KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
INFORMACIJOS IR INFORMACINIŲ TECHNOLOGIJŲ SAUGOS STUDIJŲ PROGRAMA

POVILAS NANEVIČIUS

PIRŠTO KRAUJAGYSLIŲ TINKLO TAIKYMO TIESIOGINIAM SLAPTŲ RAKTŲ GENERAVIMUI GALIMYBIŲ TYRIMAS

Magistro baigiamasis darbas

Darbo vadovas
doc. dr. A. Venčkauskas

KAUNAS, 2013

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
INFORMACIJOS IR INFORMACINIŲ TECHNOLOGIJŲ SAUGOS STUDIJŲ PROGRAMA

POVILAS NANEVIČIUS

PIRŠTO KRAUJAGYSLIŲ TINKLO TAIKYMO TIESIOGINIAM SLAPTŲ RAKTŲ GENERAVIMUI GALIMYBIŲ TYRIMAS

Magistro baigiamasis darbas

Darbo vadovas
doc. dr. A. Venčkauskas

Recenzentas
prof. dr. R. Butleris

KAUNAS, 2013

AUTORIŲ GARANTINIS RAŠTAS
DĖL PATEIKIAMO KŪRINIO

2013 – 05 - 24

Kaunas

Aš, Kauno Technologijos universiteto (toliau – Universitetas), Informatikos fakulteto, Informacijos ir informacinių technologijų saugos studijų programos studentas Povilas Nanevičius, patvirtinu, kad Universitetui pateiktas magistro baigiamasis darbas „Piršto kraujagyslių tinklo taikymo tiesioginiam slaptų raktų generavimui galimybių tyrimas“ (toliau – Kūrinys) pagal Lietuvos Respublikos autorių ir gretutinių teisių įstatymą yra originalus ir užtikrina, kad

1) jį sukūrė ir parašė Kūrinyje įvardyti autoriai;
2) Kūrinys nėra ir nebus įteiktas kitoms institucijoms (universitetams) (tiek lietuvių, tiek užsienio kalba);
3) Kūrinyje nėra teiginių, neatitinkančių tikrovės, ar medžiagos, kuri galėtų pažeisti kito fizinio ar juridinio asmens intelektinės nuosavybės teises, leidėjų bei finansuotojų reikalavimus ir sąlygas;
4) visi Kūrinyje naudojami šaltiniai yra cituojami (su nuoroda į pirminį šaltinį ir autorių);
5) neprieštarauja dėl Kūrinio platinimo visomis oficialiomis sklaidos priemonėmis.
6) atlygins Kauno technologijos universitetui ir tretiesiems asmenims žalą ir nuostolius, atsiradusius dėl pažeidimų, susijusių su aukščiau išvardintų Autorių garantijų nesilaikymu;
7) Autoriai už šiame rašte pateiktos informacijos teisingumą atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

_____ _____

(parašas) (vardas, pavardė)

SANTRAUKA

Biometrinių charakteristikų taikymas sprendžiant įvairias su vartotojų autentifikavimu ir identifikavimu susijusias problemas yra gana plačiai naudojamas praktikoje. Daugelyje komercinių sistemų nuskaitomi biometriniai duomenys yra lyginami su iš anksto išsaugotais šablonais. Biokriptografija ir galimybės generuoti pastovų slaptą raktą iš nepastovių biometrinių charakteristikų yra nauja ir perspektyvi sritis, kurios viena iš pagrindinių problemų – generuojamų raktų nepastovumas dėl natūralių biometrinių duomenų nuskaitymo skirtumų.

Šiame darbe siūlomas biometrinės sistemos, skirtos slaptų raktų generavimui iš piršto kraujagyslių tinklo, nenaudojant palyginimo su iš anksto išsaugotu šablonu, modelis ir tiriamas tokios sistemos veikimas ir galimybės generuoti slaptus raktus. Tokia sistema leistų naudoti vartotojo piršto kraujagyslių atvaizdą nesudėtingiems raktams generuoti be originalaus šablono išsaugojimo ir palyginimo. Darbe tiriamos ir pritaikomos tradicinėse (palyginimo) sistemose naudojamos piršto kraujagyslių tinklo išskyrimo funkcijos ir papildomas, darbe realizuotas raktų generavimo, taikant „Kontūro sekimo iteracijų skaičių“, metodas.

Bandymų metu nustatyta, kad generavimo algoritmams labai svarbus tikslus biometrinių duomenų nuskaitymas ir pradinis apdorojimas. *Miura ir kt.* „Pasikartojančių linijų sekimo“ algoritmu ir morfologinėmis funkcijomis apdorojus piršto kraujagyslių duomenų bazę, kurios dydis – 240 piršto kraujagyslių tinklo atvaizdų, pateiktų 10 skirtingų asmenų, ir taikant darbe siūlomą „Kontūro sekimo iteracijų skaičiaus“ metodą geriausia sistemos nustatyta bendroji klaidos tikimybė (BKT) siekė 15,75 %.

Reikšminiai žodžiai — piršto kraujagyslių tinklas; slaptų raktų generavimas; biometrija; biokriptografija; “Kontūro sekimo iteracijų skaičiaus” metodas.

SUMMARY

Biometric characteristics are widely used when solving multiple user authentication and identification related problems. Most of the commercially available systems employ methods of comparison where user supplied biometric data is compared with the data provided at the time of enrolment. Biocryptography and generation of stable encryption keys from uncertain biometric data is a new and promising area of research where one of the main issues is instability of generated keys due to fluctuation in the biometric data.

This paper proposes and researches a model for secret key generation from biometric data without using comparison with previously enrolled template. Such system would allow generating simple keys without the need to store any templates. Traditional methods for primary feature extraction are researched and a proposed „Contour Trace Iteration Number“ method is developed for key generation.

When performing key generation experiment a strong dependence of proposed method on the quality of primary feature extraction is observed. Miura et al. “Repeated line tracking” method and a custom set of mathematical morphology functions were used for pre-processing of the images in the database holding 240 finger vein images provided by 10 subjects. Best result of *EER* = 15.75% has been observed when short secret keys were generated by the proposed “Contour Trace Iteration Number” method.

Keywords — finger vein; secret key generation; biometrics; biocryptography; “Contour Trace Iteration Number” method.

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

TERMINŲ IR SANTRUMPŲ ŽODYNAS

Autentifikavimas – objekto ar subjekto tapatumo patikrinimas, patvirtinimas
BE – Biometrinis šifravimas (angl BE – Biometric Encription)
BKT – bendroji klaidos tikimybė (angl. ERR – Equal Error Rate)
IBG – Tarptautinė biometrijos tyrimų grupė (angl. International Biometrics Group)
Identifikavimas – objekto ar subjekto išskyrimas iš panašių objektų ar subjektų aibės
IR – infraraudonoji spinduliuotė
KAT – klaidingo atmetimo tikimybė (angl. FRR – False Rejection Rate)
KGV – kraujagyslės galo (pabaigos) vieta
KPT – klaidingo priėmimo tikimybė (angl. FAR – False Acceptance Rate)
KPV – kraujagyslės pradžios vieta
Kraujagyslių atvaizdas – nuskaitytas, bet neapdorotas piršto kraujagyslių atvaizdas
Kraujagyslių tinklas – kraujagyslių atvaizdas apdorotas pirminėmis ir morfologinėmis funkcijomis. Linijų plotis kraujagyslių tinkle yra lygus vienam matricos elementui
KSIM – „Kontūro sekimo iteracijų skaičiaus“ metodas
KSIM – kontūro sekimo iteracijų skaičiaus metodas
KSV – kraujagyslių susikirtimo vieta
LED – šiestukai (angl. Light Emmiting Diode)
Morfologinis apdorojimas – Pirminio apdorojimo rezultato modifikavimas taikant matematinės morfologijos funkcijų aibes
NAS – nesėkmingas atvaizdo skaitymas (angl. FTC – Failure To Capture)
NEK – nesėkmingas etalono kūrimas (angl. FTE – Failure To Enroll)
PIN – asmeninis identifikacinis numeris (angl. Personal Identification Number)
Pirminis apdorojimas – kraujagyslių ribų išskyrimas, dvinarės verčių matricos sudarymas iš nuskaityto kraujagyslių atvaizdo

ĮVADAS

Magistro baigiamajame darbe „Piršto kraujagyslių tinklo taikymo tiesioginiam slaptų raktų generavimui galimybių tyrimas“ siūlomos ir tiriamos slapto pastovaus rakto generavimo galimybės iš piršto kraujagyslių tinklo, nuskaitant laikinai saugomą, iš dalies kintantį piršto kraujagyslių atvaizdą, kuris gali būti pašalinamas iš karto, sugeneravus slaptą raktą.

Nagrinėjama biometrinė savybė – piršto kraujagyslių tinklas – pasirinkta dėl jos saugumo, patogaus naudojimo, unikalumo ir santykinai nesudėtingo nuskaitymo ir apdorojimo.

Siekiant sudaryti slapto rakto generavimo metodą, darbe nagrinėjamos praktikoje naudojamos biometrinio vartotojų identifikavimo/autentifikavimo sistemos, kuriose vartotojo pateiktas piršto kraujagyslių atvaizdas yra apdorojamas ir lyginamas su iš anksto išsaugotu šablonu. Tokios sistemos darbe yra vadinamos palyginimo sistemomis ir nagrinėjami pagrindiniai jų pirminio kraujagyslių atvaizdų apdorojimo ir tinklo sudarymo žingsniai.

Atliekant šį darbą buvo sudaryta bandymų aplinka, skirta pirminio kraujagyslių tinklo apdorojimo metodams ir matematinės morfologijos funkcijų aibėms tirti ir pasirinkti. Iš trijų išbandytų pirminio apdorojimo funkcijų pasirinkta viena, ištirti ir išbandyti šios funkcijos parametrai ir sudaryta tolesniame darbe naudojama matematinės morfologijos funkcijų aibė, skirta kraujagyslių tinklui iš tarpinio kraujagyslių atvaizdo išskirti.

Skirtingai nei daugelyje tradicinių palyginimo sistemų, kuriose kraujagyslių tinklas arba tarpinis kraujagyslių atvaizdas yra lyginamas su iš anksto išsaugotu atvaizdo šablonu arba steganografine kauke, sudaryta registruojant vartotoją, kraujagyslių tinklas yra analizuojamas taikant šiame darbe siūlomą „Kontūro sekimo iteracijų skaičiaus“ metodą ir tarpinis atvaizdas gali būti pašalintas iškart atlikus generavimą. Šio metodo sugeneruotas raktas galėtų būti naudojamas slaptų raktų palyginimui vietoje atvaizdų palyginimo arba, sujungus kelis sugeneruotus atvaizdus į seką, naudojamas kaip biokriptografinis šifravimo raktas. Darbe aprašomas kontūro sekimo metodo įgyvendinimas ir išbandomas jo veikimas.

Bandymo dalyje atliekamas siūlomo metodo tyrimas su 240 piršto kraujagyslių tinklo atvaizdų duomenų baze, kurioje saugomi 10 skirtingų individų dviejų pirštų atvaizdai (po 12 to paties piršto kraujagyslių tinklo atvaizdų), gautų atliekant dvi skenavimų serijas po 6 pirštus su vidutine 67 dienų pertrauka tarp skenavimų. Atliekami bandymai darbe vertinami skaičiuojant „Kontūro sekimo iteracijų skaičiaus metodo“ klaidingo priėmimo (KPT), klaidingo atmetimo (KAT) ir bendrąją klaidos tikimybes (BKT) bei generuojamų raktų entropiją.

Darbo pabaigoje pateikiamos išvados su bandymų įvertinimais ir pasiūlymais tolesniam darbo vystymui ir darbe siūlomo metodo tobulinimui.

Darbas „Piršto kraujagyslių tinklo taikymo tiesioginiam slaptų raktų generavimui galimybių tyrimas“ yra Kauno Technologijos universiteto, Informatikos fakulteto, Informacijos ir informacinių technologijų saugos studijų programos studento Povilo Nanevičiaus magistro baigiamasis darbas.

Darbo problematika ir aktualumas

Biometrinių savybių taikymas kriptografijai yra nauja ir perspektyvi sritis. Viena iš pagrindinių problemų, susijusių su šifravimo raktų kūrimu iš biometrinių duomenų, yra natūralus biometrinių duomenų nepastovumas. Šiame darbe siūlomas metodas, kaip iš piršto kraujagyslių tinklo generuoti pastovius raktus, kurie galėtų būti jungiami į sekas ir taikomi duomenų šifravimui. Taip pat plintant sistemoms, kuriose vartotojas identifikuojamas/autentifikuojamas pagal pateikiamas biometrines savybes, taikant palyginimą, iškyla duomenų saugomo problema: biometriniai duomenys tampa saugotina nuosavybe. Dėl to atsiranda poreikis naudoti atpažinimo metodus, kurie generuoja atšaukiamus, tik vienoje sistemoje galiojančius slaptus raktus, ir nesaugo originalių biometrinių duomenų.

Darbe siūlomo metodo generuojami raktai praktikoje realizuotose sistemose priklausytų nuo vidinio sistemos parametro – verčių priskyrimo generavimo sritims, todėl sistemos generuojami raktai galėtų būti atšaukiami.

Viena iš pagrindinių problemų, susijusių su tiesioginiu slaptų raktų generavimu, yra ribotas galimų raktų ilgis ir unikalumas. Taip pat, lyginant su palyginimo sistemomis, tiesioginio generavimo sistemų veikimą galėtų labiau trikdyti nežymios kraujagyslių tinklo nuskaitymo ir pirminio apdorojimo paklaidos.

Darbo tikslas ir uždaviniai

Darbo tikslas: Pasiūlyti ir ištirti slapto rakto generavimo metodą iš vartotojo piršto kraujagyslių tinklo, nenaudojant palyginimo su iš anksto išsaugotu šablonu.

Darbo uždaviniai:

- Atlikti biometrinių vartotojų autentifikavimo ir šifravimo raktų generavimo metodų, kuriuose taikomas kraujagyslių tinklo nuskaitymas ir palyginimas su iš anksto išsaugotu šablonu, analizę;
- Pasiūlyti naują metodą slaptiems raktams generuoti, kuriame nebūtų taikomos palyginimo ir apytikslio sutapimo funkcijos;
- Sukurti aplinką esamiems ir pasiūlytam kraujagyslių tinklo apdorojimo metodui bandyti;
- Atlikti siūlomo autentifikavimo metodo tyrimą ir skaitinį įvertinimą;
- Pateikti siūlomo metodo tinkamumo tiesiogiai generuoti slaptus raktus iš piršto kraujagyslių tinklo galimybių įvertinimą ir išskirti galimas metodo tobulinimo sritis.

Darbo struktūra

Šis dokumentas sudarytas iš 4 pagrindinių skyrių:

- Biometrinių sistemų ir metodų analizė;
- Tiesioginio slaptų raktų generavimo iš piršto kraujagyslių tinklo metodo sudarymas;
- Tiesioginio slaptų raktų generavimo iš piršto kraujagyslių tinklo metodo bandymai;
- Rezultatų apibendrinimas ir išvados.

Darbo pabaigoje pateikiami darbo priedai.

1. BIOMETRINIŲ SISTEMŲ IR METODŲ ANALIZĖ

Dažnai galutiniai vartotojai prieigos kontrolę ir saugumą informacinių technologijų terpėje yra linkę tapatinti su slaptažodžių naudojimu. Vartotojo identifikavimas vardu ir autentifikavimas slaptažodžiu yra, ko gero, labiausiai paplitęs vartotojo patikros mechanizmas, taip pat sistemos išduoti ar vartotojo sugalvoti raktai yra dažnai naudojami šifravimui. Tačiau dėl slaptažodžių sudėtingumo ir skirtingumo, gausos, jiems keliamų reikalavimų kyla sunkumų juos įsiminti [***1***]. „Bet kas, eidamas per tipinį *Fortune 500* biurą šiandien galėtų žvilgtelti į Jūsų darbo vietą, pagriebti slaptažodį ir jis jau viduje“ *Gigas Hunt* [***2***]. Ši problema suprantama jau ilgą laiką ir tiek privatiems vartotojams, tiek verslui slaptažodžių bėdos yra aktualios. Jos iš dalies sprendžiamos naudojant bendrojo prisijungimo sistemas, skirtingus vartotojų prieigos kontrolės metodus įskaitant ir biometrinę vartotojų patikrą ir kitas priemones.

Šiame darbe nagrinėjamos sistemos, kuriose naudojami biometriniai duomenys vartotojų atpažinimui ar slaptų raktų generavimui. Tokie metodai kaip vartotojų autentifikavimas pagal jų piršto atspaudą yra gan įprasti ir dažnai naudojami asmeniniuose kompiuteriuose ir kitur. Darbe plačiau nagrinėjamos sistemos, kuriose taikomas piršto kraujagyslių tinklo skenavimas. Piršto ar delno kraujagyslių atvaizdų skenavimas yra vienas iš naujausių, bet jau plačiai naudojamų vartotojų patikros metodų. Įprastai, kaip ir daugelio kitokius biometrinius duomenis naudojančių sistemų atveju, vartotojo pateiktas kraujagyslių tinklo žemėlapis yra lyginamas su iš anksto sudarytu ir išsaugotu atvaizdu, tačiau šiame darbe domimasi tiesiogine slapto pastovaus rakto generavimo galimybė iš pastovios charakteristikos – piršto kraujagyslių tinklo žemėlapio. Taip pat siekiama įvertinti, kur tokia technologija galėtų būti taikoma ir kuo būtų pranašesnė už esamas sistemas. Darbe tiriama, ar ir kokio ilgio slaptus raktus galėtų pakeisti piršto kraujagyslių atvaizdai pagrįsti metodai, aptariama slaptojo šifravimo rakto generavimo iš biometrinių duomenų problema.

1.1. Vartotojo autentifikavimas

Autentifikavimas – tai objekto ar subjekto tapatumo patikrinimas, patvirtinimas. Dažniausiai vartotojams autentifikuoti naudojamas vardas (identifikatorius) ir slaptažodis. Taip pat taikomi kiti autentifikavimo metodai: magnetinės kortelės, biometriniai duomenys, kriptografiniai metodai ir kiti [***3***].

Literatūroje išskiriami trys autentifikavimo tipai: „žmogus - kompiuteris“, „kompiuteris-kompiuteris“ ir žmogus – žmogus [***3***].

Vartotojo identifikavimo ir autentifikavimo metodai skirstomi į tris grupes [***3***]:

- Kažkas, ką žinai – slaptažodis, asmens identifikacinis numeris (PIN) ir pan.
- Kažkas, ką turi – skaitmeninis sertifikatas, lustinė kortelė, raktas ir pan.
- Kažkas, kuo esi – individualios savybės (biometrinės charakteristikos)

Dažnai vartotojams autentifikuoti naudojamos dvi iš trijų autentifikavimo grupių, pavyzdžiui norint prisijungti prie vidinio įmonės tinklo gali reikėti *žinoti* slaptažodį ir pateikti *turimo* kodų generatoriaus slaptažodį. Norint iš bankomato gauti pinigų reikia *turėti* banko kortelę ir įvesti slaptą PIN kodą.

Šiame darbe iš dalies nagrinėjamos kai kurios tipų „žmogus-kompiuteris“ ir „žmogus - žmogus“ autentifikavimo problemos ir galimybės šias problemas spręsti naudojantis individualiomis biometrinėmis subjektų savybėmis. Darbe iš dalies vertinama, kokio ilgio raktus būtų galima generuoti iš piršto kraujagyslių tinklo tiesiogiai. Jei raktai neilgi – jie galėtų būti naudojami PIN kodo lygio slaptiems raktams pakeisti arba greitesnei vartotojų identifikacijai lyginant su 1:n atvaizdų palyginimu duomenų bazėse atlikti. Jei iš kraujagyslių tinklo būtų galima patikimai generuoti ilgus slaptus raktus – tokie raktai galėtų būti naudojami kaip šifravimo raktai ir galbūt galėtų būti taikomi pakeisti šifravimo raktams, įprastai saugomiems lustinėje kortelėje ar kitose laikmenose.

1.2. Biokriptografijos metodų apžvalga

Aukščiau aptartais vartotojų autentifikavimo metodais iš dalies remiasi ir kita informacijos saugumui svarbi sritis – šifravimas. Kai kuriose sistemose pagal vartotojo įvestą slaptažodį arba jo santraukos funkciją yra generuojami blokinio šifravimo raktai ar viešojo ir privačiojo rakto infrastruktūros (*PKI*) raktai. Tokiose sistemose gali būti naudojami papildomi pseudo-atsitiktinių skaičių generatoriai arba atsitiktinių verčių generavimas iš vartotojo elgsenos (pvz. klavišų paspaudimo, kompiuterio pelės judesių ir kt.). Taip kuriami unikalūs raktai tapatinami su raktą sugeneravusiu vartotoju.

Biometrinės savybės iš esmės yra unikalios. Pirštų antspaudai, akies rainelės požymiai, piršto kraujagyslių tinklas skiriasi net lyginant du identiškus dvynius [***4***]. Iš biometrinių charakteristikų turėtų būti įmanoma sugeneruoti pastovios vertės (aš == *aš'*) unikalius raktus tinkančius tiek autentifikavimui, tiek šifravimui. Daugelyje tradicinių biometrinių slaptų raktų išdavimo arba biometrinio identifikavimo/autentifikavimo sistemų taikomi atvaizdų palyginimo metodai. Tokiose sistemose pakanka apytikslio sutapimo tam, kad vartotojas būtų atpažintas. Tačiau šifravimui būtinas visiškas rakto atitikimas. Dėl natūralaus biometrinių savybių nepastovumo tokių raktų generavimas yra sudėtingas. Galimybės generuoti slaptus raktus, tinkamus šifravimui buvo tiriamos keliuose ankstesniuose darbuose.

Ushmaev ir kt. [***5***] siūlomas slaptų raktų generavimo metodas siūlo remtos piršto antspaudų topologija slaptiems raktams generuoti. Piršto antspaudų topologija yra labai pastovi biometrinė charakteristika, o metodas leidžia pasirinkti skirtingus šifravimo raktų ilgius.

Costanzo [***6***] metode demonstruojama, kaip slaptas raktas galėtų būti generuojamas iš biometrinių savybių taikant išskirtų savybių parametrizavimą. Šio metodo veikimui nereikalingas joks iš anksto išsaugotas etaloninis biometrinis atvaizdas. Nuskaitytos biometrinės savybes *Costanzo* metode grupuojamos pagal numatytas taisykles į sekas, kurios sudaro bendrą biokriptografinį šifravimo raktą.

Zheng ir kt. [***7***] autorių siūlomas slapto kriptografinio rakto generavimo metodas pagrįstas struktūrų parametrizavimu leidžia generuoti didelės entropijos slaptus raktus ir yra saugus, nes iš sistemoje saugomų duomenų negalima atkurti jokių originalios biometrinės savybės parametrų.

Wu ir kt. [***8***] pristato biometrinę kriptografinę sistemą, kurioje iš dalinai apdoroto akies ragenos atvaizdo generuojamas slaptas raktas taikant 2-D *Gabor* filtrus ir modifikuotas *Fuzzy Vault* algoritmas naudojamas duomenų šifravimui.

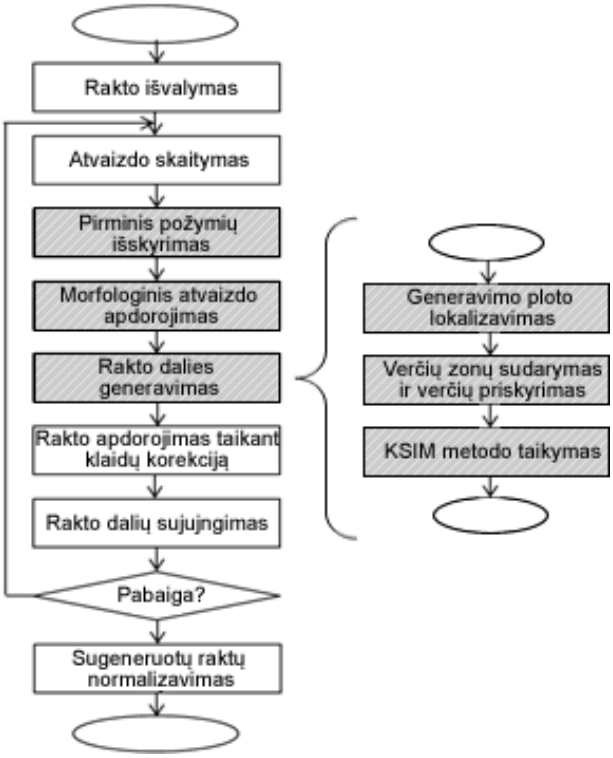
Sistemos, kuriose taikoma tik viena biometrinė charakteristika slapto rakto generavimui yra labiau priklausomos nuo tikslaus šios charakteristikos nuskaitymo. Dažnai tokiose sistemose generuojami raktai pasižymi didesnėmis klaidų tikimybėmis, nepakankamu ilgiu arba entropija. *Jagadeesan ir kt.* [***9***] pasiūlė efektyvų rakto generavimo metodą, paremtą keliomis biometrinėmis savybėmis (piršto antspaudais ir akies rainele). Šiame metode saugumas papildomai didinamas taikant didelių pirminių skaičių skaidymo dauginamaisiais problemas. Siūlomame metode piršto antspaudų ir akies rainelės išskiriamos ir sujungiamos tarpusavyje. Taip sudaroma bendra biometrinė kaukė, kuri vėliau naudojama 256 bitų šifravimo raktui gauti.

Šio skyriaus apžvalgoje dominuoja piršto antspaudais pagrįstos sistemos. Darbe siūlomas metodas generuojantis slaptus raktus iš kraujagyslių tinklo atvaizdų. Apibendrinta tiesioginio slapto rakto generavimo iš piršto kraujagyslių tinklo blokinė schema pateikiama 1.2.1 pav. Šioje schemoje numatoma, kad slaptas raktas gali būti generuojamas iš piršto ar pirštų kraujagyslių atvaizdų sekų, o ne iš vienintelio atvaizdo. Magistrinio darbo kontekste realizuotos tik tamsesne spalva pažymėtos metodo dalys.

Pagrindiniai kodo generavimo žingsniai, realizuoti šiame darbe ir išbandomi bandymų dalyje yra:

- Pirminis požymių išskyrimas, pavyzdžiui taikant *Miura ir kt.* „Pasikartojančių linijų sekimo“ metodą
- Morfologinių funkcijų aibės taikymas siekiant išvalyti, pataisyti ir susiaurinti atvaizdą iki vieno pikselio pločio tinklo

- Rakto generavimas – generavimo ploto papildomas lokalizavimas, verčių zonų sudarymas ir verčių priskyrimas, kodo generavimas taikant „Kontūro sekimo iteracijų skaičiaus“ metodą



1.2.1 pav. Slaptų raktų generavimo iš piršto kraujagyslių metodo blokinė schema [*10*]

Siekiant generuoti šifravimui tinkamus raktus, vertės gautos iš nuskaitytų biometrinių savybių galėtų būti kombinuojamos tarpusavyje. Jei Tiesiogiai iš vieno piršto generuojami raktai yra trumpi, būtų galima taikyti kelis nuskaitymus iš eilės ir kombinuoti jų rezultatus.

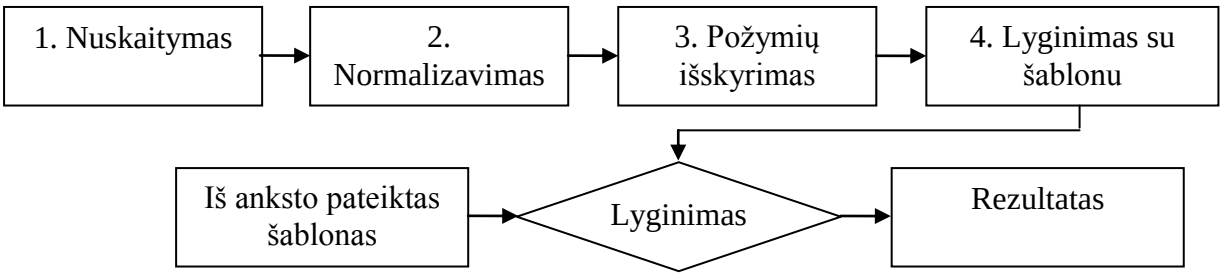
1.3. Biometrinių sistemų apžvalga

1.3.1. Biometrinių sistemų tipai

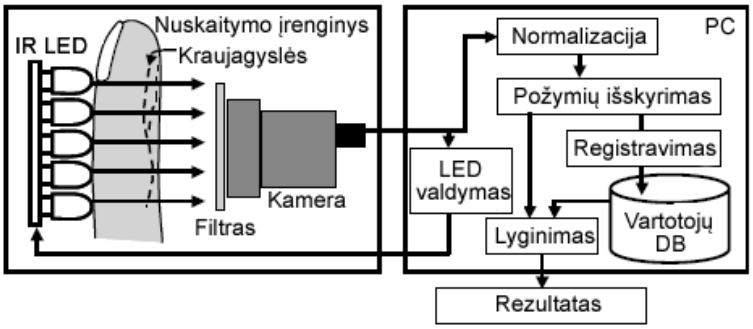
Sistemos, kurios patvirtina vartotojos tapatybę remiantis jo pateiktais biometriniais duomenimis iš esmės naudojasi vaizdų apdorojimo ir lyginimo arba analizavimo-parametrizavimo metodais. Tokias sistemas galima būtų suskirstyti į tris rūšis:

Sistemos, kuriose nuskaitytas biometrinis atvaizdas yra lyginamas su duomenų bazėje (arba kitokioje laikmenoje) išsaugotu šablonu (1.3.1.1 pav.). Šios sistemos labiausiai paplitusios, populiarios ir patikimos. Kai kuriose valstybėse autentifikavimas pagal vartotojo piršto kraujagyslių tinklą yra naudojamas bankomatuose, praėjimo kontrolės sistemose ir kitur. Pirštų antspaudų skaitytuvai supaprastina vartotojų prisijungimą prie asmeninių kompiuterių, taip pat yra naudojami praėjimo, duomenų šifravimo sistemose ir kitur. Šios sistemos dažniausiai yra tik tarpininkės ir jų tikslas – nustačius, kad pateikti biometriniai duomenys atitinka pateiktą šabloną, suteikti vartotojui iš anksto nustatytą pastovios vertės raktą. Tokias sistemas galima vadinti raktų išdavimo, naudojantis biometriniais duomenimis sistemomis. Kol kas šios sistemos yra vienos iš populiariausių ir patikimiausių, tačiau pagrindinis jų trūkumas yra tai, kad turi būti nuskaitytas ir duomenų bazėje saugomas vartotojo biometrinių duomenų šablonas. Pagrindiniai tokio tipo sistemos trūkumai [***11***]:

- Rakto patikimumas iš esmės priklauso nuo duomenų bazės apsaugos lygio
- Saugoma tikra biometrinė charakteristika, kurią galima vėliau atkurti ir padirbti
- Atliekamas 1:n atvaizdų palyginimas didelėse duomenų bazėse užtrunka ilgai, indeksavimas yra sudėtingas
- Autentifikuojant serveryje reikalingas neapsaugotos biometrinės charakteristikos perdavimas tinklu
- Biometriniai duomenys negali būti „atšukti“



1.3.1.1 pav. Palyginimo su išsaugotu šablonu sistemos blokinė schema 1

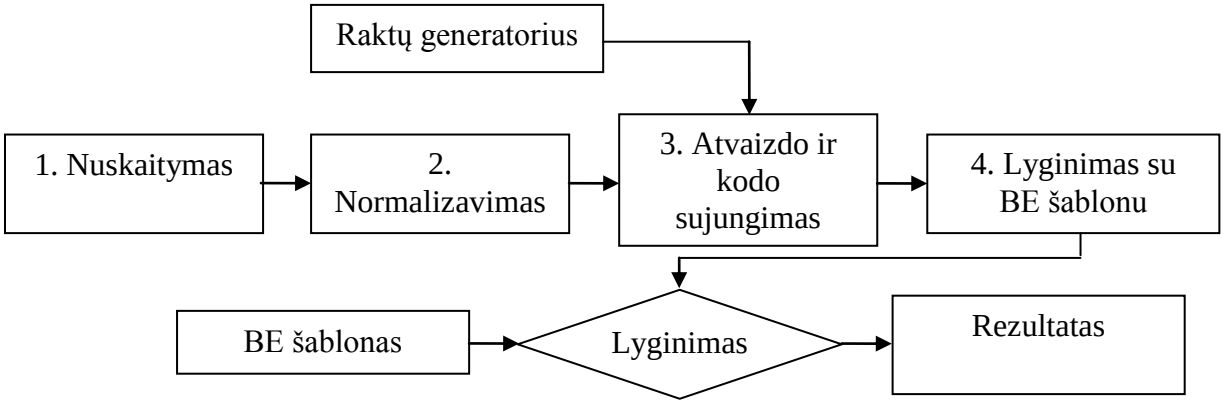


1.3.1.2 pav. Palyginimo su išsaugotu šablonu sistemos blokinė schema 2

Dalį aukščiau aprašytų sistemų trūkumų sprendžiama naudojant slaptojo šifravimo rakto surišimą su biometriniais duomenimis naudojant tarpinį šabloną (1.3.1.3 pav.). Tai vadinama biometriniu šifravimu. Iš tokiose sistemose saugomų šablonų neįmanoma išgauti nei slaptojo rakto, nei biometrinių duomenų atvaizdo. Įvedant vartotojo duomenis į sistemą generuojamas naujas raktas, taigi vartotojui ne tik nereikia jo atsiminti, tačiau net nereikia jo žinoti. Labai gerai tai, kad raktas niekaip nėra susijęs su biometriniais duomenimis, todėl jį galima keisti. Jo praradimas nenutekina informacijos apie slaptas vartotojo biometrines savybes. Sukūrus vartotojo asmeninį šabloną, kuriame saugomas slaptas raktas ir biometriniai duomenys, originalus biometrinis šablonas ir sugeneruotas raktas daugiau nebereikalingi ir gali būti sunaikinti. Asmeninis šablonas gali būti saugomas tiek duomenų bazėje, tiek nešiojamose laikmenose ar skaitytuvuose [***11***].

Trūkumai, naudojant sistemas, kuriose biometrinis raktas generuojamas iš tarpinio šablono:

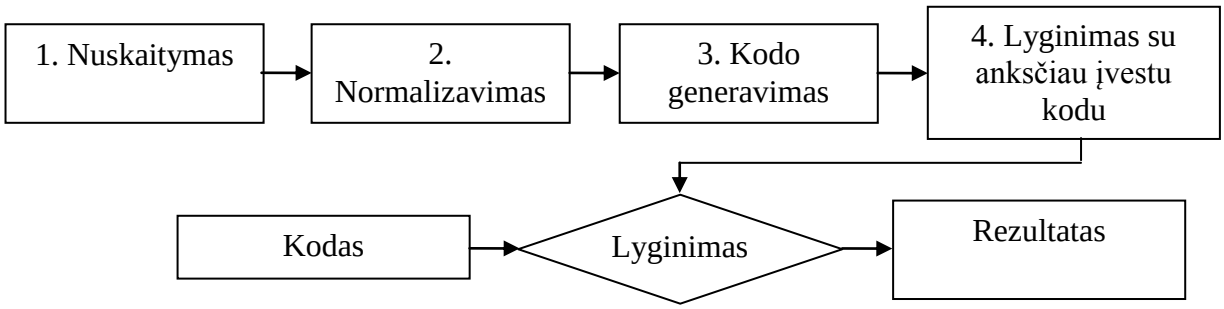
- Kai duomenys saugomi duomenų bazėse reikia atlikti 1:n palyginimą, kuris gali trukti ilgai
- Būtina žinoti algoritmų, sumaišančių sugeneruoto rakto ir biometrinio atvaizdo vertes patikimumą
- Didesnė klaidingo atmetimo (*KAT*) tikimybė, nei naudojant kai kurias lyginimo sistemas



1.3.1.3 pav. Palyginimo su BE šablonu sistemos veikimo blokinė schema

Biometrinės charakteristikos saugo daug informacijos. Pavyzdžiui 300x400 paveikslas, kurio kiekvienas pikselis saugo vieną bitą (galima būtų saugoti ir daugiau) jau gali saugoti 120000 bitų informacijos. Žinoma, pats biometrinės charakteristikos atvaizdas dažnai neturės tiek daug unikalių požymių, tačiau atsižvelgiant į biometrinių duomenų tipus ir sudėtingumą galima tikėtis išgauti reikšmingų ir unikalių duomenų, tinkančių unikaliam slaptam rakto generuoti. Neįvertinant triukšmų ir informacijos netekimo dėl aparatūrinių ribojimų, nuskaitymo sudėtingumo, vaizdo apdorojimo algoritmų ribotumo bei klaidų, galima tikėtis generuoti gana ilgus (pvz. 128 bitų) kriptografinius raktus.

Tiesioginis trumpų *PIN* ar ilgų šifravimo raktų generavimas iš biometrinių savybių yra sudėtingas dėl pradinio biometrinių duomenų nepastovumo, kuris mažiau įtakoja atvaizdų palyginimo ar *BE* kaukes sudarančių sistemų metodus. Sistemos, tiesiogiai generuojančios raktus iš biometrinių savybių pavyzdys pateiktas 1.3.1.4 pav.



1.3.1.4 pav. Sistemos su tiesioginu rakto generavimu veikimo blokinė schema

Literatūroje aptariamose tiesioginio rakto generavimo sistemose iš žmogaus veido formos pasiekiamos gana žemos *KAT* (tarp 0,02% ir 0,046%) ir *KPT* (tarp 0,026% ir 0,077%) tikimybės [***12***], tačiau detalios informacijos apie sistemas, galinčias patikimai generuoti slaptus raktus iš biometrinių savybių nepavyko surasti. Generuoti pastovius raktus tiesiogiai be jokių palyginimo funkcijų gali būti sudėtinga ir gali nepavykti gauti ilgų raktų naudojamų šifravimui dėl natūralaus biometrinių charakteristikų nepastovumo. Tokios sistemos (kol kas) negalėtų pakeisti esamų, tačiau iš esmės keičia metodą, kaip generuojami raktai. Joms nereikėtų duomenų bazių šablonų ar tarpinių šablonų saugojimui, raktų generatorių. Sistemos būtų greitos, nes nereikėtų atlikti jokių atvaizdų lyginimo ar surišimo operacijų. Galbūt tokias sistemas pavyktų pritaikyti ten, kur nėra reikalingas labai aukštas saugumo lygis – pavyzdžiui vietoje *PIN* kodo.

Tiesioginės sistemos turėtų neigiamų aspektų. Taip pat, kaip šablonus saugančios sistemos, negalėtų lengvai užblokuoti vartotojo, jei jo biometrinės charakteristikos padirbamos. Norint pakeisti vartotojo autentifikavimo duomenis reikėtų keisti vaizdų atpažinimo algoritmą arba į jo mechanizmą įdėti papildomų atsitiktinių verčių generavimo galimybę. Sistemose tikėtinas didesnis klaidino priėmimo (*KPT*) parametras. Generuojant ilgesnius raktus tikėtinos paklaidos, dėl įvesties duomenų skirtumų, todėl tikėtinas didesnis klaidingo atmetimo koeficientas (*KAT*).

1.3.2. Biometrinių savybių apžvalga ir kokybinis palyginimas

Vartotojo autentifikavimui praktikoje dažniausiai naudojamos biometrinės savybės (fizinės ir elgesio) yra pirštų atspaudai, rašymo greičio ir paspaudimo stiprumo įvertinimas, veido bruožų atpažinimas, rankos forma, akies rainelės skaitymas ir kiti metodai. Pagrindiniai kokybiniai kriterijai pagal kuriuos gali būti vertinamas vartotojų autentifikavimo ir identifikavimo metodų, patogumas naudoti yra:

- Nesudėtingas pateikimas
- Galimai nemalonių pojūčių nebuvimas autentifikuojant
- Autentifikavimo greitis
- Savybės pastovumas
- Žema klaidingo atmetimo tikimybė

Autentifikavimo ir identifikavimo metodų saugos kokybiniai vertinimo metodai galėtų būti:

- Duomenų vagystės sudėtingumas
- Padirbimo sudėtingumas
- Žemas klaidingo priėmimo tikimybė

Pirštų atspaudai – tiek kompiuterijoje, tiek kriminologijoje yra viena iš dažniausiai praktikoje taikomų biometrinių žmogaus savybių. Jų pritaikymas nėra patogus ten, kur reikalingas didelis saugumas ir identifikavimo ar autentifikavimo greitis, tačiau gana aukštas saugumo ir unikalumo lygis leidžia naudoti piršto antspaudus tiek praėjimo kontrolei, tiek elektroninių sistemų slaptažodžiams visiškai ar iš dalies pakeisti ir kitiems pritaikymams. Viena iš piršto antspaudų problemų yra tai, kad juos sąlyginai lengva padirbti, galima atkurti nuo paliestų paviršių. Daugelyje piršto antspaudus vartotojų autentifikavimui naudojančių sistemų nėra tikrinama ar pirštą patiekia žmogus, ar pavyzdžiui vietoje tikro piršto yra naudojamas silikoninis piršto lipdinys. Kita savybė, sunkinanti piršto antspaudų pritaikymą yra nuskaitymo nepatogumai. Pavyzdžiui kai kurie skaitytuvai gali neteisingai nuskaityti drėgnus arba išteptus pirštus.

Piršto kraujagyslių tinklas – po oda esančių kraujagyslių tinklo atvaizdas. Piršto kraujagyslės yra saugesnė biometrinė savybė, nes jos nematomos, jomis galima pasinaudoti tik tol, kol pirštu teka kraujas. Piršto kraujagyslių tinklui sudaryti mažiau įtakos turi aplinkos veiksniai tokie kaip drėgme, purvas, net ant piršto paviršiaus esantis kraujas gali nesutrukdyti kraujagyslių tinklo išskyrimui. Piršto kraujagyslių tinklas nekinta žmogui senstant, be to, skirtingai nei piršto antspaudų skaitymas, kraujagyslių tinklo išskyrimas gali būti bekontaktis. Vienas iš neigiamų aspektų, susijusių su piršto kraujagyslių ar delno kraujagyslių nuskaitymu yra tai, kad kraujagyslių atvaizdas iš esmės yra trimatis, todėl didesnė svarbą įgyja piršto ar delno padėties ir jo pasukimo normalizacija.

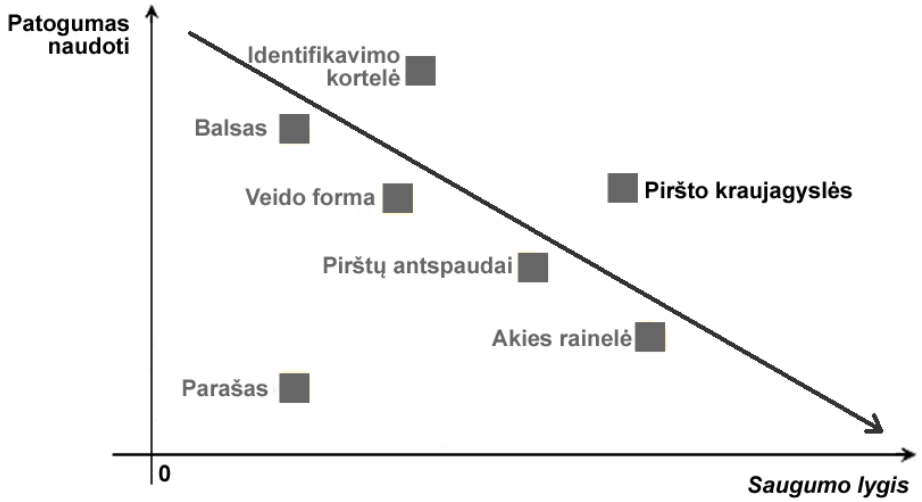
Rankos geometrija – priešingai nei pirštų atspaudai ar kraujagyslių tinklas, rankos geometrija nėra unikali [***3***], tačiau pritaikoma ten, kur nereikalingas labai aukštas saugumo lygis pvz. darbo laiko apskaitos sistemos.

Akies rainelė – labai saugi ir unikali charakteristika, tačiau jos gavimui reikia akį apšviesti intensyvia šviesa. Tai kartais nėra priimtina. Taip pat akies rainelės pritaikymą riboja tai, kad tiksliai lokalizuoti akį prieš skaitytuvą yra gana sudėtinga ir užtrunka sąlyginai ilgai.

Veido bruožai – viena iš labiausiai nepastovių biometrinių charakteristikų. Ji patogi ten, kur reikia apytiksliai įvertinti žmogaus buvimo vietą ar tapatybę (pvz. kur masiniame renginyje šiuo metu yra asmuo užfiksuotas įėjimo vaizdo kameros?), bet dėl veido išraiškų kaitos, tai daugiausiai paklaidų skenavimo metu duodanti savybė. Šis metodas taip pat gali būti apeitas naudojant kaukes ar net spausdintas veido nuotraukas.

Balsas – čia praktikoje išskiriamos kelios problemos: pastovios frazės, kurią galima lengvai perimti, atpažinimas ar kintamų frazių atpažinimas, kuriam reikalingas ilgesnis autentifikavimo laikas. Tai ribotai pritaikoma biometrinė charakteristika.

Biometrinių charakteristikų kokybinio metodų palyginimo grafikas pateiktas 1.3.2.1 paveiksle.



1.3.2.1 pav. Biometrinių savybių kokybinio palyginimo grafikas [*13*]

Svarbi biometrinių duomenų taikymo praktinėse sistemose savybė yra sukaitytos biometrinės informacijos kiekis. Tai turi įtakos sistemų greitaveikai, ypač kai yra biometrinės savybės yra naudojamos 1:n vartotojų identifikavimui. Kadangi piršto kraujagyslių tinklo kaukės dažnai užima daugiau vietos lyginant su piršto antspaudais arba akies rainelės duomenimis, ši biometrinė savybė galėtų būti mažiau patraukli 1:n vartotojų identifikavimui didelėse biometrinėse duomenų bazėse. Tačiau naudojant tiesioginį slaptų raktų generavimo metodą, aptariamą šiame darbe palyginimas galėtų būti atliekamas tarp iš piršto kraujagyslės sugeneruoto slapto rakto ir duomenų bazės. Toks palyginimas būtu kur kas greitesnis.

Lentelėje 1.3.2.1 lyginamos biometrinės savybės pagal skyriuje aptartus kokybinius kriterijus.

1.3.1 lentelė. Biometrinių savybių kokybinio palyginimo lentelė [*14*], [*15*]

Biometrinė savybė	Saugumas		Patogumas		
	Apsauga nuo padirbimo	Unikalumas	Nuskaitymo greitis	Tvarumas	Dydis
Piršto kraujagyslių atvaizdas	aukšta	aukštas	aukštas	aukštas	vidutinis
Veido kontūras ir savybės	vidutinė	žemas	vidutinis	aukštas	mažas
Akies rainelės savybės	vidutinė	aukštas	vidutinis	žemas	mažas
Balso tembras ir dažnis	žema	žemas	vidutinis	aukštas	vidutinis
Piršto antspaudų atvaizdas	vidutinė	vidutinis	vidutinis	žemas	didelis

Dėl aukšto saugumo, unikalumo ir patogumo piršto kraujagyslių tinklas taikomas kai kuriuose bankinėse sistemose, bankomatuose. Japonijoje 75% visų bankų skyrių piršto kraujagyslių tinklas gali būti naudojamas kaip vienas iš kliento autentifikavimo metodų [***14***].

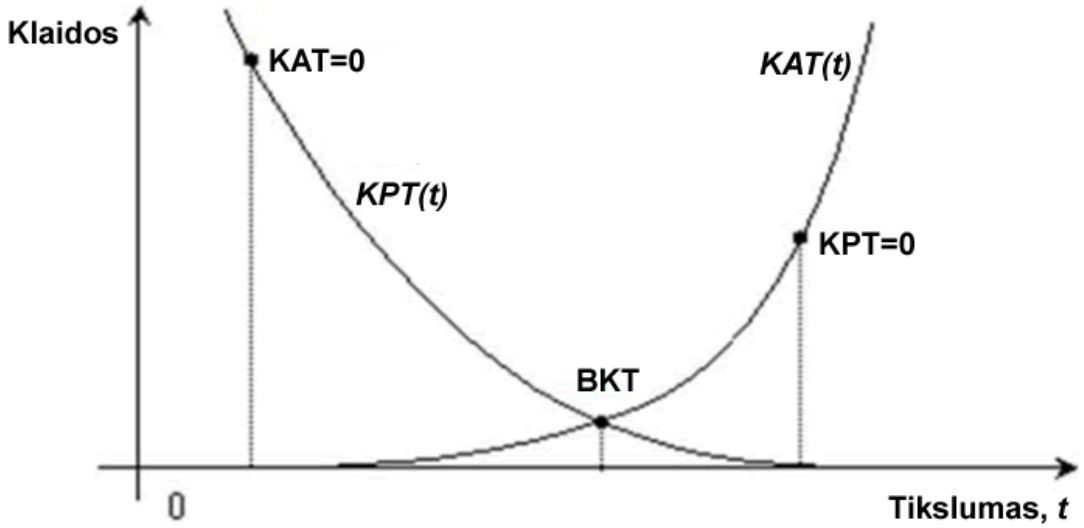
1.3.3. Kiekybiniai biometrinių sistemų vertinimo kriterijai

Biometrinėms sistemoms apibūdinti dažniausiai naudojamos tokios kiekybinės charakteristikos:

- *KAT*: klaidingo atmetimo tikimybė (angl. False Rejection Rate (*FRR*)). Tai tikimybė, kad sistema klaidingai neautentifikuos vartotojo. Šis parametras kartais taip pat vadinamas *FNMR* (angl. False Non-Match Rate) [***16***]. Dažniausiai vartotojas klaidingai atmetamas dėl biometrinių savybių nuskaitymo metu atsiradusių paklaidų. Taip pat klaidingo atmetimo priežastis gali būti atsitiktiniu principu veikiančių pirminių kraujagyslių tinklo išskyrimo algoritmų paklaidos arba netinkamas palyginimo/generavimo metodų taikymas. *KAT* skaičiuojama pagal teisingų vartotojų atmetimo skaičių visoje vartotojo pateiktoje vienodų biometrinių duomenų aibėje.
- *KPT*: klaidingo priėmimo tikimybė (angl. False Acceptance Rate (*FAR*)). Tikimybė, kad vartotojų pateikiami biometriniai duomenys sutaps ir klaidingas vartotojas bus autentifikuotas. Šios savybės priežastis yra atpažinimo algoritmuose numatytos priimtinos paklaidos dėl nuskaitymo netikslumo, per mažos raiškos biometrinių charakteristikų atvaizdai ir kitos. Šis parametras kai kurioje literatūroje yra vadinamas *FMR* (angl. False Match Rate) [***16***]. *KPT* skaičiuojama tikrinant ar yra biometrinių duomenų, kurie būtų supainioti su kito vartotojo biometriniais duomenimis visoje biometrinių duomenų aibėje.
- *BKT*: bendroji klaidos tikimybė (angl. Equal Error Rate (*ERR*)). Tai *KAT* ir *KPT* sankirtoje esanti vertė. *BKT* yra skaičiuojama pagal 1.1 formulę. Dėl *KAT* ir *KPT* kreivių specifikos, mažiausias *BKT* sistemoje gaunamas *KAT* ir *KPT* kreivių sankirtoje (1.3.3.1 pav.).

$$BKT = |KPT + KAT| \qquad \textbf{(1.3.1)}$$

KAT mažėja didinant biometrinių duomenų nuskaitymo raišką, naudojamų algoritmų tikslumą, suabstraktinant kai kurias biometrines savybes. Tai dažniausiai padidina biometrinių savybių išskyrimo ir įvertinimo laiką ir reikalauja papildomų resursų. Taip pat tikslumo didinimas gali nulemti *KAT* didėjimą dėl papildomai išskirtų parametrų arba per didelio biometrinių savybių suabstraktinimo.



1.3.3.1 pav. Kiekybiniai biometrinių sistemų vertinimo parametrai

Be jau aptartų savybių biometrines sistemas galima vertinti pagal papildomus parametrus, tokius kaip nesėkmingas etalono kūrimas (*NEK*), angl. Failure To Enroll (*FTR*), nesėkmingas atvaizdo skaitymas (*NAS*), angl. Failure To Capture (*FTC*) ir kitus parametrus [***17***].

1.3.4. Kiekybinis skirtingų komercinių biometrinių sistemų palyginimas

Biometrinių metodų tikslumas yra svarbi tiek saugumo, tiek patogumo naudotis biometrine sistema prasme. Ideali biometrinė sistema retai atmes tikrąjį vartotoją (žema *KAT*) ir labai retai priims neregistruotą vartotoją arba klaidingai išskirs vartotoją iš vartotojų aibės (žema *KPT*).

Nepriklausomas Tarptautinės biometrijos tyrimų grupės (angl. The International Biometrics Group (*IBG*)) biometrinių sistemų palyginimas pagal skirtingus kiekybinius vertinimo kriterijus pateiktas 1.3.4.1 lentelėje [***14***].

1.3.2 lentelė. Kiekybinis biometrinių metodų palyginimas (*IBG*) [*14*], [*18*]

	Piršto kraujagyslės	**Delno kraujagyslės**	**Akies rainelė**	**Piršto antspaudai**	
Gamijntojas	Hitachi-Omron	Fujitsu	IrisGuard	Precise Biometrics	Bioscript
Įrenginys	UBReader	PalmSecure	H100	Precise100 MC	Lifeview
Nesėkmingas etalono kūrimas (NEK)	0,55%	1.63%	7.01%	3.73%	0.00%
Klaidingo atmetimo tikimybė (KAT)	1,26%	4,23%	1,76%	6,47%	1,67%
Klaidingo priėmimo tikimybė (KPT)	0,01%	0,0118%	0,01%	5,86%	1,46%
Įrenginio tikslumo nustatymas	*FMR* 0,01%	Pagal nutylėjimą	*FMR* 0,01%	*FMR*: Mid *FRR*: Low	*FMR*: Mid *FRR*: Low

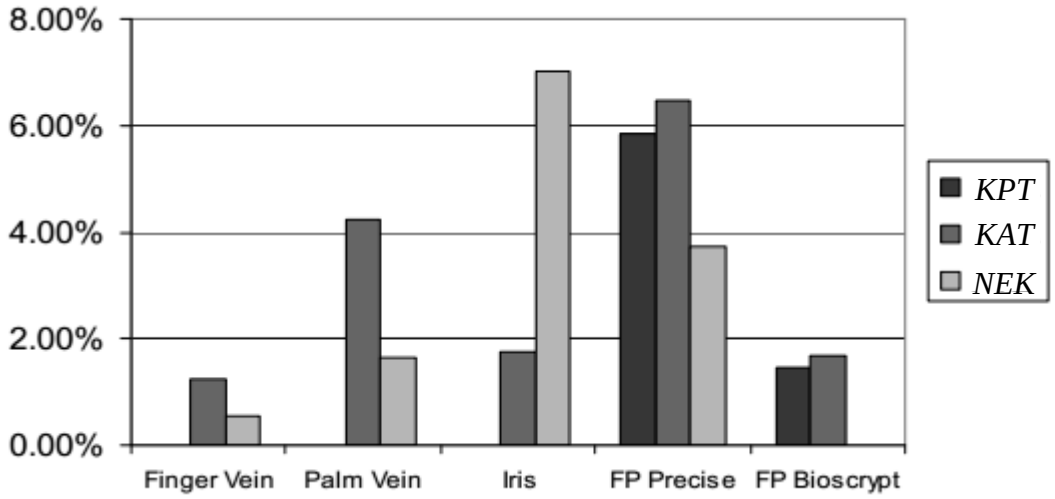
Lentelėje 1.2 pateikiami testai atlikti skirtingu laiku. Palyginimui naudotų biometrinių duomenų bazių dydžiai [***14***], [***18***]:

- Piršto kraujagyslės: *KAT* testavimui *N=111341*, kur *N* yra tikrų vartotojų palyginimų skaičius, *KPT* testavimui *N'=14368975*, kur *N'* yra apsimestinių bandymų prisijungti skaičius.
- Delno kraujagyslės: *KAT* testavimui *N=111341*, kur *N* yra tikrų vartotojų palyginimų skaičius, *KPT* testavimui *N'=14368975*, kur *N'* yra apsimestinių bandymų prisijungti skaičius.
- Akies rainelė: *KAT* testavimui *N=111341*, kur *N* yra tikrų vartotojų palyginimų skaičius, *KPT* testavimui *N'=14368975*, kur *N'* yra apsimestinių bandymų prisijungti skaičius.

- Piršto antspaudai (Precise Biometrics įrenginys): *KAT* testavimui *N=232*, kur *N* yra tikrų vartotojų palyginimų skaičius, *KPT* testavimui *N'=480*, kur *N'* yra apsimestinių bandymų prisijungti skaičius.
- Piršto antspaudai (Bioscript įenginys): *KAT* testavimui *N=239*, kur *N* yra tikrų vartotojų palyginimų skaičius, *KPT* testavimui *N'=478*, kur *N'* yra apsimestinių bandymų prisijungti skaičius.

Grafinis Tarptautinės biometrijos tyrimų grupės bandymų rezultatas pavaizduotas 1.3.4.1 paveiksle.

Pagal N. *Miura, A. Nagasaka ir T. Miyatake* atliktu bandymus su 678 individų duomenų baze taikant Pasikarto linijų sekimo pirminio kraujagyslių atvaizdo išskyrimo metodą gauta *BKT* 0,0145%. Anot šio šaltinio, *BKT* piršto antspaudus naudojančiose sistemose svyruoja tarp 0,2% ir 4% [***19***].



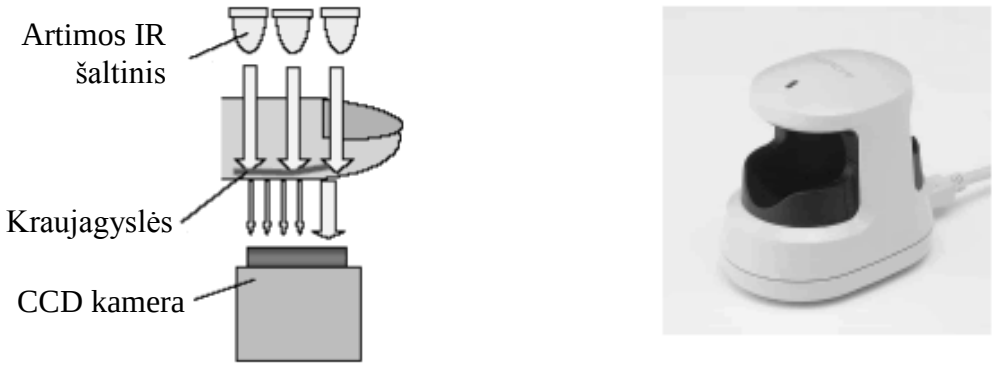
1.3.4.1 pav. *KPT, KAT, NEK* skirtingas savybes naudojančiose sistemose (*IBG*) [*14*]

1.3.5. Piršto kraujagyslių atvaizdų nuskaitymo principai ir aparatinė įranga

Piršto kraujagyslių atvaizdas yra nuskaitomas padedant pirštą tarp (šalia) infraraudonųjų spindulių šaltinio (skirtingose sistemose naudojamas bangos ilgis svyruoja tarp 750 iki 950 nm) ir kameros, fiksuojančios vaizdą. Kraujyje esantis hemoglobinas sugeria infraraudonąją spinduliuotę, todėl atvaizde kraujagyslės atrodo kaip tamsesnės linijos [***20***].

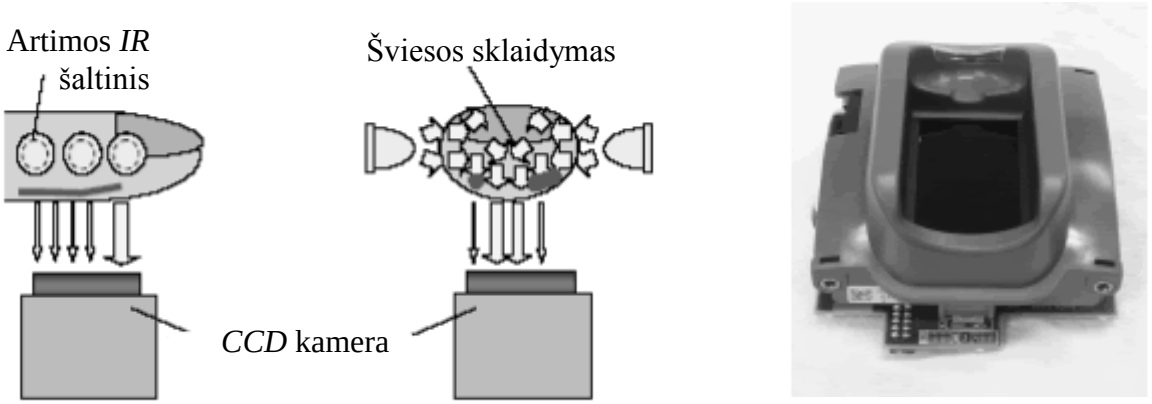
Kraujagyslių nuskaitymui naudojama įranga skirstoma į iš dalies kontaktinę ir bekontaktę. Iš dalies kontaktinėje aparatinėje įrangoje pirštas yra dedamas ant laikiklio tarp (1.3.5.1 pav. b) arba šalia (1.3.5.2 pav. c) vaizdą fiksuojančios kameros (*CCD*) ir infraraudonosios spinduliuotės šaltinio (dažniausiai – *LED*). Tokioje įrangoje reikalingas mažesnis papildomas piršto padėties normalizavimas. Nors šiame įrangos tipe dalys piršto prisiliečia prie laikiklio, tai tik iš dalies kontaktinis metodas ir, skirtingai nei pavyzdžiui piršto antspaudų skenavime, nereikia perbraukti viso piršto paviršiaus spaudžiant prie jutiklio.

Bekontakčiai skaitytuvai (1.3.5.3 pav.) nuskaito piršto kraujagyslių atvaizdus tokiu pačiu principu, kaip iš dalies kontaktiniai skaitytuvai, tačiau atstumas tarp infraraudonosios spinduliuotės šaltinio ir kameros yra didesnis ir piršto visiškai nereikia padėti ant laikiklio. Tokia įranga šiek tiek padidina biometrinės sistemos draugiškumą vartotojui, tačiau dėl atstumo nuo kameros ir šviesos šaltinio, piršto padėties, pasukimo ir kitų papildomų paklaidų padidina neteisingo nuskaitymo tikimybę. Tokio tipo skaitikliai labiau tinkami atvaizdų palyginimą naudojančioms sistemoms, nei tiesioginiam raktų generavimui.



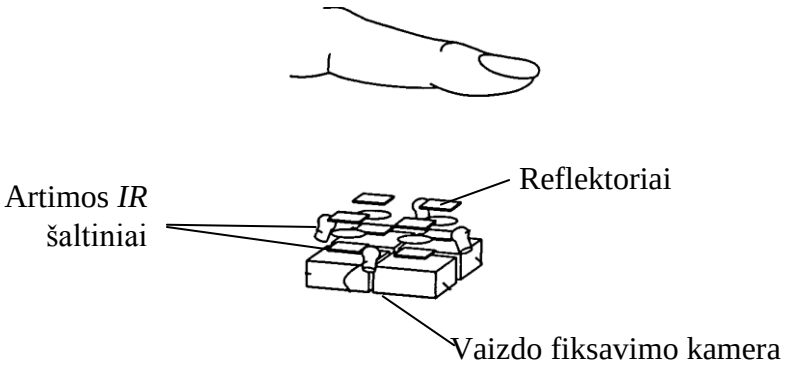
(a) (b)

1.3.5.1 pav. Iš dalies kontaktinio piršto kraujagyslių tinklo nuskaitymo įrenginys su *LED* viršuje. (a) įrenginio veikimo principas, (b) Hitachi H1 skaitytuvas [*14*]



(a) (b) (c)

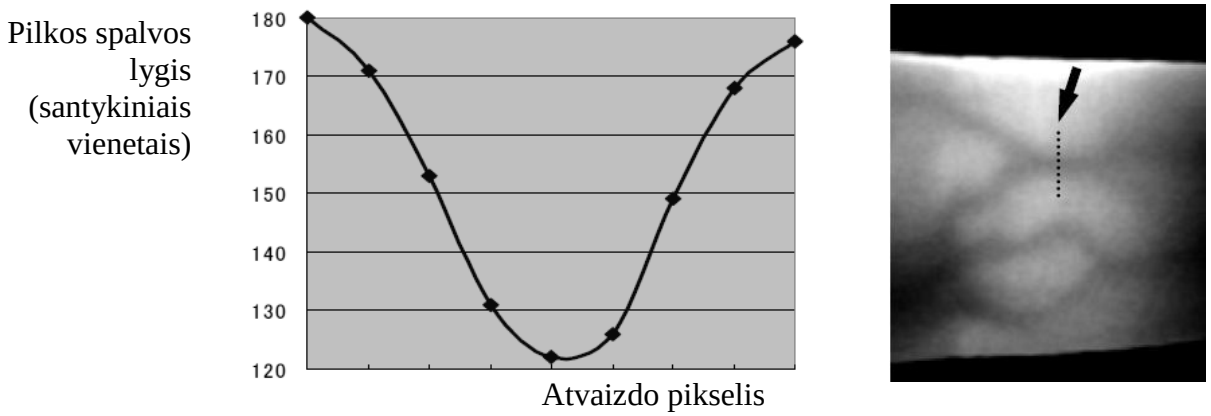
1.3.5.2 pav. Iš dalies kontaktinio piršto kraujagyslių tinklo nuskaitymo įrenginys su *LED* šonuose. (a) įrenginio veikimo principas (vaizdas iš šono), (b) įrenginio veikimo principas (vaizdas iš priekio), (c) Hitachi Embeded UBreaded skaitytuvas [*14*]



1.3.5.3 pav. Bekontakčio kraujagyslių tinklo skaitytuvo veikimo principas [*21*]

Tarp komercinių sistemų, skirtų pirštų kraujagyslių atvaizdams gauti ir apdoroti, dominuoja Hitachi, Fujitsu, M2SYS, Sony ir kitų gamintojų produktai.

Dėl kraujagyslių geometrijos, kraujagyslių centrai yra tamsesni, o juos supantys kraštai tolygiai šviesesni. Nuskaičius, kraujagyslės matomos kaip tamsūs slėniai (1.3.5.4 pav.), todėl kraujagyslių išskyrimas gali būti ganėtinai tikslus ir patikimas, bet kai nuskaitytame atvaizde yra triukšmų. Svarbus aspektas, siekiant kad kraujagyslių nuskaitymas būtų tikslus yra infraraudonosios spinduliuotės normalizavimas. Jei apšvietimas netolygus, per stiprus ar per silpnas, galimi papildomi netikslumai nuskaitomame atvaizde.



1.3.5.4 pav. Pilki atspalviai atvaizde: (a) skersinis pjūvis, (b) pjūvio vieta atvaizde [*20*]

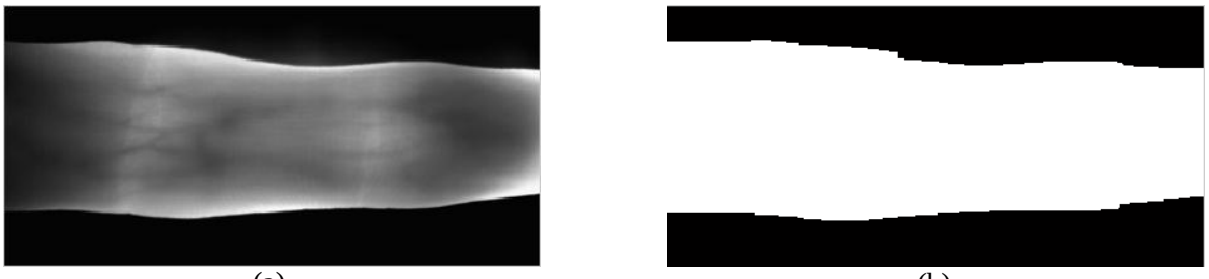
1.4. Pirminio kraujagyslių tinklo išskyrimo metodų apžvalga

Šiame skyriuje apžvelgiami pirminio kraujagyslių tinklo išskyrimo algoritmai. Daugelis aparatinės įrangos gamintojų su įrenginiais pateikia ir įrenginiams pritaikytą programinę įrangą. Gamintojų programinėje įrangoje naudojami metodai priklauso nuo aparatinės įrangos specifikos ir numatomos pritaikymo srities. Konkretūs gamintojų naudojami specifiniai metodai nėra skelbiami arba jų nepavyko surasti. Kadangi biometriniai įrenginiai dažnai dirba pagal vienokius ar kitokius standartus, pavyzdžiui *BioAPI* standartą, alternatyva gamintojų programinei įrangai galėtų būti atskirai įsigyjami programiniai paketai ir integruotos kūrimo aplinkos.

Darbe naudojami ir šiame skyriuje aptariami trys moksliniais straipsniais paremti metodai kraujagyslių tinklui išskirti. Šie metodai realizuoti *Matlab* kalba autoriaus *Bram Ton* bandymuose [***22***]. Be pirminių kraujagyslių tinklo išskyrimo funkcijų taip pat naudojama to paties autoriaus realizuota moksliniais straipsniais paremta piršto ploto lokalizavimo funkcija ir vienas pavyzdinis kraujagyslių tinklo atvaizdas, kurio pradinis dydis yra 780x380 pikselių.

1.4.1. *Lee ir kt.* piršto ploto lokalizavimo metodas

Po kraujagyslių atvaizdo nuskaitymo, daugelyje sistemų yra atliekamas piršto ploto lokalizavimas. Šiame plote toliau ieškoma kraujagyslių tinklo požymių. *Lee ir kt.* piršto ploto nustatymo metodas gana tiksliai nustato piršto plotą pirminiame atvaizde. Metodo rezultatas – [x,y] matrica žyminti piršto tūrį 1, o plotą aplink pirštą – 0. Šis piršto ploto nustatymo atvaizdas yra toliau nagrinėjamų funkcijų argumentas [***22***], [***23***].



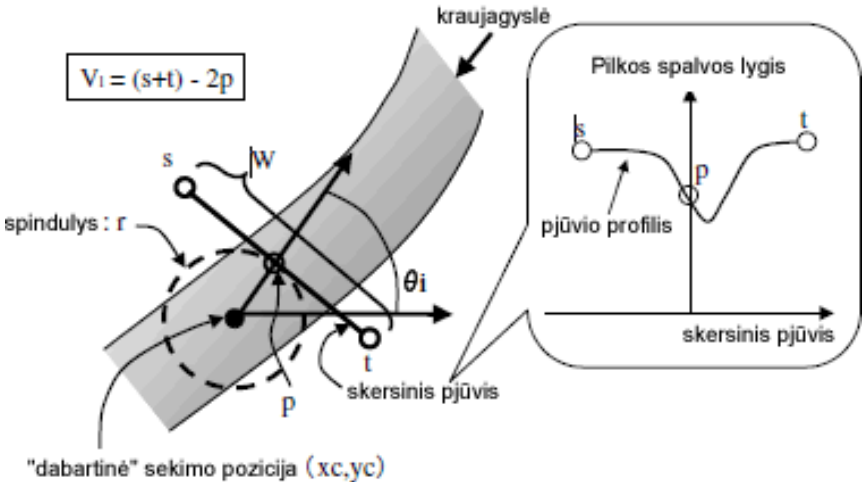
1.4.1.1 pav. *Lee ir kt.* piršto lokalizavimo funkcijos įvestis (a) ir rezultatas (b) [*22*]

1.4.2. *Miura ir kt.* kraujagyslių išskyrimo metodas, taikant pasikartojantį linijų sekimą

Dėl netolygaus piršto apšvietimo kraujagyslių išskyrimo metu ir normalizacijos problemų tokie tinklo išskyrimo metodai, kaip kaukių/filtrų taikymas ir morfologiniai metodai *minutiae* taškams išskirti tampa netikslūs. *Miura ir kt.* „Kraujagyslių išskyrimo metodas, taikant pasikartojantį linijų sekimą“ yra paremtas tamsiausių taškų kraujagyslių atvaizdo pjūvyje aptikimu ir sekimu šiais taškais

tol, kol jie apsupti gerai matomo tolygiai šviesesnio „slėnio“ (1.3.5.4 a) pav.). Nuolatinis aplinkinių plotų šviesumo tikrinimas leidžia sumažinti atsitiktinai sekamų triukšmų įtaką galutiniam rezultatui ir efektyviai pašalinti dėl kaulų ir sąnarių struktūros atvaizde atsirandančius šešėlius. Priklausomai nuo pasirinkto sekimo iteracijų skaičiaus (sekimo kartų), funkcija gali praeiti per aptiktas tamsios spalvos linijas vieną ar keletą kartų. Tikėtina, kad taškai, per kuriuos linijų sekimo algoritmas praeina keletą kartų, yra kraujagyslės [***20***].

Linijos pradedamos sekti nuo atsitiktinio taško gautame atvaizde *F*. Kiekvieno taško atvaizde intensyvumas (pilkos spalvos lygis) gali būti aprašomas funkcija *F(x,y)* Taškas, kuriame yra metodo naudojamas kursorius yra vadinamas dabartiniu tašku (x_c,y_c). Nuo šio taško kursorius gali judėti bet kuria kryptimi link tamsesnės vietos atvaizde. Kursoriaus judėjimo kryptis ribojama tik judėjimo spindulio *r* ir sekamo pločio *W* parametrais. Paveiksle 1.4.2.1 pavaizduotas erdvinis ryšys tarp „dabartinio taško“ ir atvaizdo profilio pjūvio.



1.4.2.1 pav. Tamsios linijos sekimas. Ryšys tarp atvaizdo ir atvaizdo skersinio pjūvio

Jei būtų atliekama tik viena sekimo iteracija, tik dalis kraujagyslių būtų išskirta, nes nesusijungusios kraujagyslės nebūtų sekamos. Taip pat jei metode numatytas slėnio gylis nebūtų pasiektas, sekimas nebūtų tęsiamas. Siekiant išspręsti šią problemą, metodas kartojamas numatytą skaičių kartų ir sekimas pradedamas nuo atsitiktinių taškų. Todėl *Miura ir kt.* „Pasikartojančio linijų sekimo metodas“ iš esmės yra atsitiktinis. Šio metodo atsitiktinumo ir pakankamo iteracijų skaičiaus įvertinimas yra pateikiamas darbo bandymo dalyje.

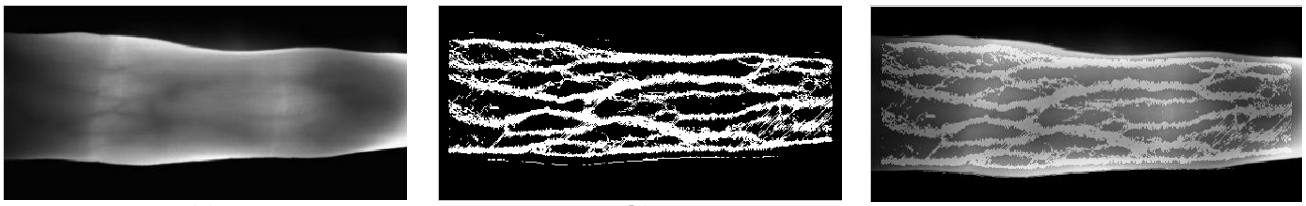
Atliekant sekimą yra registruojamas perėjimų per tam tikrus atvaizdo taškus skaičius. Taškai, per kuriuos sekimas atliekamas daug karų turi didesnę tikimybė, kad toje vietoje atvaizde užfiksuota kraujagyslė.

Miura ir kt. „Pasikartojančio linijų sekimo metodo“ savybių išskyrimas gali būti skaidomas į tokius žingsnius:

- Pradinio sekimo taško nustatymas ir judėjimo krypties parinkimas: pradinio taško nustatymas yra atsitiktinis, o tolesnio taško pozicija ribojama *r* parametro. Siekiant apriboti linijų su per dideliu linkiu sekimą, tolesnio sekimo kryptis D_{lr} ir D_{ud} gali įgyti tik reikšmes iš numatyto intervalo.
- Tamsios linijos krypties nustatymas ir kursoriaus perkėlimas
- Taškų registravimo matricos papildymas
- Pakartotinis žingsnių 1-3 atlikimas *N* kartų: metodo autorių nustatytas reikalingas pakartojimų skaičius, siekiant aušto metodo tikslumo yra *N=3000* šis parametras priklauso nuo naudojamų atvaizdų kokybės ir dydžio.
- Atvaizdo sudarymas iš perėjimo kartų matricos.

Šio metodo autorių pateiktuose bandymuose, kuriuose naudoti 678 skirtingi pirštų atvaizdai, nustatyta 0,145% *BKT*. Tokia *BKT* yra mažesnė lyginant su vidutine pirštų antspaudus naudojančia sistemos, kurios *BKT* svyruoja tarp 0,2% ir 4%.

Miura ir kt. „Pakartotino linijų sekimo metodo“ realizacija šiame darbe neatliekama. Bandymams buvo naudojama autoriaus *Bram Ton Matlab* kalba parašyta metodo versija „miura_repeated_line_tracking“ [***22***]. Šios versijos pavyzdinis atvaizdas ir išskirtas kraujagyslių tinklas pateiktas 1.4.2.2 paveiksle. Naudotas pradinis atvaizdas apdorotas taikant *r=1, W=17* pradinius parametrus. Įvesties atvaizdo dydis lygus 389x189 pikselių.



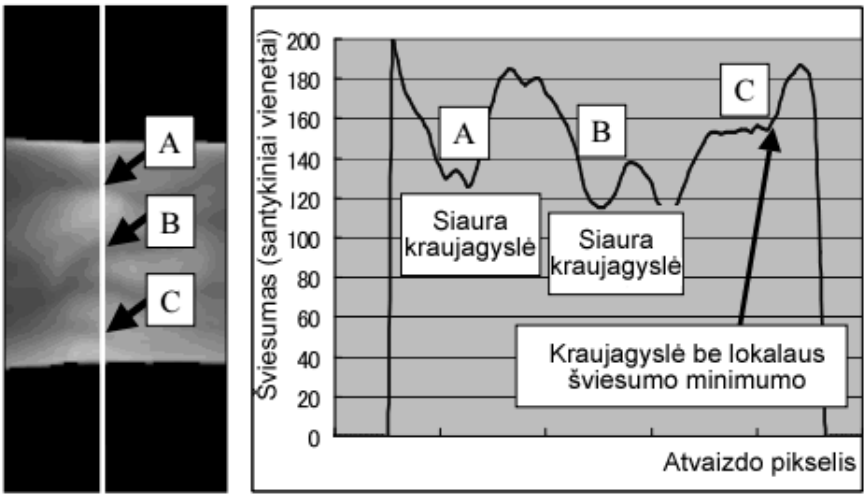
(a) (b) (c)

1.4.2.2 pav. „miura_repeated_line_tracking“ algoritmo įvestis (a), rezultatas (b) ir rezultatas užklotas ant pradinio atvaizdo (c)

1.4.3. *Miura ir kt.* Kraujagyslių išskyrimo metodas, naudojant maksimalaus linkio taškus

Tradiciniai kraujagyslių tinklo išskyrimo metodai, kaip filtro atitikmens taikymas ir morfologiniai metodai patikimai išskiria kraujagyslių tinklą tuomet, kai kraujagyslių plotai yra pastovūs. Tačiau šie metodai negali išskirti kraujagyslių, kurios yra platesnės/siauresnės, nei nustatytas plotis ir nuo to nukenčia išskiriamo tinklo tikslumas. Pasikartojančio linijų sekimo metodas gali išskirti įvairaus pločio kraujagysles, bet šis metodas yra paremtas atsitiktiniu kraujagyslių sekimu, plonesnės kraujagyslės yra išskiriamos mažiau patinimai. Trumpos plonų kraujagyslių atkarpos gali būti prarandamos [***24***].

Maksimalaus linkio kraujagyslių atvaizdo pjūvyje metodas paremtas kraujagyslių centrinių linijų išskyrimu kraujagyslių atvaizdo profilio pjūvyje (1.4.3.1 pav.). Taip išskiriamos bet kokio pločio kraujagyslės. Kraujagyslių centrinės linijos išskiriamos ieškant vietų, kur kraujagyslių atvaizdo pjūvio vietos yra maksimalios. Net siauros/plačios arba šviesios/tamsios kraujagyslės, paveiksle 1.4.3.1 pažymėtos A, B ir C taškais, kur centrinė kraujagyslės linija neturi lokalaus šviesumo minimumo (taškas C), profilio šviesumo kreivės linkis yra gana didelis ir registruojamas.



1.4.3.1 pav. Kraujagyslių skersinio pjūvio ryškumo grafikas [*24*]

Kadangi kraujagyslių skenavimas atliekamas „slenkant“ per kraujagyslių atvaizdo pjūvį, tam tikri trūkiai kraujagyslių tinkle gali būti užpildomi arba atsitiktiniai tamsūs plotai, atsiradę dėl nuskaitymo trikdžių, kurie nesusijungia su toliau esančiais skenavimo maksimumais/minimumais, gali būti pašalinami.

Tinklo generavimo iš atvaizdo metodo žingsniai pavaizduoti 1.4.3.2 paveiksle. Šių žingsnių seka yra tokia:

- Linkio profilių skaičiavimas: *F* yra piršto atvaizdas, *F(x,y)* - *(x,y)* pikselio intensyvumas. Pjūvio profilis aprašomas funkcija $P_f(z)$ gauta iš *F(x,y)* bet kokia kryptimi, bet kurioje pozicijoje, kur *z* yra pozicija profilio atvaizde. Pjūvio profilis *k(z)* gali būti atvaizduojamas funkcija, pateikta 1.4.3.1 formulėje:

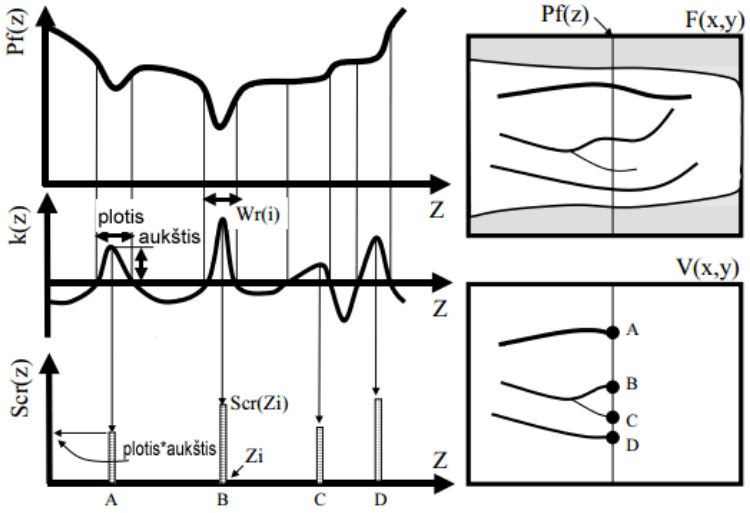
$$k(z) = \frac{d^2 P_f(z)/dz^2}{\{1+(dP_f(z)/dz)^2\}^{\frac{3}{2}}} \qquad \mathbf{(1.4.3.1)}$$

- Kraujagyslių centrų nustatymas: maksimumai k(z) profilyje nurodo kraujagyslių centro taškus. Šių taškų pozicijos apskaičiuojamos ir aprašomos z'_i, kur i=0,1,...,*N-1*, o *N* – maksimumų profilyje skaičius.

- Kraujagyslių centrams priskiriamos santykinės tikimybės reikšmės, kuriuos skaičiuojamos sudauginant *k(z)* kreivės pločio ir aukščio vertes pagal 1.4.3.2 formulę:

$$S_{cr}(z'_i)=k(z'_i) * W_r(i) \qquad (1.4.1)$$

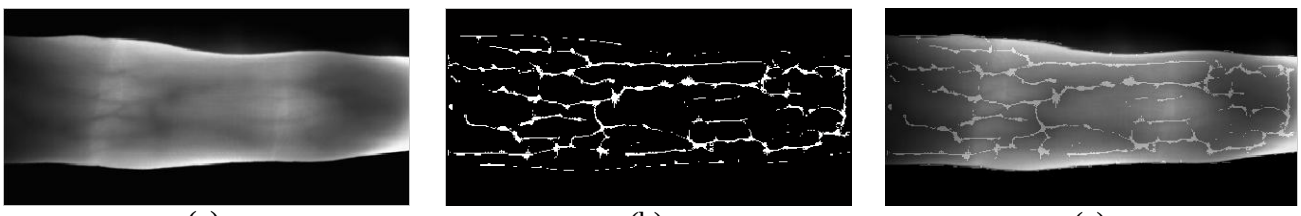
- Gautos S_{cr} vertės yra priskiriamos plokštumai *V(x,y)*, kuri yra išskirtų ir paryškintų kraujagyslių atvaizdas.



1.4.3.2 pav. Kraujagyslių išskyrimo žingsniai, taikant maksimalaus linkio metodą

Atlikus bandymus su 678 skirtingų pirštų atvaizdais, gauta šio metodo *BKT* tikimybė lygi 0,0009%. Tai kur kas mažesnė *BKT* lyginant su daugeliu kitų metodų [***24***].

Miura ir kt. „Maksimalaus linkio metodo“ realizacija šiame darbe neatliekama. Bandymams buvo naudojama autoriaus *Bram Ton Matlab* kalba parašyta metodo versija „miura_max_curvature“ [***22***]. Šios versijos pavyzdinis atvaizdas ir išskirtas kraujagyslių tinklas pateiktas 1.4.3.3 paveiksle. Naudota *sigma=3* vertė santykiniams aukščio ir pločio parametrams nustatyti.



(a) (b) (c)

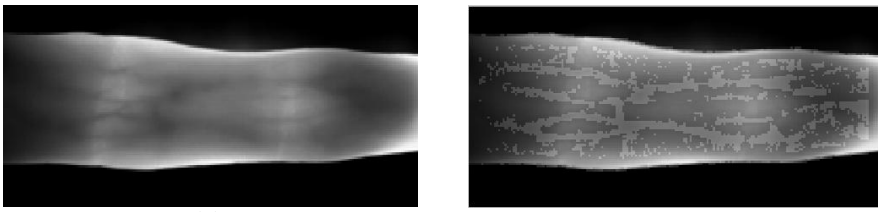
1.4.3.3 pav. „miura_max_curvature“ algoritmo įvestis (a), rezultatas (b) ir rezultatas užklotas ant pradinio atvaizdo (c)

1.4.4. *Huang ir kt.* kraujagyslių išskyrimo metodas, paremtas plačių linijų nustatymu

Kadangi dėl aplinkos veiksnių ir papildomų paklaidų, atsirandančių dėl piršto padėties (normalizacijos) blogėja nuskaitomo atvaizdo kokybė, dalis biometrinės informacijos yra prarandama. Vienas būdas pagerinti generuojamų kraujagyslių tinklų kokybę yra tobulinti

algoritmus, galinčius pataisyti netinkamai nustatytas savybes, kitas būdas – padidinti informacijos, kuri išgaunama iš patikimai nuskaitytų atvaizdų kiek *Huang ir kt.* metodas sukurtas siekiant padidinti informacijos gaunamos iš pirštų kraujagyslių atvaizdo kiekį. Tai pasiekiama nustatant ne tik kraujagyslių tinklo struktūrą, bet ir tiksliai įvertinant plačių kraujagyslių plotį [***25***]

Kraujagyslių kontūrai atvaizde *F* išskiriami naudojant [***26***] šaltinyje aprašomą metodą. Po apdorojimo gautas kraujagyslių tinklo atvaizdas žymimas *V*. Tiek F, tiek *V* autorių bandymuose buvo 8 bitų gylio 128x96 „bitmap“ tipo atvaizdai. Autorių bandymuose gaunama *BKT* taikant *Huang ir kt.* plačių linijų nustatymo metodą su papildoma normalizacija siekia 0,87%.



(a) (b)

1.4.4.1 pav. „huang_wide_line“ įvestis (a) ir rezultatas užklotas ant pradinio atvaizdo (b)

Huang ir kt. plačių linijų nustatymo metodo realizacija šiame darbe neatliekama. Bandymams buvo naudojama autoriaus *Bram Ton Matlab* kalba parašyta metodo „huang_wide_line“ versija [***22***]. Šios versijos pavyzdinis atvaizdas ir išskirtas kraujagyslių tinklas pateiktas 1.4.4.1 paveiksle.

1.4.5. Kiti metodai

Be aptartų pirminio pirštų antspaudų apdorojimo metodų paminėtini *Rosdi* ir kt. „Piršto kraujagyslių atpažinimo naudojant vietinius linijos dvinarius atvaizdus“ [***27***], *Mahri ir kt.* „Piršto kraujagyslių atpažinimo naudojant fazinę koreliaciją“ [***28***], *Qin* ir kt. „Ploto augimu paremtas požymių išskyrimas piršto kraujagyslių atpažinimui“ [***29***] ir kiti metodai. Pirminio išskirimo metodas realizuojant sistemą turėtų būti parenkamas pagal sistemai keliamus reikalavimus.

1.5. Matematinės morfologijos taikymo kraujagyslių tinklo sudarymui apžvalga

Skaitmeniniame vaizdų apdorojime matematinės morfologinės funkcijos – tai rinkinys metodų, pagristų kombinatorikos, topologijos, atsitiktinių dydžių ir kitomis technikomis. Apdorojamas juodai baltas (kartais ir pilkų atspalvių) atvaizdas yra skaidomas iki mažiausių jo elementų ir apdorojamas pagal iš anksto numatytas taisykles. Pavyzdžiui skaidant atvaizdą blokais 3x3 vaizdo elementai, kurie ribojasi ar yra arti 5 priešingos vertės elementų yra pakeičiami į priešingus [***30***]. Matematinės morfologijos technikos gali būti taikomos nuskaitytam kraujagyslių atvaizdui arba pirminėmis funkcijomis išskirtam kraujagyslių tinklui tikslinti ir taisyti. Išnagrinėjus ir pritaikius reikiamas morfologines vaizdo apdorojimo funkcijas galima transformuoti pradinius kraujagyslių tinklo atvaizdus į linijas, sujungti kai kuruos trūkius, pašalinti atsišakojimus ar triukšmus Vienokios ar kitokios matematinės morfologijos technikos taikomos daugelyje biometrinius duomenis naudojančių sistemų.

Pagrindinės dvinarės matematinės morfologijos operacijos yra: erozija, plėtimas, atidarymas, uždarymas ir kt. *Matlab* vaizdų apdorojimo programiniame pakete pateikiama 20 standartinių morfologinių funkcijų. Kai kurių *Matlab* programiniame pakete pateikiamų dvinarės matematinės morfologijos pavyzdžiai pateikiami 6.3 priede. Atvaizdas, kuriam apdoroti taikoma matematinė morfologija buvo apdorotas *Miura ir kt.* „Pasikartojančio linijų sekimo“ pirminiu požymių išskyrimo metodu.

Nors matematinės morfologijos funkcijos vienaip ar kitaip taikomos daugelyje autentifikavimo sistemų, jų aibės dažniausiai nėra viešai skelbiamos. Morfologinių funkcijų aibė tampa sistemos parametrų dalimi ir yra aptariamos šio darbo eksperimentinėje dalyje.

Viena iš sąlygų, kuri bus būtina, realizuojant pasirinktus raktų generavimo metodus yra kraujagyslių tinklo vertimas vieno pikselio pločio tinklu. Tai pasiekiama taikant *Matlab skel* matematinės morfologijos funkciją, o jos rezultatų pavyzdys parodytas 1.5.1 pav.

1.4.5.1 pav. Objekto vertimas linija taikant matematinę morfologiją

Skel funkcijos veikimas pagrįstas objektų siaurinimu tol. Kol pasiekiamas stabilus rezultatas. *Skel* funkcija mažina objektus iki minimalaus jų dydžio, tačiau išlaiko *Eulerio skaičių* atvaizde. *Eulerio* skaičius atvaizde lygus objektų skaičiui atvaizde minus uždarų skylių atvaizde skaičiui [***31***].

1.6. Klaidų taisymo algoritmų apžvalga

Klaidų taisymo algoritmai taikomi įvairiose telekomunikacijų, informacinių technologijų ir programavimo srityse. Šie algoritmai padeda sumažinti informacijos praradimą ar pagerina perduodamos informacijos kokybę ten, kur dėl triukšmų ar kitų atsirandančių netikslumų informacija galėtų būti prarandama. Pagrindinė klaidų aptikimo algoritmų funkcija yra nustatyti, kad dėl informacijos kitimo atsirado galimi netikslumai, o klaidų taisymo algoritmų funkcija – pataisyti klaidas. Klaidų aptikimo ir taisymo metodai paremti papildomos perteklinės informacijos pridėjimu prie siunčiamos (biometrijos atveju nuskaitomos) informacijos [***32***]. Pagrindiniai klaidų taisymo metodai yra vienmatis perteklinio bito pridėjimas (1.6.1 pav.), dvimatis perteklinių bitų pridėjimas, kontrolinės sumos siuntimas ir kiti metodai.

Dešimtainis skaičius	Dvejetainis skaičius	Pertekliniai bitai	
		Nelyginis	Lyginis
0	0000	1	0
1	0001	0	1
2	0010	0	1
3	0011	1	0
4	0100	0	1
5	0101	1	0
6	0110	1	0
7	0111	0	1
8	1000	0	1
9	1001	1	0

1.6.1.4.5.1 pav. Klaidų aptikimas pridedant vienmatį perteklinį bitą

Kadangi biometriniai metodai nėra tiesiogine prasme informacijos perdavimo metodai, klaidų taisymo principai čia skirsis. Šiame darbe nagrinėjami klaidų taisymo metodai pristatomi modelio realizavimo skyriuje ir yra specifiniai siūlomam raktų generavimo metodui.

Literatūroje aprašomos kai kurias biometrines savybes autentifikacijai naudojančios sistemos, kuriose taikomi klaidų taisymo kodai. Dalyje tokių sistemų nuskaitytas biometrinis atvaizdas yra naudojamas tik triukšmo kanalui simuliuoti siekiant atrakinti slepiamą šifravimo raktą [***33***]. Tokiose sistemose to paties žmogaus biometrinių charakteristikų kitimai yra traktuojami kaip klaidos ir joms taisyti taikomi klaidų taisymo kodai. Bandymai su pirštų antspaudais ir *BCH, Reed-Solomon, LDPC* klaidų taisymo kodais kriptografinio rakto generavimui patiekti šaltinyje [***34***], tačiau čia taip pat reikalingas atvaizdo išankstinis įvedimas ir sistemos apmokymas.

1.7. Išvados

Apžvalgoje išnagrinėjus biometrines savybes, biometrinių sistemų tipus ir kai kuriuos savybių išskyrimo iš piršto kraujagyslių atvaizdų metodus, nustatyta, kad pirštų kraujagyslių tinklas yra patikima biometrinė savybė plačiai taikoma įvairiose biometrinio autentifikavimo sistemose.

Dagelyje autentifikavimo sistemų, kontroliuojančių vartotojų prieigą naudojant biometrinius metodus taikomas atvaizdo palyginimo su iš anksto įvestu šablonu metodas. Šis metodas yra patikimas ir leidžia ištaisyti kai kurias kraujagyslių tinklo sudarymo klaidas, atsirandančias dėl biometrinių duomenų nepastovumo.

Daugelis komercinių produktų viešai neskelbia pirminių kraujagyslių tinklo išskyrimo ir kitokių metodų veikimo principų, todėl darbe toliau bus remiamasi literatūroje aprašomais ir šiame skyriuje aptartais metodais. Tokie metodai nėra labai patikimi ir gali būti kai kurių tolesnių rezultato netikslumų priežastis.

Atliekant literatūros analizę nebuvo surasta metodų, skirtų slaptiems raktams generuoti tiesiogiai iš piršto kraujagyslių tinklo. Analizuotos sistemos, taikančios biometriją slaptų raktų generavimui iš kitokių biometrinių savybių dažnai naudojasi papildomu lyginimu su iš anksto išsaugotais šablonais.

2. TIESIOGINIO SLAPTŲ RAKTŲ GENERAVIMO IŠ PIRŠTO KRAUJAGYSLIŲ TINKLO METODO SUDARYMAS

2.1. Darbo tikslas ir uždaviniai

Šiuolaikinės biometrines savybes vartotojų autentifikavimui naudojančios sistemos yra greitos, patikimos ir taikomos įvairiose srityse. Pasirinktoms biometrinėms savybėms išskirti yra sukurta daug metodų, kurių tikslumas ir veikimo principai yra skirtingi. Dažnai tikslus komercinių sistemų veikimas gamintojų nėra pateikiamas.

Išanalizavus literatūroje aptariamas sistemas, nebuvo surastas sistemos, galinčios generuoti slaptus šifravimo raktus iš piršto kraujagyslių tinklo tiesiogiai modelis, metodas, tyrimai ar taikymo pavyzdžiai. Anksčiau atliktuose darbuose bandant tiesiogiai generuoti raktą iš piršto antspaudų buvo gautas neigiamas rezultatas [***35***], o kai kuriose sistemose, generuojančiose šifravimo raktus iš biometrinių savybių vis tiek yra saugomas vienoks ar kitoks etaloninis atvaizdas, prieš generuojant raktą [***33***].

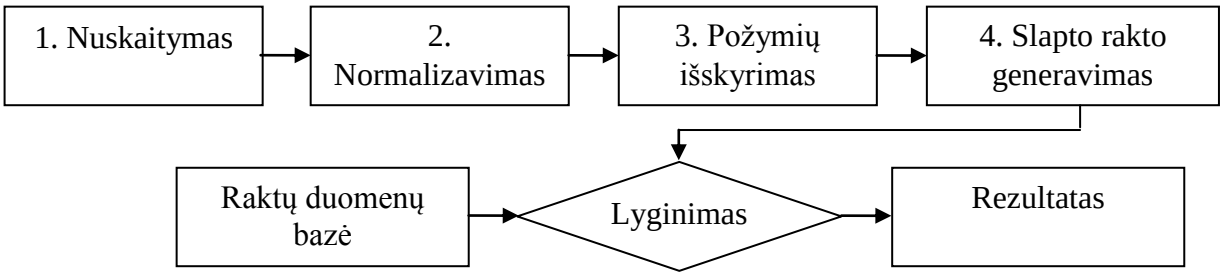
Pagrindinė šiuolaikinių sistemų problema yra poreikis saugoti asmeninius biometrinius duomenis. Siekiant išvengti bet kokio duomenų saugojimo ar atvaizdų lyginimo operacijų yra siekiama sudaryti metodą raktui tiesiogiai generuoti iš pirštų kraujagyslių tinklo nesaugant jokių tarpinių palyginimo šablonų. Tokios sistemos raktai, jei jie būtų pakankamo ilgio, galėtų pakeisti šifravimo raktus ir pavyzdžiui leisti vietoje banko kortelės naudoti pirštą kaip *tai ką turiu* autentifikavimo sudedamąją dalį. Šie raktai sistemoje galėtų būti apsaugoti papildomu *PIN* ar kitokiu identifikavimo vardu ar slaptažodžiu. Kitas aspektas – tiesiogiai iš kraujagyslių tinklo sugeneruoti slaptieji raktai, jei patikimai išgaunamas jų ilgis yra nedidelis, galėtų pakeisti asmeninius identifikavimo numerius ar PIN kodus siekiant išduoti išmaniojoje kortelėje ar kitokioje laikmenoje saugomą slaptą šifravimo raktą.

Tiesioginio slaptų raktų generavimo metodui iš piršto kraujagyslių sudaryti bus naudojami literatūros apžvalgoje aptariami priminio kraujagyslių tinklo išskyrimo metodai ir matematinės morfologijos funkcijos.

2.1.1. Darbo tikslas

Pasiūlyti ir ištirti slapto rakto generavimo metodą iš vartotojo piršto kraujagyslių tinklo nenaudojant palyginimo su iš anksto išsaugotu šablonu.

Tokį metodą naudojančios sistemos pirminė blokinė schema pateikiama 2.1.1.1 pav. Vietoje pavaizduoto lyginimo operacijos šioje sistemoje galėtų būti kombinuojami keli sugeneruoti raktai ir naudojami biokriptografijoje informacijai šifruoti.



2.1.1.1 pav. Pirminė blokinė raktų generavimo metodo schema

2.1.2. Uždaviniai

- Atlikti biometrinių vartotojų autentifikavimo metodų, kuriuose taikomas kraujagyslių tinklo nuskaitymas ir palyginimas su iš anksto išsaugotu šablonu analizę (atlikta literatūros apžvalgoje)
- Pasiūlyti naują metodą slaptiems raktams generuoti, kuriame nebūtų taikomos palyginimo ir apytikslio sutapimo funkcijos
- Sukurti aplinką esamiems ir pasiūlytam kraujagyslių tinklo apdorojimo metodui bandyti

- Atlikti siūlomo autentifikavimo metodo tyrimą ir skaitinį įvertinimą
- Pateikti siūlomo metodo tinkamumo tiesiogiai generuoti slaptus raktus iš piršto kraujagyslių tinklo galimybių įvertinimą ir išskirti galimas metodo tobulinimo sritis

2.2. Reikalavimų apibrėžimas

Šiame darbe sudaromas literatūroje neaprašomas arba nerastas metodas raktams generuoti, todėl iš anksto numatyti jo charakteristikas sudėtinga. Sudarant metodą daroma prielaida, kad jis turi generuoti pastovius slaptus raktus. Šių raktų ilgį numatoma įvertinti, tačiau pirmiausia telkiamas dėmesys į trumpų, bet kiek įmanoma pastovesnių raktų generavimą. Jei reikia prailginti raktą, siūloma vietoje padidinto raktų, generuojamų iš kiekvieno atvaizdo, kardinalumo naudoti atvaizdų vertinimo sekas ir kombinuoti jų rezultatus.

2.2.1. Funkciniai reikalavimai kuriamam metodui

Funkciniai reikalavimai nusako tai, ką sistema turės gebėti daryti. Šiuo atveju pateikiamas funkcinių reikalavimų siūlomam metodui ir tyrimo grafinei sąsajai, o ne sistemai, taikančiai tokius metodus sąrašas.

- Metodas gebės atlikti papildomą piršto kraujagyslių tinklo atvaizdo lokalizaciją ir normalizaciją ir išsaugoti rezultatą
- Metodas turės išvesti slaptą raktą iš pateikto kraujagyslių tinklo atvaizdo
- Vartotojo sąsaja leis grafiškai įvertinti taikomų pirminio apdorojimo ir matematinės morfologijos funkcijų tarpinius rezultatus
- Tyrimų aplinka galės būti naudojama duomenų bazėje pateiktų atvaizdų apdorojimui sukurtu metodu

2.2.2. Nefunkciniai reikalavimai kuriamam metodui

Nefunkciniai reikalavimai – reikalavimai leidžiantys vertinti kaip veikia sistema, o ne ką konkrečiai ji atlieka. Keli pagrindiniai nefunkciniai reikalavimai metodui ir sąsajai pateikti žemiau.

- Metodas turės galimybę abstraktinti arba tikslinti generuojamų raktų savybes: rakto ilgį, tikslumo parametrus, pagal numatytus kriterijus
- Metodas turės gebėti atlikti papildomą atvaizdų normalizaciją ir apdorojimą
- Vartotojo sąsaga galės taikyti skirtingas matematinės morfologijos funkcijų aibes ant pirminėmis funkcijomis apdoroto atvaizdo arba taikyti standartinę matematinės morfologijos funkcijų aibę ir atvaizduoti tarpinius rezultatus
- Vartotojo sąsaja galės iškviesti reikiamus kodo generavimo metodus ir atvaizduos bei leis išsaugoti jų rezultatus
- Vartotojo sąsaja leis perduoti visuose reikalavimų aprašo žingsniuose numatytoms naudoti funkcijoms reikalingus parametrus
- Vartotojo sąsaja leis vertinti *Miura ir kt. „*Pasikartojančių linijų sekimo metodo“ tarpinius parametrus: atvaizdo juoda/balta balansą, išskirtų kraujagyslių sutapimą su ankstesniais išskyrimais

2.3. Metodo esmė

Pagrindinis sudaromo metodo tikslas – iš to paties piršto kraujagyslių atvaizdo kiekvieną kartą generuoti tokį patį slaptą raktą. Metodo realizavimas būtų santykinai paprastas, jei nebūtų natūralaus biometrinių savybių kitimo, atsirandančio dėl nuskaitymo ir apdorojimo algoritmų veikimo specifikos ir paklaidų. Taip pat rakto generavimo metodui tampa daug svarbesnė griežta piršto padėties normalizacija, lyginant su palyginimo su iš anksto išsaugotu šablonu, kur priklausomai nuo įvesties atvaizdo ir etaloninio paveikslo savybių galima gana tiksliai lokalizuoti ir apriboti palyginimo plotą.

Tiesioginio slapto rakto generavimo metodui sudaryti bus naudojami keli žingsniai:

- Sekimo ploto normalizacija ir lokalizacija
- Reikšminių koordinačių išskyrimas

- Pradinių verčių prieš pradedant sekimą parinkimas
- Kontūro sekimo būdo parinkimas ir sekimas
- Kodo generavimo sričių sudarymas ir verčių priskyrimas metodui

Atlikus visus aptariamus žingsnius iš kraujagyslių tinklo būtų generuojamas slaptas raktas. Tam, kad raktas išliktų pastovus, nepaisant netikslumų nuskaitytame atvaizde ir paklaidų, metode numatomas tam tikras abstraktinimo lygis.

Nors pagrindinis šio darbo uždavinys yra kodo generavimo metodo sudarymas, kadangi yra dirbama su viešai pasiekiama piršto kraujagyslių duomenų baze ir pirminiais apdorojimo algoritmais, bei sudaroma pasirinkta matematinių morfologinių funkcijų aibe būtent šiam metodui, šie kodo generavimo aspektai taip pat gana plačiai nagrinėjami ir vertinami bandymo dalyje. Dirbant su komercinėmis sistemomis darbo apimtis galėtų mažėti iki tik kodo generavimo metodo analizės ir kūrimo, kai pradinis duomuo – lokalizuotas kraujagyslių tinklo atvaizdas.

2.4. Metodo detalizavimas

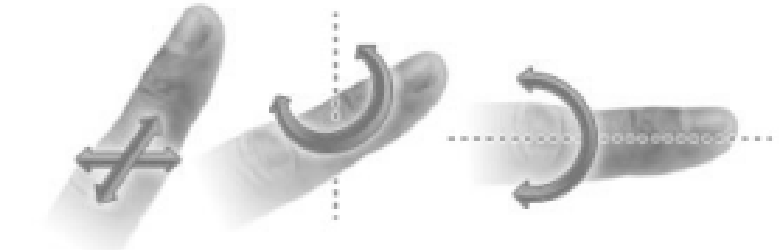
2.4.1. Sekimo ploto normalizacija ir lokalizacija

Darbe pristatomas kodo generavimo metodas atliks įvairių tipų kontūro sekimą kraujagyslių tinklo atvaizde. Bet koks sekamo ploto pastūmimas ar pasukimas turėtų įtakos galutiniam generuojamam kodui, todėl reikalingas būdas, kraujagyslių atvaizdo vietai, kurioje atliekamas sekimas patikslinti.

Tokia papildoma lokalizacija nėra labai svarbi daugelyje palyginimo operacijas atliekančių sistemų, nes jose galima atlikti dviejų atvaizdų užklojimo operacijas ir lyginti tik tas sritis, kur atvaizdų sutapimai yra tiksliausi (*Hamingo* atstumas minimalus).

Toliau darbe siūlomas kodo generavimo metodas paremtas kontūro sekimu yra labiausiai priklausomas nuo piršto padėties judinimo išilginėje ašyje, skersinėje ašyje piršto pastūmimas galėtų būti nustatomas ir įvertinamas paprasčiau.

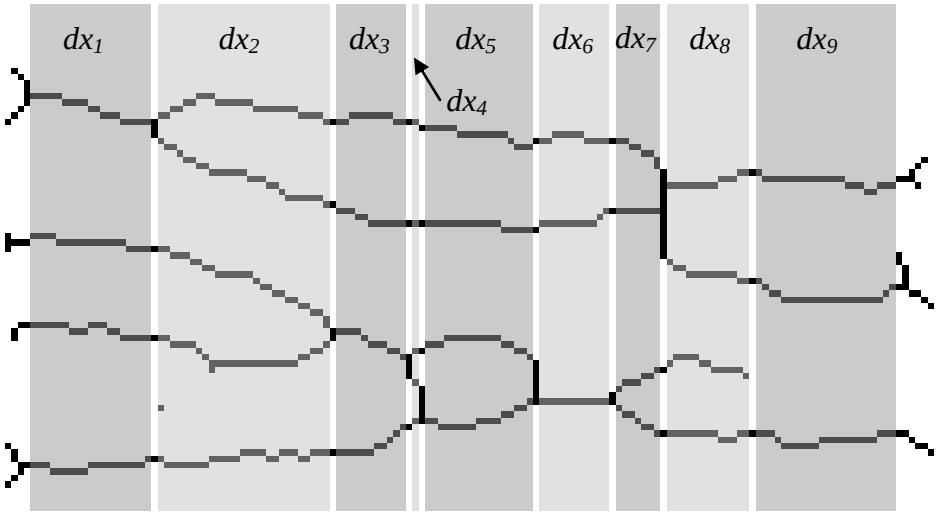
Šiame skyriuje aptariama tik piršto pastūmimo (2.4.1.1 pav. a) lokalizacija, bet daroma prielaida, kad aparatinė įranga gali pakankamai tiksliai apriboti piršto pasukimą vertikalaus ir horizontalaus piršto pasukimo ašyse (2.4.1.1 pav. b ir c).



a) b) c)

2.4.1.1 pav. Piršto padėties laisvės laipsniai nuskaitymo metu

Vienas automatinis būdas postūmio lokalizacijai atlikti galėtų būti ilgiausių lygiagrečių linijų vietos nustatymo metodas, kuris schematiškai pavaizduotas 2.4.1.2 pav. Šio metodo principas – aptikti ilgiausias atkarpas, kuriose kraujagyslės nesikerta ir nėra jų atsišakojimų. Toks papildomos lokalizacijos metodas leistų sumažinti paklaidas, atsirandančias dėl netikslumų patiektame piršto kraujagyslių atvaizde, kai piršto pastūmimas yra iš dalies skirtingas. Tokio lokalizacijos metodo trūkumas yra tai, kad būtų prarandama dalis nuskaitytų biometrinių duomenų, kurie nepatektų į sekimo plotą.



2.4.1.2 pav. Papildoma postūmio normalizacija

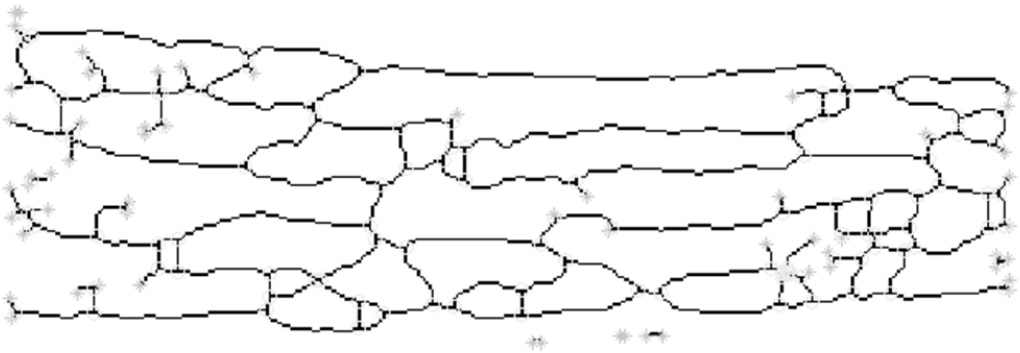
Apribotas plotas galėtų būti pasirinktas tarp ploto dx_2 pradžios ir ploto dx_9 pabaigos, nes šios dvi lygiagrečių kraujagyslių atkarpos yra ilgiausios.

Šiame darbe automatinis papildomo kraujagyslių ploto lokalizavimo metodas nebuvo realizuojamas, tačiau atliekant bandymus buvo atliktas rankinis papildomas lokalizavimas generavimo ploto lokalizavimas ir apribojimas.

2.4.2. Reikšminių koordinačių išskyrimas

Turint nustatytą piršto kraujagyslių tinklo atkarpą, kurioje numatoma atlikti kontūro sekimo metodus svarbu nustatyti reikšmines kontūro koordinates, tokias kaip kraujagyslės pradžios vietos (*KPV*), kraujagyslės galų (pabaigos) vietos (*KGV*), kraujagyslių susikirtimo vietos (*KSV*) ir kitas koordinate, jei jos reikalingos apdorojimui. Šiame darbe bus naudojamos tik *KPV* ir *KGV* koordinatės, tašiau tobulinant rakto generavimo metodus galima išskirti ir kitas savybes, pavyzdžiui sankryžų kiekį numatytuose plotuose, santykinius kraujagyslių atkarpų ilgius ir kt., siekiant didesnio generuojamų raktų kardinalumo.

Šio darbo generuojamiems raktams reikalingoms reikšminėms koordinatėms išskirti *Matlab* kalba buvo sudaryta reikšminių koordinačių išskyrimo funkcija (*koordinates1.m*). Kadangi funkcijos įvestis yra juodai balta (0,1) verčių matrica, kurioje yra tik vieno pikselio pločio linijos, kraujagyslių susikirtimams ir pradžios/pabaigos taškams nustatyti naudojamos juodai baltos matematinės morfologijos funkcijos *branchpoints* ir *endpoints*. Visos koordinatės, pritaikius šias funkcijas ant piršto kraujagyslių tinklo pavaizduotos 2.4.2.1 pav.



2.4.2.1 pav. Reikšminių koordinačių išskyrimas

Kadangi sekimas gali būti atliekamas tik nuo konkretaus taško, tinklo galuose esantys *KPV* ir *KGV* yra patikrinamos ir sumažinamos iki 1 pikselio vertikalioje ašyje.

2.4.3. Pradinių verčių prieš pradedant sekimą parinkimas

Matlab realizuota *koordinates1.m* funkcija leidžia vartotojui pasirinkti, nuo kurios *KPV* turėtų būti atliekamas kontūro sekimas ir registruoja šią vertę kintamajame, kuris vėliau perduodamas kontūro sekimo algoritmui. Praktiškai realizuotoje sistemoje ši vertė galėtų būti laikoma sistemos parametru ir nuo jos parinkimo priklausytų generuojamo slapto rakto vertė.

Ši vertė galėtų būti:

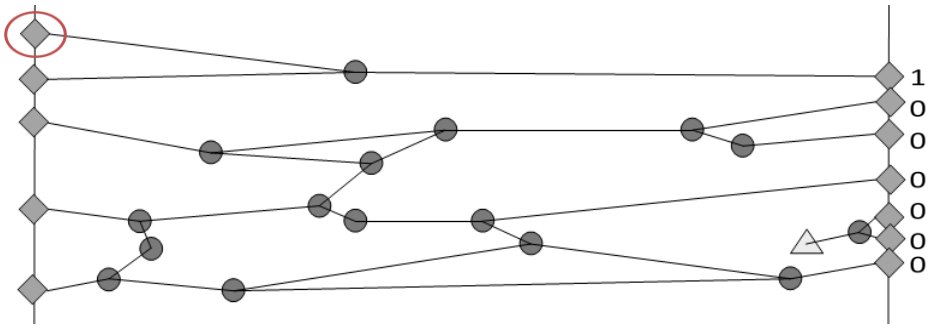
- Fiksuota: sekimas visada pradedamas nuo 1,2,..n *KPV*
- Kintama: parenkama pagal *KPV* taškų skaičių taikant tam tikras taisykles
- Dinamiškai priskiriama: priskiriama atlikus primityvią kontūro analizę ir pagal tai priskiriant generavimo pradžios tašką. Toks priskyrimas generavimo pradžios taško koordinatę padarytų ne tik sistemos, bet iš dalies ir biometrine charakteristika.
- Nurodoma vartotojo arba išskiriama iš vartotojo identifikatoriaus: taip vartotojas galėtų pasirinkti kokį kodą generuoti i to paties piršto kraujagyslių tinklo atvaizdo.

Šio darbo rėmuose testams naudojama vartotojo įvesta arba statinė pradinė kodo generavimo *KPV* vertė.

2.4.4. Siūlomi papildomi kontūro kodo generavimo metodai

Šio skyriaus tikslas yra apsvarstyti kelis papildomus kodo generavimo algoritmus. Visiems toliau aptariamiems algoritmams labai svarbus tinkamas pradinis atskaitos taškas. Hitachi piršto kraujagyslių nuskaitymo įrenginiuose piršto priekis atsiremia į atrama, todėl tikėtina, kad teisingai padėjus pirštą, atskaitos taškai būtų tinkami. Kita vertus teikės patikrinti, kokie piršto lokalizacijos metodai naudojami nuskaitymo įrenginiuose ir gali tekti papildomai nustatyti apdorojamo atvaizdo rėžius.

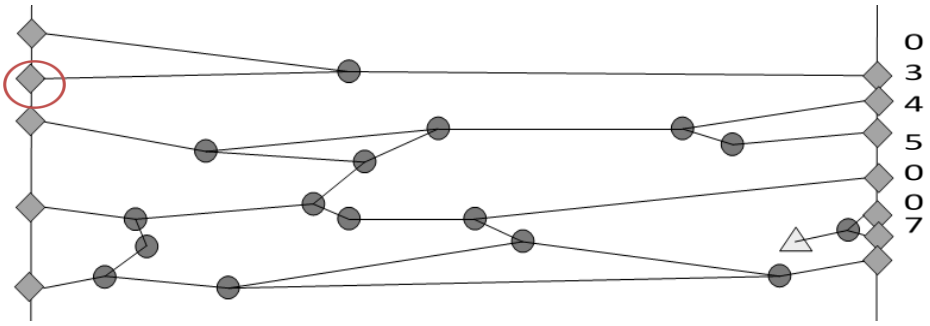
- Susijungiančių taškų metodas: šio metodo principas – tikrinti, ar galima iš vienos atvaizdo pusės pasiekti kitą keliaujant pasirinktomis venomis. Algoritmas leistų generuoti nesudėtingus raktu, galima būtų apdoroti paveikslus taip, kad smulkesnės venos būtų pašalinamos. Jei būtų naudojamos tik ryškiausios venos, algoritmui neturėtų daug įtakos smulkių trūkių atsiradimas ar panaikinimas naudojant morfologines atvaizdų apdorojimo funkcijas.



2.4.4.1 pav. Susijungiančių taškų kodo generavimo metodas

Susijungiančių taškų kodo generavimo metodo rezultatas būtų labai priklausomas nuo bet kokių trūkių ar susijungimų kraujagyslių atvaizde, todėl generuojamas rezultatas, tikėtina, kad kistų gana daug. Šis metodas netaikomas tolesniame darbe.

- Sankryžų skaičiaus metodas: šio metodo principas - skaičiuoti kiek „sankryžų“ reikia kirsti, norint nukeliauti nuo vienos atvaizdo pusės iki kitos. Šis algoritmas leidžia generuoti sudėtingesnius raktus, tačiau yra it daugiau galimybių suklysti. Pavyzdžiui jei vienas susikirtimas kartais būtų vertinamas kaip 2 „T“ formos sankryžos.



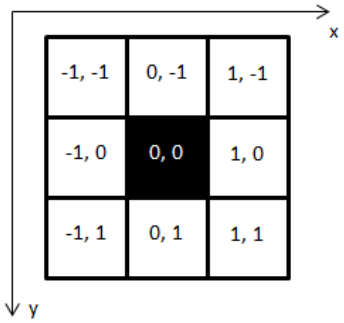
2.4.4.2 pav. Sankryžų skaičiuas kodo generavimo metodas

2.4.5. Kontūro sekimo funkcijos realizacija

Daugelyje iš numatomų naudoti kodo generavimo algoritmų remiamasi verčių „sekimu“ matricose. Kraujagyslių atvaizdas verčiamas dvimate [x,y] skaičių matrica, kur bet kurio taško (x,y) vertės yra 1 arba 0. Šis metodas dažnai taikomas vaizdų apdorojime linijų sekimui arba mašininiam „matymui“ (angl. „Computer Vision“) įgyvendinti. Taip pat šis metodas taikomas grafiniam labirintų sprendimui ir kt.

Darbui sukurtos kontūro sekimo *Matlab* funkcijos kodas pateikiamas 6.6 priede. Funkcijos įvestis yra dvimatė [x,y] verčių matrica (apdorotas kraujagyslių tinklas). Tinklas turi būti atvaizduotas 1 elemento pločio linijomis. Taip pat nurodomas matricos elementas nuo kurio pradedamas sekimas. Pradinis taškas gali būti bet kuri kraujagyslės pradžia, susikirtimas ar kitas matricos taškas, kurio vertė yra 0, darant prielaidą, kad naudojama matrica, kurioje kontūrai atvaizduojami juodai (0), o fonas yra baltas (1).

Pradedant nuo įvesties taško, gretimi elementai yra tikrinami nuo (0, -1) elemento pagal laikrodžio rodyklę. Elementų, kurių vertė yra 0 koordinatės registruojamos x,y verčių matricoje ir surastas elementas yra paverčiamas priešingu, kad išvengti pakartotinio jo registravimo atliekant kitą ciklo iteraciją.



2.4.5.1 pav. Matricos elementų išsidėstymas koordinačių ašyse

Funkcijos *konturo_sekimas.m* kvietimas, įvesties duomenys – kraujagyslių tinklo atvaizdas, paverstas juodai blatu paveikslu ir rezultatai pavaizduoti žemiau.

```
>> a=imread('base_sugadintas.png');
b = rgb2gray(a);
c = im2bw(b);
>> d=konturo_sekimas(c,24,36);
```

2.4.5.2 pav. Įvesties duomenų paruošimas *konturo_sekimas.m* kvietimas (*Matlab*)

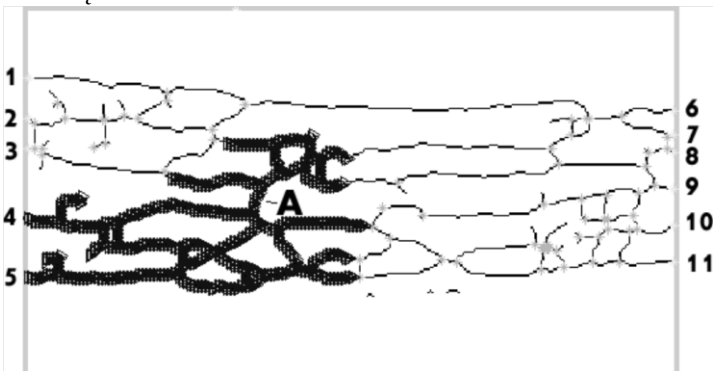
Kontūro sekimo funkcijos realizacija yra svarbus būsimo kodo generavimo parametras. Šioje kontūro sekimo realizacijoje yra atliekamas visų kontūro šakų sekimas vienu metu. Taip algoritmas „slenka“ per visas sankryžas *KGV* kryptimi. Šis funkcijos realizavimo aspektas padeda išvengti kontūro sekimo klaidų, jei jame atsiranda nedidelių nenukirptų atšakų, žiedų ir kitokių geometrinių nepastovumų.. Kontūras su sekamomis šakomis pavaizduotas 2.4.5.3 pav. Realizuota kontūro sekimo funkcija „slenka“ per kraujagyslių tinklą ir priklausomai nuo jo formos, sudėtingumo ir kitų savybių, pasiekia skirtingus kraujagyslių tinklo taškus (galus ar susikirtimus) skirtingais santykiniais laiko momentais. Išvestiniai kontūro sekimo funkcijos veikimo parametrai darbe naudojami nesudėtingam raktui generuoti.

2.4.5.3 pav. visų kontūro šakų sekimo vienu metu pavyzdys

Alternatyvi kontūro sekimo funkcija galėtų sekti tik pasirinktas kontūro šakas nuo pradžios iki pabaigos. Tokia kontūro sekimo funkcija galėtų veikti greičiau ir taip pat patikimai kaip visų krypčių sekimas sistemose, kuriose naudojami tam tikri raktų generavimo metodai. Vienos šakos kontūro sekimo funkcija galėtų būti papildyta ėjimo per sankryžas logika arba atsitiktinai rinktis ėjimo per sankryžas tinkle kelią.

2.4.6. Kontūro sekimo iteracijų skaičiaus metodas

Pagrindinis slapto rakto generavimo metodas, naudojamas tolesniame darbe yra vadinamas Kontūro sekimo iteracijų skaičiaus metodu. Metodo idėja - tam tikrų, iš anksto numatytų, verčių priskyrimas kiekvienam kontūro pradžios ir pabaigos taškui ir vertinimas, kada šiuos taškus pasiekia pasirinkta kontūro sekimo funkcija. Pavyzdyje (2.4.6.1 pav.) kiekvienam iš kraujagyslių tinklo galų priskiriamos skaitinės vertės nuo 1 iki 11. Pasirenkamas pradinis sekimo taškas (vertė 4) ir atliekamas sekimas. Pavaizduotas sekimo funkcijos rezultatas, kai pasiekiamas pirmasis „išėjimas“, atlikus 826 taškų kontūre sekimą.



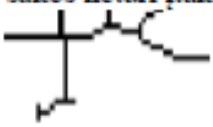
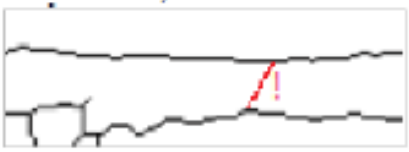
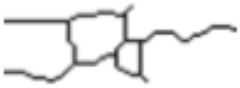
2.4.6.1 pav. Kraujagyslių tinklo kontūro sekimas pradedant nuo taško nr. 4.

- Kiekvienam pradžios ir pabaigos taškui priskirtos skaitinės vertės.
- Paryškinta sekama kontūro atkarpa po 826 kontūro sekimo algoritmo iteracijų.
- Kritinis kontūro taškas pažymėtas raide A.

Atlikus visą sekimo ciklą, metodo rezultatas – slaptas raktas, sudarytas iš skaičių 532111910678. Skaitmenys šiame skaičiuje yra lygūs po tam tikro sekimo iteracijų skaičiaus pasiekto tinklo įėjimo/išėjimo skaitinei vertei. Algoritmo generuojamas raktas priklausytų nuo įėjimams/išėjimams priskirtų pradinių verčių ir kontūro sekimo funkcijos realizacijos. Šiame pavyzdyje naudojama III. B skyriuje aprašyta kontūro sekimo funkcija. Dalis verčių, dėl to, kad jos pasiekiamos labai artimais laiko momentais ir, atsiradus netikslumams kontūro sudaryme (pavyzdžiui netiksliai atlikus piršto lokalizaciją), galėtų įtakoti galutinį rezultatą, gali būti atmetamos. Numatomas patikimas rakto ilgis galėtų būti apie 4-8 skaitmenys.

Šio metodo privalumas – santykinai maža paklaida, jei kraujagyslių tinkle yra nedidelių neatitikimų. Metodui reikšminės įtakos neturėtų linijų krypties ar vietos pasikeitimai, atsiradę pašaliniai prie pagrindinio sekamo tinklo neprisijungę elementai, žiedai, sudėtingos geometrinės formos kontūro viduje, atsišakojimai ir netiksliai nustatytos kraujagyslių sankryžų vietos. Metodui nereikalingi ir iš dalie nenaudingi nesusijungę kraujagyslių atsišakojimai, jie negeneruoja reikšminės informacijos, bet sekant tokius atsišakojimus sumažėja algoritmo greitaveika ir atsiranda papildomų paklaidų tikimybė. Daugiausiai neigiamos įtakos šiam metodui galėtų turėti netinkamai nustatyti (arba nenustatyti) kritiniai linijų susijungimai. Metodo generuojamo rakto vertė galėtų tapti netiksli, jeigu kontūre atsirastų trūkių, dėl kurių kai kurie pradžios arba pabaigos taškai taptų nepasiekiami arba pasiekiami po reikšmingai daugiau arba mažiau kontūro sekimo iteracijų. Pavyzdinio kritinio kontūro taško pavyzdys paveiksle pažymėtas simboliu A. Jei šios jungiančiosios kontūro dalies nebūtų, viršutinė kraujagyslių tinklo dalis būtų pasiekiama tik per kur kas tolesnį jungiamąjį tašką tarp išėjimų 8 ir 9 ir reikšmingai pakeistų galutinį generavimo rezultatą. Taip pat metodui neigiamos įtakos turėtų sudėtingas kraujagyslių tinklas kontūro galuose, ypač jei piršto lokalizacija būtų netiksli.

2.4.1 lentelė. „Kontūro sekimo iteracijų skaičiaus metodo“ privalumai ir trūkumai.

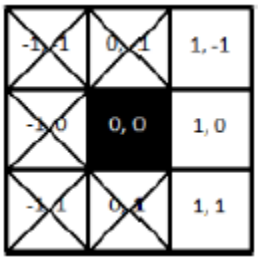
Privalumai	Trūkumai
Atskiros neprisijungusios tinklo šakos neturi įtakos rezultatui. 	Susijungimai arba trūkiai reikšminėse kraujagyslių atvaizdo tinklo vietose (pvz., tarp arti viena kitos esančių linijų) gali visiškai keisti rezultatą. 
Žiedai ir sudėtingi išsišakojimai kraujagyslių tinkle turi mažai įtakos rezultatui. 	

2.4.7. Vandens lašo metodas

Kontūro sekimo iteracijų skaičiaus ir kitų kontūro sekimo funkcija paremtų metodų veikimui naudojamas visas piršto kraujagyslių kontūras. Tokiems algoritmams įtakos galėtų turėti bet kokie tinkle atsiradę netikslumai. Priešingai nei daugiakrypčiai algoritmai, siūlomas „Vandens lašo metodas“ yra vienakryptis. Šiame metode naudojamas kraujagyslių kontūro sekimas vyksta tik išėjimo kryptimi ir algoritmui leidžiama sukti tik +/- 45 laipsnių kampu išėjimo link (2.4.7.1 pav.).

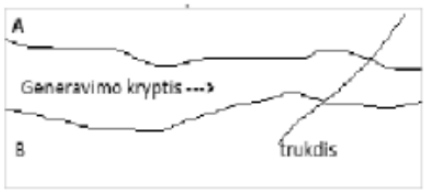
Toks algoritmas padėtų išvengti neigiamos tam tikra kryptimi atsiradusių netikslumų ar susijungimų/nesusijungimų reikšminėse kraujagyslių tinklo vietose įtakos galutiniam rezultatui, pavyzdžiui, sekant kontūrą, pavaizduotą 2.4.6.1 pav., nuo 1, 2, 3 arba 5 kairėje pusėje esančių pradžios taškų, reikšminis sujungimas A įtakos galutiniam rezultatui neturėtų.

Tačiau priklausomai nuo išpildymo būdo, galutinis vienakrypčio metodo generuojamo rakto ilgis galėtų būti trumpesnis nei naudojant daugiakrypčius generavimo metodus. Taip pat atliekant sekimą priešinga nei numatyta kryptimi, sekimo netikslumai galimai būtų didesni nei naudojant daugiakryptį kontūro sekimą.



2.4.7.1 pav. Galimos „Vandens lašo“ metode naudojamos kontūro sekimo funkcijos kryptys

2.4.2 lentelė. „Vandens lašo“ metodo privalumai ir trūkumai.

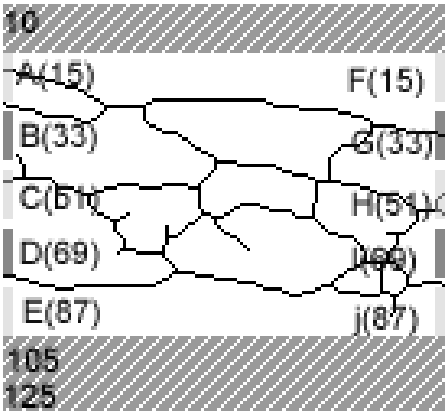
Privalumai	Trūkumai
Algoritmui įtakos turėtų tik tam tikra kryptimi atsiradę netikslumai. 	Algoritmas negalėtų įveikti T formos arba tinklo vietų, kur linijos sukasi atgal ir negeneruotų dalies rezultato. 

2.4.8. Vertinimo sričių nustatymas

Dėl piršto kraujagyslių atvaizdų nuskaitymo ir tinklo išskyrimo metodų veikimo specifikos, kraujagyslių atvaizdai ties apdorojamo atvaizdo kraštais gali būti netikslūs. Kontūro sekimo metodai būtų laibai lengvai įtakojami nuskaitytuose atvaizduose atsiradusių netikslumų, jeigu taikant Kontūro sekimo iteracijų skaičiaus metodą būtų remiamasi tik vertėmis, priskirtomis kraujagyslių tinklo *KPV* ir *KGV* taškams.

Siekiant šiek sumažinti „Kontūro sekimo iteracijų skaičiaus“ metodo *KAT* ir šiek tiek suabstraktinti generavimo procesą analizuojamo atvaizdo pradinėje ir galinėje srityse vertės yra priskiriamos ne patiems kraujagyslių įėjimams arba išėjimams, bet santykinėms sritims, kurių skaičius ir nevertinami tarpai tarp sričių tampa sistemos parametru.

Sekamo kontūro verčių zonos, kai naudojama 10 vertinimo sričių pavaizduotos 2.4.8.1 paveiksle. Kontūro sekimo metodui atliekant rakto generavimą, vertės raktui priskiriamos pagal sričiai priskirtą vertę ir tik pirmą kartą pasiekus tam tikrą vertinimo sritį.



2.4.8.1 pav. Vertinimo sričių sudarymas

2.4.9. Klaidų taisymas

Atliekant atvaizdų apdorojimą, triukšmai, nuskaitymo klaidos ar klaidos, atsiradusios dėl požymių išskyrimo metodų veikimo specifikos gali būti tiesiog lyginamos su atpažinimo klaidomis, todėl šioms klaidoms aptikti ir taisyti galima būtų taikyti adaptuotus klaidų taisymo metodus. Šiame darbe detalūs galimi klaidų korekcijos būdai generuojant slaptą raktą nebuvo nagrinėjami, tačiau siūlomas papildomas klaidų korekcijos žingsnis kuris galėtų nustatyti ir ištaisyti dalį testavimo metu pastebėtų klaidų. Dvi pagrindinės klaidų atsiradimo priežastys, pastebėtos bandymo metu buvo:

- klaidos dėl kritinių kraujagyslių tinklo taškų, aptartų „Kontūro sekimo iteracijų metodo“ aprašyme. Tokios klaidos generuojamą kodą keitė į visiškai priešingą vertę, pvz.
- klaidos dėl taškų kontūre pasiekimo kai iteracijų skaičius labai artimas. Šios klaidos kai kuriais atvejais tik sukeisdavo vietomis keletą generuojamo kodo skaitmenų, pvz.: 2653 -> 2563.

Klaidoms dėl artimo taškų pasiekimo taisyti, „Kontūro sekimo iteracijų metodas“ galėtų būti papildytas funkcija, nustatančia ar taškai buvo pasiekti per labai artimą kontūro sekimo iteracijų skaičių ir tai nustačius priskiriančia visuomet fiksuotą vertę, pvz. mažesnės vertės verčių zonos reikšmę. Tokio klaidų taisymo metodo veikimas leistų generuoti vienodą raktą visada, net jei du artimi generavimo verčių taškai būtų pasiekti su nedideliu iteracijų skaičiaus skirtumu. Klaidų taisymo metodo veikimas, kai verčių zonos 3 ir 6 yra pasiekiamos su nedideliu iteracijų skirtumu iliustruotas 2.4.9.1 pav.

k = 2361754	jei	*pos2<pos3*	NOP
k‘ = 2631754	jei	pos2<pos3	*k‘=2361754*

2.4.9.1 pav. Generuojamų kodo verčių taisymo metodas

2.5. Tiesioginio slaptų raktų generavimo iš piršto kraujagyslių tinklo metodo apibendrinimas

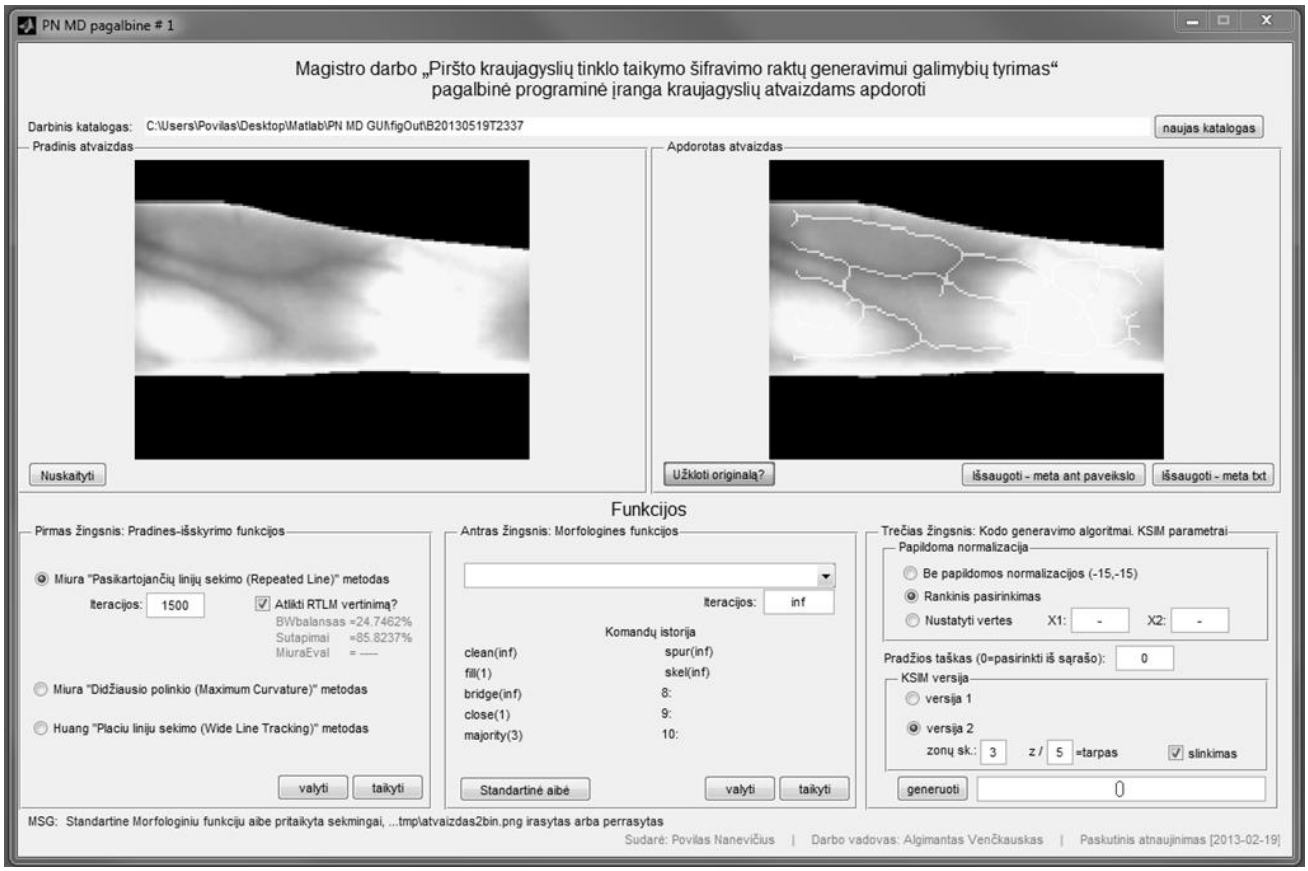
Skyriuje aptariamas slapto rakto generavimo iš piršto kraujagyslių tinklo taikant kontūro sekimo iteracijų skaičiavimą pirmiausia yra skirtas slaptiems raktams stabiliai generuoti iš piršto kraujagyslių tinklo. Toks metodas galėtų būti pritaikytas tiek biometrinei kriptografijai, tiek tam tikriems autentifikavimo sistemų aspektams pakeisti. Pagrindiniai kodo generavimo žingsniai, realizuoti šiame darbe ir išbandomi bandymų dalyje yra:

- Pirminis požymių išskyrimas, pavyzdžiui taikant *Miura ir kt.* „Pasikartojančių linijų sekimo“ metodą
- Morfologinių funkcijų aibės taikymas siekiant išvalyti, pataisyti ir susiaurinti atvaizdą iki vieno pikselio pločio tinklo
- Rakto generavimas – generavimo ploto papildomas lokalizavimas, verčių zonų sudarymas ir verčių priskyrimas, kodo generavimas taikant „Kontūro sekimo iteracijų skaičiaus“ metodą

3. TIESIOGINIO SLAPTŲ RAKTŲ GENERAVIMO IŠ PIRŠTO KRAUJAGYSLIŲ TINKLO METODO BANDYMAI

3.1. Grafinės vartotojo sąsajos raktų generavimo bandymams sudarymas

Tiesioginio raktų generavimo iš pirštų kraujagyslių tinklo bandymams, pirminio apdorojimo metodams ir morfologinėms funkcijoms tirti ir atvaizduoti darbe buvo sudaryta grafinė vartotojo sąsaja. Ši sąsaja išpildyta *Matlab* kalba ir pavaizduota 3.1.1 pav.



3.1.1 pav. Grafinė vartotojo sąsaja

Pagrindinės vartotojo sąsajos funkcijos yra suskirstytos į metodo blokinės schemos dalis atitinkančias skiltis ir yra tokios:

- Įvesties paveikslo nuskaitymas iš laikmenos (vietoje atvaizdo nuskaitymo iš biometrinės aparatinės įrangos)

Pirminio apdorojimo skiltyje:

- Pasirinktos pirminio apdorojimo funkcijos pritaikymas. Sąsajoje galima pasirinkti vieną iš trijų autoriaus *Bram Ton* realizuotų pirminių kraujagyslių tinklo išskyrimo metodų: *Miura ir kt.* „Pasikartojančio linijų sekimo“, *Miura ir kt.* „Maksimalaus linkio“ ir *Huang ir kt.* „Plačių linijų sekimo“ metodą.
- Pasirinkus taikyti *Miura ir kt.* „Pasikartojančių linijų sekimo“ metodą, galima papildoma metodo tikslumo įvertinimo funkcija.

Matematinės morfologijos funkcijų skiltyje:

- Matematinės morfologijos pavienių (iki 10) funkcijų taikymas
- Standartinės matematinės morfologijos funkcijų aibės taikymas

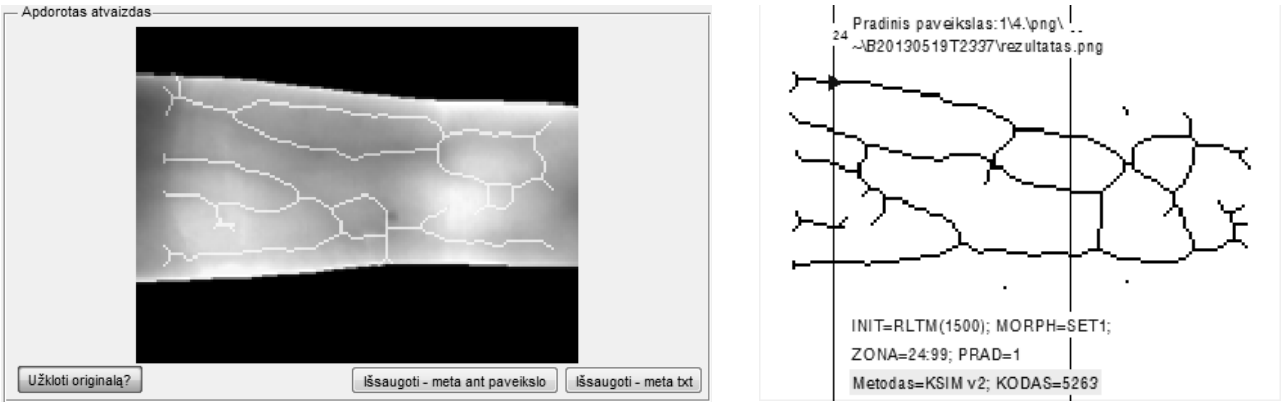
Kodo generavimo skiltyje:

- Papildomos normalizacijos atlikimas taikant rankinį generavimo ploto apibrėžimą, nustatytas koordinates arba be papildomo normalizacijos.

- Kodo generavimo pradžios taško nustatymas. Jei taškas nepasirenkamas prieš pradedant generavimą, vartotojui pateikiamas atvaizdas ir dialogas, kuriame galima nustatyti pirminį generacijos tašką.
- „Kontūro sekimo iteracijų skaičiaus“ metodo versijos pasirinkimas ir parametrų perdavimas *KSIM* algoritmui.
- Papildomas *KSIM* metodo atvaizdavimas galimas taikant visų sekamo kontūro taškų sekimo atvaizdavimą.

Bet kurioje vartotojo sąsajos stadijoje galima naudoti pradinio ir apdorojimo rezultato atvaizdų parodymo vienoje plokštumoje galimybę. Taip galima įvertinti ar raikomos funkcijos veikia tiksliai.

Svarbi grafinės sąsajos savybė – galimybė išsaugoti apdorojimo rezultatą ir tarpinius atvaizdus, atvaizde pažymint visus sąsajoje naudotus kintamuosius. Grafinės tarpinis rezultatas – pradinis atvaizdas užklotas išskirtu kraujagyslių tinklo atvaizdu pateikiamas 3.1.2 pav. a), o galutinis išsaugoto apdorojimo rezultato pavyzdys pateikiamas 3.1.2 pav. b) pav.



(a) (b)

3.1.2 pav. Tarpinis (a) ir galutinis (b) slapto rakto generavimo proceso atvaizdai

3.2. Pirminio tinklo išskyrimo funkcijos pasirinkimas

Iš trijų išbandytų pirminio kraujagyslių tinklo išskyrimo metodų buvo nutarta pasirinkti ir tolimesniame darbe naudoti *Miura ir kt.* „Pasikartojančio linijų sekimo“ metodą. Šis metodas, taikant nuo 1500 iki 3000 iteracijų (atsitiktinių linijų sekimų), ir *r=1, W=17* pradinius parametrus generavo panašiausius vienas kitam kraujagyslių tinklo atvaizdus ir vertinant vizualiai, geriausiai išskyrė kraujagyslių kontūrus. Kiti metodai, nors tinkami palyginimo operacijoms, naudoti su „Kontūro sekimo iteracijų skaičiaus“ kodo generavimo metodu buvo netinkami arba nepatogūs dėl to, kad negalėjo užpildyti trūkių tam tikrose kontūro vietos arba per daug suabstraktino kraujagyslių tinklą.

Visų trijų vartotojo sąsajoje galimų naudoti metodų įvertinimas pateikiamas 6.2 priede.

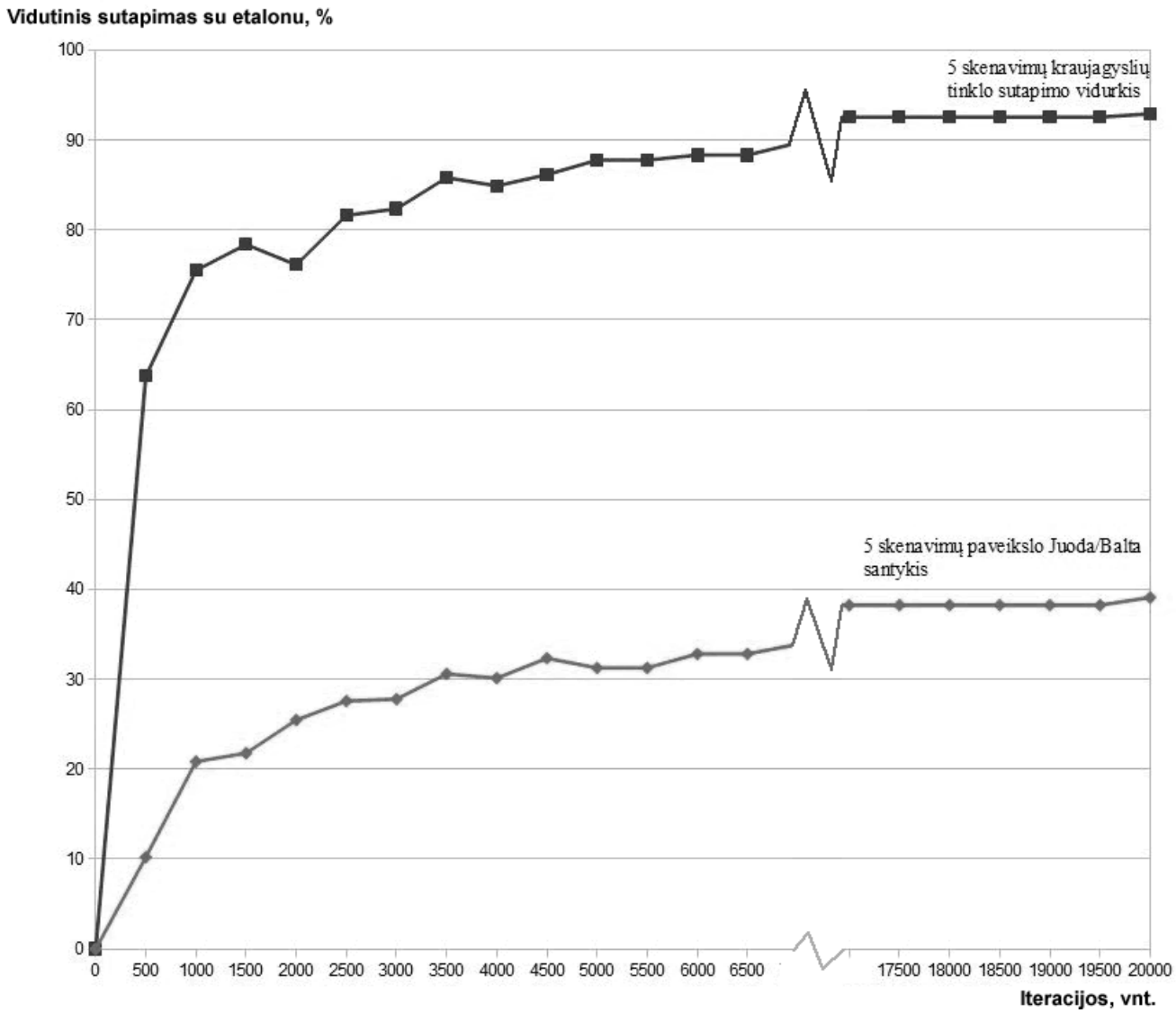
3.3. *Miura ir kt.* „Pasikartojančių linijų sekimo“ metodo iteracijų skaičiaus įvertinimas

Miura ir kt. „Pasikartojančių linijų sekimo“ metodas yra iš esmės atsitiktinis. Šiame metode linijos sekamos pradedant nuo atsitiktinių taškų atvaizde ir sekimas tęsiamas tol, kol randamas tamsus kraujagyslės centras, apsuptas tolygiai šviesesnio fono. Jei sekimas atliekamas tik vieną kartą, atsiranda tikimybė, kad ne visi kraujagyslių taškai bus išskirti. Praktikoje atliekant sekimą tik vieną kartą, jei atsitiktinai pasirinktas nepatogus pradinis sekimo taškas, gali būti identifikuota tik labai maža dalis visų kraujagyslių.

Siekiant nustatyti patikimą „Pasikartojančio linijų sekimo“ metodo iteracijų skaičių buvo atliktas bandymas naudojant 389x189 pradinį atvaizdą ir atliekant pakartotinius pirminio kraujagyslių tinklo išskyrimo ciklus penkis kartus iš eilės.

Kiekvieno pirminio kraujagyslių išskyrimo tarpinis rezultatas buvo saugomas ir atlikus 5 nuskaitymus, lyginamas su papildomu etaloniniu *Miura ir kt.* „Pasikartojančio linijų sekimo metodo“ atvaizdu. Išskirtų kraujagyslių taškų sutapimo su kraujagyslių taškais etaloniniame atvaizde

buvo naudojamas metodo iteracijų skaičiaus pakankamumo vertinimui. Taip pat buvo atliekamas santykio tarp kraujagyslių kiekio kiekviename tarpiniame kraujagyslių atvaizde ir bendro atvaizdo dydžio siekiant nustatyti ar atliekant daugiau *Miura* ir kt. PLSM iteracijų nėra per daug plečiamos jau nustatytos kraujagyslių ribos. Šio bandymo rezultatai pavaizduoti 3.3.1 pav. pateikiamame grafike.



3.3.1 pav. *Miura ir kt.* „Pasikartojančių linijų sekimo“ metodo įvertinimas

Įvertinus *Miura ir kt.* „Pasikartojančių linijų sekimo“ metodo priklausomybę nuo naudojamo sekimo pakartojimų skaičiaus nustatyta, kad bandymams naudotą 389x189 pikselių dydžio paveikslą apdorojant šiuo metodu reikia naudoti bent 3000 atsitiktinių linijų sekimų. Šia dydis yra mažesnis naudojant kitokius pradinius atvaizdus.

Atliekant daugiau *Miura ir kt.* „Pasikartojančių linijų sekimo“ metodo iteracijų kyla ir bendras juoda/balta paveikslo santykis. Taip iš dalies yra dėl to, kad metodas išskiria daugiau kraujagyslių ir užpildo kai kuriuos susidariusius tarpus. Juoda/Balta balansas, kuris lygus nustatytiems kraujagyslių taškams auga proporcingai augant iteracijų skaičiui ir bendram atvaizdų sutapimui. Tai nurodo, kad didinant atsitiktinių linijų sekimo skaičių neatsiranda jokių anomalių paklaidų dėl linijų sekimo ne per tikrąjį kraujagyslių tinklą, arba šios paklaidos yra minimalios.

Miura ir kt. „Pasikartojančio linijų sekimo“ metodo veikimas yra ganėtinai lėtas, todėl nors didesnis iteracijų skaičius gali lemti šiek tiek didesnį tarpinio kraujagyslių atvaizdo sudarymo tikslumą, laikas, reikalingas apdorojimui išauga ženkliai.

3.4. Morfologinių funkcijų aibės sudarymas

Morfologinių funkcijų aibė šiame darbe siūlomame „Kontūro sekimo iteracijų skaičiaus“ metode slaptiems raktams iš piršo kraujagyslių tinklo generuoti reikalinga tam, kad iš tarpinio kraujagyslių atvaizdo, gauto pritaikius vieną iš pirminio apdorojimo metodų būtų sudarytas vieno pikselio pločio kraujagyslių tinklo atvaizdas.

Morfologinių funkcijų pritaikymas priklauso nuo daugelio sistemos aspektų, tokių kaip siekiamas paveikslo suabstraktinimo lygis, kraujagyslių atšakų pašalinimo poreikis, norimas tuščių plotų pašalinimo lygis ar neprisijungusių elementų pašalinimas. Morfologinės aibės pasirinkimas tirtas taikant kelis pagrindinius uždavinius:

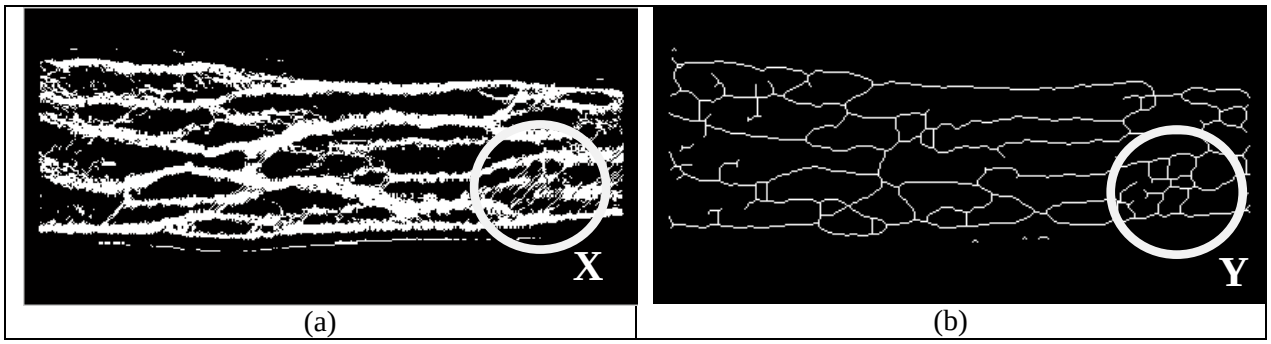
- Atvaizdo išvalymas nuo galimų triukšmų.
- Galimai netikslių pirminio išskyrimo algoritmo aspektų pataisymas.
- Sekimui tinkamo tinklo sudarymas nenukrypstant nuo pradinių kraujagyslių padėčių.

Tyrimams atlikti buvo naudojamas jau aptarta *Matlab* kalba realizuota pagalbine vartotojo sąsaja ir taikant skirtingas morfologinių funkcijų aibes be vartotojo įsikišimo, o po to peržiūrint gautus rezultatus. Galutinė pasirinkta morfologinių funkcijų aibė ir funkcijų pasirinkimo priežastys aprašomos toliau:

- Pavienių nereikalingų pikselių pašalinimas: pavieniai prie nieko neprisijungę taškai greičiausiai nėra susiję su kraujagyslių tinklu, tai atvaizde dėl vienokių ar kitokių priežasčių atsiradęs triukšmas. Šiam triukšmui pažalinti *Matlab Clean* morfologinė funkcija su *inf* pradiniu parametru. Toks funkcijos taikymas iš atvaizdo pašalina visus pavienius taškus. Pavieniai taškai atvaizde galėtų atsirasti dėl to, kad atsitiktinai pradedamas kontūro sekimas ne nuo kraujagyslės, bet pataikoma į atvaizdo vietą, kur *Miura ir kt.* „Pasikartojančių linijų sekimo“ pirminiam apdorojimo metodui nepavyksta aptikti reikiamus kriterijus atitinkančio kraujagyslės slėnio.
- Nedidelių neužpildytų plotų užpildymas: priklausomai nuo pasirinktos pirminio atvaizdo apdorojimo funkcijos atvaizde gali susidaryti nedidelių neužpildytų plotų. Tokie plotai galėtų atsirasti *Miura ir kt.* „Pasikartojančių linijų sekimo“ metodui sekant kraujagyslės slėnį šiek tiek skirtingomis kryptimis. Tokie atsiradę neužpildyti ne daugiau kaip vieno pikselio ploto taškai pašalinami taikant morfologinę užpildymo (*fill[1]*) funkciją.
- Nedidelių trūkių sujungimas: dėl atvaizdo ryškumo anomalijų, pavyzdžiui apšvietimo normalizacijos netikslumų, atvaizde gali atsirasti kraujagyslių trūkių. Tokie trūkiai pakeistų bendrą kraujagyslių tinklo geometriją ir turėtų reikšmingos įtakos galutiniam generuojamam raktui. Nedideliems trūkiams, tikėtina atsiradusiems dėl nuskaitymo netikslumų pašalinti naudojama morfologinė susijungimo (*bridge[inf]*) funkcija.
- Morfologinis uždarymas: šis metodas pasirinktas ir taikomas tam, kad būtų sušvelninti kraujagyslių krypties posūkiai. Uždarymo operacija praplečia kraujagyslių susijungimus vietose, kur jie kitaip būtų labai siauri. Ši funkcija taikoma su parametru 1, kuris nurodo, kad tik nedideli susijungimai turėtų būti praplatinti.
- Kraujagyslių tinklo suabstraktinimas: siekiant kad tinklas būtų patogesnis apdoroti it būtų pašalinami anksčiau neišvardinti tinklo netikslumai, taikoma morfologinė statistinių blokų palyginimo principu veikianti *majority* funkcija. Šiai funkcijai perduodamas parametras, kurio vertė lygi 3. Šis parametras nurodo, kad statistinis elementų vertinimas yra atliekamas 3x3 pikselių dydžio atvaizdo dalyse.
- Neprisijungusių šakų šalinimas: kadangi raktui generuoti skirto „Kontūro sekimo iteracijų skaičiaus“ metodo greitaveikai ir tikslumui neigiamos įtakos gali turėti prie nieko kito neprisijungusios atšakos, dalis tokių atšakų yra pašalinama taikant morfologinę *spur[inf]* funkciją. Šių šakų pašalinimas nesumažina pasirinkto metodo generuojamų raktų kardinalumo, bet taikant kitokius generavimo metodus toks pašalinimas gali nebūti tinkamas.
- Vieno pikselio pločio tinklo sudarymas: slapto rakto generavimas „Kontūro sekimo iteracijų skaičiaus“ metodo veikime pagrįstas tik vieno pikselio pločio linijos sekimu, todėl kraujagyslių tinklas yra sutraukiamas iki ploniausio įmanomo tinklo. Šio veiksmo metu

prarandama dalis iš biometrinės charakteristikos gautos informacijos, tačiau prarasta informacija bet kuriuo atveju pasirinktame raktų generavimo metode nebūtų vertinama.

Išvardintų funkcijų atlikimo eilės tvarka yra svarbi siekiant gauti norimą atvaizdą. Paveiksle 3.4.1 pavaizduotas pirminio *Miura ir kt.* „Pasikartojančio linijų sekimo“ metodu su 3000 iteracijų apdorotas kraujagyslių tinklo atvaizdas (a) ir išvardintomis morfologinėmis funkcijomis apdorotas atvaizdas (b).



3.4.1 pav. Morfologinio apdorojimo pavyzdys

Dėl triukšmo (a) atvaizde, tokios sritys, kaip X neturėtų būti vertinamo kodo generavime. Nepaisant to, kad morfologinėmis funkcijomis apdorotame atvaizde sritys yra kur kas aiškesnės nei pradiniame atvaizde - tai daug triukšmo įtakota sritis. Tokių sričių atsiradimas generavimui pasirinktos atkarpos viduje būtų iš dalies ignoruojamas rakto generavimo metodo, tačiau šių sričių atsiradimas apdorojimo sričių kraštuose turėtų daug neigiamos įtakos metodo generuojamiems raktams.

3.5. Pirštų kraujagyslių atvaizdų duomenų bazės aprašas ir pritaikymas

Tyrimams darbe buvo pasirinkta naudoti Honkongo politechnikos universiteto piršto kraujagyslių atvaizdų duomenų bazė [***36***]. Ši duomenų bazė sudaryta iš piršto kraujagyslių ir piršto paviršiaus atvaizdų, surinktų iš vyrų ir moterų savanorių. Duomenų bazė daugiausia surinkta tarp 2009-2010 metų naudojant bekontaktį piršto biometrinių savybių skenavimo įrenginį Honkongo Politechnikos Universiteto studentų miestelyje. Bendras atvaizdų skaičius duomenų bazėje yra 6264 atvaizdai, surinkti iš 156 individų. Pradiniai atvaizdai yra pateikti **.bmp* formatu. Daugelis (93%) biometrines savybes duomenų bazei pateikusių žmonių yra jaunesni nei 30 metų. Duomenų bazėje saugomi atvaizdai buvo gauti per dvi atsiras savybių nuskaitymo sesijas, tarp kurių minimalus laiko tarpas buvo vienas mėnuo, o maksimalus laiko tarpas – šeši mėnesiai. Vidutinis laikas tarp dviejų savybių surinkimo sesijų buvo 66,8 dienos. Per kiekvieną iš sesijų kiekvienas individas pateikė po 6 kairiosios rankos rodomojo ir vidurinio pirštų atvaizdus. Kiekvienos sesijos metu buvo nuskaityta po 12 piršto kraujagyslių tinklo atvaizdų ir 12 piršto tekstūros atvaizdų [***36***].

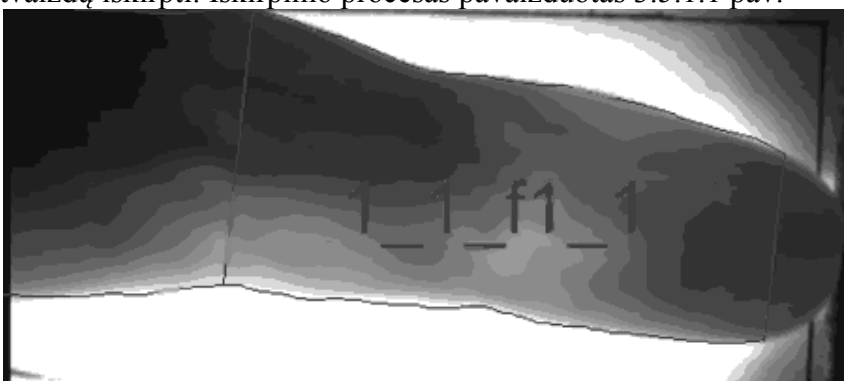
Bandymams šiame darbe buvo gauta ir pritaikyta dalis Honkongo politechnikos universiteto duomenų bazės, kurią sudarė dešimties individų kairiosios rankos rodomojo ir vidurinio pirštų atvaizdai dalis. Kiekvieno iš dešimties individų kiekvieno iš pirštų skenavimas buvo atliktas per dvi sesijas, taigi bandymui iš viso naudota maksimali 240 pradinių piršto kraujagyslių atvaizdų duomenų bazė. Kai kuriems bandymams buvo naudojama tik dalis šios duomenų bazės.

Duomenų bazėje pateikiamų atvaizdų pradinis dydis yra 513x256 pikseliai.

3.5.1. Papildoma normalizacija

Kadangi atvaizdai duomenų bazei buvo surinkti naudojant bekontaktį skaitytuvą, daugelio atvaizdų pasukimo kampas ir pastūmimas yra labai nevienodas. Darbe nagrinėjamo metodo veikimui labai svarbus tikslus generavimo ribų apibrėžimas, todėl prieš generuojant slaptus raktus, duomenų bazėje pateikti paveikslai buvo papildomai normalizuoti taikant pusiau automatinį normalizacijos metodą. Kiekvieno piršto atvaizdams buvo rankiniu būdu sukurtos piršto konkūro, kuriame

numatoma atlikti kodo generavimą, kaukės. Šios kaukės panaudotos vienodai atkarpai iš visų 12 kiekvieno piršto atvaizdų iškirpti. Iškirpimo procesas pavaizduotas 3.5.1.1 pav.



3.5.11 pav. Generavimo ploto paveiksle išskyrimas

Apdorotų atvaizdų (iškerpamų atkarpų) dydis sudarytoje modifikuotoje duomenų bazėje tampa 330x250 pikselių. Kintamas atvaizdo fonas pakeičiamas vienspalviu juodu fonu. Iškirptų atkarpų viršutinis kairysis kampas sulyginamas su *x=0* ir *y=23* koordinatėmis fono atžvilgiu.

3.6. Kontūro sekimo iteracijų skaičiaus metodo testavimas

3.6.1. Bandymo parametrai ir eiga

Siekiant įvertinti siūlomo „Kontūro sekimo iteracijų“ skaičiau metodo kiekybinius parametrus *Matlab* kalba buvo parašytas algoritmas, kuris atlieka vartotojo nurodytų pradinių atvaizdų, perskaitomų iš atvaizdų duomenų bazės, apdorojimą. Algoritmas atlieka visus 2.4.9.1 pav. pavaizduotus ir darbe realizuotus rakto generavimo metodo žingsnius:

- Papildomai normalizuoto atvaizdo nuskaitymą iš duomenų bazės (vietoje tiesioginio biometrinės savybės skaitymo). Naudojamų atvaizdų dydis yra 330x250 pikselių.
- Pirminį požymių išskyrimą. Šiuose bandymuose naudojamas *Miura ir kt.* „Pasikartojančio linijų sekimo“ metodas su 1500 kontūro sekimo iteracijų, r=1 ir W=17 parametrais. Taikant pirminę apdorojimo funkciją su nurodytais parametrais gaunamas vidutinis 82,52% kraujagyslių tinklo sutapimas ir vidutinis 25,95% atvaizdų juoda/balta balansas lyginant du iš eilės nuskaitytus atvaizdus su etaloniniu atvaizdu pagal 3.3 skyriuje pateiktą palyginimo metodą. Siekiant pagreitinti pirminį požymių išskyrimą, pradinis atvaizdas vertinimo metu yra sumažinamas iki pusės savo pradinio dydžio.
- Morfologinių funkcijų taikymą. Naudojama standartinė 3.4 skyriuje aprašoma morfologinių funkcijų aibė.
- Generavimo ploto lokalizavimą. Bandymai atliekami su standartine (-15,-15) lokalizacija arba su vartotojo pateiktomis lokalizacijos vertėmis. Vartotojas nustato lokalizavimo taškus ir įrašo juos į pirštų duomenų bazę. Vienoda lokalizacija atliekama visiems tos pašios rankoms tiems patiems pirštams.
- Verčių zonos sudarymą ir verčių priskyrimą zonoms. Bandymuose taikoma „3/5“ verčių zonos konfigūracija. Abiejuose atvaizdo pusėse atmetami vertikalūs plotai, kuriuose nėra kraujagyslių tinklo. Kiekviena likusi atvaizdo pusė padalinama į tris vertinamąsias zonas, tarp kurių paliekami $\frac{1}{5}$ zonos dydžio tarpai, kuriuose vertinimas neatliekamas. Verčių zonoms priskiriamos skaitinės vertės nuo 1 iki 6. Bandyme Nr. 5 naudojama „15/3“ verčių zonų konfigūracija.
- Kontūro sekimą taikant „Kontūro sekimo iteracijų skaičiaus“ metodą. Metodas visuomet generuoja kodą pradedant nuo kairiojoje pusėje esančio paties viršutinio kraujagyslių tinklo įėjimo.
- Apdorotas atvaizdas su visais taikytais parametrais ir sugeneruoto kodo verte yra įrašomas į išvesties atvaizdų duomenų bazę, sugeneruotas raktas yra įrašomas į atskirą bandymo sugeneruotų raktus saugantį duomenų failą.

Gauti kodai vertinami skaičiuojant metodo *KAT, KPT, BKT ir* vidutinę sugeneruotų raktų *Shannon* entropiją *H(X).*

$$H = -\sum_{i} p_i \log_b p_i \qquad (3.6.\text{Error! Bookmark not defined.})$$

KAT, KPT ir *BKT* yra standartiniai skaitiniai kriterijai biometrinėms sistemoms vertinti. Entropijos matas įvedamas tam, kad atvaizduoti generuojamų raktų kardinalumo kitimą.

3.6.2. Bandymas Nr.1: „Kontūro sekimo iteracijų metodo“ testas

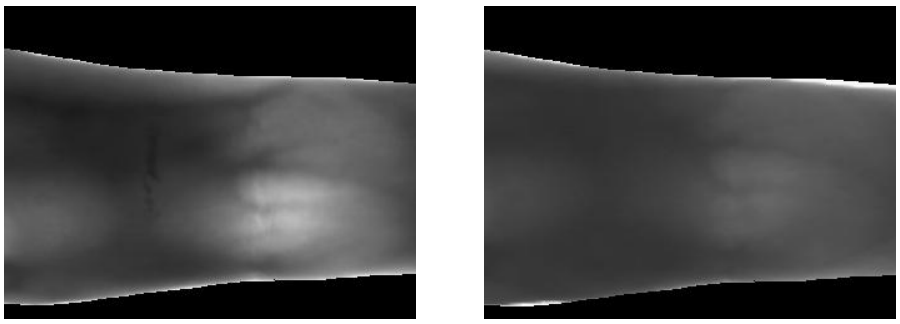
Šiame teste raktai generuojami iš nuskaityto normalizuoto ir papildomai lokalizuoto atvaizdo, tačiau netaikoma antrinė generavimo srities lokalizacija. Generavimas atliekamas su visais duomenų bazėje esančiais pirštų atvaizdams (iš viso 240 atvaizdų).

Metodo bandymo metu gautos tokios pagrindinės skaitinės vertės:

3.6.1 lentelė. Bandymo rezultatai Nr.1

Kriterijus	Rezultatas
KAT (FRR)	61,25%
KPT (FAR)	2,22%
BKT (EER)	63,48%
H(X)	2,04

Rezultatuose aiškiai pastebima, kad dalis duomenų bazėje esančių pirštų labai skiriasi tarpusavyje. Tai – atvaizdo sudarymo trūkumai atsiradę dėl aparatinės įrangos trūkumų, apšvietimo normalizacijos ir kitų priežasčių (3.6.2.1 pav.).



(a) (b)

3.6.2.1 pav. Apdorojamų atvaizdų skirtumai

3.6.3. Bandymas Nr.2: KSIM testas taikant papildomą lokalizaciją

Teste raktai generuojami tik iš pasirinktos atvaizdo srities. Ši sritis visuomet tokia pati tam pačiam pirštui, tašiau gali keistis skirtingiems pirštams. Generavimo sritys parinktos kiekvienam iš pirštų individualiai. Bandymas atliekamas su pilna pirštų duomenų baze (iš viso 240 atvaizdų).

Metodo bandymo metu gautos tokios pagrindinės skaitinės vertės:

3.6.2 lentelė. Bandymo rezultatai Nr.2

Kriterijus	Rezultatas
KAT (FRR)	53,75%
KPT (FAR)	3,29%
BKT (EER)	57,04%
H(X)	1,97

Apribojus generavimo srities plotą gaunami šiek tiek geresni rezultatai, nes iš atvaizdo pašalinam dalis kraštinių netikslių atvaizdo sričių. Nors generavimo sritis sumažinama, taigi ir biometrinių duomenų kiekis įvesties atvaizde sumažinamas, entropijos vertė pasikeičia nežymiai.

3.6.4. Bandymas Nr.3: KSIM testas su pataisytais kraujagyslių tinklais

Daugelis klaidų generuojant slaptą rakta atsiranda dėl to, kad pradiniame atvaizde ir sudarytame kraujagyslių tinkle atsiranda netikslumų, kuriuos iš dalies galėtų pašalinti geresnė aparatinė ar programinė atvaizdų apdorojimo įranga. Siekiant išbandyti kaip „Kontūro sekimo iteracijų skaičiaus“ metodas apdoroja geresnės kokybės atvaizdus, iš bendros pirštų kraujagyslių atvaizdų duomenų bazės buvo pasirinkta 10 pirštų (120 atvaizdų), iš kurių sudarytame tinkle rankiniu būdu buvo pataisyti kai kurie, galimai dėl aparatinės įrangos veikimo ar pirminio atvaizdų apdorojimo atsiradę netikslumai. Daugelyje apdorotų atvaizdų reikėjo tik pridėto arba pašalinti vieną ar keletą linijų kritinėse atvaizdo vietose. Iš 120 apdorotų atvaizdų papildomai modifikuoti 57 atvaizdai.

Bandymas atliktas du kartus: pirmąjį karta sugeneruoti raktai iš netaisytų atvaizdų, antrąjį kartą – pataisius dalį atvaizdų, kurių kodas buvo netikslus. Bandymo rezultatai pateikti 3.6.4.1 lentelėje.

3.6.3 lentelė. Bandymo rezultatai Nr.3

Kriterijus	Rezultatas prieš pataisymus	Rezultatas pataisius atvaizdus
KAT (FRR)	46,667%	13,333%
KPT (FAR)	4,250%	2,417%
BKT (EER)	50,917%	15,750%
H(X)	1,919	2,039

3.6.5. Bandymas Nr.4: KSIM testas su vienu iš pirštų generuojant kodą 10 kartų iš eilės

Bandymui pasirinktas vienas iš pirštų, kurio atvaizdų kokybė buvo santykinai gera, papildomas atvaizdų taisymas šiame bandyme netaikomas. *KPT* parametras neskaičiuojamas, nes bandymo imtis – vienas pirštas. Iš viso atliekama 10 generavimo serijų po 12 piršto atvaizdų kiekvienoje serijoje. Taigi bendras sugeneruotų raktų skaičius yra 120.

3.6.4 lentelė. Bandymo rezultatai Nr.4

Kriterijus	Rezultatas
KAT (FRR)	25%
KPT (FAR)	neskaičiuojamas
BKT (EER)	25%
H(X)	1,971

3.6.6. Bandymas Nr.5: KSIM testas taikant „15/5“ verčių zonų suskirstymą

Siekiant įvertinti, kaip priklauso slaptų raktų generavimo patikimumas nuo generuojamo slapto rakto kardinalumo atliktas eksperimentas, kuriame generavimo sričių konfigūracija pakeista iš „3/5“ (kodas generuojamas iš skaičių [1,2,..,6]) į „15/5“ (kodas generuojamas iš skaičių [1,2,...30]).

Bandymas atliktas su visa 240 piršto atvaizdų, o gauti rezultatai pavaizduoti 3.6.4 lentelėje.

3.6.5 lentelė. Bandymo rezultatai Nr.5

Kriterijus	Rezultatas
KAT (FRR)	90%
KPT (FAR)	0,125%
BKT (EER)	90,125%
H(X)	2,29

Padidinus generavimo sričių skaičių iki 30, *BKT* išaugo iki 90,125%. Šio bandymo metu užfiksuotas aukštesnis rezultatų entropijos laipsnis dėl to, kad generuojami raktai buvo ilgesni.

3.7. Rezultatų apibendrinimas

Atlikus bandymus buvo suskaičiuoti pagrindiniai sistemos, naudojančios pirštų kraujagyslių tinklą slaptų raktų generavimui, kriterijai: klaidingo atmetimo tikimybė *(KAT)*, klaidingo priėmimo tikimybė *(KPT)*, bendroji klaidos tikimybė *(BKT)* ir vidutinė generuojamų raktų *Shannon* entropija *H(X)*. Raktams generuoti buvo taikomas darbe siūlomas „Kontūro sekimo iteracijų skaičiaus“ metodas. Bandymų rezultatų apibendrinimas pateikiamas 3.7.1 lentelėje. *BKT, KAT* ir *KPT* kitimo grafikas pateiktas 3.7.1 paveiksle.

3.7.1 Bandymų rezultatų apibendrinimas

Kriterijus	**Rezultatas**				
	Pradinė piršto kraujagyslių atvaizdų DB	**Atvaizdai papildomai lokalizuoti**	**Pašalinti blogiausiai kodą generuojantys paveikslai**	**Kraujagyslių tinklas papildomai pataisytas**	**Tas pats pirštas vertinamas 10 kartų**
Bandymo nr.	Nr.1	Nr.2	Nr.3 (A)	Nr.3 (B)	Nr.4
Pirštų skaičius	240	240	120	120	120
KAT (FRR), %	61,25	53,75	46,667	13,333	25
KPT (FAR), %	2,22	3,29	4,25	2,417	neskaičiuojamas
BKT (EER), %	63,48	57,04	50,917	15,75	25
***H(X),* santykiniai vnt**	2,04	1,97	1,919	2,039	1,971

Atliekant papildomą normalizaciją buvo sumažintos paklaidos dėl netikslumų kraujagyslių tinklų kraštuose. Nors buvo sumažintas atvaizdo dydis, tai beveik nepakeitė generuojamų raktų entropijos.

Dalis duomenų bazėse turėtų pirštų buvo nuskaityti nekokybiškai ir generavo labai nepatikimas kodo vertes. Atliekant generavimą nevertinant blogiau kodą generuojančių pusės pirštų gautos geresnė *KAT*, *KPT* ir *BKT* vertės, tačiau, dėl pašalintų atsitiktinių verčių, sumažėjo generuojamų raktų entropija.

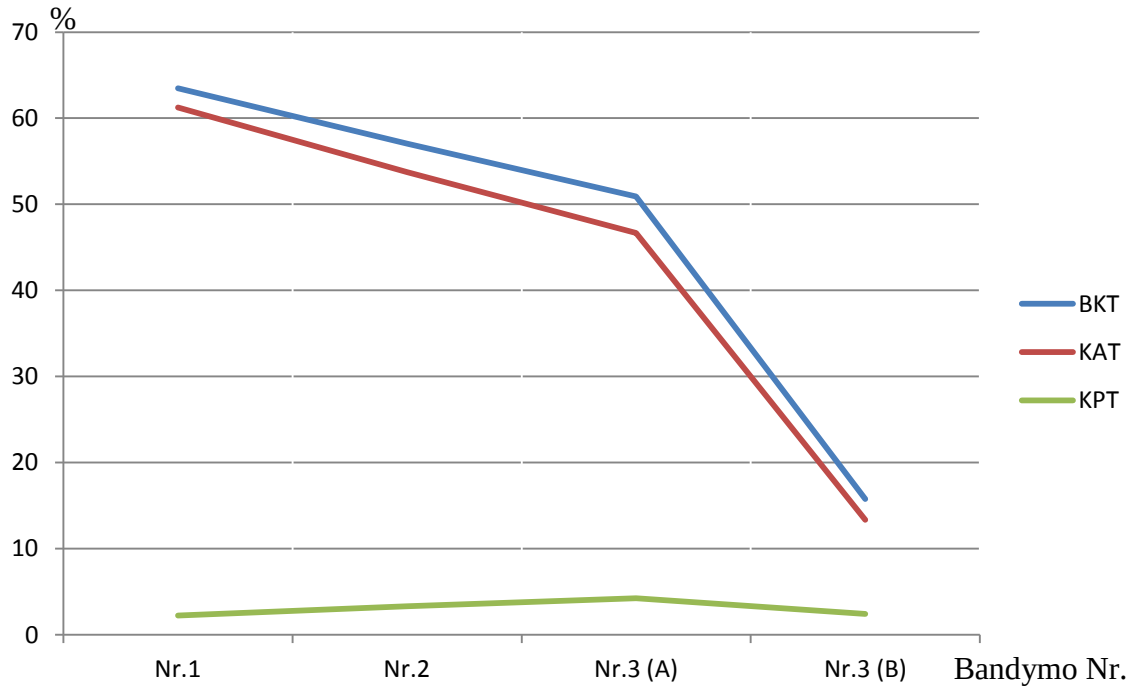
Trečiajame bandyme naudota dešimties pirštų duomenų bazė buvo papildomai modifikuota rankiniu būdu pataisant kai kuriuos kraujagyslių tinkle esančius netikslumus. Šio bandymo rezultatas – ženkliai sumažintos *KPT*, *KAT* ir *BKT* reikšmės. Gauta *BKT* reikšmė yra 15,750%. Šio bandymo metu taip pat pakilo vidutinė generuojamų raktų entropija. Pakilimo priežastis – kai kuriuose atvaizduose buvo pataisyti trūkiai reikšminiuose kraujagyslių tinkle taškuose. Esant šiems trūkiams dalis kraujagyslių tinklo įėjimų/išėjimu nebuvo pasiekiami.

Ketvirtajame bandyme atliktas vieno gana stabiliai slaptą generavimą atliekančio piršto kodo generavimo bandymas. Visi šio piršto atvaizdai (12) buvo naudojami raktui generuoti po 10 kartų iš eilės. Tinklo taisymas šiame bandyme nebuvo naudojamas. Klaidos dažnai kartojosi apdorojant tuos pačius atvaizdus, kas leidžia daryti išvadą, kad nuskaitymo netikslumai lėmė didžiąją dalį sistemos veikimo klaidų.

Penktajame bandyme išbandytas slaptų raktų generavimas, kai verčių zonų konfigūracija pakeičiama į „15/5“ vietoje „3/5“. Šiame bandyme generuoti raktai buvo ilgesni, nei ankstesniuose bandymuose, bet sistemos *KAT* pakilo beveik iki 100%.

Iš 3.7.1 pav. matome, kad didžiausią įtaką *BKT* vertei turi *KAT*, o ne *KPT* vertė. Pirmuose trijuose bandymuose (Nr.1, Nr.2 ir Nr.3(A)) keičiant raktų generavimo veikimą siekiama sumažinti BKT pirm pirmiausia mažinant *KAT*. *KAT* mažinimo pasekmė yra krentanti generuojamų raktų entropija ir dėl to šiek tiek kylanti *KPT*, tačiau *KPT* kilimas yra nežymus palyginti su KAT mažėjimu.

Bandyme Nr. 3 (B) yra ženkliai sumažinamos tiek *KPT* tiek *KAT* vertės. Tai pasiekiama padidinus kraujagyslių tinklų, iš kurių generuojami raktai, kokybę.



3.7.1 pav. Bandymo rezultatų apibendrinimas

4. IŠVADOS

Vartotojų autentifikavimas ir identifikavimas pagal jų biometrines charakteristikas yra plačiai taikomas įvairiose informacinių technologijų srityse. Daugelyje šiuolaikinių sistemų nuskaityti biometrinių savybių atvaizdai yra lyginami su iš anksto išsaugotais atvaizdų šablonais. Biometrinių savybių naudojimas slaptiems raktams, tinkamiems tiek autentifikavimui/identifikavimui, tiek kriptografijai (biokriptografijai) generuoti yra nauja ir perspektyvi sritis. Šioje srityje yra atlikta įvairių tyrimų su akies ragenos atvaizdais, piršto antspaudais, tačiau pirštų kraujagyslių tinklo taikymas yra mažai ištirtas.

Šiame darbe aptariamos pirštų kraujagyslių tinklo tinkamumo slaptų raktų generavimui, nenaudojant tradicinių palyginimo funkcijų galimybės, pristatomos kelios pagrindinės pirminio kraujagyslių tinklo apdorojimo, morfologinio išskyrimo funkcijos ir aptariami galimi slapto rakto generavimo būdai. Šie biometrinių savybių aspektai yra vienodi tiek tiesioginio generavimo, tiek tradicinėse palyginimo sistemose.

Darbo projektinėje dalyje pasiūlytas ir *Matlab* kalba realizuotas „Kontūro sekimo iteracijų skaičiaus“ (KSIM) metodas, skirtas slaptiems raktams tiesiogiai generuoti iš pirminėmis ir morfologinėmis funkcijomis apdorotų kraujagyslių tinklo atvaizdų. Generuojami raktai galėtų būti atšaukiami, nes priklauso nuo generatoriaus charakteristikų. Be paties metodo, sudarytos reikalingos pagalbinės funkcijos ir tyrimų aplinka, numatytos priemonės rezultatų netikslumams dėl biometrinių charakteristikų nepastovumo koreguoti ir kompensuoti.

Remiantis eksperimento rezultatais, galima teigti, kad taikant KSIM metodą galima generuoti gana pastovios vertės neilgus (4 – 6 skaitmenų) slaptus raktus iš pirštų kraujagyslių tinklo. Siekiant gerų slaptų raktų generavimo rezultatų, būtina, kad pradinės biometrinės savybės būtų nuskaitomos labai kokybiškai. Nors gautos *BKT* vertės nuo 15,75% iki 63,48% yra blogesnės nei deklaruojamos komercinių sistemų *BKT* reikšmės, reikia prisiminti, kad tai – tiesioginio pastovių raktų generavimo metodas, o ne metodas paremtas atvaizdų apytiksliu palyginimu.

Šiame darbe nustatyta, kad KSIM metodas nepatikimai generuoja ilgus raktus. Tolesniuose darbuose būtų galima atlikti papildomus bandymus su geresnės kokybės pirštų kraujagyslių duomenų baze ir patobulinti KSIM ar pasiūlyti naują metodą ilgiems slaptiems raktams sudaryti.

KSIM metodas galėtų būti adaptuotas ir taikomas tradicinių autentifikavimo/identifikavimo sistemų greitaveikos padidinimui, pavyzdžiui, generuojami raktai galėtų būti naudojami 1 : n atvaizdų palyginimo operacijų skaičiui duomenų bazėse sumažinti ir bendram sistemos veikimui paspartinti. Taip pat, kombinuojant kelių pirštų kraujagyslių tinklų nuskaitymą į bendrą raktą, KSIM generuojami raktai galėtų būti naudojami nesudėtingiems biokriptografiniams šifravimo raktams kurti.

5. LITERATŪRA

[1] "An Overview of Biometric Recognition." [Tinkle]. http://biometrics.cse.msu.edu/info.html [Kreiptasi 2013-05-22]

[2] "Is your business as safe as you think?"Mindy Blodgett. [Tinkle]. http://edition.cnn.com/TECH/computing/9907/16/security-ent.idg/index.html?_s=PM:TECH [Kreiptasi 2013-05-22]

[3] A. Venčkauskas ir E. Kazanavičius, *Informacinių technologijų saugos metodai*. Kaunas, Lietuva, 2011.

[4] J. Hashimoto, "Finger Vein Authentication Technology and Its Future," straipsnis konferencijoje *VLSI Circuits*, Honolulu, HI, 2006, pp. 5-8.

[5] O. Ushmaev, V. Kuznetsov ir V. Gudkov, "Extraction of Binary Features from Fingerprint Topology," straipsnis konferencijoje *Hand-Based Biometrics (ICHB)*, 2011, pp. 1,6.

[6] C. R. Costanzo, "Active Biometric Cryptography (ABC): Key Generation Using Feature and PArametric Agregation," straipsnis konferencijoje *Internet Monitoring and Protection, ICIMP Second International Conference*, 2007, pp. 1-5.

[7] G. Zheng, W. Li ir C. Zhan, "Cryptographic Key Generation from Biometric Data Using Lattice Mapping," straipsnis konferencijoje *18th International Conference on Pattern Recognition (ICPR), 2006*, 2006, pp. 513-516.

[8] X. Wu, N. Qi, K. Wang ir D. Zhang, "An Iris Cryptosystem for Information Security," straipsnis konferencijoje *2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processsing (IIHMSP)*, 2008, pp. 1533-1536.

[9] J. Jagadeesan, T. Thillaikarasi ir K. Duraisnamy, "Cryptographic Key Generation from Multiple Biometric Modalities: Fusing Minuae with Iris Feature," straipsnis konferencijoje *International Journal of Computer Applications*, vol. 2, no. 6, pp. 16-26, June 2010.

[10] A. Venčkauskas ir P. Nanevičius, "Cryptographic Key Generation from Finger Vein," straipsnis konferencijoje *2nd International Conference on Conference of Infromatics and Management Schences*, 2013, pp. 327-331.

[11] A. Stoianov, "Biometric Encription: A Positive-Sum Technology That Achieves Strong Authentication," straipsnis žurnale *Security and Privacy*, 2007.

[12] Y.-J. Chang, W. Zhang ir C. Tsuhan, "Biometric-Based Cryptographic Key Generation," straipsnis konferencijoje *IEEE International Conference on Multimedia and Expo (ICME)*, 2004, pp. 2203-2206.

[13] "Door-access-control System by Finger Vein Authentication." [Tinkle]. http://www.hitachi-ics.co.jp/product/english/about_fv.htm [Kreiptasi 2013-05-22]

[14] Ben Edgington, "Introducing Hitachi's Finger Vein Technology" May 2007. [Tinkle]. http://www.hitachi.eu/veinid/documents/veinidwhitepaper.pdf [Kreiptasi 2013-05-22]

[15] "Comparitive Analysis: Finger vein authentication technology." [Tinkle]. http://www.hitachi.co.jp/products/it/veinid/global/introduction/comparison.html [Kreiptasi 2013-05-22]

[16] British Standards, "BioAPI Specification", 2006, BS ISO/IEC 19784-1:2006.

[17] Wikipedia. "Biometrics". [Tinkle]. http://en.wikipedia.org/wiki/Biometrics [Kreiptasi 2013-05-22]

[18] "Comparative Biometric Testing," Internatiuonal Biometrics Group, Round 6 Public Report 2006.

[19] N. Miura, A. Nagasaka ir T. Miyatake, "Automatic Feature Extraction from non-uniform Finger Vein Image and its Application to Personal Identification," straipsnis konferencijoje *IAPR Workshop on Machine Vision Applications*, Nara- ken New Public Hall, Nara, Japan, 2002, pp.

11-13.

[20] N. Miura, A. Nagasaka ir T. Miyatake, "Feature extraction of finger vein patterns based on repeated line tracking and its application to personal identification," Straipsnis žurnale *Machine Vision and Applications, Volume 15, Number 4*, pp. 194-203, 2004.

[21] S. P. Corcoran, M. Ennis ir Robert K. Rowe, "Contactless multispectral biometric capture," US 7995808 B2, Patentas Aug. 09, 2011.

[22] Bram Ton. (2012, Nov.) Mathworks: Miura et al. vein extraction methods. [Tinkle]. http://www.mathworks.com/matlabcentral/fileexchange/35716-miura-etal-al-vein-extraction-methods [Kreiptasi 2013-05-22]

[23] E. C. Lee, H. C. Lee ir K. R. Park, "Finger vein recognition using minutia-based alignment and local binary pattern-based feature extraction," straipsnis žurnale *International Journal of Imaging Systems and Technology*, vol. 19, no. 3, pp. 179-186, Sep. 2009.

[24] N. Miura, A. Nagasaka ir T. Miyatake, "Extraction of Finger-Vein Patterns Using Maximum Curvature Points in Image Profiles," straipsnis konferencijoje *IAPR Conference on Machine Vision Applications*, Tsukuba, 2005, pp. 347-350.

[25] B. Huang, Y. Dai, R. Li, D. Tang ir W. Li, "Finger-vein Authentication Based on Wide Line Detector and Pattern Normalization," straipsnis konferencijoje *International Conference on Pattern Recognition*, 2010, pp. 1269-1272.

[26] L. Liu, D. Zhang ir J. You, "Detecting Wide line Using Isotropic Nonlinear Filtering," straipsnis konferencijoje *IEEE Transactions on image processing*, 2007, pp. 1584-1595.

[27] B. A. Rosdi, C. W. Shing ir S. A. Suandi, "Finger Vein Recognition Using Local Line Binary Pattern," straipsnis žurnale *Sensors*, vol. 11, pp. 111357-222371, 2011.

[28] N. Mahri, S.A.S. Suandi ir B.A. Rosdi, "Finger Vein Recognition Algorithm Using Phase Only Correlation," straipsnis konferencijoje *Emerging Techniques and Challenges for Hand-Based Biometrics (ETCHB)*, Istanbul, 2010, pp. 1-6.

[29] H. Qin, L. Qin ir C. Yu, "Region growth–based feature extraction method for finger-vein recognition," straipsnis žurnale *Optical Engineering*, vol. 50, no. 5, p. 13, May 2011.

[30] Wikipedia. "Mathematical morphology". [Tinkle]. http://en.wikipedia.org/wiki/Mathematical_morphology [Kreiptasi 2013-05-22]

[31] C. Eidheim. "Introduction to Mathematical Morphology". [Tinkle]. http://www.idi.ntnu.no/emner/tdt4265/lectures/lecture3b.pdf [Kreiptasi 2013-05-22]

[32] Wikipedia. "Error detection and correction". [Tinkle]. http://en.wikipedia.org/wiki/Error_detection_and_correction [Kreiptasi 2013-05-22]

[33] S. Kanade, D. Petrovska-Delacretaz ir B. Dorizzi, "Cancelable Iris Biometrics and Using Error Correcting Codes to Reduce Cancelable Iris Biometrics and Using Error Correcting Codes to Reduce," straipsnis konferencijoje *Computer Vision and Pattern Recognition IEEE Conference*, 2009, pp. 120-127.

[34] P Li et al., "An effective biometric cryptosystem combining fingerprints with error correction codes," straipsnis žurnale *Expert Systems with Applications*, vol. 39, pp. 6562-6574, 2011.

[35] D. Burba, "Piršto antspaudo naudojimas šifravimo rakto generavimui", magistro darbas, 2010.

[36] Hong Kong Politechnic University. "Finger Image Database (Version 1.0)". [Tinkle]. http://www4.comp.polyu.edu.hk/~csajaykr/fvdatabase.htm [Kreiptasi 2013-05-22]

[37] A. Jonaitis. (2008, Jan.) "Akys nemeluoja, pirštai garantuoja (2 dalis)". [Tinkle]. http://www.elektronika.lt/straipsniai/pazintiniai/10120/akys-nemeluoja-pirstai-garantuoja-2-dalis/ [Kreiptasi 2013-05-22]

[38] E. C. Lee ir K. R. Park, "Image restoration of skin scattering and optical blurring for finger vein recognition," straipsnis žurnale *Optics and Lasers in Engineering*, vol. 49, pp. 816-828, 2011.

6. PRIEDAI

6.1. priedas. Magistro baigiamojo darbo suderinimo forma

Magistro baigiamojo darbo tvirtinimo forma

Studentas: Povilas Nanevičius (Vardas, Pavardė, parašas) Vadovas: doc. dr. Algimantas Venčkauskas (Vardas, Pavardė, parašas)	SUDERINTA: Kompiuterių katedros vedėjas (parašas)

Darbo tema: Piršto kraujagyslių tinkolo taikymo šifravimo raktų generavimui galimybių tyrimas

Sprendžiama problema: nuskaitant biometrinius duomenis galimos paklaidos. Dabar naudojamose sistemose dažniausiai taikomas nuskaitytų duomenų palyginimas su atitikmenimis. Kadangi įvestis nėra pastovi, tokie duomenys nėra patogūs stipriems pastovios vertės raktams generuoti. Daugelyje sistemų, naudojančių biometrinius metodus dažniausiai saugomi šablonai. Šiame darbe tiriamos galimybės raktus generuoti tiesiogiai iš nuskaityto paveikslo, be lyginimo su šablonu. Numatoma ištirti tokių raktų stiprumą, klaidino atmetimo ir kitas savybes.

Tyrimo sritis ir objektas: darbe nagrinėjami piršto kraujagyslių tinklo atvaizdo nuskaitymo įrenginiai, atpažinimo metodai ir šifravimo algoritmai.

Darbo tikslas ir uždaviniai: tikslas – įvertinti galimybę generuoti šifravimo raktus tiesiogiai iš nuskaitytų kraujagyslių paveikslų. Užduotys - susipažinti su biometrinių duomenų nuskaitymo įranga ir duomenų atpažinimo metodais (filtravimo, vektorizavimo ir pan.). Įvertinti galimybes generuoti pastovios vertės raktus iš informacijos nuskaitytos su paklaidomis ir tokių raktų patikimumą. Atlikus bandymus įvertinti, kokio sudėtingumo raktus galima generuoti laikantis sąlygos, kad sugeneruotas raktas turi būti pastovus.

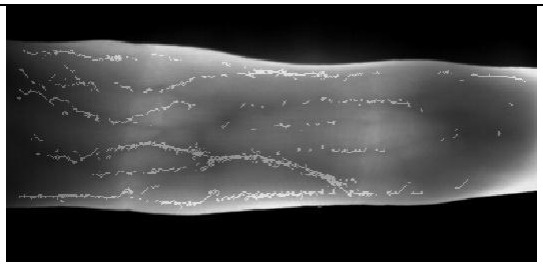
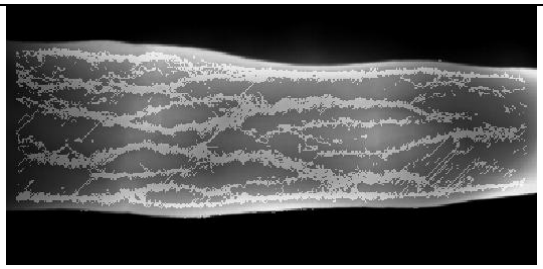
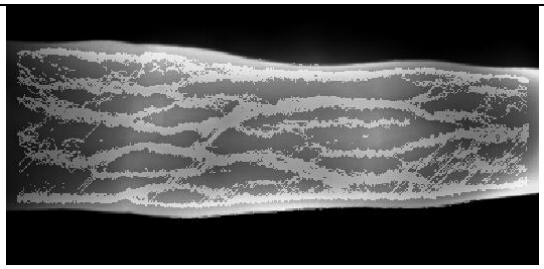
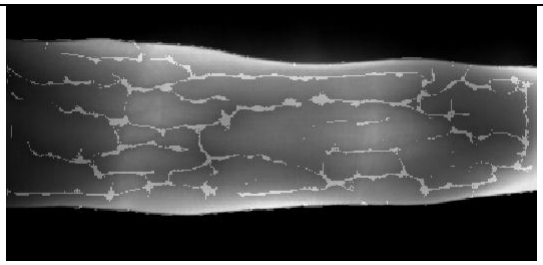
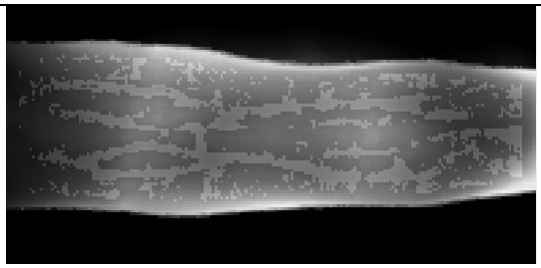
Kas numatoma atlikti darbo analizės dalyje: susipažinti su esamomis piršto kraujagyslių atvaizdo duomenų nuskaitymo sistemomis ir atpažinimo algoritmais. Išnagrinėti vaizdų atpažinimo metodus. Pasirinkit tinkamiausią vaizdo apdorojimo modelį. Išnagrinėti galimas paklaidas dėl skirtingo piršto padėjimo ant skaitytuvo, aplinkos veiksnių ir kitų sąlygų.

Koks bus pasiūlytas problemos sprendimo metodas / modelis / algoritmas / metodika / aparatinės realizacijos projektas / kita : iš analizės dalyje išnagrinėtų metodų bus sufomuluotas modelis, kaip pastovus raktas galėtų būti generuojamas iš piršto kraujagyslių atvaizdo.

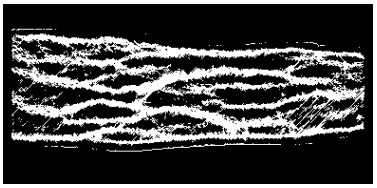
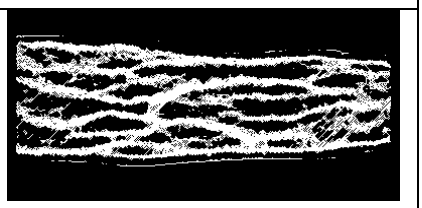
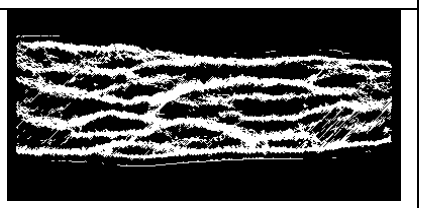
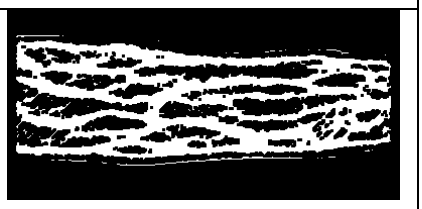
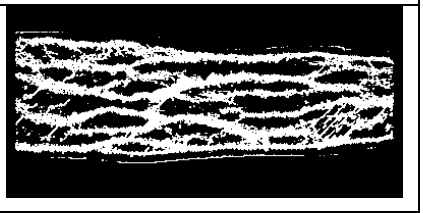
Kokiomis priemonėmis ar būdais numatoma įgyvendinti darbo realizaciją: Naudojantis esama aparatine įranga ir pritaikyta ar parašyta programine įranga bus sukurta sistema, leidžianti atlikti bandymus ir įvertinti generuojamų raktų savybes.

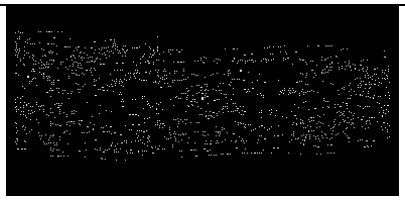
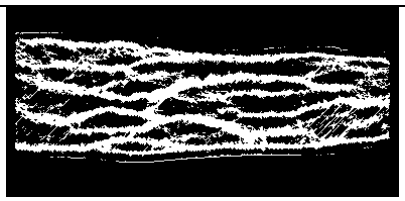
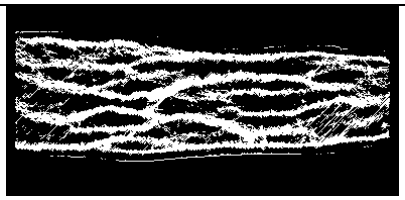
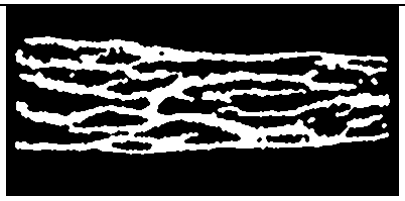
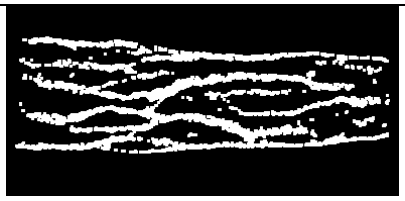
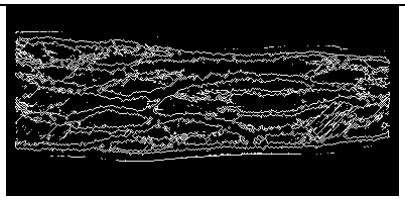
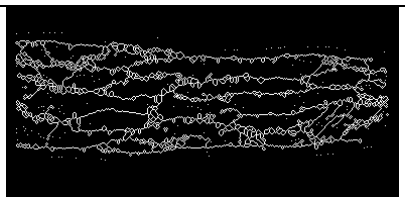
Kokie bus eksperimento rezultatai ir kaip jie bus apdorojami: darbo rezultatas – atpažinimo sistema skirta slaptajam šifravimo raktui generuoti iš piršto kraujagyslių atvaizdo. Iš tyrimo duomenų bus įvertintos galimybės generuoti skirtingo stiprumo slaptuosius raktus iš nepastovių įvesties duomenų.

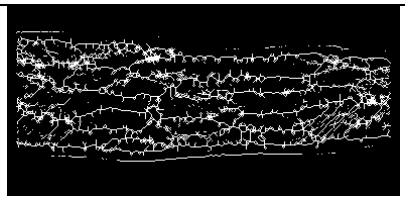
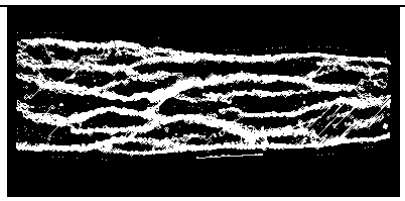
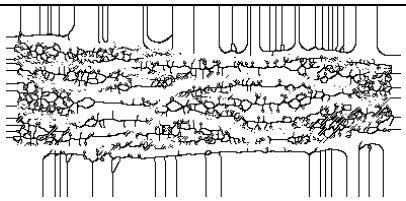
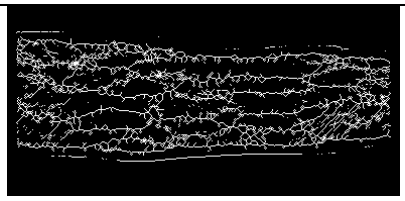
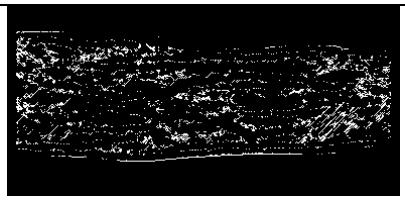
6.2. priedas. „Miura“ ir „Huang“ pirminių kraujagyslių kontūrų išskyrimo algoritmų pavyzdžiai naudojant standartinį įvesties atvaizdą

Metodas	Parinktys	Rezultatas
Miura „Pasikartojančių linijų“	Iteracijos = 100;	
Miura „Pasikartojančių linijų“	Iteracijos = 1000;	
Miura „Pasikartojančių linijų“	Iteracijos = 3000;	
Miura „Maksimalaus linkio“	Sigma = 3;	
Huang „Plačių linijų“	-	

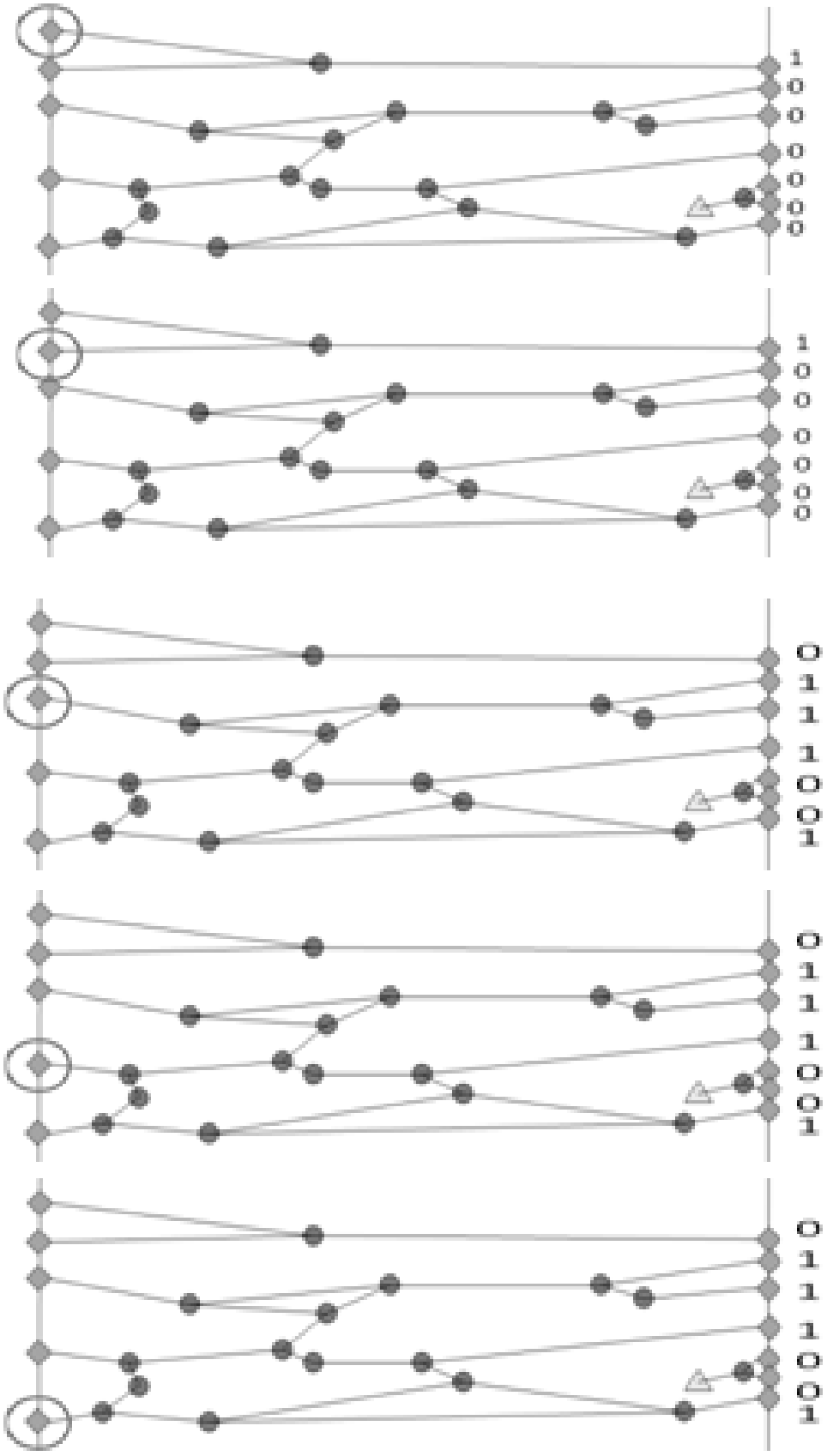
6.3. „Matlab“ matematinės morfologijos funkcijų, naudojamų skaitmeninių atvaizdų apdorojimui, pavyzdžiai

Funkcija	Apibūdinimas	Rezultatų pavyzdys, kai įvesties paveikslas:  Ne visos funkcijos sėkmingai grąžino lauktus rezultatus dėl įvesties parametrų
'bothat'	Morfologinė „bottomhat“ operacija. Grąžina atvaizdą – atvaizdo morfologinė uždarymo operacija.	
'branchpoints'	Suranda išsišakojimus. Pvz: 0 0 1 0 0 0 0 0 0 0 0 0 1 0 0 taps 0 0 0 0 0 1 1 1 1 1 0 0 1 0 0 0 0 1 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0	
'bridge'	Sujungia atskirtus taškus – t.y. paverčia 0 pikselius 1 pikseliais jei šalia yra du [1] pikseliai: 1 0 0 1 1 0 1 0 1 taps 1 1 1 0 0 1 0 1 1	
'clean'	Pašalina visiškai izoliuotus pikselius.	
close'	Morfologinė ‚uždarymo‘ operacija.	
'diag'	Šalina įstrižus „8“ formos sujungimus: 0 1 0 0 1 0 1 0 0 taps 1 1 0 0 0 0 0 0 0	

'dilate'	Atlieka paveikslo išskaidymą/išliejimą (dilate)	
'endpoints'	Randa vaizdinio baigtinių linijų galų koordinates: 1 0 0 0 1 0 0 0 0 1 0 0 taps 0 0 0 0 0 0 1 0 0 0 1 0 0 0 0 0 0 0 0 0	
'erode'	Išgraužimas	
'fill'	Užpildo izoliuotus tuščius pikselius, pvz: 1 1 1 1 0 1 1 1 1	
'hbreak'	Pašalina H forma sujungtus pikselius: 1 1 1 1 1 1 0 1 0 taps 0 0 0 1 1 1 1 1 1	
'majority'	Paverčia pikselį 1 jei 5 ar daugiau kaimyninių pikselių 3x3 elemente yra 1	
'open'	Morfologinė atidarymo operacija	
'remove'	Pažalina figūrų užpildus	
'shrink'	Sutraukimas iki taško. Objektai su skylėmis sutraukiami į 1/2r spindulio apskritimus.	

'skel'	Susiaurina plačius objektus iki linijos, bet neleidžia jiems išsiskirti	
'spur'	Genėjimo funkcija – pašalina viename gale neprijungtas atšakas	
'thicken'	Plėtimas. Vykdomas tol, kol anksčiau nesujungti objektai susijungia H sujungimais	
'thin'	Susiaurinimas iki linijos. Objektai su skylėmis sutraukiami į apskritimus.	
'tophat'	Morfologinė „TopHat“ operacija – grąžina paveikslą – jo morfologinės „open“ operacijos rezultatas	

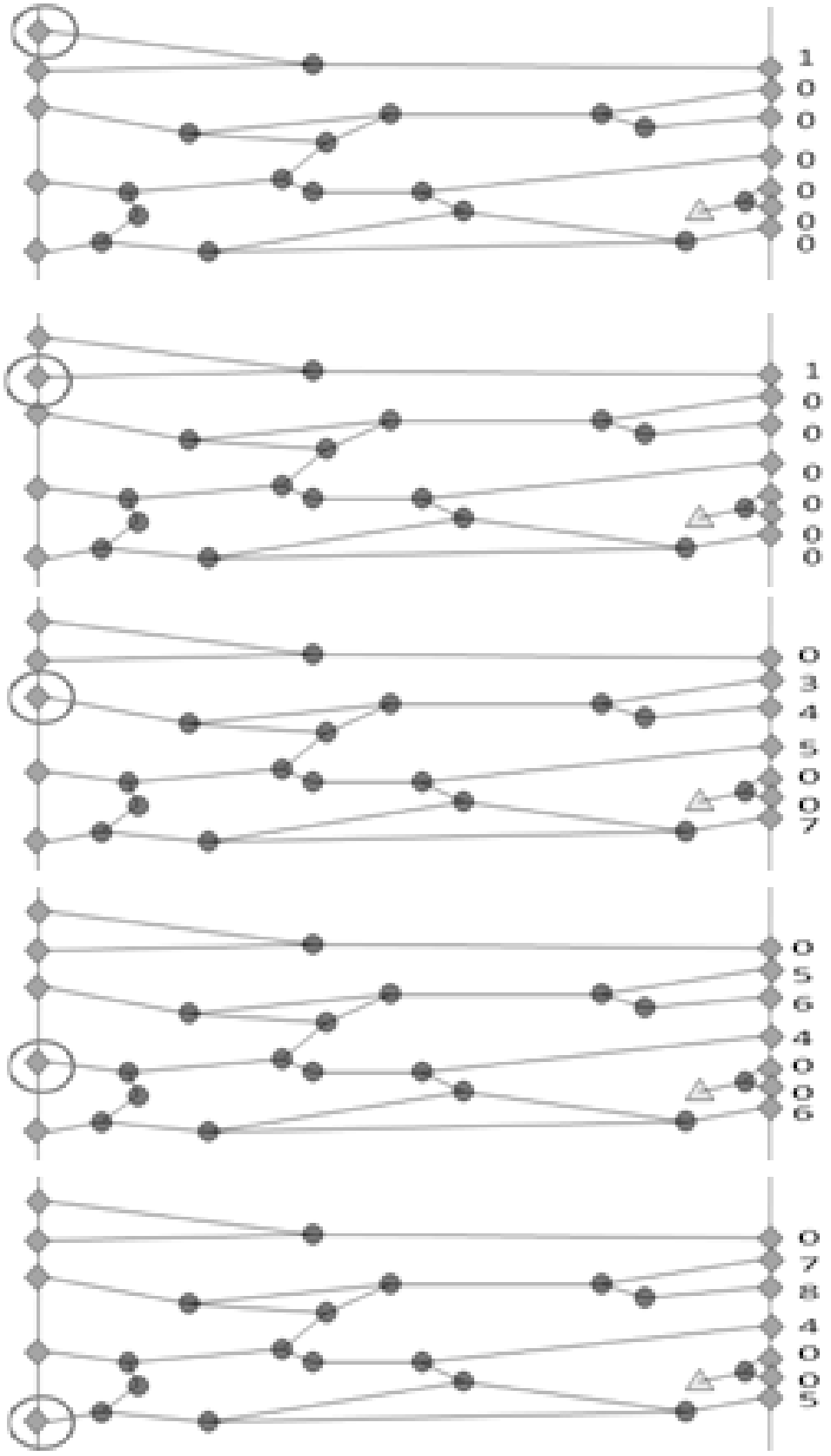
6.4. Susijungiančių taškų metodo kodo generavimo seka



Seka: 10000001000000011100101110010111001

Sekos elementai [0,1];

6.5. Sankryžų skaičiaus metodo generavimo seka



Seka: 1000000100000003450070564006078400 5

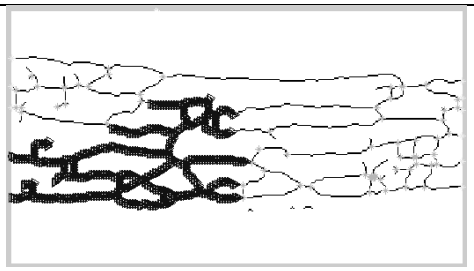
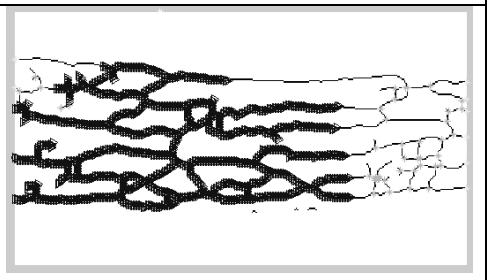
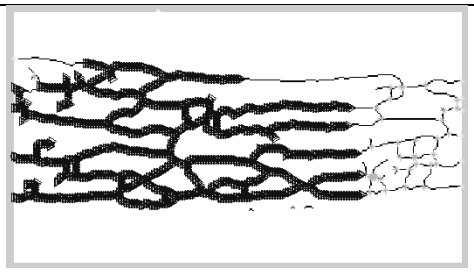
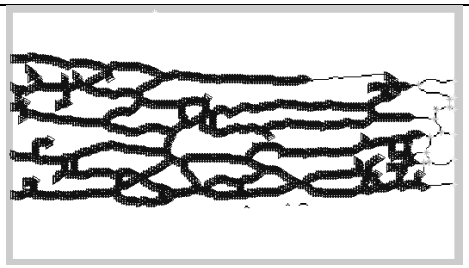
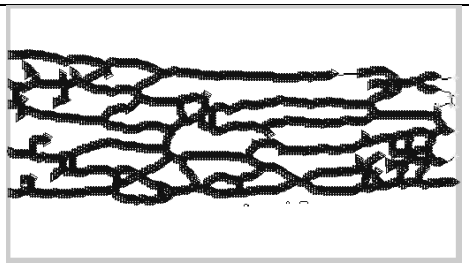
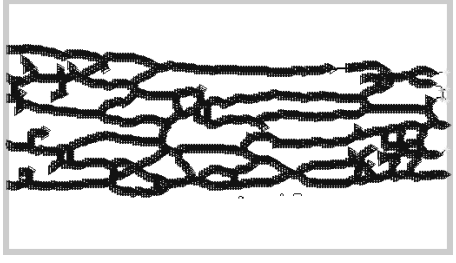
Sekos elementai [0,n];

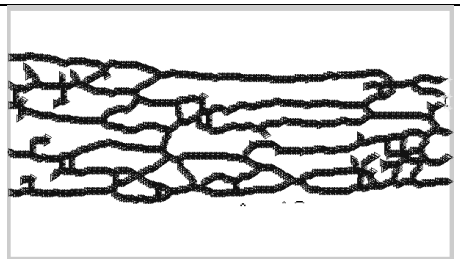
6.6. „Matlab“ kontūro sekimo funkcijos „konturo_sekimas.m“ realizacija („Matlab“ kodo pavyzdys)

```
function [taskai]=konturo_sekimas(IMG,pr_x,pr_y)
%
% File Name  : konturo_sekimas.m
% Sukure       : Povilas Nanevicius
% Data         : 2013-01-15
%
% Dvinario (juoda/balta) paveikslo konturo sekimas
%
 % Pradedant nuo ivesties tasko (pr_x, pr_y) analizuojamas IMG atvaizdas ir
 % registuojamos elementu, kuriu verte yra == 0 koordinates. Analize
 % atliekama su kiekvienu tasku atskirai. Sioje funkcijoje daroma prielaida, kad ivesties paveikslo
konturo spalva
 % yra juoda (0), o fono spalva balta (1).
%
% Kvietimas:
% [taskai]=konturo _sekimas(PAV,x,y)
%
%   Ivestis:
%   PAV - juodai baltas dvinaris atvaizdas
%   x, y - pradinio sekimo tasko koordinates
%
%   Isvestis:
%   taskai - N x 2 matrix konturo koordinaciu matrica
%
forb=1;iter=0;
taskai(1,1)=pr_x;       % pradzios x tasko koordinate
taskai(1,2)=pr_y;       % pradzios y tasko koordinate

% Postumiai:  [x; y]
postumis(1,:)=[0;-1];
postumis(2,:)=[1;-1];
postumis(3,:)=[1;0];
postumis(4,:)=[1;1];
postumis(5,:)=[0;1];
postumis(6,:)=[-1;1];
postumis(7,:)=[-1;0];
postumis(8,:)=[-1;-1];

while(1)
```

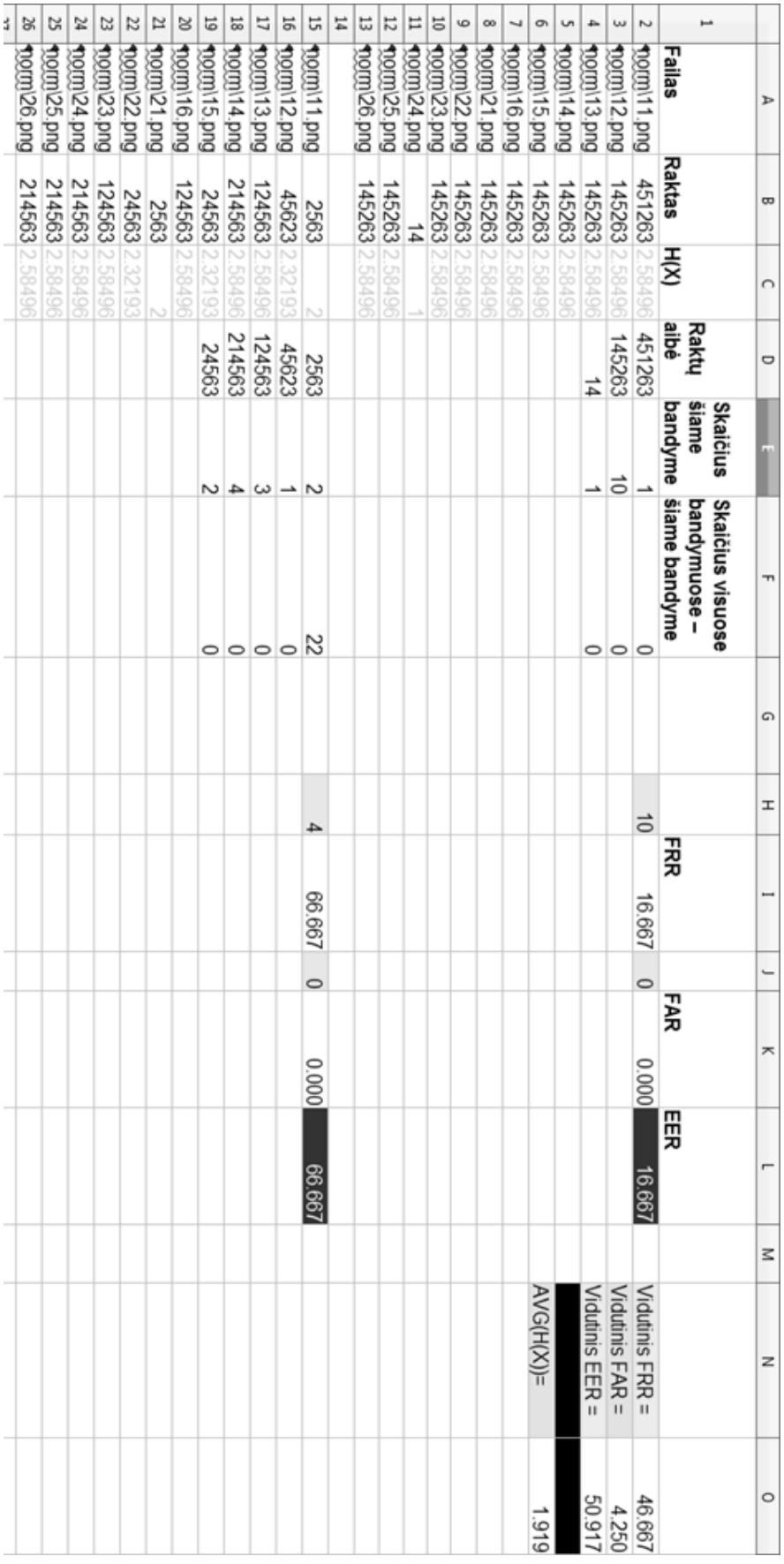
```
        elem_prad=size(taskai,1);                                   % fiksuojam pradini masyvo elementu skaiciu
(pirma karta 1)
        while(1)
          iter=iter+1;
          for fora=1:8                                              % po viena karta kiekvienam kaimyniniam masyvo
elementui (postumiui)
            dx = postumis(fora,1);
            dy = postumis(fora,2);
            if ((taskai(iter,1)+dx)>=1 && (taskai(iter,2)+dy)>=1)    % ar yra x, y vertes?
              if  (IMG((taskai(iter,2)+dy),(taskai(iter,1)+dx))==0)    % ar sis elementas priklauso konturui
(==0)?
                forb=forb+1;                                        % kursorius "sekanciuam" elemento numeriui
saugoti
                taskai(forb,1)=taskai(iter,1)+dx;
                taskai(forb,2)=taskai(iter,2)+dy;
                IMG((taskai(iter,2)+dy),(taskai(iter,1)+dx))=1;      % korekcija. statom atrasta nauja nulini
taska vienetu, kad nebekartoto jo apdorojimo
              end
            end
          end
          if (iter>=elem_prad)                %kartojam
            break;                           % vidinis while
          end
        end
        if (elem_prad==size(taskai,1))              % jegu isvesties masyve esanciu elementu skaicius lygus
praeito masyvo elementu skaiciui
          break;                                % nutraukiam isorini while(1)
        end
      end % end of while
```

6.7. Kontūro sekimo iteracijų skaičiaus metodo generavimo seka

Atvaizduojamų kontūro taškų skaičius	Pasiekto įėjimo/išėjimo koordinatės	Kraujagyslių tinklo atvaizdas, uždengtas atvaizduojamais taškais
826	įėjimas 5 (1,140), kodo vertė 5	
1602	įėjimas 3 (1,73), kodo vertė 3	
1727	įėjimas 2 (1,57) kodo vertė 2	
2273	įėjimas 1 (1, 36), kodo vertė 1	
2483	išėjimas 6 (338, 132), kodo vertė 11	
2512	išėjimas 4 (338, 94), kodo vertė 9	

2544	išėjimas 5 (338, 113), kodo vertė 10	
2561	išėjimas 1 (338, 53), kodo vertė 6	-
2566	išėjimas 2 (338, 66) kodo vertė 7	-
2568	išėjimas 3 (338, 75) kodo vertė 8	-

6.8. Bandymų rezultatų apdorojimo aplinkos ištrauka



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Failas	Raktas	H(X)	Raktų aibė	Skaičius šiame bandyme	Skaičius visuose bandymuose – šiame bandyme		FRR		FAR	EER				
2	norm\11.png	451263	2.58496	451263	1	0		10	16.667	0	0.000	16.667		Vidutinis FRR =	46.667
3	norm\12.png	145263	2.58496	145263	10	0								Vidutinis FAR =	4.250
4	norm\13.png	145263	2.58496	14	1	0								Vidutinis EER =	50.917
5	norm\14.png	145263	2.58496												
6	norm\15.png	145263	2.58496											AVG(H(X))=	1.919
7	norm\16.png	145263	2.58496												
8	norm\21.png	145263	2.58496												
9	norm\22.png	145263	2.58496												
10	norm\23.png	145263	2.58496												
11	norm\24.png	14	1												
12	norm\25.png	145263	2.58496												
13	norm\26.png	145263	2.58496												
14															
15	norm\11.png	2563	2	2563	2	22		4	66.667	0	0.000	66.667			
16	norm\12.png	45623	2.32193	45623	1	0									
17	norm\13.png	124563	2.58496	124563	3	0									
18	norm\14.png	214563	2.58496	214563	4	0									
19	norm\15.png	24563	2.32193	24563	2	0									
20	norm\16.png	124563	2.58496												
21	norm\21.png	2563	2												
22	norm\22.png	24563	2.32193												
23	norm\23.png	124563	2.58496												
24	norm\24.png	214563	2.58496												
25	norm\25.png	214563	2.58496												
26	norm\26.png	214563	2.58496												

6.9. Publikacija XVIII tarpuniversitetinėje tarptautinėje magistrantų ir doktorantų konferencijoje „Informacinė visuomenė ir universitetinės studijos” (IVUS 2013)

INFORMACINĖS TECHNOLOGIJOS • IVUS 2013 • ISSN 2029-249X • eISSN 2029-4824

Piršto kraujagyslių tinklo taikymo slaptų raktų generavimui galimybių tyrimas

Povilas Nanevičius
Informatikos Fakultetas
Kauno Technologijos universitetas
Kaunas, Lietuva
povilas.nanevicius@stud.ktu.lt

doc. dr. Algimantas Venčkauskas
Informatikos Fakultetas
Kauno Technologijos universitetas
Kaunas, Lietuva
algimantas.venckauskas@ktu.lt

Santrauka. **Biometrinės sistemos, skirtos slaptų raktų generavimui iš piršto kraujagyslių tinklo, nenaudojant palyginimo su iš anksto išsaugotu šablonu, galimybių tyrimas. Tokia sistema leistų naudoti vartotojo piršto kraujagyslių atvaizdą nesudėtingiems raktams generuoti be originalaus šablono išsaugojimo ir palyginimo. Darbe naudojamos tradicinėse (palyginimo) sistemose taikomos piršto kraujagyslių tinklo išskyrimo funkcijos ir papildomos raktų generavimo funkcijos. Bandymo metu iš pavyzdinio kraujagyslių tinklo atvaizdo, apdoroto Miura „Pasikartojančių linijų sekimo“ algoritmu ir morfologinėmis funkcijomis, pritaikius darbe siūlomą „Kontūro sekimo iteracijų skaičiaus“ metodą, gautas 12 simbolių ilgio slaptas raktas.**

Reikšminiai žodžiai — piršto kraujagyslių tinklas; raktų generavimas; biometrija

I. ĮVADAS

Piršto kraujagyslių atvaizdų skenavimas yra vienas iš naujausių, bet jau plačiai taikomų biometrinių vartotojų autentifikavimo metodų. Lyginant su viena dažniausiai biometrijoje naudojamų savybių – piršto antspaudais – kraujagyslių tinklas yra saugesnis, nes jis yra nematomas, nuskaitomas tik tol, kol piršty teka kraujas [1]. Taip pat kraujagyslių išskyrimo algoritmų bendroji klaidos tikimybė EER=FAR-FRR (angl. Equal Error Rate), kur FAR yra klaidingo priėmimo tikimybė (angl. False Acceptance Rate), o FRR – klaidingo atmetimo tikimybė (angl. False Rejection Rate) dažnai yra mažesnė, lyginant su piršto antspaudų autentifikavimo sistemų EER. Miura „Pasikartojančių linijų sekimo“ algoritmo EER = 0,145%, o skirtingų piršto antspaudus naudojančių sistemų EER rodikliai svyruoja tarp 0,2 ir 4% [2]. Piršto kraujagyslių taikymas autentifikacijai patogus ir dėl to, kad, lyginant su kai kuriais kitais biometriniais autentifikavimo metodais, atvaizdo gavimui mažiau įtakos turi tokie aplinkos veiksniai kaip purvas, piršto ar skaitytuvo paviršiaus drėgnumas ir kt. [1].

Daugelio šiuolaikinių piršto kraujagyslių tinklą autentifikacijai naudojančių sistemų veikimas paremtas vartotojo pateikto kraujagyslių tinklo žemėlapio palyginimu su iš anksto išsaugotu pavyzdžiu arba tam tikru būdu suformuotu šablonu. Plintant sistemoms, naudojančioms piršto kraujagyslių tinklą autentifikacijai, iškyla keletas naujų problemų: to paties kraujagyslių tinklo naudojimas skirtingos sistemose kelia abejonių dėl tokių sistemų saugumo – kraujagyslių tinklas tampa saugotina savybe. Norint lyginti atvaizdus su šablonais reikia brangesnės nuskaitymo įrangos su daugiau vidinės atminties arba tenka siųsti nuskaitytus atvaizdus į centrinį serverį – tai gali sukurti papildomą tinklo srautą ir padidinti galimų sistemos pažeidžiamumų kiekį.

Šiame darbe aptariamos slapto pastovaus rakto generavimo galimybės iš piršto kraujagyslių tinklo, nuskaitant laikinai saugomą iš dalies kintantį piršto kraujagyslių tinklo žemėlapį. Tokios sistemos sugeneruoti raktai priklausytų nuo naudojamo generavimo algoritmo ir skirtingose autentifikavimo sistemose būtų unikalūs. Kadangi nuskaitytas piršto kraujagyslių tinklo žemėlapis, sugeneravus slaptą raktą, būtų iš karto pašalinamas, iš sistemoje saugomų raktų nebūtų galima atkurti pradinio kraujagyslių tinklo savybių.

Viena iš pagrindinių problemų, susijusių su tiesioginiu slaptų raktų generavimu, yra ribotas galimų raktų ilgis ir unikalumas. Taip pat, lyginant su palyginimo sistemomis, tiesioginio generavimo sistemų veikimą galėtų labiau trikdyti nežymios kraujagyslių tinklo nuskaitymo ir pirminio apdorojimo paklaidos.

Šiame darbe aptariamos kelios skirtingos raktų generavimo funkcijos ir jų savybės bei išbandomas rakto generavimo, skaičiuojant kontūro sekimo iteracijas, metodas, kuris iš pateikto kraujagyslių tinklo generuoja 12 skaitmenų ilgio raktą.

II. ATVAIZDO GAVIMAS

A. Piršto kraujagyslių tinklo nuskaitymas

Piršto kraujagyslių tinklas yra nuskaitomas padedant pirštą tarp infraraudonųjų spindulių šaltinio (skirtingose sistemose naudojamas bangos ilgis svyruoja tarp 750 iki 950 nm) ir kameros, fiksuojančios vaizdą. Kraujyje esantis hemoglobinas sugeria infraraudonąją spinduliuotę, todėl atvaizde kraujagyslės atrodo kaip tamsesnės linijos [3]. Dėl kraujagyslių geometrijos, kraujagyslių centrai yra tamsesni, o juos supantys kraštai tolygiai šviesesni. Kraujagyslės matomos kaip tamsūs sleniai.

Tarp komercinių sistemų, skirtų pirštų kraujagyslių tinklo atvaizdams gauti ir apdoroti, dominuoja Hitachi, Fujitsu, M2SYS, Sony ir kitų gamintojų produktai.

Šiame darbe aptariamoms raktų generavimo funkcijoms analizuoti naudojamas pavyzdinis piršto kraujagyslių atvaizdas [4], pateiktas 1 paveiksle (a), gautas naudojant 830 nm bangos ilgį. Vėlesniuose darbuose numatoma atlikti bandymus su didesnėmis pirštų kraujagyslių duomenų bazėmis.

B. *Pirminis kraujagyslių išskyrimas*

Kraujagyslių atvaizdas bandomoje sistemoje yra apdorojamas Miura „Pasikartojančių linijų sekimo“ funkcija [2]. Ši funkcija, pradėdama nuo atsitiktinių taškų atvaizde, ieško tamsesnių plotų, apsuptų tolygiai šviesesnio fono. Nuo surastų taškų atliekamas linijų sekimas tamsiais kontūrais (slėniais). Nuolatinis aplinkinių plotų šviesumo tikrinimas leidžia sumažinti atsitiktinai sekamų triukšmų įtaką galutiniam rezultatui ir efektyviai pašalinti dėl kaulų ir sąnarių struktūros atvaizde atsirandančius šešėlius. Priklausomai nuo pasirinkto sekimo iteracijų skaičiaus (sekimo kartų), funkcija gali praeiti per aptiktas tamsios spalvos linijas vieną ar keletą kartų. Tikėtina, kad taškai, per kuriuos linijų sekimo algoritmas praeina keletą kartų, yra kraujagyslės [3].

Taip pat darbe buvo išbandyti Miura „Maksimalaus linkio“ bei Huang „Plačių linijų sekimo“ [5] algoritmai, kurių veikimas daugeliu atveju buvo greitesnis, leido pasiekti geresnių rezultatų apdorojant blogesnės kokybės atvaizdus, bet gautas tinklas buvo labiau tinkamas palyginimo operacijoms nei numatomam linijų sekimui atlikti. Priklausomai nuo sekamų taškų skaičiaus, „Pasikartojančių linijų sekimo“ algoritmas gali būti vienas iš lėčiausių, tačiau jo rezultatas pastoviausias.

Darbe naudotų Matlab ir Lee „Piršto ploto nustatymo“ funkcijų realizacijos buvo atliktos Bram Ton [4]. Lee „Piršto ploto nustatymo“ funkcija naudojama riboms, kuriose atliekamas apdorojimo funkcijų sekimas, išskirti.

C. *Morfologinis kraujagyslių tinklo apdorojimas*

Siekiant supaprastinti ir papildomai pataisyti gautus kraujagyslių tinklų atvaizdus, daugelyje kraujagyslių autentifikaciją naudojančių biometrinių sistemų taikomos įvairios morfologinių funkcijų aibės. Šiame darbe naudotos morfologinės funkcijos yra standartinės Matlab paketo funkcijos, tačiau jų aibės pasirinkimas ir taikymo seka yra svarbūs žingsniai siekiant suformuoti norimą kraujagyslių tinklo atvaizdą.

Miura „Pasikartojančių linijų sekimo“ funkcijos išvestyje (2 pav. atvaizdas dešinėje) yra daug pavienių taškų, nedidelių neužpildytų plotų, su kitomis kraujagyslėmis nesusijungiančių atšakų ir kitokių triukšmų. Taip pat ryškiausiai matomos arba tam tikrose vietose esančios kraujagyslės gali būti sekamos daugiau kartų, todėl atrodo platesnės.

Siūlomiems raktų generavimo metodams reikalingas vieno pikselio pločio kraujagyslių tinklas, todėl pasirinkta tokia morfologinių funkcijų aibė: pavienių taškų pašalinimas (*clear*[inf]), vieno pikselio dydžio plotų, visiškai apsuptų priešingos vertės elementais, invertavimas (*fill*[1]), vieno pikselio pločio linijų trūkių sujungimas (*bridge*[inf]), pakartotinė morfologinė „uždarymo“ funkcija (*close*[1]), pikselių invertavimas, jei penki ar daugiau supantys pikseliai yra priešingos vertės 3x3 elemente (*majority*[3]), „genėjimo“ funkcija, pašalinanti vienoje puséje neprisijungusius elementus (*spur*[inf]), objektų susiaurinimas iki vieno pikselio pločio linijos, neleidžiant objektams išsiskirti (*skel*[inf]).

Kai kurie tarpiniai taškai (susijungimai ar žiedai tinkle) tokio apdorojimo metu gali būti prarandami. Taikant kitokius raktų generavimo metodus morfologinių funkcijų aibė gali būti koreguojama [6][7].

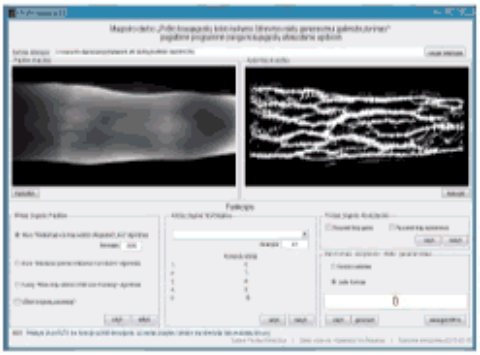
D. *Galutinis atvaizdas*

Galutinis atvaizdas po pirminio ir morfologinių funkcijų apdorojimo yra [0,1] verčių matrica, kurioje linijomis išskirtos piršto kraujagyslės. Galutinio atvaizdo pavyzdys pateikiamas 1 paveiksle (b).

(a) Neapdorotas piršto kraujagyslių tinklo atvaizdas

(b) Galutinis apdorotas kraujagyslių tinklo atvaizdas

1 paveikslas. Pradinis (a) ir galutinis (b) piršto kraujagyslių atvaizdai.



2 paveikslas. Pagalbinė Matlab grafinė sąsaja pirminių, morfologinių ir rakto generavimo funkcijų taikymui ir atvaizdavimui.

III. RAKTO GENERAVIMO ALGORITMAI

Tradicinėse autentifikavimo sistemose atvaizdas, apdorotas pirminėmis arba pirminėmis ir morfologinėmis funkcijomis,

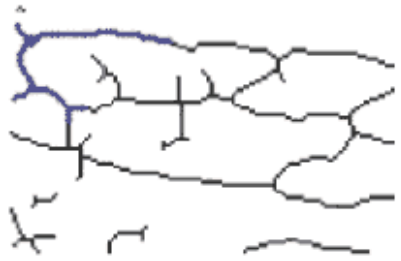
galėtų būti lyginamas su iš anksto išsaugotu šablonu. Tačiau šiame darbe, užuot atlikus palyginimą, atvaizdas toliau apdorojamas, siekiant išskirti reikšminius požymius ir sugeneruoti pastovų šifravimo raktą [8]. Šiame skyriuje aptariamos siūlomos funkcijos ir metodai raktui generuoti.

A. Reikšminių koordinačių nustatymo funkcija

Tolesnis skaitinių verčių gavimas iš kraujagyslių tinklo gali būti pagrįstas kontūrų sekimu. Tokiam metodui svarbu „žinoti" reikšmines tinklo koordinates: linijų pradžių ir pabaigų koordinates, linijų susikirtimo taškus, pradinį sekimo tašką ir kt. Šioms reikšminėms koordinatėms nustatyti darbe naudojamos matematinės morfologijos sankryžų ir galų nustatymo funkcijos. Funkcijų rezultatas yra sankryžų, pradžios ir pabaigos taškų koordinačių matricos.

B. Kontūro sekimo funkcija

Antras žingsnis pasirinktame tinklo apdorojimo metode yra kontūro sekimas. Nuo sekimo funkcijos realizacijos priklauso ir galutinis kontūro sekimo rezultatas. Darbui realizuota kontūro sekimo funkcija, sekanti tašką iki susikirtimo. Po susikirtimo aptikimo visos linijos toliau sekamos vienu metu (3 pav.). Alternatyvi sekimo funkcija galėtų sekti tik vieną iš šakų iki galutinio taško, atsitiktinai pasirinkdama kelią per sankryžas arba taikydama tam tikras ėjimo per sankryžas taisykles. Šie funkcijos veikimo aspektai turėtų įtakos galutiniam rezultatui ir jo maksimaliam kardinalumui. Tolesnėse darbo stadijose numatoma ištirti kitokių kontūro sekimo funkcijų realizacijų rezultatus.

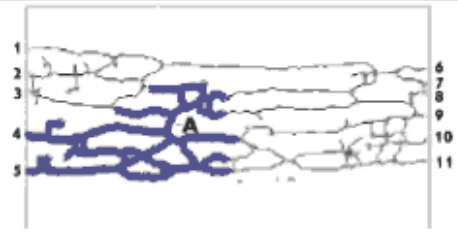


3 paveikslas. kraujagyslių tinklo atvaizdas, uždengtas sluoksniu, paryškinančiu sekamą kontūrą. Paryškinta dalis yra lygi 100 sekamo kontūro taškų, vaizdas padidintas.

Realizuota kontūro sekimo funkcija „slenka" per kraujagyslių tinklą ir priklausomai nuo jo formos, sudėtingumo ir kitų savybių, pasiekia skirtingus kraujagyslių tinklo taškus (galus ar susikirtimus) skirtingais santykiniais laiko momentais. Išvestiniai kontūro sekimo funkcijos veikimo parametrai darbe naudojami nesudėtingam raktui generuoti.

C. Kontūro sekimo iteracijų skaičiaus metodas

Šio metodo idėja yra tam tikrų, iš anksto numatytų, verčių priskyrimas kiekvienam kontūro pradžios ir pabaigos taškui ir vertinimas, kada šiuos taškus pasiekia pasirinkta kontūro sekimo funkcija. Pavyzdyje (4 pav.) kiekvienam iš kraujagyslių tinklo galų priskiriamos skaitinės vertės nuo 1 iki 11. Pasirenkamas pradinis sekimo taškas (vertė 4) ir atliekamas sekimas. Pavaizduotas sekimo funkcijos rezultatas, kai pasiekiamas pirmasis „išėjimas", atlikus 826 taškų kontūre sekimą.



4 paveikslas. Kraujagyslių tinklo kontūro sekimas pradedant nuo taško nr. 4.

- Kiekvienam pradžios ir pabaigos taškui priskirtos skaitinės vertės.

- Paryškinta sekama kontūro atkarpa po 826 kontūro sekimo algoritmo iteracijų.

- Kritinis kontūro taškas pažymėtas raide A.

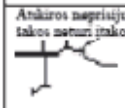
Atlikus visą sekimo ciklą, metodo rezultatas – slaptas raktas, sudarytas iš skaičių 532111910678. Skaitmenys šiame skaičiuje yra lygūs po tam tikro sekimo iteracijų skaičiaus pasiekto tinklo įėjimo/išėjimo skaitinei vertei. Algoritmo generuojamas raktas priklausytų nuo įėjimams/išėjimams priskirtų pradinių verčių ir kontūro sekimo funkcijos realizacijos. Šiame pavyzdyje naudojama III. B skyriuje aprašyta kontūro sekimo funkcija. Dalis verčių, dėl to, kad jos pasiekiamos labai artimais laiko momentais ir, atsiradus netikslumams kontūro sudaryme (pavyzdžiui netiksliai atlikus piršto lokalizaciją), galėtų įtakoti galutinį rezultatą, gali būti atmetamos. Numatomas patikimas galutinis rakto ilgis galėtų būti apie 4-8 skaitmenys.

Šio metodo privalumas – santykinai maža paklaida, jei kraujagyslių tinkle yra nedidelių neatitikimų. Metodui reikšminės įtakos neturėtų linijų krypties ar vietos pasikeitimai, atsiradę pašaliniai prie pagrindinio sekamo tinklo neprisijungę elementai, žiedai, sudėtingos geometrinės formos kontūro viduje, atsišakojimai ir netiksliai nustatytos kraujagyslių sankryžų vietos.

Daugiausiai neigiamos įtakos šiam metodui galėtų turėti netinkamai nustatyti (arba nenustatyti) kritiniai linijų susijungimai. Metodo generuojamo rakto vertė galėtų tapti netiksli, jeigu kontūre atsirastų trūkių, dėl kurių kai kurie pradžios arba pabaigos taškai taptų nepasiekiami arba pasiekiami po reikšmingai daugiau arba mažiau kontūro sekimo iteracijų. Pavyzdinio kritinio kontūro taško pavyzdys 3 paveiksle pažymėtas simboliu *A*. Jei šios jungiamčiosios

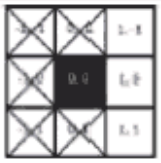
kontūro dalies nebūtų, viršutinė kraujagyslių tinklo dalis būtų pasiekiama tik per kur kas tolesnį jungiamąjį tašką tarp išėjimų 8 ir 9 ir reikšmingai pakeistų galutinį generavimo rezultatą. Taip pat metodui neigiamos įtakos turėtų sudėtingas kraujagyslių tinklas kontūro galuose, ypač jei pirštо lokalizacija būtų netiksli.

1 lentelė. „Kontūro sekimo iteracijų skaičiau metodo" privalumai ir trūkumai.

Privalumai	Trūkumai
Atskiros nepriisijungusios tinklo takos neturi įtakos rezultatui. 	Susijungimai arba trūkiai reikšminėse kraujagyslių atvaizdo tinklo vietose (pvz., tarp arti viena kitos esančių linijų) gali visiškai keisti rezultatą. 
Žiedai ir sudėtingi išsišakojimai kraujagyslių tinkle turi mažai įtakos rezultatui. 	

D. „Vandens lašo" metodas

Kontūro sekimo iteracijų skaičiaus ir kitų kontūro sekimo funkcija paremtų metodų veikimui naudojamas visas pirštо kraujagyslių kontūras. Tokiems algoritmams įtakos galėtų turėti bet kokie tinkle atsiradę netikslumai. Priešingai nei daugiakrypčiai algoritmai, siūlomas „vandens lašo" metodas yra vienakryptis. Šiame metode naudojamas kraujagyslių kontūro sekimas vyksta tik išėjimo kryptimi ir algoritmui leidžiama sukti tik +/- 45 laipsnių kampu išėjimo link (5 pav.).

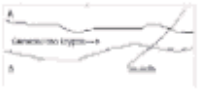


5 paveikslas. Galimos „Vandens lašo" metode naudojamos kontūro sekimo funkcijos kryptys, kai kontūras sekamas iš kairės į dešinę

Toks algoritmas padėtų išvengti neigiamos tam tikra kryptimi atsiradusių netikslumų ar susijungimų/nesusijungimų reikšminėse kraujagyslių tinklo vietose įtakos galutiniam rezultatui, pavyzdžiui, sekant kontūrą, pavaizduotą 4 pav., nuo 1, 2, 3 arba 5 kairėje pusėje esančių pradžios taškų, reikšminis sujungimas A įtakos galutiniam rezultatui neturėtų.

Tačiau priklausomai nuo išpildymo būdo, galutinis vienakrypčio metodo generuojamo rakto ilgis galėtų būti trumpesnis nei naudojant daugiakrypčius generavimo metodus. Taip pat atliekant sekimą priešinga nei numatyta kryptimi, sekimo netikslumai galimai būtų didesni nei naudojant daugiakryptį kontūro sekimą.

2 lentelė. „Vandens lašo" metodo privalumai ir trūkumai.

Privalumai	Trūkumai
Algoritmui įtakos turėtų tik tam tikra kryptimi atsiradę netikslumai. 	Algoritmas negalėtų įveikti T formos arba tinklo vietų, kur linijos sikasi arba susijungia. 

E. Papildomų reikšminių koordinačių vertinimas rakto generavimo algoritmuose

Siekiant generuoti ilgesnius slaptus raktus, anksčiau aptarti generavimo algoritmai gali būti papildyti reikšminių taškų fiksavimo funkcijomis. Pavyzdžiui, kontūro sekimo algoritmui „slenkant" per kraujagyslių kontūrą, galima fiksuoti pakelinį pereitų sankryžų skaičių arba matuoti santykinius atkarpų, per kurias atliekamas kontūro sekimas, ilgius. Toks papildomų reikšminių koordinačių fiksavimas leistų padidinti generuojamų raktų ilgį kelis kartus, tačiau raktų generavimo metodai taptų labiau priklausomi nuo tikslių pirminių funkcijų rezultatų.

IV. IŠVADOS

Šiame darbe aptariamos pirštų kraujagyslių tinklo tinkamumo slaptų raktų generavimui, nenaudojant tradicinių palyginimo funkcijų, galimybės, pristatomos kelios pagrindinės pirminio kraujagyslių tinklo apdorojimo, morfologinio išskyrimo funkcijos ir aptariami galimi slapto rakto generavimo metodai. Kituose darbuose numatoma realizuoti papildomus rakto generavimo metodus, atlikti algoritmų bandymus su skirtingomis pirminių ir morfologinių funkcijų aibėmis ir pateikti išvadas apie siūlomų metodų tinkamumą slaptų raktų generavimui.

ŠALTINIAI

[1] Algimantas Venčkauskas, Egidijus Kazanavičius. „Informacinių technologijų saugos metodai", 2011, Kaunas.

[2] N. Miura, A. Nagasaka ir T. Miyatake, „Automatic Feature Extraction from non-uniform Finger Vein Image and its Application to Personal Identification" IAPR Workshop on Machine Vision Applications, Dec. 11 - 13.2002, Nara- ken New Public Hall, Nara, Japan

[3] N. Miura, A. Nagasaka ir T. Miyatake „Feature extraction of finger vein patterns based on repeated line tracking and its application to personal identification", Machine Vision and Applications, Volume 15, Number 4 (2004), pp. 194—203

[4] Bram Ton, "Miura et al. vein extraction methods", http://www.mathworks.com/matlabcentral/fileexchange/37716-miura-et-al-vein-extraction-methods, tikrinta 2013-05-30

[5] Beining Huang, Yanggang Dai, Rongfeng Li, Darun Tang and Wenxin Li, „Finger-vein Authentication Based on Wide Line Detector and Pattern Normalization", 2010 International Conference on Pattern Recognition

[6] Petros Maragos,Ronald W. Schafer,Muhammad Akmal Butt „Mathematical Morphology and its applications to image and vygnam proce-ssing", Kluwer Academic Publishers, 1996

[7] Henk J. A. M. Heijmans „Mathematical morphology: a modern approach in image processing based on algebra and geometry" Society for Industrial and Applied Mathematics, Vol.37, No.1,pp 1-36, March 1995

[8] Wendle Zhang, Yao-Jan Chang, and Tsuhan Chen "Biometric-Based cryptographic Key Generation" 2004 IEEE International Conference on Multimedia and Expo (ICME)

6.10. Publikacija II tarptautinėje konferencijoje „Informatics and Management Sciences“

Cryptographic Key Generation from Finger Vein

Algimantas Venckauskas
Department of Computers
Kaunas University of Technology
Kaunas, Lithuania
algimantas.venckauskas@ktu.lt

Povilas Nanevicius
Department of Computers
Kaunas University of Technology
Kaunas, Lithuania
povilas.nanevicius@stud.ktu.lt

Abstract— **Bio-cryptography is a progressive technology that combines biometrics with cryptography. The use of biometric data for security purposes has become increasingly popular, but the use of biometric data in cryptography is a new, growing and promising area of research. One of the most important problems of bio-cryptography is generation of a stable encryption key. This paper proposes the method of cryptographic key generation from finger vein pattern. The approach is based on the established finger vein image pre-processing methods and authors' proposed Contour-tracing algorithm.**

Keywords- information security; cryptographic key generation; biometrics

I. INTRODUCTION

Information security today is becoming more and more important. Cryptography is one of the most effective ways to solve the problem of information security. In the cryptographic algorithms information is encrypted and decrypted using cipher keys, which can cause some problems [1]. Simple users keys are easy to be remember, but they can also easily be cracked. Complex keys are difficult to crack, but they are difficult to remember as well and may have to be stored in a medium that could get lost or stolen. In addition, the cipher keys may be illegally shared and cannot provide non repudiation. In order to solve these problems, the biometric features which cannot be forgotten, stolen or cracked, have been combined with the cryptography to form biometric cryptography. One of the most important problems of biometric cryptography is generation of stable encryption key [2].The encryption keys must be generated truly randomly, to contain sufficient entropy and be of a sufficient length [3].

Biometrics employs a number of physiological and behavioural characteristics: face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice.

One of the newest biometric methods is finger vein recognition [4, 5]. The finger vein pattern based authentication method is highly reliable; veins are hidden underneath the skin surface so forgery is extremely difficult; it is non-invasive and easy to use, offering a balance of advantages. Unique aspects of finger vein pattern recognition set this method apart from other forms of biometrics. Expazeriments indicate that equal error rate (EER) of Miura "Repeated Line Tracking" finger vein method is 0.145%. To compare, ERR in fingerprint based systems ranges from 0.2% to 4%. This indicates, that finger vein based authentication is very effective [6].

Riley et al. study [7] suggests that vein technology is more suitable for use by the older population compared to fingerprint technology. The use of fingerprint based technologies is problematic for the following reasons: it is more susceptible to the environmental conditions (dust, dirt, temperature fluctuation), fingerprint image quality is lower, fingerprints can be forged and the process of enrolment and scanning may be more complicated.

Finger vein recognition is a relatively embryonic field, new methods are developed and existing ones are examined. In this paper we explore the possibilities of key generation from finger vein patterns.

Further parts of this paper are organized as follows: section II summarizes conventional methods used to retrieve cryptographic keys from biometric characteristics. A proposed method of cryptographic key generation directly from finger vein pattern is presented in section III. Investigation and discussion of the proposed method is presented in section IV. Conclusions are provided in the last section.

II. RELATED WORK

Many cryptographic algorithms are available for securing information, but all of them are dependent on the security of the encryption or decryption key. To overcome this dependency, biometric techniques can be applied to ensure the security of keys and documents. Different methods can be used to securely store and retrieve cipher keys from biometric characteristics.

The first method involves stored template matching to unlock a cipher key storage. If the user is authenticated, the key is released. The main problem here is using an insecure storage media [8].

The second method hides the cipher key within the enrolment template itself via a secret bit-replacement algorithm. If the user is successfully authenticated, this algorithm extracts the key bits from the appropriate place and releases the key [9].

Another method is to use data derived directly from a biometric image. In this method biometric data are used to generate a cryptographic key [10]. Quality of biometric data depends on the person's physiological characteristics and is strongly influenced by the environment; it is characterized by inaccuracy. Therefore, generation of cryptographic keys directly from biometric data is challenging. There are many works, aiming to fill the gap between the fuzziness of biometrics and achieving cryptographic accuracy. This would enable keys to be generated directly from biometric images. The main problem is that biometric data is noisy and only an

approximate comparison is possible with the template. But cryptography requires that the cipher keys are absolutely correct.

Further a few works describing various methods for generating cryptographic keys directly from biometric data are analysed.

Topological fingerprint pattern minutiae point neighbourhood descriptors based approach has been proposed by Ushmaev et al. [11]. It has the following advantages: Topological descriptors are very stable fingerprint features. They don't depend on finger alignment and elastic deformations. The approach allows varying decryption rates and key lengths.

The core of bio-cryptography lies in the stability of cryptographic keys generated from uncertain biometrics. Hu et al. [12] investigated the effect on the generated keys when an original fingerprint image is rotated. Analysis indicates that information integrity of the original fingerprint image can be significantly compromised by image rotation transformation process. It was discovered that the quantization and interpolation process can change the fingerprint features significantly without affecting the visual image.

Costanzo [13] proposed an approach that eliminates the need for template storage and demonstrates how a cryptographic key can be constructed through the use of biometric feature and parametric aggregation along with certain mathematical combinatorial and permutation constructs.

Zheng et al. [14] paper presents a lattice mapping based fuzzy commitment method for cryptographic key generation from biometric data. The proposed method not only outputs high entropy keys, but also conceals the original biometric data such that it is impossible to recover the biometric data even when the stored information in the system is opened to an attacker.

Wu et al [15] proposed a novel biometric cryptosystem based on the most accurate biometric feature - iris. In this system, a 256-dimension textural feature vector is extracted from the pre-processed iris image by using a set of 2-D Gabor filters. And then a modified fuzzy vault algorithm is employed to encrypt and decrypt the data.

Unimodal biometric systems, which utilize a single trait for recognition, have certain problems like noisy sensor data, non-universality, unacceptable error rates, insufficient length and entropy of generated key. Jagadeesan et al. [16] proposed an efficient approach based on multimodal biometrics (iris and fingerprint) for generating a secure cryptographic key, where the security is further enhanced with the difficulty of factoring large numbers. At first, the features, minutiae points and texture properties are extracted from the fingerprint and iris images respectively. Then, the extracted features are fused at the feature level to obtain the multi-biometric template. Finally, a multi-biometric template is used to generate a 256-bit cryptographic key.

As seen, mainly researches were performed for generating keys using fingerprints. We propose the method of cryptographic key generation from finger vein pattern.

III. Key Generation from Finger Vein

This paper proposes a method for cryptographic key generation from finger vein pattern images.

A schematic representation or proposed cryptographic key generation method from finger vein patterns is shown in Fig. 1.

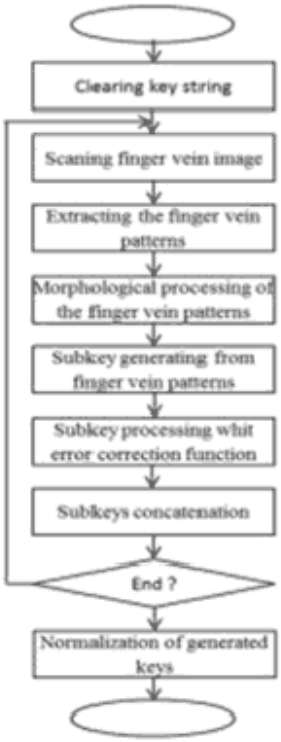


Figure 1. Schematic representations of proposed cryptographic key generation method using finger vein patterns

The essence of this method is:

1. The key is generated using multiple finger vein patterns. It's a certain implementation of pseudo-multimodality, where a biometric method is combined with a password. The password is 'entered' by providing different finger sequences for the system. A total of 10 different finger vein patterns and combinations of enrolling these images to the system allows for virtually endless number of keys to be generated. Also longer keys and keys with higher entropy can be generated.
2. Initial vein pattern image is processed using established methods: *Miura "Repeated Line Tracking"*, *Miura "Maximum Curvature"*, *Huang "Wide Line Tracking"* and additional sets of mathematical Morphology functions [17, 18, 19].

3. The processed vein pattern is used as an input to *Contour Tracing Algorithm* to generate a partial cryptographic key.
4. *Error Correcting Code* (ECC) [20] method is used to reduce the variability of biometric data.
5. Partial cryptographic keys are concatenated to combine a final cryptographic key.
6. Generated variable length cryptographic key is normalized using *Key Derivation Functions* [21].

A binary finger vein pattern $FVP(n \times m)$, previously processed using initial and morphological functions is further processed by *Meaningful Coordinate Detection Algorithm* (Fig. 2).

```
% Input:
% IMG – B/W [0,1] 1 pixel width vein image
%
% Output:
% IMG2 – reduced size image;
% VBP - Nx2 vessel beginning point matrix;
% VEP - Nx2 vessel end point matrix;
% CVP - N x 2 vessel intersection point matrix;
% xy0 - initial tracing point;

% image measurement and resize
  {IMG > CROP > IMG2}
% detecting VBP
  for i = 1:IMG2_height
    if {vein starting point detected}
      {note VBP point coordinates and assigned
       entrance number}
    end
  end
% detecting VEP
  for i = 1:IMG2_height
    if {vein end point detected}
      {note VEP point coordinates and assigned
       exit number}
    end
  end
% detecting intersections
  CVP=bwmorph(IMG2,'branchpoints',1);
% selecting initial tracing point
  {Display pattern and prompt user to select
   initial tracing point}
  xy0={user selected starting point}
```

Figure 2. Meaningful Coordinate Detection Algorithm

The supplied vein network is a 1 pixel width line in the image. Algorithm is used to identify blood vessel beginning point $VBP(n \times 2)$, vessel end point $VEP(n \times 2)$ and crossing vessel point coordinates $CVP(k \times 2)$. Finger vein pattern may be cropped depending on it's size to ensure, that vein beginning and end points reach edges of the image. Vein beginning and end points are found by scanning binary values along the edges of the image and coordinates of intersections in the network are identified using a morphological *branchpoints* function. *Meaningful coordinate Detection algorithm* is also used to visualise and allow user to select which VBP will be used as a starting point for contour tracing. Extracted coordinates will be later used by other algorithms.

Contour Tracing Algorithm (Fig. 3) is used to trace the contour and allows generating partial cryptographic key from the image processed by initial functions and with meaningful pattern points detected. The algorithm is used to identify which Vessel Beginning Points and which vessel end points are connected with a selected VBP or VEP. The contour is traced until a vessel intersection is detected. After an intersection is detected, all following branches are traced simultaneously. Fig. 4, shows a vascular pattern image with 100 initial contour points highlighted by *Contour Trace Algorithm*.

```
% Input:
% IMG – B/W [0,1] 1 pixel width vein image
% xy0 – Trace starting point
%
% Output:
% CNTR - N x 2 contour coordinate matrix

% Trace directions: [x; y]
  superposition(1)=[0;-1];
  superposition(2)=[1;-1];
  superposition(3)=[1;0];
  superposition(4)=[1;1];
  superposition(5)=[0;1];
  superposition(6)=[-1;1];
  superposition(7)=[-1;0];
  superposition(8)=[-1;-1];
% Tracing the contour
  while(1)
    {check all contour directions (point superpositions)
     starting from the xy0}
    if {contour point detected}
      {record contour point coordinate and
       algorithm iteration number}
      {invert traced point value to avoid
       repeated tracing}
    end
    if {no more points to trace}
      {exit from while(1) loop}
  end
```

Figure 3. Contour Trace Algorithm

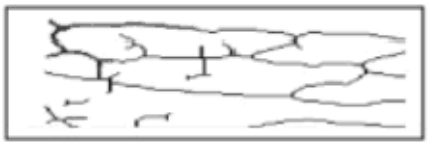


Figure 4. Finger vein patter being traced by *Contour Trace Algorithm*. The first 100 algorithm iteration points are highlighted.

Contour Trace Iteration Number Method (Fig. 5) combines the results of *Meaningful Coordinate Detection Algorithm* and *Contour Trace Algorithm*. The previously numbered vein beginning points (*VBP*) and vein end points (*VEP*) each have digital value assigned to them. When contour is traced starting from the initial point *xy0* different *VBP* and *VEP* points will be reached after a different number of *Contour Trace Algorithm* iterations.

Figure (Fig. 5) shows a vascular pattern image with values from 1 to 11 assigned in sequence to each VBP and VEP. An initial tracing point is set as point number 4 and contour is traced. Figure 5 illustrates contour tracing at a point when first 'exit' point (number 5) is reached after 826 iterations of the *Contour Trace Algorithm*.

After all accessible VBP and VEP points are reached, the values assigned to each of these points are concatenated into one partial key in order of when they were hit by the *Contour Trace Algorithm*.

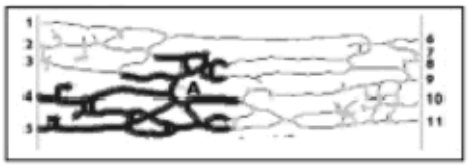


Figure 5. *Contour Trace Iteration Method* used on an image starting from VBP number 4

IV. Investigation and Discussion

Steps 1 to 3 of the proposed cryptographic key generation method using finger vascular pattern have been implemented and tested. For investigation of proposed method, a Matlab graphical testing model has been created using Bram Ton [22] implementations of *Miura "Repeated Line Tracking"*, *Miura "Maximum Curvature"* and *Huang "Wide Line Tracking"* and a set of mathematical Morphology functions. Additional functions, required for key generation were created in this research. Initial and morphological image processing and partial key generation interface are presented in Fig. 6. The model allows visualising intermediate stages of key generation. This allows to dynamically asses possible issues in steps of key generation and selects optimal settings in each step.

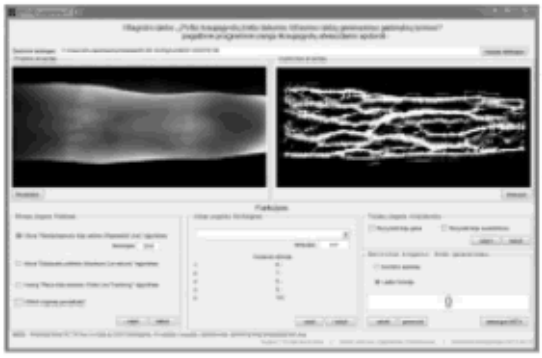


Figure 6. Matlab graphical interface

Original vascular pattern (left) and binary vein image (right) created using Miura et al. *"Repeated Line Tracking Method"* after 3000 line tracking iterations are shown in Fig. 6. Initial vascular pattern image source is Bram Ton [22].

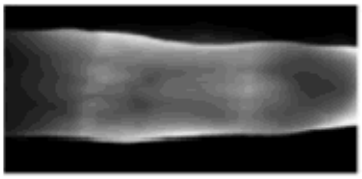


Figure 7. Initial finger vascular pattern image

Resulting image after Miura "*Repeated line tracking*" and a set of mathematical morphology functions is a binary matrix (image), where 1 pixel wide lines represent finger veins. The processed image is shown in Fig. 8.

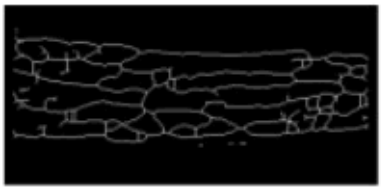


Figure 8. Processed finger vascular pattern image

Fig. 5 illustrates *Contour Trace Iteration Number Method* when the first 'exit' point is reached after tracing 826 points in the vascular pattern. After a full processing cycle a result – secret key composed of numbers „532111910678" is obtained. The sequence of numbers (a sub-key) generated by this method depends on the values assigned to the *VBP* and *VEP* points and functionality of contour trace algorithm. A previously discussed *Contour Trace Algorithm* has been used in this example.

In *Contour Trace Algorithm* the contour is traced until a vessel intersection is detected. After an intersection is detected, all following branches are traced simultaneously. An

alternative to such operation could be to trace one of the branches applying predetermined set of rules on how all following intersections should be crossed. These aspects of algorithm operation would have influence on the end result of the method, accuracy and key cardinality.

The advantage of using *Contour Trace Iteration Number Method* is a relatively small probability of error when the vein pattern image is altered insignificantly. The algorithm would not be affected by minor changes in the direction or position of certain veins in the pattern or any noise that is not directly connected to the main vein network. Algorithm is also able to manage additional loops, more complex junction structure and branches in the vein pattern. This algorithm is mostly misleading by incorrectly detected (or undetected) line connections in the main vein pattern and false *VBP*/*VEP* determination. Method generates incorrect code when when vein pattern changes significantly shortens or lengthens certain sections of the vein images. Further research will be carried out to analyse *Contour Trace Iteration Number Method* properties and possibilities for improvement.

This paper does not cover steps 4, 5 and 6 (Fig.1) of cryptographic key generation. Research of these key generation steps will be carried out in future work.

V. Conclusions

A method to generate cryptographic keys from finger vein patterns is proposed in this paper.

The pseudo-multimodal key generation method could be used to generate a virtually limitless number of keys from finger vein characteristics of an individual.

Proposed *Contour-tracing algorithm* generates cryptographic key directly from finger vein patterns without using any pre-captured samples or templates.

In the future work all steps of proposed method of cryptographic key generation will be implemented and quality properties of the generated keys will be investigated.

References

[1] A. Venckauskas, N. Jusas, I. Mikuckiene, S. Maciulevicius, "Generation of the secret encryption key using the signature of the embedded system", Information technology and control, T. 41, nr. 4, pp. 368–375, 2012.

[2] Yao-Jen Chang, Wende Zhang, Tsuhan Chen, "Biometrics-based cryptographic key generation," Multimedia and Expo, 2004. ICME '04. 2004 IEEE International Conference on , vol.3, pp. 2203,2206 Vol.3, 27-30 June 2004.

[3] C. Tilborg (Ed). Encyclopedia of Cryptography and Security. Springer, 2005.

[4] J. Hashimoto, Finger "Vein Authentication Technology and Its Future", VLSI Circuits, Digest of Technical Papers. – pp. 5–8, 2006.

[5] A. Venckauskas, N. Morkevicius, K. Kulikauskas, "Study of Finger Vein Authentication Algorithms for Physical Access Control", Electronics and Electrical Engineering, No. 5(121). – pp. 101–104, 2012.

[6] N. Miura, A. Nagasaka ir T. Miyatake, "Automatic Feature Extraction from non-uniform Finger Vein Image and its Application to Personal Identification" IAPR Workshop on Machine Vision Applications, Dec. 11 - 13.2002, Nara- ken New Public Hall, Nara, Japan, 2002.

[7] C. Riley, H. McCracken, K. Buckner, "Fingers, veins and the grey pound: accessibility of biometric technology", Proceedings of the 14th European conference on Cognitive ergonomics (ECCE'07). – New York, NY, USA, 2007. – pp. 149–152, 2007.

[8] Handbook of Information and Communication Security, P. Stavroulakis, M. Stamp (Eds.), Springer, 2010.

[9] U. Uludag, "Secure biometric systems," Ph.D. dissertation, Michigan State University, http://biometrics.cse.msu.edu/Publications/Thesis/UmutUludag_SecureBSecureBio_PhD06.pdf, 2006.

[10] M. S. Al-Tarawneh, L. C. Khor, W. L. Woo, and S. S. Dlay, "Crypto key generation using contour graph algorithm", in Proceedings of the 24th IASTED international conference on Signal processing, pattern recognition, and applications (SPPRA'06), M. H. Hamza (Ed.). ACTA Press, Anaheim, CA, USA, pp. 95-98, 2006.

[11] O. Ushmaev, V. Kuznetsov, V. Gudkov, "Extraction of Binary Features from Fingerprint Topology," Hand-Based Biometrics (ICHB), 2011 International Conference on , vol., no., pp.1,6, 17-18 Nov. 2011.

[12] Peng Zhang, Jiankun Hu, Cai Li, Mohammed Bennamoun, Vijayakumar Bhagavatula, "A pitfall in fingerprint bio-cryptographic key generation", Computers & Security, Volume 30, Issue 5, July 2011, pp. 311–319, 2011.

[13] C. R. Costanzo, "Active Biometric Cryptography (ABC): Key Generation Using Feature and Parametric Aggregation," Internet Monitoring and Protection, 2007. ICIMP 2007. Second International Conference on , vol., no., pp.28,28, 1-5 July 2007.

[14] Gang Zheng, Wanqing Li, Ce Zhan, "Cryptographic Key Generation from Biometric Data Using Lattice Mapping," Pattern Recognition, 2006. ICPR 2006. 18th International Conference on , vol.4, pp.513–516, 2006.

[15] Xiangqian Wu, Ning Qi, Kuanquan Wang, Zhang D., "An Iris Cryptosystem for Information Security", Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP '08 International Conference on, pp. 1533–1536, 2008.

[16] J. Jagadeesan, T.Thillaikkarasi, K.Duraiswamy, "Cryptographic Key Generation from Multiple Biometric Modalities: Fusing Minutiae with Iris Feature", International Journal of Computer Applications 2(6), pp. 16–26, June 2010.

[17] N. Miura, A. Nagasaka ir T. Miyatake, "Automatic Feature Extraction from non-uniform Finger Vein Image and its Application to Personal Identification" IAPR Workshop on Machine Vision Applications, Dec. 11 - 13.2002, Nara- ken New Public Hall, Nara, Japan, 2002.

[18] N. Miura, A. Nagasaka ir T. Miyatake "Feature extraction of finger vein patterns based on repeated line tracking and its application to personal identification", Machine Vision and Applications, Volume 15, Number 4, pp. 194—203, 2004.

[19] P. Maragos, R. W. Schafer, M. Akmal Butt,",,Mathematical Morphology and its applications to image and sygnam processing", Kluwer Academic Publishers, 1996.

[20] S. Kanade, D. Petrovska-Delacrétaz, B. Dorizzi, "Cancelable iris biometrics and using Error Correcting Codes to reduce variability in biometric data", Computer Vision and Pattern Recognition, 2009. CVPR 2009. IEEE Conference on , vol., no., pp.120–127, 20-25 June 2009.

[21] International Organization for Standardization. ISO/IEC FCD 18033–2, IT Security techniques — Encryption Algorithms — Part 2: Asymmetric Ciphers, 2004.

[22] T. Bram, "Miura et al. vein extraction methods", http://www.mathworks.com/matlabcentral/fileexchange/35716-miura-et-al-vein-extraction-methods.