KAUNO TECHNOLOGIJOS UNIVERSITETAS
VYTAUTO DIDŽIOJO UNIVERSITETAS
VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

MARTYNAS VAIDELYS

SAVAIME BESIFORMUOJANTYS RAŠTAI INFORMACIJOS SLĖPIMO UŽDAVINIUOSE

Daktaro disertacijos santrauka
Fiziniai mokslai, informatika (09P)

2018, Kaunas

Disertacija rengta 2013–2018 m. Kauno technologijos universitete, Matematikos ir gamtos mokslų fakultete, Matematinio modeliavimo katedroje.

Mokslinis vadovas:
Prof. habil. dr. Minvydas Kazys RAGULSKIS (Kauno technologijos universitetas, fiziniai mokslai, informatika, 09P).

Redagavo: Aurelija Gražina Rukšaitė (Leidykla "Technologija")

Informatikos mokslo krypties disertacijos gynimo taryba:
Prof. habil. dr. Rimantas BARAUSKAS (Kauno technologijos universitetas, fiziniai mokslai, informatika – 09P) – **pirmininkas**;
Prof. habil. dr. Gintautas DZEMYDA (Vilniaus universitetas, fiziniai mokslai, informatika – 09P);
Doc. dr. Kristina POŠKUVIENĖ (Kauno technologijos universitetas, fiziniai mokslai, informatika – 09P);
Prof. dr. Vacius JUSAS (Kauno technologijos universitetas, fiziniai mokslai, informatika – 09P);
Prof. dr. Miguel A. F. SANJUAN (Rey Juan Carlos universitetas, Ispanija, fiziniai mokslai, informatika – 09P).

Disertacija bus ginama viešame informatikos mokslo krypties disertacijos gynimo tarybos posėdyje 2018 m. rugsėjo 4 d. 10:00 val. Kauno technologijos universiteto Disertacijų gynimo salėje.

Adresas: K. Donelaičio g. 73-403, 44249 Kaunas, Lietuva.
Tel. (370) 37 300 042; faks. (370) 37 324 144; el. paštas doktorantura@ktu.lt.

Disertacijos santrauka išsiųsta 2018 m. rugpjūčio 3 d.
Su disertacija galima susipažinti internetinėje svetainėje http://ktu.edu, Kauno technologijos universiteto (K. Donelaičio g. 20, 44239 Kaunas), Vytauto Didžiojo universiteto (K. Donelaičio g. 52, Kaunas) ir Vilniaus Gedimino technikos universiteto (Saulėtekio al. 14, 10223 Vilnius) bibliotekose.

PADĖKA

Norėčiau išreikšti ypatingą padėką moksliniam vadovui profesoriui dr. Minvydui Ragulskiui už galimybę dirbti drauge, už mokslines idėjas ir galimybę augti kaip jaunajam mokslininkui. Jūsų patarimai, lydėję visą disertacinį laikotarpį, yra neįkainojami.

Esu dėkingas Matematinio modeliavimo katedros darbuotojams už paskatinimą studijuoti doktorantūroje. Labai svarbus buvo profesoriaus dr. Vidmanto Pekarsko padrąsinimas aktyviai dalyvauti profesoriaus dr. Minvydo Ragulskio mokslinėje grupėje.

Nuoširdų ačiū tariu savo žmonai, šeimos nariams ir draugams. Dėkoju už kantrybę, supratimą ir paramą.

Taip pat esu dėkingas visiems, kurie tiesiogiai ar netiesiogiai prisidėjo prie mano mokslinių tyrimų.

ĮVADAS

Temos aktualumas

Poreikis slėpti perduodamą informaciją atsirado nuo pat pirmųjų komunikacijos dienų. Nors iš pradžių tai daugiausia buvo taikoma karinėje srityje, tačiau sparti interneto plėtra ir augantis naudojimas viešojoje erdvėje didino poreikį apsaugoti verslo, medicinos ar asmeninius duomenis, pinigines perlaidas ir kitose srityse perduodamą informaciją. Priklausomai nuo informacijos tipo, taikomos kriptografijos, steganografijos ir vandens ženklų technologijos, kurios neretai yra derinamos tarpusavyje, siekiant užtikrinti aukščiausią apsaugos lygį. Srityse, kuriose būtinas privatumas, neaptinkamumas ir konfidencialumas, svarbų vaidmenį atlieka steganografijos ir vizualinės kriptografijos principai. Tačiau šios technikos atskirai tampa jautrios atakoms, vos tik paviešinamas kodavimo algoritmas. Taigi, šiuo metu reikalingos patikimos, steganografiškai saugios ir greitos informacijos slėpimo technikos.

Sudėtingi savaime besiformuojantys raštai, pagrįsti biologiniais, cheminiais ar fizikiniais procesais, buvo sėkmingai pritaikyti slaptai vizualinei informacijai slėpti ir perduoti. Saugios steganografinės komunikacijos algoritme sėkmingai naudojamas Beddingtono ir DeAngelis (Beddington-DeAngelis) tipo „grobuonies-aukos“ modelis su savidifuzija ir kryžmine difuzija. Slaptai vizualinei informacijai slėpti ir perduoti pasitelkiami savaime besiformuojantys raštai (angl. *self-organizing patterns* (SOP)), kuriuos sukelia „kalinio dilemos“ tipo sąveikos tarp konkuruojančių individų. Komunikacijos algoritmui realizuoti reikalingi du sugeneruoti raštai, o skirtumas tarp šių raštų išryškina paslėptą vaizdą. Tačiau šie metodai pasižymi skaičiavimo spartos problemomis ir nejautrumu mažoms vietinėms perturbacijoms, todėl tyrimus savaime besiformuojančiais raštais (SOP) pagristų algoritmų srityje būtina plėtoti. Informacijai slėpti taip pat buvo sukurtas dinaminės vizualinės kriptografijos (angl. *dynamic visual cryptography* (DVC)) algoritmas, pagrįstas optinio laike vidurkinto muaro technika. Šis metodas yra pranašesnis už SOP, kadangi, virpinant ar deformuojant vaizdą, į muaro gardeles įterptam slaptam vaizdui iššifruoti užtenka žmogaus regos sistemos; be to, komunikacijos metu naudojamas tik vienas vaizdas. Natūralus dinaminės vizualinės kriptografijos (DVC) išplėtimas galėtų būti fizikinio proceso, apibūdinančio deformacijos dėsnius slaptos informacijos šifravimo ir iššifravimo procesuose stochastinėse deformuojamose muaro gardelėse, pasitelkimas.

Įvairūs raštų formavimo mechanizmai ir parametrai lemia tai, kad sukuriami skirtingų savybių vaizdai, todėl būtina įvertinti jų sudėtingumą ir tinkamumą informacijai slėpti. Vaizdų analizėje sėkmingai taikomi standartiniai metodai, tokie kaip Shannono entropija, eilučių (stulpelių) koreliacija, vaizdo taškų analizė ar steganografinių savybių aptikimas. Tačiau fizikiniai procesai gali formuoti sudėtingus raštus ir išsaugoti papildomą informaciją kaip mažo

mastelio erdvinį chaosą, todėl reikalingi nauji identifikavimo būdai.

Tyrimo objektas – vaizdinės informacijos slėpimas pasitelkiant savaime besiformuojančius raštus.

Tyrimo tikslas – sukurti savaime besiformuojančių raštų principu pagrįstus matematinius modelius ir algoritmus, tinkančius vaizdinei informacijai slėpti ir perduoti.

Pagrindiniai tyrimo uždaviniai:

1. Sukurti efektyvius ir steganografiškai saugius skaitmeninio vaizdo slėpimo algoritmus, paremtus savaime besiformuojančių raštų principu, kurie būtų tinkami slaptai vaizdinei informacijai perduoti.
2. Sukurti matematinius pagrindus vaizdams formuoti harmoninius virpesius generuojančių struktūrų paviršiuje.
3. Sukurti naujus algoritmus, skirtus savaime besiformuojančių raštų sudėtingumui vertinti.

Metodai, programinės priemonės ir eksperimentinė įranga

• Dinaminės vizualinės kriptografijos koncepcijai, pagrįstai netiesiniais virpesiais, kurti ir realizuoti naudojami informacijos vizualizavimo ir apdorojimo metodai.

• Tyrimuose naudojami optinio muaro skaičiavimai ir teorija, ji praplečiama ir toliau vystoma.

• Eulerio metodas naudojamas cheminei reakcijai imituoti ir skaitinėms diferencialinėms lygtims integruoti.

• Tiesinių rekurentinių sekų (angl. *linear recurrent sequences* (LRS)) teorija naudojama algebrinei bet kurio 2D vaizdo aproksimacijai konstruoti.

• „Matlab R2016a“ paketas naudojamas skaičiavimams atlikti ir eksperimentiniams įrankiams kurti.

• „COMSOL Multiphysics“ (programinis paketas, paremtas baigtinių elementų metodo modeliavimu) naudojamas deformacijos laukui modeliuoti.

Ginami teiginiai

• Įprasti steganografijos metodai dažniausiai yra jautrūs steganalizei ir neužtikrina komunikacijos saugumo. Savaime besiformuojančius raštus, paremtus biologiniais, cheminiais ar fizikiniais procesais, galima sėkmingai pritaikyti kaip papildomą apsaugos sluoksnį slepiant konfidencialią vaizdinę informaciją.

• Dinaminės vizualinės kriptografijos algoritmas, paremtas harmoninės muaro gardelės deformavimu harmoniniais virpesiais pagal numatytą tikrinę baigtinių elementų formą, leidžia paslėpti konfidencialią informaciją naudojant tik vieną skaidrę. Algoritmo pritaikymas Ronchi gardelei palengvina muaro vaizdo suformavimą ant fizinių objektų paviršių.

• Būtina apsvarstyti saugiai komunikacijai naudojamo vaizdo tinkamumą. 2-LRS pseudorangas gali suteikti daugiau informacijos apie vaizdo sudėtingumą.

Darbo mokslinis naujumas ir praktinė svarba

• Siūlomi informacijos slėpimo metodai, pagrįsti SOP, išsprendžia ankstesnių panašaus tipo algoritmų trūkumus. Galimybė nenaudoti atsitiktinių pradinių sąlygų ir perturbacijas atlikti savaime besiformuojančio rašto generavimo metu padidina komunikacijos algoritmo saugumą.

• Įgyvendintas deformuojamose vienmatėse gardelėse, virpinamose pagal iš anksto nusakytą fizikiniais procesais pagrįstą tikrinę formą, dvimačių skaitmeninių dichotominių slaptų vaizdų kodavimo algoritmas. Deformuojamo kūno tikrinė forma veikia kaip vizualinės komunikacijos algoritmo dekodavimo raktas.

• 2-LRS galima pritaikyti savaime besiformuojančių raštų sudėtingumo analizei atlikti. Priešingai nei Shannono entropija, 2-LRS galima pasitelkti vertinant savaime besiformuojančių atvaizdų sudėtingumą kiekvienos erdvinės koordinatės atžvilgiu ir transformacijoms iš mažo mastelio į didelio mastelio erdvinį chaosą aptikti.

Darbo rezultatų aprobavimas

Pagrindiniai disertacijos rezultatai paskelbti 8 moksliniuose straipsniuose, iš jų 6 straipsniai Mokslinės informacijos instituto (ISI) pagrindinio sąrašo leidiniuose su citavimo indeksais; 2 paskelbti recenzuojamuose konferencijų leidiniuose. Disertacijoje nagrinėjamos problemos pristatytos dviejose tarptautinėse konferencijose.

Disertacijos struktūra

Daktaro disertaciją sudaro įvadas, 4 pagrindiniai skyriai, išvados, literatūros sąrašas ir autoriaus publikacijų sąrašas. Disertacijos pagrindinėje dalyje yra 53 paveikslai, 2 lentelės ir 143 šaltinių cituojamos literatūros sąrašas.

1. LITERATŪROS APŽVALGA

Duomenų saugumu susirūpinta gerokai anksčiau, nei atsirado skaitmeniniai komunikacijos būdai. Iš pradžių duomenys buvo saugomi fiziniu būdu, slepiant ar koduojant paprastais šifravimo algoritmais, pvz., Cezario šifras, o vėliau – pasitelkiant mašinas, pvz., „Enigma“ mašina, naudota Antrojo pasaulinio karo metu kariniams duomenims koduoti ir dekoduoti; o dabar šiam tikslui tarnauja kompiuterinė įranga (Simon, 2011). Sparčiai augantis ir plačiai praktikuojamas duomenų apdorojimas elektroninėje erdvėje bei internetu vykdomi verslo sandoriai kartu su tarptautinio terorizmo atakų grėsme skatina ieškoti geresnių metodų kompiuteriams ir juose saugomai, apdorojamai ir perduodamai informacijai apsaugoti, nesvarbu, ar ta informacija priklauso

kariuomenei, vyriausybei, korporacijoms, ar civiliams gyventojams (Kaur ir kt., 2014).

Išskiriama begalė informacijos slėpimo technikų, skirtų įvairiems tikslams ir paskirtims, kurias iš esmės galima suskirstyti į kriptografiją, steganografiją ir vandens ženklus (Cheddad ir kt., 2010).

Kriptografija apibrėžiama kaip sistema, su kuria įprastus įrašus (dažniausiai rašytinius ar skaitmeninius duomenis) galima paversti į neperskaitomus, pasitelkiant sudėtingus kompiuterinius algoritmus (Mishra ir kt., 2015). Tačiau tradicinė kriptografija turi trūkumų, tokių kaip raktų platinimas (Maqsood ir kt., 2017), šifro teksto prieinamumas pašaliniam asmeniui, pasyvios atakos (Moizuddin ir kt., 2017) ir skaičiavimo greitis.

Vizualinė kriptografija (angl. *visual cryptography* (VC)) (Weir ir kt., 2012) – tai kriptografijos šaka, kuri leidžia vaizdinę informaciją užkoduoti tokiu būdu, kad šiai informacijai iššifruoti užtektų žmogaus regos sistemos. 1994 m. mokslininkai Naoras ir Shamiras pasiūlė slaptų skaidrių algoritmą, kurio principas yra tas, kad šifruojamas dvejetainis vaizdas yra dalijamas į keletą dalių; šias dalis sudėjus kartu, išryškinamas slaptas vaizdas (Naor ir kt., 1994). Vėliau vietoje stãtinės skaidrių superpozicijos buvo pasiūlyta nauja koncepcija – dinaminė vizualinė kriptografija (DVC) (Ragulskis ir kt., 2009a).

Steganografija yra technika, kurios metu kituose objektuose yra slepiamas pats slaptos informacijos egzistavimo faktas. Modernioji steganografija užtikrina perduodamų duomenų privatumą, autentiškumą, vientisumą, prieinamumą ir konfidencialumą (Sheshasaayee ir kt., 2017). Tačiau dėl didelio šio metodo pažeidžiamumo kartu derinamos kitos technikos, tokios kaip kriptografija (Zhou ir kt., 2016), vizualinė kriptografija (Nandakumar ir kt., 2011) ar fizikiniais procesais pagrįsti raštai (Saunoriene ir kt., 2011; Ishimura ir kt., 2014).

Erdvinių raštų formavimas yra pagrindinė fizikos, chemijos ir biologijos srityse egzistuojančių natūralių sistemų savybė. Raštų formavimas tiriamas taikant dalines diferencialines lygtis (Saunoriene ir kt., 2011; Ishimura ir kt., 2014; Barkley ir kt., 1990), sudėtingas sąveikas tarp konkuruojančių asmenų (Ziaukas ir kt., 2014), netiesinius konkurencingai susietus iteracinius modelius (Killingback ir kt., 2013) ar susietų iteracinių modelių tinklus (Xu ir kt., 2016).

Ne visi raštai ar raštų formavimo mechanizmai yra tinkami konfidencialiai informacijai slėpti dėl jų neatsparumo statistinei analizei ar ekspertinei patikrai. Stipriosios ir silpnosios metodų pusės įvertinamos, pvz., taikant vaizdo taškų ar spalvų paletės raštų analizę, vizualinę vaizdo patikrą, automatizuotą steganografinių požymių aptikimą (Johnson ir kt., 2012), santykinę entropiją tarp nepakeisto vaizdo ir steganografinio vaizdo (Roy ir kt., 2016), įvertinant rašto tekstūros ypatybes (Yang ir kt., 2014) ar taikant kitus metodus.

2. VIZUALINĖS INFORMACIJOS SLĖPIMAS PASITELKIANT SAVAIME BESIFORMUOJANČIUS RAŠTUS

Šiame skyriuje aprašyti keli savaime besiformuojančių raštų generavimo būdai bei pavaizduotas konfidencialios informacijos slėpimas ir perdavimas tarp siuntėjo ir gavėjo.

Ankstesnių tyrimų sukurti raštų formavimo algoritmai turi tam tikrų trūkumų bandant juos pritaikyti slaptiems vaizdams perduoti. Savaime besiformuojantis raštas, pagrįstas reakcijos ir difuzijos ląstelinio automato modeliu, aiškiai primena pradinį vaizdą ir negali būti laikomas vaizdo slėpimo algoritmu (Ishimura ir kt., 2014). Savaime besiformuojantys raštai, paremti Tiuringo nestabilumu ir sugeneruoti naudojant Beddingtono ir DeAngelis tipo „grobuonies-aukos“ modelį, turi trūkumą, susijusį su skaičiavimo greičiu (Saunoriene ir kt., 2011; Ishimura ir kt., 2014). Greičio problema buvo išspręsta erdvinio evoliucinio 2×2 žaidimo modelyje (Ziaukas ir kt., 2014), tačiau čia iškilo kita problema, susijusi su sistemos nejautrumu mažoms vietinėms perturbacijoms.

Pagrindinis šio skyriaus tikslas – sukurti algoritmą, kuris būtų steganografiškai saugus, slapta vaizdinė informacija būtų koduojama tik šiek tiek pakeičiant pavienius vaizdo taškus, ir kad šis komunikacijos algoritmas būtų efektyvus greičio atžvilgiu.

2.1. Konkurencingai susietas iteracinis modelis slaptai vaizdinei informacijai slėpti[1]

Panagrinėkime vienmatį vaizdavimą, išreikštą $f(x) = x \cdot F(x)$, kur $F: \mathbb{R} \to \mathbb{R}$. Naudosime Maynardo Smitho garbei (Killingback ir kt., 2013) pavadintą funkciją

$$F(x) = \eta(1 + x^b), \tag{1}$$

čia η ir b parametrai yra teigiamos konstantos. Dvimatis šio vaizdavimo apibendrinimas, į modelį įvedant konkurencingumo aspektą, sukelia tam tikros būsenos $x(t)$ evoliuciją t laiko momentu stačiakampėje srityje $[1; L_x] \times [1; L_y]$:

$$x_{i,j}(t+1) = x_{i,j}(t) \cdot F\left[x_{i,j}(t) + \alpha \cdot \Sigma_{i,j}(t)\right]. \tag{2}$$

Čia

---

[1] *Šiame skyriuje pristatomi rezultatai buvo publikuoti straipsnyje*:

Competitively coupled maps for hiding secret visual information
Vaidelys M., Ziaukas P., Ragulskis M.

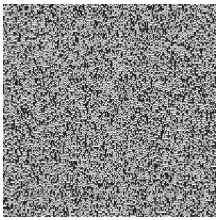
$$\Sigma_{i,j}(t) = \sum_{p,q\in\{-1,0,1\}(p,q)\neq(0,0)} x_{k,l}(t),$$
$$k = mod(i+p-1, L_x)+1; l = mod\big(j+q-1, L_y\big)+1, \quad (3)$$

yra 8 aplink elementą $x_{i,j}(t)$ išsidėsčiusių Mūro kaimynų suma; α yra neneigiamas parametras, žymintis konkurencijos tarp kaimyninių elementų stiprumą. Atkreipkite dėmesį, kad lokali dinamika yra siejama su konkurencine, o ne difuzine sąveika. Modelyje taikomos 2D periodinės kraštinės sąlygos; L_x ir L_y apibrėžia elementų skaičių stačiakampėje srityje. Kur kiekvienas $x_{i,j}$ elementas žymi vieną skaitmeninio vaizdo tašką.

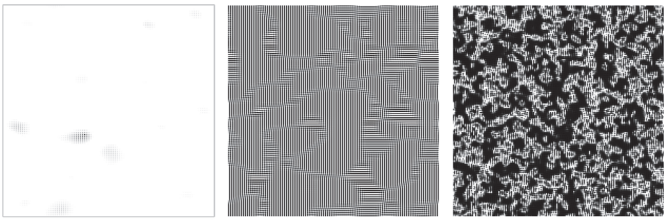
2.1.1. Savaime besiformuojančių raštų generavimas

Chaotinis logistinis žemėlapis $a_{i+1} = ra_i(1-a_i)$ (čia $r = 4$, $a_0 \in [0; 1]$) naudojamas visų 200×200 srityje esančių elementų pradinėms būsenoms generuoti, kurių vertės pasiskirsčiusios intervale [0,1] (Yu ir kt., 2017). Sugeneruotas pradinis skaitmeninis vaizdas pateiktas 2.1 pav.

Maynardo Smitho funkcijos (1) parametrai (η ir b), konkurencinės sąveikos tarp kaimyninių elementų stiprumas α ir iteracijų skaičius n turi didelį poveikį savaime besiformuojančių raštų generavimui. Skirtingi šių parametrų deriniai lemia skirtingų raštų formavimąsi (2.2 pav.).



2.1 pav. Logistinio žemėlapio nuosekliai generuojamos pseudoatsitikinės pradinės sąlygos; pradinė vertė $a_0 = 0{,}05$; matmenys $L_x = L_y = 200$



a) b) c)

2.2 pav. Maynardo Smitho iteraciniu modeliu (1) kuriami raštai priklauso nuo sistemos parametrų (pradinės sąlygos vienodos). Parametrų $\eta = 5$, $\alpha = 0{,}25$, $b = 1$ rinkinys nesukuria rašto net po 300 iteracijų (a). $\eta = 4$, $\alpha = 0{,}26$, $b = 2$ sukuria raštą po 300 iteracijų (b). $\eta = 7$, $\alpha = 0{,}3$, $b = 4$ raštas sukuriamas vos po 6 iteracijų (c)

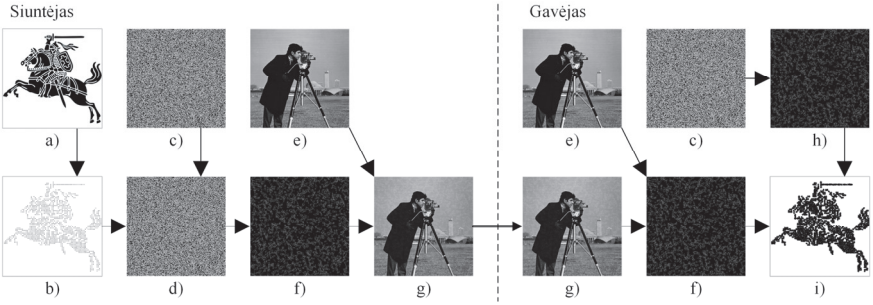
2.1.2. Komunikacijos algoritmas

Savaime besiformuojančius raštus (SOP) galima efektyviai pritaikyti kaip vaizdus slaptai vaizdinei informacijai perduoti. Siuntėjas ir gavėjas gali naudoti asimetrinį (sutartinį) protokolą pradinei vertei a_0 ir iteracijų skaičiui n, reikalingam SOP raštui generuoti, nustatyti (SOP parametrai η, α, b, L_x, L_y turi būti iš anksto apibrėžti).

Komunikacijos algoritmą, kai SOP generuojamas naudojant konkurencingai susietus iteracinius modelius, galima pavaizduoti 2.3 pav. pateikta srauto diagrama. Siuntėjas nuskaito a_0 parametrą ir iš pradinių sąlygų, pasitelkdamas logistinį žemėlapį, generuoja atsitiktinį vaizdą ((c) dalis). Slaptas vaizdas taškine skeletine forma įterpiamas į atsitiktinį pradinių sąlygų vaizdą, atsitiktine tvarka pridedant ar atimant 0,01 prie / iš atitinkamų atsitiktinio vaizdo taškų (gerokai žemiau triukšmo lygio) ((d) dalis).

Toliau siuntėjas vykdo rašto formavimo algoritmą ir iš modifikuotų pradinių sąlygų ((d) dalis) sukuria SOP vaizdą ((f) dalis). Siekdamas nuslėpti įtartino SOP vaizdo perdavimą, siuntėjas paslepia SOP vaizdą ((f) dalis) dengiančiajame vaizde (angl. *cover image*), pasitelkdamas standartinį dengiantįjį vaizdą ((e) dalis) ir standartinį mažiausiai reikšmingu bitu pagrįstą steganografinį algoritmą. Gautas vaizdas ((g) dalis) perduodamas gavėjui.

Gavėjas naudoja tą patį dengiantįjį vaizdą ((e) dalis) ir gautą vaizdą ((g) dalis), kad atkurtų SOP vaizdą ((f) dalis). Tada, naudojant tą patį parametrą a_0 ir pasitelkiant logistinį žemėlapį ((c) dalis), generuojamas atsitiktinis pradinių sąlygų vaizdas. Gavėjas naudoja identišką rašto formavimo algoritmą, kurį naudojo siuntėjas, ir sukuria savo SOP vaizdo kopiją ((h) dalis). Išryškintas gauto ir sugeneruoto SOP vaizdų skirtumas atskleidžia paslėptą informaciją ((i) dalis).

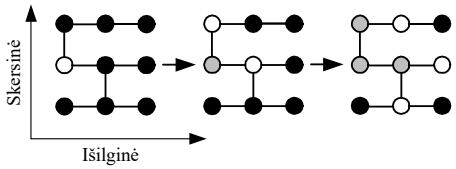


2.3 pav. Komunikacijos algoritmo diagrama: (a) originalus vaizdas; (b) taškinis skeletinis atvaizdas; (c) pradinės sąlygos; (d) perturbuotos pradinės sąlygos; (e) dengiantysis vaizdas; (f) perturbuotas savaime besiformuojantis raštas; (g) perturbuotas pradinis vaizdas; (h) savaime besiformuojantis raštas; (i) skirtuminis vaizdas

2.2. Vaizdo slėpimo algoritmas, paremtas prieširdžių virpėjimo modeliu[2]

Prieširdžių raumuo sudarytas iš miocitų, kurie sudaro pirminę audinio struktūrą. Šioje struktūroje ląstelės daugiau jungiasi išilginėmis (angl. *longitudinal*) (galas su galu) nei skersinėmis (angl. *latitudinal*) (šonas su šonu) jungtimis, todėl primena signalų perdavimą kabeliu (Luke ir kt., 1991; Nakamura ir kt., 2011).

Bendroji kabelio tipo perdavimų idėja (Christensen ir kt., 2015), imituojanti sujungtų širdies raumens ląstelių tinklą, yra įgyvendinta diskrečiame tinklelyje, kaip pavaizduota 2.4 pav. Atsižvelgiama į tris galimas ląstelių būsenas: ramybės būseną, sužadinimo būseną ir refraktorinę būseną. Ramybės ir sužadintos būsenos ląstelės sąveikauja dviem kryptimis su skirtingomis tikimybėmis: l išilginės krypties ir ν skersinės krypties. Sužadinta ląstelė iškart pereina į refraktorinę būseną, ir tokios būsenos išlieka τ laiko tarpą (kaip pavaizduota 2.4 pav.).



2.4 pav. Sąveikos tarp tinklą sudarančių ląstelių diagrama. Ramybės būsenos ląstelės (juodos) ir sužadintos ląstelės (baltos) sąveikauja dviem kryptimis su skirtingomis tikimybėmis. Ramybės būsenos ląstelė sužadinama, kai sąveikauja su kita sužadinta ląstele. Sužadinta ląstelė pereina į refraktorinę būseną (pilka) τ laiko tarpui

2.5 pav. (a) Stimuliuojančios ląstelės pradinę vertikalią bangą sužadina kairėje pusėje. (b) Viena ląstelė funkcionuoja netinkamai ir blokuoja bangų fronto sklidimą. (c) Dėl vertikalių jungčių tarp išilginių kabelių vykstantis procesas generuoja raštą

[2] *Šiame skyriuje pristatomi rezultatai buvo publikuoti straipsnyje*:

Image hiding scheme based on the atrial fibrillation model
Vaidelys M., Ragulskiene J., Ziaukas P., Ragulskis M.
Applied Sciences, 2015

Ląstelių sąveiką gali stipriai apsunkinti netinkamai funkcionuojančios ląstelės (žr. 2.5 pav.). Disfunkcinės ląstelės gali blokuoti sužadinimo bangos frontą, kuris persiduoda į dešinę pusę (2.5 pav. (b) dalis), o bangų frontų sąveika gali generuoti skirtingus raštus, kaip pavaizduota 2.5 pav. (c) dalyje.

Pristatytas prieširdžių virpesių modelis yra apytikrė sudėtingų širdies audinyje vykstančių biologinių procesų aproksimacija. Sudėtingų širdyje vykstančių reiškinių negalima modeliuoti taikant šį prieširdžių virpesių modelį.

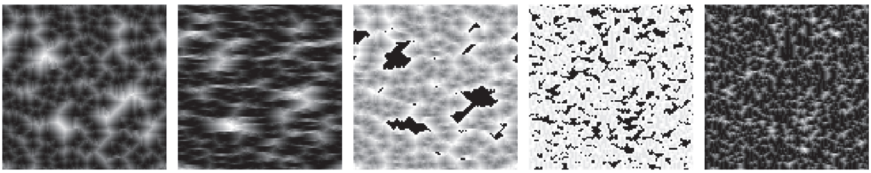
2.2.1. Savaime besiformuojančių raštų generavimas

Pradinis prieširdžių virpėjimo (angl. *atrial fibrillation* (AF)) skaičiavimų modelis, kaip pavaizduota 2.5 pav., gerai išvystytiems raštams formuoti reikalauja daug iteracijų. Bangos frontas privalo sklisti per visą plokštumą (ir, pageidautina, daugiau kaip vieną kartą); jis turi susidurti su visomis sutrikusios funkcijos ląstelėmis.

Panagrinėkime alternatyvų skaičiavimų modelį, kuriame visų ląstelių pradinės būsenos yra tolygiai atsitiktinai pasiskirsčiusios intervale $[0; 1]$. Chaotinis logistinis žemėlapis su $a_0 = 0{,}02$ pradine verte yra naudojamas chaotinei sekai generuoti (panašiai, kaip 2.1 pav.); sugeneruotos sekos diskrečiosios vertės yra nuosekliai priskiriamos kiekvienam tinklelio mazgui (eilė po eilės). Šio metodo pranašumas yra tas, kad viena atsitiktinių skaičių generatoriaus pradinė sekos reikšmė apibrėžia visas būsenas ir ryšius tarp ląstelių.

Ląstelė nustatoma būti sužadintos būsenos, kai tinklelio mazgo vertė yra mažesnė nei δ; $0 < \delta \ll 1$. Taigi, pradinėje būsenoje bus sužadinta tik $\delta \cdot 100$ proc. ląstelių. Ta pati taisyklė taikoma jungčių žemėlapiui sukurti, tačiau skersiniams ryšiams apibrėžti vietoje δ naudojama skersinių ryšių tikimybė ν.

Keletas tipinių raštų pavaizduota 2.6 pav.

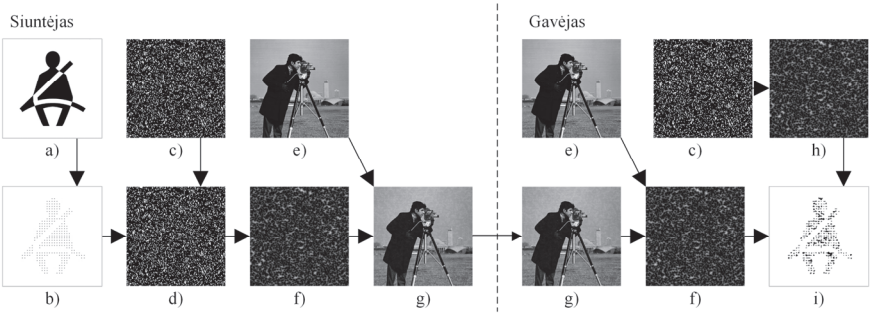


2.6 pav. Savaime besiformuojančių raštų (SOP) palyginimas esant skirtingoms parametrų reikšmėms. (a) $\nu = 0{,}1$, $\tau = 20$, $n = 20$, $\delta = 0{,}001$ (b) $\nu = 0{,}9$, $\tau = 20$, $n = 20$, $\delta = 0{,}001$ (c) $\nu = 0{,}5$, $\tau = 20$, $n = 10$, $\delta = 0{,}001$ (d) $\nu = 0{,}5$, $\tau = 10$, $n = 2$, $\delta = 0{,}1$ (e) $\nu = 0{,}5$, $\tau = 10$, $n = 8$, $\delta = 0{,}1$

2.2.2. Komunikacijos algoritmas

SOP pagrįstas slaptos vizualinės komunikacijos algoritmas naudojant AF modelį yra iliustruotas 2.7 pav. ($\nu = 0{,}2$, $\tau = n = 20$, $\delta = 0{,}08$). Sistemos parametrai ν, τ, δ, L_x, L_y ir pseudoatsitiktinė pradinė sekos reikšmė a_0 privalo

būti nusakyta iš anksto. Komunikacijos algoritmas analogiškas aprašytam 2.1.2 skirsnyje. Pagrindinis šio algoritmo privalumas, palyginti su Maynardo Smitho modeliu paremtu algoritmu, yra didesnė informacijos talpa ir sudėtingesni raštai.



2.7 pav. Komunikacijos algoritmo diagrama: (a) originalus vaizdas; (b) taškinis skeletinis atvaizdas; (c) pradinės sąlygos; (d) perturbuotos pradinės sąlygos; (e) dengiantysis vaizdas; (f) perturbuotas savaime besiformuojantis raštas; (g) perturbuotas pradinis vaizdas; (h) savaime besiformuojantis raštas; (i) binarinis skirtuminis vaizdas

2.3. Skaitmeninių vaizdų komunikacijos algoritmas, pagrįstas lūžtančiomis spiralinėmis bangomis[3]

Visi aukščiau aptarti skaitmeninių vaizdų komunikacijos algoritmai yra pagrįsti pradinių sąlygų pakeitimu SOP formavimo metu. Savybė, kai SOP generuoti nėra būtinos atsitiktinės pradinės sąlygos, užkirstų kelią sukčiavimo atakoms ir būtų svarbus pranašumas komunikacijos algoritmo saugumo atžvilgiu.

Šiame poskyryje spiralinėms bangoms modeliuoti sužadinamoje ir virpinamoje terpėje naudojamas Barkley modelis (Barkley ir kt., 1990; Dowle ir kt., 1997). Modelis susideda iš reakcijos ir difuzijos lygčių sistemos, apibrėžiančios sąveiką tarp aktyvatoriaus u ir inhibitoriaus v:

$$\begin{cases} \dfrac{\delta u}{\delta t} = f(u,v) + \nabla^2 u, \\ \dfrac{\delta v}{\delta t} = g(u,v) + D\nabla^2 v, \end{cases} \tag{4}$$

[3] *Šiame skyriuje pristatomi rezultatai buvo publikuoti straipsnyje*:

Digital image communication scheme based on the breakup of spiral waves
Vaidelys M., Lu C., Cheng Y., Ragulskis M.

čia $f(u,v)$ ir $g(u,v)$ yra kinetinės reakcijos funkcijos, D parametras yra difuzijos koeficientų santykis. Reakcijos dedamoji $f(u,v)$ užrašoma formule:

$$f(u,v) = \frac{h(x)}{\varepsilon} u(1-u)(u-u_{th}(v)), \tag{5}$$

čia ε parametras nustato laiko mastelio atskyrimą tarp greitos u lygties ir lėtos v lygties (todėl ε reikšmė dažniausiai yra maža); $h(x)$ ir $u_{th}(v)$ funkcijos apibrėžia lėto kintamojo evoliuciją. Paprasčiausiu atveju:

$$h(x) = 1, \;\; u_{th}(v) = \frac{v-b}{a}, \tag{6}$$

čia a ir b yra sistemos parametrai – dėl didesnio a gaunama ilgesnė sužadinimo trukmė, o didesnis b/a santykis duoda didesnę sužadinimo ribą.

Spiralinė banga vystosi į nereguliarią spiralinę bangą su pertrūkiais, kai reakcijos dedamoji g yra netiesinė funkcija (kaip siūlo Bär ir kt., 1993):

$$g(u,v) = u^3 - v. \tag{7}$$

Ši reakcija modeliuojama taikant paprastą Eulerio schemą; Laplaso operatorius modeliuojamas naudojant baigtinių skirtumų metodą reguliariame kvadratiniame tinklelyje su penkių taškų formule (Dowle ir kt., 1997):

$$\frac{\nabla^2 u}{4} = \frac{1}{4}\left(u_{i+1,j} + u_{i-1,j} + u_{i,j+1} + u_{i,j-1}\right) - u_{i,j}. \tag{8}$$

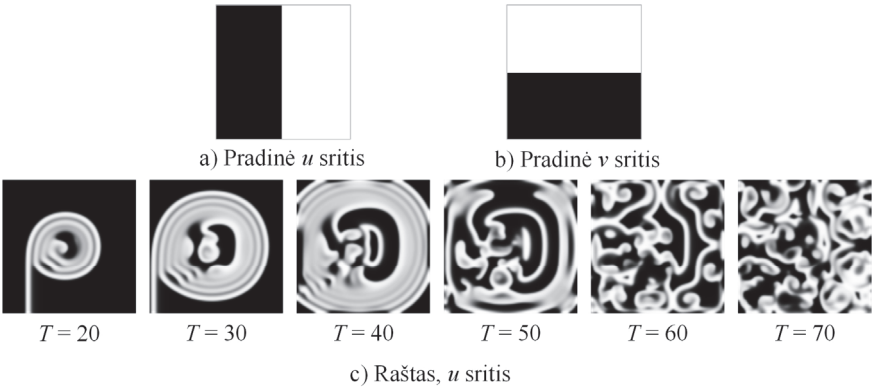
Derinant penkių taškų formulę su dideliais laiko žingsniais, reakcija gali būti pagreitinta su santykinai mažais skaičiavimo pajėgumais.

2.3.1. Savaime besiformuojančių raštų generavimas

Sritis atvaizduojama kaip dvimatis L dydžio kvadratas su uždaromis (angl. *zero-flux*) kraštinėmis sąlygomis. Pradines sąlygas nustatome kaip dvireikšmes sritis (vertikalias – u, horizontalias – v), kuriuose juoda spalva atitinka 0, o balta – 1 (2.8 pav.). Laiko žingsnis dt nustatomas 0,05; skaičiavimui atlikti reikalingas laiko periodas žymimas T. Pasirenkami a, b ir ε parametrai, kaip aptarta (Barkley, 2008). Besivystanti spiralinė banga, kuri galiausiai visiškai lūžta, pavaizduota 2.8 pav., kai $T = 20, 30, 40, 50, 60$ ir 70.

2.3.2. Informacijos slėpimo algoritmas

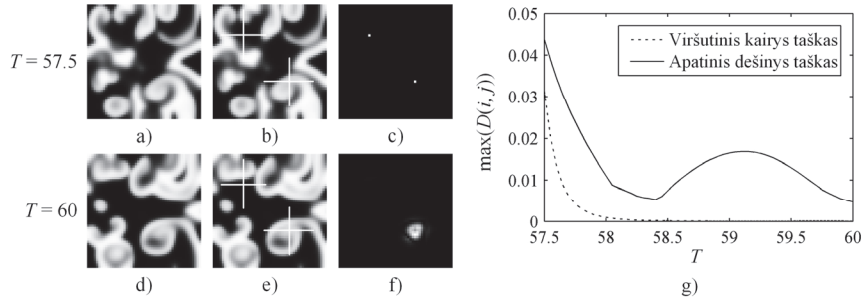
Kaip aprašyta 2.1 ir 2.2 skirsniuose, SOP raštais pagrįstam skaitmeninio vaizdo komunikacijos algoritmui konstruoti reikalingi du suformuoti raštai. Antrasis vaizdas gaunamas slaptą informaciją atspindinčias perturbacijas įvedant pradinėse sąlygose. Tačiau tyrimais nustatyta, kad dėl nedidelės spiralinės bangos pradinių sąlygų perturbacijos pasikeičia visas raštas.



2.8 pav. Reguliarios spiralinės bangos evoliucija. Nustatomi modelio parametrai: $L = 100$, $\varepsilon = 0{,}1$, $a = 0{,}7$, $b = 0{,}06$, $g = u^3 - v$; $dt = 0{,}05$. Pradinės sąlygos pavaizduotos (a) ir (b); u srities evoliucija – (c)

2.3.2.1. Uždelsta perturbacija diskrečiajame taške

Nagrinėkime eksperimentą, kuriame į antrąjį raštą laiko momentu $T = 57{,}5$ įvedama perturbacija, o abiejų raštų evoliucija užbaigiama pasiekus laiko momentą $T = 60$ (pradinės sąlygos tokios pat, kaip 2.8 pav.). Perturbuojame du antrojo rašto taškus, prie jų verčių pridėdami 5 proc., kai pasiekiamas laiko momentas $T = 57{,}5$ (2.9 pav.).



2.9 pav. Perturbacijos įvedamos, kai $T = 57{,}5$. a) neperturbuotas raštas, b) perturbuotas vaizdas (pliusu pažymėtos perturbacijos yra mažos ir nematomos plika akimi); c) skirtuminis vaizdas, kuriame matomos perturbacijos (vaizdas paryškintas); d), e) ir f) neperturbuotas, perturbuotas vaizdas ir skirtuminis vaizdas, kai $T = 60$; g) maksimalios u srities vertės kitimas skirtuminiame vaizde

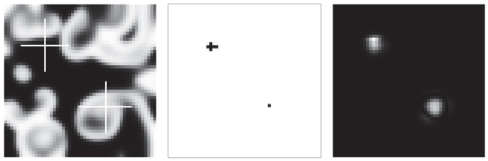
Maksimali u srities vertė skirtuminiame vaizde ilgainiui mažėja (2.9 pav. (g) dalis), tačiau pastebima, kad dviejų perturbuotų taškų kontrasto mažėjimas yra visiškai skirtingas. Šį efektą galima paaiškinti sąveika tarp perturbacijos ir sklindančio lūžtančios spiralinės bangos fronto. Viršutinis

kairysis perturbacijos taškas įvedamas į sritį, kurioje likusiu modeliavimo metu neatsiranda naujų bangų; todėl didžiausias intensyvumas taško aplinkoje monotoniškai mažėja. Apatinis dešinysis perturbacijos taškas yra srityje, per kurią iki modeliavimo pabaigos pereina keletas bangos frontų; to rezultatas – intensyvumo svyravimai.

2.3.2.2. Adaptyvios perturbacijos strategija

Problemos, susijusios su skirtingais perturbacijų intensyvumo mažėjimo greičiais skirtingose besivystančio rašto vietose, gali būti sprendžiamos varijuojant perturbacijos laiko momentą ar perturbacijų dydį, t. y. taikant adaptyvią perturbacijos strategiją.

2.10 pav. besivystantis raštas buvo perturbuotas ne viename taške, bet šešiuose gretimuose taškuose p_2 aplinkoje (2.10 pav. (b) dalis). Siekiant dar labiau suvienodinti intensyvumą ir formas, perturbacijos gali būti įvedamos skirtingais laiko momentais. Reiktų paminėti, kad visuose šešiuose taškuose išlaikomas vienodas perturbacijų intensyvumas; perturbuojamų taškų specifinė geometrinė vieta ir laikas parenkamas eksperimentiniu būdu (2.10 pav. (c) dalis).



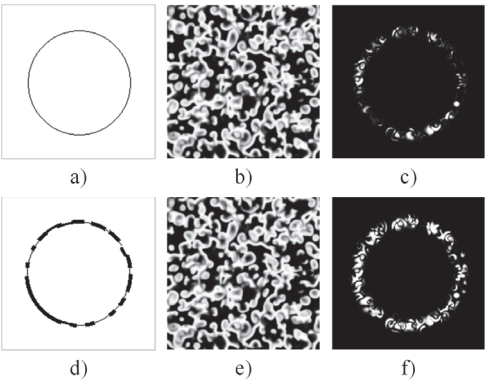
2.10 pav. Taikoma adaptyvios perturbacijos strategija leidžia išlyginti skirtuminio vaizdo taškų intensyvumą ir formas. Perturbuojamų taškų vietos yra tokios pat, kaip 2.9 pav. Perturbacija apatiniame dešiniajame taške (p_1) atliekama, kai $T = 57{,}8$; perturbacija viršutiniame kairiajame taške (p_2) atliekama, kai $T = 56$. Perturbuojami šeši p_2 aplinkoje esantys taškai

Adaptyvi strategija ypač aktuali didesnių geometrinių pirminių elementų skirtuminio vaizdo intensyvumui ir formoms suvienodinti (2.11 pav.). 2.11 pav. (c) dalyje pavaizduoti aptikti trūkiai ir mažesnio intensyvumo zonos; perturbacija adaptyviai koreguojama (2.11 pav. (d) dalis). Gautas skirtuminis vaizdas dabar aiškiai atvaizduoja reguliarią geometrinę formą (2.11 pav. (f) dalis). Gautą vaizdą 2.11 pav. (c) ir (f) galima toliau tobulinti taikant vaizdo ryškinimo technologiją. Šiame eksperimente trūkiai yra aptinkami pasitelkiant žmogiškąjį faktorių, tačiau, naudojant specialius algoritmus, procesą galima automatizuoti.

Pristatytoje adaptyvioje perturbacijos strategijoje (2.11 pav.) perturbacijos taikomos vienodu laiko momentu, varijuojant tik perturbacijos vietą skaitmeniniame vaizde. Pritaikius perturbacijos laiko parinkimą, skirtuminio vaizdo kokybė galėtų labai pagerėti.

Pristatytoje adaptyvioje perturbacijos strategijoje (2.11 pav.) perturbacijos

taikomos vienodu laiko momentu, varijuojant tik perturbacijos vietą skaitmeniniame vaizde. Pritaikius perturbacijos laiko parinkimą, skirtuminio vaizdo kokybė galėtų labai pagerėti.



2.11 pav. Adaptyvios perturbacijos strategija žiedo formai formuoti skirtuminiame vaizde. Raštui taikomos siauros žiedo formos perturbacijos ((a) dalis), kai $T = 145$. Gautas raštas, kai $T = 150$, pavaizduotas (b) dalyje; skirtuminis vaizdas (kai $T = 150$) – (c) dalyje. Adaptyvios perturbacijos strategija taikoma perturbacijai modifikuoti ((d) dalis). Gautas raštas (kai $T = 150$) pavaizduotas (e) dalyje; skirtuminis vaizdas – (f) dalyje

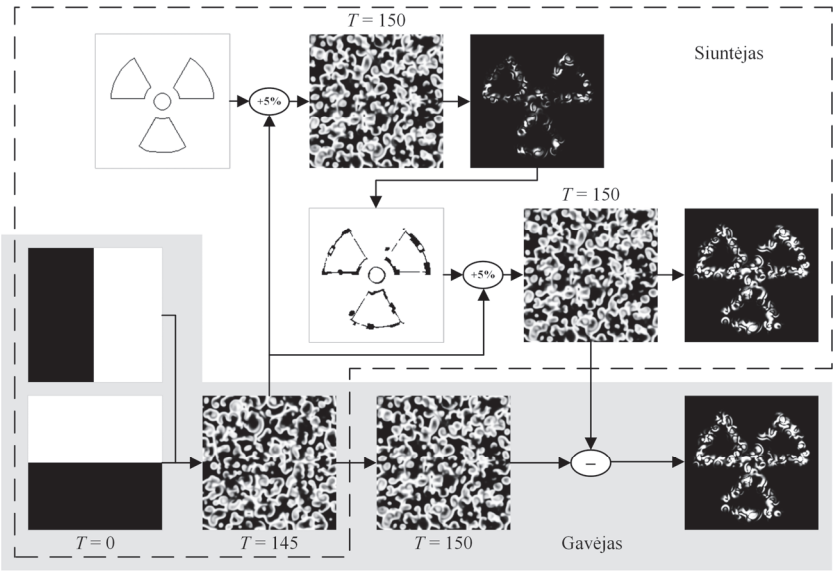
2.3.3. Komunikacijos algoritmas

Siūlomas komunikacijos algoritmas, paremtas spiralinėmis lūžtančiomis bangomis, yra pavaizduotas 2.12 pav. pateiktoje diagramoje. Panagrinėkime dvi komunikacijos šalis – siuntėją ir gavėją. Siuntėjas perduoda slaptą skaitmeninį vaizdą gavėjui. Veiksmai, kuriuos turi atlikti siuntėjas, apibrėžti punktyrine linija; veiksmai, kuriuos turi atlikti gavėjas, pažymėti pilkos spalvos srityje.

Iš pradžių (kai $T = 0$) siuntėjas parenka u ir v sričių pradines sąlygas (pradiniai reakcijos-difuzijos lygčių (4) parametrai), kaip pavaizduota 2.12 pav. (atkreipkite dėmesį, kad atsitiktinių pradinių sąlygų generavimas nėra būtinas). Pasiekus $T = 145$, siuntėjas stabdo spiralinių bangų evoliuciją ir perturbuoja slaptą vaizdą atitinkamuose taškuose. Siuntėjas tęsia perturbuojamo rašto vystymą, kol pasiekiama $T = 150$ (100 žingsnių nuo perturbacijos momento). Tuo pat metu siuntėjas iki galutinio laiko momento $T = 150$ iš pradinių sąlygų plėtoja raštą be jokių perturbacijų. Taip siuntėjas gali patikrinti, kaip atrodo skirtuminis perturbuoto ir neperturbuoto raštų vaizdas.

Dabar siuntėjas taiko adaptyvios perturbacijos strategiją ir kartoja modeliavimą, siekdamas užtikrinti, kad skirtuminis vaizdas būtų pakankamai aiškus ir reprezentatyvus. Tada siuntėjas perduoda perturbuotą raštą gavėjui. 100 žingsnių visiškai paslepia perturbaciją spiralinių bangų rašte, kad jokie algoritmai (statistiniai ar deterministiniai) neaptiktų perturbacijų šiame rašte. Be

to (net jei visi sistemos parametrai būtų žinomi pašaliniam asmeniui), atvirkštinė modelio evoliucija yra neįmanoma dėl evoliuciją aprašančių lygčių netiesiškumo.



2.12. pav. Skaitmeninio vaizdo komunikacijos algoritmas, paremtas lūžtančiomis spiralinėmis bangomis

Dekodavimo procesas vykdomas tiesiogiai. Gavėjas naudoja identiškas pradines sąlygas ir vysto raštą, kol pasiekiamas laiko momentas $T = 150$. Tada išryškinamas skirtuminis vaizdas tarp išvystyto ir atsiųsto raštų – gautas vaizdas atskleidžia paslėptą informaciją.

2.4. Poskyrio išvados

Konkurencingai ir nedifuziškai susieti iteraciniai modeliai ir bangos sklidimas anizotropinėje prieširdžių virpėjimų terpėje gali būti taikomi slaptai informacijai slėpti ir padeda išvengti anksčiau paskelbtų komunikacijos algoritmų trūkumų, tokių kaip ilgas pereinamasis procesas, santykinai dideli pirminiai elementai ar santykinai paprastas raštas. Slaptas vaizdas taškinio skeletinio atvaizdo forma gali būti įterpiamas į vienalytį pradinį vaizdą gerokai žemiau triukšmo lygio. Parametrai gali būti naudojami kaip privatūs ar vieši raktai, todėl kuriama saugi ir efektyvi SOP paremta komunikacijos sistema.

Siūlomas lūžtančiomis spiralinėmis bangomis paremtas skaitmeninio vaizdo komunikacijos algoritmas raštams formuoti nenaudoja atsitiktinių pradinių sąlygų ir netaiko pradinių perturbacijų slaptam vaizdui slėpti ir perduoti. Toks metodas gali būti laikomas svarbiu žingsniu komunikacijos algoritmo

saugumo link. Tačiau, norint tinkamai įterpti slaptą vaizdą į vystomą raštą, siūlomam algoritmui reikalinga speciali adaptyvi perturbacijos technika.

SOP komunikacijos algoritmas gali būti naudojamas ir be LSB (mažiausio reikšmingumo bito) steganografijos. Tačiau perduodamas SOP vaizdas atkreips pašalinių asmenų dėmesį. SOP komunikacijos algoritmas užtikrina slapto vaizdo saugumą net tuo atveju, kai LSB steganografija yra pažeidžiama.

3. DINAMINĖS VIZUALINĖS KRIPTOGRAFIJOS ALGORITMAS, PAGRĮSTAS BAIGTINIAIS ELEMENTAIS[4]

Skaitmeninių vaizdų komunikacijos algoritmai, aprašyti 2 skyriuje, yra paremti SOP generavimu, o dekodavimo proceso metu reikalingas palyginamasis raštas (iš viso 2 skaidrės), norint išryškinti skirtumą ir atskleisti paslėptą informaciją. Šiuos trūkumus galima pašalinti pritaikant dinaminę vizualinę kriptografiją (DVC). DVC komunikacijos algoritmas, panašiai kaip ir SOP, raštams formuoti taiko fizikinius procesus, tačiau pasitelkiami procesai skiriasi. DVC atveju laike vidurkintos muaro juostos formuojasi taikant fizines deformacijas.

Informacijos slėpimo deformuojamose muaro gardelėse idėja nėra nauja (Palivonaitė ir kt., 2014). Tačiau deformuojamos muaro gardelės fizikiniuose procesuose dar nebuvo nagrinėtos. Pagrindinis šio skyriaus uždavinys – užkoduoti konfidencialią informaciją stochastinėje deformuojamoje muaro gardelėje taip, kad komunikacijai užtektų tik vienos skaidrės, o sistemos virpesius apibrėžiantys procesai būtų naudojami kaip dekodavimo raktas.

3.1. Laike vidurkintas muaras

Panagrinėkime vienmatę harmoninę muaro gardelę (Kobayashi, 1993):

$$F(x) = \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right), \tag{9}$$

čia x yra išilginė koordinatė; λ – gardelės žingsnis; 0 skaitinė vertė atitinka juodą spalvą; 1 – baltą spalvą, o visos tarpinės vertės – atitinkamą pilkos spalvos lygį. Tarkime, kad muaro gardelė formuojama vienmačio deformuojamo kūno

[4] *Šiame skyriuje pristatomi rezultatai buvo publikuoti straipsniuose*:

paviršiuje. Laikykime, kad deformacija nuo pusiausvyros padėties x taške, esant t laiko momentui, yra lygi $u(x,t)$. Tada deformuojama muaro gardelė gali būti išreikšta tokia forma:

$$F(x,t) = \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}\mu(x,t)\right), \tag{10}$$

jei tik nepriklausomas kintamasis x gali būti išreikštas iš:

$$x + u(x,t) = z \tag{11}$$

ir įgautų formą:

$$x = \mu(z,t). \tag{12}$$

Laikykime, kad $u(x,t)$ funkcija apibrėžia harmoninius virpesius pusiausvyros padėtyje (Ragulskis ir kt., 2009a):

$$u(x,t) = a(x)\sin(\omega t + \varphi), \tag{13}$$

čia $a(x)$ aprašo plokštumoje vykstančius virpesius; ω ir φ kampinis dažnis ir harmoninių svyravimų fazė.

Išskleiskime $a(x)$ funkciją x_0 taško aplinkoje:

$$a(x) = a_0 + \dot{a}_0(x - x_0) + O(x - x_0)^2, \tag{14}$$

čia $a_0 = a(x_0)$; $\dot{a}_0 = \left.\frac{da(x)}{dx}\right|_{x=x_0}$. Darome prielaidą, kad $\omega = 1$ ir $\phi = 0$. Tada iš (12) lygties gaunama:

$$x \approx \frac{z - (a_0 - \dot{a}_0 x_0)\sin t}{1 + \dot{a}_0 \sin t}. \tag{15}$$

Tuomet deformuotos muaro gardelės pilkos spalvos lygis x koordinatėje t laiko momentu gali būti išreiškiamas tokia forma:

$$F(x,t) = \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}\cdot\frac{x - (a_0 - \dot{a}_0 x_0)\sin t}{1 + \dot{a}_0 \sin t}\right). \tag{16}$$

3.2. Deformuojama muaro gardelė; netiesinės deformacijos laukas

Netiesine funkcija apibrėžtam deformacijos laukui $a(x)$ gali būti pritaikytas (16) lygtimi aprašytas atvejis. Koks turėtų būti vienmatės muaro gardelės žingsnis $\lambda(x)$, kad visas laike vidurkintas vaizdas būtų transformuojamas į laike vidurkintą juostą, nepriklausomai nuo funkcijos $a(x)$?

(16) lygties kosinuso argumentas gali būti perrašytas taip:

$$\frac{x - (a_0 - \dot{a}_0 x_0)\sin t}{1 + \dot{a}_0 \sin t} = (x - (a_0 - \dot{a}_0 x_0)\sin t)\big((1 - \dot{a}_0 \sin t) + O(\dot{a}_0^2)\big). \tag{17}$$

Pažymėkime $\overline{a}(x) = a_0 + \dot{a}_0(x - x_0)$. Tuomet (16) lygtis:

$$F(x,t) \approx \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}(x + (a_0 - \dot{a}_0 x_0)\dot{a}_0 \sin^2 t)\right)\cos\left(\frac{2\pi}{\lambda}\overline{a}(x)\sin t\right) + \frac{1}{2}\sin\left(\frac{2\pi}{\lambda}(x + (a_0 - \dot{a}_0 x_0)\dot{a}_0 \sin^2 t)\right)\sin\left(\frac{2\pi}{\lambda}\overline{a}(x)\sin t\right). \quad (18)$$

Kadangi sinuso funkcija yra nelyginė, tuomet $\lim_{T\to\infty}\frac{1}{T}\int_0^T \sin\left(\frac{2\pi}{\lambda}\overline{a}(x)\sin t\right)dt = 0$. Be to, $\lim_{T\to\infty}\frac{1}{T}\int_0^T \sin^2 t\, dt = 0{,}5$. Todėl laike vidurkintas vaizdas gali būti aproksimuojamas kaip:

$$\bar{F}(x) = \lim_{T\to\infty}\frac{1}{T}\int_0^T F(x,t)dt \approx \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}\left(x + \frac{1}{2}(a_0 - \dot{a}_0 x_0)\dot{a}_0\right)\right) J_0\left(\frac{2\pi}{\lambda}\overline{a}(x)\right), \quad (19)$$

čia J_0 yra pirmo tipo nulinės eilės Beselio funkcija. Laike vidurkintos muaro juostos formuojasi, kai $J_0\left(\frac{2\pi}{\lambda}\overline{a}(x)\right) = 0$. Tai vyksta amplitudei tenkinant sąlygą $\frac{2\pi}{\lambda}A_k = r_k$, čia r_k yra J_0 šaknys; $k = 1,2,\ldots$. Norint, kad DVC algoritmas būtų įgyvendintas sėkmingai, būtina, kad iš anksto pasirinkta pradinio vaizdo sritis būtų transformuota į tolygią laike vidurkintą muaro juostą. Vienintelis kontroliuojamas vaizdo parametras yra žingsnis $\lambda(x)$. Atsižvelgiant į (19) lygtį, gardelės žingsnių pasiskirstymas turėtų būti išreikštas taip:

$$\lambda(x) = \frac{2\pi}{r_k}\overline{a}(x), \quad k = 1,2,\ldots. \quad (20)$$

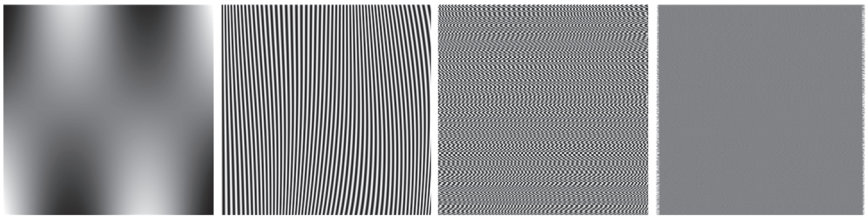
Hipotezė, kad $\overline{a}(x)$ (20) lygtyje galima pakeisti $a(x)$, buvo patvirtintas skaitiniais metodais.

3.3. Dinaminės vizualinės kriptografijos algoritmas, paremtas deformuojamomis muaro gardelėmis

Laike vidurkintoms muaro juostoms formuoti bus pasitelkiami netiesiniai deformacijos laukai, aprašomi baigtiniais elementais. Kadangi iki šiol buvo naudojamos vienmatės muaro gardelės, dvimatis deformacijų laukas $a(x,y)$ bus dalijamas horizontaliai, o gaunamų vienmačių gardelių žingsnių pasiskirstymas bus skaičiuojamas atskirai. Todėl kiekviena 2D deformacijų skaitmeninio vaizdo taškų eilė interpretuojama kaip atskira vienmatė amplitudžių $a(x)$ variacija. Šis procesas pavaizduotas 3.1 pav.

3.1 pav. (a) dalyje pavaizduota plokštės 12 tikrinė baigtinių elementų forma – baltos zonos žymi maksimalias deformacijas nuo pusiausvyros padėties, tamsios zonos žymi minimalias. Pirmiausia būtina nustatyti maksimalią

svyravimų amplitudę – tikrinė forma yra dauginama iš iš anksto nustatytos konstantos. Kitas žingsnis – vienmačių muaro gardelių formavimas. 3.1 pav. (a) dalies raišką yra 500 × 500 taškų. Taigi, 3.1 pav. (b) dalyje generuojama 500 horizontalių vienmačių muaro gardelių, o žingsnio variacija gardelės srityje yra konstruojama pagal (20) lygtį. Vienintelė išimtis – deformacijos laukas $\overline{a}(x)$ yra keičiamas $ka(x) + b$, čia $a(x)$ yra esamos gardelės tikrinių formų skaitinės vertės, o k, b yra teigiamos konstantos, didesnės už 0. Konstanta b reikalinga norint išvengti singuliarumo taškuose, kuriuose amplitudės $a(x)$ tampa lygios 0; k reikalingas amplitudžių skaitinių verčių diapazonui kontroliuoti. Visuose tolesniuose skaičiavimuose nustatoma $k = 0{,}0025$ ir $b = 0{,}0075$, todėl pradinis tikrinės formos reikšmių diapazonas $[-1; 1]$ pakeičiamas į amplitudžių veikimo diapazoną $[0{,}005; 0{,}01]$.



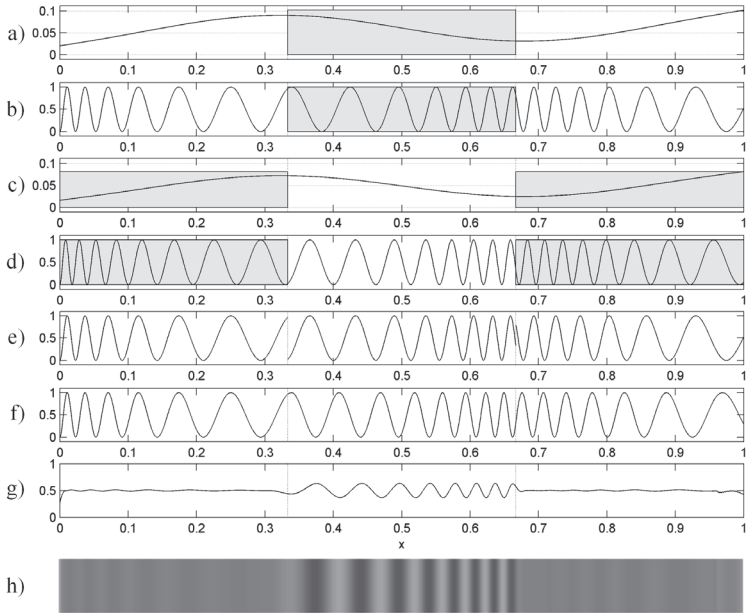
a) b) c) d)

3.1 pav. Laisvos stačiakampės plokštės harmoniniai svyravimai pagal 12 tikrinę formą sukuria pilką dvimatį vaizdą; (a) dalyje pavaizduota tikrinė forma; (b) dalyje pavaizduota stacionari muaro gardelė (gardelės žingsnis varijuoja intervale $\lambda = [0{,}013; 0{,}026]$; $\lambda(x) = \frac{2\pi}{r_1} a(x)$; (c) dalis iliustruoja gardelės vaizdą gautą naudojant atsitiktinę pradinę fazę; (d) dalyje pavaizduotas laike vidurkintas vaizdas, virpinant pagal 12 tikrinę formą

Atkreipkite dėmesį, kad pradinė visų 500 vienmačių gardelių fazė yra nustatyta 0, taigi, 3.1 pav. (b) dalyje pateiktas vaizdas gali atskleisti pačią tikrinę formą. Todėl vaizdo sudėtingumui padidinti yra naudojamos stochastinės pradinės fazės Ragulskis ir kt., 2009a) (3.1 pav. (c) dalis).

Dabar plokštumoje vykstantys vienkrypčiai svyravimai pagal x ašį generuoja laike vidurkintas muaro juostas kiekvienos vienmatės gardelės srityje – 3.1 pav. (d) dalyje pavaizduotas gautasis vaizdas yra visiškai pilkas. Išimtis yra dešinioji ir kairioji kraštinės, kuriose vaizdas tampa šiek tiek nevienodas dėl vidurkinimo su numatytąja balta fono spalva.

Slaptas vaizdas įterpiamas į pradinį vaizdą taikant fazių reguliarizacijos algoritmą, aprašytą (Ragulskis ir kt., 2009a). Algoritmo veikimas pademonstruotas 3.2 pav. Laike vidurkinant (f) dalį, gaunama (g) dalis, kadangi ji virpinama pagal (12) lygtyje apibrėžtą dėsnį, o amplitudžių $a(x)$ laukas nustatomas pagal (a) dalį. Laike vidurkintos muaro juostos susiformuoja vaizdo kairiajame ir dešiniajame trečdaliuose; vidurinis laike vidurkinto vaizdo trečdalis aiškiai išsiskiria pilkos spalvos fone ((h) dalis).



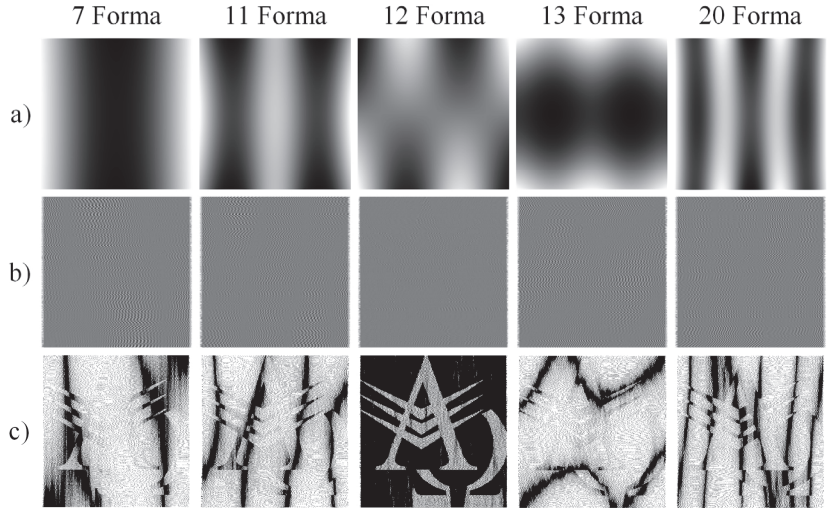
3.2 pav. Slaptos informacijos užkodavimo vienmatėje muaro gardelėje iliustracija: (a) amplitudžių $a(x)$ laukas (pagal iš anksto nustatytą tikrinę formą); (b) iliustruoja atitinkamą muaro gardelę. (c) amplitudžių, naudojamų srityse, kuriose yra slapta informacija, laukas; (d) atitinkama muaro gardelė. Sudėtinėje muaro gardelėje naudojamas kairysis ir dešinysis trečdaliai iš (b) dalies ir vidurinis trečdalis iš (d) dalies. Visi pertrūkiai (e) dalyje yra pašalinami taikant fazės reguliarizacijos algoritmą ((f) dalis). (f) dalies laike vidurkintas vaizdas pateiktas (g) ir (h) dalyse

3.3 pav. (a) dalyje pateiktas slaptas vaizdas; (b) dalyje pavaizduotas statinis vaizdas su įterpta slapta informacija (gardelės tankis yra nuo 0,013 iki 0,026)

Toliau pateiktas eksperimentas buvo pasitelktas siekiant pademonstruoti tokio vaizdo slėpimo algoritmo, paremto dinamine vizualine kriptografija, veikimą. Slaptas dichotominis vaizdas (pavaizduotas 3.3 pav. (a) dalyje) įterpiamas į pradinį vaizdą (3.3 pav. (b) dalis) pagal stačiakampės plokštės 12 tikrinę formą – slaptai informacijai slėpti naudojama stochastinė pradinė fazė ir

fazių reguliarizacijos algoritmai. Plika akimi neįmanoma įžiūrėti pradiniame vaizde užkoduoto slapto vaizdo; be to, slapta informacija gali būti išryškinta tik tuo atveju, jei deformuojamam pradiniam vaizdui deformuoti būtų naudojama tik ta pati tikrinė forma, kuri buvo taikoma ją užšifruojant.

Kitaip tariant, pati tikrinė forma gali būti laikoma vizualinės dekodavimo procedūros raktu. 3.4 pav. pateikti vizualinio dekodavimo rezultatai, kai vaizdas yra virpinamas pagal skirtingas tikrines formas; muaro juostos laike vidurkintuose vaizduose išryškintos pasitelkiant kontrasto didinimo procedūras.



3.4 pav. Tikrinė forma naudojama kaip slapto vaizdo iššifravimo raktas. Pirmoje eilėje pateiktos skirtingos tikrinės formos; antroje eilėje – laike vidurkinti vaizdai; trečioje eilėje – padidinto kontrasto laike vidurkinti vaizdai

3.4. Poskyrio išvados

Vaizdo šifravimo deformuojamose vienmatėse muaro gardelėse, virpinamose pagal iš anksto nustatytą tikrinę formą, algoritmas įgyvendintas dvimačiams skaitmeniniams dichotominiams slaptiems vaizdams konstruoti. Slapta informacija vaizde išryškinama laike vidurkintų muaro juostų rašto pavidalu, virpinant vaizdą pagal iš anksto nustatytą tikrinę baigtinių elementų formą.

Darbe pristatomi du dinaminės vizualinės kriptografijos algoritmai, kuriuose taikoma ši technika. Pirmasis yra paremtas deformuojamos harmoninės muaro gardelės deformuojamos harmoniniais virpesiais, o antrasis – Ronchi gardelių deformavimu pagal trikampės formos funkciją. Ronchi tipo gardelės yra pranašesnės taikant praktiškai, kadangi stochastinį vaizdą paprasčiau suformuoti gembės ar diafragmos paviršiuje.

4. DVIMAČIŲ SEKŲ PSEUDORANGAS IR SKAITMENINIŲ VAIZDŲ SUDĖTINGUMAS[5]

Vienmačių tiesinių (1D) rekurentinių sekų (LRS) išplėtimas iki dviejų dimensijų atveria naujų skaitmeninio vaizdo analizės galimybių. Šiame skyriuje parodyta, kad 2D sekų rangas gali būti taikomas savaime besiformuojančių raštų sudėtingumui vertinti kiekvienos erdvinės koordinatės atžvilgiu. Šį pranašumą galima išnaudoti analizuojant rašto būseną formavimo metu ir siekiant nustatyti, ar raštas yra pakankamai išvystytas.

4.1. 1D sekos pseudorangas

1-LRS pseudorangui nustatyti naudojama skaičiavimo sistema, pagrįsta Hankelio matricų SVD išskaidymu, pristatyta (Landauskas ir kt., 2016).

Kadangi Hankelio determinantų skaičiavimas skaitiniais metodais yra nestabilus, 2-LRS apibrėžimo negalima taikyti siekiant tiesiogiai nustatyti, ar duotosios 2D sekos turi baigtinį rangą. Siekiant užtikrinti stabilesnį 2D sekų rango vertinimą, pasitelkiama pseudorango koncepcija.

1D sekos $(p_j; j \in Z_0)$ atveju, pseudorangas skaičiuojamas pasitelkiant SVD išskaidymą pagal šį algoritmą (Landauskas ir kt., 2016):

1. Hankelio matrica H_K formuojama iš $(p_j; j \in Z_0)$ sekos, naudojant pirmuosius K elementus.

2. Atliekamas H_K SVD išskaidymas:

$$H_K = USV^T, \tag{21}$$

čia U, V yra HH^T ir H^TH ortonormuotų tikrinių vektorių matricos, o S yra įstrižainė matrica, sudaryta iš suranguotų singuliarių verčių:

$$\sigma_1^2 \geq \sigma_2^2 \geq \cdots \geq \sigma_K^2 \geq 0. \tag{22}$$

3. Pasirinktam $\varepsilon > 0$ apibrėžiamas duotos sekos pseudorangas $\widetilde{K}$ kaip singuliarių verčių, didesnių už ε, skaičius:

$$\widetilde{K}: \sigma_{\widetilde{K}}^2 > \varepsilon, \sigma_{\widetilde{K}+1}^2 \leq \varepsilon. \tag{23}$$

Pagal (Landauskas ir kt., 2016) matoma, kad sekos pseudorangas artėja į tikrąjį rangą, kai $\varepsilon \to 0$, tačiau, $\varepsilon = 0$ nustatymas padidina jautrumą triukšmui

---

[5] *Šiame skyriuje pristatomi rezultatai buvo publikuoti straipsnyje*:

The order of a 2-sequence and the complexity of digital images,
Telksnys T., Navickas Z., Vaidelys M., Ragulskis M.

sekoje $\left(p_j; j \in Z_0\right)$. Taigi, realaus taikymo atveju rekomenduojama rinktis $\varepsilon > 0$ ir naudoti pseudorangą.

4.2. 2D sekos pseudorangas

1D sekos pseudorango koncepcija negali būti tiesiogiai taikoma 2D sekoms, kadangi jos yra sudarytos iš dviejų rinkinių, kuriuose galimas begalinis 1D sekų skaičius. Šiai problemai išspręsti siūlome naudoti vidutinį duotų 2D sekų eilučių (stulpelių) rangą. Naudojant SVD išskaidymą, 2D sekų eilučių (stulpelių) pseudorangas X gali būti įvertintas pasitelkiant 4.1 skyriuje pateiktą algoritmą su tuo pačiu ε kiekvienoje eilutėje ir atsižvelgiant į gautų pseudorangų vidutinę vertę. Taigi, homogeninių 2D sekų X eilutės (stulpelio) pseudorangas $\widetilde{N}$, apskaičiuotas iš pirmų m eilučių (stulpelių) rinkinio, apibrėžiamas kaip:

$$\widetilde{N} \coloneqq \frac{1}{m}\sum_{j=0}^{m-1} \widetilde{K}_j. \tag{24}$$

4.3. Savaime besiformuojančių raštų 2D sekų pseudorangas

Siekiant pademonstruoti LRS pseudorangų galimybes skaitmeniniuose vaizduose, naudojamas Beddingtono ir DeAngelis-tipo „grobuonies–aukos“ modelis su savidifuzija ir kryžmine difuzija (Saunoriene ir kt., 2011, Wang ir kt., 2011):

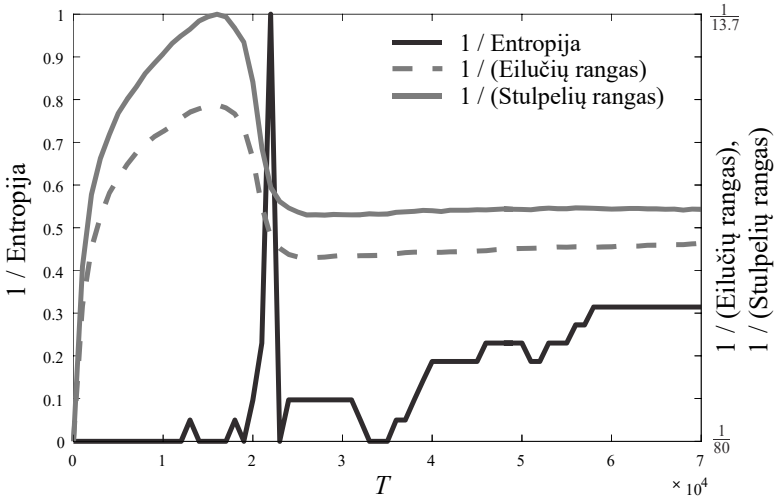
$$\frac{\partial N}{\partial t} = r\left(1 - \frac{N}{K}\right) - \frac{\beta N}{B + N + \omega P}P + D_{11}\nabla^2 N + D_{12}\nabla^2 P, \tag{25}$$

$$\frac{\partial P}{\partial t} = \frac{\epsilon\beta N}{B + N + \omega P}P - \eta P + D_{21}\nabla^2 N + D_{22}\nabla^2 P, \tag{26}$$

čia t yra laikas; N ir P yra aukų ir grobuonių tankiai; β maksimali suvartojimo norma; B yra sočio (angl. *saturation*) konstanta; w yra grobuonies interferencijos parametras; η reprezentuoja grobuonies mirtingumo dydį vienam individui; ϵ yra maisto konversijos į prieaugį koeficientas. Nenulinės pradinės sąlygos $N(x, y, 0) > 0$; $P(x, y, 0) > 0$ nustatomos stačiakampėje srityje su periodinėmis kraštinėmis sąlygomis. Nustačius pradinius parametrus D_{11} = 0,01, D_{12} = 0,0115, D_{21} = 0,01, D_{22} = 1, r = 0,5, ϵ = 1, β = 0,6, K = 2,6, w = 0,4, B = 0,3154, gaunama savaime besiformuojančio rašto evoliucija nuo pusiausvyros taško (N^*, P^*) = (0,430580; 0,718555) (Saunoriene ir kt., 2011). Grobuonių savaime besiformuojančių raštų kompiuterinė rekonstrukcija iš atsitiktinių pradinių sąlygų pavaizduota 4.1 pav.

Galime pakartoti skaičiavimo eksperimentus su vaizdų sekomis ir palyginti savaime besiformuojančių raštų evoliuciją su tų pačių raštų Shannono entropija (4.2 pav.), kai ε nustatytas 0,5. Shannono entropija $H(X) = -\sum_{k=1}^{m} p_k \log_2 p_k$ įvertina skaitmeninio vaizdo atsitiktinumą (Borda, 2011).

4.1 pav. Savaime besiformuojančių Beddingtono ir DeAngelis tipo raštų evoliucija. a)-e) dalyse yra pateikti vaizdai po 0, 15000, 25000, 50000 ir 70000 laiko žingsnių



4.2 pav. Entropijos evoliucija ir eilučių (stulpelių) savaime besiformuojančio rašto Beddingtono ir DeAngelis tipo LRS pseudorangas per 70000 laiko žingsnių. Kairioji y-ašis vaizduoja atvirkštinę entropiją $H(X)$. Dešinioji y-ašis vaizduoja vidutinio eilučių ir stulpelių LRS pseudorango inversiją

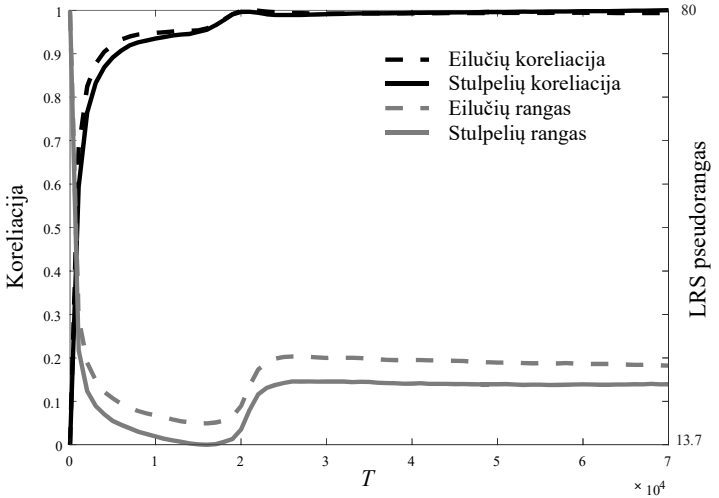
Kaip pavaizduota (4.2 pav.), evoliucijos entropija yra labai sudėtinga ir nemonotoniška, o savaime besiformuojančių raštų evoliucijos metu 2-LRS pseudorangų skaičiavimas išryškina paslėptas rašto sudėtingumo kitimo savybes.

Iš pradžių vaizdas yra atsitiktinis, taigi triukšmo vaizdo 2-LRS pseudorangas yra lygus (80; 80) (4.2 pav.). Tuomet pradeda vystytis savaime besiformuojantys raštai, ir vaizdų sudėtingumas sumažėja – 2-LRS pseudorangas yra lygus (16,6; 13,7), kai t = 15000 (laiko iteracijos laiko žingsnis yra 0,01). Tačiau vaizdo sudėtingumas staiga vėl pradeda didėti, kai $15000 \leq t \leq 25000$. Įdomu tai, kad visiškai išsivysčiusio rašto sudėtingumas yra didesnis, palyginti su rašto sudėtingumu vidurinėje vystymo stadijoje (2-LRS pseudorangas yra lygus (24,2; 21,2), kai t = 70000).

Tokį rezultatą paprasta paaiškinti, tačiau tai nereiškia, kad jis yra nereikšmingas. Iki galo išvystytas raštas nėra reguliarus raštas. Juostų

pasiskirstymas (taip pat juostų formos) visiškai išvystytame vaizde veikia pagal didelio mastelio erdvinio chaoso dėsnius.

Šiuo atžvilgiu pradinės atsitiktinės sąlygos gali būti laikomos mažo mastelio erdviniu chaosu. Tačiau įdomu pastebėti, kad evoliucija iš mažo mastelio į didelio mastelio erdvinį chaosą nėra tiesioginė. Visų pirma, atsitiktinės pradinės sąlygos vystosi į iš pažiūros įprastą raštą. Tačiau dėl Turingo nestabilumo (Murray, 2013) šios beveik įprastos bangos deformuojamos į sudėtingą ir netaisyklingą didelio mastelio raštą. 2-LRS pseudorangai leidžia efektyvią ir aiškią šių sudėtingų transformacijos procesų vizualizaciją.

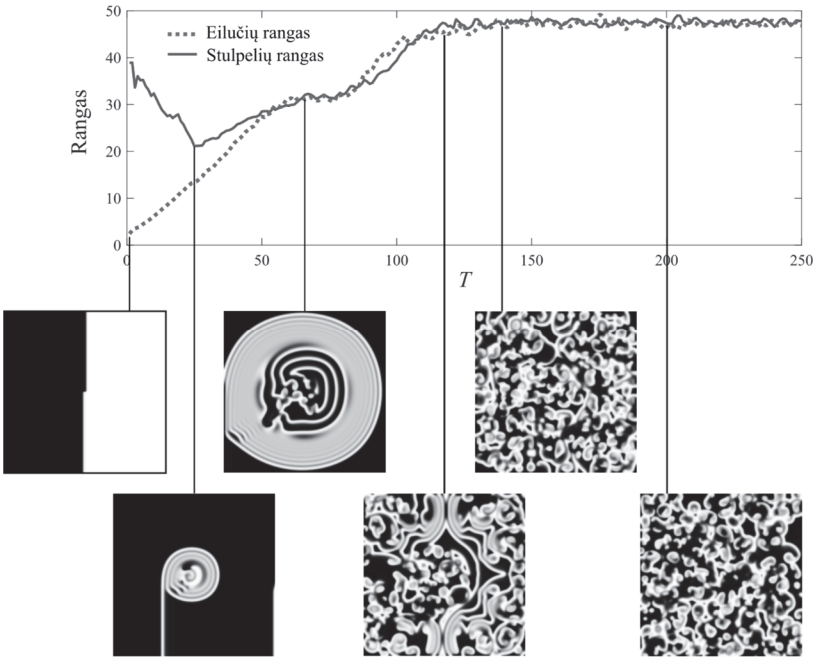


4.3 pav. Eilučių (stulpelių) koreliacijos evoliucija ir Beddingtono ir DeAngelis tipo savaime besiformuojančių raštų eilučių (stulpelių) LRS pseudorangas per 70000 laiko žingsnių. Kairioji y-ašis vaizduoja eilučių (stulpelių) koreliacijas $\rho_H(X)$. Dešinioji y-ašis vaizduoja vidutinį eilučių (stulpelių) LRS pseudorangą

Nemonotoniškumo efektai taip pat stebimi skaičiuojant eilučių ir stulpelių evoliucijos koreliacijas (4.3 pav.). Tiek eilučių, tiek stulpelių koreliacijos pasiekia beveik pikines vertes, lygias 1, kai $t = 20000$. Pasiekusios šią pikinę vertę, abi koreliacijos šiek tiek sumažėja, tačiau nesvyruoja – vertės išlieka daugiau kaip 0,98, esant $20000 < t \leq 70000$ intervalui. Atkreipkite dėmesį, kad vaizdo evoliucijos metu eilučių ir stulpelių koreliacijų vertės viena nuo kitos skiriasi, bet labai nedaug. Ši situacija yra visiškai priešinga eilučių ir stulpelių pseudorangui, kurio atveju jos skiriasi viena nuo kitos. Ši savybė leidžia daryti išvadas apie skaitmeninio vaizdo sudėtingumą horizontaliomis ir vertikaliomis kryptimis. 4.2 ir 4.3 pav. pavaizduota, kad vidutinis eilutės LRS rangas yra didesnis, palyginti su vidutiniu stulpelio LRS rangu. Tai reiškia, kad pseudoperiodas išilgai eilučių 4.1 pav. yra ilgesnis, palyginti su stulpeliais.

4.4. Optimali rašto formavimo trukmė[6]

Panaudokime 2-LRS pseudorangus savaime besiformuojančių raštų, pagrįstų spiralinių bangų modeliu, aprašytu 2.3 skyriuje, sudėtingumui įvertinti. Pradinės rašto formavimo sąlygos ir parametrai nustatomi tokie pat, kaip 2.8 pav., išskyrus srities dydį $L = 200$ ir eilučių (stulpelių) pseudorangui apibrėžti reikalingą $\varepsilon = 0{,}5$. Rašto evoliucija ir atitinkamas rangų grafikas pateiktas 4.4 pav.



4.4 pav. Besivystančio rašto sudėtingumas skirtingais laiko momentais. Maksimalus rašto sudėtingumas pasiekiamas ties $T = 140$

Rašto pradinis formavimasis tęsiasi, kol pasiekiamas $T = 25$, čia stulpelio rangas mažėja dėl vertikalių pradinių sąlygų. Kai pradinių sąlygų sukelta banga nusklinda tolyn, eilučių ir stulpelių rangas pradeda didėti. Tarp $T = 60$ ir 80 pastebimas trumpas stabilumo periodas, sukeltas bangų atspindžių nuo vaizdo

[6] *Šiame skyriuje pristatomi rezultatai buvo publikuoti straipsnyje*:

Image hiding in dynamic unstable self-organizing patterns
Vaidelys M., Lu C., Cheng Y., Vaideliene G.

kraštinių, po jo eina antras didėjimo intervalas, kurio metu visoje srityje prasideda bangų lūžiai. Pasiekus $T = 120$, rašto formavimas yra beveik baigtas, tačiau rangas toliau po truputį didėja iki $T = 140$. Vėlesnės bangų sąveikos rašto sudėtingumo nedidina, todėl $T = 140$ yra optimali trukmė raštui sukurti. Panašus rašto sudėtingumas kiekvienos erdvinės koordinatės atžvilgiu garantuoja, kad nebus horizontalaus ar vertikalaus kryptingumo.

2-LRS pagrįstas rašto sudėtingumo vertinimas padeda rasti optimalią rašto skaičiavimo trukmę. Optimali trukmė $T = 140$ yra artima taikomai 2.3.2 skyriuje, kur $T = 145$ buvo pasirinktas vizualiai vertinant keletą skirtingų rašto evoliucijų. Taigi 2D sekų rangai gali pašalinti žmogiškojo faktoriaus poreikį ir sutrumpinti rašto evoliucijos laiką.

4.5. Poskyrio išvados

Šiame skyriuje pateiktas praktinis 2D sekų rango pritaikymas. Pademonstruota, kad, naudojant SVD išskaidymą, 2-LRS koncepcija gali būti sėkmingai pritaikyta vaizdo sudėtingumo analizei atlikti. Dėl galimybės išmatuoti sudėtingumą x ir y ašyse eilučių (stulpelių) 2-LRS pseudorangai suteikia daugiau informacijos apie vaizdų sudėtingumą nei Shannono entropija ar koreliacija.

2-LRS taip pat galima pritaikyti savaime besiformuojančių raštų analizei. Parodyta, kad 2-LRS pseudorangas gali būti taikomas beveik reguliarių raštų formavimuisi aptikti. Šį pranašumą galima pritaikyti optimaliai rašto suformavimo trukmei nustatyti.

5. IŠVADOS

1. Pademonstruota, kad savaime besiformuojantys raštai gali būti taikomi slaptiems vaizdams slėpti ir leidžia sukurti saugius komunikacijos algoritmus. Išvystyti trys komunikacijos algoritmai, pagrįsti konkurencingai ir nedifuziškai susietais netiesiniais iteraciniais modeliais, prieširdžių virpesių modeliu ir lūžtančiomis spiralinėmis bangomis. Šie algoritmai išsprendė daugumą ankstesnių realizacijų trūkumų.

2. Lūžtančiomis spiralinėmis bangomis pagrįstam algoritmui nereikalingi privatūs ar vieši raktai, kurie apibrėžtų pradinių atsitiktinių sąlygų generavimą. Taip pat pastebėta, kad rašto formavimosi proceso viduryje vykdoma perturbacija yra jautri sklindančių lūžtančių bangų fronto poveikiui. Siekiant kontroliuoti rašto formavimąsi, reikalinga adaptyvios perturbacijos strategija, kuri prideda naują apsaugos lygį. Nepaisant reikalingos adaptyvios perturbacijos procedūros, slapto vaizdo iššifravimas išlieka toks pat paprastas, kaip anksčiau.

3. Sukurtas ir įgyvendintas vaizdo užšifravimo deformuojamoje vienmatėje harmoninėje muaro gardelėje, virpinamoje pagal tikrine baigtinių elementų forma nusakomą harmoninį dėsnį, algoritmas, skirtas dvimačiams dichotominiams slaptiems vaizdams slėpti. Slapta informacija iš vaizdo,

virpinamo pagal iš anksto nusakytą tikrinę formą, išryškinama laike vidurkintų muaro juostų rašto forma.

4. Pagrindinis algoritmo trūkumas yra susijęs su technologiniu harmoninių muaro gardelių formavimu ant deformuojamos struktūros paviršiaus. Dėl šios priežasties buvo pasitelkta Ronchi tipo muaro gardelė. Toks komunikacijos algoritmas imituoja fizikinius procesus ir gali būti pritaikomas, pvz., optiškai valdant MOEMS (mikrooptoelektromechanines) sistemas.

5. Pademonstruota, kad, pasitelkiant SVD išskaidymą, vaizdo ir savaime besiformuojančių raštų analizei atlikti įmanoma sėkmingai pritaikyti 2-LRS rangų koncepciją. Dėl galimybės įvertinti sudėtingumą x ir y ašimis, eilučių ir stulpelių 2-LRS pseudorangas suteikia daugiau informacijos apie vaizdų sudėtingumą nei Shannono entropija. Priešingai nei Shannono entropija ar vaizdo eilučių (stulpelių) koreliacija, 2-LRS pseudorangas gali būti pritaikytas beveik reguliarių raštų, kurie vystosi iš mažo mastelio erdvinio chaoso ir ilgainiui deformuojasi dėl Turingo nestabilumo, kai atsiranda didelio mastelio erdvinis chaosas, formavimuisi aptikti. Tai yra svarbus raštų formavimosi kriterijus, norint sukurti steganografiškai saugų raštą.

6. LITERATŪROS SĄRAŠAS

1. **Bär M., Eiswirth, M.** (1993). Turbulence due to spiral breakup in a continuous excitable medium. *Physical Review E*. 1993, 48, 1635-1637. ISSN 2470-0045.
2. **Barkley, D.** (2008). Barkley model. *Scholarpedia*. 2008, 3(11), 1877. ISSN 1941-6016.
3. **Barkley D., Kness, M., Tuckerman, L. S.** (1990). Spiral-wave dynamics in a simple model of excitable media: The transition from simple to compound rotation. *Physical Review A*. 1990, 42, 2489-2492. ISSN 2469-9926.
4. **Borda, M.** (2011). *Fundamentals in Information Theory and Coding*. Springer-Verlag Berlin Heidelberg, 2011, 485. ISBN 9783642203466.
5. **Cheddad, A. et al.** (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing*. 2010, 90(3), 727-752. ISSN 0165-1684.
6. **Christensen, K., Manani, K. A., Peters, N. S.** (2015). Simple model for identifying critical regions in atrial fibrillation. *Physical Review Letters*. 2015, 114, 028104. ISSN 0031-9007.
7. **Dowle, M., Mantel, R. M., Barkley, D.** (1997). Fast simulations of waves in three-dimensional excitable media. *International Journal of Bifurcation and Chaos*. 1997, 7, 2529-2546. ISSN 0218-1274.
8. **Ishimura, K., Komuro, K., Schmid, A., Asai T., Motomura, M.** (2014). Image steganography based on reaction diffusion models toward hardware implementation. *Nonlinear Theory and Its Applications, IEICE*. 2014, 5(4), 456-465. ISSN 2185-4106.
9. **Johnson, N., Duric, Z., Jajodia, S.** (2012). *Information Hiding: Steganography and Watermarking – Attacks and Countermeasures: Steganography and*

Watermarking. Springer Science and Business Media. 2012, 137. ISBN 978-0-7923-7204-2.

10. **Kaur, S. et al.** (2014). Steganography and classification of image steganography techniques. Inter*national Conference on Computing for Sustainable Global Development (Indiacom)*. 2014, 870-875.
11. **Killingback, T., Loftus, G., Sundaram, B.** (2013). Competitively coupled maps and spatial pattern formation. *Physical Review E*. 2013, 87(2), 022902. ISSN 2470-0045.
12. **Kobayashi, A.** (1993). *Handbook on Experimental Mechanics. 2nd Ed*. Bethel, SEM. 1993, 1074. ISBN 9781560816409.
13. **Landauskas, M., Navickas, Z., Vainoras, A., Ragulskis, M.** (2016). Weighted moving aver-aging revisited: an algebraic approach. *Computational and Applied Mathematics*. 2016, 1-14. ISSN 0101-8205.
14. **Luke, R. A., Saffitz, J. E.** (1991). Remodeling of ventricular conduction pathways in healed canine infarct border zones. *The Journal of Clinical Investigation*. 1991, 87, 1594-1602. ISSN 0021-9738.
15. **Maqsood, F. et al.** (2017). Cryptography: a comparative analysis for modern techniques. *International Journal of Advanced Computer Science and Applications*. 2017, 8(6), 442-448. ISSN 2158-107X.
16. **Mishra, R. et al.** (2015). A review on steganography and cryptography. *International Conference on Advances in Computer Engineering and Applications (ICACEA)*. 2015, 119-122. ISBN 978-1-4673-6911-4.
17. **Moizuddin, M. et al**. (2017). A comprehensive survey: quantum cryptography. *2nd International Conference on Anti-Cyber Crimes (ICACC)*. 2017, 98-102. ISBN 9781509058150.
18. **Murray, J. D.** (2013). *Mathematical Biology*. Springer Science and Business Media. 2013, 770. ISBN 9783662085424.
19. **Nakamura, K., Funabashi, N., Uehara, M., Ueda, M., Murayama, T., Takaoka, H., Komuro, I.** (2011). Left atrial wall thickness in paroxysmal atrial fibrillation by multislice-CT is initial marker of structural remodeling and predictor of transition from paroxysmal to chronic form. *International Journal of Cardiology*. 2011, 148, 139-147. ISSN 0167-5273.
20. **Nandakumar, A. et al.** (2011). A secure data hiding scheme based on combined steganography and visual cryptography methods. *Advances in Computing and Communications, Part 2*. 2011, 191, 498-505. ISSN 1865-0929.
21. **Naor, M., Shamir, A.** (1994). Visual cryptography. *Advances in Cryptology – EUROCRYPT'94*. 1994, 1-12. ISSN 0302-9743.
22. **Palivonaite, R., Aleksa, A., Paunksnis, A., Gelzinis, A., Ragulskis, M.** (2014). Image hiding in time-averaged deformable moiré gratings. *Journal of Optics*. 2014, 16(2), 025401. ISSN 2040-8986.
23. **Ragulskis, M., Aleksa, A.** (2009). Image hiding based on time-averaging moiré. *Optics Communications*. 2009, 282(14), 2752-2759. ISSN 0030-4018.

24. **Roy, R., Changder, S.** (2016). Quality evaluation of image steganography techniques: a heuristics based approach. *International Journal of Security and Its Applications*. 2016, 10(4), 179-196. ISSN 1738-9976.

25. **Saunoriene, L., Ragulskis, M.** (2011). Secure steganographic communication algorithm based on self-organizing patterns. *Physical Review E*. 2011, 84, 056213. ISSN 2470-0045.

26. **Sheshasaayee, A. et al.** (2017). A framework to enhance security for OTP SMS in e-banking environment using cryptography and text steganography. *Proceedings of the International Conference on Data Engineering and Communication Technology*. 2017, 469, 709-717. ISSN 2194-5357. 113.

27. **Simon, S.** (2011). *The code book: the science of secrecy from ancient egypt to quantum cryptography*. Knopf Doubleday Publishing Group. 2010. ISBN 978-0385495325.

28. **Wang, W., Lin, Y., Zhang, L., Rao, F., Tan, Y.** (2011). Complex patterns in a predator–prey model with self and cross-diffusion. *Communications in Nonlinear Science and Numerical Simulation*. 2011, 16, 2006-2015. ISSN 1007-5704.

29. **Weir, J. et al.** (2012). *Visual Cryptography and Its Applications*. Ventus Publishing ApS. 2012. ISBN 9788740301267.

30. **Xu, L. et al. (**2016). Dependence of initial value on pattern formation for a logistic coupled map lattice. *PLOS ONE*. 2016, 11(7), e0158591. ISSN 1932-6203.

31. **Yang, F., Xu Y.-Y., Shen, H.-B.** (2014). Many local pattern texture features: which is better for image-based multilabel human protein subcellular localization classification? *The Scientific World Journal*. 2014, 2014, 429049-14. ISSN 2356-6140.

32. **Yu, J. et al. (**2017). Image encryption algorithm by using the logistic map and discrete fractional angular transform. *Optica Applicata*. 2017, 47(1), 141-155. ISSN 0078-5466.

33. **Zhou, X. Y. et al.** (2016). An improved method for LSB based color image steganography combined with cryptography. *IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS)*. 2016, 1339-1342. ISBN 9781509008056.

34. **Ziaukas, P., Ragulskis, T., Ragulskis, M.** (2014). Communication scheme based on evolutionary spatial games. *Physica A: Statistical Mechanics and its Applications*. 2014, 403, 177-188. ISSN 0378-4371.

7. MOKSLINIŲ PUBLIKACIJŲ SĄRAŠAS

Straipsniai Mokslinės informacijos instituto (ISI) duomenų bazėse referuojamuose leidiniuose (pagrindinių ISI žurnalų sąrašas):

1. **Vaidelys, Martynas**; Lu, Chen; Cheng, Yujie; Ragulskis, Minvydas Kazys. Digital Image Communication Scheme Based on the Breakup of Spiral Waves // Physica A: Statistical mechanics and its applications. Amsterdam: Elsevier. ISSN 0378-4371. 2017, vol. 467, p. [1–10]. [Science Citation Index Expanded (Web of Science); Scopus; Current

Contents (Physical, Chemical & Earth Sciences)]. [IF: 2.243, AIF: 2.777 (2016)]

2. **Vaidelys, Martynas**; Ragulskienė, Jūratė; Aleksienė, Sandra; Ragulskis, Minvydas Kazys. Image Hiding in Time-Averaged Moiré Gratings on Finite Element Grids // Applied Mathematical Modelling. New York: Elsevier. ISSN 0307-904X. 2015, vol. 39, iss. 19, spec. iss. SI, p. 5783–5790. [Science Citation Index Expanded (Web of Science); Current Contents (Engineering, Computing & Technology); Science Direct]. [IF: 2.291, AIF: 1.671 (2015)]
3. **Vaidelys, Martynas**; Ragulskienė, Jūratė; Žiaukas, Pranas; Ragulskis, Minvydas. Image Hiding Scheme Based on the Atrial Fibrillation Model // Applied Sciences. Basel: MDPI AG. ISSN 2076-3417. 2015, vol. 5, iss. 4, p. 1980–1991. [Science Citation Index Expanded (Web of Science); Current Contents (Physical, Chemical & Earth Sciences); Current Contents (Engineering, Computing & Technology)]. [IF: 1.726, AIF: 4.276 (2015)]
4. **Vaidelys, Martynas**; Žiaukas, Pranas; Ragulskis, Minvydas Kazys. Competitively Coupled Maps for Hiding Secret Visual Information // Physica A: Statistical Mechanics and Its Applications. Amsterdam: Elsevier. ISSN 0378-4371. 2016, vol. 443, p. 91–97. [Science Citation Index Expanded (Web of Science); Scopus; Current Contents (Physical, Chemical & Earth Sciences)]. [IF: 2.243, AIF: 2.777 (2016)]
5. **Vaidelys, Martynas**; Aleksienė, Sandra; Ragulskienė, Jūratė. Dynamic Visual Cryptography Scheme on the Surface of a Vibrating Structure // Journal of Vibroengineering. Kaunas: JVE International. ISSN 1392-8716. 2015, vol. 17, iss. 8, p. 4142–4152. [Science Citation Index Expanded (Web of Science); Inspec; Academic Search Complete; Central & Eastern European Academic Source (CEEAS); Computers & Applied Sciences Complete; Current Abstracts; TOC Premier]. [IF: 0.384, AIF: 2.315 (2015)]
6. Telksnys, Tadas; Navickas, Zenonas; **Vaidelys, Martynas**; Ragulskis, Minvydas. The Order of a 2-Sequence and the Complexity of Digital Images // Advances in Complex Systems. Singapore: World Scientific Publishing. ISSN 0219-5259. 2016, vol. 19, iss. 4–5, article 1650010, p. [1–25]. [Science Citation Index Expanded (Web of Science); Scopus; Current Contents/Physical, Chemical & Earth Sciences]. [IF: 0.833, AIF: 3.263 (2016)]

Straipsniai Lietuvos mokslo tarybos patvirtinto sąrašo tarptautinėse duomenų bazėse referuojamuose leidiniuose:

1. **Vaidelys, Martynas**; Lu, Chen; Yujie, Cheng; Vaidelienė, Gintarė. Image Hiding in Dynamic Unstable Self-Organizing Patterns // Vibroengineering

Procedia: [28th International Conference on Vibroengineering, Beijing, China, 19–21 October, 2017]. Kaunas: JVE International. ISSN 2345-0533. 2017, vol. 14, p. 328–333. DOI: 10.21595/vp.2017.18296.

2. Aleksienė, Sandra; **Vaidelys, Martynas**; Aleksa, Algiment; Ragulskis, Minvydas Kazys. Dynamic Visual Cryptography on Deformable Finite Element Grids // AIP Conference proceedings: International conference of numerical analysis and applied mathematics (ICNAAM 2016). Melville, NY: AIP Publishing. ISSN 0094-243X. 2017, vol. 1863, iss. 1, article 440002, p. 1–4. DOI: 10.1063/1.4992606.

TRUMPA INFORMACIJA APIE DISERTACIJOS AUTORIŲ

Gimė: 1988 m. balandžio 25 d. Kaune.

Išsilavinimas:

2007–2011 m. – Kauno technologijos universiteto Fundamentaliųjų mokslų fakultetas, matematikos bakalauro laipsnis.

2011–2013 m. – Kauno technologijos universiteto Fundamentaliųjų mokslų fakultetas, matematikos magistro laipsnis.

2013–2017 m. – Kauno technologijos universiteto Fundamentaliųjų mokslų fakultetas, informatikos (09P) doktorantūros studijos.

Pedagoginis darbas:

2014 m. iki dabar – Kauno technologijos universiteto Matematikos ir gamtos mokslų fakulteto Matematinio modeliavimo katedra, asistentas.

Mokslinių interesų sritys:

Informacijos slėpimas, vaizdų analizė ir rašto evoliucija.

E. paštas: martynas.vaidelys@ktu.lt

SUMMARY

Relevance of the Work

The importance of hiding information when transferring data has been highlighted since the early days of communication. Even though initially information hiding was mainly used in military areas, the exponential growth and the widespread use of the internet in the public domain fueled the need to secure business, medical or personal data, money transactions, and other sensitive areas of information exchange. Depending on the information type, cryptography, steganography or watermarking techniques are used. They are usually interrelated with each other to ensure a higher level of security. In the areas where privacy, undetectability and confidentiality is required, steganography and visual cryptography take an important role. However, these techniques alone are prone to attacks as soon as the algorithm of encoding becomes public. Thus reliable, steganographically secure and fast-working information hiding techniques are required.

The complex self-organizing patterns emerging from the biological, chemical or physical processes have been successfully adapted for hiding and communicating secret visual information. The Beddington-DeAngelis type predator prey model with self- and cross-diffusion has been successfully employed in a secure steganographic communication algorithm. SOP induced by prisoner dilemma type interactions between competing individuals has also been exploited for hiding and transmitting secret visual information. These communication schemes require the generation of two patterns while the difference image reveals the secret. Computational speed issues and the system insensitivity to small local perturbations of these approaches influences the further development of the communication schemes based on SOP. DVC scheme based on the optical time-averaging moiré technique has also been developed for information hiding. This approach is denoted by advantages over SOP because the secret image embedded into a moiré grating can be interpreted by a naked eye when the image is oscillated or deformed; also, it does utilize only a single image during communication. A natural extension of DVC could be the employment of a physical process describing the deformation law in encryption and decryption of the secret information in a stochastic deformable moiré grating.

Various pattern formation mechanisms and parameters result in different characteristic images which require the evaluation of complexity and feasibility for information hiding applications. Standard approaches, such as Shannon entropy, row/column correlation, image pixel analysis, or detection of steganographic characteristics, have been successfully used in image analysis. However, physical processes could form complex patterns and conceal additional information – e.g., small scale spatial chaos could be mentioned in this

context; hence, novel approaches towards identification are required.

The object of the research is visual information hiding based on self-organizing patterns.

The aim of the work is to develop mathematical models and algorithms for visual information hiding and communication based on self-organizing patterns.

The Main Tasks of this Research Are:

1. to develop an effective and steganographically secure digital image hiding schemes based on self-organizing patterns which can be used to transmit secret visual information;
2. to build the mathematical foundation for the formation of cover images on the surface of structures performing harmonic oscillations;
3. to develop novel algorithms for the assessment of the complexity of self-organizing patterns.

Methods, Software, and Experimental Tools

• Information visualization and processing methods have been used for the creation and realization of dynamic visual cryptography conception based on non-linear oscillations.

• The mathematical apparatus and the theory of the optical moiré method was used for the researches. Its application is extended and further developed.

• The Euler method (the forward Euler method) was applied to simulate a chemical reaction and to numerically integrate differential equations.

• The theory of linear recurrent sequences was employed for the construction of algebraic approximation of any 2D image.

• Matlab R2016a was used for developing computational and experimental tools.

• COMSOL Multiphysics (the scientific package for physics-based finite element method modeling) was employed for the simulation of the deformation field.

Defended Statements

• Typical steganographic techniques are usually prone to steganalysis and do not guarantee the security of communication. Self-organizing patterns emerging from biological, chemical or physical processes can be successfully employed as an additional layer of security in concealing secret visual information.

• Dynamic visual cryptography schemes based on harmonic oscillations of the deformable harmonic moiré grating according to the predefined Eigen-shape enable to hide secret information by using only one share. Scheme adaptation for Ronchi grating makes the formation of the stochastic cover moiré image on the

surface of physical objects easier.

• It is important to consider the feasibility of an image used in secure communication. 2-LRS pseudo-order can provide a deeper insight on the pattern complexity.

Scientific Novelty and Significance

• The proposed techniques for information hiding based on SOP amend and overcome the drawbacks of the previously introduced similar schemes. The ability to avoid the necessity of using random initial conditions and the perturbation of initial conditions for the generation of a self-organizing pattern is a serious enhancement in terms of the security of the communication scheme.

• An image encoding scheme in deformable one-dimensional moiré gratings oscillating according to a predefined Eigen-mode describing a physical process is implemented for the construction of two-dimensional digital dichotomous secret images. The Eigen-shape of the structure serves as the decoding key for a visual communication scheme.

• 2-LRS can be used to analyze the complexity of self-organizing patterns. Unlike Shannon entropy, the order of 2-LRS can be applied to estimate the complexity of self-organizing patterns with respect to each spatial coordinate and to detect the transformation from a small scale spatial chaos to a large scale spatial chaos.

Approval of the Results

The major results of the thesis have been presented in 8 publications, 6 of which were delivered in journals listed by the Institute for Scientific Information (ISI) as the main list of publications with citing indexes; the two remaining articles were announced in peer-reviewed conference proceedings. The topics covered in the dissertation were presented at two international conferences.

The Structure

This doctoral dissertation consists of the introduction, 4 major sections, conclusions, a list of references and a list of the author's publications. In total, there are 53 figures and 2 tables in the thesis. The list of 143 cited sources within the main part of the dissertation is added to the main body of the dissertation.

UDK 004.056.55 (043.3)

SL344. 2018-05-31, 2.5 leidyb. apsk. l. Tiražas 50 egz.
Išleido Kauno technologijos universitetas, K. Donelaičio g. 73, 44249 Kaunas
Spausdino leidyklos „Technologija“ spaustuvė, Studentų g. 54, 51424 Kaunas