KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

KOMPIUTERIŲ KATEDRA

Kristijonas Kulikauskas

BIOMETRINĖS AUTENTIFIKACIJOS MODELIO AUTOMOBILIAMS SUKŪRIMAS IR TYRIMAS

Informacinių technologijų magistro baigiamasis darbas

Darbo vadovas
doc. dr. A. Venčkauskas

KAUNAS, 2011

KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

KOMPIUTERIŲ KATEDRA

TVIRTINU
Katedros vedėjas
prof. dr. E. Kazanavičius
2011 05

BIOMETRINĖS AUTENTIFIKACIJOS MODELIO AUTOMOBILIAMS SUKŪRIMAS IR TYRIMAS

Informacinių technologijų magistro baigiamasis darbas

Vadovas
doc. dr. A. Venčkauskas
2011 05

Recenzentas
doc. dr. Stasys Maciulevičius
2011 05

Atliko
IFN-9/1 gr. stud.
Kristijonas Kulikauskas
2011 05

KAUNAS, 2011

TURINYS

DEVELOPMENT AND RESEARCH OF BIOMETRIC AUTHENTICATION MODEL FOR CARS

SUMMARY

Automobile security is always relevant. Existing security systems could be easily bypassed and are not a big barrier for thieves. So there is a necessity for a innovative authentication system.

Biometrics consist of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In computer science, in particular, biometrics is used as a form of identity access management and access control. It could be also used for automobile security.

Finger vein comparison is a relatively new form of biometrics, which could also be used for authentication. Images of finger veins could be obtained illuminating fingers with near-infrared light. Those images are very unique and different for every person and every finger.

In this research biometric authentication model for automobiles is developed and researched. Three image recognition algorythms were tested in the experiment, determining which one is less sensitive to resolution changes and noise. The results were given, proposing use of one algorythm, in our model of biometric authentication system for automobiles.

Keywords: biometrics, authentication, finger vein, image comparison, automobile security.

ĮVADAS

Automobilių apsauga visada buvo, yra ir bus aktuali. Esamos apsaugos priemonės nesunkiai apeinamos ir nesudaro didelių kliūčių, norint transporto priemonę pasisavinti. Reikalinga naujoviška vairuotojo autentifikavimo sistema, galinti sumažinti šią, pasisavinimo tikimybę.

Tam tinka biometrija – asmens bruožų ar charakteristikų statistinė analizė ir nustatymas. Juos nustačius, gali būti naudojami asmens autentifikacijai. Tai daroma lyginant su anksčiau užfiksuotu šablonu. Naudojama šioms autentifikacijoms: kompiuteriuose tinklų, praėjimo kontrolės, bankomatuose, apsipirkimams kreditinėmis kortelėmis, mobiliuosiuose telefonuose, delniniuose kompiuteriuose, medicininių įrašų valdymui, nuotoliniame mokymesi ir t.t.

Pirštų kraujagyslės – nauja biometrinės autentifikacijos forma. Kadangi kraujagyslės yra po oda, jos yra nematomos apšviečiant natūralia šviesa. Tačiau jos puikiai matomos apšvietus artima infraraudoniems spinduliams šviesa, kadangi ši šviesa lengvai sklinda per žmogaus kūno audinius, bet yra blokuojama tokių pigmentų, kaip hemoglobinas ar melaninas. Kadangi hemoglobino didelė koncentracija yra tik kraujagyslėse, apšvietus artima infraraudonosioms bangos šviesa, šios atrodo kaip tamsios linijos. Tai yra palyginti nauja technologija, Japonijoje plačiai naudojama autentifikacijai bankomatuose, o nuo 2010 gegužės mėn. tokia autentifikacija paremti bankomatai pradėti eksploatuoti ir Europoje.

Šio darbo tyrimo sritis – biometriniai autentifikavimo metodai, objektas – biometrinė autentifikavimo sistema automobiliui. Tyrimo problema – vairuotojo autentifikacijos problema automobiliuose: autentifikavimo patikimumas, naudojimo patogumas, riboti ištekliai.

Darbo tikslas – sukurti ir ištirti biometrinės autentifikacijos automobiliams modelį.

Kraujagyslių skaneris būtų montuojamas automobilio išorėje, durelių rankenoje. Esant automobilinei kompiuterio sistemai su ekranu bei valdymu, šios sistemos galėtų būti jungiamos kartu. Neesant – prie autentifikavimo sistemos galėtų būti jungiamas atskiras lietimui jautrus ekranas, taip suteikiant sistemos valdymo bei rezultatų gavimo galimybes. Vartotojų administravimas būtų atliekamas įgaliotame gamintojo servise. Skaičiavimams atlikti būtų naudojamas signalinis, specialiai optimizuotas skaitmeninių signalų apdorojimui, procesorius.

Eksperimento metu tyrėme trijų atvaizdų apdorojimo algoritmų tinkamumą pirštо kraujagyslių atvaizdų autentifikacijos tinkamumui. Stebėjome bei fiksavome, kaip keičiasi rezultatai, kintant atvaizdo raiškai ir kokybei.

Nustatėme mažiausiai, esant žemesnei raiškai, į atvaizdo kokybę neigiamai reaguojantį algoritmą. Kad užtikrintai siūlyti šį algoritmą naudoti mūsų siūlomame autentifikacijos sistemos modelyje, reiktų atlikti daugiau eksperimentinių tyrimų su didesniu skaičiumi didesnės pradinės raiškos pirštо kraujagyslių atvaizdų, raišką mažinant, o triukšmą didinant mažesniais, tolygiais žingsniais, ištirti ir kitus atvaizdų atpažinimo algoritmus.

Darbo struktūra:

- Pirmajame skyriuje apžvelgiamos automobilių apsaugos priemonės ir metodai. Iškeliama saugos problema, aprašomi autentifikavimo būdai. Taip pat atliekama biometrinių priemonių analizė, aprašomas autentifikacijos veiklos modelis, biometrinių sistemų veikimo principas bei situacija Lietuvoje.

- Antrajame skyriuje aprašomas siūlomas naudoti autentifikacijos metodas, paremtas pirštо kraujagyslių vaizdu. Aprašoma sistemos architektūra bei atliekami veiksmai, duomenų bazė, biometrinės automobilių apsaugos sistemos modelis. Išsikeltas darbo tikslas, suformuluoti uždaviniai bei apsibrėžta metodo taikymo sritis ir pagrindiniai reikalavimai.

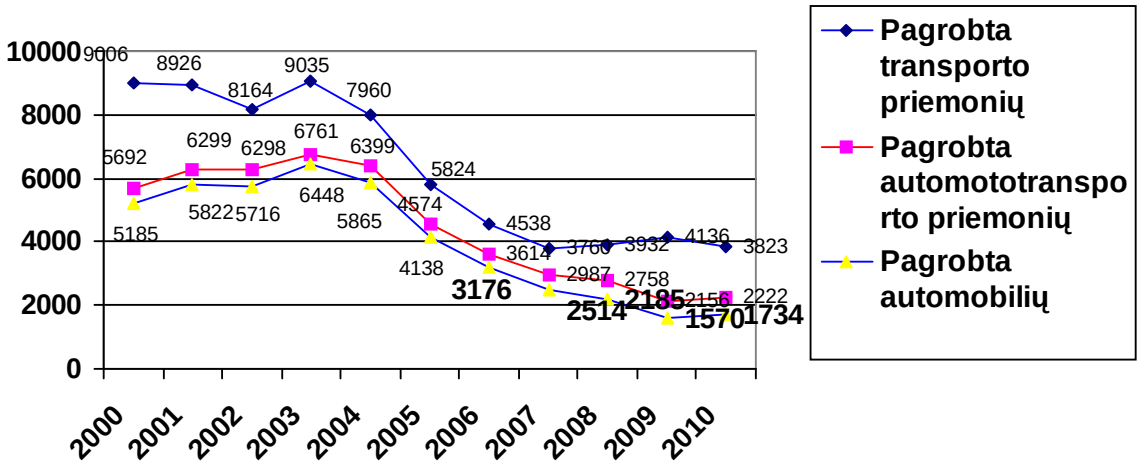
- Trečiasis skyrius skiriamas eksperimentui. Tiriamas trijų atvaizdų apdorojimo algoritmų tinkamumas pirštо kraujagyslių atvaizdų autentifikacijai. Aprašoma tyrimo eiga, pateikiami gauti rezultatai, jų analizė.

- Ketvirtajame skyriuje pateikiama trumpa viso darbo santrauka ir bendros išvados, paminėti tolimesni darbai.

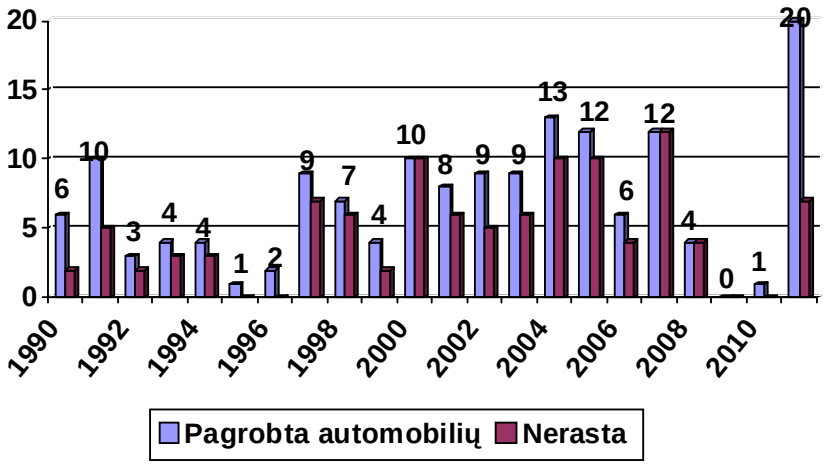
1. AUTOMOBILIŲ APSAUGOS PRIEMONIŲ IR METODŲ ANALIZĖ

1.1 Automobilių apsaugos problema

Kriminogeninė situacija transporto priemonių vagysčių srityje šalyje keičiasi – pagrobiama šiek tiek daugiau automobilių. 2010 metais šalyje pagrobti 1 734 automobiliai, tai 164 automobiliu arba 10.4 proc. daugiau nei 2009 metais (1570). Lengvųjų automobilių buvo pagrobta 1 631, tai 135 automobiliais arba 9 proc. daugiau nei 2009 metais arba 94 proc. visų šalyje pagrobtų automobilių. [1]. Nors kalbant apie paskutinius 10 metų, automobilių vagysčių skaičius mažėjo, trumpuoju laikotarpiu, pastaruoju metu matoma šio skaičiaus didėjimo tendencija. Pablogėjus ekonominei situacijai bei iš užsienio grįžtant asmenims, užsiėmusiems šia veikla, galima numatyti, kad ir kriminogeninė situacija tik blogės, apsaugos problema vėl taps aktualesne . Nors automobilių parkas „jaunėja“, vis daugiau jų įsigyjama su gamyklinėmis signalizacijomis, vagys irgi nesnaudžia, prisitaiko prie jų. Taigi būtina išnaudoti naujas technologijas, kiek įmanomą apsunkinant jiems darbą.



1 pav. Automobilių grobimų dinamika 2000 – 2010 metais



2 pav. 1990-2010 m. sausio mėnesio automobilių grobimai pagal pagaminimo metus

1.2 Automobilių apsaugos priemonės

Daugumoje nuo 1995 m. pagamintų automobilių yra montuojamas stabdiklis (*immobilizer*) – automobilio gamintojo įdiegta apsaugos sistema, kuri elektroniniu būdu blokuoja variklio įpurškimo kompiuterio darbą. Atsakiklis (*transponder*) – tai specializuota mikroschema, talpinama į rakto korpusą, veikia per atstumą induktyvinių kilpų pagalba. Stabdiklis - tai elektroninis valdymo blokas, nuskaitantis informaciją iš atsakiklio, kuri sulyginama su nustatyta. Taip pat naudojamos sistemos, kuriose reikia įvesti *PIN* kodą, infraraudonųjų spindulių pulteliai ar kortelės [10].

Signalizacijos naudojamos įvairiausios: nuo kainuojančių kelis šimtus, turinčių tik paprastą smūgio jutiklį, iki naujų, turinčių magnetinio rezonanso smūgio daviklius, interaktyvų pranešimų gaviklį su *LED* displėjumi, ultragarsinius tūrinius, posvyrio ir kt. jutiklius.

Mechaniniai pavarų dėžės užraktai automatinėms ir mechaninėms pavarų dėžėms pavarų svirtis blokuoja atbulinės eigos ir „P“ pozicijose.

Yra sukurtos ir naudojamos kelios biometrinės automobilinės autentifikacijos sistemos. Dauguma jų paremtos pirštų atspaudų skanavimu. Tokie skaneriai yra sumontuoti išorėje ant durelių, viduje atsidarančioje panelėje, ant užvedimo mygtuko ir pan. [6], [7]

Naujuose, aukštesnės, vadinamuose *premium* klasės automobiliuose, (Audi A6, A8, Q7, BMW 5 ir 7 klasės ir t.t.), naudojamos balsu paremtos sistemos. Jos naudojamos

autentifikacijai bei jų pagalba galima valdyti radiją, telefoną, navigacijos sistemą. Šios sistemos remiasi kalbos atpažinimo principu [20].

Naudojamos ir autentifikavimo sistemos, kur piršto antspaudų skaneris įmontuotas kartu su raktais nešiojamame pultelyje.

Lentelė nr. 1 Dažniausiai naudojamų automobilių autentifikacijos metodų įvertinimas

Autentifikacijos būdas	**Naudojimosi lengvumas**	**Klaidų priežastys**	**Užtikrinamas apsaugos lygis**
Raktas	Aukštas	Pamestas/pavogtas	Žemas
Pin kodas	Vidutinis	"Nužiūrėtas"	Vidutinis
Transponderis	Aukštas	Pamestas/pavogtas	Vidutinis
Mechaninis pavarų dėžės užraktas	Vidutinis	Pamestas/pavogtas	Vidutinis
Išorinis piršto antspaudų skeneris	Vidutinis	Purvas, temperatūrų svyravimai, galimybė panaudoti kitur paliktus antspaudus	Vidutinis
Nešiojamas piršto antspaudų skeneris	Aukštas	Pamestas/pavogtas	Vidutinis

1.3 Vartotojų autentifikavimo metodai

Vienu didžiausių informacijos saugumo prioritetų yra patvirtinimas, kad asmuo, pasiekiantis konfidencialią ar slaptą informaciją, yra įgaliotas tai atlikti. Jei asmuo įrodo, kas esąs, jam tai leidžiama daryti. Kitu atveju – priėjimas bus uždraustas.

Kitaip tariant, autentifikacija - tai sugebėjimas įrodyti, kad esi tas, kuo sakai esąs.

Trys naudojami autentifikacijos tipai:

- Kažkas, ką turi - skaitmeninis sertifikatas, sumanioji kortelė, raktas ir pan.
- Kažkas, ką žinai – slaptažodis, asmeninis identifikacinis numeris (*PIN*) ir pan.
- Kažkas, kuo esi – biometrinis bruožas.

Paskutinis tipas yra pats saugiausias, nes jo negalima pamesti, paskolinti, pavogti ar užmiršti [2].

1.3.1 Biometrinių priemonių analizė

Biometrija, tai asmens bruožų ar charakteristikų statistinė analizė ir nustatymas. Juos nustačius, gali būti naudojami asmens autentifikacijai. Tai daroma lyginant su anksčiau užfiksuotu šablonu.

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 šia savybę;
- *Pastovumas*, parodantis, jog savybė turi būti pakankamai atspari ir nekintanti bėgant laikui ar keičiantis aplinkos sąlygoms;
- *Renkamumas*, reiškia paimtą savybių požymį esant neskaičiuojamu;
- *Priimtinumas*, rodantis 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 apgauti sistemą.

Ši sritis nepasiduoda pasaulinei krizei, kadangi dėl savo unikalių galimybių yra kritinė tapatybės identifikacija paremtų IT sprendimų evoliucijai. Planuojama, kad kasmet ši rinka augs 19,96%, bei 2017 pasieks 11 milijardų JAV dolerių metinę apyvartą. [3]

Pirštų antspaudai bus saugojami elektroninėse schemose pasuose, kurie bus naudojami Europos sąjungai priklausančiose valstybėse nuo 2012 metų.

Naudojama šioms autentifikacijoms: kompiuteriuose tinklų, praėjimo kontrolės, bankomatuose, apsipirkimams kreditinėmis kortelėmis, mobiliuosiuose telefonuose, delniniuose kompiuteriuose, medicininių įrašų valdymui, nuotoliniame mokymesi ir t.t. Tačiau vien tik kelių rūšių biometrinių duomenų naudojimas nereiškia geresnių sistemos charakteristikų. Blogai suprojektuota sistema gali turėti blogesnes charakteristikas, nei naudojant vienos rūšies duomenis, kainuoti brangiau ir sukelti papildomus nepatogumus vartotojams bei administratoriams (pvz. sudėtingos registracijos procedūros).[4]

1.3.2 Biometrinės autentifikacijos veiklos modelis

Nepaisant, kad naudojami skirtingi biometrinės autentifikacijos metodai, visi jie turi bendrą teorinį veiklos modelį:

- Informacijos surinkimas ir įtraukimas į sąrašą,
- Šablono saugojimas,
- Informacijos lyginimas.

1.3.2.1 Informacijos surinkimas

Tai procesas, kai asmens biometrinės fizinės ir elgesio savybės yra įvedamos į sistemą. Skirtingos sistemos naudoja skirtingus įrenginius duomenų paėmimui. Originalūs įrenginio signalai tuomet verčiami į skaitmeninius. Labai svarbi paimtų duomenų kokybė, kuo ji geresnė, tuo mažiau pašalinių veiksnių ir triukšmų.

1.3.2.2 Šablono saugojimas

Kai vartotojo duomenys įtraukiami į sistemą ir šablonas užfiksuojamas, jis turi būti saugomas, kad vėliau galėtų būti pasiektas. Yra trys pasirinkimo kaip juos saugoti variantai, kiekvienas turintis privalumų ir trūkumų:

- Saugoti šabloną biometriniame skaitymo įrenginyje.
- Saugoti šabloną centralizuotai nuotolinėje duomenų bazėje.
- Saugoti šabloną nešiojamame žetone (intelektualiojoje kortelėje).

Pagrindinis laikymo skaitymo įrenginyje privalumas yra atsakymo laikas. Nereikia laukti kitų sistemų, ar tinklo įrenginių atsakymų. Daugumą sistemų gali valdyti nedidelį kiekį šablonų. Bei jei yra keli tūkstančiai vartotojų, sistema nebeveikia kaip tikėtasi. Taip pat sugedus šiai sistemai, dingtų visi įvesti duomenys, vartotojus reiktų pakartotinai registruoti.

Informacijos centralizuotas saugojimas nuotolinėje duomenų bazėje labiausiai tinka, jei sistemoje yra daugybė vartotojų. Tai taip pat suteikia galimybę pridėti papildomų saugumo lygių. Pagrindiniai trūkumai yra papildomos įrangos reikalingumas bei tinklo srautas, sukuriamas tarp skaitytuvo ir duomenų bazės. Taip pat sutrikus tinklo ryšiui, iš skaitytuvo nebūtų jokios naudos.

Šablono saugojimo intelektualiojoje kortelėje pagrindinis privalumas yra tai, kad vartotojas vienintelis turės šabloną. Tokiu atveju kortelę galima naudoti neribotame skaičiuje skaitymo įrenginių, taip supaprastinant autentifikavimąsi skirtinguose įmonės padaliniuose. Tačiau gali brangiai kainuoti kortelės išdavimas kiekvienam įmonės darbuotojui. Taip pat papildomų išlaidų gali prireikti, jei darbuotojai nelinkę saugoti kortelės ir laikas nuo laiko reikia išduoti naujas.

1.3.2.3 Informacijos lyginimas

Šiame žingsnyje vyksta ką tik nuskaityto biometrinio požymio lyginimas su anksčiau nuskaitytu ir įvestu į duomenų bazę šablonu. Gali veikti identifikavimo režimu, kai biometrinė sistema turi lyginti nuskaitytą požymį su visais turimais šablonais, vykdomas „vieno su daugeliu“ lyginimas. Tačiau dažniau naudojamas autentifikavimo režimas, kai prieš lyginimą nurodamas vartotojas, ar įdedama sumanioji kortelė, o vietoj slaptažodžio nuskaitomas biometrinis požymis ir vykdomas „vieno su vienu“ lyginimas.

1.3.3 Našumo matavimai

Renkantis biometrinę sistemą, yra keturi pagrindiniai efektyvumo matavimai, į kuriuos turėtų būti atsižvelgta. Pirmieji trys nagrinėja sistemos tikslumą. Tikslumas yra svarbiausias bet kokios autentifikavimo sistemos kriterijus. Jei sistema negali tiksliai atlikti savo veiksmų, tuomet saugumas yra sukompromituotas. Ketvirtasis matavimas nagrinėja sistemos greitį. Nors jis ir ne toks svarbus iš sistemos funkcionalumo pusės, visos sistemos darbo greitis yra labai svarbus galutiniam vartotojui.

1.3.3.1 Neteisingo atmetimo galimybė (*FRR*)

Neteisingo atmetimo galimybė išreiškiama procentais, nurodant kaip dažnai sistema neteisingai atmeta bandymą teisėtai prisijungti jau įvestam vartotojui. Kiek svarbus yra šis dažnis, priklauso nuo autentifikacijos sistemos vaidmens. Jei pagrindinis sistemos tikslas yra praėjimo kontrolė nuo nepageidaujamų įsilaužėlių, jis gali būti mažiau svarbus. Tačiau jei sistema naudojama klientų autentifikavimui, pvz. bankomatuose ar parduotuvėse, klaida gali būti labai svarbi. Jei klientas negali autentifikuotis, jis bus nepatenkintas, ir galbūt bus prarastos pajamos.

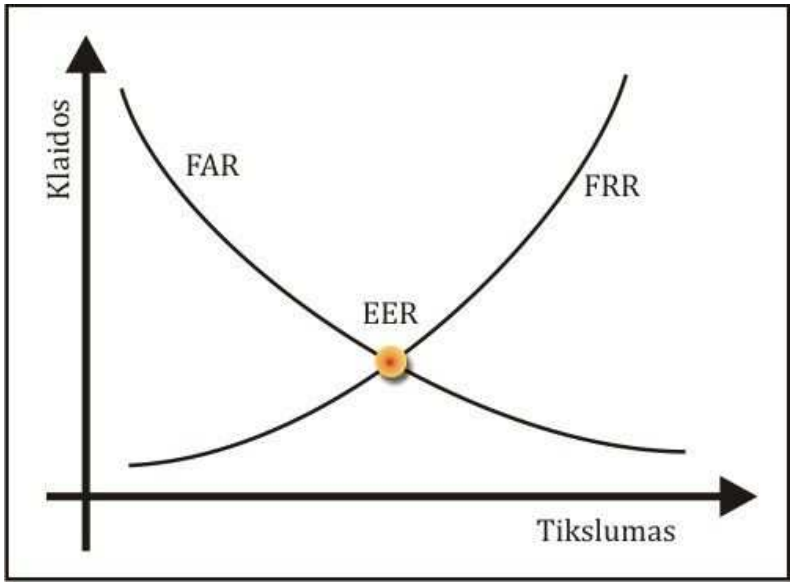
Taip pat reiktų atskirti neteisingą atmetimą nuo nesugebėjimo į sistemą įvesti duomenis. Jei dažnai maišomi ar net laikomi vienu. Nesugebėjimu įvesti duomenis laikoma, kai sistemai nepateikiama pakankamai biometrijos informacijos. Tai gali nutikti pvz. atsiradus purvui ant piršto antspaudų skaitytuvo, nepakankamo apšvietimo esant veido atpažinimui, ar neaiškiai kalbant į balso atpažinimo sistemą. Visais atvejais vartotojas, o ne sistema, yra kalta dėl neteisingo veikimo. Tai gali būti daroma specialiai arba netyčia.

1.3.3.2 Neteisingo priėmimo galimybė (*FAR*)

Taip pat išreiškiama procentais, nurodant kaip dažnai sistema neteisingai autentifikuoja neįvestą vartotoją. Suprantama, į šią galimybę labiausiai yra atsižvelgiama renkantis biometrinę autentifikacijos sistemą.

1.3.3.3 Bendra klaidos galimybė (*EER*)

Ši galimybė yra prieš tai buvusių galimybių susikirtimo taškas, kai jų reikšmės sutampa. Nors neteisingo atmetimo ir neteisingo priėmimo galimybės yra nepriklausomos, jos viena kitą veikia. Daugumą biometrinių sistemų galima koreguoti, nurodant kuris rodiklis yra svarbesnis. Tačiau mažinant vienos klaidos tikimybę, didėja kitos. [38]



3 pav. Klaidos galimybės priklausomybė nuo tikslumo[38]

1.3.3.4 Greitis ir pralaidumas

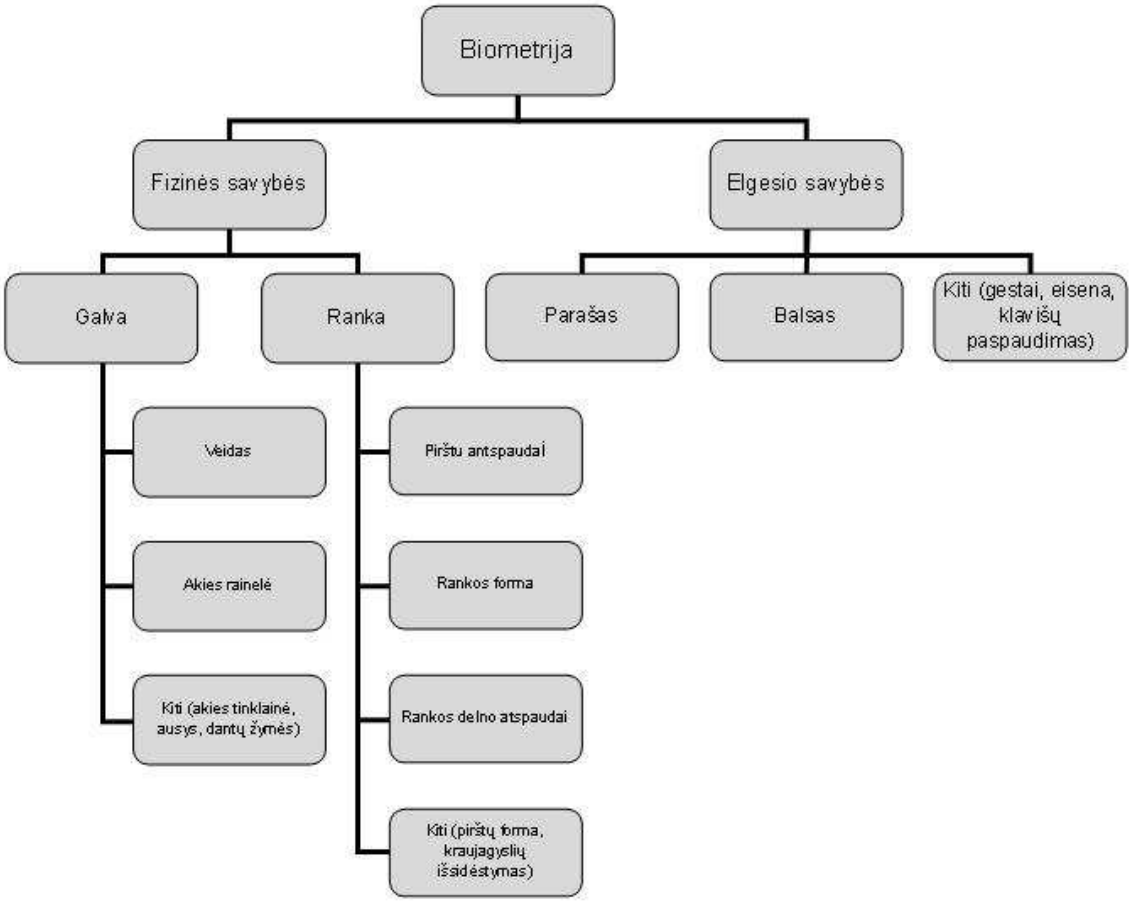
Paskutinis, bet ne mažiau svarbus yra ir biometrinės sistemos greitis bei pralaidumas. Jis nurodo ne tik apskaičiavimo laiką, lyginant nuskaitytus biometrinius duomenis su jau užfiksuotu šablonu. Skaičiuojamas visas sistemos veikimo laikas, nuo duomenų įvedimo pradžios iki sistemos teigiamo ar neigiamo autentifikacijos atsako. [9]

1.3.4 Biometrinių sistemų veikimo principas

Biometrinės sistemos skirstomos į veikiančias remiantis dviem principais:

- fizinėmis savybėmis (pirštų antspaudai, pirštų kraujagyslės, rankos geometrija, pėdos geometrija [12] ir spaudimo pasiskirstymo kitimas [13], akies tinklainė, rainelė [11], veidas);
- elgesio savybėmis (balsas, parašas, eisena ir t.t.).

Yra ir rečiau naudojamų metodu, tokių kaip klavišų paspaudimų analizė [14], rankos mostai su akselerometru [15, 16], rankos krumpliai [17], delnų linijos [18], liežuvio formos, ausies formos, lūpų formos, asmens kūno formos, kvapo, širdies plakimo, DNR [21].



4 pav. Biometrijos rūšys pagal duomenų pasiskirstymą

Pirštų atspaudai – labiausiai paplitęs metodas, naudojamas jau nuo senų laikų. Šis metodas remiasi piršto epidermio struktūra, kuri nesikeičia per visą gyvenimą.

Pirštų kraujagyslės – apšviečiant artima infraraudoniems spinduliams šviesa užfiksuojamas kraujagyslių išsidėstymas.

Rankos geometrija – asmens atpažinimui naudojamas delnas. Kreipiamas dėmesys į daugybę bruožų: pirštų storis, ilgis, atstumai tarp sąnarių, bendra kaulų struktūra [5].

Tinklainė – matuojamas unikalus akies dugne esančių kraujagyslių išsidėstymas.

Rainelė – rainelė nesikeičia per visą gyvenimą ir šis metodas laikomas itin tiksliu, nes tikimybė, kad du asmenys turėtų tokią pat rainelę yra 1 iš 10^{78}, kai šiuo metu žmonių populiacija neviršija 10^{10} [4, 5].

Veidas – laikomas greičiausiai ir aiškiausiai nurodomu biometriniu duomenų tipu, jei tik laikomas reikiamoj pozicijoj ir užtikrinamas geras apšvietimas.

Parašas – matuojamas rašiklio spaudimo lygis, greitis, taškai kuriuose atkeliama nuo pagrindo, taip pat atliekama ir paties parašo analizė.

Balsas – nors naudojamas sakomo teksto atpažinimui, pagrindinis dėmesys kreipiamas į balso analizę, kuris priklauso nuo fizinių charakteristikų: balso trakto, burnos, nosies ertmės ir lupų.

Lentelė nr.2. Populiariausių biometrinių metodų palyginimas

Charakteristikos	**Naudojimo lengvumas**	**Klaidų priežastys**	**Tikslumas**	**Kaina**	**Vartotojų pripažinimas**	**Užtikrinamas saugumo lygis**	**Ilgalaikis stabilumas**
Pirštų antspaudai	Aukštas	Sausumas, purvas, amžius	Aukštas	*	Vidutinis	Aukštas	Aukštas
Pirštų kraujagyslės	Aukštas	-	L. aukštas	*	Vidutinis	Aukštas	Aukštas
Rankos geometrija	Aukštas	Rankų pažeidimai, amžius	Aukštas	*	Vidutinis	Vidutinis	Vidutinis
Tinklainė	Žemas	Akiniai	L. aukštas	*	Vidutinis	Aukštas	Aukštas
Rainelė	Vidutinis	Prastas apšvietimas	L. aukštas	*	Vidutinis	L. aukštas	Aukštas
Veidas	Vidutinis	Apšvietimas, amžius, akiniai, plaukai	Aukštas	*	Vidutinis	Vidutinis	Vidutinis

Parašas	Aukštas	Parašo keitimasis	Aukštas	*	Labai aukštas	Vidutinis	Vidutinis
Balsas	Aukštas	Triukšmas, peršalimas.	Aukštas	*	Aukštas	Vidutinis	Vidutinis

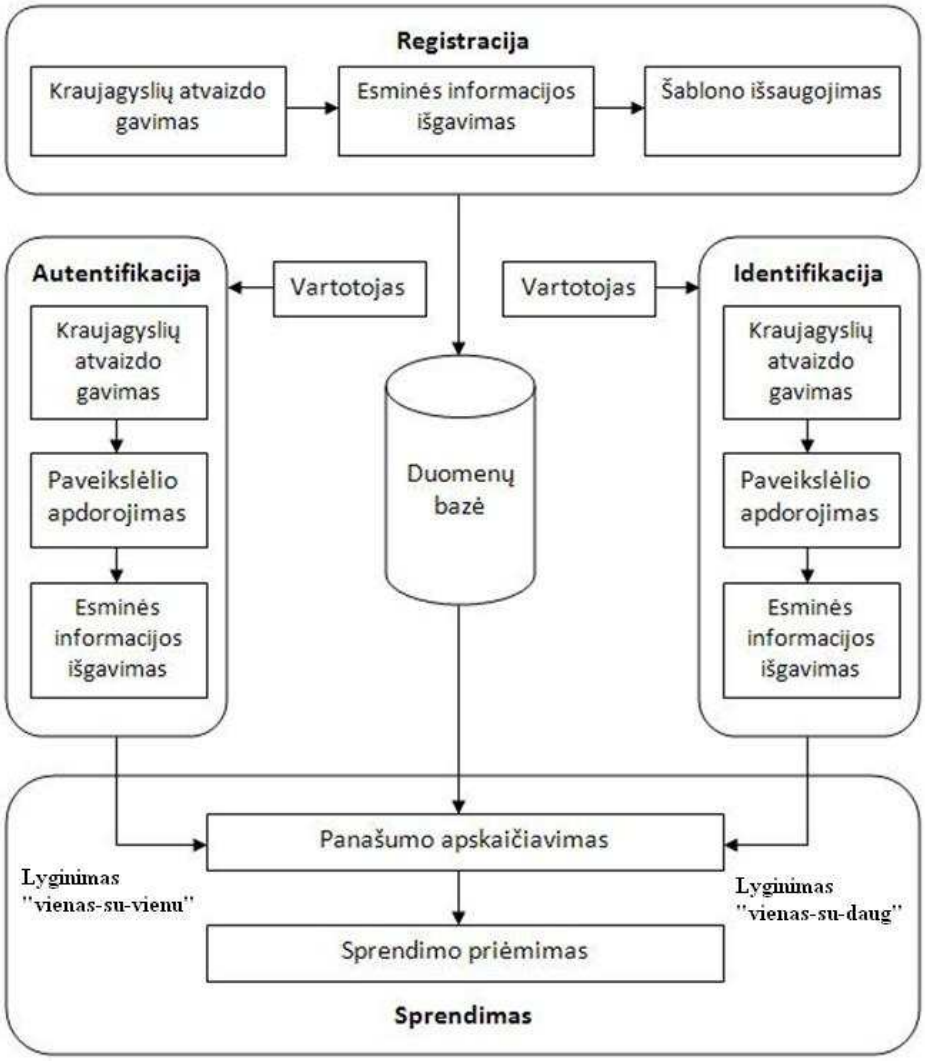
*- Didelis svarstomų faktorių skaičius daro paprastą palyginimą nepraktišku

Kad kiekvienai situacijai būtų rastas tinkamas metodas, reikalinga analizė, atlikta kreipiant didelį dėmesį ne tik į dabartinį patogumą, tačiau ir į ateityje numatomą plėtrą bei technologijų standartus.

Mūsų atveju piršto kraujagyslių skanavimas turi daugiau privalumų lyginant su kitais plačiau naudojamais metodais kaip piršto antspaudai, rainelė, veidas ir t.t.:

- Gyvo kūno identifikavimas: kraujagyslėse esančio hemoglobino dėka jos matomos tamsiau ir tai galima pamatyti tik esant gyvam kūnui.
- Vidiniai požymiai: kadangi remiamasi duomenimis, gautais iš kūno vidaus, nėra tikslumo sumažėjimo tikimybės dėl pvz. purvino, išsausėjusio ar sudrėkusio, pažeisto rankų paviršiaus.
- Bekontaktis skanavimas: įmanomas skanavimas tiesiogiai neliečiant skanerio, todėl tai yra higieniška.
- Didelis saugumo lygis: kadangi sistema remiasi trim ypatybėmis, kaip gyvas kūnas, vidiniai požymiai bei bekontaktis skanavimas, neįmanoma to sufalsifikuoti, šią technologiją galima naudoti, kur reikalingas didelis saugumo užtikrinimas. [8]

Pavyzdžiui, piršto antspaudai gali būti ne tik nesunkiai pasisavinti, tačiau yra problemų ir su registracija, kai antspaudai būna pažeisti, ar bandomas skanuoti drėgnas pirštas. Rainelės atpažinimas žinomas, kaip užtikrinantis mažą klaidų dažnį, bet kai kuriems asmenims yra nepriimtinas ir nemalonus akies apšvietimas ryškia šviesa. Taip pat būtina užtikrinti ir precizišką veido padėtį skanavimo metu.



5 pav. Apibendrinta piršto kraujagyslių atpažinimo sistemos struktūra [21]

Taigi piršto kraujagyslių skanavimas tai aukšto patikimumo autentifikacijos metodas, kuris tuo pat metu labai sunkiai suklastojamas, neinvazinis ir lengvas naudoti, siūlantis privalumų balansą. Tai daro jį nepralenkiama biometrinės autentifikacijos forma [9].

Hitachi sukūrė daug skirtingų skanerių, kiekvienas jų – skirtingai sričiai:

Įėjimo kontrolė

Vairo kraujagyslių skaitytuvas

Bankomatų sistemos

Skanerio, sumontuoto rankenoje sistema

PK autentifikavimo sistema

PK autentifikavimo sistema

6 pav. Įvairiose srityse naudojamos autentifikavimo sistemos, paremtos kraujagyslių atvaizdu [41]

1.3.5 Situacijos Lietuvoje įvertinimas

Biometrijos technologijų naudojimas Lietuvoje vystomas labai lėtai. Oficialių statistinių duomenų apie biometrijos naudojimą nėra, arba jie neprieinami. Yra keletas firmų, kurios užsiima biometrija, kuria specializuotus produktus, tačiau rinka yra dar labai jauna.

Lietuvoje galima sutikti ir įsigyti biometrinius durų užraktus ir seifus. Jie galimai naudojami „protinguose“ namuose, tačiau tokių namų Lietuvoje galima rasti vos keletą.

1.4 Išvados

Automobilių apsauga visada buvo, yra ir bus aktuali. Esamos apsaugos priemonės nesunkiai apeinamos ir nesudaro didelių kliūčių, norint transporto priemonę pasisavinti. Todėl reikalinga naujoviška vairuotojo autentifikavimo sistema, galinti sumažinti šią, pasisavinimo tikimybę.

Kažkas, kuo esi – biometrinis bruožas yra pats saugiausias, nes jo negalima pamesti, paskolinti, pavogti ar užmiršti.

Biometriniai metodai turi bendrą teorinį veiklos modelį:

- informacijos surinkimas ir įtraukimas į sąrašą,
- šablono saugojimas,
- informacijos lyginimas.

Biometrinių autentifikavimo sistemų našumas priklauso nuo: teisingo priėmimo, neteisingo priėmimo, neteisingo atmetimo, greičio ir pralaidumo

Mūsų atveju piršto kraujagyslių skanavimas turi daugiau privalumų lyginant su kitais plačiau naudojamais metodais kaip piršto antspaudai, rainelė, veidas ir t.t. Piršto kraujagyslių skanavimas tai aukšto patikimumo autentifikacijos metodas, kuris tuo pat metu labai sunkiai suklastojamas, neinvazinis ir lengvas naudoti, siūlantis privalumų balansą. Tai daro jį nepralenkiama biometrinės autentifikacijos forma, ją ir naudosime savo darbe.

2. BIOMETRINĖS AUTOMOBILIŲ APSAUGOS SISTEMOS MODELIS

2.1 Darbo tikslas

Tikslas – sukurti ir ištirti biometrinės autentifikacijos automobiliams modelį.

Uždaviniai:

- Išanalizuoti automobilių saugos priemones, taikomus metodus,
- Apžvelgti ir ištirti autentifikacijos metodus, geriausiai tinkančius šiai sistemai,
- Pasirinkti metodus ir išanalizuoti skirtingus algoritmus, siekiant pasirinkti geriausiai tenkinančius užduotus kriterijus,
- Suprojektuoti įterptinę sistema, atitinkančią nustatytus reikalavimus,
- Atlikti eksperimentą bei paaiškinti gautus rezultatus.

2.2 Reikalavimų specifikavimas

2.2.1 Funkciniai reikalavimai

2.2.1.1 Bendri reikalavimai

- Sistema turi leisti registracijos metu įvesti kelis vartotojus, jiems priskiriant skirtingus identifikacinius numerius (*ID*);
- Sistema turi leisti vieną vartotoją paskirti administratoriumi;
- Sistema turi leisti tinkamai autentifikavusis redaguoti vartotojų sąrašą bei saugomus šablonus;
- Sistema turi įvedus piršto kraujagyslių pavyzdį, palyginti su *DB* esančiais šablonais, o jiems atitinkant – autorizuoti vartotoją;
- Sistema turi užsiblokuoti, neleidžiant ja naudotis 10 minučių laikotarpiu, tris kartus nesėkmingai autentifikavusis;
- Sistema turi kaupti statistinę informaciją apie kiekvieno vartotojo nuvažiuotus atstumus, laiką;
- Sistema turi išvesti statistinę informaciją apie pasirinktą vartotoją.

2.2.1.2 Autentifikavimasis kraujagyslių atvaizdu

- Sistema turi registracijos metu nuskaityti po kelis piršto kraujagyslių šablonus kiekvienam pirštui;
- Sistema turi atsitiktine tvarka parinkti pirštą ir pareikalauti nuskaityti būtent jį.

2.2.2 Nefunkciniai reikalavimai

- Sistema turi būti paprasta naudoti;
- Programinė įranga turi užtikrinti, kad duomenys sistemoje būtų saugūs ir neprieinami pašaliniams naudotojams;
- Neturi būti galimybės apeiti sistemą, neteisingai autentifikavusis arba to visai nepadarius.

2.2.3 Reikalavimai aparatūrai

- Ekranas turi būti jautrus lietimui;
- Procesorius turi būti pakankamai spartus, kad greitai apdorotų gautus duomenis bei palygintų su esančiais duomenų bazėje;
- Kraujagyslių skaneris turi būti pakankamai spartus;
- Sistema turi būti pritaikyta integravimui su automobilio kompiuteriu;
- Reikalavimą kurį pirštą pateikti nuskaitymui autentifikacijos metu sistema turi parodyti skirtingų *LED* diodų pagalba ant durų.

2.2.4 Reikalavimai vartotojo sąsajai

- Vartotojo sąsaja turi būti paprasta, lengvai suprantama, neperkrauta, lengvai valdoma;
- Tekstas turi būti aiškiai išdėstytas, lengvai matomas tiek šviesioje, tiek tamsioje aplinkoje.

2.3 Sistemos architektūra

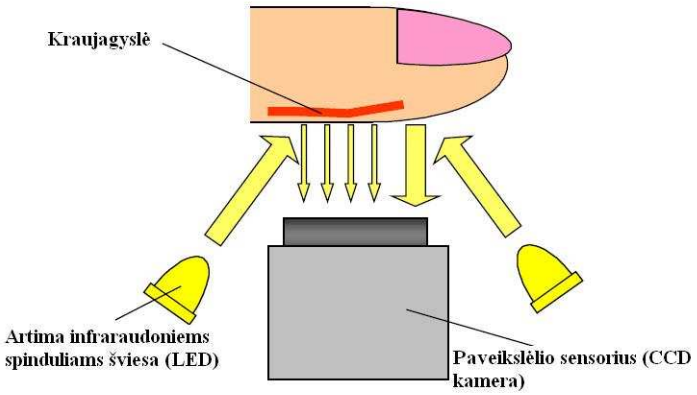
2.3.1 Kraujagyslių skanavimas

Kraujagyslės yra po oda, jos yra nematomos apšviečiant natūralia šviesa. Tačiau jos puikiai matomos apšvietus artima infraraudoniems spinduliams šviesa (bangos ilgis tarp

700 ir 1000 nanometrų), kadangi ši šviesa lengvai sklinda per žmogaus kūno audinius, bet yra blokuojama tokių pigmentų, kaip hemoglobinas ar melaninas. Kadangi hemoglobino didelė koncentracija yra tik kraujagyslėse, apšvietus artima infraraudonosioms bangos šviesa, šios atrodo kaip tamsios linijos.

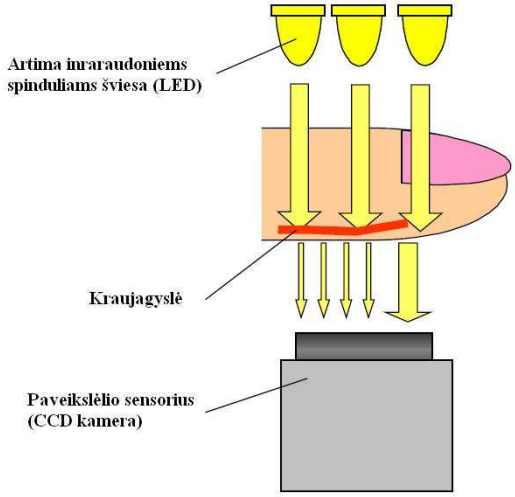
Yra du kraujagyslių skanavimo metodai:

- Fiksuojant atsispindėjusią šviesą
- Fiksuojant praėjusią šviesą



7 pav. Atsispindėjusios šviesos principinė veikimo schema [9]

Šviesos šaltinis bei sensorius sumontuojami toje pačioje plokštumoje, sensorius fiksuoja atsispindėjusią nuo piršto šviesą. Šis metodas reikalauja didesnių apdorojimo pajėgumų, nes dėl atspindžių nuo odos, kontrastas tarp kraujagyslių ir kitų vietų yra minimalus. Be to odos pažeidimai bei raukšlės neigiamai įtakoja kraujagyslių atpažinimą.

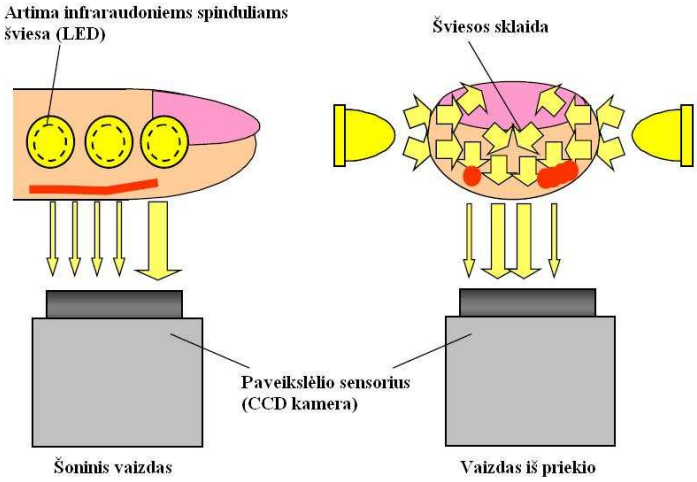


8 pav. Praėjusios šviesos principinė veikimo schema [9]

Pirštas patalpinamas tarp šviesos šaltinio bei sensoriaus, fiksuojamos per pirštą praėjusios šviesos bangos.

Fiksuojant praėjusią šviesą, gauname kontrastingesnį vaizdą, kadangi nėra šviesos atspindžių. Tačiau atspindžio metodu veikianti aparatūrinė įrangą užima mažiau vietos, nes montuojama vienoje plokštumoje, kai praėjusios šviesos įranga būna didesnė.

Taip pat kartais naudojamas ir kombinuotas – šoninis apšvietimas.

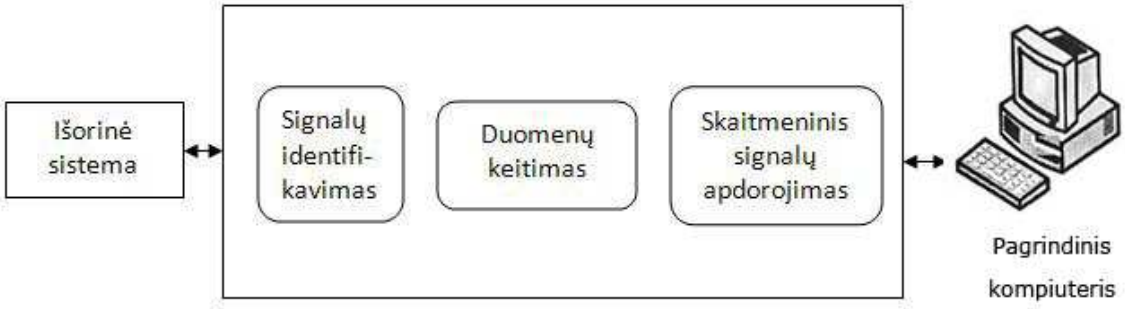


9 pav. Šoninio apšvietimo principinė veikimo schema [9]

Taigi šviesos šaltinis ir sensorius yra esminiai įrenginiai, nuo kurių priklauso tikslumas. Kraujagyslių vaizdai yra palyginti stambūs, todėl kitaip nei akies, ar piršto antspaudų atveju, užtenka ir *QVGA* (320x240 taškų) raiškos. Tačiau sensorius turi būti labai jautrus vaizdui ir nejautrus triukšmui. Be to, dėl skirtingo piršto dydžio, šviesos šaltinis bei sensorius turi atitinkamai prisitaikyti, kad išgauti maksimaliai tikslų atvaizdą.

2.3.2 Bendros žinios apie *SAS* architektūras

Realaus pasaulio signalų apdorojimo įrangos apibendrinta struktūra pateikta 10 paveiksle.



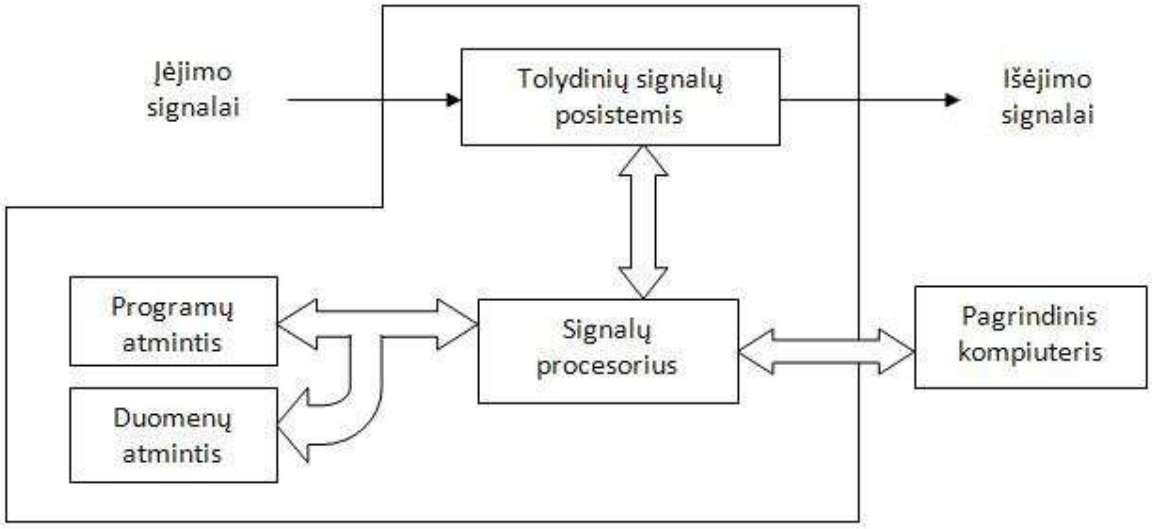
10 pav. Signalų apdorojimo kompiuterinė sistema

Skaitmeninių signalų apdorojimo realiu laiku sistema – *SAS*, atliekanti tris pagrindines funkcijas: signalų identifikavimą, keitimą ir skaitmeninį jų apdorojimą.

Skaitmeninį signalų apdorojimą sistemoje atlieka diskretinių signalų procesorius (*DSP*), kurio architektūra apima:

- į signalų įvedimą ir išvedimą orientuotą įranga. Greitoms įvedimo ir išvedimo operacijoms atlikti naudojamas tiesioginis mainų kanalas tarp signalų įvedimo ir išvedimo posistemio ir *DSP* duomenų atminties;
- specializuota komandų sistema, kurios dėka laikui imlios operacijos ar skaičiavimai atliekami aparatiniu būdu (pavyzdžiui, daugyba, Furjė bei kitos transformacijos ir kt.);
- mažo latentiškumo (greito reagavimo) pertraukimų sistema;
- *DSP* išorinę magistralė, skirtą analoginių – skaitmeninių ir skaitmeninių – analoginių keitiklių, duomenų ir programinės atminties prijungimui;

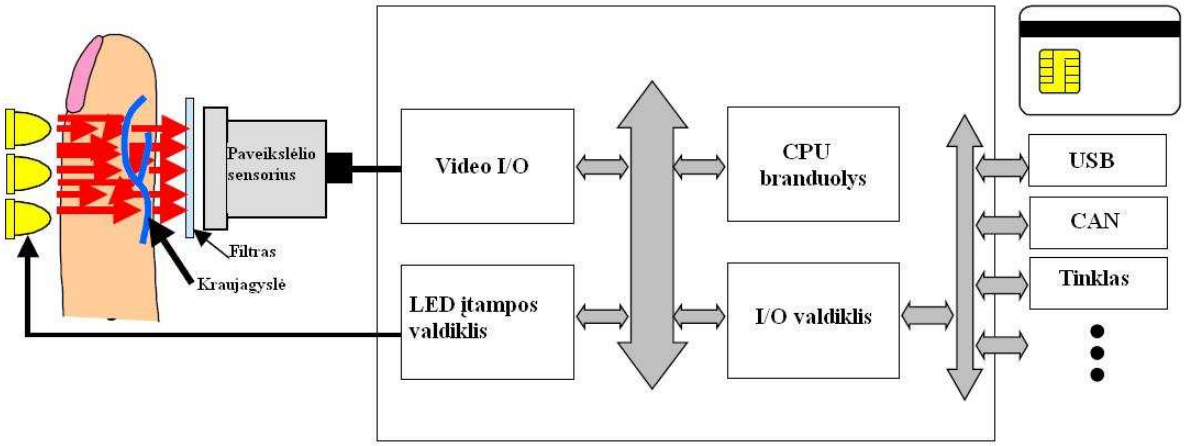
- komunikavimo įranga ryšiui palaikyti su pagrindiniu kompiuteriu arba kitomis *SAS*;
- priemones laiko atskaitoms formuoti – specialios paskirties laikmačius, kurie naudojami signalų diskretizavimui, formavimui ir procesų sinchronizavimui;
- signalų apdorojimo sistemoje, be *DSP*, programų ir duomenų atmintį, analoginių signalų įvedimo ir išvedimo sistemą, atliekančia signalų identifikavimo ir analoginių signalų keitimo į skaitmeninius funkcijas (10 pav.) ;
- blokinė signalų apdorojimo sistemos (*SAS*) struktūra (11 pav.).



11 pav. Blokinė SAS schema

Informacijos apdorojimo sistema – visuma, apimanti *SAS*, diskretinių signalų duomenų komponentus ir jų apdorojimo programas. [37]

2.3.3 Sistemos architektūra

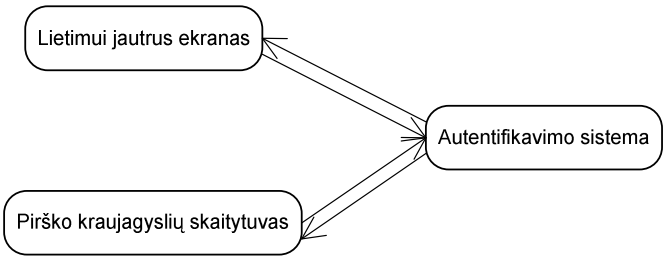


12 pav. Blokinė kraujagyslių autentifikavimo sistemos diagrama [9]

Sistemą sudaro autentifikavimo blokas bei kiti susiję įrenginiai kartu su šviesos šaltiniu ir sensoriumi. Blokas susideda iš procesoriaus signalų apdorojimui, vaizdo įvedimo/išvedimo įrenginio paveikslėlio iš sensoriaus priėmimui, *LED* įtampos kontrolerio ir duomenų įvedimo/išvedimo kontrolerio.

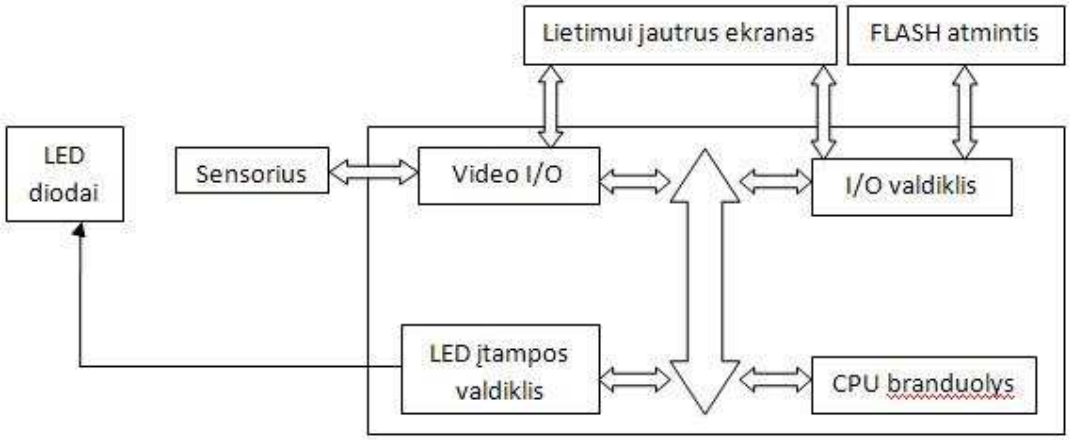
2.3.4 Siūlomas modelis

Piršto kraujagyslių skanavimo sistema paprašytų nuskaityti kaskart vis kitą pirštą. Šablonams naudojami į sistemą įvedami pavyzdiniai duomenys būtų skaitomi po kelis kartus. Tai sukels nepatogumų pirmą kartą registruojantis sistemoje, nes užtruks šiek tiek laiko, tačiau padidins jos patikimumą. Sistemos konfigūravimą galėtų atlikti pats pirmasis įvestas vartotojas, jam registracijos metu suteikiant *super* vartotojo statusą.



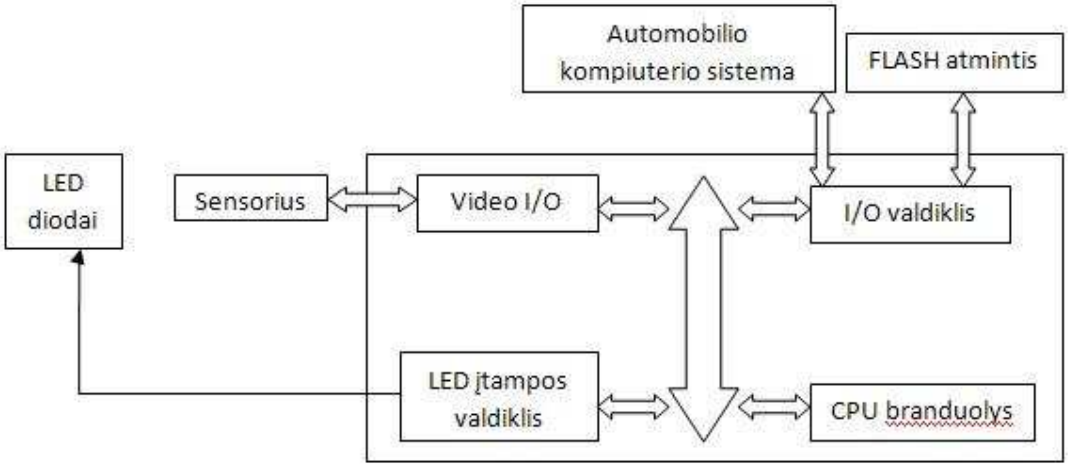
13 pav. Apibendrinta aparatūrinės įrangos diagrama

Esant automobilinei kompiuterio sistemai su ekranu bei valdymu, šios sistemos galėtų būti jungiamos kartu. Neesant – prie autentifikavimo sistemos galėtų būti jungiamas atskiras lietimui jautrus ekranas, taip suteikiant sistemos valdymo bei rezultatų gavimo galimybes. Kadangi orientuojamės į kelių vartotojų, o ne pramoninę sistemą, *super* vartotojo statuso dalijimosi/perdavimas nebus nagrinėjamas. Taip pat nebus detaliai nagrinėjamos ir fizinės visos sistemos ir jos komponentų instaliavimo ypatybės. Vartotojų administravimas galėtų būti atliekamas įgaliotame gamintojo servise.



14 pav. Aparatūrinės įrangos diagrama, sistemą jungiant prie jai skirto ekrano

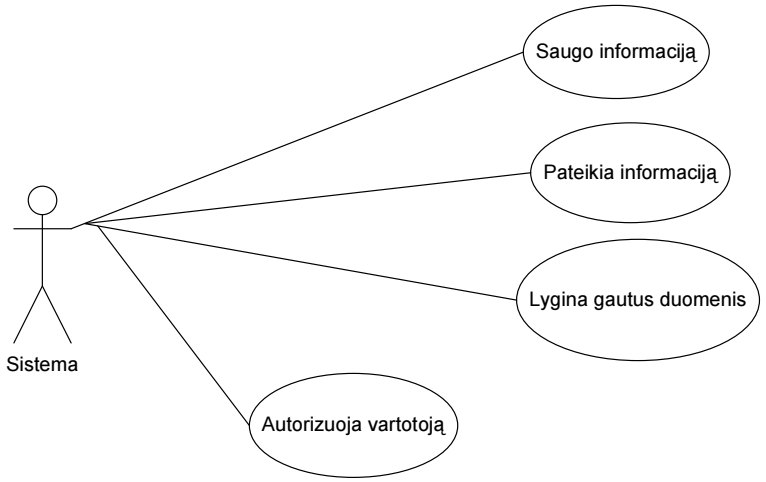
Skaičiavimams atlikti galėtų būti naudojamas signalinis procesorius – procesorius, specialiai optimizuotas skaitmeninių signalų apdorojimui. Jiems nereikalingas specializuotas aušinimas ar didelis energijos kiekis, tačiau naudodami specializuotus instrukcijų rinkinius, veiksmus atlieka greičiau ir su mažesniu užlaikymu.



15 pav. Aparatūrinės įrangos diagrama, sistemą integruojant su jau automobilyje esančia kompiuterine sistema

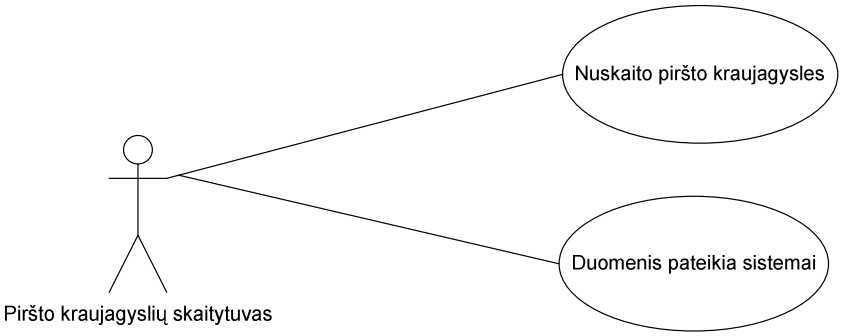
2.3.5 Panaudojimo atvejų diagramos

Sistemos funkcionavimo algoritmai, panaudojimo atvejų algoritmai



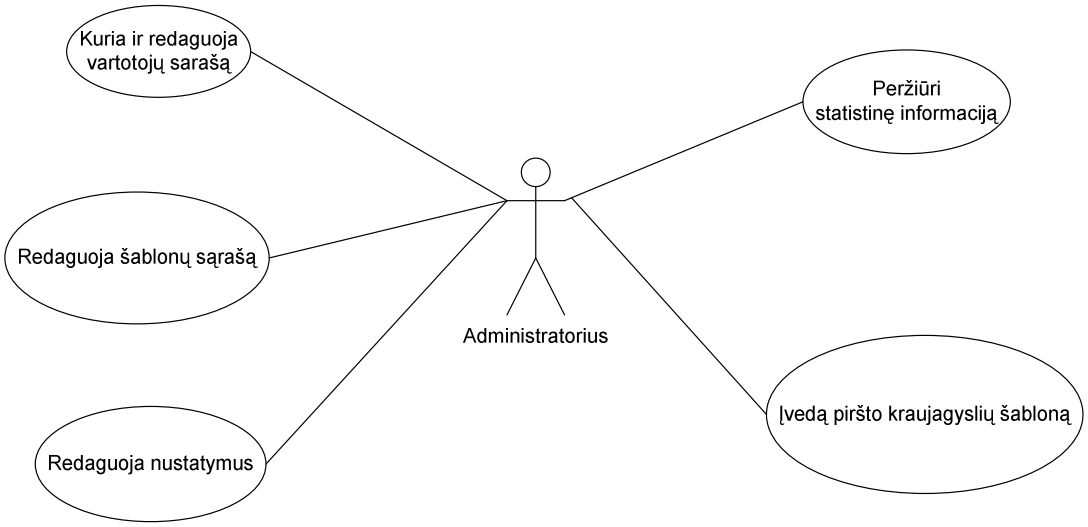
16 pav. Sistemos panaudos atvejų diagrama

Sistema saugo, pateikia informaciją, lygina gautus duomenis su esančiais duomenų bazėje, bei autorizuoja vartotoją arba jo neautorizuoja.



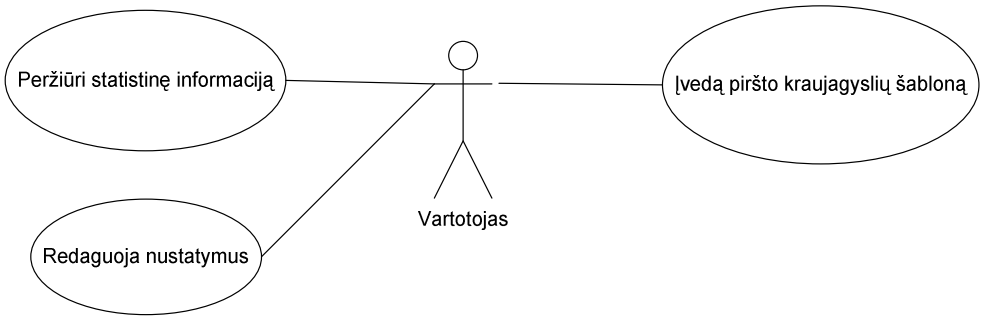
17 pav. Skaitytuvo panaudos atvejų diagrama

Piršto kraujagyslių skaitytuvas nuskaito piršto kraujagysles ir skaitmenine forma duomenis pateikia sistemai.



18 pav. Administratoriaus panaudos atvejų diagrama

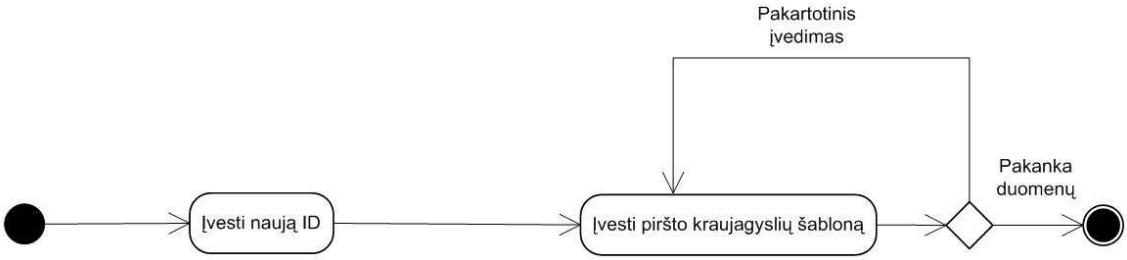
Administratorius gali kurti ir redaguoti vartotojų sąrašą, įvesti kraujagyslių šabloną ir redaguoti jų sąrašą, redaguoti bendrus nustatymus ir peržiūrėti statistinę informaciją.



19 pav. Vartotojo panaudos atvejų diagrama

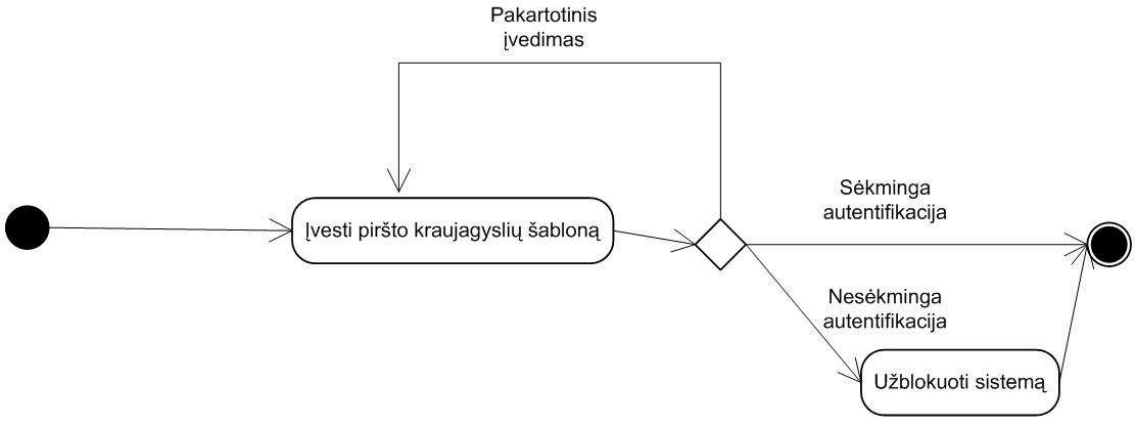
Vartotojas gali įvesti piršto kraujagyslių šabloną, peržiūrėti statistinę informaciją ir redaguoti nustatymus.

2.3.6 Sekų diagramos



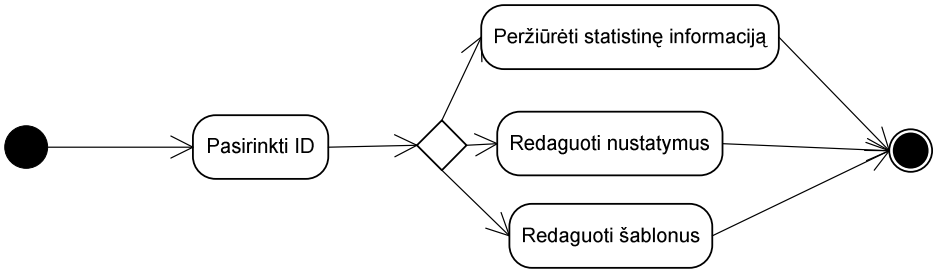
20 pav. Vartotojo registracijos sekų diagrama

Įvedus naują vartotojo *ID*, skaitomi kraujagyslių atvaizdai, o kuomet jų pakanka, įvedimo sistema baigia darbą.



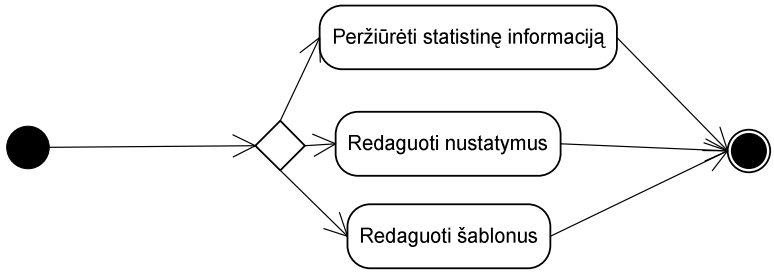
21 pav. Autentifikacijos sekų diagrama

Nuskaičius šabloną, jis tikrinamas su esančiu duomenų bazėje, esant sėkmingai autentifikacijai, sistema baigia darbą. Tris kartus šablonams nesutapus, sistema blokuojama ir baigia darbą.



22 pav. Sėkmingai autentifikuoto administratoriaus veiksmų sekų diagrama

Administratorius pasirinkęs vartotojo *ID* gali: peržiūrėti statistinę informaciją, redaguoti nustatymus, redaguoti šablonus.



23 pav. Sėkmingai autentifikuoto vartotojo veiksmų sekų diagrama

Vartotojas gali: peržiūrėti statistinę informaciją, redaguoti nustatymus, redaguoti šablonus.

2.4 Atliekami veiksmai

Sistema atlieka šias užduotis:

2.4.1 Piršto kraujagyslių vaizdo užfiksavimas

Sistema sensoriaus pagalba fiksuoja paveiksliuką ir perduoda informaciją procesoriui. Šis per *LED* įtampos kontrolerį kontroliuoja optimalų šviesos šaltinio galingumą.

2.4.2 Paveikslėlio normalizacija

Paveikslėlis normalizuojamas, kad ištaisyti piršto pasukimo ar pozicionavimo klaidas.

a. Triukšmo šalinimas

Tam gali būti naudojamas Gauso metodas.

$$G(u,v) = \frac{1}{2\pi\sigma^2} e^{-(u^2+v^2)/(2\sigma^2)}$$

, kur r - susiliejimo spindulys ($r^2=u^2+v^2$), δ – standartinis Gauso pasiskirstymo nuokrypis. Iš šių reikšmių apskaičiuojama konvoliucijos matrica bei pritaikoma originaliam paveikslėliui.

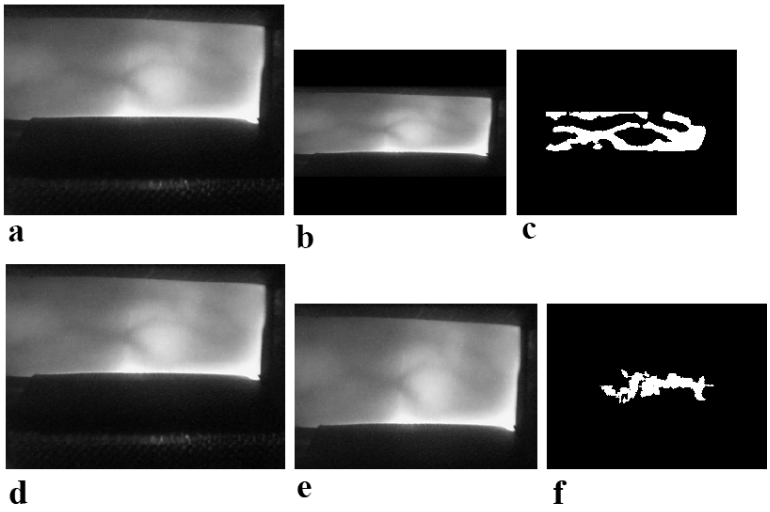
b. Apšvietimo lyginimas

Dėl nevienodo pirštо storio, skiriasi ir kraujagyslių apšvietimo intensyvumas. Tai sukelia sunkumų lyginant su užfiksuotu šablonu, todėl paveikslėlis turi būti normalizuotas. Naudojamas pustonių normalizavimas:

G=((g-min g) x 255) / (max g – min g), kur g – originalaus paveikslėlio pustonių reikšmė, G – pustonių reikšmė po pakeitimo, min g – minimali, o max g – maksimali originalaus paveikslėlio pustonių reikšmė.

c. Normalizacija

Šioje fazėje mes stengiamės rasti mus dominančią paveikslėlio vietą. Kad paspartinti procesą vėlesniems veiksmams, paveikslėlis sumažinamas iki 240 x 180 taškų, o mus dominanti vieta patalpinama paveikslėlio centre.



24 pav. (a),(d) – originalus 320 x 240 taškų paveikslėlis, (b) – normalizuotas iki 240 x 180, (c) – kraujagyslės, gautos iš (b), (e) – normalizuotas iki 320 x 175, (f) – kraujagyslės, gautos iš (e) [22]

2.4.3 Šablono išskyrimas

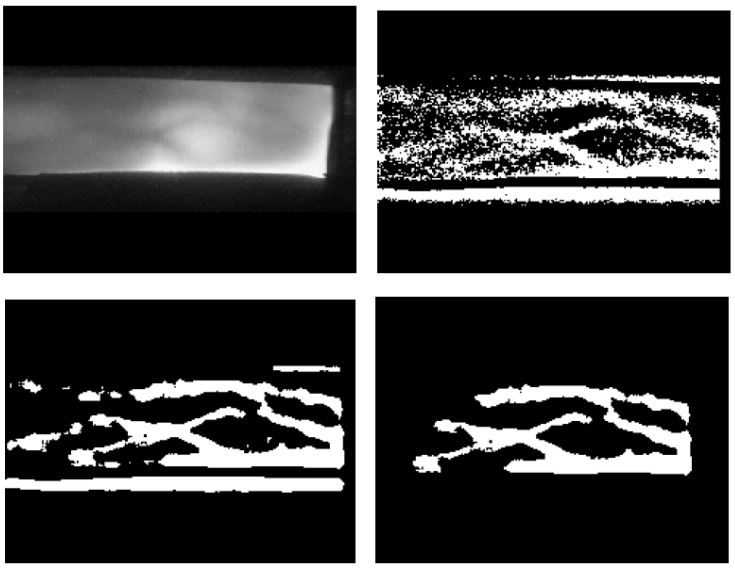
Išskiriamas savitas šablonas. Šis veiksmas yra esminis, norint užtikrinti patikimą autentifikacija. Tam turi būti atlikti keli paveikslėlio apdorojimo žingsniai, naudojant skirtingus metodus.

Populiariausi metodai yra:

- Tinkamo filtro [25,31],
- Matematinės morfologijos [26],
- Pabrėžtų linijų kraštų sujungimo [27],
- Kraštinės linijos sekimas minutiae aptikimui pustonių pirštų antspaudų paveikslėliuose [28],
- Linijos sekimo kartojimas [24, 29],
- Maksimalaus išlinkio taškų paveikslėlio kontūre [30].

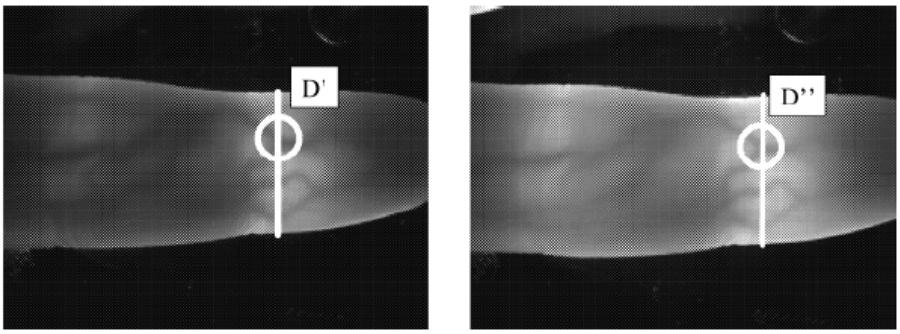
Taip pat gali būti naudojami ir šie atvaizdų atpažinimo algoritmai:

- Figūros konteksto ir orientacijos deskriptoriais pagrįsto piršto atspaudų atpažinimo [35],
- Filtrais paremto piršto atspaudų atpažinimo [36],
- Gretimos orientacijos vektoriais pagrįsto pirštų atspaudų atpažinimo [34].



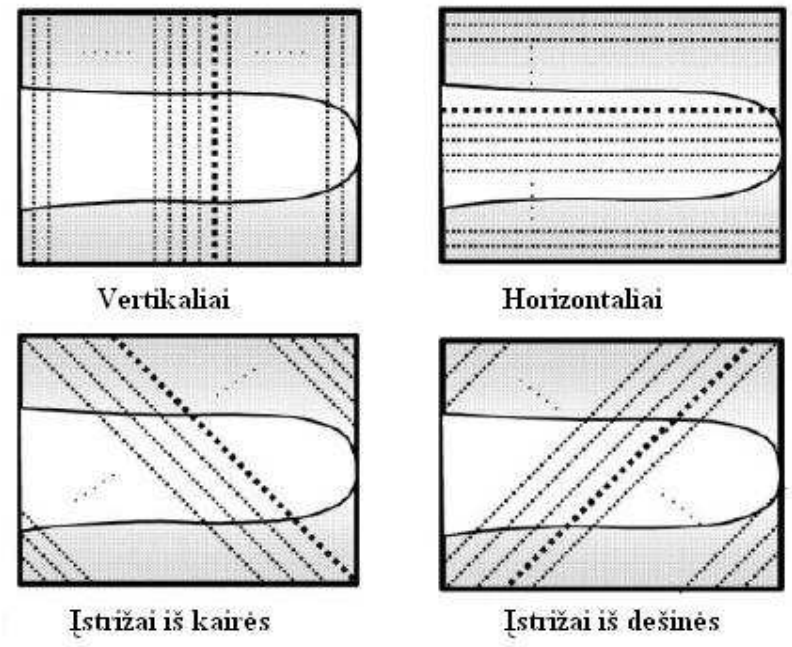
25 pav. Originalaus piršto kraujagyslių paveikslėlio apdorojimas [22]

Kraujagyslių ryškumas paveikslėlyje priklauso nuo kraujo kiekio pasikeitimų, kurį įtakoja fizinės sąlygos kaip kad temperatūros pasikeitimas.



26 pav. Kraujagyslių matomumo pasikeitimas [22]

Pirmame paveikslėlyje piršto kraujagyslių atvaizdas, kai kraujagyslėmis teka įprastas kraujo kiekis, antrame – kai mažesnis. Kad gauti identiškus rezultatus, išgaunamos centrinės linijos. Kad tai padaryti, turime jų ieškoti keturiomis kryptimis: vertikaliai, horizontaliai, įstrižai iš kairės ir įstrižai iš dešinės.



27 pav. Daugiakryptė paieška [41]

Gauname keturis paveikslėlius, kuriuos reikia sujungti į vieną. Taip išryškinamos kraujagyslės ir išvengiama triukšmų.

Algoritmą sudaro 3 žingsniai:

- Kraujagyslių centrinės linijos išskyrimas
- Kraujagyslių centrų sujungimas
- Paveikslėlio pažymėjimas

Tarkim F(x,y) yra taško (x,y) ryškumas.

a. Kraujagyslių centrinės linijos išskyrimas

Manykime, kad $P_f(z)$ yra skerspjūvio profilis, gautas iš F(x,y) vertikalia kryptimi:

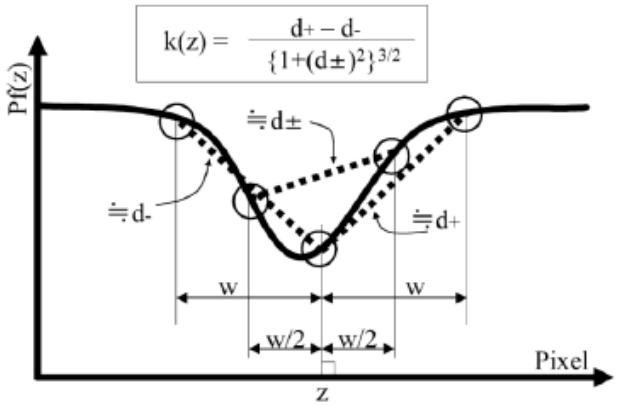
$P_f(z)=F(x,y)$, kur z yra profilio pozicija. Plano funkcija Trs nusakoma:

$F(x,y)=Trs(Pf(z))$

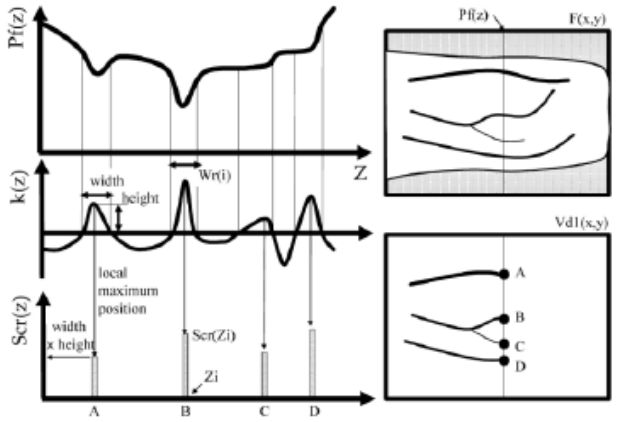
Kad apskaičiuoti išlinkį pozicijoje X, mes skaičiuojame $K_f(x)$:

$$K_f(x)=\frac{\frac{d^2f(x)}{dx^2}}{\left\{1+\left(\frac{df(x)}{dx}\right)^2\right\}^{\frac{3}{2}}}, \qquad k(z)=\frac{d_+-d_-}{\{1+d_\pm{}^2\}^{3/2}}$$

kur w naudojamas profilio vidurkio skaičiavimui. Jeigu k(z) yra teigiamas, $P_f(z)$ yra išlinkis. Dabar skaičiuojami vietiniai kiekvieno k(z) maksimumai išlinkio vietoje. Ši vieta nurodo kraujagyslių centro taškus. Jie nurodomi kaip z‘i, kur i=0,1,… N-1, o n yra vietinių maksimumo taškų skaičius.



28 pav. Profilio išlinkimo skaičiavimas [30]



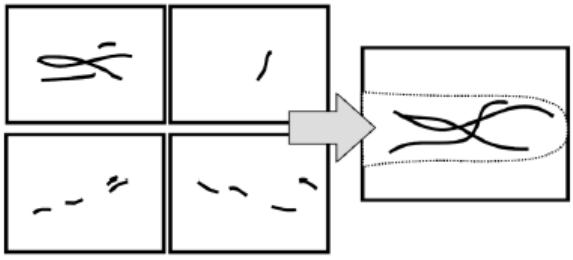
29 pav. Profilio, išlinkio ir tikimybės rezultato sąryšis [30]

Rezultatas Scr(zi‘) = k(zi‘)xWr(i), kur Wr(i) yra f regiono plotis, kai išlinkis yra teigiamas. Šis rezultatas parodo centro taškų buvimo kraujagyslėje ir tikimybę.

Rezultatai yra priskiriami plokštumai Vd1(xi‘,yi‘), kur Vd1(x,y) yra kraujagyslių ryškinimo vertikaliame paveikslėlio profilyje rezultatas:

Vd1(xi‘,yi‘)=F(xi‘,yi‘)+Scr(Zi‘), kur (xi‘,yi‘) reiškia taškus, nurodytus F(xi‘,yi‘)=Trs(zi‘).

Dabar analizuoti profiliai keturiomis kryptimis



30 pav. Kraujagyslių modelio gavimas iš keturių kryptinių paveikslėlių

b. Kraujagyslių centrų sujungimas

Pirmiausia tikrinamas Vd1 taškas (x,y) ir kaimyniniai (x-1,y) ir (x+1,y). Jei (x,y) turi mažą vertę, o jo kaimyniniai taškai didesnę – (x,y) turi būti padidintas. Jei (x,y) vertė

didesnė nei kaimyninių taškų – (x,y) turi būti sumažintas, taip išvengiama triukšmo. Tai nusakoma išraiška:

C(x,y)d1=med{Vd1(x-1,y),Vd1(x,y),Vd1(x+1,y)}, kur med{…} yra funkcija vidurkio radimui.

Kraujagyslių šablonas G gaunamas: G(x,y)=max{Cd1,Cd2,Cd3,Cd4}.

c. Paveikslėlio žymėjimas.

Kraujagyslių atvaizdas verčiamas skaitmeniniu naudojant Otsu metodą [31]:

$$\sigma^2{}_B = \omega_o(\mu_o - \mu_r)^2 + \omega_1(\mu_1 - \mu_r)^2$$

, kur

$$w_0 = \sum_{q=0}^{k-1} p_q(r_q)$$

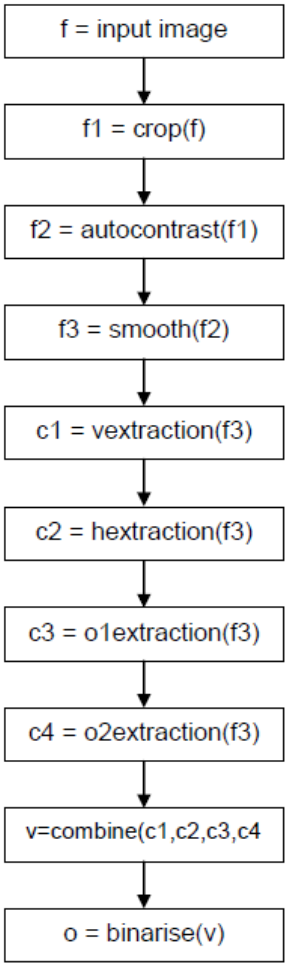
$$w_1 = \sum_{q=k}^{L-1} p_q(r_q)$$

$$\mu_0 = \sum_{q=0}^{k-1} qp_q(r_q)/\omega_0$$

$$\mu_1 = \sum_{q=k}^{L-1} qp_q(r_q)/\omega_1$$

$$\mu_T = \sum_{q=0}^{L-1} qp_q(r_q)$$

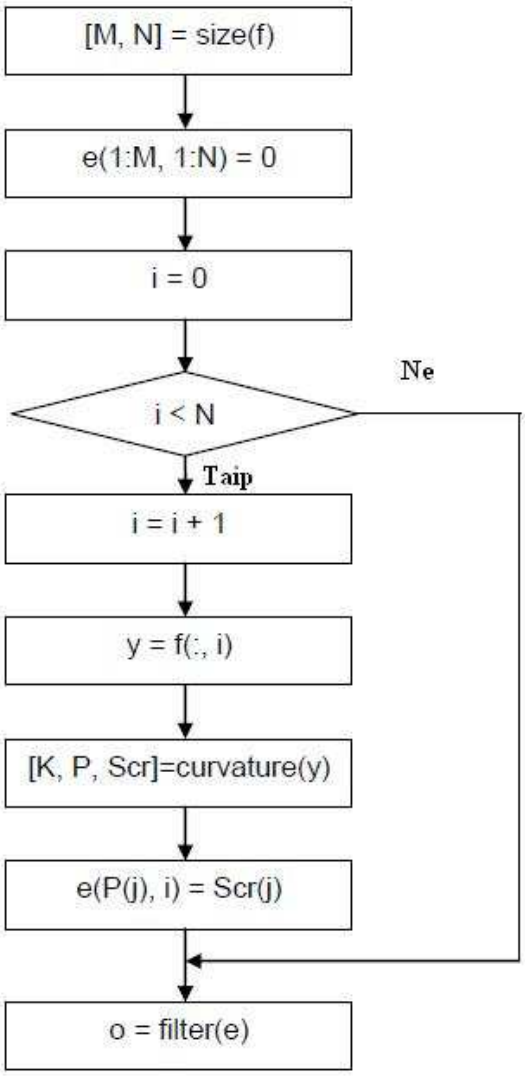
Taip pat galima naudoti *Matlab* funkciją *graythresh*, kad gauti k: T=graythresh(f), kur f yra įvesties paveikslėlis.



31 pav. Bendra kraujagyslių išgavimo struktūrinė schema

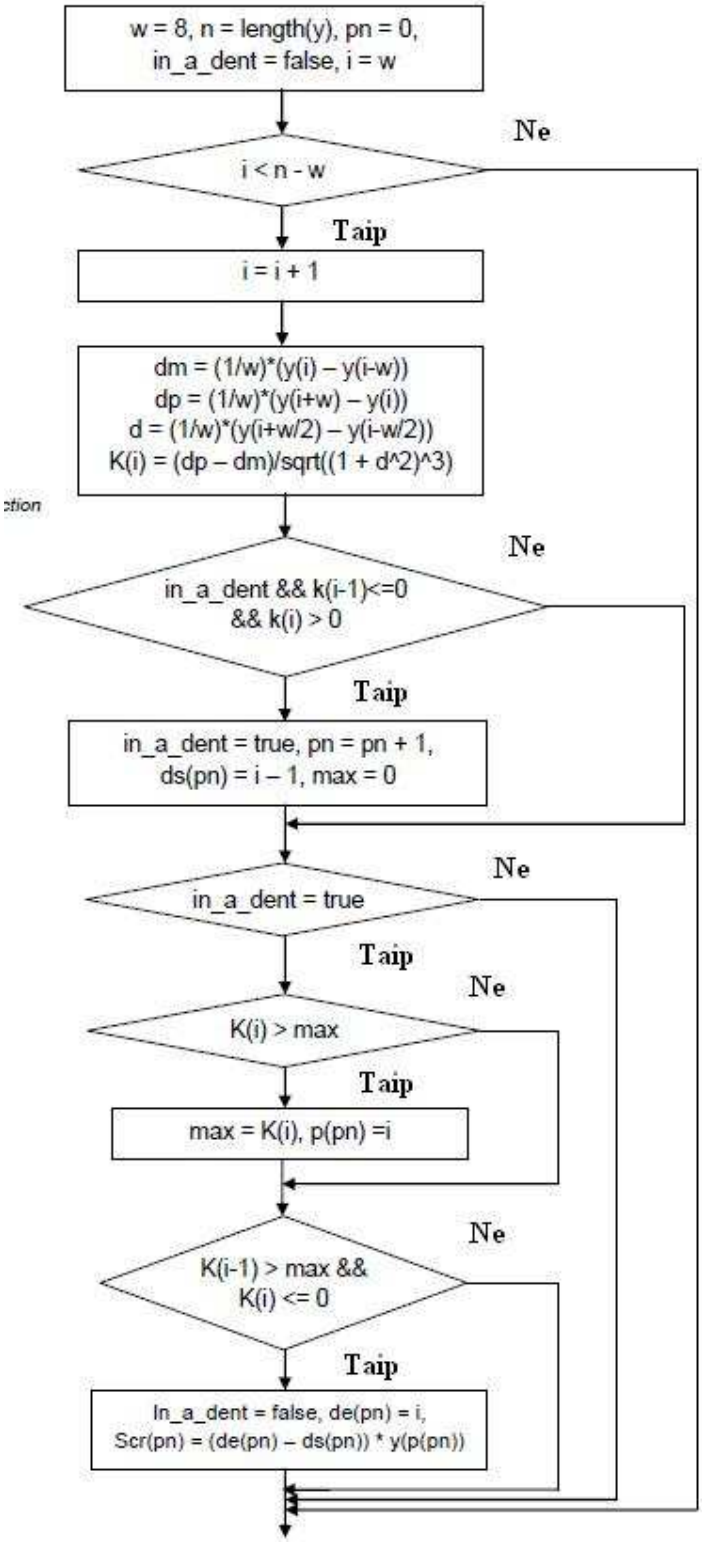
Funkcijos *autocontrast* ir *smooth* aprašytos aukščiau. *Vextraction, hextraction, o1extraction, o2extraction* reiškia vertikalų, horizontalų, ištrižai iš kairės ir įstrižai iš dešinės. *Combine* naudojama max{Cd1, Cd2, Cd3, Cd4} paskaičiavimui, *binarise* – skaitmenizavimui naudojant *Otsu* metodą.

Vextraction struktūrinė schema rodoma žemiau. *Hextraction, o1extraction* ir *o2extration* yra labai panašios.



32 pav. Extraction funkcijos struktūrinė schema

Curvature funkcija naudojama maksimalaus taško radimui bendro pjūvio profilyje y. Funkcijos sintaksė: [K, P, Scr] = curvature(y). Ji grąžina tris kintamuosius [K, P, Scr], kurie atitinkamai reiškia k(z), zi‘, reikšmę, kurie aprašyti aukščiau. *Filter* funkcija naudojama linijų centro ryškinimui ir triukšmo mažinimui.

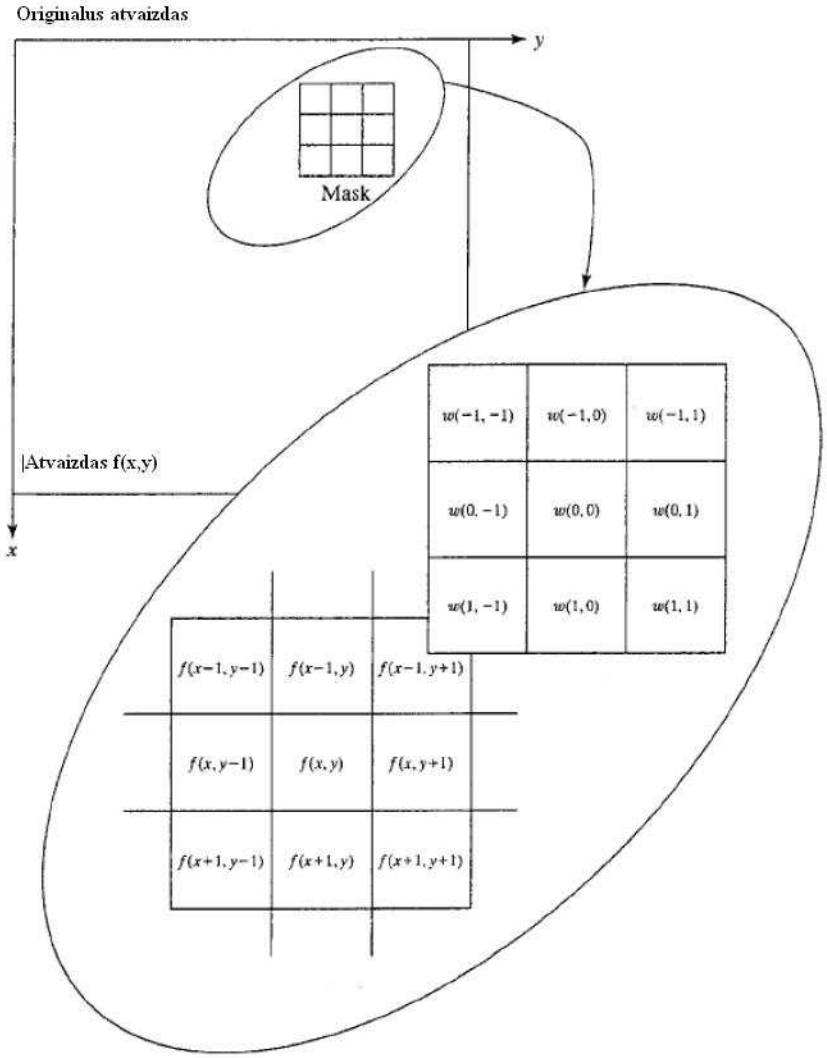


33 pav. Curvature funkcijos struktūrinė schema

2.4.4 Šablonų lyginimas bei sprendimo priėmimas

Šiame žingsnyje kraujagyslių struktūra paverčiama duomenimis, kurie su esančiais duomenų bazėje. Lyginimui naudojamas patobulintas šablonų lyginimo metodas [23]. Jei koreliacinė reikšmė yra didesnė, nei numatyta, vykdoma sėkminga autentifikacija. [22]

Taip pat gali būti naudojama dvidimensė koreliacija. Turime paveikslėlį f(x,y), koreliacija reiškia visų jo vietų radimą, kurios atitiktų šabloną w(x,y). Tam šablonas w judinamas paveikslėlyje nuo taško prie taško. Kiekviename (x,y) taške gauname šablono ir kaimyninių taškų sandaugų sumą.



34 pav. Linijinio erdvinio filtravimo principas

Matlab tai aprašoma:

```
Function g=dftcorr(f,w);

[M,N] = size(f);

f=fft2(f);

w=conj(fft2(w,M,N));

g=real(fft2(w.*f));
```

Ši funkcija grąžina M x N dydžio paveikslėlį c(x,y). Maksimali jo reikšmė yra maksimalus atitinkamų f ir w paveikslėlių taškų skaičius. Funkcija, grąžinanti baltų taškų kiekį: b(f). Atitikimo apskaičiavimui naudojame:

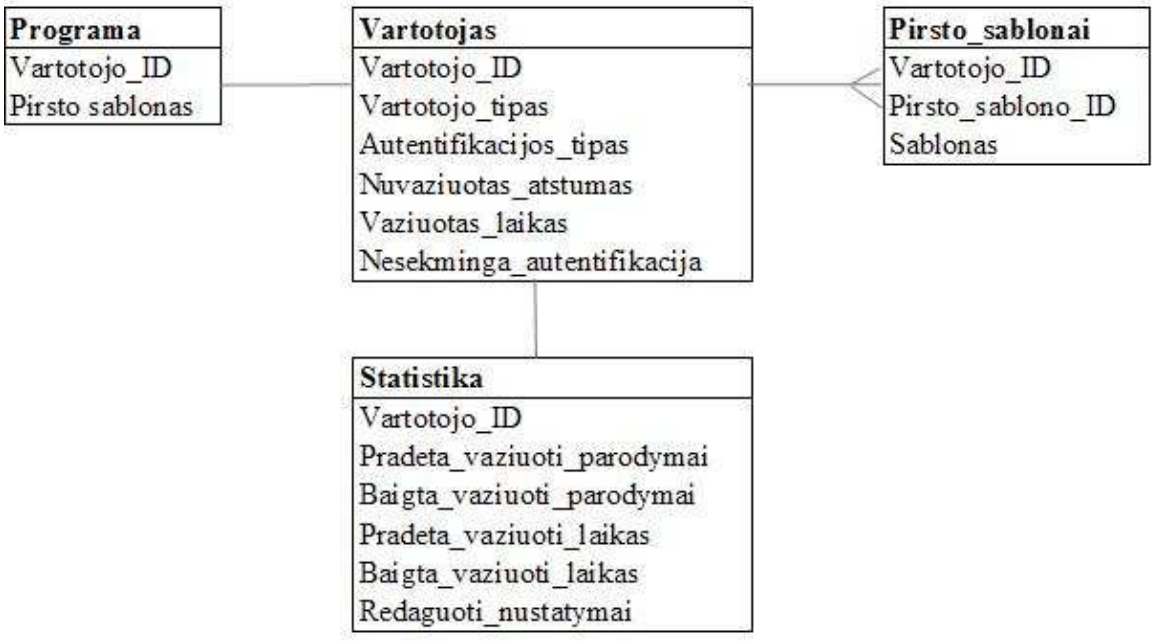
$$\frac{C}{F} = \frac{\max(c)}{\sigma(f)} x100\%$$

$$\frac{D}{F} = \frac{|\sigma(w) - \sigma(f)|}{\sigma(f)} x100\%$$

C/F rodo kiek lyginami šablonai turi vienodų, o D/F – kiek skirtingų taškų [41].

2.5 Duomenų bazė

2.5.1 Duomenų bazės schema



35 pav. Duomenų bazės schema

2.5.2 Duomenų bazės lentelių aprašymas

Vartotojas:

Šioje lentelėje bus saugomi vartotojo duomenys

3 lentelė. Lentelės "Vartotojas" laukai.

Pavadinimas	**Tipas**	**Paskirtis**
Vartotojo_ID	CHAR(5)	Vartotojo *ID*
Vartotojo_tipas	SET('vartotojas','administratorius')	Vartotojo tipas
Nuvaziuotas_atstumas	INT(11)	Vartotojo nuvažiuotas atstumas metrais
Vaziuotas_laikas	INT(10)	Vartotojo važiuotas laikas minutėmis
Nesekminga_autentifikacija	INT(1)	Nesėkmingų autentifikacijų skaitliukas

Statistika:

Šioje lentelėje bus saugoma statistinė informacija apie kiekvieną vartotoją

4 lentelė. Lentelės "Statistika" laukai.

Pavadinimas	**Tipas**	**Paskirtis**
Vartotojo_ID	CHAR(5)	Vartotojo *ID*
Pradeta_vaziuoti_parodymai	INT(10)	Automobilio odometro parodymai pradėjus važiuoti
Baigta_vaziuoti_parodymai	INT(10)	Automobilio odometro parodymai baigus važiuoti
Pradeta_vaziuoti_laikas	DATETIME	Laikrodžio parodymai pradėjus važiuoti

Baigta_vaziuoti_laikas	DATETIME	Laikrodžio parodymai baigus važiuoti
Redaguoti_nustatymai	DATETIME	Paskutinio nustatymų redagavimo data

Pirsto_sablonai:

Šioje lentelėje bus saugomi visų vartotojų piršto kraujagyslių šablonai, apsaugoti naudojant vandens ženklų [39], chaoso fenomeno [40] ar pan. metodus.

5 lentelė. Lentelės "Pirsto_sablonai" laukai.

Pavadinimas	**Tipas**	**Paskirtis**
Vartotojo_ID	CHAR(5)	Vartotojo *ID*
Pirsto_sablono_ID	INT(4)	Piršto kraujagyslių šablono *ID*
Sablonas	LONGBLOB	Laukas piršto kraujagyslių šablonui

Programa:

Šioje lentelėje bus saugomi identifikacijos metu vartotojo įvesti ID ir piršto kraujagyslių šablonai

6 lentelė. Lentelės "Programa" laukai.

Pavadinimas	**Tipas**	**Paskirtis**
Vartotojo_ID	CHAR(5)	Vartotojo įvestas *ID*
Pirsto sablonas	LONGBLOB	Piršto kraujagyslių skaitytuvo nuskaityta informacija

2.6 Išvados

Naudojamos autentifikacijos sistemos neužtikrina reikalingo saugumo, yra nepatvarios ir nesunkiai apeinamos.

PIN kodas, sudarytas iš 4 skaitmenų reikiamos saugos neužtikrina, jį lengvai galima „nužiūrėti“. Atsakiklis, ar nešiojamas pirštų antspaudų skaneris gali būti pamestas ar pavogtas,. Pirštų antspaudai „nuimti“ nuo paties skanerio, ar kito asmens liesto paviršiaus ir vėliau gali būti panaudoti atrakinant ir/ar užvedant transporto priemonę. Mechaniniai užraktai patikimos apsaugos negarantuoja, sumanūs kriminalinio pasaulio atstovai juos atrakina su specialią įrangą. Taip pat atrakinimui naudojami raktai gali būti pamesti ar pavogti. Įprastos išorinės biometrinės autentifikacijos sistemos yra labai nepatvarios ir nepatikimos, nes veikiamos išorinių veiksnių, tokių kaip temperatūros svyravimai, purvas bei drėgmė negali užtikrinti teisingo veikimo. Atsiranda ir akies rainelės atpažinimo metodais paremtos sistemos [6], tačiau yra nepatogus pats autentifikacijos procesas, reikalingas ypatingas tikslumas.

Susiduriama su problema - yra reikalinga patogi, greitai veikianti, ypatingai aukštą saugumo lygį užtikrinanti sistema.

Sistema turi būti patikima, patogi naudoti, turi užtekti ribotų išteklių (procesoriaus, atminties).

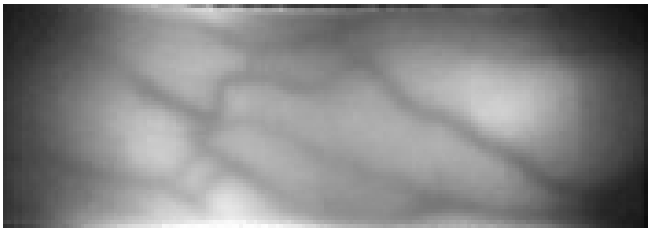
Šio darbo tikslas yra sukurti biometrinės autentifikacijos modelį automobiliams ir jį ištirti. Uždaviniai – išanalizuoti automobilių saugos priemones, apžvelgti esamus sprendimus, detaliau išanalizuoti biometrinių priemonių savybes, trūkumus bei privalumus, į kuriuos atsižvelgdami rinksimės šiai panaudojimo sričiai tinkamiausius.

Suprojektuosime tenkinančią nustatytus reikalavimus įterptinę sistemą, aprašysime eksperimentą, paaiškinsime gautus rezultatus.

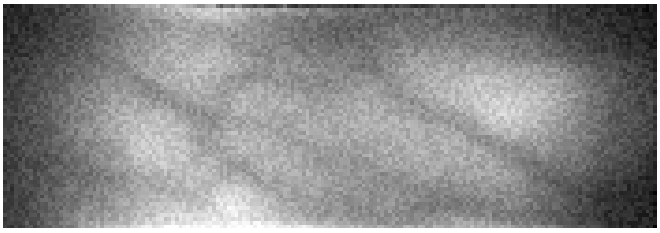
Eksperimento metu, palyginus kelis algoritmus išrinksime labiausiai tinkantį šiai sistemai.

3. EKSPERIMENTAS

Eksperimento metu tyrėme piršto antspaudų autentifikavimo algoritmų tinkamumą piršto kraujagyslių atvaizdų autentifikacijai bei raiškos ir triukšmų įtaką rezultatams. Eksperimentui naudojome *Inteligent Biometric Group* atlikto eksperimento atvaizdus [32]. Imituojant skirtingus to paties piršto skanavimus, paveikslėlių apdorojimo programa pakeitėme atvaizdų atspalvį, kontrastą ir šviesumą, taip gaunant po 5 to paties piršto atvaizdus. Imituojant aplinkos įtaką, tokią kaip purvas, ar aplinkos apšvietimas, paveikslėlių apdorojimo programa įvedėme skirtingo lygio triukšmą, naudojant funkciją *noise*, atitinkamai: 1 lygis 0%, 2 lygis - 5%, 3 lygis - 10% ir 4 lygis - 20%: . Imituojant skirtingos raiškos skanerio *CCD* kameras, eksperimentui naudojome skirtingų raiškų atvaizdų serijas: 1 lygis - 180 x 60 taškų, 2 lygis - 150 x 50 taškų, 3 lygis - 120 x 40 taškų, 4 lygis – 90 x 30 taškų. Toliau tokiu pat žingsniu mažinant raišką, tirti algoritmai nebeatpažįsta atvaizdų, nebeišskiria būdingų taškų palyginimui. Taip gavome 16 serijų, kiekvieną sudarytą iš 20 atvaizdų.



36 pav. Nemodifikuotas originalios raiškos atvaizdas



37 pav. Originalios raiškos atvaizdas imituojant triukšmą

38 pav. Mažiausios raiškos atvaizdas imituojant triukšmą

Modeliavimą atlikome *Matlab* 2007b aplinkoje, naudojome 3 algoritmus:

- Figūros konteksto ir orientacijos deskriptoriais pagrįsto atvaizdų atpažinimo [34],
- Filtrais paremto atvaizdų atpažinimo [35],
- Gretimos orientacijos vektoriais pagrįsto atvaizdų atpažinimo [36].

3.1 Algoritmų aprašymas

3.1.1 Figūros konteksto ir orientacijos deskriptoriais pagrįsto atvaizdų atpažinimo

a) Surandami formos kraštų taškai

Skaitoma, kad figūros formą sudaro baigtinis taškų skaičius. Kraštai gali būti nesunkiai randami naudojant išmanų kraštų aptikimo algoritmą ir atsitiktinai pasirenkant kraštų taškus. Šie taškai paprastai neatitinka esminių, kaip kad išlinkio, taškų. Pageidaujama, kad lyginamų bandinių forma būtų apgaubta vienodais tarpais, tačiau tai nėra būtina.

b) Apskaičiuojamas figūros kontekstas

Figūros kontekstas leidžia išmatuoti figūrų panašumą, palyginant atitinkamus taškus. Pasirenkama n figūros kontūro taškų. Kiekvienam p_i figūros taškui gauname n-1 vektorių, jungiant p_i su likusiais taškais. Šių vektorių rinkinys yra puikus formos lokalizavimo aprašymas, tačiau per daug detalus. Taigi taškui p_i apibrėžiama susijusių n-1 koordinačių grubi diagrama, ji ir yra figūros kontekstas:

$$h_i(k) = \#\{q \neq p_i : (q - p_i) \in \mathrm{bin}(k)\}.$$

c) Apskaičiuojama verčių matrica

Du taškai p ir q turi normalizuotas K-bin histogramas g(k) ir h(k). Formų kontekstai yra išsidėstymai, kuriuos atvaizduoja histogramos.

$$C_S = \frac{1}{2}\sum_{k=1}^{K}\frac{[g(k) - h(k)]^2}{g(k) + h(k)}$$

Gaunama vertė nuo iki 0 iki 1. Taip pat galima pridėti vertę, priklausiančią nuo išvaizdos. Pavyzdžiui matuojant kampo tangento skirtumus.

$$C_A = \frac{1}{2}\left\| \begin{pmatrix} \cos(\theta_1) \\ \sin(\theta_1) \end{pmatrix} - \begin{pmatrix} \cos(\theta_2) \\ \sin(\theta_2) \end{pmatrix} \right\|$$

Tai yra pusė stygos ilgio tarp bloko vektorių su kampais θ1 ir θ2. Gaunama vertė nuo iki 0 iki 1. Tada galima apskaičiuoti bendrą palyginimo sumą tarp dviejų taškų:

$$C = (1 - \beta)C_S + \beta C_A$$

Kiekvienam p_i taškui pirmoje figūroje ir q_j taškui antroje, apskaičiuojama vertė, kuri pažymima $C_{i,j}$. Tai ir yra verčių matrica.

d) Surandamas atitikmuo, kad minimizuoti bendrą vertę

Tada reikalingas vieno-su-vienu lyginimas kiekvienam pirmos figūros p_i ir antros figūros g_j taškui, kad sumažinti bendrą vertę:

$$H(\pi) = \sum_i C\left(p_i, q_{\pi(i)}\right).$$

e) Modeliuojama transformacija

Turėdami atitikmenų rinkinį tarp baigtinio skaičiaus taškų dviejose figūrose, galime atlikti transformaciją $T=R^2->R^2$, kad pažymėti bet kurį vienos figūros tašką kitoje figūroje:

$T(x,y) = (f_x(x,y), f_y(x,y))$, kur kiekvienas f_x ir f_y turi formą:

$$f(x,y) = a_1 + a_x x + a_y y + \sum_{i=1}^{n} \omega_i U\left(\left\|(x_i, y_i) - (x,y)\right\|\right),$$

ir funkcija $U(r)=r^2 \log r^2$.

f) Apskaičiuojamas formų atstumas

Pirmiausia apskaičiuojamas figūrų konteksto atstumas:

$$D_{sc}(P,Q) = \frac{1}{n}\sum_{p \in P} \arg\min_{q \in Q} C(p, T(q)) + \frac{1}{m}\sum_{q \in Q} \arg\min_{p \in P} C(p, T(q))$$

Tada randama išvaizdos vertė, kuri gali būti nusakoma kaip kvadratiniai šviesumo skirtumai Gauso languose apie atitinkamus atvaizdo taškus:

$$D_{ac}(P,Q) = \frac{1}{n}\sum_{i=1}^{n}\sum_{\Delta\in Z^2} G(\Delta)\left[I_P(p_i+\Delta) - I_Q(T(q_{\pi(i)})+\Delta)\right]^2,$$

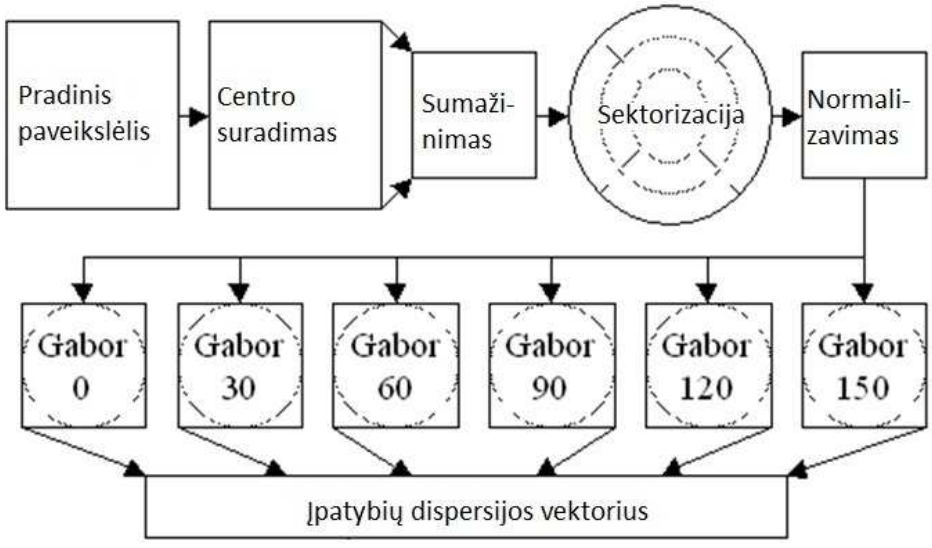
kur I_p ir I_q yra pilki atvaizdai, o G – Gauso langa funkcija.

Galiausiai skaičiuojama transformacijos vertė $D_{be}(P,Q)$, kuri nurodo kiek daug reikia transformuoti du paveikslėlius, kad jie vienas kitą atitiktų.

3.1.2 Filtrais paremto atvaizdų atpažinimo

Pirmiausia surandamas paveikslėlio centras ir paveikslėlis sumažinamas, taip pagreitinant sekančius veiksmus. Tuomet atliekama sektorizacija bei normalizavimas, siekiant gauti kuo tikslesnį atvaizdą. Sekančiu žingsniu pritaikomas Gabor filtras šešiomis skirtingomis kryptimis bei susumavus gautus rezultatus gaunamas ypatybių dispersijos vektorius. Gabor yra linijinis filtras, skirtas kampų atpažinimui. Šioje lygtyje, λ reiškia sinusoidinio faktoriaus bangos ilgį, θ – statmens orientacija su Gabor funkcijos paralelinėmis juostomis, ψ – fazės kompensacija, σ – Gauso apvalkalo sigma, γ – erdvinis kraštinių santykis:

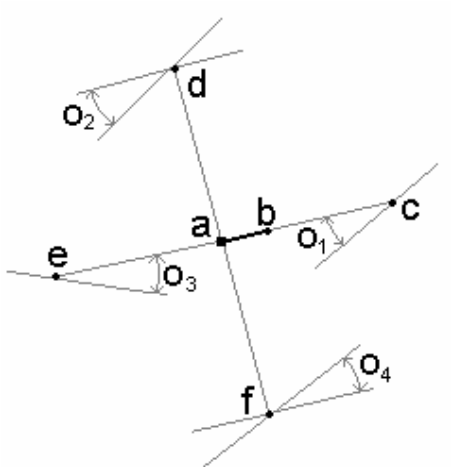
$$g(x,y;\lambda,\theta,\psi,\sigma,\gamma) = \exp\left(-\frac{x'^2+\gamma^2y'^2}{2\sigma^2}\right)\exp\left(i\left(2\pi\frac{x'}{\lambda}+\psi\right)\right).$$



39 pav. Filtrais paremto atpažinimo veikimo principas

3.1.3 Gretimos orientacijos vektoriais pagrįsto atvaizdų atpažinimo

Pirmiausia gretimos orientacijos vektoriai (*GOV*) naudojami rasti galimas *minutiae* poras. Tada vienas *minutiae* rinkinys yra pasukamas ir interpretuojamas. Po to seka preliminarus palyginimas, kad užtikrinti patikimumą, kaip ir tikslų atitikimą, išvengiant galimo iškraipymo. Vektorius sudaromas iš *minutiae* tipo, koordinačių ir tangentinio *minutiae* kampo. Tuomet palyginami ne paveikslėliai, o taškai.



40 pav. Gretimos orientacijos vektorius

a yra minutiae taškas, b – atitinkamas orientacijos taškas, c, d, e ir f yra keturi gretimos orientacijos taškai, tenkinantys sąlygas: $|ac|=|ad|=|ae|=|af|=D_{dis}$, $\angle bac=0$, $\angle bad=\angle bae=\pi$, o $\angle baf=3\pi/2$, o D_{dis} – konstanta. Kadangi a, b, c ir d yra keturi taškai antspaude, jie turės orientacijas. Skirtumą tarp šių ir minutiae taško orientacijų žymėsime o_1, o_2, o_3 ir o_4. Briaunų skaičius tarp ac, ad, ae ir af taip pat naudojamas patikimam palyginimui, juos pažymint n_1, n_2, n_3 ir n_4. Taigi vektorius $< o_1, o_2, o_3, o_4, n_1, n_2, n_3, n_4 >$ vadinamas gretimos orientacijos vektoriumi. p ir q yra atitinkami to paties piršto dviejų atvaizdų taškai, taigi jie turės labai panašias gretimumų savybes, taigi ir labai panašius *GOV*. Šiuos vektorius lengva išgauti, o dėl jų paprastos struktūros, dviejų atvaizdų sulyginimas tampa greitesniu.

Tarkim $< o_{11}, o_{12}, o_{13}, o_{14}, n_{11}, n_{12}, n_{13}, n_{14} >$ ir $< o_{21}, o_{22}, o_{23}, o_{24}, n_{21}, n_{22}, n_{23}, n_{24} >$ yra du *GOV*. Kad juos palyginti, turime rasti panašumą tarp jų. Jis apskaičiuojamas: $f_0(|o_{11}-o_{12}|+|o_{21}-o_{22})+f_0(|o_{13}-o_{14}|+|o_{23}-o_{24}|)+f_n(|n_{11}-n_{12}|+|n_{21}-n_{22}|)+f_n(|n_{13}-n_{14}|+|n_{23}-n_{24}|)$, kur f_0 yra orientacijos koeficientas, o f_n – briaunų skaičiaus faktorius. Skaitome, kad iš dviejų antspaudų atvaizdų išgaunami minutiae taškai P ir Q, galima gauti visas galimas sutampančias poras $<p_m,q_n>$, kai $p_m \in P$ ir $q_n \in Q$.

Pirmiausia vykdomas preliminarus lyginimas, kuris reikalingas patikimumui. S_g yra atitikusi pora, T_p – lyginimo slenkstis:

S_g =NULL
PreScore=0
  for all $p \in P$ and $q \in Q$ {
      if $< p.q > \in S_m$ {
       PreScore=PreScore+1
      }
  }
  if (PreScore > T_p){
     add $< p.q >$ to sets S_g
  }

41 pav. Preliminaraus lyginimo algoritmas

Toliau vykdomas tikslus lyginimas, kad išvengti galimų iškraipymų. T_y ir $T\theta$ ribos naudojamos nustatyti, ar minutiae poros gali būti pridėtos prie S_g. Veiksmai kartojami, kol prie S_g daugiau negalima pridėti minutiae porų.

$< i, j > \in S_g$ $< s, t > \notin S_g$

if ($\left|\left(i_y - s_y\right) - \left(j_y - t_y\right)\right| < T_y$ and
   $\left|\left(i_\theta - s_\theta\right) - \left(j_\theta - t_\theta\right)\right| < T_\theta$) {
   add $< s, t >$ to S_g
}

42 pav. Tikslaus lyginimo algoritmas

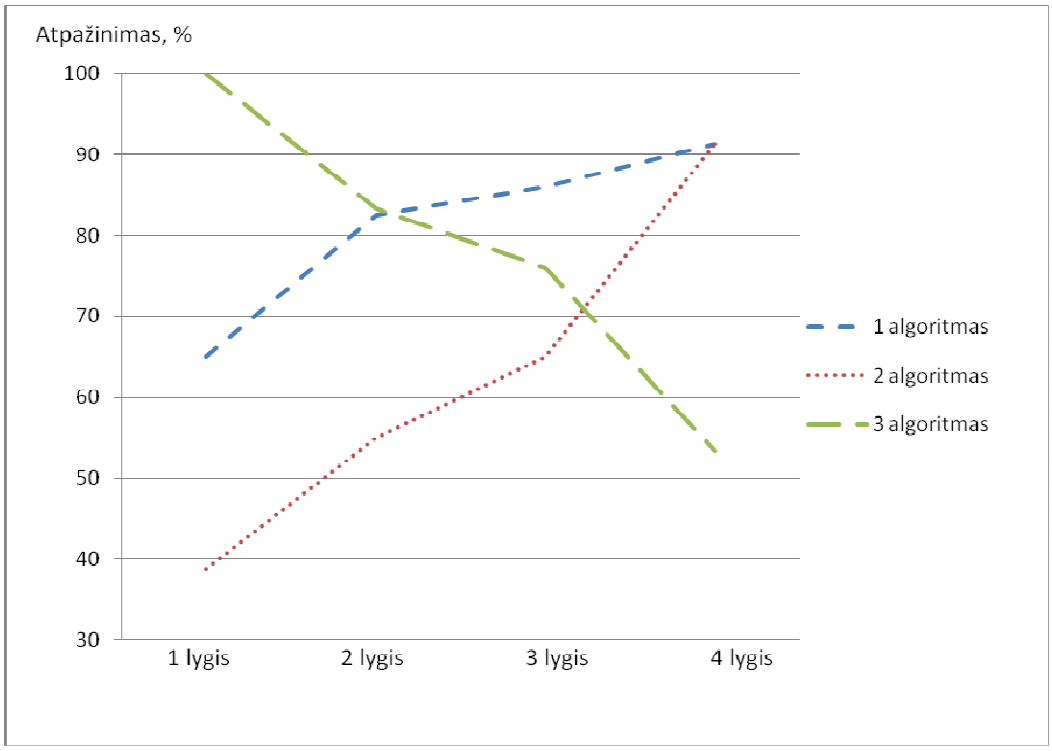
3.2 Eksperimento eiga

Lyginome kiekvieną serijos atvaizdą su likusiais tos pačios serijos atvaizdais bei fiksavome gautus rezultatus: sėkmingą atpažinimą, nesėkmingą atpažinimą, neteisingą atmetimą, neteisingą priėmimą.

Atvaizdų lyginimo laiko neskaičiavome, nes *Matlab* aplinka labai neefektyviai atlieka veiksmus su paveikslėliais. Optimizavus programinį kodą žemesnio lygio programavimo kalboms, galima pasiekti daugiau kaip 750 kartų pagerėjimą, naudojant mažesnio pajėgumo įterptinį procesorių [33]. Literatūroje rašoma, kad naudojant 550Mhz procesorių ir 128Mb operatyvinės atminties bei Visual C++ platformą, autentifikacijai užtenka 460 milisekundžių: 450 milisekundžių esminių taškų išskyrimui ir dar 10

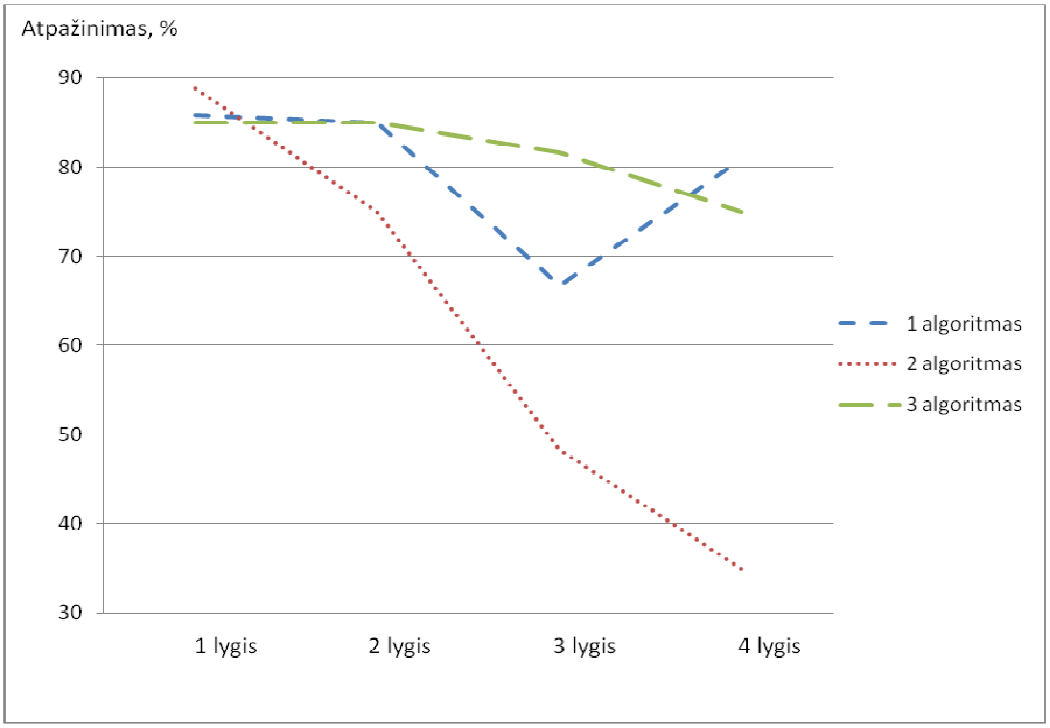
milisekundžių – jų palyginimui [21], o naudojant specializuotą 150Mhz ARM9 šeimos procesorių, autentifikavimui užtenka 250 milisekundžių [19].

Atlikus eksperimentą, gavome rezultatus, kuriuos sugrupavome, kad aiškiai matytųsi algoritmų sugebėjimas teisingai atpažinti atvaizdus, priklausomai nuo atvaizdo dydžio bei triukšmo.



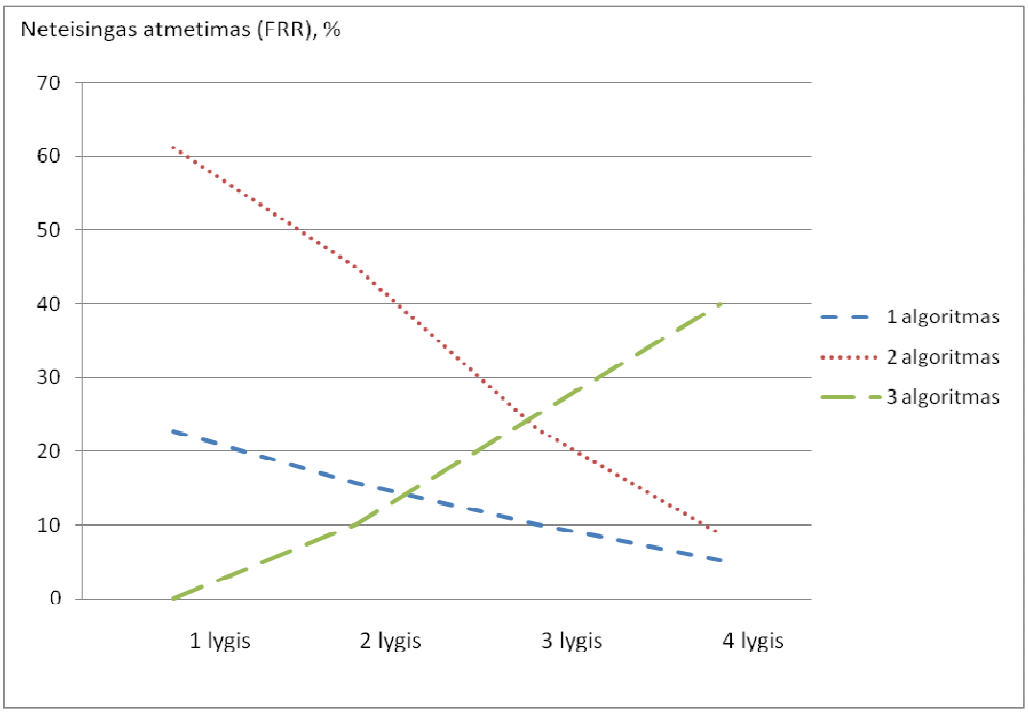
43 pav. Sėkmingo atpažinimo priklausomybė nuo atvaizdo raiškos. Didesnis skaičius reiškia geresnį rezultatą

Sėkmingo atpažinimo rezultatai esant pradinei lyginamo atvaizdo raiškai geriausi algoritmui nr. 3. – teisingai atpažįstami visi bandiniai. Algoritmas nr. 1 sėkmingai atpažįsta 65% bandymų autentifikuotis, nr. 2 – 39%. Mažinant lyginamų atvaizdų raišką, algoritmo nr. 2 rezultatai ženkliai krenta, kai tuo tarpu algoritmų nr.1 ir nr.2 – rezultatai gerėja. Esant 4 lygio raiškai, algoritmai nr. 1 ir nr. 2 sėkmingai atpažįsta 91% bandymų autentifkuotis, nr. 3 – tik 53%.



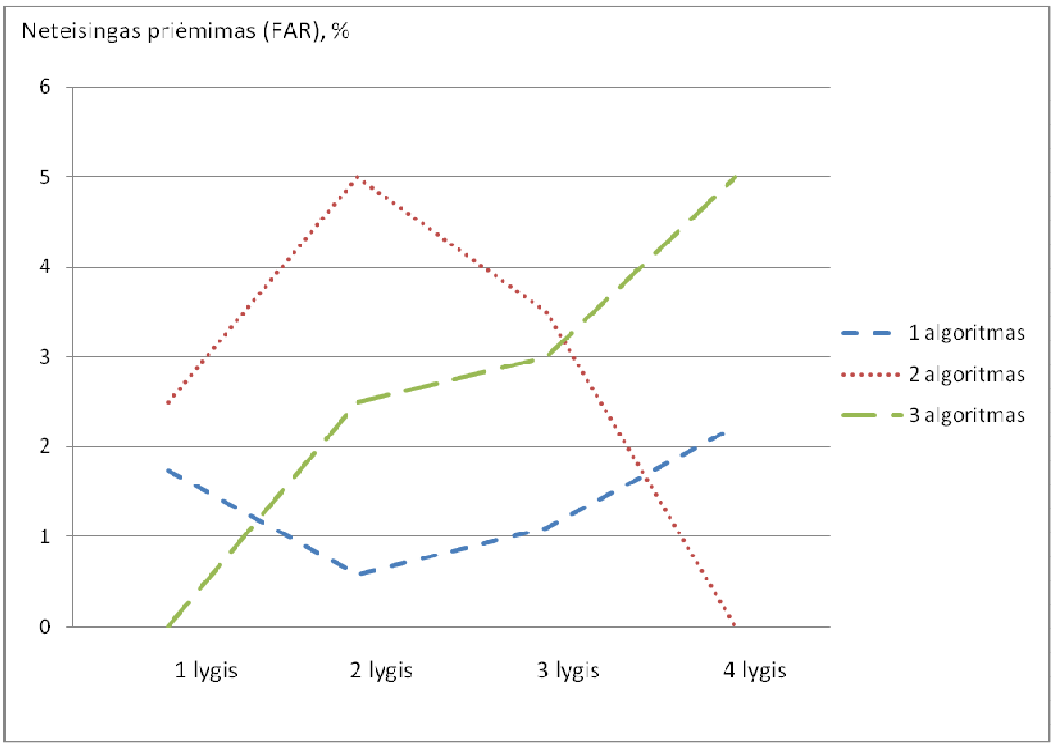
44 pav. Sėkmingo atpažinimo priklausomybė nuo triukšmo. Didesnis skaičius reiškia geresnį rezultatą

Sėkmingo atpažinimo rezultatai esant pradiniam triukšmo lygiui labai panašūs visiems algoritmams: nr.1 sėkmingai atpažįsta 89%, nr.2 – 86%, nr.3 – 85%. Didinant triukšmą lyginamuose atvaizduose, algoritmo nr.2 rezultatai ženkliai krenta, pasiekus 4 lygį, atpažįstama mažiau nei 40% bandymų autentifikuotis. Algoritmų nr.1 ir nr.3 – kinta ne taip ženkliai, sėkmingai atpažįstama atitinkamai 81% ir 75%.



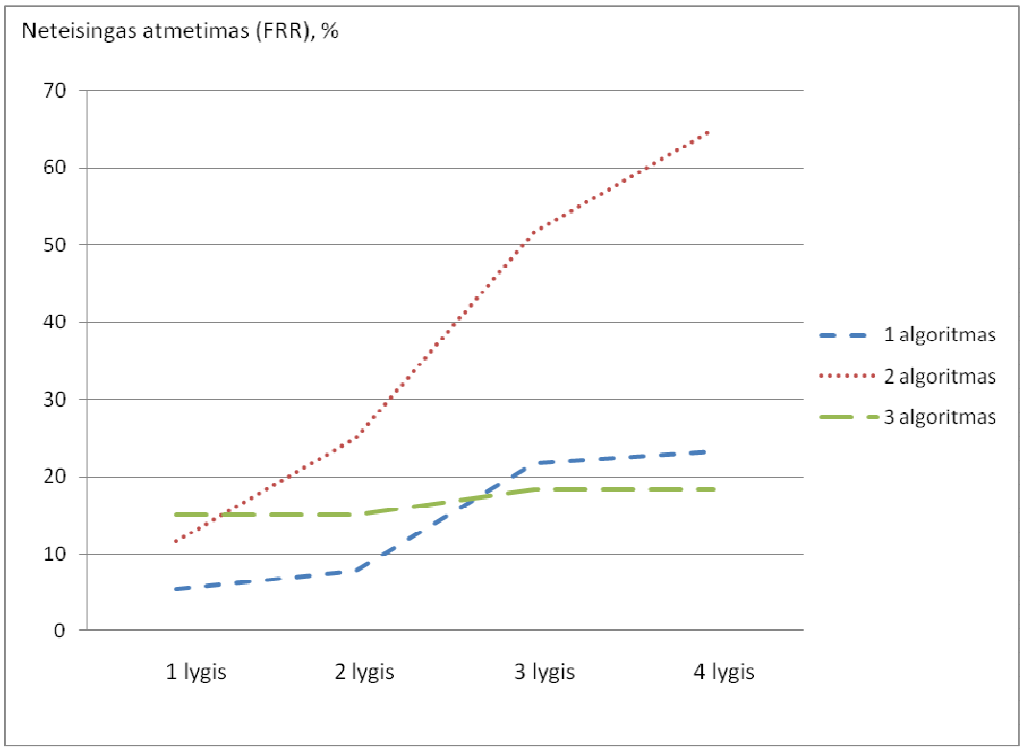
45 pav. Neteisingo atmetimo (FRR) priklausomybė nuo raiškos. Mažesnis skaičius reiškia geresnį rezultatą

Neteisingo atmetimo rezultatai esant pradinei lyginamo atvaizdo raiškai yra geriausi algoritmui nr. 3 – neteisingai neatmetama nei vienas bandymas autentifikuotis. Algoritmas nr. 1 neteisingai atmeta 22%, nr. 2 – net 61%. Mažinant lyginamų atvaizdų raišką, algoritmo nr.3 rezultatai ženkliai krenta – didėja neteisingai atmestų bandymų autentifikuotis skaičius, pasiekus 4 lygio raišką jis siekia 40%. Tuo tarpu algoritmų nr.1 ir nr.2 rezultatai mažinant raišką iki 4 lygio gerėja ir pasiekia atitinkamai 5% ir 9% neteisingų atmetimų.



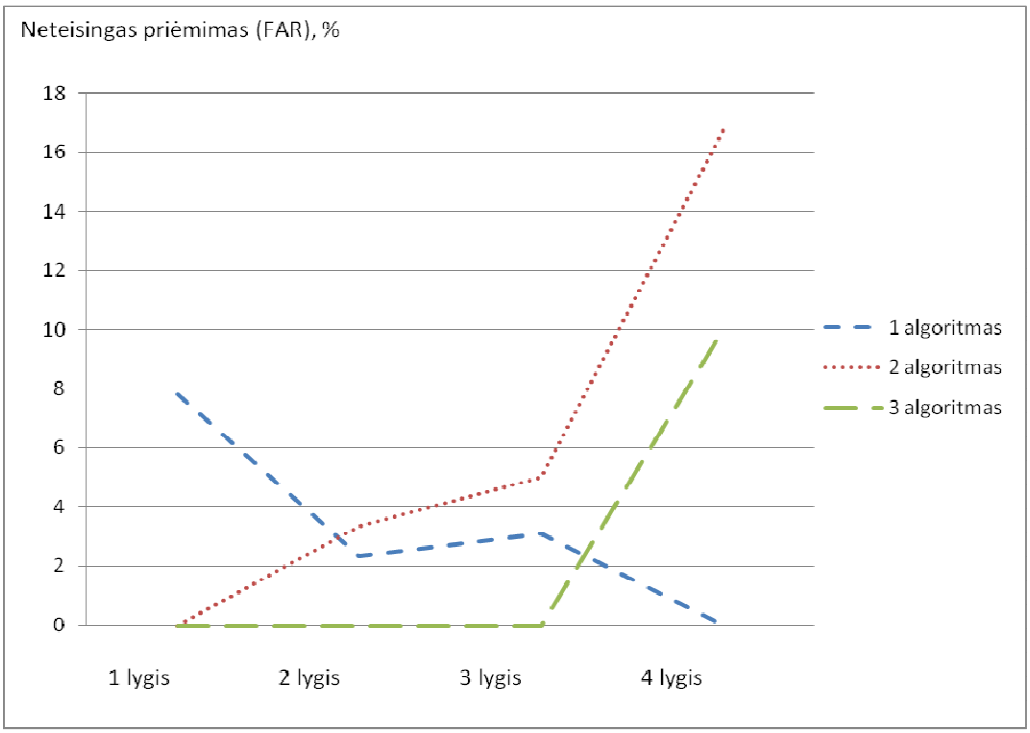
46 pav. Neteisingo priėmimo (FAR) priklausomybė nuo raiškos. Mažesnis skaičius reiškia geresnį rezultatą

Neteisingo priėmimo rezultatai esant pradinei lyginamo atvaizdo raiškai geriausi algoritmui nr. 3 – nefiksuojamas nei vienas neteisingas priėmimas. Algoritmas nr. 1 neteisingai priima 1.7%, o nr.2 – 2.5% bandymų autentifkuotis. Mažinant atvaizdų raišką, algoritmo nr.3 rezultatai akivaizdžiai blogėja ir pasiekus 4 lygį, neteisingai priimama jau 5% . Algoritmo nr.1 pasiekus 4 raiškos lygį nežymiai pablogėja – iki 2.2%, o algoritmo nr. 2 atveju – nefiksuojama nei vieno neteisingo priėmimo



47 pav. Neteisingo atmetimo (FRR) priklausomybė nuo triukšmo. Mažesnis skaičius reiškia geresnį rezultatą

Neteisingo atmetimo rezultatai esant pradiniam triukšmo lygiui geriausi algoritmui nr. 1 – neteisngai atmetama 5% bandymų. Nr. 2 atveju neteisingai atmetama 12%, o nr. 3 – 15% bandymų autentifikuotis. Didinant triukšmo intensyvumą, visų algoritmų rezultatai blogėja: nr. 1 iki 23%, nr. 2 net iki 65%, nr.3 – iki 18%.



48 pav. Neteisingo priėmimo (FAR) priklausomybė nuo triukšmo. Mažesnis skaičius reiškia geresnį rezultatą

Neteisingo priėmimo rezultatai esant pradiniam triukšmo lygiui geriausi algoritmams nr. 2. ir nr.3. – neteisingų priėmimų nefiksuojama, o algoritmo nr. 1 atveju neteisingai priimama 8% bandymų autentifikuotis. Didinant triukšmo intensyvumą, algortimų nr. 2 ir nr. 3 rezultatai blogėja, pasiekdami atitinkamai 10% ir 17%. Tuo tarpu, esant pradinėms sąlygoms blogiausius rezultatus parodęs algoritmas nr.1 esant didžiausiam, 4-am triukšmo lygiui, rodo geriausius rezultatus – neteisingų priėmimų nefiksuojama.

Rezultatų lentelę sudarėme įvertindami algoritmų rezultatus: 3 balai – gerai, 2 balai – vidutiniškai, 1 balas – blogai. Vertinome tik 4 raiškos ir triukšmo lygių rezultatus. Susumavus juos gavome, kad geriausiai iš šių trijų, mūsų sąlygomis, veikia algoritmas nr. 1 - figūros konteksto ir orientacijos deskriptoriais atvaizdų atpažinimo principu veikiantis algoritmas.

7 lentelė. Galutiniai algoritmų rezultatai. Didesnis skaičius reiškia geresnį rezultatą

	Algoritmai		
	1	2	3
Raiška			
Sėkmingas atpažinimas	3	3	2
Neteisingas atmetimas	2	1	3
Neteisingas priėmimas	2	3	1
Viso	7	7	6
Triukšmas			
Sėkmingas atpažinimas	3	1	3
Neteisingas atmetimas	2	1	2
Neteisingas priėmimas	3	1	2
Viso	8	3	7
Galutinis rezultatas	**15**	**10**	**13**

Naudojome pradinį 180 x 60 taškų raiškos vaizdą, nors realiai naudojamose sistemose neapdoroto atvaizdo rekomenduojama raiška yra 320 x 240 taškų, todėl gauti rezultatai gali būti neitin tikslūs. Kadangi nuo atvaizdo raiškos priklauso įrenginio kainą, jos minimizavimo tikslu, tačiau išlaikant pakankamą sistemos užtikrinamą saugumą, didesnį dėmesį skyrėme mažesnės raiškos atvaizdų atsparumui triukšmui. Mažėjant atvaizdo raiškai ir blogėjant atvaizdo kokybei, teisingiausiai veikia algoritmas nr. 1 - formos konteksto ir orientacijos deskriptoriais atvaizdų atpažinimo principu veikiantis algoritmas, nors esant pradinėms sąlygoms, rezultatai gaunami vidutiniški. Esant pirminei raiškai, su visais triukšmo lygiais teisingiausiai veikia trečiasis algoritmas. Antrasis algoritmas labai jautrus triukšmui ir šiam didėjant, žymiai išauga neteisingų atmetimų skaičius.

4. IŠVADOS

Automobilių apsauga visada buvo, yra ir bus aktuali. Esamos apsaugos priemonės nesunkiai apeinamos ir nesudaro didelių kliūčių, norint transporto priemonę pasisavinti. Todėl reikalinga naujoviška vairuotojo autentifikavimo sistema, galinti sumažinti šią, pasisavinimo tikimybę. Mūsų atveju piršto kraujagyslių skanavimas turi daugiau privalumų lyginant su kitais plačiau naudojamais metodais kaip piršto antspaudai, rainelė, veidas ir t.t. Piršto kraujagyslių skanavimas tai aukšto patikimumo autentifikacijos metodas, kuris tuo pat metu labai sunkiai suklastojamas, neinvazinis ir lengvas naudoti, siūlantis privalumų balansą. Tai daro jį nepralenkiama biometrinės autentifikacijos forma.

Kraujagyslės yra po oda, jos yra nematomos apšviečiant natūralia šviesa. Tačiau jos puikiai matomos apšvietus artima infraraudoniems spinduliams šviesa (bangos ilgis tarp 700 ir 1000 nanometrų), kadangi ši šviesa lengvai sklinda per žmogaus kūno audinius, bet yra blokuojama tokių pigmentų, kaip hemoglobinas ar melaninas. Kadangi hemoglobino didelė koncentracija yra tik kraujagyslėse, apšvietus artima infraraudonosioms bangos šviesa, šios atrodo kaip tamsios linijos.

Literatūros šaltinių analizė parodė, jog ši autentifikacijos forma yra plačiai nagrinėjama, tyrinėjami geriausiai tinkantys algoritmai. Realiose sistemose ji plačiau naudojama Japonijoje (beveik 80% bankomatų turi kraujagyslių skanerius, jais naudojasi daugiau kaip 15 milijonų klientų), o nuo 2010 m. gegužės mėn. ir Europoje. Kitose srityse taikymas dar labai ribotas, tačiau situaciją keičia didieji elektronikos gamintojai, mažindami sistemos gabaritus ir kainą.

Atliekant šį magistrinį darbą, buvo sukurtas biometrinės autentifikacijos modelis: sudarėme sistemos reikalavimus, apibrėžėme sistemos architektūrą, duomenų bazės schemą.

Tyrėme atvaizdų atpažinimo algoritmų veiksmingumą dirbant su piršto kraujagyslių atvaizdais. Eksperimento metu nustatėme, kad šiai, siūlomai sistemos architektūrai, iš trijų tirtų algoritmų, sumažinus atvaizdo raiška ir kokybę, labiausiai tiktų figūros konteksto ir orientacijos deskriptoriais atvaizdų atpažinimo principu veikiantis algoritmas.

Tolimesniuose darbuose eksperimentui reiktų naudoti didesnės pradinės raiškos atvaizdus, išbandyti daugiau atvaizdų atpažinimo algoritmų. Raišką ir kokybę reiktų mažinti toliau, mažesniais žingsniais.

5. LITERATŪROS SĄRAŠAS

1. **[D. Zasas]**. [Pažyma apie transporto priemonių grobimų tyrimo būkle Lietuvos Respublikoje 2010 metais]. *[2011-04, Vilnius*].

2. **[Simon Liu and Mark Silverman]** [A practical guide to biometric security]. *[IT Pro January/February 2001, p.27 - 32*]

3. **[C. Maxine Most]**. [Biometrics Buck the Global Economic Meltdown; Industry Poised for Sustained Growth Reaching Nearly $11 Billion in Annual Revenues by 2017]. [interaktyvus] - *[žiūrėta 2009-11-15*]. Prieiga per internetą http://acuity-mi.com/FOB%20PR%201.pdf

4. **[Anil K. Jain, Arun Ross, Sharath Pankanti].** [Biometrics: a tool for information security, *IEEE transactions on informatikon forensics and security vol1, no. 2, june 2006]*.

5. **[Salah M. Rahal, Hatim A. Aboalsamah, Khaled N. Muteb]**. [Multimodal biometric autentication system – mbas, *IEEE 2006*].

6. **[United Linkers Biometric & Robotic Solutions].** [interaktyvus] - [*žiūrėta 2009-11-13*]. Prieiga per internetą http://www.automobile-security.com/.

7. **[Touch-n-Drive Biometric Ignition Auto Starter].** [interaktyvus] - [*žiūrėta 2009-11-20*]. Prieiga per internetą http://solarcorebiometricdevices.com/tobiaust.html.

8. **[Kejun Wang, Yan Zhang, Zhi Yuan and Dayan Zhuang].** [Hand vein recognition based on multi supplemental features of multi-classified fusion decition, *Proceedings of the 2006 IEEE International Conference on Mechatronics and Automation June 25 - 28, 2006, Luoyang, China*].

9. [**Junichi Hashimoto**]. [Finger vein authentication technology and its future, *Symposium on VLSI Circuits Digest of Technical Papers, 2006 Japan*].

10. **[Imobilaizeriai]** . [interaktyvus] - [*žiūrėta 2009-11-15*]. Prieiga per internetą http://www.lbm.lt/imobilaizeriai.htm.

11. **[Chowhan.S.S, G.N.Shinde].** [Iris biometrics recognition application in security management, *2008 Congress on Image and Signal Processing, 2008*].

12. **[Andreas Uhl and Peter Wild]**. [Personal identification using eigenfeet, ballprint and foot geometry biometrics, *IEEE, 2007*].

13. **[Takahiro Takeda, Kazuhiko Taniguchi, Kazunari Asari, Kei Kuramoto, Syoji Kobashi, Yutaka Hata].** [Biometric personal authentication by one step foot pressure distribution change by load distribution sensor, *FUZZ-IEEE 2009, Korea, August 20-24*].

14. **[Ibrahim Khalil, Fahim Sufi].** [Legendre polynomials based biometric authentication using QRS complex of ECG, *IEEE, 2008*].

15. **[Fuminori Okumura, Akira Kubota, Yoshinori Hatori, Kenji Matsuo, Masayuki Hashimoto, Atsushi Koike].** [A study on biometric authentication based onarm sweep action with acceleration sensor, *2006 International Symposium on intelligent signal processing and communication systems, Yonago convention center, Japan*].

16. **[Davrondzhon Gafurov, Einar Snekkenes].** [Arm swing as a weak biometric for unobtrusive user authentication, *International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008*].

17. **[Ajay Kumar, Ch. Ravikanth].** [Personal authentication using finger knuckle surface, *IEEE transactions on informatikon forensics and security, vol. 4, no. 1, march 2009*].

18. **[Xiangqian Wu, David Zhang, Kuanquan Wang].** [Palm line extraction and matching for personal authentication, *IEEE transactions on systems, man, and cybernetics — part a: systems and humans, vol. 36, no. 5, september 2006*].

19. **[Finger vein authentication].** [interaktyvus] – [*žiūrėta 2009-12-01*]. Prieiga per internetą http://portal.etsi.org/docbox/Workshop/2009/200901_SECURITYWORKSHOP/SONY_SATO_FingerVeinAuthentication.pdf

20. **[R.G. Maduranga Mjayamaha, Maduri R.R. Senadheera, T. Nuwan C. Gamage, K. D. Pavithra B. Weerasekara, Gayan A. Dissanayaka, G. Nuwan Kodagota]**. [VoizLock – Human Voice Authentication System using Hidden Markov Model, *Information and Automation for Sustainability 2008, ICIAFS*].

21. **[Luo, H., F.X. Yu, J.S. Pan, S.C. Chu, P.W. Tsai].** [A survey of vein recognition techniques. *Inform. Technol. J., 9: 1142-1149, 2010*].

22. **[David Mulyono, Horng Shi Jinn].** [A Study of Finger Vein Biometric for Personal Identification, *IEEE 1-4244-2427-6/08,* 2008].

23. [**Naoto Miura, Akio Nagasaka, Takafumi Miyatake**]. [Feature Extraction of Finger Vein Patterns Based on Repeated Line Tracking and Its Application to Personal Identification, *Machine Vision and Applications*, HI-TACHI, Ltd, 1-280, 2004].

24. [**Naoto Miura, Akio Nagasaka, Takafumi Miyatake**]. [Automatic feature extraction from non-uniform finger vein image and its application to personal identification, *Nara, Japan : IAPR, 2002, Vol. MVA2002*.]

25. **[A. Hoover, V. Kouznetsova, and M. Goldbaum].** [Locating blood vessels in retina image by piece-wise threshold probing of a matched filter response. *3, s.l. : IEEE Tras. Med. Imaging, 2000, Vol. 19, pp. pp 203-210.*]

26. **[T. Walter, J. Klein, P. Massin, and F. Zana]**. [Automatic segmentation and registration of retinal fluorescein angiograpies - Application to diabetic retinopathy. *Copenhagen, Denmark : s.n., May 2000. Vol. First international Workshop on Computer Assisted Fundus Image Analysis, pp. pp 15-20*.]

27. **[P. Montesinos and L. Alquier].** [Perceptual organization of thin networks with active contour functions applied to medical and aerial images. *Veinne, Autriche : ICPR'96, 1996. pp. pp 647-651*.]

28. **[D. Maio and D. Maltoni].** [Direct gray-scale minutiae detection in fingerprints. *s.l. : IEEE Trans. Pattern Anal. Mach. Intell., Jan 1997. Vol. 19, pp. 27-40.*]

29. [**Naoto Miura, Akio Nagasaka, Takafumi Miyatake**]. [An extraction of finger vein patterns based on multipoint interative line tracing. *2001. Proc. IEICE. Gen. Conf. 2001*.]

30. [**Naoto Miura, Akio Nagasaka, Takafumi Miyatake**]. [Extraction of finger-vein patterns using maximum curvature points in image profile. *8, s.l. : IEICE TRANS. INF. & SYST, August 2007, Vols. E90-D*.]

31. **[Nagao, M].** [Methods of image pattern recognition. *s.l. : Corona publishing, 1983*.]

32. **[Finger vein biometric system].** [interaktyvus] - [*žiūrėta 2011-02-26*]. Prieiga per internetą http://ibg-usm.org/v1/index.php?option=com_content&view=article&id=97&Itemid=71.

33. [**Víctor López Lorenzo, Pablo Huerta Pellitero, José Ignacio Martínez Torre, Javier Castillo Villar**]. [Fingerprint Minutiae Extraction Based On FPGA and MatLab. *Grupo de Diseño HwSw, 2005.*]

34. **[Fingerprint matching algorithm using shape context and orientation descriptors].** [interaktyvus] - [*žiūrėta 2011-02-28*]. Prieiga per internetą http://www.mathworks.com/matlabcentral/fileexchange/29280.

35. **[A.K.Jain, S.Prabhakar, L.Hong and S.Pankanti].** Filterbank-Based fingerprint matching. [interaktyvus] - [*žiūrėta 2011-02-28*]. Prieiga per internetą http://utenti.multimania.it/matlab/fingerprint4.htm.

36. **[G. S. Ng, X. Tong, X. Tang and D. Shi].** Adjacent orientation vector based fingerprint minutiae matching system. *Pattern recognition ICPR, 2004*.] Prieiga per internetą http://www.advancedsourcecode.com/aovminutiae.asp

37. **[Egidijus Kazanavičius]** [Signalų apdorojimo sistemos]. *[Kaunas, Technologija 2004, p.8 – 9.*]

38. **[Stan Z. Li, Anil K. Jain].** [Enciplopedia of biometrics]. [*Springer, 2009*. p. 192-195 .]

39. **[Islam, Md. Rajibul, Sayeed Md. Shohel, Samraj Andrews].** [Biometric template protection using watermarking with hidden password encryption. *Internation symposium on information technology, Kuala Lumpur, Malaysia, 2008*].

40. **[Maithili Arjunwadkar, R. V. Kulkarni].** [Robust Security Model for Biometric Template Protection using Chaos Phenomenon. *International Journal of Computer Applications (0975 – 8887) Volume 3 – No.6, June 2010*].

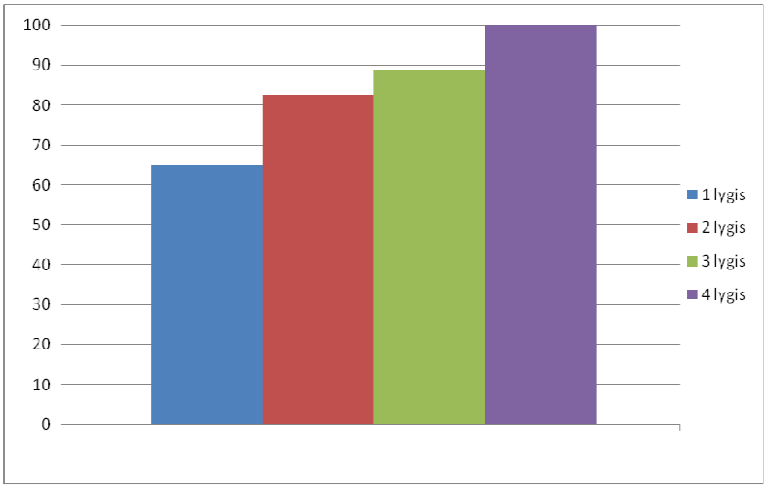
41. **[Trung Huyng].** [Finger Vein Authentication System. *BSC Electronic Communication System, University of Plymouth, United Kingdom*].

PRIEDAI

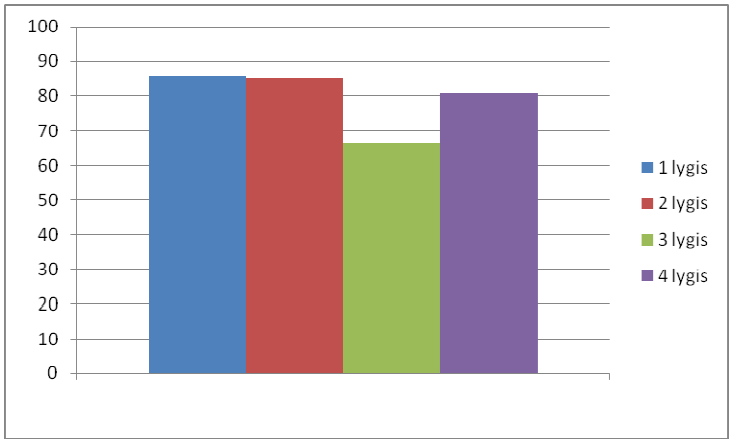
1 priedas. Pilni eksperimento rezultatai

8 lentelė. Pirmojo algoritmo rezultatai

Raiška	Triukšmas	Teisingi, %	Neteisingai atmesti, %	Neteisingai priimti, %
1	1 lygis	97.67	0	2.32
	2 lygis	90.69	6.97	2.32
	3 lygis	58.14	39.53	2.32
	4 lygis	55.81	44.18	0
2	1 lygis	90.69	9.3	0
	2 lygis	83.72	16.28	0
	3 lygis	81.39	16.28	2.32
	4 lygis	79.07	20.93	0
3	1 lygis	91.91	6.69	1.4
	2 lygis	90.97	6.8	2.23
	3 lygis	87.03	12.1	0.87
	4 lygis	85.7	14.3	0
4	1 lygis	93.02	6.98	0
	2 lygis	95.35	0	4.65
	3 lygis	86.05	9.3	4.65
	4 lygis	94.35	4.65	0



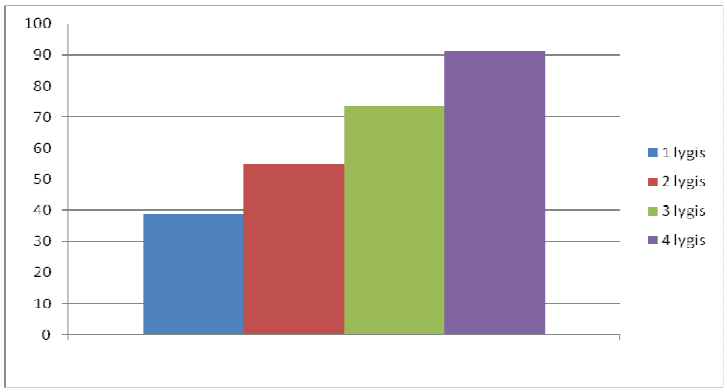
49 pav. Pirmo algoritmo sėkmingo atpažinimo priklausomybė nuo atvaizdo dydžio. Didesnis skaičius reiškia geresnį rezultatą



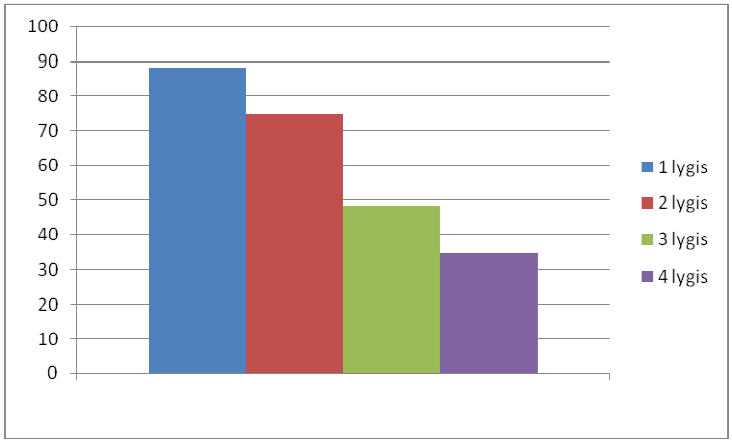
50 pav. Pirmo algoritmo sėkmingo atpažinimo priklausomybė nuo triukšmo. Didesnis skaičius reiškia geresnį rezultatą

9 lentelė. Antrojo algoritmo rezultatai

Raiška	Triukšmas	Teisingi, %	Neteisingai atmesti, %	Neteisingai priimti, %
1	1 lygis	90	10	0
	2 lygis	55	45	5
	3 lygis	5	90	5
	4 lygis	0	100	0
2	1 lygis	90	10	0
	2 lygis	70	25	5
	3 lygis	35	55	10
	4 lygis	5	90	5
3	1 lygis	87	13	0
	2 lygis	76	18	6
	3 lygis	69	23	8
	4 lygis	62	38	0
4	1 lygis	85	15	0
	2 lygis	95	5	0
	3 lygis	90	10	0
	4 lygis	95	5	0



51 pav. Antro algoritmo sėkmingo atpažinimo priklausomybė nuo atvaizdo dydžio. Didesnis skaičius reiškia geresnį rezultatą

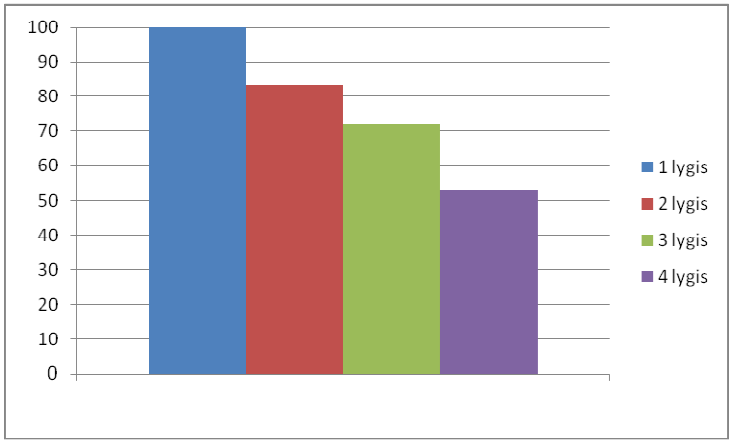


52 pav. Antro algoritmo sėkmingo atpažinimo priklausomybė nuo triukšmo. Didesnis skaičius reiškia geresnį rezultatą

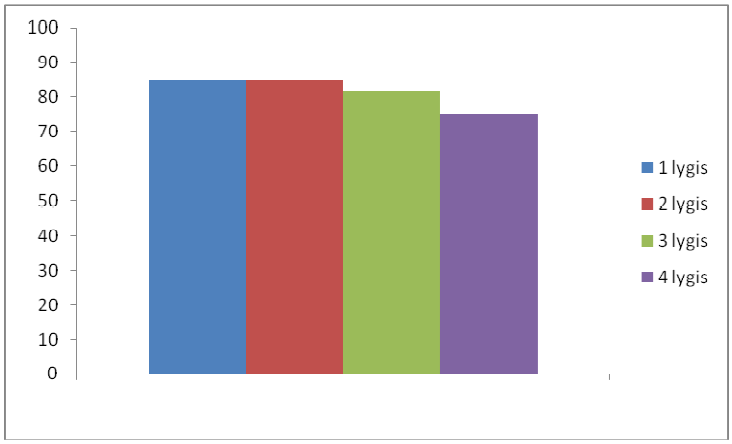
10 lentelė. Trečiojo algoritmo rezultatai

Raiška	Triukšmas	Teisingi, %	Neteisingai atmesti, %	Neteisingai priimti, %
1	1 lygis	100	0	0
	2 lygis	100	0	0
	3 lygis	100	0	0
	4 lygis	100	0	0
2	1 lygis	95	5	0
	2 lygis	95	5	0
	3 lygis	85	15	0

	4 lygis	75	15	10
3	1 lygis	83	17	0
	2 lygis	82	18	0
	3 lygis	70	30	0
	4 lygis	53	35	12
4	1 lygis	60	40	0
	2 lygis	60	40	0
	3 lygis	60	40	0
	4 lygis	40	40	20



53 pav. Trečio algoritmo sėkmingo atpažinimo priklausomybė nuo atvaizdo dydžio. Didesnis skaičius reiškia geresnį rezultatą



54 pav. Trečio algoritmo sėkmingo atpažinimo priklausomybė nuo triukšmo. Didesnis skaičius reiškia geresnį rezultatą

2 priedas. Santrumpų ir terminų žodynas

CCD	Krūvio sąsajos įtaisas (charge-coupled device)
CPU	Procesorius
DB	Duomenų bazė
DSP	Diskretinių signalų procesorius
EEQ	Sutampantis klaidų dažnis (equal error rate)
FAR	Klaidingų priėmimų dažnis (false acceptance rate)
Flash	Atmintinės rūšis
FRR	Klaidingų atmetimų dažnis (false rejection rate)
GOV	Gretimos orientacijos vektorius
I/O	Įvedimas/išvedimas (input/output)
ID	Identifikacija
LED	Šviesą skleidžiantis diodas (light emitting diode)
Minutiae	viena iš esminių piršto atspaudo ypatybių
PIN	Asmeninis identifikacinis numeris (personal identification number)
QVGA	Raiškos režimas (quarter video graphics array)
SAS	Signalų apdorojimo procesorius