KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

PROGRAMŲ INŽINERIJOS KATEDRA

Kęstutis Mačiulaitis

Biometrinių sistemų naudojimo saugumo tyrimas

Magistro darbas

Darbo vadovas:
Kęstutis Motiejūnas

Kaunas, 2009

KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

PROGRAMŲ INŽINERIJOS KATEDRA

Kęstutis Mačiulaitis

Biometrinių sistemų naudojimo saugumo tyrimas

Magistro darbas

Recenzentas

A. Ostreika

2009-05-25

Vadovas

doc. K. Motiejūnas

2009-05-25

Atliko

IFM-3/2 gr. stud.

Kęstutis Mačiulaitis

2009 05 25

Kaunas, 2009

TURINYS

1. ĮVADAS 6
   1.1. Kodėl biometrija? 6
   1.2. Kas yra biometrija? 7
   1.3. Asmenybės nustatymas, atpažinimas ir patikrinimas 8
2. KAIP BIOMETRINĖS SISTEMOS VEIKIA? 10
   2.1. Biometrijos sistemos struktūra 10
      2.1.1. Informacijos paėmimo dalis. 10
      2.1.2. Savybių paėmimo stadija 11
      2.1.3. Palyginimo stadija 11
      2.1.4. Apsisprendimo stadija 12
   2.2. Charakteristikų įvertinimas 12
   2.3. Biometrinių sistemų privalumai 13
   2.4. Kur naudojamos biometrinės sistemos 14
      2.4.1. Teisėsauga 15
      2.4.2. Seifų apsauga 15
      2.4.3. Parduotuvės ir aptarnavimo sfera 15
      2.4.4. Bankai 16
      2.4.5. Kompiuterių sistemos (dar žinoma kaip loginė prieigos kontrolė) 16
      2.4.6. Fizinis priėjimas 16
      2.4.7. Imigracija, sienos apsauga 17
      2.4.8. Akies rainelės biometrijos panaudojimas oro uostuose 17
      2.4.9. Nacionalinė tapatybė 19
      2.4.10. Ryšiai ir telefonija 20
      2.4.11. Laiko ir lankymo stebėjimas 20
   2.5. Kitos panaudojimo sritys 20
   2.6. Naujos biometrijos technologijos 21
      2.6.1. Ausyse „saugomi“ slaptažodžiai 21
      2.6.2. Vietoje pirštų atspaudų – prakaito lašeliai 22
3. NUOTOLINIO PRISIJUNGIMO NAUDOJANT BIOMETRIJĄ SISTEMA 24
   3.1. Projektas 24
   3.2. Situacijos Lietuvoje Įvertinimas 26
   3.3. Produkto apibūdinimas 26
      3.3.1. Programų sistemos funkcijos 26
      3.3.2. Vartotojo charakteristikos 26
      3.3.3. Vartotojo problemos 27
      3.3.4. Vartotojo tikslai 27
   3.4. Sukurtos sistemos vaizdas 27
      3.4.1. Sistemos konteksto diagrama 27
      3.4.2. Sistemos panaudojimo atvejų vaizdas 28
      3.4.3. Sistemos statinis vaizdas 29
      3.4.3.1. Apžvalga 29
      3.4.3.2. Vartotojo programinė dalis 30
      3.4.3.3. Serverio dalis 30
      3.4.3.4. Pirštų antspaudų nuskaitymo įrenginys 31
      3.4.4. Sistemos dinaminis vaizdas 31

3.4.4.1. Bendradarbiavimo diagramos ... 31
3.4.4.2. Būsenos diagrama ... 33
3.4.4.3. Sekų diagrama ... 33
3.4.4.4. Veiklos diagrama ... 34
3.5. Egzistuojančių sistemų palyginimo analizė ... 35
3.5.1. Microsoft Fingerprint Reader ... 35
3.5.2. Firefox Password Manager ... 36
3.5.3. PasswordSafe.com ... 36
3.6. Tolimesnio sistemos tobulinimo ir plėtojimo galimybės ... 37
4. BIOMETRINIŲ SISTEMŲ SAUGUMAS ... 38
4.1. Saugumas biometrinėse sistemose apskritai ... 38
4.2. Saugumas pirštų antspaudais paremtose sistemose ... 41
4.2.1. Pirštų antspaudų sistemų patikimumas ... 41
4.2.2. Nuotolinio prisijungimo naudojant biometriją sistemos tyrimas ... 41
4.2.3. Pirštų antspaudų sistemų apsaugų apėjimas ... 42
5. IŠVADOS ... 44
6. LITERATŪROS IR INFORMACIJOS ŠALTINIAI ... 45
7. TERMINŲ IR SANTRUMPŲ ŽODYNAS ... 47
8. PRIEDAI ... 48

Security Analysis of Using Biometrics

Summary

Biometrics finds more ways into personal and daily life in these days, than it was a decade before. This kind of technology is now used in shops, border control, put into credit cards and passports more and more, even it is possible to pay for one's meal using fingerprint. Researchers find more accurate, faster and less disturbing ways of how biometrics can be measured. Technology was invented and used to protect our daily life, but wrong and misleading usage of it will not give any good results. And with usage spreading, security concerns arise.

The objectives of this project was to learn the technology, develop remote access system using fingerprint biometrics as one way of practice use, and test the system in real life. Fingerprint biometrics was chosen because of availability and relatively low-cost value. During system analysis, main point was to investigate security concerns of such usage, and prepare the plan for further system development.

1. ĮVADAS

Tyrinėtojai, programuotojai ir paprasti vartotojai iškelia sau įvairių klausimų apie biometrijos technologiją. Ir vis daugiau žmonių įsitraukia į diskusijas apie vieną ar kitą biometrijos pritaikymo būdą. Žmonės iš skirtingų grupių žvelgia į šią technologiją įvairiai. O tyrėjai su dideliu susidomėjimu ieško naujų būdų, kaip būtų galima sumažinti ir apeiti problemas, kurios iškyla naudojant šią naujovišką technologiją. Po tokių aptarimų, kūno kvapas, klavišų paspaudimai, eisena ir kitos biometrinės savybės neseniai buvo pradėtos taikyti, norint identifikuoti asmenis. Bet šie nauji metodai yra vis dar projektavimo stadijoje. Rinkos standartai, realaus laiko našumas, didelio masto projektų efektyvumas ir žmonių priešiškumas sukelia dideles problemas programų kūrėjams. Vartotojai, kurie naudojasi biometrinėmis sistemomis, nori žinoti, ar sistema gali nors kiek pakenkti jų organizmui, paveikti jų privatumą ar tiesiog sistemos vartotojo sąsaja yra draugiška. Nepaisant to, kad skirtingos grupės žmonių į biometriją žiūri skirtingai, vienas dalykas tarp jų yra bendras – biometrija sulaukia vis daugiau dėmesio.

1.1. Kodėl biometrija?

Kartu su šiuolaikinio gyvenimo automatizavimu iškyla vis didesni reikalavimai saugumui. Kiekvieną dieną daugybę kartų užduodami klausimai: „Ar šis asmuo turi teisę patekti į šią saugią sistemą?“, „Ar šis asmuo turi pakankamas teises atliktį tam tikrą veiksmą?“, „Ar šis asmuo yra mūsų valstybės pilietis?“. Klausiant bandoma išsiaiškinti tą pačią saugumo problemą – kaip teisingai identifikuoti žmones.

Šiuo metu yra keli populiarūs būdai tokių problemų sprendimui. Vienas susijęs su „kažkuo, ką mes turime“, tai gali būti kortelės, saugumo raktai, ir pan., o kitas priklauso nuo „ką mes žinome“, tai slaptažodžiai, įvairūs prisijungimo kodai ir panaši informacija. Abu šie sprendimo būdai suteikia įgaliojimus tam tikriems daiktams, ar tai yra įėjimo kortelės, ar slaptažodžiai, tačiau ne pačiam asmeniui. Jei asmuo gauna kokią nors prisijungimo informaciją, jis gauna įgaliojimus, priešingu atveju jis jų neturi. Taikant tokią saugumo politiką, žmonės su savimi turi nešiotis įvairias korteles ir prisiminti dešimtis slaptažodžių. Kortelės praradimas ar slaptažodžio užmiršimas gali vartotojui sukelti didelių problemų. Pavyzdžiui, bankai, įvairios ryšių bendrovės ir vyriausybės institucijos patiria didelius metinius nuostolius dėl esamų kortelių ar slaptažodžių saugumo sistemų pažeidimų.

Tyrėjai, norėdami išspręsti šią problemą, pasitelkia įvairias priemones, tačiau biometrijos naudojimas yra daugiausiai žadantis. Biometrija turėtų būti technologija, kuri, pasinaudodama

žmogaus unikaliomis fizinėmis ar elgesio savybėmis, juos atskiria vieną nuo kito, arba teisingai identifikuoja. Biometrija remiasi „kuo mes esame“, duodama mums tam tikrus įgaliojimus priėjimui prie tam tikrų sistemų, todėl gali natūraliai atskirti įgaliotus asmenis nuo apsišaukėlių [3]. Kadangi asmens unikalios savybės negali būti pavogtos, užmirštos, nukopijuotos, pasidalintos ar susektos, biometrija paremtų saugumo sistemų yra beveik neįmanoma suklastoti.

1.2. Kas yra biometrija?

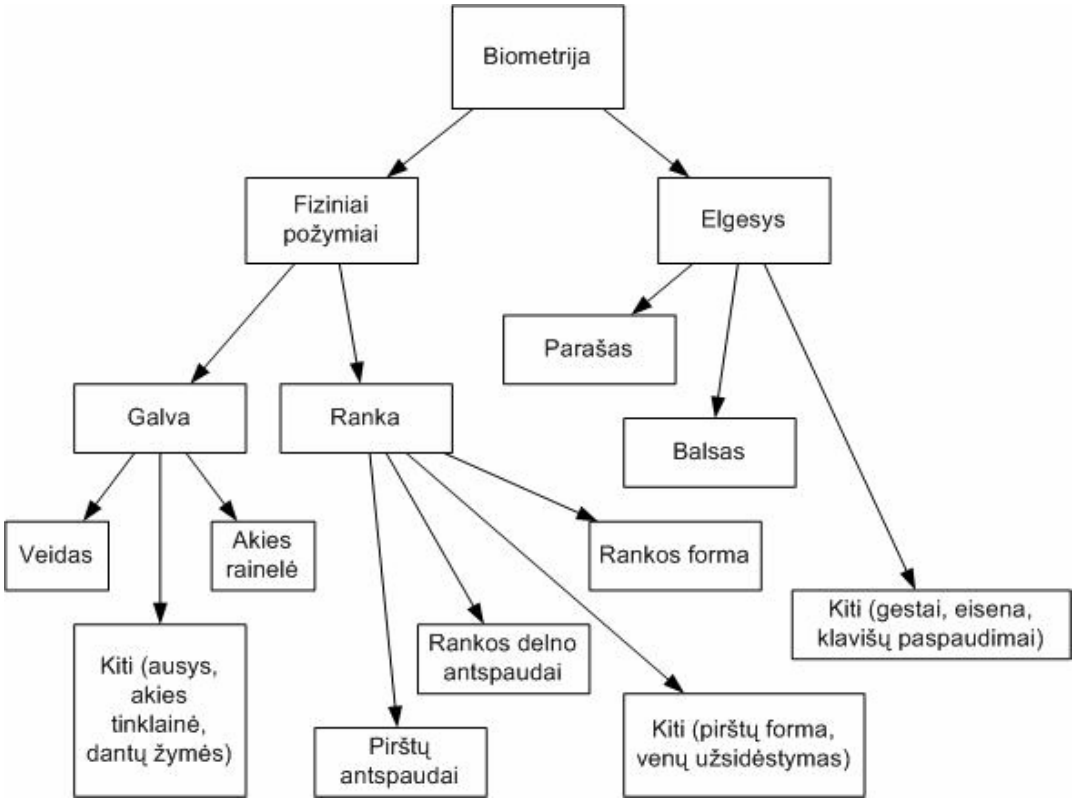
Sąvoka „biometrija“, apskritai, aprašo mokslą, apimantį statistinę biologinių požymių analizę. Tačiau, kompiuterių mokslas yra dažniau susijęs su technologijomis, kurios analizuoja žmogaus savybes automatiniam atpažinimui ar nustatant tapatybę, kur biometrija yra fizinių ar elgesio savybių matavimas. Fizinės ar elgesio savybės, pasirinktos nustatant tapatybę bendrai, atitinka tokias sąlygas:

- *Universalumas*, kuris parodo jog kiekvienas žmogus turi turėti tokią savybę;
- *Unikalumas*, reiškiantis, kad bet kurie du žmonės turi būti pakankamai skirtingi, atsižvelgiant tik į šią savybę;
- *Pastovumas*, parodantis, jog savybė turi būti pakankamai atspari ir nekintanti bėgant laikui ar keičiantis aplinkos sąlygoms;
- *Renkamumas*, reiškia paimtą savybių požymį esant suskaičiuojamam;
- *Priimtinumas,* tai kiek žmonėms yra priimtinas toks požymio rinkimas;
- *Atlikimas*, reiškiantis pasiekiamą identifikacijos tikslumą, išteklių poreikį, norint pasiekti tokį tikslumą, ir darbo ar aplinkos požymiai, kurie veikia identifikacijos tikslumą.
- *Apėjimas*, kuris parodo kaip lengva yra apgauti sistemą apgaulingais metodais.

Ar žmogaus savybė yra tinkama biometrijos sistemai, gali būti nustatoma tik po plataus mąsto ir geros kokybės testų.

Kalbant apie biometriją, turbūt pirmas iškylantis vaizdas yra pirštų antspaudai, tačiau biometrija tikrai neapsiriboja tuo. Bendrai, fizinės ir elgesio savybės, naudojamos biometrijoje, apima tokias savybes (žr. pav. 1)

- Fizinės savybės: cheminė kūno kvapo sudėtis, veido geometrija ir šilumos pasiskirstymas, akies rainelės ar tinklainės savybės, pirštų antspaudai, delno atspaudai, rankos forma, odos porų išsidėstymas, riešo ar rankos venos;
- Elgesio savybės: asmens parašas, teksto rinkimas klaviatūra, balso spektrograma, eisena, gestai.



Pav. 1. Biometrijos rūšys pagal duomenų pasiskirstymą

1.3. Asmenybės nustatymas, atpažinimas ir patikrinimas

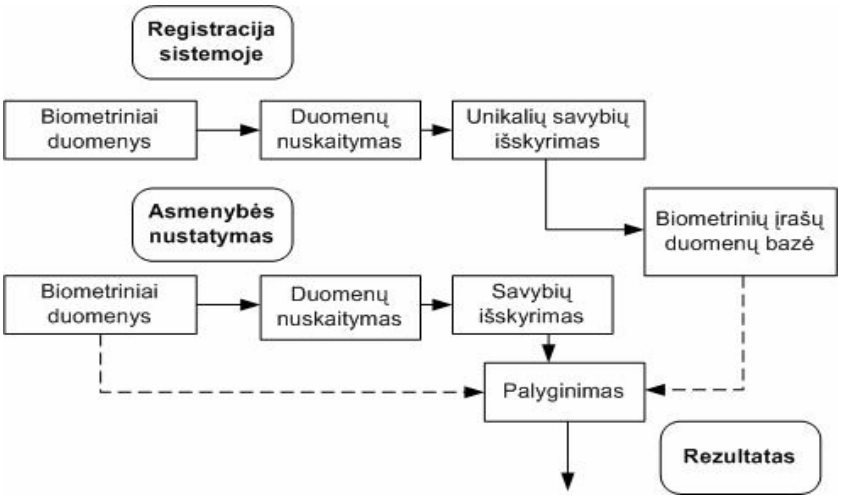
Reikia aiškiai nustatyti skirtumus tarp šių trijų sąvokų: nustatymas (*identification*), atpažinimas (*recognition*) ir patikrinimas (*verification*), kadangi kalbant apie biometriją, visi šie trys terminai yra dažnai sutinkami ir vartojami. Nustatymas ir atpažinimas gali būti grupuojami drauge. Nustatymo sistema atsako į klausimą „Kas aš esu?“, o patikrinimo sistema atsako į klausimą „Ar aš esu tuo, kuo deduosi?“.[6-11].

Asmenybės nustatymo sistemose dažniausiai yra naudojama didžiulė duomenų bazė, sauganti tūkstančius biometrinių įrašų apie asmenis. Nustatymo procesas (žr. Pav. 2):

- Asmuo įveda savo biometrinius duomenis į sistemą.
- Sistema apdoroja surinktą informaciją, gaudama tam tikrus kontrolinius duomenis, kuriuos paskui galima palyginti su kitais duomenimis, esančiais duomenų bazėje.
- Sistema pateikia rezultatą, ar asmuo yra tas, kuo dedasi, ar ne. Sistema taip pat gali nustatyti, kas jis yra iš tikrųjų.

Patikrinimo sistemoms nebūtina turėti didžiules duomenų bazes, nes tokios sistemos tikslas – patikrinti, ar asmuo yra tikrai tas, ar ne. Sistemos veikimo principas:

- Tikrinamasis asmuo įveda savo slaptažodį ar pateikia nuskaitymui savo kortelę.
- Sistema nuskaito jo biometrinius požymius.
- Biometriniai požymiai yra sulyginami su tais, kuriuos nurodo kortelė ar slaptažodis.
- Sistema išduoda patikrinimo rezultatą, ar asmuo yra tas, kuris nurodytas ant kortelės, ar ne tas.



Pav. 2 Automatinė asmenybės nustatymo sistema

2. KAIP BIOMETRINĖS SISTEMOS VEIKIA?

2.1. Biometrijos sistemos struktūra

Bendrai, visos biometrijos sistemos savyje turi dvi dalis: registracijos ir nustatymo. Registracijos dalies funkcijų paskirtis - užregistruoti vartotojo biometrines savybes, kurias vėliau bus galima panaudoti kaip duomenis atpažinimo procese. Nustatymo dalis pateikia vartotojo sąsają ir funkcijas, kuriomis galima paimti vartotojo biometrinę informaciją, ją sutikrinti su ankščiau įvestąja, ir bandyti nustatyti vartotoją. Nors skirtingos sistemos naudoja skirtingus biometrinius duomenis ir su jais atlieka skirtingas operacijas, tačiau pati biometrinių sistemų esmė išlieka ta pati ir esminės funkcijos lieka tos pačios. Vartotojo įvedimo dalyje procedūros susideda iš informacijos paėmimo, savybių išskyrimo ir saugojimo. Nustatymo dalies procedūra yra sudaroma iš keturių dalių: informacijos paėmimo, savybių išskyrimo, sulyginimo ir sprendimo.

Kadangi informacijos paėmimo ir savybių išskyrimo dalys registracijos ir nustatymo procedūrose yra tokios pačios, todėl, paprastai, kuriant biometrines sistemas, visas dėmesys telkiamas asmenybės nustatymui.

2.1.1. Informacijos paėmimo dalis.

Tai procesas, kai asmenybės biometrijos fizinės ar elgesio savybės yra įvedamos į sistemą. Skirtingos sistemos naudoja skirtingus įrenginius paimant duomenis. Originalūs įrenginio signalai tuomet yra paverčiami į skaitmeninius, be jokio arba su menku pradiniu apdorojimu. Apskritai, fiziniai biometriniai duomenys yra paimami vienokio ar kitokio tipo kameromis ir yra išsaugomi tolimesniam apdorojimui skaitmeniniu pavidalu kaip paveikslėlis. Vaizdo kameros naudojamos, paimant akies rainelės ir veido formos duomenis, tuo tarpu šilumai jautrios kameros naudojamos, paimti veido ar rankos šilumos pasiskirstymo vaizdą.

Automatinis pirštų antspaudų atpažinimas turi pakankamai ilgą istoriją, todėl rinkoje galima sutikti įvairaus tipo, specialių gaminamų ir parduodamų įrenginių. Vieno tipo įrenginiuose yra įmontuota vaizdo kamera, kito tipo įrenginiuose galima aptikti šilumai jautrius daviklius. Akies rainelės duomenų paėmimo įrenginys yra speciali kamera su labai aiškia ir tikslia šviesa. Asmens elgesio savybių įrenginiai tarpusavyje skirtingi. Balsu paremtos sistemos naudoja tik kompiuterio garsiakalbius, o sistemoms, naudojančioms elektroninį parašą, reikalinga tik parašo lentelė. Duomenų paėmimas - pati pirma automatinių asmens atpažinimo procesų stadija, todėl labai svarbi paimtų duomenų kokybė, kuo ji geresnė ir turi mažiau pašalinių veiksnių ar triukšmų, tuo geriau.

2.1.2. Savybių paėmimo stadija

Savybių paėmimas - tai procesas, kurio metu iš pradinių duomenų išgaunama unikali informacija ir iš jos padaromas šio asmens biometrinių duomenų šablonas. Šablonai iš duomenų, paimtų skirtingų asmenų turi pakankamai skirtis, o tokių pačių duomenų šablonai paimti kelis kartus iš to paties asmens turi būti kiek galima daugiau panašūs.

Išgaunant informacijos šablonus yra naudojami dviejų tipų metodai. Vienas iš jų, kai išgaunamas ir patvirtinamas reikšmingų vienetinių požymių rinkinys. Tai gali būti odos rievės, poros ant pirštų antspaudų arba akys, burna, nosis, ausys veide. Tuomet šioje stadijoje šios savybės gali būti išgaunamos ir paverčiamos kokiu nors matematiniu pavidalu. Toks būdas yra naudojamas daugelyje vaizdų apdorojimo algoritmų, paimant esmines savybes iš duomenų.

Antras būdas, kai jokių reikšmingų požymių nerandama, ir pradiniai duomenys yra pertvarkomi į kitokių matmenų ir svarbos informaciją, kuomet triukšmo lygis yra sumažinamas ir visas bendras informacijos kiekis sumažėja. Gaunama apvalyta informacija. Tuomet yra atliekami daugkartiniai testai ir pastebima, jog vieno asmens išvalyta biometrinė informacija labai mažai varijuoja tarpusavyje ir pakankamai daug skiriasi tarp dviejų skirtingų asmenų tos pačios rūšies informacijos. Po šių testų išvalytoji informacija tampa šablonu. Šis būdas naudojamas balso, akies rainelės, akies tinklainės, ir kai kurių veido bruožų atpažinime. Furjė Transformacija ir Dažninės srities transformacija - pagrindiniai algoritmai, naudojantys šį metodą. Tai tarsi statistinis tradicinių šablonų atpažinimo tam tikru laipsniu būdas.

2.1.3. Palyginimo stadija

Šioje proceso stadijoje naujai išgautas šablonas yra palyginamas su seniau išgautais pavyzdžiais, saugomais sistemoje. Kadangi duomenys, išgauti iš vieno žmogaus, per tam tikrą laiką gali šiek tiek pakisti, naudojamas algoritmas turi toleruoti tokius mažus pokyčius, tačiau aiškiai atskirti gautus duomenis iš skirtingų asmenų. Pavyzdžiui, pirštas gali kontaktuoti su piršto antspaudo nuskaitymo įrenginiu įvairiais paspaudimo laipsniais, kampais, pasukimais, skirtingose vietose, todėl, praktiškai, nė viena pora duomenų nebus tokia pat.

Biometrijos sistemos yra skirstomos į dvi kategorijas - tai asmenybės nustatymo arba patikrinimo sistemos. Nustatymas reiškia, jog naujai įvesti duomenys ir iš jų išgautas unikalus šablonas turi būti patikrinamas su visais kitais sistemoje registruotais šablonais, tuo tarpu patikrinimas reiškia jog nauji duomenys bus tikrinami tik su tam tikrais sistemoje registruotais įrašais. Nustatymo sistemose verta registruotus vartotojus skirstyti į tam tikras grupes, kad visas palyginimo procesas neužimtų daugiau laiko nei reikia.

2.1.4. Apsisprendimo stadija

Šioje proceso stadijoje sistema nusprendžia, ar naujai gautas šablonas, išskirtas iš nuskaitytų biometrinių duomenų, atitinka esantį sistemoje. Tam tikras atitikimo laipsnis yra pasiekiamas lyginant naujus duomenis su esamais. Tam kad būtų galima pateikti atsakymą „taip“ arba „ne“, yra nustatomas slenkstis. Kada atitikimo laipsnis yra didesnis nei slenksčio reikšmė, atsakymas būna teigiamas, priešingu atveju – neigiamas.

2.2. Charakteristikų įvertinimas

Kai biometrijos sistema yra paleidžiama veikti, ji arba ras arba neras atitikmenį tarp jau registruotų įrašų ir naujos informacijos. Šiam palyginimui yra duodamas tam tikras įvertinimas. Jei rezultatas yra didesnis nei slenkstis, tada manoma, jog palyginimas sėkmingas ar atitikmuo rastas, atsižvelgiant į sistemos paskirtį. Ši metodika biometrijai suteikia daug daugiau lankstumo, nei „taip arba ne“ būdas, naudojamas slaptažodžiais ar prieigos kodais paremtose sistemose.

Biometrijos pramonėje jau daug metų naudojamos dvi charakteristikos, reikalingos atitikimo tikslumą nusakymui [12]. Šie įverčiai dar žinomi kaip klaidingo atmetimo laipsnis *(False Rejection Rate (FRR))* ir klaidingo priėmimo laipsnis *(False Acceptance Rate (FAR))*. FRR dar yra žinomas kaip pirmo tipo klaidų koeficientas, o FAR – antro tipo klaidų koeficientas. FRR dydis pažymi, bandymų prisijungti skaičių, kuomet įgaliotas vartotojas yra klaidingai atmetamas. FAR, savo ruožtu, reiškia prisijungimų skaičių, kuomet neturintis teisės asmuo per klaidą patenka į sistemą.

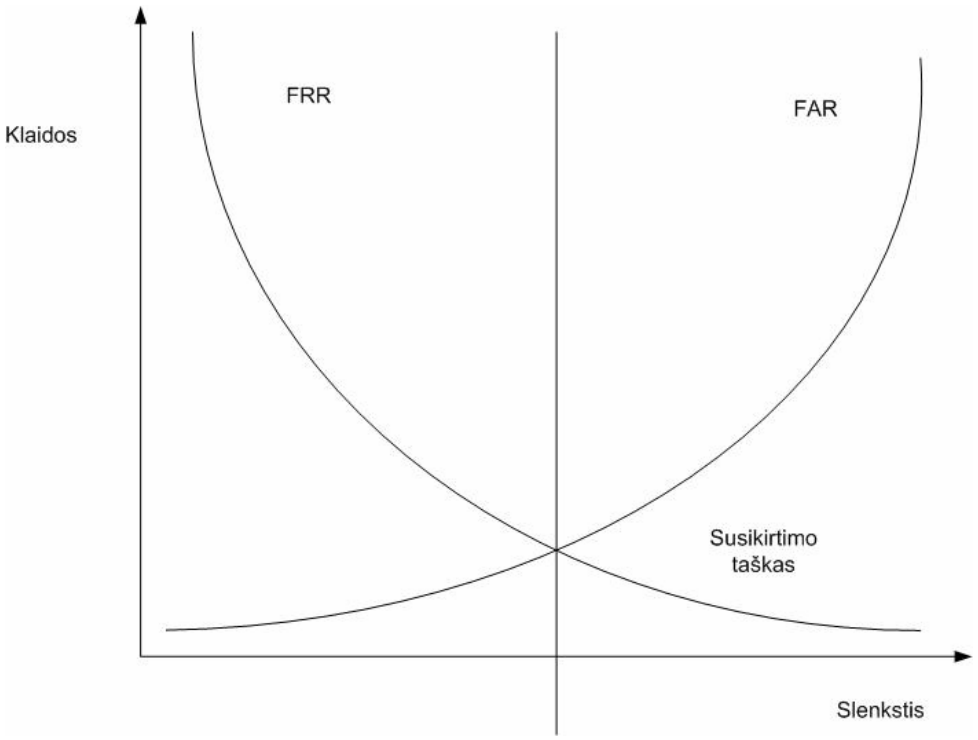
Mažiau sutinkamas dydis - vienodas klaidų santykis *(Equal Error Rate (EER))*, kuris reiškia tašką, kuomet duotojoje sistemoje abiejų tipų klaidų santykiai pasiekia pusiausvyrą (žr. pav. 3). Pavyzdžiui, biometrinės sistemos charakteristikas, tuo pačiu ir abi klaidų tipų reikšmes, lemia:

- Aplinkos sąlygos (temperatūros pokyčiai, santykinė drėgmė);
- Asmenų amžius, lytis, etninė grupė ir profesija;
- Asmenų įsitikinimai, norai ir ketinimai (jei asmuo nelabai noriai naudojasi sistema, tai paveikia ir sistemos darbą)
- Asmens fizinė išvaizda (asmuo be rankos negali naudotis sistema, kurioje reikia pasirašyti...)

Kiekvienas toks faktorius gali paveikti FRR ir FAR. Abi šios reikšmės, po to kai sistemos gamintojas jas paviešina, parodydamas sistemos efektyvumą, gali atspindėti tik rezultatą, kai bandymai atliekami laboratorijose, kontroliuojamomis sąlygomis. Tokiu būdu į sistemos efektyvumą reikia žiūrėti atidžiai. Į FRR ir FAR reikšmes taip pat reikia žvelgti atidžiai, nes jos gali būti tyrimų rezultatas, kai atliekami vieno arba trijų bandymų skaičiavimai, atsižvelgiant į

biometrijos sistemos tipą ir kur ji bus naudojama. Tai reiškia, ar vartotojui bus leista vieną kartą pabandyti įeiti į sistemą, ar bus duoti trys bandymai.

Praktika rodo, kad atliekant tris bandymus, pagerinamas FRR rodiklis. Iš to kylanti objektyvumo problema ta, kad šie klaidų tipai gali iš pradžių būti nustatomi rankiniu būdu. Tai reiškia, kad, pavyzdžiui, bankui reikalaujant ypač didelio saugumo lygio prie durų į pagrindinį seifą, kur pašaliniams asmenims įėjimas draudžiamas. Bankas gali nuspręsti, kad FAR koeficientas turi būti ne daugiau kaip 0,1%, tai reiškia, jog tik vienas iš tūkstančio klaidingų prisijungimų gali būti leidžiamas. Bankas taip pat gali pareikalauti, jog šis dydis būtų 0,001%. Biometrijos sistemos tiekėjai gali pakeisti sistemos FAR koeficientą, kad šis santykis būtų pasiektas, tačiau šiuo atveju daroma labai didelė įtaka FRR dydžiui.



Pav. 3. FRR, FAR ir EER

2.3. Biometrinių sistemų privalumai

Biometrijos technologija yra vadinama „kas aš esu“, t.y. asmuo pats yra kaip reikiamas raktas, jam nereikia nieko prisiminti ar nešiotis. Tokiu būdu slaptažodžiai ir panaši prisimenama informacija vadinama „ką aš žinau“, tuo tarpu įvairios identifikavimo kortelės, raktai ir pan. vadinama technologija „ką aš turiu“. Tuo biometrija yra laikoma pranašesne ir kartu saugesne. Taip

norint identifikuoti save pakanka duoti savo pirštą ar kokį kitą požymį nuskaityti specialiai įrangai. Speciali programinė įranga, surinkusi reikiamą informaciją, sutikrina su jau anksčiau įrašyta ir specialiais algoritmais apdorota informacija duomenų bazėje. Jei yra randamas teisingas atitikmuo, esate sistemos identifikuojamas kaip teisėtas jūs.

Taip pat yra skelbiama, kad biometrija besiremianti technologija yra saugiausia iš šių trijų (biometrijos, slaptažodžių ir specialių kortelių), nes sužinoti prisijungimo slaptažodžius ar pavogti identifikavimo kortelę yra daug lengviau.

Slaptažodžius sužinoti yra keletas būdų, tai arba jie yra atspėjami, nes naudojami pakankamai aiškūs ir trumpi (slaptažodis, slapt123, 123456 ir pan.), arba išgaunami įvairiais kitais būdais: perskaitomi nuo priklijuoto lapuko ant monitoriaus, sužinomi iš kolegų įvairiais būdais socialinės inžinerijos pagalba, atspėjami tiesioginės perrinkimo (*Brute Force*) ar žodyno (*Dictionary attack*) atakos būdu, kuomet yra slaptažodis randamas bandant įvairius variantus. Tačiau biometrijos technologijos taip pat nėra visiškai saugios.

2.4. Kur naudojamos biometrinės sistemos

Šiuo metu pasaulyje yra naudojama daug ir įvairių biometrinių sistemų tipų. Keturi pagrindiniai tipai: įėjimo ir leidimų sistemos, medicinos diagnozės, ateities spėjimai ir naudojimas, skirtas etnologinių judėjimų išsiaiškinimui. Dauguma pritaikymo būdų dar tik testavimo stadijoje, nebūtini paprastam vartotojui, ir tokiu sistemų efektyvumas dar turi būti išmatuotas realiomis veikimo sąlygomis.

Bet kokia situacija, kuri leidžia žmonių ir mašinų bendravimą, gali savyje turėti biometriją. Tokias situacijas galima suskirstyti į keletą pritaikymo sričių. Biometrija šiuo metu yra naudojama srityse su personaliniais kompiuteriais, tinklais, bankų sistemose, imigracijos stebėjimui, teisėsaugoje, ryšių tinkluose ar personalo darbo laiko stebėjime. Ir visos šios panaudojimo sritys turi vieną bendrą sudedamąją dalį - žmones. Visame pasaulyje vyriausybės yra be galo įsitraukusios į biometrijos sistemų kūrimą ir naudojimą. Apgaulės mastai didėja nuolat ir kuo toliau, tuo vis dažniau saugumas tampa būtinybe. Šiuolaikinis biometrinių sistemų panaudojimas gali būti sutinkami daug ir įvairių sričių.

Biometrinių technologijų yra daug ir įvairių. Vienos yra plačiau naudojamos, kitos rečiau, skiriasi reikalavimai įrangai bei panaudojimo sritys. Išsiaiškinus kaip kiekviena iš tokių technologijų veikia, ir pagrindinį dėmesį kreipiant ne į algoritmus ar duomenų apdorojimo metodus, o į sistemų panaudojimą, galima aiškiau suprasti, kokios yra galimos tokių technologijų naudojimo grėsmės.

2.4.1. Teisėsauga

Biometrija, konkrečiu atveju pirštų antspaudai, nėra šių dienų išradimas. Anksčiau ji buvo taikoma identifikuojant nusikaltėlius, teismo procesuose nustatant kam priklausė vienas ar kitas įkaltis ar įrankis, ir panašiai. Šiais laikais biometrija gali būti sutinkama nemažai įvairių sričių. Jos panaudojimas tapo platus ir visuotinai pritaikomas, nes kompiuteriams surasti, patikrinti ar atpažinti asmenį pagal saugoma informaciją tūkstančius įrašų turinčiose duomenų bazėse užtrunka sekundžių.

Todėl galima teigti, kad teisėsaugos bendruomenė yra viena didžiausių biometrijos vartotojų ir panaudojimo grupių. Policija visame pasaulyje vysto AFIS [2] technologijos naudojimą, apiforminant įtariamuosius, atliekant tyrimo dalį pagal pirštų antspaudus ir atvedant kaltuosius stojimui prieš teisingumą. Kai kurių biometrinių sistemų gamintojai užsidirba nemažą dalį biudžeto, pateikdami savo biometrines sistemas vartojimui. Šios sistemos yra paremtos AFIS ir delnų antspaudų technologijomis.

2.4.2. Seifų apsauga

Pirštų antspaudų panaudojimas taikomas saugiems ir naujoviškiems seifų užraktams. Tokie užraktai gali turėti atmintyje iki 50 skirtingų pirštų įrašų, kas leidžia šitų pirštų savininkams prieiti prie seifo turinio, ir gali būti naudojamas ligoninėse, viešbučio priimamuosiuose ir panašiai. Taip pat gali tai būti tiesiog šeimos seifas.

2.4.3. Parduotuvės ir aptarnavimo sfera

Visai neseniai pirštų antspaudų nuskaitymo technologija rado savo nišą parduotuvių kasose. Finansinėse operacijose savu laiku perversmą padarė bankinės mokėjimų kortelės - su savimi nebereikia nešiotis pilnų piniginių ar bijoti, jog prekėms apmokėti pritrūks kelių centų. Tačiau kartu su privalumais atsirado ir nauji trūkumai - pirkėjai pamiršta kortelės saugos kodus, jos pametamos arba dar blogiau - pavagiamos ir ištuštinamos. Tad kartu su kortelėmis sparčiai vystėsi ir jų apsaugos priemonės - tobulinamos pačios kortelės, integruojamos miniatiūrinės signalizacijos priemonės. Tačiau galimas ir kitas kortelių apsaugos metodas - tiesiog jų nenaudoti arba vietoj kortelių naudotis pirštų anspaudais. Tokio tipo atsiskaitymo sistemos jau įdiegtos Vokietijoje ir sėkmingai naudojamos.

Pirkėjas, prieš tai savanoriškai suvedęs savo duomenis į sistemą, gali ateidamas į parduotuvę nesinešti nei grynųjų pinigų, nei mokėjimo kortelių. Tokia sistema yra sujungiama su vienu ar kitu banku, ir pirkėjui atsiskaitant už prekes piršto antspaudu, pinigai yra automatiškai nuskaičiuojami nuo jo asmeninės sąskaitos į tos parduotuvės sąskaitą. Tai galėtų pasirodyti ypač naudinga senyvo

amžiaus žmonėms, kurie dažnai vaikšto į parduotuves ir neretai pamiršta pasiimti su savimi mokėjimo priemonę.

Nemažai klausimų keliantis, bet pasisekimą radęs biometrijos panaudojimas, tai vaikų valgyklose sumontuotos pirštų antspaudų sistemos. Jų pagalba nebūtina mokėti už maistą grynaisiais, pakanka nurodyti savo piršto antspaudą sistemai. Tuo pačiu sistema gali sekti vaiko mitybos istoriją, ir taip tėvai gali pamatyti, ir sekti ką valgo jų vaikai mokykloje.

2.4.4. Bankai

Bankai naudoja nemažai įvairių biometrijos technologijų jau daugybę metų. Mokėjimo, atsiskaitymo sistemos ir pavedimai šioje stadijoje yra pažeidžiami, todėl gali būti apsaugoti naudojant biometriją. Kitos sritys, kaip telefoninė ir internetinė bankininkystė, taip pat gali būti visiškai saugios vartotojams ir banko darbuotojams, naudojant biometriją. įvairialypėje rinkoje siekiama įrodyti biometrijos technologijos pranašumą.

2.4.5. Kompiuterių sistemos (dar žinoma kaip loginė prieigos kontrolė)

Biometrinės sistemos įrodo, kad gali daugiau nei reikia, norint apsaugoti kompiuterinių tinklų sistemas. Ši rinka turi fenomenalų potencialą, ypač jei biometrijos pramonė pradėtų migruoti į didelio mąsto internetinius projektus. Kai bankiniai duomenys, verslo planai, kreditinių kortelių numeriai, medicininiai įrašai ir kita asmeninė informacija tampa piktybinių atakų taikiniu, biometrijos rinkos galimybės yra neaprėpiamos.

2.4.6. Fizinis priėjimas

Mokyklos, atominės elektrinės, kariuomenės bazės, parkai, ligoninės, biurai ir prekybos centrai visame pasaulyje pradeda naudoti biometriją, norėdami sumažinti pavojų saugumui. Kai saugumas tampa vis aktualesnis tėvams, darbuotojams, valstybės tarnautojams ir kitoms asmenų grupėms – biometrija tampa vis dažniau ir plačiau priimtinu ir todėl būtinu įrankiu, kurio panaudojimo galimybės begalinės. Automobiliai, namai - paprastų piliečių prieglobstis - dažnai tampa vagysčių taikiniais, ir biometrija – jei jos kaina priimtina ir sistema įrengta patogiai – galėtų suteikti tobulą saugumo sprendimą.

Pirštų antspaudai kiek seniau pradėti naudoti pakeičiant durų spynas. Pagal galimybes jose gali būti saugoma nuo vieno ar kelių įrašų neprijungtose prie sistemos spynose, iki praktiškai neriboto kiekio vartotojų. Tai yra išgaunama naudojant biometrines spynas kartu su kompiuterine sistema ir duomenų baze, identifikuojant asmenį. Tai reiškia nustatant, kad tai yra „žinomas“ žmogus, anksčiau įvestas į duomenų bazę. Spynose, tiksliau tariant praėjimo kontrolės sistemose

taip pat gali būti biometrinės technologijos panaudojamos sąjungoje su kortele ar prisijungimo informacija. Tai vadinama dviejų faktorių [18] tikrinimu (*Two-factor identification*). Naudojant kortelę kartu su pirštų antspaudų tikrinimu, sistema nuo kortelės nuskaito reikiamą informaciją, dažniausiai PIN[1] kodą, pagal kurį susiranda duomenų bazėje reikiamą įrašą. Vėliau yra nuskaitomas pirštų antspaudas, apdorojamas reikiamais algoritmais ir sutikrinamas su rastu įrašu. Atsakymas yra arba asmuo yra teisėtas kortelės savininkas, arba ne.

Jei dviejų lygiu tikrinimo sistemose yra naudojama veido atpažinimo technologija, tuomet nuo kortelės yra nuskaitoma anksčiau išsaugota asmens nuotrauka, ir ji yra sutikrinama su paimta realaus laiko asmens nuotrauka.

2.4.7. Imigracija, sienos apsauga

Terorizmas, prekyba narkotikais, nelegali imigracija ir dideli turistų srautai sunkina imigracijos departamentų veiklą visame pasaulyje. Būtina, jog šios įstaigos galėtų greitai ir automatiškai apiforminti gerbiančius įstatymą turistus ir atpažinti nusikaltėlius. Biometrija padeda šiuos poreikius įgyvendinti. Biometrija jau naudojama ir renka informaciją apie imigrantus tokiose šalyse kaip JAV, Australija, Bermudai, Vokietija, Malaizija ir Taivanis.

Sienos apsaugos srityje biometrijos panaudojimas labai suaktyvėjo po visai nesenų rugsėjo 11 įvykių. Tokios sistemos yra metamos kaip ginklas kovai prieš terorizmą ir kitus, įvairaus plauko nusikaltėlius. Pagrindinės funkcijos yra patikrinti, ar asmens dokumentas priklauso konkrečiam asmens dokumento turėtojui, ar asmens dokumentas nėra padirbtas, taip pat ar asmuo, bandantis kirsti sieną gali tai padaryti. Sienos apsauga bando užkirsti kelią arba sulaikyti asmenis, kurie yra ieškomi vienoje ar kitoje šalyje už padarytus nusikaltimus, kurie anksčiau buvo deportuoti iš šalies dėl vienos ar kitos priežasties, ir pan.

Sienų apsaugoje pagrinde naudojamos kelios technologijos, tai pirštų antspaudų arba akies rainelės nuskaitymas. Asmens nustatymo sistemos šiuo metu yra kuriamos tokios, kad interesantui nereikėtų sustoti prie jo informaciją nuskaitančio įrenginio, o geriausia būtų, kad sistema galėtų veikti iš didesnio atstumo, bent jau 3m vietoj dabar naudojamų 10-90 cm. Tokiu būdu asmuo galėtų būti patikrinimas net ir be jo žinios, kas savaime kelia susirūpinimą elementariomis žmogaus teisėmis ir laisvėmis. Tačiau apie tai vėliau. kituose skyreliuose.

2.4.8. Akies rainelės biometrijos panaudojimas oro uostuose

Šiuo metu jau visi naujojo - penktojo - Londono Heathrow oro uosto terminalo keleiviai gali būti privalomai tikrinami, nuskaitant jų akies rainelę. Sistema eksperimentiniu režimu jau veikė

[1] PIN – Personal Indetification Number

pirmajame terminale, skirtame į Londoną atvykstantiems ir vidiniais Britanijos oro keliais besinaudojantiems svečiams. Procedūros metu įrenginys nuskaito akies rainelę tarsi brūkšninį kodą.

Europos Sąjunga svarsto įvesti biometrinių duomenų kontrolę visiems, kertantiems Šengeno erdvę. Iki šiol tik Britanija reikalavo atvykstančių pirštų atspaudų, bet, pasiduodamos Jungtinių Valstijų spaudimui, ES šalys artėja prie nuosavos biometrinių duomenų bazės kūrimo. Pirmiausia, į ją bus įtraukti asmens paso duomenys, pirštų atspaudai ir akies rainelės arba tinklainės atvaizdas. Skaičiuojant ir tikrinant minėtus duomenis kyla sunkumų – padirbti paso duomenis ir perkelti juos į paso laikmeną, saugančią informaciją apie asmenį, kompiuterių įsilaužėlių teigimu, yra gan paprasta kaip ir nuotolinis informacijos nuskaitymas.

Suklastoti arba pakeisti pirštų atspaudus taip pat nesudėtinga. Tuo metu akies rainelės atvaizdo koregavimas gerokai sunkesnis uždavinys. Įprasta manyti, kad rainelės nuskaitymas – vienas geriausių tapatybės nustatymo būdų. Pasaulyje nėra dviejų vienodas raineles turinčių žmonių. Tai nebūdinga ir dvyniams. Atliekant nuskaitymą, atstumas tarp kameros ir žmogaus gali svyruoti nuo 10 iki 90 centimetrų. Tuomet prietaisas įrašinėja asmens akių atvaizdą 30 kadrų per sekundę greičiu. Programa atrenka pačius raiškiausius kadrus ir, lygindama juos pagal 266 pagrindinius taškus bei požymius, analizuoja ir identifikuoja keliaujančiojo tapatybę. Lazerinis spindulys skenuojant akies rainelę nėra naudojamas, todėl toks būdas saugesnis nei tinklainės nuskaitymas. Tačiau jis brangesnis, o gauti duomenys turi didesnę paklaidą.

Su amžiumi dėmių išsidėstymas rainelėje gali stipriai pasikeisti. Vaiko akies rainelė per porą metų pasikeičia taip, kad jokia biometrinė sistema jos neatpažins. Sergant tam tikromis ligomis, gali kisti rainelės spalva, atsirasti pigmentinės dėmės. Sunkumų identifikuojant atsiranda žmonėms su nusilpusiu regėjimu ar besiskundžiantiems žvairumu. Klaidų nustatant asmens tapatybę gali kilti esant nedidelėms akių traumoms, akių nuovargiui ar po bemiegės nakties, o tai ypač dažnai pasitaiko skrendant tolimus atstumus.

Tokiu būdu sistema, patikrinusi keleivį išskrendant, susidurs su biometrinės informacijos neatitikimu šiam nusileidus. Iki šiol panašaus pobūdžio tapatybės nustatymo sistemos buvo naudojamos tik itin griežtai saugomuose objektuose, siaurame, specialiai tam parengtų žmonių rate. Ir kuo didesnis slaptumas – tuo didesni ir sveikatos reikalavimai personalui. Tačiau sunku pasakyti, kas bus, kai akies rainelę naudojanti asmens identifikavimo sistema įsilies į kasdienį milžiniškus keleivių srautus aptarnaujančių oro uostų ar pasienio kontrolės postų gyvenimą. Aišku, jog papildoma techninė ir programinė įranga, patikra ir ilgesnės eilės oro uostuose keliaujančiųjų nenudžiugins.

Atskirai nagrinėjimas ir milžiniško duomenų kiekio klausimas. Bet kuriame biologiniame kode slypi gerokai daugiau informacijos nei reikalaujama patikros metu. Naudodamasis tokiais duomenimis specialistas gali nustatyti žmogaus sveikatos būklę, ligas, kuriomis jis serga arba kurios yra įgimtos, asmens jautrumą įvairioms cheminėms medžiagoms ir pan.

Tai per daug asmeniška informacija, bet ja tektų dalintis kiekvienos kelionės į užsienį metu. Kad ir kokios slaptos būtų duomenų bazės, anksčiau ar vėliau, teisėtai ar ne kam nors jos vis vien parūps. Būdų pasinaudoti slapta nutekintais asmeniniais biometriniais duomenimis netrūksta. Pvz., akies rainelės nuskaitymą ketinama naudoti ir bankomatuose.

Akies tinklainės nuskaitymas yra tikslesnis, tačiau gerokai pavojingesnis būdas, mat atliekamas naudojant specialų lazerinį spindulį. Niekas negali užtikrinti, kad toks skenavimas žmogaus sveikatai nepakenks ateityje. Be to, griežtinami šiam veiksmui atlikti reikalingi reikalavimai. Atstumas tarp akies ir nuskaitančio įrenginio turi būti ne didesnis kaip 1,5 centimetro, žvilgsnį reikia nukreipti į atitinkamą tašką ir išlaikyti nejudant viso proceso metu.

Ne kiekvienam suaugusiam tai pavyksta iš pirmo karto, juolab ryte ar vėlai vakare, nekalbant apie vaikus, kuriems akies tinklainės nuskaitymas atrodo gąsdinantis. Visiems žinoma, kaip sunku įkalbėti vaikus fotografuojantis nejudėti ir žiūrėti į vieną tašką. Todėl galima tik įsivaizduoti, kas atsitiks vasaros atostogų įkarštyje, kuomet poilsiauti vyksta tūkstančiai šeimų.

Tačiau tai dar ne visos su biometrija susijusios problemos. Neseniai JAV pareikalavo duomenų ne tik apie visus į šią valstybę atvykstančius žmones, bet ir informacijos apie virš Jungtinių Valstijų teritorijos praskrendančius keleivius, jų giminaičius ir draugus. Sakoma, kad visi pasaulio žmonės pažįstami vienas su kitu per septynis rankos paspaudimus, todėl niekas negali pasakyti, kokio lygio pažintis valdininkams pasirodys pakankama priežastimi įtraukti asmenį į „juoduosius sąrašus“ už talkinimą teroristams.

2.4.9. Nacionalinė tapatybė

Biometrija pradeda padėti vyriausybei, kai šioji matuoja populiacijos augimą, nustato piliečių tapatybę ir kerta kelią sukčiavimams vykstant vietiniams ar nacionaliniams rinkimams. Dažnai tai apima biometrinės informacijos šablono saugojimas asmens tapatybės kortelėse, kuris laikomas nacionaliniu dokumentu. Būtent pirštų antspaudų nuskaitymo technologija yra išvystyta šioje srityje ir tokie dokumentai jau naudojami arba ruošiamasi naudoti Jamaikoje, Filipinuose, Pietų Afrikos Respublikose, Vokietijoje, JAV, Lietuvoje ir kitoms šalis. Taip pat biometrija padeda suskaičiuoti ir surašyti dykumų gyventojus.

Lietuvoje jau yra leidžiami biometriniai pasai, kuriuose specialioje RFID mikroschemoje saugoma skaitmeninė asmens nuotrauka ir pirštų antspaudas. Tokie pasai yra pagrindinis reikalavimas, norint vykti į JAV ar Kanadą be vizų ir kuris įsigaliojo 2008 metų pabaigoje.

2.4.10. Ryšiai ir telefonija

Pasaulinės komunikacijos per paskutinį dešimtmetį labai išsiplėtė. Telefono kompanijų paslaugos dažnai tampa sukčiavimo taikiniu. Vėlgi, biometrija gali padėti apsisaugoti nuo tokių veiksmų. Kalbančiojo identifikacija yra akivaizdus metodas, tinkantis ryšių sistemai ir skinasi kelią į daug žadančią rinką.

2.4.11. Laiko ir lankymo stebėjimas

Registruojant ir stebint darbuotojų judėjimą, kuomet jie ateina į darbą, išeina pietauti arba palieka darbo vietą po darbo, buvo tradiciškai naudojami tam tikri atskaitos įrenginiai. Pakeičiant šį rankinį procesą, biometrija apsaugo nuo bet kokių piktnaudžiavimų ir technologija gali būti sujungta su laiko apskaitos sistemomis, kad būtų galima teisingai vesti darbo laiko apskaitą ir formuoti įvairias personalo darbo ataskaitas. Todėl viena iš sėkmingai biometriją naudojančių sričių yra darbininkų laiko apskaita ir kontrolė. Darbininkas ar darbuotojas, atėjęs į darbą, parodo sistemai kortelę su savo duomenimis, sistema nuskaito reikiamą informaciją, ir paskui naudojant veido ar kokią kitą technologiją asmuo yra patikrinamas su pagal kortelės duomenis ir įleidžiamas (arba ne) į ten, kur norėjo ateiti. Tai gali būti darbo kabinetas, gamybinės ar kokios kitos patalpos. Tokiu būdu įmonės vadovas gali rinkti pakankamai tikslią informacija apie darbininkų darbo laiką.

2.5. Kitos panaudojimo sritys

Viena iš kitokio tipo biometrinių technologijų pritaikymo sričių yra darbuotojo streso matuoklis, kurio prototipas buvo lietuvių pristatymas konferencijoje INFOBALT‘08[2]. Tokiai technologijai pritaikyti yra naudojama speciali kompiuterio pelė, kuri, kartu su įprasta žymeklio ekrane valdymo funkcija, turi keletą skirtingų įmontuotų sensorių. Korpuse gali būti įmontuoti temperatūros, drėgmės (prakaito), spaudimo ir kiti jutikliai, kurių pagalba sistema gali darbuotojui duoti patariamąją informaciją. Tokiu būdu esant nestabiliai ar streso būsenoje vieną ar kitą užduotį, kuri tam tikru metu nėra tinkama prie darbuotojo būsenos, sistema pasiūlys atidėti.

Biometrinės technologijos gali būti naudingos ir kitais, ne tokiais linksmais atvejais, pavyzdžiui žmogui patekus į vienokį ar kitokį nelaimingą įvykį. Asmuo sunkiai sužeistas, be sąmonės, negali bendrauti, ir gabendami sužeistąjį į reanimaciją medikai nerimauja, nes nežino, ar

[2] Nanotechnologija

asmuo nėra alergiškas kokiems nors nuskausminamiems preparatams. Jie taip nežino nei kraujo grupės, nei ligų, kuriomis sirgęs ankščiau. Galų gale nežino asmens duomenų bei adreso ir taip negali apie jo buvimo vietą pranešti artimiesiems. Siekdami išgelbėti gyvybę, medikai yra priversti rizikuoti. Ši situacija būtų visai kitokia, jei sveikatos paslaugų sektoriuje būtų taikoma biometrija. Pavyzdžiui, savanorišką sutikimą davusio piliečio sveikatos istorija būtų perkelta į duomenų bazę, o su ja būtų susietas to piliečio biometrinių duomenų algoritmas. Medikai, norėdami greitai išsiaiškinti kuo šis pilietis yra sirgęs, kokia jo kraujo grupė, kam jis yra alergiškas, naudodamiesi veido, pirštо antspaudų ar akies rainelės atpažinimo technologijomis greitai identifikuotų asmens tapatybę ir gautų reikalingus jo ligos istorijos duomenis. Taip žmogui būtų greičiau suteikiama pagalba, ir kai laikas toks svarbus, kiekviena sutaupyta minutė yra naudinga.

2.6. Naujos biometrijos technologijos

2.6.1. Ausyse „saugomi“ slaptažodžiai

Galima įsivaizduoti, kad apgavikas skambina į banką, prašydamas, kad jūsų pinigai būtų pervesti į jo sąskaitą. Užuot prašęs jūsų asmeninės informacijos, bankininkas tiesiog nuspaudžia mygtuką, kuris priverčia telefoną sukelti trumpą seriją trakštelėjimų į apgaviko ausį. Žinutė iš karto įspėja banką, kad asmuo nėra tas, kuo dedasi ir skambutis baigiamas.

Vieną dieną tokia apsauga gali būti įprastas dalykas, jei tik nauja biometrinė technika, sukurta, kad atpažintų asmenį kitoje telefono linijos pusėje, pasirodys sėkminga. Koncepcija remiasi idėja, kad ausis ne tik fiksuoja garsus, bet taip pat ir sukelia tokio lygio garsus, kad juos gali aptikti superjautrūs mikrofonai. Jeigu paaiškėtų, kad kiekvieno asmens ausų sukeliami garsai yra unikalūs, tai galėtų padidinti skambučių centro ir telefoninės bankininkystės sandorių saugumą ir sumažintų poreikį prisiminti daug identifikacijos kodų. Vogti mobilieji telefonai taip pat galėtų tapti beverčiais, jeigu būtų suprogramuoti taip, kad neveiktų, nustačius, jog telefono naudotojas nėra teisėtas savininkas.

Ausies sukeliami garsai, pavadinti otoakustinėmis emisijomis (*OAE - otoacoustic emissions*), sklinda iš vidinėje ausyje esančios spiralės formos sraigės [18]. Manoma, kad juos sukelia plaukuotųjų ląstelių virpesiai per sraigės išorinę dalį. Paprastai garsai, įeinantys į ausį, sukelia šių išorinių plaukuotųjų ląstelių virpesius, kurie konvertuojami į elektrinius signalus ir perduodami klausos nervui, todėl leidžia užfiksuoti garsą. Svarbiausia, kad išsiplėsdamos ir susitraukdamos, šios ląstelės taip pat sukuria savo garsus.

Taip yra dėl to, kad klausa yra aktyvus procesas – ausis skiria energijos įeinančioms garso bangoms, kad grąžintų energiją, kuri prarandama, kai ausies struktūra sugeria garsą. Dėl šio proceso

mes girdime garsus, kurių kitaip negirdėtume, tačiau dalis plaukuotųjų ląstelių duotos energijos išsilaisvina kaip OAE.

Šie ausies sukeliami garsai buvo nustatyti 1940 m., bet neatskleisti iki 1970 m., kai buvo sukurti ultražemų garsų mikrofonai. OAE gali būti sukelti, kai serija trakštelėjimų nukreipiama į ausį. Sugrįžtančios garso emisijos sudaro 0-5 kilohercų signalus, kintančius amplitudėje. Trakštelėjimo testai yra naudojami tikrinant kūdikių ausis, kai norima nustatyti, ar yra klausos sutrikimų: OAE yra silpnesni, jei vidinė ausis neišsivysčiusi.

Stephen Beeby ir jo kolegoms susidomėjimą sukėlė tai, kad konkrečios serijos trakštelėjimų sukeltas OAE stiprumo ir dažnio pasiskirstymas atrodo labai savitas ir priklauso nuo žmogaus ausies formos. Audiologai gali atskirti skirtingus žmones – vyrus, moteris, net įvairios etninės kilmės žmones pagal trakštelėjimų sukeltas emisijas. Didžiosios Britanijos Inžinerijos ir fizikos mokslų tyrimų tarybos („Engineering and Physical Sciences Research Council“) finansavimo dėka Beeby grupė bando išsiaiškinti, ar šie OAE modeliai gali būti naudojami biometrijoje, pavyzdžiui, akies rainelės ar pirštų atspaudų nuskaitymui.

Kontroliuojamomis laboratorijos sąlygomis emisijos yra tikrai skirtingos, tačiau norint nustatyti, ar tai tikrai praktiškas būdas atskirti žmones, dar reikia labai daug dirbti, H pripažino jis. Dar yra daug problemų, kurias reikia išnagrinėti. Pavyzdžiui, emisijos sumažėja asmenims, kurie vartojo alkoholį. Įvairūs vaistai taip pat pakeičia OAE amplitudę, kaip ir ausų infekcijos bei ausų sieros susikaupimas. Jeigu pavyks pasiekti tikslą iki galutinio projekto termino 2010 metų viduryje, jie tikisi sudominti elektronikos įmones gaminti ausines ir mobiliuosius telefonus su superjautriais mikrofonais. Visa kita padarys programinė įranga.

Sukurti naują biometriją yra didžiulė užduotis. Didžiosios Britanijos Nacionalinės fizikos laboratorijos („National Physical Laboratory“) Teningtone biometrijos vertinimo vadovas Tony Mansfield nuomone, grupė turi ne tik įrodyti, kad technikos klaidų tikimybė yra maža, bet ir tai, jog žmogaus OAE nepasikeis ir po ilgo laikotarpio. Kitaip tariant, uri būti įmanoma patikimai atpažinti žmones ir po ilgo laiko tarpo. Pavyzdžiui, pirštų atspaudai, paimti iš dvidešimtmečio, vis dar tokie patys ir kai žmogui yra šešiasdešimt.

2.6.2. Vietoje pirštų atspaudų – prakaito lašeliai

JAV šalies saugumo departamentas ketina užsakyti tyrimą dėl galimybės naudoti prakaitą asmenų tapatybei nustatyti ir kaip melavimo faktą patvirtinantį identifikatorių vykdant įtariamųjų apklausas, praneša dienraštis „Washington Times“. Tai pranešė departamento Mokslo ir technologijų direktoratas. Jo atstovų teigimu tokie tyrimai dar tik pradedami. Remiantis ankstesniais

tyrimais daro prielaida, kad žmogaus prakaite, seilėse ir šlapime esantys lakieji organiniai junginiai gali būti analizuojami naudojant dujų chromatografą su masės spektrometru. Šios medžiagos esą gali būti naudojamos kaip asmenį identifikuojančios žymos, nes ankstesni tyrimai leidžia manyti, jog prakaito kvapas toks pat individualus, kaip ir piršto atspaudai.

Kita vertus, mokslininkai perspėja, kad kai kurių žmonių prakaito kvapas gali būti ne toks išskirtinis, kaip kitų. Analizuojant 179 tiriamųjų prakaito mėgini paimtus per 10 savaičių periodą, buvo nustatyta, kad kiekviename iš jų yra apie 100 individualių cheminių žymenų, kurie daugiau ar mažiau išliko nepakitę per visą tą laiką. Šių žymenų analizė patvirtino, kad savo išskirtinumu jie panašūs į individualius pirštų atspaudus.

Ekspertai taip pat pažymi, kad prakaito lakiųjų audinių analizę apsunkins vadinamasis „cheminis užterštumas“ – tabako produktuose, higienos priemonėse kvepaluose esančios medžiagos. Nustatyta, kad iš 44 tariamai pastovių prakaito žymenų apie 25 proc. sudarė būtent tokie „cheminės taršos“ produktai.

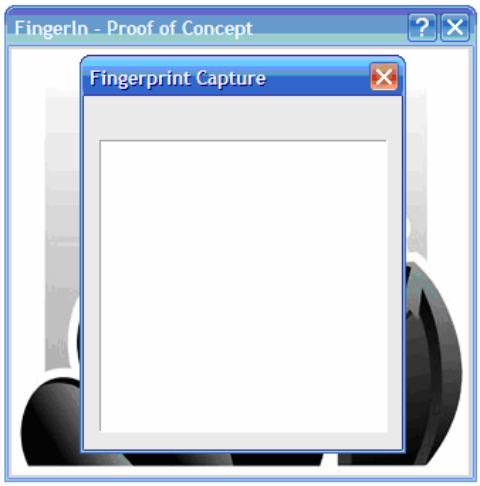
3. NUOTOLINIO PRISIJUNGIMO NAUDOJANT BIOMETRIJĄ SISTEMA

Biometrinės technologijos neapsiriboja vien tiktai praėjimo kontrolės sistemomis. Viena iš galimų pritaikymo sričių buvo kaip magistrinio darbo projektas sukurta nuotolinio prisijungimo sistema, panaudojant pirštų antspaudus kaip vieną biometrijos priemonių. Biometrinio panaudojimo šioje sistemoje idėja tokia, kad vartotojas yra įvedamas į sistemą, nuskaitomi jo pirštų antspaudai ir jis gauna priėjimą, vartotoją sistemoje.

3.1. Projektas

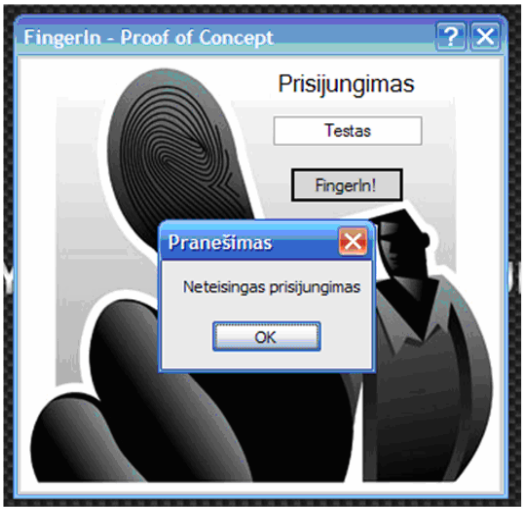
Prisijungimui prie sistemos nėra naudojama vien tik biometrija, ir asmeniui, norint sėkmingai prisijungti, reikia žinoti savo prisijungimo vardą arba išduotą tam tikrą PIN kodą. Kitaip tariant naudojamas dviejų faktorių tikrinimas[3], kuomet neužtenka vieno iš faktorių, kad sistema sėkmingai atpažintų bandantį prisijungti vartotoją. Šiuo atveju yra naudojama tai, kas žinoma (PIN kodas arba vartotojo vardas), ir tai, kas esame (piršto antspaudas). Trečiu faktoriumi yra vadinama tai, ką turime, kas galėtų būti įvairios kortelės su informacija apie kortelės savininką arba ant jos kokiu nors būdu pažymėtas specialus kodas. Programos prisijungimo langas parodytas 4-6 pav.

Pav. 4. Prisijungimo langas



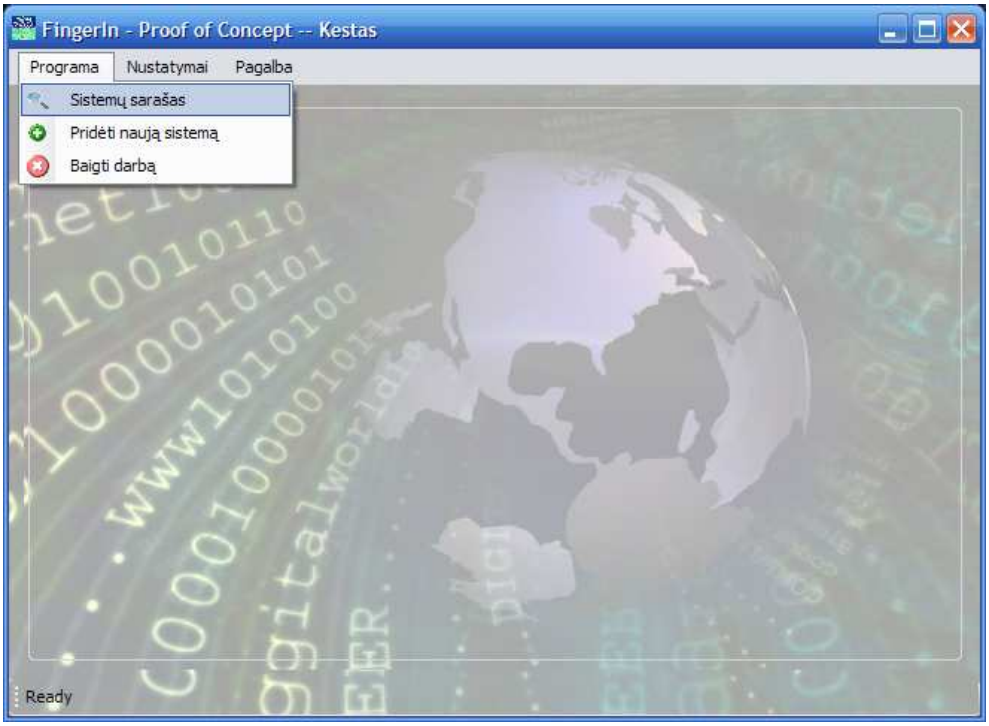
Pav. 5. Piršto antspaudo nuskaitymo patikrinimui langas

[3] Two factor authentification



Pav. 6. Nesėkmingo prisijungimo pranešimas

Sėkmingai prisijungus parodomas pagrindinis sistemos langas (žr. 7 pav). Tokiu būdu vartotojas prisijungęs prie sistemos gauna pilną savo nuotolinių sistemų administravimo galimybę. Nuotolinės sistemos gali būti įvedamos, keičiami jų duomenys ir prie jų prisijungiama. Vartotojas gali įsirašyti prisijungimo informaciją apie nutolusias sistemas, ir vėliau prie jų norint prisijungti nereikės kaskart vėl per naujo įvesti tos pačios informacijos. Taip taupomas laikas.



Pav. 7. Pagrindinis sistemos langas

Ką reikės padaryti tai vieną kartą suvesti savo prisijungimo vardą ir leisti sistemai nuskaityti piršto antspaudą. Tokiu būdų tai tampa saugesne ir paprastesne alternatyva, jei dėl vienos ar kitos priežasties negalima išsaugoti savo informacijos naršyklės slaptažodžių saugojimo sistemose, nes prie jos gali prieiti visi norintys. Šios sistemos saugumo tyrimas aprašytas kituose šio darbo skyriuose.

3.2. Situacijos Lietuvoje įvertinimas

Biometrijos technologijų panaudojimas Lietuvoje yra vystomas labai lėtai. Oficialių statistinių duomenų apie biometrinių duomenų panaudojimą nėra, arba jie yra neprieinami. Yra keletas firmų, kurios užsiima biometriją, kuria specializuotus produktus, tačiau rinka yra dar labai jauna, yra kur plėstis.

Lietuvoje iš biometrines technologijas naudojančių produktų, kuriuos galima sutikti ir įsigyti, galima paminėti biometrinius durų užraktus, spynas bei specialius seifus. Tokie įtaisai ir įrengimai yra galimai naudojami šiuolaikiniuose „protinguose“ namuose, tačiau kita vertus tokių namų Lietuvoje galima sutikti tik keletą.

3.3. Produkto apibūdinimas

3.3.1. Programų sistemos funkcijos

Vartotojas prisijungia prie sistemos savo kompiuteryje, su savo prisijungimo informacija. Sistema paprašo vartotojo įvesti savo pirštų antspaudą, kad galėtų patikrinti jo tapatybę su jau esančiu vartotoju sistemoje. Nuskaitytojo pirštų antspaudo kontroliniai duomenys yra sulyginami su gautaisiais iš sistemos serverio, ir jeigu jie atitinka, sistema išveda visas nutolusias prisijungimo sistemas, kuriose vartotojas turi paskyrą. Dabar vartotojui belieka pasirinkti vieną anksčiau įvestą sistemą iš sąrašo, ir jis bus nukreipiamas į tą sistemą ir joje galės dirbti kaip registruotas ir prisijungęs vartotojas.

3.3.2. Vartotojo charakteristikos

Šios sistemos vartotojams keliami minimalūs kompiuterinio raštingumo reikalavimai, ir pagal nutylėjimą sistemos vartotojai jau turėtų būti susipažinę su biometrijos sąvoka, jos teikiama nauda ir patogumu. Sistema turi išsamų vartotojo vadovą su sistemos naudojimosi instrukcijomis.

3.3.3. Vartotojo problemos

Aktualiausia problema, dėl kurios šis projektas gali būti naudingas, tai daug ir įvairios vartotojo prisijungimo informacijos prisiminimo būtinybė. Sistemos pagalba galima nebegalvoti apie įvairius prisijungimo vardų ir slaptažodžių derinius.

Iki šiol vartotojai tokiai problemai spręsti naudodavo ne itin geras išeitis, kurios yra įvardijamos kaip bloga saugumo praktika: informacijos užsirašymas ant lapelių, visose sistemose naudojama labai panaši, kartais ir tokia pati prisijungimo informacija, lengvi slaptažodžiai. Naudojant tokią sistemą galima nustatyti stiprius ir skirtingus slaptažodžius kiekvienai suderinamai nutolusiai sistemai, ir nebereikia jų prisiminti kiekvieną kartą jungiantis darbui prie tos sistemos.

3.3.4. Vartotojo tikslai

Produkto paskirtis – susisteminti ir apjungti labai dažnai naudojamas sistemas, palengvinti prisijungimą, taip pat galima vienoje vietoje turėti darbui skirtas sistemas, kaip elektroninis paštas, failų apsikeitimo serveris, dokumentų ar projektų valdymo sistema. Vartotojo tikslas yra susipažinti su biometrinėmis sistemomis, naudoti patikimus ir skirtingus slaptažodžius visose sistemose.

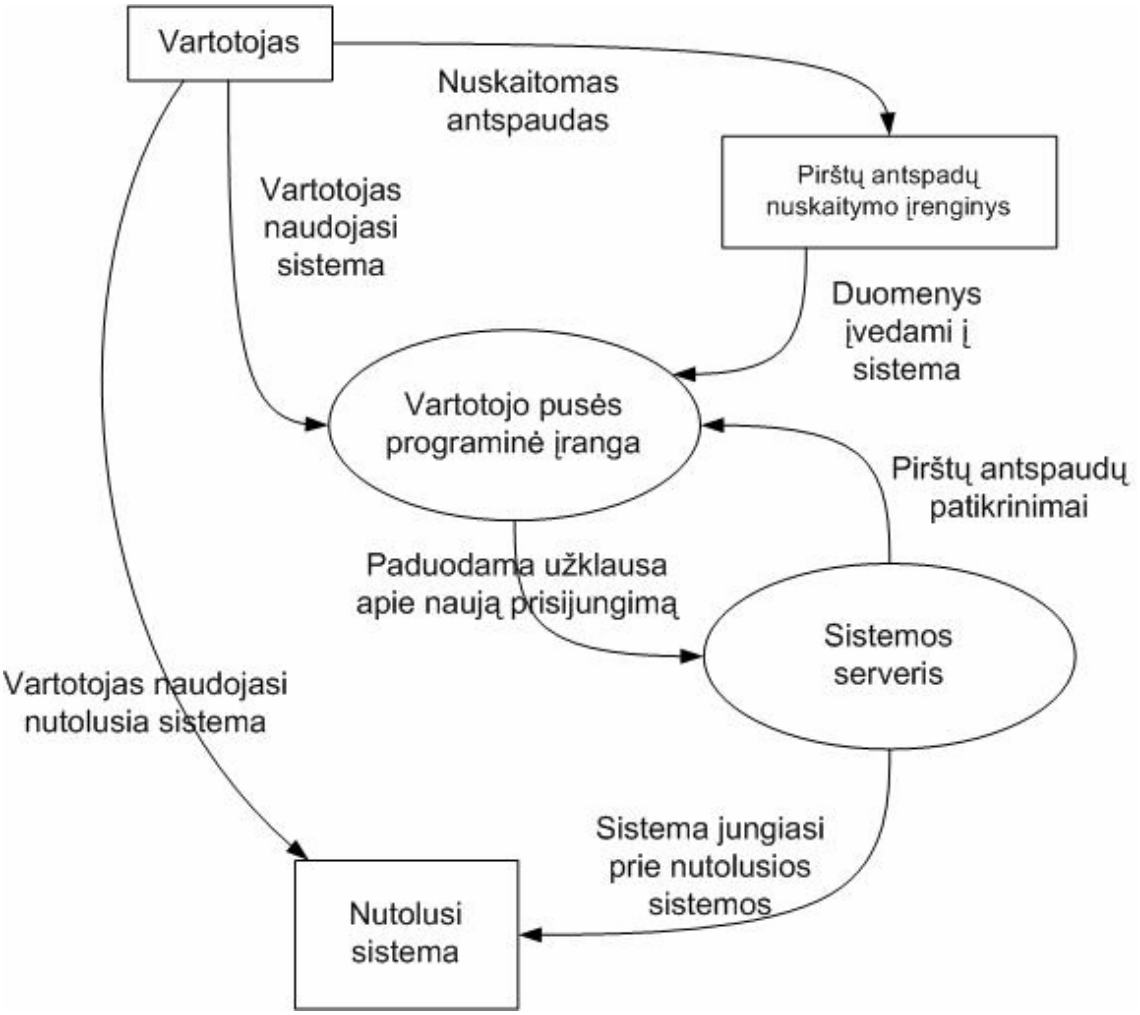
3.4. Sukurtos sistemos vaizdas

3.4.1. Sistemos konteksto diagrama

Sistemos konteksto diagrama ir veikimo principas pateikiamas 8 pav. Kaip galima pastebėti, sistemos funkcinės dalys yra tarpusavyje stipriai susijusios. Sistema buvo kuriama skaidant ją į dalis todėl, kad nesaugoti vartotojo pusėje jokių duomenų apie patį vartotoją, o tai daryti vienoje vietoje centralizuotai. Taip yra todėl, kad geriau galima užtikrinti duomenų apsaugojimą nuo pašalinių.

Sistemą sudaro tokios dalys:

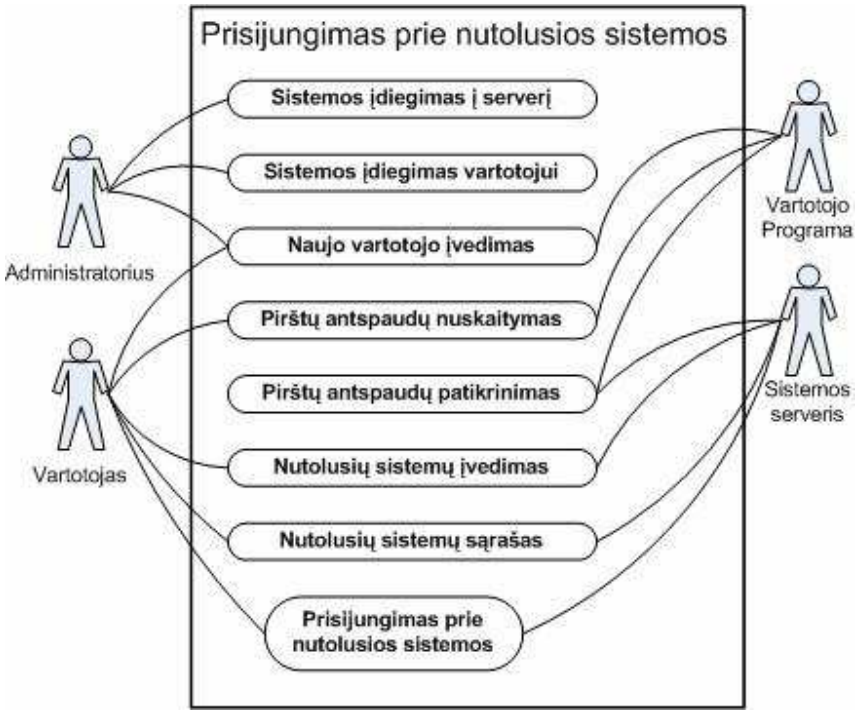
- Vartotojas, kuris naudojasi sistema,
- Pirštų antspaudų nuskaitymo įrenginys,
- Sistemos serveris, kuriame saugoma informacija apie vartotojus ir prisijungimus prie nutolusių sistemų,
- Vartotojo kompiuteryje įdiegta programinė įranga, ir reikalingos tvarkyklės sėkmingam pirštų antspaudų nuskaitymo įrenginio veikimui užtikrinti,
- Nutolusi sistema, su kuria vartotojas nori prisijungęs dirbti.



Pav. 8. Sistemos konteksto diagrama.

3.4.2. Sistemos panaudojimo atvejų vaizdas

Pateikiamas sistemos panaudojimo atvejų vaizdas (žr. 9 pav). Iš jo galima matyti, kokie veiksmai atliekami kokių vartotojų ar sistemos dalių. Taip pat paminėtina, kad sistemos veikime dalyvauja administratoriaus teises turintis vartotojas, kurio tikslas yra į sistemą įvesti naujus vartotojus. Šiame projekte realizuota, kad pirmam vartotojui, kuris yra prisijungia ir įveda savo informaciją į sistemą, yra suteikiamos administratoriaus teisės. Todėl geriau apmokyti vartotojai susipažinę su sistemos naudojimo aprašu, jau gali patys pradėti naudotis sistema be sistemos kūrėjų priežiūros.



Pav. 9. Sistemos konteksto diagrama.

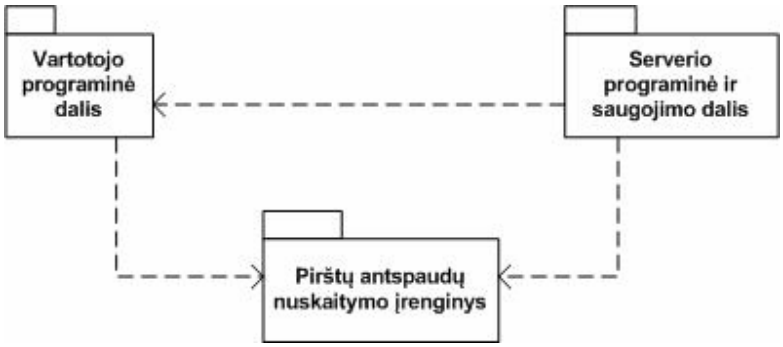
3.4.3. Sistemos statinis vaizdas

Šiame skyrelyje pateikiamas sistemos skirstymas į paketus ir paketų detalizavimas.

3.4.3.1. Apžvalga

10 pav. pateikiamas sistemos skaidymas į dalis. Išskiriamos 3 pagrindinės sukurtos nutolusio prisijungimo naudojant biometriją sistemos dalys:

1. Vartotojo programinė dalis
2. Serverio programinė ir saugojimo dalis
3. Pirštų antspaudų nuskaitymo įrenginys



Pav. 10. Pagrindiniai sistemos paketai

3.4.3.2. Vartotojo programinė dalis

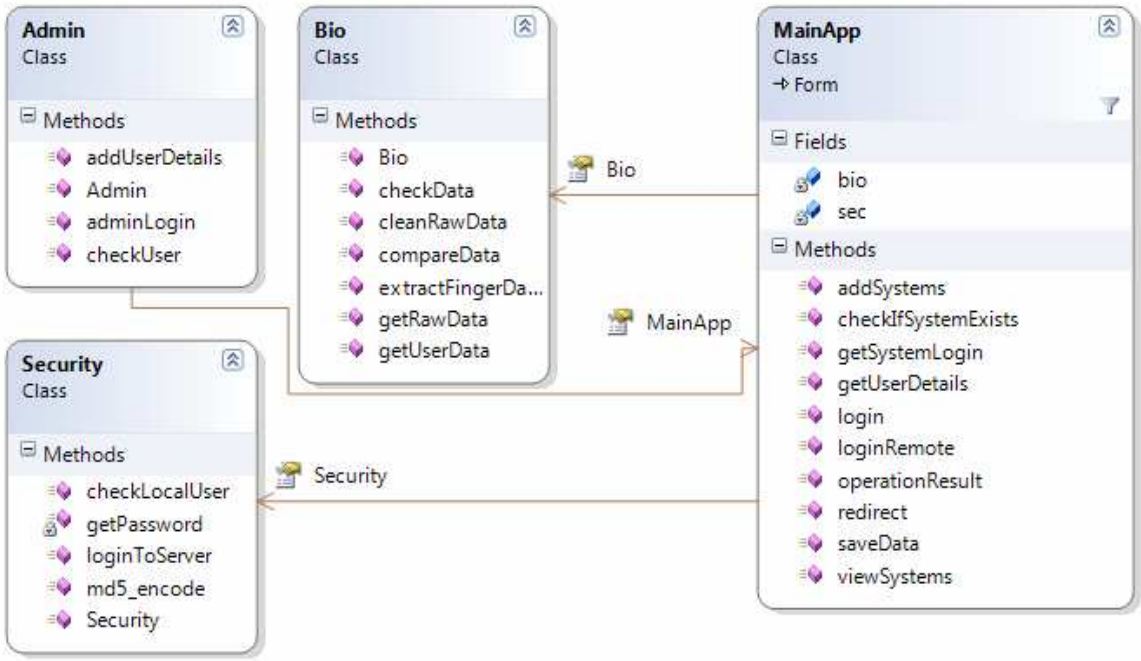
Pateikiama vartotojo programinės įrangos pagrindinių klasių diagrama. Sistemą sudaro penkios pagrindinės klasės, naudojamos pagrindiniams veiksmams.

MainApp – Sistemos valdymo klasė. Joje atliekami visi grafinės aplinkos veiksmai, kitų klasių metodų iškvietimas per sąsajas.

Admin – Sistemos administravimui reikalingų metodų rinkinys.

Security – Saugumo užtikrinimo perduodant ir saugant duomenis užtikrinimo klasė. Šioje klasėje vyksta prisijungimo prie sistemos funkcinė realizacija, perduodamų duomenų šifravimas.

Bio – Darbui su biometrija ir su pirštų antspaudų nuskaitymo įrenginiu skirta klasė. Joje taip pat atliekami pirštų antspaudų informacijos išgavimo iš grafinės nuskaitymo įrenginio informacijos, taip pat tikrinimas ir paruošimas saugojimui duomenų bazėje.



Pav. 11. Vartotojo programinės įrangos pagrindinių klasių diagrama

3.4.3.3. Serverio dalis

Sistemos serverį sudaro kelios loginės dalys:

Duomenų bazė – vieta duomenims saugoti. Naudojama *MySQL* programinė įranga.

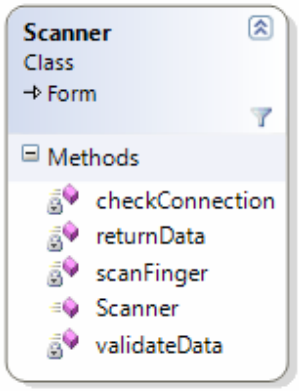
Saugojimo klasė – funkcijų rinkinys darbui su duomenų baze, užklausų vykdymui, klaidų apdorojimui ir rezultatų gražinimui.

Valdymo klasė – tai internetinis servisas ir visas užklausas tiesiogiai priimanti klasė, kviečianti visas kitas klases.

Nukreipimo klasė – funkcijų rinkinys, kuriame tikrinami perduoti sistemai duomenys ir jų kiekis. Taip yra paskirstomos užklausas tarp serverio pusės dalių, atliekamas duomenų šifravimas perdavimui atgal į vartotojo pusės programinę įrangą.

3.4.3.4. Pirštų antspaudų nuskaitymo įrenginys

12 pav. pateikiama įrenginio aptarnavimui skirtos pagrindinės klasės vaizdas su pagrindiniais metodais. Klasės užduotis yra bendrauti su įrenginiu, nuskaityti iš jo duomenis ir perduoti juos biometrijos funkcijas realizuojančioje klasėje tolesniam apdorojimui ir panaudojimui. Taip pat šios klasės užduotis yra teisingai nustatyti, kada įrenginys yra prijungtas, kada atjungtas, kada neveikia, ir bet kokiu kitu momentu, bei gražinti informacinius pranešimus apie tai.



Pav. 12. Klasė darbo su pirštų antspaudų įrenginiu

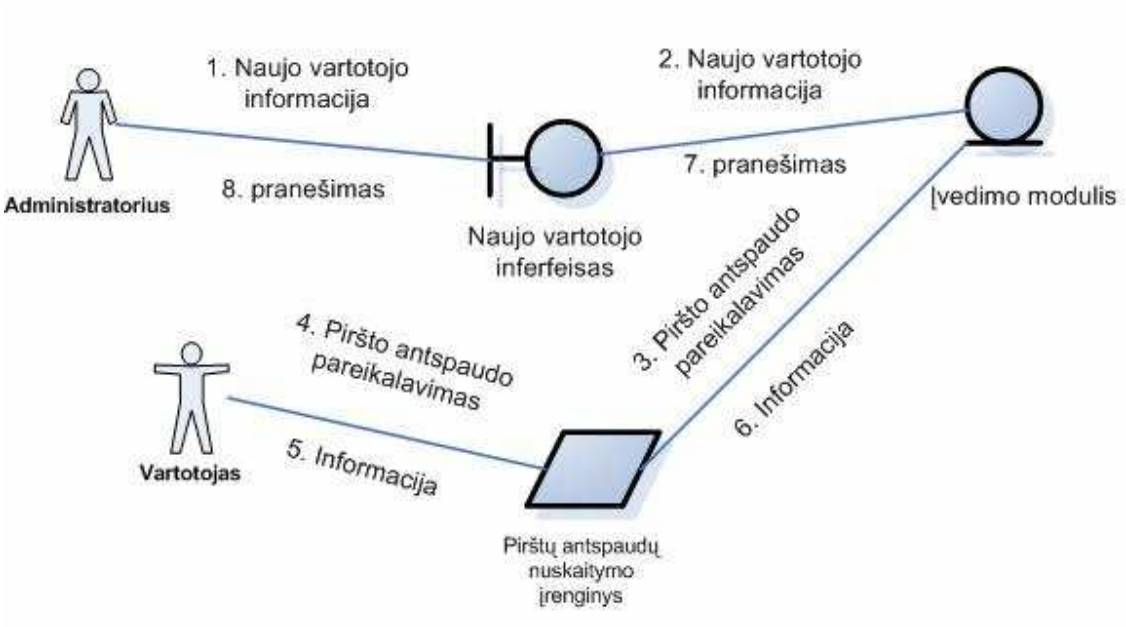
Ši klasė vartotojo pusės programinėje įrangoje, panašiai kaip ir *saugojimo* klasė serverio pusės programinėje įrangoje sukurtos nepriklausomos nuo kitų dalių. Kitaip tariant, pakeitus patį įrenginį, ir aprašius atskirą klasę darbui su juo pagal šios struktūrą, bendru atveju nereikia keisti nieko kito kitose programinės įrangos dalyse. Toks buvo vienas iš sistemos užsakovo reikalavimų, ir rezultatas gautas teigiamas.

Duomenų bazę apdorojanti klasė yra sukurta tokiu pat principu. Norint pakeisti pavyzdžiui iš *MySQL* į *Oracle* ar kokią kitą duomenų bazės valdymo sistemą, reikia tik perrašyti ir pritaikyti specifinius kreipinius ir užklausas konkrečiai naudojamai duomenų bazei.

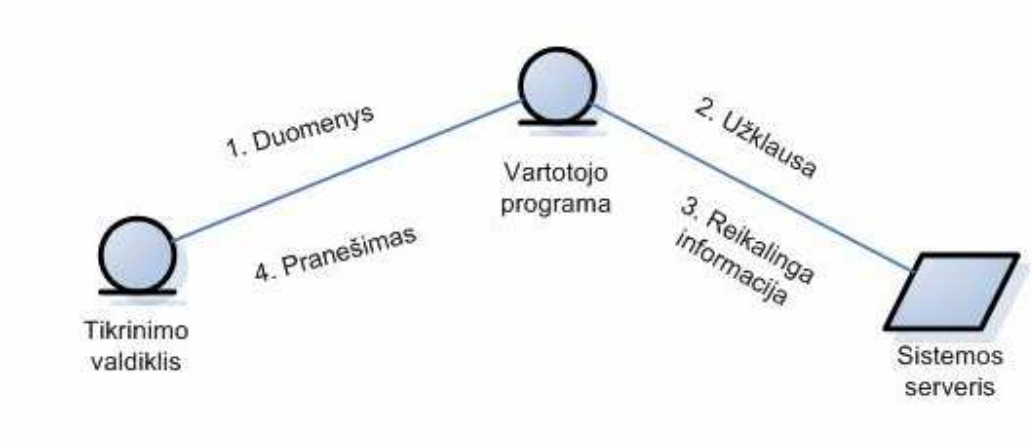
3.4.4. Sistemos dinaminis vaizdas

3.4.4.1. Bendradarbiavimo diagramos

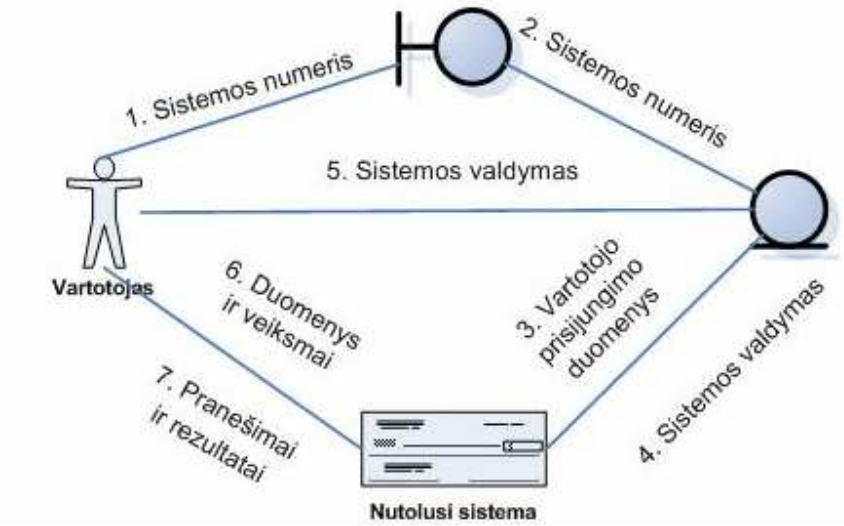
Pateikiamos pagrindinės sistemos dalių bendradarbiavimo diagramos.



Pav. 13. Naujo vartotojo sukūrimo bendradarbiavimo diagrama



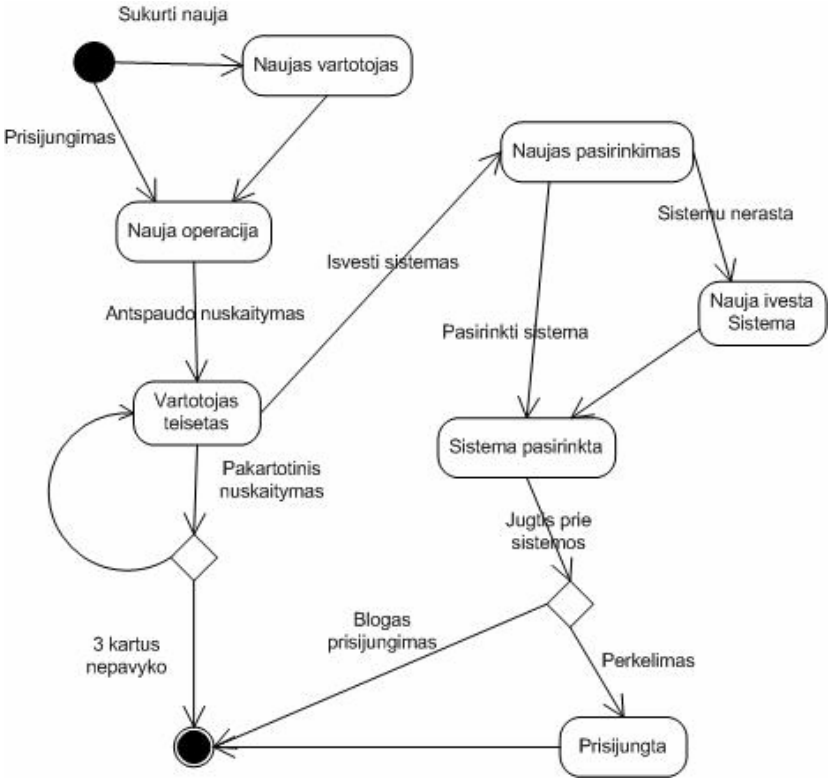
Pav. 14. Pirštų antspaudų patikrinimo bendradarbiavimo diagrama



Pav. 15. Prisijungimo prie nutolusios sistemos bendradarbiavimo diagrama

3.4.4.2. Būsenos diagrama

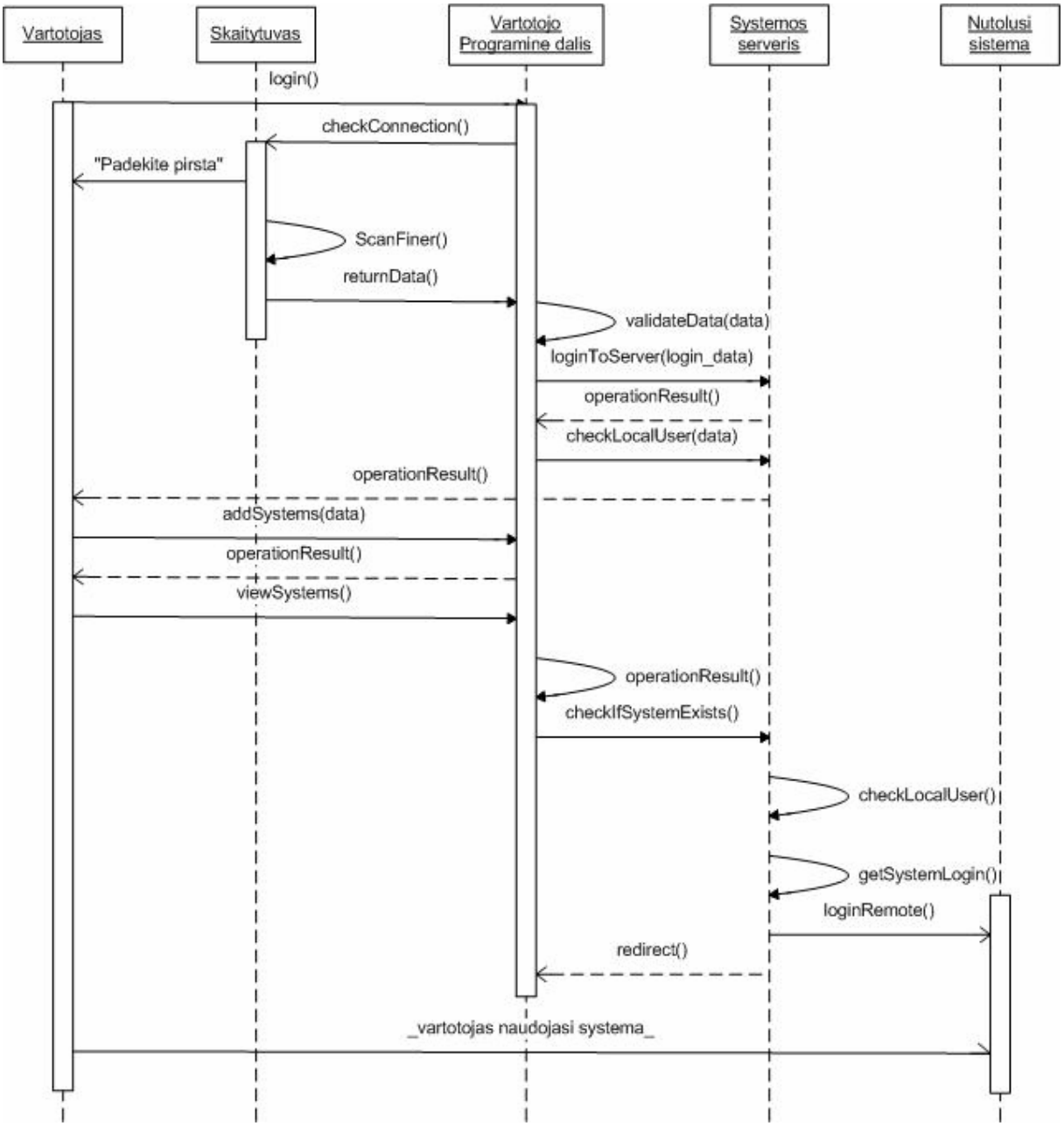
Pateikiama apibendrinta sukurto projekto būsenų diagrama.



Pav. 16. Apibendrinta kuriamos programinės įrangos projekto būsenų diagrama

3.4.4.3. Sekų diagrama

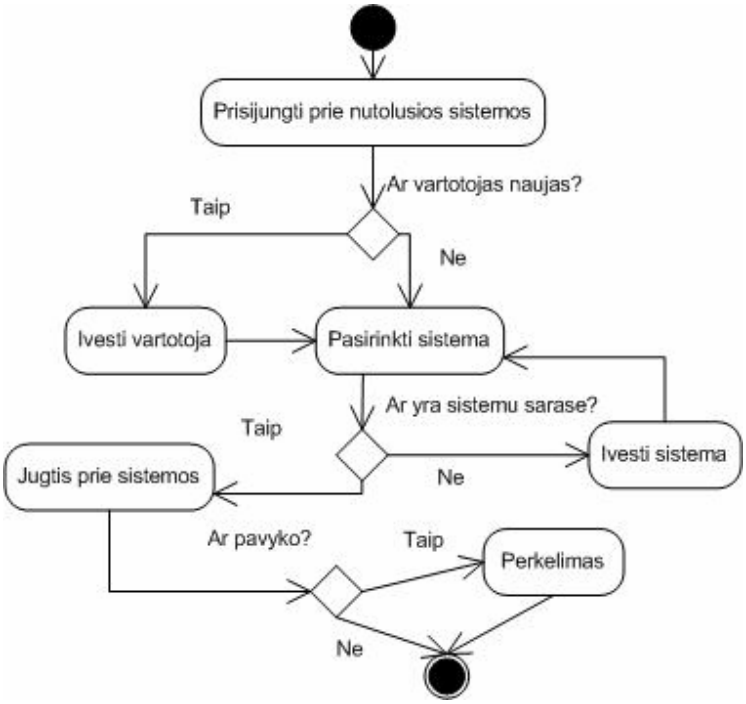
Pateikiama sistemos apibendrinta sekų diagrama (žr. 17 pav). Joje galima matyti, kokie veiksmai yra kokioje programos veikimo stadijoje kviečiami, ir kokie duomenys bei rezultatai yra perduodami tarp konkrečių metodų.



Pav. 17. Apibendrinta sistemos sekų diagrama.

3.4.4.4. Veiklos diagrama

Pateikiamos apibendrinta sistemos veiklos diagrama.



Pav. 18. Sistemos apibendrinta veiklos diagrama.

3.5. Egzistuojančių sistemų palyginimo analizė

Projekto kūrimo metu rinkoje panašių technologijų sprendimų, kuriuose būtų naudojama biometrija, nebuvo, neskaitant vieno sudėtinio produkto, kurį platino *Microsoft* kompanija. Galutinio darbo rengimo metu daugiau panašių sprendimų su realizuotomis biometrinėmis galimybėmis nebuvo sukurta, o pastarasis paminėtasis *Microsoft* sprendimas jau technologiškai atgyveno.

Pagal sistemos savybės, nuotolinio prisijungimo naudojant biometriją sistemą galima gretinti ir palyginti su slaptažodžių saugojimo sprendimais. Buvo išnagrinėta keletas technologinių sprendimų ir pritaikymų, kurie vienu ar kitu aspektu yra panašūs į sukurtą projektą.

3.5.1. Microsoft Fingerprint Reader

Tai produktas, platinamas *Microsoft* kompanijos, kurio pagrindinė užduotis - padėti namų vartotojams lengviau ir paprasčiau prisijungti prie savo *Microsoft Windows XP/Vista* namų operacinės sistemos. Tačiau jau šio produkto aprašyme galima sutikti punktą, kad sistema nėra naudotina kaip saugumo produktas. Kitaip tariant, šio įrenginio saugumo lygis nėra aukštas. Buvo atliktas ne vienas tyrimas, kurio rezultatai patvirtina, kad duomenys iš įrenginio į kompiuterį perduodami neužšifruoti geros kokybės paveiksliuko pavidalu. O su pirštų antspaudu jau galima padaryti ne vieną dalyką. Plačiau apie tai skyriuje apie biometrinių sistemų saugumo testus.

Pats įrenginys - licencijuotas produktas, kurį Microsoft kompanija įsigijo iš kitos kompanijos, *Digital Persona*. Pastaroji gamina ir platina technologiškai identišką produktą *U.are.U 4000*, kuris nuo Microsoft versijos skiriasi įjungtu šifravimu. Pati Microsoft šio fakto, kad jos įrenginyje yra šifravimas išjungtas, nekomentuoja. Todėl už tokio produkto naudojimą versle nėra labai daug argumentų.

3.5.2. Firefox Password Manager

Mozilla kompanijos interneto naršyklė *Firefox* paimta kaip pavyzdys, tačiau egzistuoja panašūs technologiniai sprendimai pritaikyti ir kitoms naršyklėms. Šios sistemos veikia taip, kad pasirinktame puslapyje esančios slaptažodžio įvedimo formos duomenys yra išsaugomi šifruoti kompiuteryje. Tačiau kiek teko susipažinti su tokiomis galimybėmis, tai sistema vartotojui padeda automatiškai suvesti slaptažodį, kai vartotojas suveda savo prisijungimo vardą. Iš to seka, kad tokios sistemos naudojimas yra gana ribotas. Viena, kad paprasta slaptažodžių sistema gali veikti tik vienoje naršyklėje, ir nelabai tinka, kai keli žmonės gali naudotis ta pačia naršyklė ir tomis pačiomis interneto tarnybomis. Antra, kad žinant vartotojo vardą, slaptažodis jau yra suvedamas automatiškai, nebereikia stengtis jį atspėjant. Ir trečia, kad išsiaiškinus tokių sistemų technologinį įgyvendinimą, galima gavus priėjimą prie kompiuterio išsisaugoti reikiamus duomenis ir failus, naudotis jais saugioje vietoje. O žinant, kokio lygio yra prisijungimo prie *Windows* sistemų apsauga, tai nebeatrodo neįveikiamas uždavinys.

3.5.3. PasswordSafe.com

Tai jau keletą metų, sėkmingai ar ne, veikianti tarnyba internete, kuri suteikia galimybę naudojantis jų interneto sistema saugoti savo slaptažodžius. Sistema paprasta, vartotojas užsiregistruoja su stipriu vienu slaptažodžiu, ir prisijungęs joje gali išsisaugoti savo kitus prisijungimo vardus ir slaptažodžius. Taip tenka prisiminti tik vieną prisijungimo ir slaptažodžio kombinaciją.

Tačiau, žiūrint iš pažengusio vartotojo pusės, šioje sistemoje yra vienas niuansas, tai kad visi duomenys saugomi neaišku kur, ir nėra aišku, kas prie jų gali prieiti. Kitaip tariant, išsamiau panagrinėjus tokį sprendimą ir atmetus patogumą, sistemos patrauklumas atrodo toks, kad geriau visgi saugoti svarbią savo informaciją žinomoje vietoje. Tai galima daryti vienu ar kitu būdu apsaugojus savo asmeniniame ar darbo kompiuteryje.

3.6. Tolimesnio sistemos tobulinimo ir plėtojimo galimybės

Sistema kurta su tikslu susipažinti ir išmokti daugiau apie biometriją, apie pirštų antspaudus, kūrimo metu sistema projektuota ir realizuota pagal mokymosi procese išmoktus projektavimo principus. Taip pat sistema kurta taip, kad paskui ją būtų galima panaudoti ir pritaikyti tolimesniems projektams.

Tobulinimo galimybės, kurios buvo aptarinėjamos sistemos kūrimo metu, gali sudaryti:

- Nauja išvaizda, programos dizainas
- Peržiūrėti sistemos duomenų šifravimo algoritmus ir galimai pereiti prie saugesnių technologijų.
- Tikrinti sistemos metu perduodamus duomenis tarp pirštų antspaudų nuskaitymo įrenginio ir programinės įrangos. Pats įrenginys atlieka duomenų šifravimą pagal dokumentaciją, tačiau giliau ir išsamiau ta sritis nebuvo nagrinėta.
- Sistemos serverio dalyje tiesioginio administravimo galimybės, kuriamas atskiras modulis serverio programinėje dalyje.
- Realizuoti programinį kodą su kitokio tipo duomenų bazėmis.
- Sistemos serverio pusės dalies automatinis įdiegimas, nes dabar visus tikrinimus dėl įdiegtų reikalingų komponentų, bei duomenų bazės struktūra turi būti sukuriama rankiniu būdu.

Plėtojimo galimybės gali sudaryti:

- Prisijungimą pritaikyti prie daugiau žinomų sistemų, nes dabar yra padaryta, kad sistema pilnai veikia, atlieka visas funkcijas ir yra ištestuota su užsakovo naudojama Turinio Valdymo Sistema kuriant internetinius sprendimus. Galimas sprendimas peržiūrėti ir modifikuoti išeities tekstą, pritaikant nuotolinio prisijungimo sistema prie kelių žinomų turinio kūrimo ar turinio valdymo sistemų (*Wordpress, Joomla*).
- Galima tokią prisijungimo sistemą pritaikyti prie paprastų kompiuteryje veikiančių sistemų, arba tinklinio sprendimo. Tokiu būdu keičiant ir nereikalaujant, kad sistemos serverio programinė dalis veiktų būtinai serveryje, taip sistemą patalpinant į vieną kompiuterį tinkle.
- Pritaikyti keletui kitų pirštų antspaudų nuskaitymo įrenginių, kad sistema nebūtų pririšta prie vieno tipo įrenginio.

4. BIOMETRINIŲ SISTEMŲ SAUGUMAS

Šiame skyriuje aptariamos biometrinių technologijų savybės apėjimo ir klastojimo būdai, realizuotų sprendimų apžvalga su aprašymais, priemonės galimai tokiems klastojimams apsisaugoti. Taip pat sukurtos sistemos ir naudoto įrenginio tyrimai.

4.1. Saugumas biometrinėse sistemose apskritai

Biometrinių sistemų saugumas ir jo būtinas užtikrinimas tiesiogiai priklauso nuo sistemų panaudojimo srities. Bankuose reikalingas vienoks saugumas, parduotuvėse apsiperkant reikalingas kitoks saugumas, prisijungiant prie asmeninio kompiuterio namuose dar kitoks.

Sistemos bendras saugumas priklauso nuo pasirinktos biometrinės technologijos, kuri gali padėti tą saugumą užtikrinti. Pirštų antspaudai yra laikomi paprasčiausiai naudojama, viena iš tiksliausių ir pakankamai vartotojų priimtina technologija, padedanti atpažinti ar sėkmingai nustatyti asmenis. Tiesa, klaidų kiekis, dėl netinkamai nuskaitytų duomenų šioje technologijoje išlieka gana aukštas. Šiuo atžvilgiu pati geriausia technologija yra akies rainelės nuskaitymas, tačiau taip pat ir nepigi. Biometrinių technologijų palyginimas pateikiamas 1 ir 2 lentelėse, kuriose galima pamatyti visus sėkmingo naudojimo aspektus.

Lentelė 1

Biometrijos Tipas	**Patik-rinimas**	**Atpaži-nimas**	**Tiks-lumas**	**Patiki-mumas**	**Klaidų kiekis**	**Klaidos Tipas I**	**Klaidos Tipas II**
Pirštų antspaudai	Taip	Taip	Didelis	Didelis	1/500	4	4
Veido atpažinimas	Taip	Ne	Vidutinis	Vidutinis	-	3	1
Rankos geometrija	Taip	Ne	Vidutinis	Vidutinis	1/500	5	2
Kalbos atpažinimas	Taip	Ne	Mažas	Mažas	1/50	2	1
Akies rainelė	Taip	Taip	Didelis	Didelis	1/131K	5	5
Akies tinklainė	Taip	Taip	Didelis	Didelis	1/10M	4	4
Parašas	Taip	Ne	Mažas	Mažas	1/50	3	1
Spausdinimas	Taip	Ne	Mažas	Mažas	-	4	1

DNR	Taip	Taip	Didelis	Didelis	-	5	5

Lentelė 2

Biometrijos Tipas	**Saugumo lygis**	**Pastovumas**	**Priimti-numas**	**Atgra-sumas**	**Patogumas**	**Žema kaina**
Pirštų antspaudai	Didelis	Didelis	Vidutinis	4	Didelis	Taip
Veido atpažinimas	Vidutinis	Vidutinis	Vidutinis	5	Vidutinis	Taip
Rankos geometrija	Vidutinis	Vidutinis	Vidutinis	5	Didelis	Ne
Kalbos atpažinimas	Vidutinis	Vidutinis	Didelis	5	Didelis	Taip
Akies rainelė	Didelis	Didelis	Vidutinis	5	Vidutinis	Ne
Akies tinklainė	Didelis	Didelis	Vidutinis	2	Mažas	Ne
Parašas	Vidutinis	Vidutinis	Vidutinis	5	Didelis	Taip
Spausdinimas	Vidutinis	Mažas	Didelis	5	Didelis	Taip
DNR	Didelis	Didelis	Mažas	1	Mažas	Ne

Lentelių 1, 2 paaiškinimai

Patikrinimas (*Verification*) – Ar galima biometrijos tipą panaudoti asmens patikrinimui. Patikrinimas, tai procesas, kurio metu duomenys paimti iš asmens sutikrinami su duomenimis, ankščiau paimtais iš to asmens. Rezultatas pasako, ar tai asmuo yra tas, kuo dedasi.

Atpažinimas (*Identification*) – Ar galima biometrijos tipą panaudoti asmens atpažinimui. Atpažinimas, tai procesas, kurio metu duomenys sutikrinami su didele duomenų baze, ir rezultatas pasako, kuris įrašas atitinka konkretų asmenį, arba jo duomenų bazėje nebuvo.

Tikslumas (*Accuracy*) – tai matas, nusakantis biometrijos tipo gebėjimą atskirti asmenis tarpusavyje. Ši sąvybė dalinai parodo, kiek informacijos yra surenkama vieno matavimo metu ir kiek yra galimų duomenų kombinacijų.

Patikimumas (*Reliability*) – kiek naudinga šio tipo biometrija yra atpažinimo tikslais.

Klaidų kiekis (*Error Rate*) – tai dar žinomas kaip EER santykis ir laikomas vienas pagrindinių biometrijos tipo sistemų kokybę ir saugų naudojimą užtikrinantis matas.

Klaidos tipas I (*False Possitive*) – kaip lengvai galima atkurti duomenis, kad sistema juos atpažintų tinkamais ir priklausančiais visai kitaip įrašui duomenų bazėje.

Klaidos tipas II (False Negative) – kaip lengvai sistema gali neatpažinti tikro jos naudotojo, nors pateikiami korektiški duomenys.

Saugumo lygis (*Security Level*) – Saugumo sistemos nustatymai, kuriems esant dar galimas biometrijos sistemos naudojimas, kuomet yra įvykdomas pakankamas kiekis sėkmingų sistemos veiksmų.

Pastovumas (Long-term Stability) – kaip biometriją naudojanti sistema gali veikti laikui bėgant su tais pačiais duomenimis, jų neatnaujinant.

Priimtinumas (User Acceptance) – kaip noriai visuomenė reaguoja už tokių duomenų nuskaitymą.

Atgrasumas (*Intrusiveness*) – Kiek yra patenkama į asmens privatumą arba kiek reikalaujama specialaus dėmesnio iš asmens biometrinjos duomenų paėmimo metu.

Šiuo atveju kalbos atpažinimas gali atrodyti kaip labai aiškus ir paprastas dalykas, tačiau norint nuskaityti akies tinklainę, asmuo turi tam tikrą laiką labai artimu atstumu žiūrėti į nuskaitymo kamerą, kas nėra labai malonu ar priimtina.

Patogumas (Easy of Use) – Kaip lengva yra naudotis tokios biometrijos teikiamomis paslaugomis tiek vartotojui, tiek pagalbiniam personalui, galimai padedančiam paimti šiuos duomenis.

Žema kaina (*Low cost*) – kiek išlaidų reikalauja tokios sistemos įdiegimas ir įranga.

Faktoriai, lemiantys sėkmingą technologijos panaudojimą:

Pirštų anspaudai – sausumas, nešvarumas, amžius

Veido atpažinimas – apšvietimas, amžius, akiniai, plaukai

Rankos geometrija – sužeidimai, amžius

Balso atpažinimas – triukšmas, oras, peršalimo ligos

Akies rainelė – apšvietimas

Akies tinklainė – akiniai

Parašo atpažinimas – keičiamas parašas

Spausdinimo atpažinimas – rankos ar pirštų traumos, nuovargis

DNR atpažinimas – nėra klaidas lemiančių veiksnių

Apibendrinant galima sakyti, kad sėkmingą biometrijos panaudojimą lemia tai, kaip lengva yra naudotis ta biometrijos sistema, kaip noriai vartotojai ją priima, bei kokias galimybes suteikia prisijungus prie tokios sistemos. Jei sistema bus lengva naudotis, vartotojai bus suinteresuoti pateikti teisingus savo duomenis taisyklingai. Tačiau jei tai bus priėmimas prie kokios svarbios informacijos, piktų ketinimų vedini vartotojai stengsis ją apeiti. Klaidų kiekis apibendrinančioje lentelėje 1 gali parodyti, kaip tai jiems pavyks. Todėl visais aspektais akies rainelės nuskaitymo technologija gali pasirodyti naudinga saugumui užtikrinti reikalingose sistemose, o pirštų antspaudai dėl savo kainos ir prieinamumo naudingesni paprastesnėse sistemose. Tačiau jie naudojami visur, kur gal būt ir netiktų.

4.2. Saugumas pirštų antspaudais paremtose sistemose

Pirštų antspaudais paremtose sistemose vartotojai atpažįstami arba identifikuojami pagal informaciją, saugomą pirštų galuose.

4.2.1. Pirštų antspaudų sistemų patikimumas

Tokiose sistemose saugumas ir patikimumas gali būti užtikrinamas keliais būdais:

- Naudojami pirštų antspaudų nuskaitymo įrenginiai, kurie nepalieka pėdsakų po panaudojimo. Tai gali būti tokie, kuriuos reikia perbraukti pirštu, norint kad įrenginys nuskaitytų duomenis. Tokiu būdu užkertamas kelias paimti piršto antspaudą nuo paties įrenginio, ir atgaminus ant kito paviršiaus, juo pasinaudoti. Tarpinė išeitis sistemose, kurios nėra labai apkrautos naudotojais, reguliariai valyti nuskaitymo įtaisą nuo apnašų.
- Naudojami įrenginiai, kurie savyje turi taip vadinamą gyvumo patikrinimo[4] mechanizmą. Su tokiomis galimybėmis įrenginys ne tik nuskaito pačius biometrinius duomenis, tačiau yra patikrinama, ar tie duomenys yra perduodami gyvo žmogaus konkrečiu matavimo metu. Gyvumo patikrinimą gali sudaryti:
    - Pulso matavimas
    - Drėgmės arba prakaito matavimas
    - Temperatūros nustatymas
    - Atsakas į leidžiama silpną srovę

4.2.2. Nuotolinio prisijungimo naudojant biometriją sistemos tyrimas

Po atlikto tyrimo, naudojantis magistrinio projekto metu sukurta programine įranga, buvo gautos tokios išvados:

[4] Liveness detection

- Kol asmuo nėra susipažinęs su biometrijos technologijomis, tokia sistema jam atrodo sudėtinga, tačiau įdomi. Buvo paprašyta 20 eilinių asmenų pasinaudoti šia sistema, ir po trumpo instruktažo apie sistemos veikimą nė vienas neatsisakė pasitikrinti, ar jo pirštų anspaudai gali būti vartojami kaip slaptažodis. Galima sakyti, kad Lietuvoje visuomenės informavimas apie biometrines technologijas yra labai mažas.
- Pirštų antspaudų nuskaitymo įrenginys palieka pėdsakus po pasinaudojimo. Bendru atveju tai matosi ant šiek tiek apdulkėjusio paviršiaus, arba su šiek tiek nešvariais pirštais pasinaudojus nuvalytu įtaisu. Todėl, autoriaus teigimu, toks įrenginys tinka tik namų vartotojo reikmėms.
- Įrenginys taip pat nepalaiko gyvumo testo, yra nuskaitoma tik informacija apie piršto antspaudo struktūrą, tačiau nematuojami jokie kiti papildomi veiksniai.
- Su turimomis ir prieinamomis priemonėmis, šios sistemos nepavyko apeiti. Todėl iš biometrinio įrenginio pusės saugumo lygis tokioje sistemoje yra užtikrinamas pakankamas.

4.2.3. Pirštų antspaudų sistemų apsaugų apėjimas

Yra nemažai metodų, kaip galima apeiti pirštų antspaudais paremtas sistemas, tačiau visi jie susideda iš kelių esminių etapų:

- Originalaus piršto antspaudo paėmimas. Tai gali būti sėkmingiausiai atliekam nuo stiklo ar stiklinio paviršiaus. Su specialiomis priemonėmis, naudojamomis teisėsauginiknų, galima tai padaryti ir nuo kitų nemedžiaginių paviršių. Stiklas tinka todėl, kad ant piršto galo yra susikaupę tam tikri riebalai, kurie prisilietus prie stiklo geriausiai matomi. Toks antspaudas išryškinamas su greitai limpančių klijų pagalba, nes klijuose esanti medžiaga reaguoja su riebalais, ir juos padaro geriau matomus. Taip pat išryškinimui naudojama smulki miltelinė medžiaga, kuri prilimpa prie riebalų.
- Išryškintas piršto antspaudas yra nufotografuojamas, ir apdorojamas specialiomis grafikos apdorojimo programomis, norint paryškinti piršto antspaudą sudarančias rieves.
- Toks gautas apdorotas rezultatas yra atspausdinamas ant specialaus permatomo popieriaus, naudojamo projektuoti skaidres, su lazeriniu spausdintuvu. Toneris prilimpa prie skaidrės, ir susidaro nedideli iškilumai.
- Tolesnis etapas gali būti atliekamas keliais būdais. Viena iš paprasčiausių yra naudojant baltos masės medžio ir popieriaus klijus užtepti atspausdintą vietą, ir palaukti kol išdžiūs.

Kitas būdas yra naudojant balistinę želė, kurios rezultatas negaunamas toks kietas kaip iš medžio klijų.

- Galutinis etapas yra priklijuoti gautą rezultatą prie piršto permatomais klijais ir jau galima sakyti turime naują tapatybę.

Kiekvienas iš punktų gali turėti tam tikrų niuansų, todėl testuojant turimą *Microsoft Fingerprint Reader* įrenginį norimą rezultatą pavyko gauti ne iš pirmo bandymo. O rezultatas buvo prisijungti prie operacinės sistemos įrenginio pagalba.

Kitas iš būdų yra tiesiog reikiamos kokybės piršto antspaudą atsispausdinti ant balto popieriaus ir išsikirpti. Tokiu būdu galima apeiti ne vieną įrenginį, pavyko ir jau minėtą iš Microsoft kompanijos. Tačiau nei pasidarius antspaudą sudėtinguoju būdu, nei atsispausdinus ant popieriaus, nepavyko apeiti pagrindinio projekto nuskaitymo įrenginio.

5. IŠVADOS

1. Magistriniame darbe aptartos bei magistrinio projekto metu panaudotos biometrinės technologijos leido iš arčiau ir išsamiau susipažinti su šia įdomia, naujoviška ir perspektyvia sritimi.
2. Buvo išanalizuotos galimos biometrinių technologijų taikymo sritys praktikoje, bei atliekamas tyrimas, kokios technologijos galėtų būti panaudojamos Lietuvos rinkoje, kokie biometrinių technologijų panaudojimo atvejai nesuteikia pranašumo prieš paprastas slaptažodžių ar kortelių sistemas.
3. Praktinio darbo metu buvo sukurtas nuotolinio prisijungimo prie nutolusių sistemų naudojant pirštų antspaudų biometriją projektas ir programinė įranga. Jos pagalba supaprastinamas prisijungimas prie dažnai naudojamų sistemų, įgalinantis tokiose sistemose naudojamus slaptažodžius pakeisti saugesniais ir sudėtingesniais, pagerinant bendrą sistemos ir vartotojo saugumą.
4. Eksperimento būdu patikrintas magistrinio projekto metu naudojamų pirštų antspaudų nuskaitymo įrenginių patikimumas
5. Išanalizuota magistrinio projekto metu sukurta programinė įranga bei pateikti siūlymai, kaip ją galima būtų patobulinti, kokie galimi tolesni projekto vystymo etapai bei realus panaudojimas.

6. LITERATŪROS IR INFORMACIJOS ŠALTINIAI

1. http://www.m-w.com/dictionary/biometrics [Žiūrėta 2009-05-20]
2. http://en.wikipedia.org/wiki/Automated_Fingerprint_Identification_System [2009-05-20]
3. R. Klarke, *„Human Identification In Information Systems: Management Challenges And Public Policy Issues,“*, Info. Technol. People, vol 7, no. 4, p. 6-37, 1994
4. D. Sims, *„Biometrics Recognition: Our Hands, Eyes and Faces Give Us Away“*, IEEE Computer Graphics and Applications, 0272-17-16/94, 1994
5. J.D. Woodward, *„Biometrics: Pricacy‘s Foe or Pricacy‘s Friend?“*, Proc. IEEE Special Issue on Automated Biometrics, vol. 85, no. 9, p. 1480-1492, 1997
6. B. Carter, *„Biometrics Technologies, What They Are and How They Work“*, in Proc. CTST’97, Orlando, EL, 1997
7. R. Chandrasekaran, *„Brave New Whorl: ID Systems Using The Human Body Are Here, But Privacy Issues Persist“*, Washington Post, Mar. 30, 1997
8. A. Davis, *„The Body as Password“*, Wired, July, 1997
9. D.R. Richards, *„Rules of Thumbs For Biometrics Systems“*, Security Manage, Oct. 1, 1995
10. G. Lanton, *„Biometrics: A New Era in Security“*, IEEE Spectrum, p. 16-18, Aug. 1998
11. R.Mandelbaum, *„Vital Signs of Identity“*, IEEE Spectrum, p. 22-30, Feb. 1994
12. M. Golfarelli, D. Maio and D. Maltoni, *„On the Error-Reject Trade-Off in Biometrics Verification Systems“*, IEEE Trans. Pattern Anglysis and Macine Intelligence, vol. 19, no. 7, p. 786-796, 1997
13. H.C. Lee and R.E. Gaensslen, editors, *„Advances in Fingerprint Technology”*, Elsevier, New York, 1991
14. A.K. Jain, R. Bolle and S.Pankanti (editors), *„Biometrics Indentification in a Networked Society“*, Kluwer Academic Press, 1999
15. A. Jain, L. Hong and R. Bolle, *“On-Line Fingerprint Verification”*, IEEE Trans. Pattern. Analysis and Machine Intelligence, vol. 19, no. 4, p. 302-314, 1997
16. http://biometric.lt/2009/04/biometrijos-galimybes-i-musu-ausis-gali-buti-imontuoti-slaptazodziai/ [Žiūrėta 2009-05-20]
17. http://www.tech-faq.com/two-factor-authentication.shtml [Žiūrėta 2009-05-20]
18. http://www.pcworld.com/article/124978/researcher_hacks_microsoft_fingerprint_reader.html [Žiūrėta 2009-05-20]
19. http://ignoranceisfutile.wordpress.com/tag/biometrics/ [Žiūrėta 2009-05-20]

20. http://ctl.ncsc.dni.us/biomet%20web/BMCompare.html [Žiūrėta 2009-05-20]
21. http://en.wikipedia.org/wiki/Type_I_and_type_II_errors [Žiūrėta 2009-05-20]
22. http://portal.acm.org/citation.cfm?id=1153776 [Žiūrėta 2009-05-20]
23. http://en.wikipedia.org/wiki/RFID [Žiūrėta 2009-05-20]

7. TERMINŲ IR SANTRUMPŲ ŽODYNAS

FRR – *False Rejection Rate* – klaidingo atmetimo laipsnis biometrinėse sistemose

FAR – *False Acceptance Race* – klaidingo priėmimo laipsnis biometrinėse sistemose

EER – *Equal Error Rate* - vienodas klaidų santykis, reikšmių susikirtimas

AFIS – *Automated Fingerprint Identification System* – automatinė pirštų antspaudų atpažinimo sistema

PIN – *Personal Identification Number* – asmens tapatybės

RFID – *Radio-frequency identification* – asmens, prekės ar objekto sekimas, stebėjimas ir informacijos nuskaitymas per atstumą, radijo bangų pagalba.

8. PRIEDAI

1 Priedas. Sistemos įdiegimo dokumentas

SISTEMOS ĮDIEGIMO AKTAS

Šiuo aktu Paslaugos gavėjas priima, o Kęstutis Mačiulaitis perduoda Sistemos gavėjo naudojimui sukurtą Prisijungimo prie nuotolinių sistemų, naudojant biometriją sistemą, ir atlieka šios paslaugos įdiegimo darbus pagal 2008-10-13 sutartį Nr. 1478-20-05.

1.SISTEMOS GAVĖJAS

fizinio asmens vardas, pavardė/ juridinio asmens pavadinimas	UAB „UNIVELAS“	fizinio asmens nuolatinė gyvenamoji vieta / juridinio asmens buveinės adresas	Žemgulio g. 8, Kaunas
fizinio asmens kodas, paso/asmens tapatybės kortelės nr./juridinio asmens kodas	136048069	Atsiskaitomosios sąskaitos Nr.	
PVM mokėtojo kodas	LT360480610	Banko kodas ir pavadinimas	
Įgaliotas asmuo	Giedrius Kurlavičius	Atstovavimo dokumento Nr. ir išdavimo data	
Asmuo ryšiams	Giedrius Kurlavičius	Telefono numeris	837761703
Faksas	837761703	El. Paštas	info@univelas.lt

2. SISTEMOS ĮDIEGIMO ADRESAS

Žemgulio g. 8, Kaunas

3. PERDUOTA IR ĮDIEGTA SISTEMA

Nr.	Sistemos pavadinimas	Tipas
1	NUOTOLINIO PRISIJUNGIMO NAUDOJANT BIOMETRIJĄ SISTEMA	Programinė įranga

4. DARBUS ATLIKO IR ĮDIEGTĄ SISTEMĄ PERDAVĖ

Vardas, pavardė, pareigos	Parašas, data
KĘSTUTIS MAČIULAITIS, KTU STUDENTAS	

5. SISTEMOS GAVĖJAS:

Pasirašęs asmuo patvirtina, kad jam perduota sistema, nurodyta šio akto 3 punkte, veikia tvarkingai, ir dėl šios sistemos įdiegimo bei veikimo jokių pretenzijų jis neturi.	
Vardas, pavardė, pareigos	Parašas, data
GIEDRIUS KURLAVIČIUS, PROJEKTŲ VADOVAS	