öelda järgmise sõna.

Kõnetehnoloogias on peamiseks probleemiks asjaolud, et inimestel on sarnased hääled ja hääl võib mingil põhjusel muutuda (haigus, emotsioonid, depressioon jne).

Järgnevalt on välja toodud hääle tehnoloogia tugevused ja nõrkused. Üks väljakutseid laiaulatuslikes rakendustes biomeetrias on see, et paigaldamaks uut riistvara on vaja eraldi töölisi, kliente ja kasutajaid. Üks tugevaid külgi telefonil baseeruvatel hääle tuvastamise rakendustel on see, et nendega on võimalik vältida seda probleemi, eriti kui need on veel elluviidavad helistamiskeskusel ja arvele juurdepääsu võimalustega. Ilma täiendava riistvarata kasutaja suhtes saab häälel baseeruvaid äratundmissüsteeme lihtsalt paigaldada alamprogrammiga läbi mille saab kõnesid suunata juba enne ligipääsu delikaatse informatsiooni tagamist. (Voice Recognition, Rosistem Build Your Business, 11.03.2008)

Häälel tuvastamisel on võimalik saada juurdepääse arvetele ja autentimist vajavatele protsessidele, leppides eelnevalt lihtsa mitte laialt levinud ja segadusse mitteajava autentimis-stsenaariumi kokku. Hääle ja kõne äratundmised saavad toimida samaaegselt, kasutades sama ütlust, võimaldades tehnoloogial sujuvalt seguneda. Häälel äratundmise funktsioon on usaldusväärne autentimismehhanism automatiseeritud telefonide süsteemidel, lisades

turvalisust automatiseeritud telefonil baseeruvatel tehingutel, nagu finantsteenustel ja tervishoius. (Speech Recognition and Voice Biometric Dictionary, Vee Commerce, 14.03.2008)

2.7. Käekiri

Minevikus ei olnud vajadust arvutiseeritud allkirja kinnitamiseks, kuna arvuteid ei olnud kasutuses igas meie elu valdkonnas. Viimaste aastatega on see aga muutunud ja lähitulevikus on see biomeetriline autentimine igapäevases kasutamises meile kõigile.

Käekirja äratundmist või siis ka allkirja äratundmist kutsutakse ka Dünaamiliseks Allikirja Kinnitamiseks. Allkirja äratundmine on protsess, kus kasutatakse äratundmaks individuaalset käsitsi kirjutatud allkirja. Dünaamiline allkirja kinnitamise tehnoloogia kasutab käitumuslikku biomeetriat käsitsi kirjutatud allkirjast, et kinnitada identsust arvuti kasutajaga. Mille ajal analüüsitakse vormi, kiirust, joont, pliiatsi survet ja informatsiooni ajastust allkirja kirjutamise momendil. Loomulik ja intuitiivne - seda tehnoloogiat on lihtne seletada ja usaldada. (Signature Recognition, Rosistem Build Your Business, 13.03.2008)

Asendades enda salasõna või pinkoodi numbri, dünaamilise allkirjaga on see biomeetriline tehnoloogia, mis kasutab isiku tõestamisel enda käsitsikirjutatud allkirja. (Understanding Signature Verification, FindBiometrics.com, 16.12.2007)

Peamine eelis allkirja kinnitamise süsteemidel teiste biomeetriliste süsteemide ees on see, et allkirjad on enne omaks võetud, kui tavalised meetodid identifitseerimiste rakendustel. Ajalugu näitab, et inimesed on väga vastuvõtlikud aktsepteerimaks allkirjal baseeruvaid tuvastusseadmeid. (Signature Recognition, Rosistem Build Your Business, 13.03.2008)

3. BIOMEETRILISE TEHNOLOOGIA VÕRDLUS

Töö kolmandas peatükis on võrdluseks ära toodud erinevate biomeetriliste seadmete töömetoodikad, kirje suurus, tuvastamistehingu aeg ja maksumus.

3.1. Seadmete kiirus ja tuvastamise täpsus

Enne kui soetada biomeetriline seadeldis tuleks kindlaks teha, milleks seda kasutada ja kui täpset tulemust on vaja tuvastamisel saada. Tabelis 3 on toodud nelja erineva enamlevinud biomeetrilise seadme võrdlused 2005. aasta seisuga, kus põhi- tähelepanu on pööratud tuvastamise täpsusele ja kiirusele.

Tabel 3. Erinevate biomeetriliste seadmete kiiruse ja täpsuse võrdlus.

Tehnoloo-giline tunnus	**Sõrmejälg**	**Silmaiiris**	**Nägu**	**Käsi**
Tööpõhimõte	Salvestab ja võrdleb sõrmeotsa mustreid	Salvestab ja võrdleb silmaiirise mustreid	Salvestab ja võrdleb näo mustreid	Mõõdab ja võrdleb käe ja sõrmede mõõtmeid
Seadme maksumus	Odav	Kallis	Odav	Keskmine
Tehingu aeg	9-19 sekundit	12 sekundit	10 sekundit	4-10 sekundit
Registreeri-mise aeg	~3 minutit, 30 sekundit	2 minutit, 15 sekundit	~3 minutit	~1 minut
Vale mitte sobivuse määramine	2-36%	1,9-6%	3,3-70%	0%-5%
Vale sobivuse määramine	0-8%	Vähem kui 1%	0,3-5%	0%-2,1%
Tegurid, mis mõjutavad esitlust	Määrdunud, kuivad või kulunud sõrmeotsad	Halb silmside, jõllitamine või peegeldused	Valgustus, näo orientatsioon ja päikseprillid	Käe vigastused, liigese põletik, pundumine
Muutlikus vanusele	Stabiilne	Stabiilne	Muutlik vanadusest	Stabiilne

Allikas: Global Security.org, Biometrics 2008

Nagu näha tabelist 3 omavad parimat tuvastamistäpsust silmaiirise ja käe geomeetrial põhinevad süsteemid. Samuti on samad seadmed parimad ka registreerimise kiiruse, kui ka tehingu toimumise aja poolest, kuid samas on need seadmed suhteliselt kallid. Kui aga täpsus

ja ajakulu ei ole nii tähtsad, siis võib valida odavama ja enimkasutatava variandi ehk siis sõrmejälje tuvastamisseade.

3.2. Biomeetriliste seadmete tugevad ja nõrgad küljed

Järgnevalt on välja toodud kuue enamlevinud biomeetriliste süsteemide eelised ja puudused.

Sõrmejälje tuvastamine

Tugevused: Kõige laialdasemalt levinud tehnoloogia. Kõrge täpsusega tõestatud tehnoloogia. Võimalus registreerida mitmeid sõrmi. Laiaulatuslik paigaldamine keskkonda.

Piirangud: Seadme täpsust võivad mõjutada kahjustatud või vigastatud sõrmejäljed. Võivad vajada täiendavat riist- või tarkvara.

Näo tuvastamine

Tugevused: Suured olemas olevad andmebaasid. Võib tegutseda ilma kasutaja nõusolekuta. Ainuke tehnoloogia, mis on võimeline identifitseerima isikut kaugustest.

Piirangud: Füsioloogiliselt muutuvad tunnused vähendavad sobivuse täpsust. Valgustus ja kaamera vaatenurk vähendavad sobivuse täpsust.

Käe geomeetria

Tugevused: Laialdaselt paigaldatav ja ajaliselt-testitud (1980 aastast alates). Väljakujunenud usaldusväärne tehnoloogia. Võimalik kasutada mitmetel üksustel. Tajudes ei ole pealetükkiv.

Piirangud: Disain raskendab kasutamist teatud populatsioonil. Võimalikud käe muudatused aja möödudes. Oht saada pisikuid.

Silmaiirisel tuvastamine

Tugevused: kõige täpsem biomeetriline tehnoloogia. Väga usaldusväärne käed-vaba süsteem.

Väga stabiilsed tunnused kogu elu jooksul. Edukad katsetused lennunduses. Silmaiiris on väga rikkalik biomeetrilisuse allikas.

Piirangud: Silmakujutise omandamine nõuab rohkem aega ja tähelepanu kui teised biomeetriad. Tark- ja riistvara litsentseerimine kallis. Tugevate läätsedega prillid võivad mõju avaldada esitusele. (Biometrics, Global Security.org, 13.03.2008)

3.3. Biomeetrilise kirje suurus

Andmete jäädvustamiseks biomeetrilisel sensoril võetakse tavaliselt nendest pildi vorm. Sõrmejälje tuvastamisel on pildi suuruse tulemuseks ligikaudu 1 kb, sõltuvalt sensori kvaliteedist. Suurtes süsteemides, kus on mitmeid tuhandeid kasutajaid on ladustamisnõuded, mis tagavad 1 kb suuruse šablooni salvestamise andmebaasis, väga suured. Et lahendada seda probleemi, toodetakse pilt sensoril hinnanguliselt ja iseloomulikud atribuudid ning nende kooskõlastamised salvestatakse. Sõrmejälgedel põhinevatel süsteemidel on iseloomulikeks tunnusteks "üksikasjad". Samuti ka kujutise tõlgendamisel sõrmejäljest kogusse, kus üksikasjad võimaldavad luua uuesti originaalse sõrmejälje. Võimalik on luua sõrmejälg, mis koosneb sarnastest tunnustest, punktidest kust üksikasju loetakse. Turvalisuse perspektiivis tuleb siiski meeles pidada, et süsteemi usaldusväärsus ei sõltu mitte ainult kujutise kvaliteedist, kuid samuti ka informatsiooni kogusest kujutisel, mis esineb šabloonil – mida rohkem atribuute on salvestatud šabloonile seda täpsem on identifitseerimine. Erinevate biomeetriliste seadmete šabloonide suurused on välja toodud tabelis 4.

Tabel 4. Biomeetrilise kirje suurus

Biomeetria	Šablooni suurus
Hääl	70-80k
Nägu	84-2k
Allkiri	500-1000b
Sõrmejälg	256-1,2k
Käe geomeetria	9b
Silmaiiris	256-512b
Võrkkest	96b

Allikas: Garfinkel,S.L. Computer Security, Privacy and Usability 2008

Mida rohkem informatsiooni on salvestatud šabloonile seda suuremaks see läheb. Selleks, et valida välja teatud hulk iseloomulike atribuute, mis mõjutavad šablooni suurust, kasutatakse algoritme.

4. MULTIMODAALNE BIOMEETRIA

Mille jaoks kasutada multimodaalset biomeetriat? (A. Ross, A.K. Jain, Multimodal Biometrics: An Overview, 18.02.2008):

- lubamatute vigade hindamisel, kasutades tavalist biomeetriat;
- lärmakad biomeetrilised andmed;
- vähendada ebaõnnestunud registreerimiste hinnangut;
- raskusi vale biomeetria töötlemisel.

4.1. Sissejuhatus multimodaalsesse biomeetriasse

Järgnev peatükk annab ülevaate erinevatest multimodaalsetest biomeetrilistest seadmetest ja nende kasutus võimalustest, alljärgnev tekst on koostatud West Virginia University professori A. Rossi ja Michigan State University professori A.K. Jaini poolt .

Biomeetrilised süsteemid, mis kasutavad üksikuid tunnuseid äratundmiseks (mittemodaalsed biomeetrilised süsteemid) on tihti mõjutatud mitme praktilise probleemi tõttu, nagu näiteks lärmakas andmete sensor, mitteuniversaalne või puuduv eristatavus biomeetrilisel tunnusel ja lubamatud vigade hinnangud. Multimodaalsetele biomeetrilistele süsteemidele üleminekul tugevdatakse mõningaid nendest probleemidest tõestuse saavutamisel erinevate allikate kaudu. Need allikad võivad olla mitmekordsed sensorid samalt biomeetrialt (optilistelt ja samalaadsetelt sõrmejälje sensoritelt), mitmekordse kasutajaliidesega sama biomeetria (sõrmejäljed erinevatelt sõrmedelt samalt isikult), mitmekordse hetkepildi saavutamine samalt biomeetrialt (neli jäljendid kasutaja parema sõrme kohta), mitmekordsed esituste ja sobivuste algoritmid sama biomeetria kohta (mitmekordne näo sobitavus), või mitmekordsed erinevad biomeetriad (nägu ja sõrmejälg).

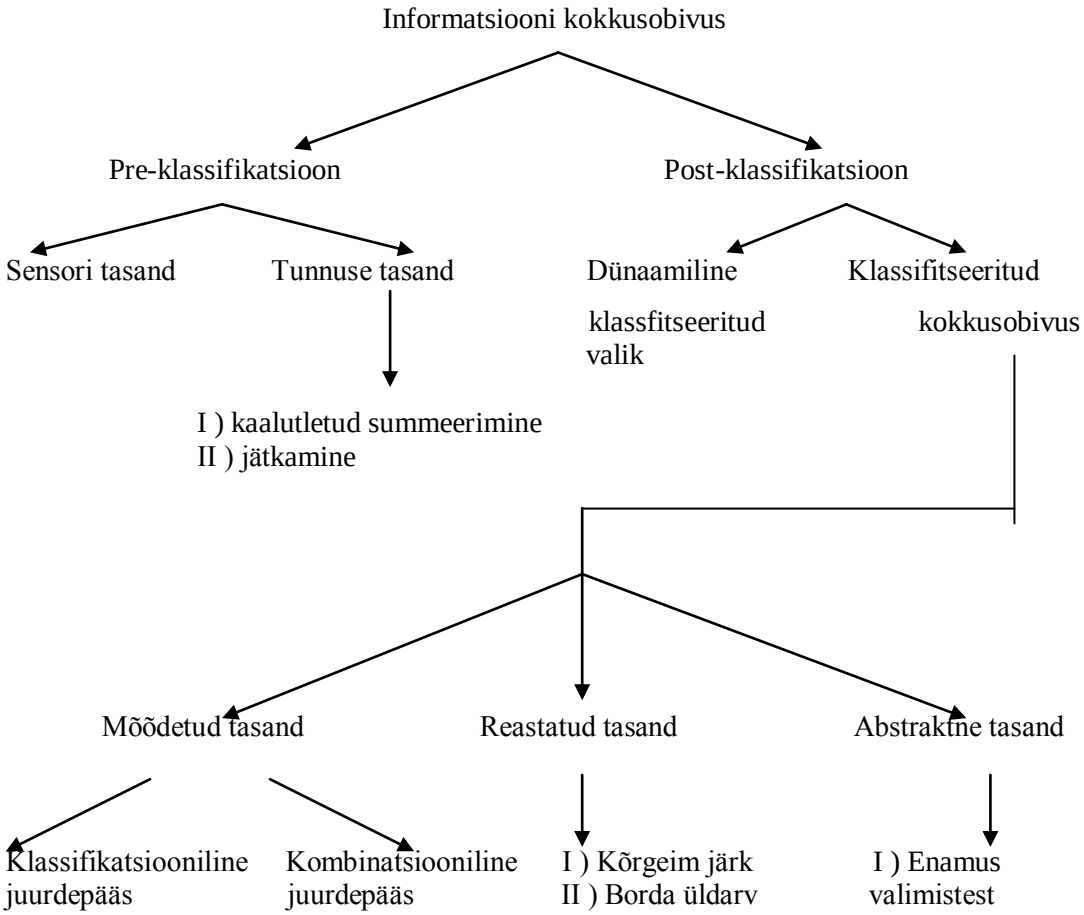
Mitmekordsete sensorite kasutamine kõrvaldab probleemid lärmakate sensoritega, kuid kõik teised potentsiaalsed probleemid, mis seostuvad mittemodaalsete biomeetriliste süsteemidega jäävad alles. Äratundmissüsteemid, mis töötavad mitmekordsetel astmetel sama biomeetriaga saab kindlustada kohalolekut otsese kasutajaga, paludes temalt tagada juhuslikku alamhulka biomeetrilisest mõõtmetest (vasakaule sõrmele järgneb parem sõrm). Samuti võidakse

kasutada mitmekordseid hetkepilte samast biomeetriast, või mitmekordseid esituste ja sobivuste algoritme samast biomeetriast, et täiustada tuvastuse toimimist seadmetel. Siiski kõik need meetodid kannatavad endiselt mitmete probleemide all, mis esinesid ka mittemodaalsetel süsteemidel.

4.2. Kokkusobivus multimodaalsel biomeetrial

Järgnevad andmed on valminud "Department of Computer Science and Engineering" lektorite poolt 2005 aastal, kus autorite poolt on lahti seletatud üksikasjaliselt multimodaalse biomeetria tuvastamisviisid.

Klassifitseeritud informatsiooni kokkusobivus biomeetrilistes süsteemides jaguneb kaheks suuremaks kategooriaks: pre-klassifikatsiooniliseks ja post-klassifikatsiooniliseks kokkusobivuseks. Pre-klassifikatsiooniline kokkusobivus viitab informatsiooni kombineerumisele, eelnevalt rakendusele klassifitseeruva või sobiva algoritmiga. Post-klassifikatsioonilisel kokkusobivusel on informatsioon kombineeritud pärast otsustamist, kui klassifitseerimine on saavutatud. Informatsiooni kokkusobivus multimodaalsel biomeetrial on näidatud joonisel 6.



III) Logistiline regressioon

II) Käitumuslikud tunnused
III) Dempster Shaferi teooria tõestused
IV) JA reegel
V) VÕI reegel

Joonis 6. Informatsiooni kokkusobivuse lähenemistee

Allikas: Score Normalization in Multimodal Biometric Systems 2008

Pre-klassifikatsiooniline kokkusobivus ja Post-klassifikatsiooniline kokkusobivus jagunevad omakorda neljaks erinevaks mooduliks: 1.) sensori moodul omandab biomeetrilisi andmeid kasutajalt 2.) tunnuseid väljavõttev moodul töötleb omandatud biomeetrilised andmed ja väljastab tunnuste hulga ja esindab seda 3.) sobivuse moodul võrdleb väljastatud tunnuste hulka salvestatud šabloonidega kasutades klassifitseeritud või sobivuse algoritmi, käsklusel genereerida sobiv tulemus 4.) otsustamise moodulis kasutatakse sobivaid tulemusi, kas identifitseerida registreeritud kasutaja või kinnitada kasutaja identsust.

4.2.1. Pre-klassifikatsiooniline kokkusobivus

Enne klassifiaktsiooni/sobivust toimub informatsiooni integratsioon, kas anduri tasemel või siis tunnuste tasemel. Toored andmed sensoril on kombineeritud sensori tasemeliseks kokkusobivuseks. Nagu näiteks näo kujutis saadakse mitmelt kaameralt, mis kombineeritakse üheks näo pildiks. Sensori tasemel kokkusobivusel saadakse andmed kätte erinevatelt sensoritelt, mis peavad omavahel kokku sobima, kuid see ei ole alati võimalik (ei ole võimalik kokku sobitada näo kujutisi, mis on saavutatud erinevate resolutsioonidega töötavate kaameratega).

Tunnuste tasemeline kokkusobimine eeldab erinevate tunnusvektorite kombineerimist, mis saadakse kasutades mitmekordseid sensoreid või mitmekordsete tunnuste väljavõttel algoritmide abil sama sensori andemetest. Kui tunnuse vektorid on homogeensed (mitmekordsed sõrmejälje kujutised kasutaja sõrmest) saadakse tulemuseks üksiktunnuse vektor, mida on võimalik arvutada kaalutud keskmisega individuaalsetest tunnuse vektoritest. Kui tunnuse vektorid on mitte-homogeensed (tunnuse vektoreid saadakse kasutades erinevaid väljavõtte tehnikaid), või tunnuse vektorid pärinevad erinevatelt biomeetrilistelt moodulitelt nagu näiteks näo- ja käegeomeetria, saame liita need üksikuks tunnuse vektoriks. Liitmine ei ole võimalik kui tunnuste hulk ei ühildu.

Biomeetrilised süsteemid, mille integreeritav informatsioon varajases staadiumis töödeldakse on efektiivsemad, kui need süsteemid, millel teostatakse integratsioon hilisemas staadiumis. Sellest ajast kui tunnused sisaldavad endas rikkalikumat informatsiooni sisendandmetest, kui sobiva tulemuse sobitamisest, peab integratsioon tunnuste tasemel tagama parema äratundmistulemuse, kui teiste tasemete integratsioonid. Siiski integratsiooni tunnuste tasemel on raske teostada praktikana järgmiste põhjuste tõttu:

a) Suhe tunnuste vahel erinevatel biomeetrilistel süsteemidel ei ole teada. See nõuab tunnuste valiku algoritmide eelnevat liigitust.

b) Enamus kommertsiaalseid biomeetrilisi süsteeme ei taga juurdepääsu tunnusvektoritele, mida nad kasutavad enda toodetes. Seega väga vähestel teadlastel on selge integratsioon tunnuste tasemele mille tõttu enamus neist eelistab peamiselt post-klassifikatsioonilist kokkusobivusskeemi.

4.2.2. Post-klassifikatsiooniline kokkusobivus

Skeemid informatsiooni integreerimisest pärast klassifikatsiooni/sobitamise taset jaotatakse neljaks kategooriaks: dünaamiline klassifitseeritud valik, kokkusobivus abstraktsel tasandil, kokkusobivus reastatud tasandil ja kokkusobivus sobiva tulemuse tasandil. Dünaamiline klassifitseeritud valiku skeemis valitakse tulemused, mida klassifitseeritakse ja kus enamasti antakse õige otsus kindla sisendnäidise põhjal. Seda tuntakse ka, kui võitja-võtab-kõik juurdepääsu ja seadeldist, mis teostab seda valikut, tuntakse seostava lüliti nime all.

Informatsiooni integreerimisest abstraktsel otsustuse tasemel, saab teostada, kui igal biomeetrilisel sobitamisel, otsustatakse eraldi paremal sobitamisel sisend šablooniga. Meetodid nagu enamus valimistest, käitumuslikel tunnetusel, Dempster Shaferi teeoria tõestustest, JA reegel ja VÕI reegel, võivad mõjutada lõpliku otsust.

Kui igal biomeetrilisel sobitamisel on väljundiks alamhulk võimalikest sobivatest variantidest järjestatakse need kahanevas järjekorras, kokkusobitamist teostab reastatud tase. Kõrgeimal reastatud meetodil on iga võimalik sobivus määratud kõrgeimal (miinimum) tasemel, mis arvutatakse erinevatel sobitamistel. Borda üldarvu meetod kasutab reastatuse summat, mis on määratud individuaalsel sobimisel, et välja arvutada kombineeritud rida. Logistiline regressiooni meetod on üldistatud Borda üldarvu meetod, kus on kaalutletud summa

individuaalsest reastatamisest välja arvutatud ja mille tulemusena tehakse kindlaks logistiline regressioon.

Kui tulemuseks on igal biomeetrilisel sobitamisel alamhulk võimalikest sobivustest, saab integratsiooni teostada sobiva tulemuse tasemel. Seda tuntakse kui ka kokkusobivust mõõdetud tasandil või konfidentsiaalsuse tasemest. Järgnevad tunnusvektorid, sobivate tunnuste tulemusest sisaldavad rikkaliku informatsiooni sisendmustrist. Samuti on sellel ka suhteliselt lihtne juurdepääs ja tulemusi kombineeritakse erinevatel sobimistel. Järelikult informatsiooni integratsioon sobiva tulemuse tasemel on kõige tavalisem lähenemine multimodaalsetel biomeetrilistel süsteemidel. Nii siis on selles ehtsuse kontrolli kontekstis olemas kaks põhilist lähenemist, et tugevdada tulemusi, mis saadakse erinevatel sobitamistel.

Esimesel lähenemisel formuleeritakse klassifikatsiooni probleem, samas kui teine lähenemine taltsutab kombinatsiooni probleemi. Klassifitseerimisel põhineval lähenemisel on tunnusvektor konstrueeritud kasutades sobivaid tulemusi individuaalsel sobitamisel. See tunnusvektor on konstrueeritud, kasutades sobivaid tulemusi individuaalse sobitajana. Klassifitseeritud tunnusvektor on jaotatud üheks-kahest klassist: “aktsepteeritud” (ehtne kasutaja) või “tagasi lükatud” (pettur).

Kombinatsioonilisel juurdepääsul on individuaalselt sobivad tulemused kombineeritud nii, et genereerida üksik skalaarne tulemus, mida siis kasutatakse, et langetada lõplik otsus.

5. TESTID BIOMEETRILISTE SEADMETEGA

Järgnevad katsed viidi läbi seitsme erineva biomeetrilise süsteemiga, *"National Physical Laboratory"*-s, maist-detsembrini, 2000. aastal. Testi programmi sponsoreeris *"Communications Electronics Security Group"* (CESG).

5.1. Ülevaade

Testprogrammi eesmärkideks olid:

- näidata toimimise taseme saavutatavust valitud biomeetriliste süsteemidega;
- määrata otstarbekust, demonstreerides rahuldatavuse kasutamist testimistel;
- edendada rohkem testimise sponsoreerimist ja edendada metoodilist kaasaaitamist biomeetrilise testimise täiustamiseks.

Näo, sõrmejälje, käegeomeetria, silmaiirise, käeveeni ja häälel tuvastamise süsteeme testiti positiivse identifitseerimise stsenaariumis, normaalses kontori keskkonnas koostöös tavakasutajatega. Hindamisel juhiti tähelepanu vastavalt "Parimad harjutused testimisel ja esitamise toimimist biomeetrilistel seadmetel", mis on toodetud "*UK Government Biometrics Working Group"*-i poolt. Testimiseks kasutati 200 vabatahtlikku inimest.

Tulemustes fikseeriti:

- tõrked ja nende esinemise hindamine;
- sobitavuse vead (vale sobiv vs. vale mitte sobiv) ja otsustamise vead (vale aktsepteeritavus vs. vale äraütlemine);
- läbilaske hindamine kasutajate poolt otsesel rakendusel, sobiva algoritmi lahtiühendamine töötlemisel;
- süsteemide tundlikkus, toimimine keskkonna tingimustes, erinevust toimimisel erinevate kasutajatega.

Biomeetriliste süsteemide toimimine sõltub rakendusest, keskkonnast ja rahvastikust. Järelikult toimimise tulemused, mis esitati ei olnud eeldatud haarama kõiki teisi rakendusi,

või kõiki keskkonna tingimusi. Ettevaatlik tuleb olla nende tulemuste võrdlemisel teiste süsteemidega, mis testiti teistes tingimustes.

5.2. Süsteemide valik

Testi programm kuulutati välja "Biomeetria Konsortsum" list serveri poolt ja lisaks osales selles ka 30 ettevõtet, kes vastasid üleskutsele testida oma seadmeid. Testi programmis katsetati umbes 20 erinevat süsteemi.

Kriteeriumid süsteemide valikust, mida testiti, lepiti kokku *CESG* ja *Biometrics Working Group*-i poolt:

- sõltumata tehnoloogiast, pidi valik olema laialdaselt kättesaadav ja tavakasutamiseks mõeldud;
- süsteemid pidid olema võimelised kohtumiseks elementaarsete CESG esinevate nõuetega;
- süsteemid pidid olema katseliselt tõestatavad, vastavalt kokkulepitud metoodikatele;
- tarnija pidi olema võimeline toetama katseid sõltumata nõutavast ajagraafikust.

Kasutades neid kriteeriume, valiti välja seitse erinevat süsteemi testimiseks, milleks olid näo, käe geomeetria, sõrmejälje, silmaiirise, veeni mustri ja häälel tuvastamine. Katsete juures kasutati kahte sõrmejälje tuvastamise süsteemi; üks kasutas optilist sõrmejälje salvestamist teine mahtuvustundliku sõrmejälje salvestamist (kiip1 ja kiip2). Tabel 5 annab põgusad detailid testitud süsteemidest. Süsteemid on välja toodud tarnijate nõusolekul avalikustada tulemused.

Tabel 5. Lühidetailid testitud süsteemidest

Lühinimetus	**Lühikirjeldus**
Nägu Nägu(2)	Visionics – Facelt Verification Demo Alternatiivsed registreerimised ja sobitamise algoritmid nende süsteemide jaoks
Sõrmejälg – kiip Sõmerjälg – kiip(2)	VeriTouch–vr-3(U) Alternatiivne registreerimise ja sobitamise algoritm - Infincon
Sõrmejälg - optiline	Sõrmejälje tuvastamise süsteem
Käsi	Tuvastamise süsteem – HandKey II

Silmaiiris	Irdiani tehnoloogia – IriScan system 2200
Veeni muster	Veenikontrollimise arengu prototüüp - Neuschiences-Biometrics
Hääl	SecurPBX süsteemi demonstratsioon - OTG

Allikas: Biometric Product Testing Final Report, National Physical Laboratory 2008

Nagu näha tabelist 5. kasutati ainult ühte seadeldist tehnoloogia kohta. Sel juhul tuleb märkida, et esitatud tulemused ei ole tingimata täielikult esindatud kõikidel süsteemidel, mis põhinevad samadel tüüpidel. Osutub, et isegi suhtelised väikesed muudatused süsteemide testimisel võivad anda märgatavalt erinevaid tulemusi.

5.3. Keskkond

Katseid teostati ruumis, mis oli eelnevalt tavakontorina kasutuses.

Valgustustase oli kontrollitud. Toa helendav valgus oli alati sees ja ribikardinad olid alati alla tõmmatud, et vähendada päevavalguse muutlikkusest tulenevat efekti. Seadeldised olid asetatud vastavalt nõudmistele toodete tarnijate poolt, ning kõige tundlikumad seaded valguse muutlikkuse suhtes paigutati akendest eemale. Sarnaselt oli üks seadeldis, mida kasutati, tundlik tausta müra suhtes, ning selle katsed toimusid vaiksemal alal, põhitestimise laboris.

Käsklused, mida kasutati seadeldistel, mõjutasid potentsiaalselt nende esitlust.

Saabudes laborisse, võis vabatahtlikel testijatel juhtuda, et nad hingeldasid (kui nad kiirustasid, et jõuda kohtumisele) või neil olid külmad käed/sõrmed (kui oli väljas külm), taastuti mõne minutiga rohkem loomulikku seisundisse.

Valgustus, näo tuvastamise süsteemidel, suurendas silmaiirise nähtavuse kogust (vähendas pupilli suurust), mis võis põhjustada võimalikke muutusi silmaiirise tuvastamisel.

Tagasisidet sõrmejälje seadeldisel võis mõjutada kasutaja käitumine (surve sõrmele).

Osad vabatahtlikud üritasid häält tuvastada, kui nad hingeldasid, need mõjutused ei ilmnenud oluliselt. Teisi käsklustel mõjutusi esines samamoodi, kuid need olid samuti ebaolulised. Tegevusi hääle süsteemidel ei teostatud enne, kuni vabatahtlikud olid tagasi saanud enda tavapärase hingamise.

5.4. Tõrked ja rikked

5.4.1. Tõrgete ennetamine

Vaatlused eeltestimisel näitasid, et tihti oli vaja rohkem, kui kahte katset, et teostada registreerimine. See paistis eriti silma hääle ja sõrmejälje tuvastamise süsteemidel, kus hea kvaliteediga kujutise saavutamine sõltus rohkem kasutaja käitumisest ja lähedusest.

Täiendavad protseduurid pandi paika, et vältida andmete kogumise rikkeid:

- rikked põhjustati vale käe, sõrmega jne;
- rikked omastati, üritades kasutada valet identsust.

Kasutajatel kästi alati tegevusi teostada õige sõrme, silma või käega, mis oli vastavalt kohaldatud. Ilma järjekindluseta oleks raske ülevaatajatel jälgida ja ära hoida vale sõrme, käe või silma registreerimist ja tuvastamist. Salvestatud kujutised võimaldasid edasisi kontrollimisi teostada õige silmaiirise, käe või sõrmega, mida kasutati.

Iga kasutaja varustati spetsiaalse PIN koodiga, mis oli välja antud katseteks ja oli näidatud iga kasutaja ankeedil igal katsel.

5.4.2. Tõrke registreerimine

Tõrke registreerimise hindamist mõõdeti süsteemidel individuaalselt, milline masinatest ei olnud võimeline genereerima korratavat šablooni. Tabelist lähtub, et kõige suurema tõrke registreerimisega olid sõrmejälje tuvastamise seadmed, millest mahtuvustundlikul sõrmejälje sensoril registreeriti tõrge (1%) ja optilisel sensoril registreeriti tõrge (2%) juhtudest, nendele järgnes silmaiirisel põhinev tuvastamise seade (0,5%). Ülejäänutel seadmetel registreerimisel tõrkeid ei esinenud. Tõrke registreerimise hinnangud erinevatel süsteemidel on näidatud tabelis 6.

Tabel 6. Tõrke registreerimise hinnangud.

Süsteem	**Tõrke registreerimise hinnang**
Nägu	0,0%
Sõrmejälg - mahtuvustundlik	1,0%
Sõrmejälg - optiline	2,0%
Käsi	0,0%
Silmaiiris	0,5%
Veen	0,0%
Hääl	0,0%

Allikas:Biometric Product Testing Final Report, National Physical Laboratory 2008

5.4.3. Tõrke omandamine

"Tõrke omandamises" mõõdeti katsete osakaalu süsteemidele, mis olid võimetud salvestama või asukohta määrama kujutisest, mis oleks olnud piisava kvaliteediga. Tõrke omandamisel oli kõige suurem ebastabiilsus ühekiibilisel sõrmejälje tuvastamisseadmel, kus vea hinnang oli (2,8%), sellele järgnes häälel tuvastamine (2,5%), kolmandal kohal oli optiline sõrmejälje skanner (0,8%) ja neljandal kiip(2), kus tõrget esines (0,4%) juhtudest. Ülejäänutel seadmetel puudusid tõrked.

Tabel 7. Tõrke omandamine

Süsteem	**Tõrke omandamise hinnang**
Nägu	0,0%
Sõrmejälg - kiip Sõrmejälg kiip(2)	2,8% 0,4%
Sõrmejälg - optiline	0,8%

Käsi	0,0%
Silmaiiris	0,0%
Veen	0,0%
Hääl	2,5%

Allikas: Biometric Product Testing Final Report, National Physical Laboratory 2008

5.5. Kasutaja läbilaske aeg

Aeg, mis kulus kasutaja läbilaskmiseks oli välja arvutatud kasutades ajalisi erinevusi järjestikuste tehingute vahel. Tabel 8 näitab maksimaalset, keskmist ja miinimaalset tehingute aega.

Näo tuvastamise süsteemidel kulus piltide jada kogumiseks minimaalselt 10 sekundit, salvestades paremini sobiva.

Kiibil põhinevad sõrmejälje süsteemid, kogusid pilte kuni oli üles leitud sobiv paariline või kuni lõppes ajalimiit.

Optilised sõrmejälje süsteemid skaneerisid sõrmejälge seni, kuni kujutis oli piisava kvaliteediga kätte saadud või kuni lõppes ajalimiit.

Käe geomeetrial põhinevad süsteemid nõudsid aeg-ajalt teise käe asetamist, kui tulemuses võis kahelda.

Silmaiirisel otsiti seni sobivat paarilist kuni see leiti või kui lõppes ajalimiit.

Silmaiirise seadmed töötasid normaalses tuvastamise režiimil, mitte nõudes PIN koodi sisestamist, tänu millele taandati tehingute aegasid.

Veeni süsteemidel ei olnud võimalik sisestada kiirelt PIN koodi, mistõttu selleks kulunud aeg mõjutas üldist tehingute aega.

Tehingu ajaks, hääle süsteemidel oli domineerivaks ajakulu, mis kulus kasutajatele tagasiside andmiseks.

Tabel 8. Tuvastamise tehingute aeg sekundites

Süsteem	**Tehingu aeg**			**Aeg, sisaldades PIN sissekannet**
	maksimaalne	**kekmine**	**minimaalne**	
Nägu	15	14	10	Välistatud
Sõrmejälg (optiline)	9	8	2	Välistatud
Sõrmejälg (kiip)	19	15	9	Välistatud
Käsi	10	8	4	Välistatud
Silmaiiris	12	10	4	Välistatud
Veen	18	16	11	Välistatud
Hääl	12	11	10	Välistatud

Allikas: Biometric Product Testing Final Report, National Physical Laboratory 2008

5.6. Kasutamise erinevused

Katseid sai liigitada järgmiselt:

- kas tehti registreerimise visiit, või teine ja kolmas visiit vabatahtliku kasutaja poolt;
- süsteemi kasutaja sugu;
- süsteemi kasutaja vanus;
- kas kasutaja kandis prille näo ja silmaiirisel põhinevate süsteemide katsetes;
- kasutaja pikkuse suhe häälesüsteemide kaugusest.

Kasutuse erinevusi, nende hulkade vahel analüüsiti ja nende kohta koostati vastav aruanne iga süsteemi kohta. Kasutajate erinevused on toodud tabelis 9.

Tabel 9. kasutajate erinevused.

Süsteem	Sugu	Vanus	Külastas	Muu
Nägu	M<N	noorem<vanem	registreerimine<hiljem	ilma<prillidega
Sõrmejälg kiip	M<N	noorem<vanem	registreerimine<hiljem	
Sõrmejälg kiip (2)	M<N	noorem<vanem	registreerimine<hiljem	
Sõrmejälg optiline	M<N	noorem<vanem	registreerimine<hiljem	
Käsi	M<N			
Silmaiiris				ilma<prillidega
Veen	M<N	noorem<vanem	registreerimine<hiljem	
Hääl	N<M	noorem<vanem	registreerimine<hiljem	

Allikas: Biometric Product Testing Final Report, National Physical Laboratory 2008

Üldjoontes oli meestel väiksem valede tagasilükkamiste hinnang kui naistel (hääle süsteemidel põhinevad seadmed olid ainukesed erandid) ja samuti oli ka noorematel vabatahtlikel madalam valede vastuste hinnang kui nende vanematel kolleegidel. Soolised erinevused ilmnesid rohkem näol, käel ja veenil põhinevatel süsteemidel ja vanuselised erinevused olid rohkem tähenduslikud sõrmejälgede tuvastamise süsteemidel.

Naisterahvad, kes olid üle 45 aasta vanad oli vabatahtlike seltskonnas vähem esindatud, tänu millele võib ka suhtuda tulemustesse erapooletult. Kuigi arvuliselt oli meeste ja naiste vahekord sama, võib vähesel määral kõrgem olla vale mittesobivuse hinnang. Kuid siiski, kui sarnased valesti sobivad tulemused olid suurema tõenäosusega samast soolisest klassist, siis toodavad need süsteemid valesti sobivaid tulemusi samal künnisel. (Tony Mansfield, Gavin Kelly, David Chandler, Jan Kane Biometric Product Testing Final Report, 15.01.2008)

6. TUVASTAMISE VIISI JA VARIANDI VALIK

Eesmärgiks on selgitada välja milline biomeetria on etteantud tingimustel sobivaim kasutamiseks. Täpsustada tuleks, et välja selgitatakse mitte ainult tuvastamise viis vaid ka konkreetne variant, sest ka sama tuvastamise viis annab erinevate parameetrite väärtuste korral erinevad tulemused (näiteks on osadel juhtudel võimalik saada suurem täpsus kasutades suuremaid šabloone või pikemat tuvastamise aega). Töö autori poolt on uuritud ja võrreldud omavahel enim kasutuses olevate biomeetriliste seadmete täpsust, kiirust, keskmist hinda ja šablooni suurust. Iga konkreetse seadmete kasutaja jaoks on nõudmised eespooltoodud omaduste suhtes vägagi erinevad, samuti on erinev raha hulk mida ollakse valmis tuvastamise teostamiseks kulutama. Seetõttu on paindlik lahendus selline, kus kasutaja sisestab just temale sobivad parameetrid, ning optimaalne lahendus leitakse vastavalt sisestatud parameetrite väärtustele.

NB: Et, tegemist on optimiseerimisülesandega, kus on vaja minimiseerida (maksimiseerida) mitut kriteeriumi samaaegselt, siis ei saa tingimata eeldada ühese lahendi leidmist.

6. 1. Optimiseerimisülesande üldine püstitus

On ilmne, et tegelikult sõltub ülesande püstitus ja sellest tulenevalt ka lahendus ikka sellest mida kõige olulisemaks peetakse. Antud töös on valitud optimiseerimise kriteeriumiteks tuvastamise täpsus ja hind. Samas on täiesti mõeldav, et tuvastamise aega arvestatakse kolmanda kriteeriumina või siis kasutatakse ühe arvesse võetud kriteeriumi (täpsuse või hinna) asemel. Põhimõtteliselt võib kasutada kriteeriumina ka šablooni suurust jne. Seetõttu esitame parima tuvastamisvariandi väljaselgitamiseks multikriteriaalse optimiseerimisülesande mõnevõrra üldisemal kujul, mis sisaldab väga erinevaid võimalusi. Ülesande püstituse esitamiseks on kasutatud järgmist allikmaterjali (Pohlak, M. Majak J., Karjust K, Küttner R. Optimization study of composite bathtub, Second International Conference on Multidisciplinary Design Optimization and Applications, Gijon, 2008):

Minimiseerida funktsiooni $F(\boldsymbol{x})$

$$\min F(\boldsymbol{x}) = (F_1(x), F_2(\boldsymbol{x}), \dots, F_l(\boldsymbol{x})), \quad (1)$$

$$\begin{cases} F_1(\boldsymbol{x}) = F_1(x_1, x_2, \dots, x_n) \to max, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ F_p(\boldsymbol{x}) = F_p(x_1, x_2, \dots, x_n) \to max, \\ F_{p+1}(\boldsymbol{x}) = F_{p+1}(x_1, x_2, \dots, x_n) \to min, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ F_l(\boldsymbol{x}) = F_l(x_1, x_2, \dots, x_n) \to min, \end{cases} \quad ($$

Etteantud kasutajapoolsete piirangute ehk lisakitsenduste korral

$$x_{i*} \le x_i \le x_i^*, \quad i = 1, \dots, m, \tag{4}$$

$$g_j(x) \le 0, \qquad j = 1, \dots, k. \tag{5}$$

Nagu eelnevast näha sisaldab minimiseeritav funktsioon $F(\boldsymbol{x})$ kokku l kriteeriumi, millest esimesed p on vaja maksimiseerida ja ülejäänud $l - p$ on vaja minimiseerida.

Valemites (1)-(5) tähistab $\boldsymbol{x}$ parameetrite vektorit ehk $\boldsymbol{x} = (x_1, x_2, \dots, x_n)$, selle vektori komponendid x_i $(i = 1, \dots, n)$ tähistavad kõikvõimalikke parameetreid, millest tuvastamise tulemus sõltub (aeg, šablooni suurus). Valemis (4) tähistavad x_{i*} ja x_i^* parameetri x_i väärtustele vastavat lubatut vähimat ja suurimat väärtust ning kitsenduste arv m on võetud kasutusele seepärast et kõigile parameetritele ei pruugi olla kitsendusi peale pandud ehk $m \le n$. Funktsioonid $g_j(x)$ on parameetrite vektorist ehk siis parameetritest sõltuvad funktsioonid, mis on esitatud sellisel kujul et paremale poole võrratust jääb null (selline esitus on tavaks optimiseerimisülesannete püstitamisel, kuna mitmed lahendustarkvarad eeldavad sellist esitust). Kitsendused (5) võivad olla nii lineaarsed kui ka mittelineaarsed.

Eespool on toodud optimiseerimisülesande üldine püstitus, mida ei saa koheselt numbriliselt lahendama hakata, sest täpsustamist vajab nii kriteeriumite kui ka kitsenduste konkreetne kuju.

6. 2. Optimiseerimisülesande konkreetne püstitus

Optimiseerimisülesande konkreetse püstituse all peame silmas seda, et valimtakse välja konkreetsed kriteeriumid mida minimiseerida (maksimiseerida) ning samuti lisakitsendused.

Nagu eespool märgitud on selleks mitmeid võimalusi, kuid töö autorile tundus ühe olulisema püstitusena, kus samaaegselt minimiseeritakse kulusid ja maksimiseeritakse täpsust. Seega valemid (1)-(2) omandavad lihtsma kuju

$$\min F(\boldsymbol{x}) = (F_1(x), F_2(\boldsymbol{x})), \tag{6}$$

$$\begin{cases} F_1(\boldsymbol{x}) = Täpsus(t,s,v) \to max, \\ F_2(\boldsymbol{x}) = Hind(t,s,v) \to min. \end{cases} \tag{7}$$

Lisakitsendused on rakendatud tuvastamise ajale t ja šablooni suurusele s, mida antud püstituses on vaadeldud parameetritena (kolmanda parameetrina on arvestatud tuvastamise viisi). Kitsendused (4) saavad kuju

$$0 \le t \le 15 \quad (sekundites), \tag{8}$$

$$0 \le s \le 1 \quad (kb), \tag{9}$$

kus $x_1 = t$, $x_2 = s$, $x_3 = v$ ning otsesed kitsendused on rakendatud kahele esimesele parameetrile. Selgituseks niipalju, et terminit „parameeter" on kasutatud muutuja tähenduses ehk parameeter ei tähenda fikseeritud väärtusega paramaatrit.

Parameetritest sõltuvad kitsendused (5) nii lihtsalt esitatavad pole, sest konkreetsete funktsioonide kuju on teadmata. Me teame vaid, et nii hind kui täpsus sõltuvad parameetritest t,s ja v aga täpsed valemid, mis neid seoseid väljendavad pole teada. Viimane fakt pole siiski otseseks takistuseks nii ülesande püstitamisel kui ka lahendamisel

$$g_1(t,s,v) = Hind(t,s,v) - H_0 \le 0 \ \ (EEK), \tag{10}$$

$$g_2(t,s,v) = T_0 - Täpsus(t,s,v) \le 0\,, \tag{11}$$

kus H_0 on hinna ülempiir ja T_0 on minimaalne lubatud väärtus täpsuse jaoks.

Lisame et teine kitsendus oli esialgsel kujul $Täpsus(t,s,v) \ge T_0$, kuid valemiga (5) kooskõlla viimiseks on teisendatud kujule (11).

Seega on optimiseerimisülesandes kasutatavad kriteeriumid ja lisakitsendused paika pandud, kuid sellegipoolest ei saa veel numbrilise ülesande lahendamisega tegelema hakata, sest esialgu on määramata kuidas koostada funktsioon $F(\boldsymbol{x})$, mis sõltub üksikutest kriteeriumitest. Mitme kriteeriumi samaaegne arvestamine optimiseerimisel on sedavõrd keeruline, et väga selget ühest lahendust on raske leida. Siinkohal kasutame funkstiooni $F(\boldsymbol{x})$ koostamiseks kahte enamlevinumat lähenemist (vt. järgmine lõik).

6. 3. Kaalutud summeerimise meetod

Kaalutud summeerimise meetod (weighted summation) on enimkasutatud ja lihtsaim formulatsioon mitmekriteriaalse optimiseerimisülesande lahendamiseks. (Hajkowicz, S., Higgins A. A comparison of multiple criteria analysis techniques for water resource management: Journal of Operational Research, 184, 255-265, 2008) Vältimaks sagedast viitamist samadele allikatele on korrektne täpsustada, et järgnevas optimiseerimisülesande analüüsis ja lahendamisel on kasutatud kahte viimati viidatud kirjanduse allikat. Kuna antud optimiseerimisülesandes kasutatavad kaks kriteeriumi on mõõdetavad erinevate ühikutega ja samuti erinevas suurusjärgus (hind kümnetes tuhandetes kroonides ja täpsus kuni 100 %) siis on mõistlik võtta kasutusele uued dimensioonita funktsioonid kujul:

$$f_1 = \frac{F_1^* - F_1(x)}{F_1^* - F_{1*}}, \quad f_2 = \frac{F_2(x) - F_{2*}}{F_2^* - F_{2*}}, \tag{12}$$

Kus alumine ja ülemine tärn funktsioonide indeksis tähendab vastavalt nende funktsioonide maksimaalset ja minimaalset väärtust. Mõningane erinevus nende kahe funktsiooni lugejas tuleneb sellest et funktsiooni $F_1(x)$ maksimiseeritakse ja funktsiooni $F_2(x)$ minimiseeritakse. Märkimist väärib asjaolu, et uute funktsioonide f_1 ja f_2 väärtused on vahemikus [0;1] ja neid mõlemaid tuleb minimiseerida. Muidugi on eeldatud et hind on positiivne ja täpsus alla 100%. Antud ülesande korral valime parimat lahendit olemasolevast diskreetsest hulgast ja seetõttu on viimane nõu>=0 ja täpsus<=100% automaatselt täidetud. Kaalutud summeerimise meetodi korral koostatakse minimiseeritav üksikute kriteeriumite korrutamisel kaaludega ja tulemuste liitmisel ehk antud juhul

$$f_{KSM} = \sum_{i=1}^{l} w_i f_i = w_1 f_1 + w_2 f_2, \tag{13}$$

kus w_1 ja w_2 on esimese ja teise kriteeriumi osatähtsust iseloomustavad kaalud mis rahuldavad järgmisi tingimusi:

$$w_1 + w_2 = 1, \quad 0 \le w_1 \le 1, \quad 0 \le w_2 \le 1. \tag{14}$$

Indeks KSM valemis (13) tähistab kaalutud summeerimise meetodit.

6. 4. Kompromissprogrammeerimise meetod

Kaalutud summeerimise meetod ei anna kahjuks alati head tulemust. Üks ilmseid põhjusi on selles, et lineaarne funktsioon (13) ei suuda katta keerulisi seoseid, mis üksikute kriteeriumite vahel võivad olla. Üks paindlikum, aga ka keerukam võimalus on kasutada kompromiss-programmeerimise meetodit millega tutvume veidi lähemalt järgnevas. Lähtudes kompromissprogrammeerimise reeglitest koostame minimiseeritava funktsiooni järgmiselt

$$f_{KPM} = [\sum_{i=1}^{m}(w_i f_i)^c]^{1/c} = [(w_1 f_1)^c + (w_2 f_2)^c]^{1/c}, \quad (15)$$

kus parameeter c iseloomustab maksimaalse kõrvalekalde tähtsust ja muud suurused omavad sama tähendust nagu eespool (v.a. indeks KPM, mis tähendab kompromissprogrammeerimise meetodit). Juhul kui $c>1$ on suuremad erinevused ideaalsest tulemusest „karistatud rangemalt" kui väiksemad kõrvale-kalded. Huvitav on teada, et erijuhul kui $c = 1$ realiseerub kaalutud summeerimise meetod. Tegelikult pole kompromissprogrammeerimise rakendamine ilmselt paljude ülesannete korral oluliselt raskem kaalutud summeerimise tehnoloogia rakendamisest, sest sageli on põhitööks funktsioonide f_1 ja f_2 väärtustamine.

6. 5. Optimaalsete väärtuste arvutamine ja tulemuste analüüs

Järgnevalt vaadeldakse optimiseerimisülesande lahendamist mõlema eespooltoodud funktsiooni abil ning analüüsitakse tulemusi. Kõigepealt täpsustus, et optimaalsete väärtuste arvutamiseks kasutatakse väga lihtsat viisi, väärtused arvutatakse välja kõigi „lubatud lahendite" jaoks. Terminit „lubatud lahendid" kasutatakse nende lahendite jaoks, mille korral kõik kitsendused on täidetud. Seejärel võrreldakse igale lähteandmete komplektile vastavat minimiseeritavat funktsiooni. Lähteandmete komplekti, mille korral minimiseeritava funktsiooni väärtus on vähim, loetakse optimaalseks. Antud lähenemise põhjuseks on asjaolu, et püstitatud ülesande korral võib eeldada suhteliselt väikest lähteandmete komplektide diskreetset hulka. Autori käsutuses olevad andmed piirduvad kümnetega ja ei ole ette näha et need võiksid tuhandetesse või miljonitesse kasvada. Minimiseeritava funktsioonina kasutatakse funktsioone (13) ja (15) ning võrreldakse tulemusi. Optimaalne lahend sõltub peamiselt sellest kuidas üksikuid kriteeriume kombineeritakse minimiseeritavaks funktsiooniks. Lähteandmed on toodud tabelis 10.

Tabel 10. Lähteandmed mõnede biomeetriliste seadmete jaoks

	Täpsus	**Aeg**	**Tuvastusviis**	**Keskmine hind**	**Šabloon**
Silma võrkkest	99,99999%	11s	1	5000$	300b
Silmaiiris	99,999%	10s	2	4000$	512b
Sõrme geomeetria	99,9%	12s	3	1200$	300b
Sõrme geomeetria	99,8%	13s	3	1000$	300b
Silmaiiris	99,98%	9s	2	3300$	512b
Käe geomeetria	98,5%	8s	4	2000$	9b
Allkirja dünaamika	98%	13s	5	150$	750b
Hääle dünaamika	98%	11s	6	200$	75kb
Näokuju	90%	14s	7	500$	2kb

Allikas: erinevate kirjandusallikate põhjal tehtud autoripoolne kokkuvõte

Tabel 11. Lähteandmetele vastavad lubatud lahendid

x1	**x2**	**x3**	**F1**	**F2**
Aeg	**Šabloon**	**Tuvastus viis**	**Täpsus**	**Hind**
11	300	1	99,99999	5000
10	512	2	99,999	4000
12	300	3	99,9	1200
13	300	3	99,8	1000
9	512	2	99,98	3300
8	9	4	98,5	2000
13	750	5	98	150
11	7500	6	98	200
14	2000	7	90	500

1. Kitsendused

			g2	**g1**
Kitsendus miinimum	0	0	1	95	
Kitsendus maksimum	15	1000	7		5000

Allikas: autori arvutused

Tabelite 10 ja 11 põhjal on näha, et kasutaja poolt määratud kitsenduste põhjal langevad välja tuvastusviisid hääle dünaamika ja näo kuju.

2. Kaalud $w1 = 0,2$ $w2 = 0,8$

3. Ideaalne ja halvim väärtus iga kriteeriumi jaoks

$F1^{*} = 100$ $F1_{*} = 95$ $F2^{*} = 5000$ $F2_{*} = 0$

4. Parameeter c ehk maksimaalse kõrvalekalde tähtsust hindav suurus (mida suurem c seda kõvemini on karistatud suuremad kõrvalekalded).

Kõrvalekaldele c = 2 vastavad tulemused on esitatud tabelis 12.

Tabel 12. Lahendustulemused (c=2).

f1	f2	f_KSM	f_KPM	Tuvastusviis
2E-06	1	0,8	0,8	Silma võrkkest
0,0002	0,8	0,64004	0,64	Silmaiiris
0,02	0,24	0,196	0,19204	Sõrme geomeetria
0,04	0,2	0,168	0,1602	Sõrme geomeetria
0,004	0,66	0,5288	0,528	Silmaiiris
0,3	0,4	0,38	0,32558	Käe geomeetria
0,4	0,03	0,104	0,08352	Allkirja dünaamika

Allikas: autori arvutused

Tabeli 12 põhjal selgub, et antud lähteandmete, kaalude (w1 = 0,2 w2 = 0,8) ja parameetri c (c=2) korral osutub nii kaalutud summeerimise meetodi kui ka kompromissprogrammeerimise meetodi korral sobivaimaks tuvastamise viisiks allkirja dünaamika.

Kui tabeli 12 korral olid ka kaalud fikseeritud (w1 = 0,2 w2 = 0,8) on järgnevalt tehtud arvutused varieerides kaalude väärtusi. Kõrvalekalde parameetri väärtuse c = 5, korral saadud tulemused on esitatud tabelis 13, kus on toodud juba ainult iga kaalu jaoks parimateks osutunud tuvastamise viisid.

Tabel 13. Parimad tuvastusviisid erinevate kaalude korral

w1	w2	f_KSM	f_KPM	Tuvastusviis
0,667	0,333	0,09326	0,066737	Sõrme geomeetria
0,5	0,5	0,12	0,100006	Sõrme geomeetria
0,333	0,667	0,14672	0,133202	Sõrme geomeetria; Allkirja dünaamika
0,2	0,8	0,104	0,080039	Sõrme geomeetria; Allkirja dünaamika

Allikas: autori arvutused

Nagu näha tabelist 13 osutusid antud kaalude väärtuste korral parimateks tuvastamise viisideks sõrme geomeetria ja allkirja dünaamika. Ehk lõpptulemus sõltub küll kaalude

valikust aga pole ka väga tundlik (sõrme geomeetria on siiski alati üheks parimaks lahenduseks).

KOKKUVÕTE

Käesoleva bakalaureusetöö eesmärk oli uurida ja võrrelda omavahel erinevaid biomeetrilisi autentimisvõimalusi, mida kasutatakse tänapäeval erinevates eluvaldkondades.

Isikuid on võimalik tuvastada mitmete erinevate biomeetriliste tunnuste abil. Erinevatel elualadel kasutatakse erinevaid biomeetrilisi meetodeid ja tihti mitut meetodit korraga. Igal biomeetrilisel tunnusel on oma tugevused ja nõrkused.

Samuti kuulus töö eesmärkide hulka selgitada välja, milline on parim biomeetriline autentimise viis etteantud tingimustel (täpsus, kiirus, hind, kasutuskõlblikkus jne.). Viimane ülesanne on aktuaalne sobivate autentimise seadmete soetamiseks.

Töö eesmärgi saavutamiseks on autori poolt analüüsitud kõige levinumaid biomeetrilisi autentimisvahendeid kahel erineval meetodil: kaalutud summeerimise meetodil ja kompromissprogrammeerimise meetodil. Autori poolt on uuritud ja võrreldud omavahel enim kasutuses olevate biomeetriliste seadmete täpsust, kiirust, keskmist hinda ja šablooni suurust.

Seatud eesmärkide saavutamiseks on formuleeritud optimiseerimise ülesanne ning pakutud lahendus vastavalt kliendi nõuetele ja piirangutele (muidugi ka lähteandmetele).

Rakendusnäitena on realiseeritud lahendus väikese lähteandmete komplekti korral, et kogu andmehulk ning samuti lahenduse realiseerimise protsess oleks lihtsamalt jälgitav. Ülesande keerukus seisneb asjaolus, et vaja on täita samaaegselt mitut erinevat kriteeriumi (minimaalne hind, maksimaalne täpsus). Seetõttu on formuleeritud multikriteriaalne optimiseerimise ülesanne. Antud probleemi korral oli kriteeriumite hindamine ja valik keerukamad, kui sellele järgnev parima lahendi leidmine (kasutatud lähteandmete hulk oli väike). Töös kasutatud lähteandmete, nõuete ning piirangute korral osutus parimaks lihtne ja odav allkirja dünaamikal põhinev autentimine (osadel juhtudel ka sõrme geomeetria), mis oli piisavalt täpne, kuid samas üks odavaimaid biomeetrial põhinevaid autentimise viise.

Peamiste tulemustena võib välja tuua (autoripoolne panus töös):

- parima biomeetrilise autentimise viisi määramise ülesande formuleerimine multikriteriaalse optimiseerimise ülesandena;

– multikriteriaalse optimiseerimisülesande lahendamine sõltuvalt lähteandmetest, nõuetest, piirangutest.

Autori püstitatud hüpotees, kõige optimaalsemaks autentimisviisiks osutub sõrme geomeetria, leidis osaliselt kinnitust. Erinevate kaalude korral osutus osadel juhtudel parimaks tuvastusviisiks sõrme geomeetria, kuid mõnedel juhtudel ka allkirja dünaamika. Ei olegi võimalik välja tuua üht konkreetset lahendit. Optimaalne biomeetriline autentimisviis sõltub etteantud kriteeriumitest nagu tuvastamise täpsus ja hind.

KASUTATUD KIRJANDUS

1. BBC News. Airport tests passenger eye ID's. [http://news.bbc.co.uk/1/hi/uk/1808187.stm]. 22. detsember 2007.

2. **Blackburn, D.M.** Face Recognition 101: A Brief Primer. [http://www.frvt.org/DLs/FR101.pdf]. 14. märts 2008.

3. **Blake, A.** Introduction to Active Contours and Visual Dynamics. [http://www.robots.ox.ac.uk/~vdg/dynamics.html]. 20. märts 2008.

4. FindBiometrics.com. Understanding Signature Verification. [http://www.findbiometrics.com/Pages/signature articles/signature_1.html]. 16. detsember 2007.

5. FindBiometrics.com. Understanding Voice Recognition. [http://www.findbiometrics.com/Pages/voice articles/voice_1.html]. 10. jaanuar 2008.

6. Federal Deposit Insurance Corporation. Putting an End to Account-Hijacking Identity Theft. [http://www.fdic.gov/consumers/consumer/idtheftstudy/technology.html]. 13. veebruar 2008.

7. **Garfinkel, S.L.** Computer Security, Privacy and Usability. [www.simson.net/ref/2004/csg357/handouts/L10_**biometrics**.ppt]. 13. märts 2008.

8. Global Security.org. Biometrics. [http://www.globalsecurity.org/security/systems/biometrics.htm]. 13. märts 2008.

9. **Henry, V.** GIAC Certified Professionals. Biometrics: Face Recognition Technology. [http://www.giac.org/practical/gsec/Veronica_Henry_GSEC.pdf]. 03. jaanuar 2008.

10. **Hajkowicz, S., Higgins, A.** (2008). A comparison of multiple criteria analysis techniques for water resource management. In European Journal of Operational Research. Lk 184, 255-265.

11. IEEE Xplore. Matching 2,5D face scans to 3D models. [http://ieeexplore.ieee.org/Xplore/login.jsp?url=/iel5/34/32932/01542029.pdf?isNumber=32932&arNumber=01542029&isnumber=32932&arnumber=01542029]. 12. märts 2008.

12. Irdian Technologies. Products. [http://www.iridiantech.com/products.php]. 09.märts 2008.

13. **Jain, A.K., Ross, A., Prabhakar, S.** An Introdution to Biometric Recognition. [http://www2.citer.wvu.edu/members/publications/files/RossBioIntro_CSVT2004.pdf]. 13. märts 2008.

14. **Mainguet, J.F.** Face Recognition/ Reconnaissance du visage. [http://pagesperso-orange.fr/fingerchip/biometrics/types/face.htm]. 05. veebruar 2008.

15. **Mansfield, T., Kelly, G., Chandler, D., Kane, J.** (2001). Biometric Product Testing Final Report.
[http://www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf]. 13. jaanuar 2008.
16. **Mets, O.** Biomeetria, sõrmejälgede tuvastus ja nende tuvastusseadmed.
[http://www.hot.ee/electronic/bio+.htm]. 05. jaanuar 2008.
17. National Center for State Courts. Hand Geometry. [http://ctl.ncsc.dni.us/biomet web/BMHand.html] 12. detsember 2007.
18. National Centre Of State Court. Iris Scan.
[http://ctl.ncsc.dni.us/biomet%20web/BMIris.html]. 11. märts 2008.
19. Nationaltime Systems. [http://www.nationaltime.com/nt1k_bap.html]. 22. märts 2008.
20. **Nixon, M.S., Carter, J.N.** On Gait As a Biometric: Progress And Prosspects.
[http://eprints.ecs.soton.ac.uk/10101/1/nixon_eusipco04.pdf]. 15. märts 2008.
21. Oki. Oki introduces the irispass-WG.
[http://www.oki.com/en/press/2002/z02011e.html%20]. 10. märts 2008.
22. **Pohlak, M., Majak, J., Karjust, K., Küttner, R.** Optimization study of composite bathtub, Second International Conference on Multidisciplinary Design Optimization and Applications. Gijon. 2008.
23. Rosistem Build Your Business. Fingerprint.
[http://www.barcode.ro/tutorials/biometrics/fingerprint.html]. 12. märts 2008.
24. Rosistem Build Your Business. Signature Recognition.
[http://www.barcode.ro/tutorials/biometrics/signature.html]. 13.märts 2008.
25. Rosistem Build Your Business. Voice Recognition.
[http://www.barcode.ro/tutorials/biometrics/voice.html]. 11. märts 2008.
26. **Ross, A., Jain, A. K.** Multimodal Biometrics: An Overview.
[http://biometrics.cse.msu.edu/Publications/Multibiometrics/RossJain_MultimodalOverview_EUSIPCO04.pdf]. 18. veebruar 2008.
27. Rycom. Iris Recognition Frequently Asked Questions.
[http://www.rycom.ca/index.php?section=2&sub1=2&sub2=2]. 28. veebruar 2008.
28. ScienceDirect. Automatic gait recognition using area-based metrics.
[http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6V15-48TMJSN-1&_user=10&_rdoc=1&_fmt=&_orig=search&_sort=d&view=c&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=1348c58c09c10d12fe68f20bcb1994aa]. 13. märts 2008.

29. Sourcesecurity.com. LG Irisacess 4000. [http://www.sourcesecurity.com/new-products/listing/1/product-profile/access-control/access-control-systems-and-kits.2/access-control-systems-and-kits/lg-iris-irisaccess-4000.html%20]. 10. märts 2008.
30. Transportation Security. The Eyes Have It. [http://transportationsec.com/ar/security_eyes/index.htm]. 10. märts 2008.
31. **Vare, J.** (2004). IBM loeb sõrmejälgi. Arvutimaailm, nr 10, lk 24-25.
32. Vee Commerce. Speech Recognition and Voice Biometric Dictionary. [http://www.vecommerce.com/faq/dictionary.aspx]. 14. märts 2008.
33. Western Carolina Univeristy. Iris and retinal identification. [http://et.wcu.edu/aidc/BioWebPages/Biometrics_Eye.html]. 12. märts 2008.
34. Winkpedia The Free Encyclopedia. Biometrics. [http://en.wikipedia.org/wiki/Biometrics]. 12. märts 2008.

RESUME

Title: Biometric Authentication Instruments

Author: Martin Tuude

Language: Estonian

Keywords: biometrics, authentication, template, fingerprint, hand geometry, multimodal, iris, voice, identity, environment, recognition

This bachelor's work contains 52 pages, including 13 tables and 6 figures. Used literature contains 34 different location pointers.

Biometrics are automated methods of recognising a person, based on a physiological or behavioural characteristic. Biometric-based authentication applications include workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and Web security.

One of the aims of this current work was to acquaint yourself the main basics of biometric authentication. The other aim was to find out which biometric is the best in case of given restrictions on speed, accuracy, cost and template size, etc. The solution of the problem is complex due to fact that several criteria must be applied silultanously.

In order to achieve desired purposes the multicriteria optimization problem has been formulated and solved. The weighted summation and compromise programming methods are applied for creating multicriteria objective function. An approach developed can be used in the case of different criteria, initial data, requirements and limitations defined by costumer.