



Kauno technologijos universitetas

Matematikos ir gamtos mokslų fakultetas

Informacijos slėpimas dvimatėse stochastinėse muaro gardelėse

Baigiamasis magistro studijų projektas

Dorotė Kriukaitė

Projekto autorė

Doc. Dr. Loreta Saunorienė

Vadovė

Kaunas, 2024



Kauno technologijos universitetas

Matematikos ir gamtos mokslų fakultetas

Informacijos slėpimas dvimatėse stochastinėse muaro gardelėse

Baigiamasis magistro studijų projektas

Taikomoji matematika (6211AX006)

Dorotė Kriukaitė

Projekto autorė

Doc. Dr. Loreta Saunorienė

Vadovė

Doc. Dr. Paulius Palevičius

Recenzentas

Kaunas, 2024



Kauno technologijos universitetas

Matematikos ir gamtos mokslų fakultetas

Dorotė Kriukaitė

Informacijos slėpimas dvimatėse stochastinėse muaro gardelėse

Akademinio sąžiningumo deklaracija

Patvirtinu, kad:

1. baigiamąjį projektą parengiau savarankiškai ir sąžiningai, nepažeisdama(s) kitų asmenų autoriaus ar kitų teisių, laikydamasi(s) Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymo nuostatų, Kauno technologijos universiteto (toliau – Universitetas) intelektinės nuosavybės valdymo ir perdavimo nuostatų bei Universiteto akademinės etikos kodekse nustatytų etikos reikalavimų;
2. baigiamajame projekte visi pateikti duomenys ir tyrimų rezultatai yra teisingi ir gauti teisėtai, nei viena šio projekto dalis nėra plagijuota nuo jokių spausdintinių ar elektroninių šaltinių, visos baigiamojo projekto tekste pateiktos citatos ir nuorodos yra nurodytos literatūros sąrašė;
3. įstatymų nenumatytų piniginių sumų už baigiamąjį projektą ar jo dalis niekam nesu mokėjęs (-usi);
4. suprantu, kad išaiškėjus nesąžiningumo ar kitų asmenų teisių pažeidimo faktui, man bus taikomos akademinės nuobaudos pagal Universitete galiojančią tvarką ir būsiu pašalinta(s) iš Universiteto, o baigiamasis projektas gali būti pateiktas Akademinės etikos ir procedūrų kontrolieriaus tarnybai nagrinėjant galimą akademinės etikos pažeidimą.

Dorotė Kriukaitė

Patvirtinta elektroniniu būdu

Kriukaitė Dorotė. Informacijos slėpimas dvimatėse stochastinėse muaro gardelėse. Magistro studijų baigiamasis projektas / vadovė doc. dr. Loreta Saunorienė; Kauno technologijos universitetas, Matematikos ir gamtos mokslų fakultetas.

Studijų kryptis ir sritis (studijų krypčių grupė): Taikomoji matematika (Matematikos mokslai).

Reikšminiai žodžiai: dinaminė vizualinė kriptografija, informacijos slėpimas, geometrinis muaras, stochastinė gardelė, vidurkinimas laike.

Kaunas, 2024. 67 p.

Santrauka

Vizualinė kriptografija – tai informacijos slėpimo skaitmeniniuose vaizduose metodika, kai slaptas vaizdas yra išskaidomas į du ar daugiau skirtingų vaizdų taip, kad nei viename iš jų, atskirai paėmus, slaptos informacijos išvelgti neįmanoma. Sudėjus visas vaizdo dalis, slapta informacija atkoduojama tiesiog plika akimi. Dinaminėje vizualinėje kriptografijoje slaptas vaizdas yra užkoduojamas į įterpiančią muaro linijų tinklą taip, kad užkoduotame statiniame vaizde slaptos informacijos būtų neįmanoma įžiūrėti, tačiau atkoduoti informaciją taip pat galima plika akimi, kaip ir klasikinėje vizualinėje kriptografijoje. Tam užkoduotą vaizdą reikia virpinti iš anksto numatyto dėsnio su iš anksto fiksuotais parametrais.

Dauguma dinaminės vizualinės kriptografijos schemų yra pagrįstos slaptos informacijos įterpimu į periodines muaro gardeles, todėl nėra atsparios statistinės analizės algoritmams. 2023 m. buvo pristatyta tokia schema, leidžianti slėpti informaciją vienmatėse neperiodinėse stochastinėse muaro gardelėse. Ši schema pasižymi didesniu atsparumu statistinės analizės algoritmams lyginant su dinaminės vizualinės kriptografijos schemomis, pagrįstomis informacijos kodavimu periodinėse muaro gardelėse. Deja, slaptai informacijai užkoduoti bei atkoduoti šioje schemoje įmanoma panaudoti tik horizontalios ar vertikalios krypties harmoninius virpesius. Įvairių krypčių harmoninių ar netgi elipsinių virpesių panaudojimas tokio tipo schemoje ne tik padidintų įterpiamos informacijos saugumą, bet ir išplėstų dinaminės vizualinės kriptografijos taikymo galimybes.

Todėl šio tyrimo tikslas yra pasiūlyti dinaminės vizualinės kriptografijos schemą, pagrįstą neperiodinėmis stochastinėmis muaro gardelėmis ir skirtingų krypčių harmoniniais bei elipsiniais virpesiais. Siekiant integruoti bet kurios krypties harmoninius ar elipsinius virpesius, bus naudojamos dvimatės stochastinės neperiodinės muaro gardelės. Tyrime generuojami du stochastiniai vaizdai: slaptai informacijai ir fonui užkoduoti. Šie vaizdai pusiausvyros būsenoje yra labai panašūs, o juos suvidurkinus laike, akivaizdžiai skiriasi. Tokiems vaizdams sugeneruoti yra konstruojamos specialios tikslo funkcijos; joms optimizuoti naudojami evoliuciniai optimizavimo algoritmai. Informacijos slėpimo tokiuose stochastiniuose vaizduose efektyvumą iliustruoja skaitiniai eksperimentai ir grafiniai rezultatai.

Kriukaitė Dorotė. Information Hiding in Two-Dimensional Stochastic Moiré Gratings. Master's Final Degree Project / supervisor Assoc. Prof. Loreta Saunorienė. Faculty of Mathematics and Natural Sciences, Kaunas University of Technology.

Study field and area (study field group): Applied Mathematics (Mathematical Sciences).

Keywords: dynamic visual cryptography, information hiding, geometric moiré, stochastic grating, averaging in time.

Kaunas, 2024. 67.

Summary

Visual cryptography is a method of hiding information in digital images, when a secret image is split into two or more different images in such a way that it is impossible to see the secret information in any of them, taken separately. When all the parts of the image are put together, the secret information is decoded simply with the naked eye. In dynamic visual cryptography, a secret image is encoded by embedding it in a grid of moiré gratings in such a way that it is impossible to see the secret information in the encoded static image, but the information can be decoded with the naked eye, as in classical visual cryptography. This requires oscillating the coded image in a predetermined pattern with pre-fixed parameters.

Most dynamic visual cryptography schemes are based on embedding secret information into periodic moiré gratings and are therefore not immune to statistical analysis algorithms. In 2023, a this kind of scheme was introduced to hide information in one-dimensional non-periodic stochastic moiré gratings. This scheme has greater resistance to statistical analysis algorithms compared to dynamic visual cryptography schemes based on information coding in periodic moiré gratings. Unfortunately, it is only possible to use horizontal or vertical harmonic oscillations in this scheme to encode and decode secret information. The use of harmonic or even elliptical oscillations in different directions in this type of scheme would not only increase the security of the inserted information, but also expand the application possibilities of dynamic visual cryptography.

Therefore, the aim of this study is to propose a dynamic visual cryptography scheme based on non-periodic stochastic moiré gratings and harmonic and elliptical oscillations of different directions. Two-dimensional stochastic aperiodic moiré gratings will be used to integrate harmonic or elliptical oscillations of any direction. The study generates two stochastic images: for secret information and background embedding. At the equilibrium these images are very similar but distinctly different when averaged over time. Specific objective functions are constructed to generate such images; evolutionary optimization algorithms are used to optimize them. The effectiveness of information hiding in such stochastic images is illustrated by numerical experiments and graphical results.

Turinys

Lentelių sąrašas.....	7
Paveikslų sąrašas	8
Santrumpų ir terminų sąrašas.....	14
Įvadas.....	15
1. Literatūros apžvalga.....	16
1.1. Steganografija.....	17
1.1.1. Steganografija erdvinėje srityje	18
1.1.2. Steganografija dažnio srityje	18
1.2. Vizualinė kriptografija.....	18
1.2.1. Klasikinė vizualinė kriptografija	19
1.2.2. Modifikuota vizualinė kriptografija	20
1.2.3. Dinaminė vizualinė kriptografija.....	20
1.3. Išvados	25
2. Tyrimo metodai.....	26
2.1. Wada indeksas gardelės vertinime	26
2.2. Reikalavimai stochastinėms gardelėms	27
2.3. Laike vidurkinta gardelė	28
2.4. Tikslų funkcijos F1 sudarymas	32
2.5. Tikslų funkcijos F2 sudarymas	33
2.6. Stochastinės gardelės optimizavimas	34
3. Tyrimų rezultatai ir jų aptarimas	37
3.1. Pirmojo optimalaus vaizdo sudarymas	37
3.1.1. Harmoninis svyravimas kampu	37
3.1.2. Elipsinis svyravimas	43
3.2. Antrojo optimalaus vaizdo sudarymas	46
3.2.1. Atsitiktinių reikšmių gardelės sudarymas	46
3.2.2. Optimizuotos gardelės sudarymas	48
3.3. Informacijos slėpimas.....	53
Išvados	62
Literatūros sąrašas	63

Lentelių sąrašas

1 lentelė. Kriptografijos, vizualinės kriptografijos ir steganografijos kriterijų palyginimas.	16
2 lentelė. Atsitiktinai ir optimizavimo būdu sudarytos antrosios gardelės parametrų reikšmės prie skirtingų pirmosios gardelės parametrų.....	52

Paveikslų sąrašas

1 pav. Informacijos slėpimo metodų schema.....	16
2 pav. Klasikinio vizualinės kriptografijos metodo demonstracija. Skaidrės, kurios naudojamos informacijos atkodavimui, pavaizduotos (b) ir (c), originalus slaptas vaizdas pavaizduotas (a), o atkodavimo rezultatas pavaizduotas (d) vaizde.....	19
3 pav. Trys galimos vaizdo taško būsenos skaidrėse, skaidant tašką į keturias dalis. Pirmas ir antras vaizdai atitinka horizontalųjį, 3-4 vertikaliųjį, o 5-6 įstrižąjį vaizdo taško skaidymą.....	20
4 pav. Laike vidurkintų juostų formavimasis, kai $\lambda = 1.5$: (a) vienmačių pilkos spalvos tonų vidurkinti vaizdai didinant harmoninio vaizdo judinimo amplitudę; (b) nulinės eilės Beselio funkcijos reikšmių priklausomybė nuo $2\pi a/\lambda$ [50].....	22
5 pav. Harmoninė (a) ir Ronči tipo (b) muaro gardelė. Diagramos kairėje iliustruoja vienmatės gardelės funkciją, dešinėje esančios diagramos rodo pilkos spalvos reikšmių pasiskirstymą vaizde [51].....	22
6 pav. Pirmasis (a) ir antrasis (b) DVK schemos vaizdai, sudaryti iš 180 skirtingų beveik optimalių vienmačių muaro gardelių, sudėtų horizontaliai [44].	24
7 pav. Vienmatės gardelės taškų judėjimas pagal harmoninę funkciją [63].	28
8 pav. Dvimačio vaizdo harmoninio judėjimo vieną periodą schemą.	30
9 pav. Matricų vertimo į vektorius schema. Paveikslai (a) ir (b) grafiškai vaizduoja, kaip iš matricos gaunamas vektorius ir atvirkščiai [63].....	31
10 pav. Vaizdo taškų spalvos intensyvumo reikšmių skaičiavimo formulės $B \cdot P = V$ grafinė interpretacija [63].	32
11 pav. Gardelės transformacijos matricos B grafinis atvaizdavimas, kai gardelės svyravimo parametrai yra tokie: $a = 5, \alpha = \pi/4$	37
12 pav. Pirmoji stochastinė stacionari (pirmas vaizdas) ir laike vidurkinta (trečias vaizdas) gardelė, kai svyravimai atliekami $\pi/4$ kampų, amplitudė lygi 2, vaizdo dydis 30x30. Antrajame ir ketvirtajame vaizduose atitinkamai parodyti gardelių Wada indeksai. $F1$ optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 34x34, nežinomų sprendinių skaičius $34^2 = 1156$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 900, populiacijos dydis – 600 dalelių, tikslo funkcijos $F1$ koeficientų reikšmės: $k_1 = k_2 = k_3 = 1$	38
13 pav. Pirmosios gardelės optimizavimo konvergavimo grafikas: kiekvienoje iteracijoje rasto geriausio sprendinio reikšmė, kai svyravimai atliekami $\pi/4$ kampų, amplitudė lygi 2, vaizdo dydis 30x30. $F1$ optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 34x34, nežinomų sprendinių skaičius $34^2 = 1156$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 900, populiacijos dydis – 600 dalelių, tikslo funkcijos $F1$ koeficientų reikšmės: $k_1 = k_2 = k_3 = 1$	39
14 pav. Pirmoji stochastinė stacionari (pirmas vaizdas) ir laike vidurkinta (trečias vaizdas) gardelė, kai svyravimai atliekami $\pi/4$ kampų, amplitudė lygi 2, vaizdo dydis 30x30. Antrajame ir ketvirtajame vaizduose atitinkamai parodyti gardelių Wada indeksai. $F1$ optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 34x34, nežinomų sprendinių skaičius $34^2 = 1156$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 900, populiacijos dydis – 600 dalelių, tikslo funkcijos $F1$ koeficientų reikšmės: $k_1 = k_2 = k_3 = 0$	39

15 pav. Pirmoji stochastinė stacionari (pirmas vaizdas) ir laike vidurkinta (trečias vaizdas) gardelė, kai svyravimai atliekami $\pi/4$ kampų, amplitudė lygi 2, vaizdo dydis 30x30. Antrajame ir ketvirtajame vaizduose atitinkamai parodyti gardelių Wada indeksai. $F1$ optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 34x34, nežinomų sprendinių skaičius 342 = 1156, sprendinių reikšmių ribos [0;255], $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 900, populiacijos dydis – 600 dalelių, tikslo funkcijos $F1$ koeficientų reikšmės: $k1 = 1$, $k2 = k3 = 0$	40
16 pav. Pirmoji stochastinė stacionari (pirmas vaizdas) ir laike vidurkinta (trečias vaizdas) gardelė, kai svyravimai atliekami $\pi/4$ kampų, amplitudė lygi 2, vaizdo dydis 30x30. Antrajame ir ketvirtajame vaizduose atitinkamai parodyti gardelių Wada indeksai. $F1$ optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 34x34, nežinomų sprendinių skaičius 342 = 1156, sprendinių reikšmių ribos [0;255], $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 900, populiacijos dydis – 600 dalelių, tikslo funkcijos $F1$ koeficientų reikšmės: $k1 = 100$, $k2 = k3 = 1$	41
17 pav. Pirmoji stochastinė stacionari (pirmas vaizdas) ir laike vidurkinta (trečias vaizdas) gardelė, kai svyravimai atliekami $\pi/4$ kampų, amplitudė lygi 5, vaizdo dydis 30x30. Antrajame ir ketvirtajame vaizduose atitinkamai parodyti gardelių Wada indeksai. $F1$ optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 38x38, nežinomų sprendinių skaičius 382 = 1444, sprendinių reikšmių ribos [0;255], $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos $F1$ koeficientų reikšmės: $k1 = 100$, $k2 = k3 = 1$	42
18 pav. Pirmosios gardelės optimizavimo konvergavimo grafikas: kiekvienoje iteracijoje rasto geriausio sprendinio reikšmė, kai svyravimai atliekami $\pi/4$ kampų, amplitudė lygi 5, vaizdo dydis 30x30. $F1$ optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 38x38, nežinomų sprendinių skaičius 382 = 1444, sprendinių reikšmių ribos [0;255], $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos $F1$ koeficientų reikšmės: $k1 = 100$, $k2 = k3 = 1$	42
19 pav. Pirmoji laike vidurkinta gardelė, kai svyravimai atliekami $\pi/4$ kampų, tokiomis amplitudėmis: $a = 2$ (kairėje), $a = 5$ (viduryje), $a = 8$ (dešinėje), kai vaizdo dydis 60x60. $F1$ optimizavimo algoritmo parametrai: sprendinių reikšmių ribos [0;255], $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1100, populiacijos dydis – 600 dalelių, tikslo funkcijos $F1$ koeficientų reikšmės: $k1 = 100$, $k2 = k3 = 1$	43
20 pav. Gardelės transformacijos matricos B * grafinis atvaizdavimas, kai gardelė judinama elipsiniais svyravimais su tokiais parametrais: $a = 5$, $b = 5$	44
21 pav. Pirmoji stochastinė stacionari (pirmas vaizdas) ir laike vidurkinta (trečias vaizdas) gardelė, kai atliekami elipsiniai svyravimai, amplitudės lygios 5 ir 5, vaizdo dydis 30x30. Antrajame ir ketvirtajame vaizduose atitinkamai parodyti gardelių Wada indeksai. $F1$ optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 40x40, nežinomų sprendinių skaičius 402 = 1600, sprendinių reikšmių ribos [0;255], $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos $F1$ koeficientų reikšmės: $k1 = 100$, $k2 = k3 = 1$	44
22 pav. Gardelės transformacijos matricos B * grafinis atvaizdavimas, kai gardelė judinama elipsiniais svyravimais su tokiais parametrais: $a = 5$, $b = 3$	45

23 pav. Pirmoji stochastinė stacionari (pirmas vaizdas) ir laike vidurkinta (trečias vaizdas) gardelė, kai atliekami elipsiniai svyravimai, amplitudės lygios 5 ir 3, vaizdo dydis 40x40. Antrajame ir ketvirtajame vaizduose atitinkamai parodyti gardelių Wada indeksai. *F1* optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 40x40, nežinomų sprendinių skaičius $402 = 1600$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos *F1* koeficientų reikšmės: $k1 = 100$, $k2 = k3 = 1$ 45

24 pav. Pirmoji (a) ir antroji (b) stochastinė stacionari (pirmas vaizdas) ir laike vidurkinta (trečias vaizdas) gardelė, kai svyravimai atliekami $\pi/4$ kampų, amplitudė lygi 5, vaizdo dydis 30x30. Antrajame ir ketvirtajame vaizduose atitinkamai parodyti gardelių Wada indeksai. *F1* optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 38x38, nežinomų sprendinių skaičius $382 = 1444$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos *F1* koeficientų reikšmės: $k1 = 100$, $k2 = k3 = 1$ 47

25 pav. Pirmoji (a) ir antroji (b) stochastinė stacionari (pirmas vaizdas) ir laike vidurkinta (trečias vaizdas) gardelė, kai atliekami elipsiniai svyravimai, amplitudės lygios 5 ir 3, vaizdo dydis 30x30. Antrajame ir ketvirtajame vaizduose atitinkamai parodyti gardelių Wada indeksai. *F1* optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 40x40, nežinomų sprendinių skaičius $402 = 1600$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos *F1* koeficientų reikšmės: $k1 = 100$, $k2 = k3 = 1$ 48

26 pav. Pirmoji (a) ir antroji (b,c) stochastinė stacionari (pirmas stulpelis) ir laike vidurkinta (trečias stulpelis) gardelė, kai svyravimai atliekami $\pi/4$ kampų, amplitudė lygi 5, vaizdo dydis 30x30. Antrajame ir ketvirtajame vaizduose atitinkamai parodyti gardelių Wada indeksai. *F1* optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 38x38, nežinomų sprendinių skaičius $382 = 1444$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių. Antroji gardelė sudaryta optimizuojant pirmąją gardelę. *F2* optimizavimo algoritmo parametrai: (b) vaizdo optimizavimo sprendinių ribos $[-50;50]$, (c) vaizdo optimizavimo sprendinių ribos $[-85;85]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 400, populiacijos dydis – 500 dalelių, tikslo funkcijos *F1* koeficientų reikšmės: $k1 = 100$, $k2 = k3 = 1$ 49

27 pav. Antrosios gardelės optimizavimo konvergavimo grafikas: kiekvienoje iteracijoje rasto geriausio sprendinio reikšmė, kai svyravimai atliekami $\pi/4$ kampų, amplitudė lygi 5. *F1* optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 38x38, nežinomų sprendinių skaičius $382 = 1444$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos *F1* koeficientų reikšmės: $k1 = 100$, $k2 = k3 = 1$. Antroji gardelė sudaryta optimizuojant pirmąją gardelę. *F2* optimizavimo algoritmo parametrai: vaizdo optimizavimo sprendinių ribos $[-85;85]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 400, populiacijos dydis – 500 dalelių. 50

28 pav. Pirmoji (a) ir antroji (b) stochastinė stacionari (pirmas stulpelis) ir laike vidurkinta (trečias stulpelis) gardelė, kai atliekami elipsiniai svyravimai, amplitudės lygios 5 ir 3, vaizdo dydis 30x30. Antrajame ir ketvirtajame vaizduose atitinkamai parodyti gardelių Wada indeksai. *F1* optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 40x40, nežinomų sprendinių skaičius $402 =$

1600, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos $F1$ koeficientų reikšmės: $k1 = 100$, $k2 = k3 = 1$. Antroji gardelė sudaryta optimizuojant pirmąją gardelę. $F2$ optimizavimo algoritmo parametrai: (b) vaizdo optimizavimo sprendinių ribos $[-50;50]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 250, populiacijos dydis – 500 dalelių. 51

29 pav. Antrosios gardelės optimizavimo konvergavimo grafikas: kiekvienoje iteracijoje rasto geriausio sprendinio reikšmė, kai atliekami elipsiniai svyravimai, amplitudės lygios 5 ir 3, vaizdo dydis 30×30 . $F1$ optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 40×40 , nežinomų sprendinių skaičius $402 = 1600$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos $F1$ koeficientų reikšmės: $k1 = 100$, $k2 = k3 = 1$. Antroji gardelė sudaryta optimizuojant pirmąją gardelę. $F2$ optimizavimo algoritmo parametrai: (b) vaizdo optimizavimo sprendinių ribos $[-50;50]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 250, populiacijos dydis – 500 dalelių.... 51

30 pav. Stacionarių gardelių reikšmių pasiskirstymo grafikai: pirmoji stacionari gardelė (kairėje), antroji atsitiktinai sudaryta gardelė (viduryje) ir antroji optimizuota gardelė (dešinėje), kai svyravimai atliekami $\pi/4$ kampų, amplitudė lygi 5. $F1$ optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 38×38 , nežinomų sprendinių skaičius $382 = 1444$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos $F1$ koeficientų reikšmės: $k1 = 100$, $k2 = k3 = 1$. Antroji gardelė sudaryta optimizuojant pirmąją gardelę. $F2$ optimizavimo algoritmo parametrai: vaizdo optimizavimo sprendinių ribos $[-85;85]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 400, populiacijos dydis – 500 dalelių..... 52

31 pav. Stacionarių gardelių reikšmių pasiskirstymo grafikai: pirmoji stacionari gardelė (kairėje), antroji atsitiktinai sudaryta gardelė (viduryje) ir antroji optimizuota gardelė (dešinėje), kai atliekami elipsiniai svyravimai, amplitudės lygios 5 ir 3, vaizdo dydis 30×30 . $F1$ optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 40×40 , nežinomų sprendinių skaičius $402 = 1600$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos $F1$ koeficientų reikšmės: $k1 = 100$, $k2 = k3 = 1$. Antroji gardelė sudaryta optimizuojant pirmąją gardelę. $F2$ optimizavimo algoritmo parametrai: (b) vaizdo optimizavimo sprendinių ribos $[-85;85]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 250, populiacijos dydis – 500 dalelių. 53

32 pav. Slaptos informacijos slėpimas dvimatėje muaro gardelėje: slaptos informacijos vaizdas (a), slaptas vaizdas dvimatėje statinėje (kairėje) ir laike vidurkintoje (dešinėje) muaro gardelėje, kai antroji gardelė sudaryta atsitiktinai (b), slaptas vaizdas dvimatėje statinėje (kairėje) ir laike vidurkintoje (dešinėje) gardelėje, kai antroji gardelė sudaryta optimizuojant (c). $F1$ optimizavimo algoritmo parametrai: amplitudė lygi 5, svyravimų kampas $\pi/4$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, o vaizdo dydis yra 30×30 , optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 40×40 , nežinomų sprendinių skaičius $402 = 1600$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, tikslo funkcijos $F1$ koeficientų reikšmės: $k1 = 1$, $k2 = k3 = 1$. $F2$ optimizavimo algoritmo parametrai: (c) vaizdo optimizavimo sprendinių ribos $[-85;85]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi =$

0.5839, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 250, populiacijos dydis – 500 dalelių, tikslo funkcijos koeficientų reikšmės: $k_1 = 1, k_2 = k_3 = 1$ 54

33 pav. Slaptos informacijos slėpimas dvimatėse muaro gardelėse: laike vidurkinta slapta informacija, kai svyravimų amplitudė lygi 2 (kairėje), 5 (viduryje) ir 8 (dešinėje), o svyravimų kryptis yra kampas $\pi/4$ 55

34 pav. Slaptos informacijos slėpimas dvimatėse muaro gardelėse: slaptos informacijos vaizdas (a), slaptas vaizdas dvimatėje statinėje (kairėje) ir laike vidurkintoje (dešinėje) muaro gardelėje, kai antroji gardelė sudaryta atsitiktinai (b), slaptas vaizdas dvimatėje statinėje (kairėje) ir laike vidurkintoje (dešinėje) gardelėje, kai antroji gardelė sudaryta optimizuojant (c). *F1* optimizavimo algoritmo parametrai: amplitudė lygi 5, svyravimų kampas $\pi/4$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, o vaizdo dydis yra 100x100, optimizuojamas vaizdo dydis 108x108, nežinomų sprendinių skaičius 1082 = 11664, sprendinių reikšmių ribos [0;255], $\kappa = 0.8, c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, tikslo funkcijos *F1* koeficientų reikšmės: $k_1 = 100, k_2 = k_3 = 1$. *F2* optimizavimo algoritmo parametrai: (c) vaizdo optimizavimo sprendinių ribos [-85;85], $\kappa = 0.8, c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 250, populiacijos dydis – 500 dalelių, tikslo funkcijos *F1* koeficientų reikšmės: $k_1 = 1, k_2 = k_3 = 1$ 56

35 pav. Slaptos informacijos slėpimas dvimatėse muaro gardelėse: slaptos informacijos vaizdas (a), slaptas vaizdas dvimatėje statinėje (kairėje) ir laike vidurkintoje (dešinėje) muaro gardelėje, kai antroji gardelė sudaryta atsitiktinai (b), slaptas vaizdas dvimatėje statinėje (kairėje) ir laike vidurkintoje (dešinėje) gardelėje, kai antroji gardelė sudaryta optimizuojant (c). *F1* optimizavimo algoritmo parametrai: amplitudė lygi 5, svyravimų kampas $\pi/4$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, o vaizdo dydis yra 100x100, optimizuojamas vaizdo dydis 108x108, nežinomų sprendinių skaičius 1082 = 11664, sprendinių reikšmių ribos [0;255], $\kappa = 0.8, c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, , tikslo funkcijos koeficientų reikšmės: $k_1 = 100, k_2 = k_3 = 1$. *F2* optimizavimo algoritmo parametrai: (c) vaizdo optimizavimo sprendinių ribos [-85;85], $\kappa = 0.8, c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 250, populiacijos dydis – 500 dalelių, tikslo funkcijos koeficientų reikšmės: $k_1 = 1, k_2 = k_3 = 1$ 57

36 pav. Slaptos informacijos slėpimas dvimatėse muaro gardelėse: slaptos informacijos vaizdas (a), slaptas vaizdas dvimatėje statinėje (kairėje) ir laike vidurkintoje (dešinėje) muaro gardelėje, kai antroji gardelė sudaryta optimizuojant su [-50;50] korekcijomis (b) ir [-85;85] korekcijomis (c). *F1* optimizavimo algoritmo parametrai: amplitudė lygi 5, svyravimų kampas $\pi/4$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, o vaizdo dydis yra 100x100, optimizuojamas vaizdo dydis 108x108, nežinomų sprendinių skaičius 1082 = 11664, sprendinių reikšmių ribos [0;255], $\kappa = 0.8, c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos koeficientų reikšmės: $k_1 = 100, k_2 = k_3 = 1$. *F2* optimizavimo algoritmo parametrai: $\kappa = 0.8, c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 250, populiacijos dydis – 500 dalelių, tikslo funkcijos koeficientų reikšmės: $k_1 = 1, k_2 = k_3 = 1$ 58

37 pav. Slaptos informacijos slėpimas dvimatėse muaro gardelėse: slaptos informacijos vaizdas (a), slaptas vaizdas optimizuotoje dvimatėje statinėje (kairėje) ir laike vidurkintoje (dešinėje) muaro gardelėje, kai antroji gardelė sudaryta optimizuojant su [-35;35] korekcijomis (b) ir [-50;50] korekcijomis (c). *F1* optimizavimo algoritmo parametrai: elipsinių svyravimų amplitudės lygios 5 ir 3, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, o vaizdo dydis yra 100x100,

optimizuojamas vaizdo dydis 110x110, nežinomų sprendinių skaičius 1102 = 12100, sprendinių reikšmių ribos [0;255], $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, tikslo funkcijos koeficientų reikšmės: $k_1 = 100$, $k_2 = k_3 = 1$. F2 optimizavimo algoritmo parametrai: $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 300, populiacijos dydis – 300 dalelių, tikslo funkcijos koeficientų reikšmės: $k_1 = 1$, $k_2 = k_3 = 1$ 59

38 pav. Informacijos slėpimo rezultatai: užkoduotos informacijos vaizdas (kairėje) ir atkoduotos informacijos vaizdas (dešinėje), kai dvimatė stochastinė gardelė svyruoja harmoniniais svyravimais su amplitude 5 (a) ir elipsiniais svyravimais su amplitudėmis 5 ir 3 (b).). F1 optimizavimo algoritmo parametrai: iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, o vaizdo dydis yra 100x100, optimizuojamas vaizdo dydis 110x110, nežinomų sprendinių skaičius 1102 = 12100, sprendinių reikšmių ribos [0;255], $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, tikslo funkcijos koeficientų reikšmės: $k_1 = 100$, $k_2 = k_3 = 1$. F2 optimizavimo algoritmo parametrai: $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 250 (b) ir 300 (c), populiacijos dydis – 250 (b) ir 300 (c) dalelių, tikslo funkcijos koeficientų reikšmės: $k_1 = 1$, $k_2 = k_3 = 1$ 60

39 pav. Informacijos atkodavimo vaizdai (pirmoje eilutės) ir jų transformacijos operatorių vaizdai (antroje eilutėje), kai naudojami šie vidurkinimo parametrai: $a = 2, \alpha = \pi/4$ (a), $a = 7, \alpha = \pi/4$ (b) ir $a = 5, \alpha = \pi/3$ (c). Informacijos slėpimas pradinėje gardelėje atliktas su šiais vidurkinimo parametrais: $a = 5, \alpha = \pi/4$ 61

Santrumpų ir terminų sąrašas

Santrumpos:

CMY (ŽPG) – spalvų modelis skirtas spalvos intensyvumo koregavimui, naudojant šias tris spalvas, kaip pagrindines: žydrą (*angl. cyan*), purpurinę (*angl. magenta*) ir geltoną (*angl. yellow*).

DVK – dinaminė vizualinė kriptografija.

LSB - steganografijos metodas, kuris remiasi informacijos paslėpimu mažiausiai svarbiame vaizdo taško bite (paskutinis vaizdo taško bitas) (*angl. Least Significant Bit*).

PSO – dalelių spiečiaus optimizavimas (*angl. particle swarm optimization*).

PVD – steganografijos metodas, kuris skaičiuoja dviejų vaizdo taškų reikšmių skirtumą (*angl. Pixel Value Differencing*). Jeigu reikšmių skirtumas yra didesnis, daugiau slaptos informacijos bitų yra koduojama tuose taškuose.

Terminai:

Dinaminė vizualinė kriptografija – kriptografijos atšaka, kai slapta informacija yra slepiama viename vaizde, o jos atkodavimas atliekamas pasitelkiant tam tikrus dinامينius dėsnius.

Maišos funkcija – kriptografijoje naudojama funkcija, kuri įvairias įvestis paverčia į numatyto ilgio ženklų eilutes.

Muaro gardelė – optikos srityje naudojama frazė, kuri apibūdina antrinę interferencinę vaizdą, susidarantį iš kelių tam tikro rašto rastrų.

Nešėjas – skaitmeninis objektas, per kurį slapta informacija yra perduodama (gali būti teksto ar vaizdo formate) (*angl. carrier*).

Vandenženkliai – matomi arba nematomi ženklai, kurie yra įterpiami į įvairias skaitmenines medijas (*angl. watermarking*).

Įvadas

Slaptos komunikacijos idėja yra tokia pat sena, kaip pati komunikacija. Pirmosios istorijos, kurios interpretuojamos kaip slaptas komunikavimas, pasirodė jau senovės graikų literatūroje, pavyzdžiui, Homero “Iliadoje” ar Herodoto pasakose [1]. Šiais laikais saugus informacijos perdavimas ypač svarbus finansų, sveikatos ar krašto apsaugos srityse, autentifikacijoje. Todėl informacijos slėpimo schemų kūrimas yra aktuali tyrimo tema.

Informacijos slėpimas tiriamas tokių praktikų kaip kriptografija, steganografija ar vandenženklių kūrimas. Steganografija ir kriptografijos atšaka vizualinė kriptografija tiria informacijos slėpimą vaizduose. Pačio termino “steganografija” pažodinis vertimas iš graikų kalbos reiškia “uždengtas raštas” [2,3]. Pagrindinis steganografijos principas informacijos slėpime yra išskaidyti kiekvieną vaizdo tašką bitais ir paslėpti informaciją mažiausiai reikšminguose bituose. Vizualinė kriptografija – tai informacijos slėpimo skaitmeniniuose vaizduose metodika, kai slaptas vaizdas yra išskaidomas į du ar daugiau skirtingų vaizdų taip, kad nei viename iš jų, atskirai paėmus, slaptos informacijos įžvelgti neįmanoma, tačiau sudėjus visas vaizdo dalis, slapta informacija atkoduojama tiesiog plika akimi. Dinaminėje vizualinėje kriptografijoje (DVK) slaptas vaizdas yra užkoduojamas jį įterpiančią muaro linijų tinklą taip, kad užkoduotame statiniame vaizde slaptos informacijos būtų neįmanoma įžiūrėti, tačiau atkoduoti informaciją taip pat galima plika akimi, kaip ir klasikinėje vizualinėje kriptografijoje. Tam užkoduotą vaizdą reikia virpinti iš anksto numatyto dėsnio su iš anksto nustatytais parametrais. 2023 m. buvo pristatyta DVK schema, leidžianti slėpti informaciją vienmatėse neperiodinėse stochastinėse muaro gardelėse. Deja, slaptai informacijai užkoduoti bei atkoduoti šioje DVK schemoje įmanoma panaudoti tik horizontalios ar vertikalios krypties harmoninius virpesius. Įvairių krypčių harmoninių ar netgi elipsinių virpesių panaudojimas tokio tipo schemoje ne tik padidintų įterpiamos informacijos saugumą, bet ir išplėstų DVK taikymo galimybes. Todėl šiame tyrime siūloma DVK schema, pagrįsta dvimatėmis stochastinėmis muaro gardelėmis.

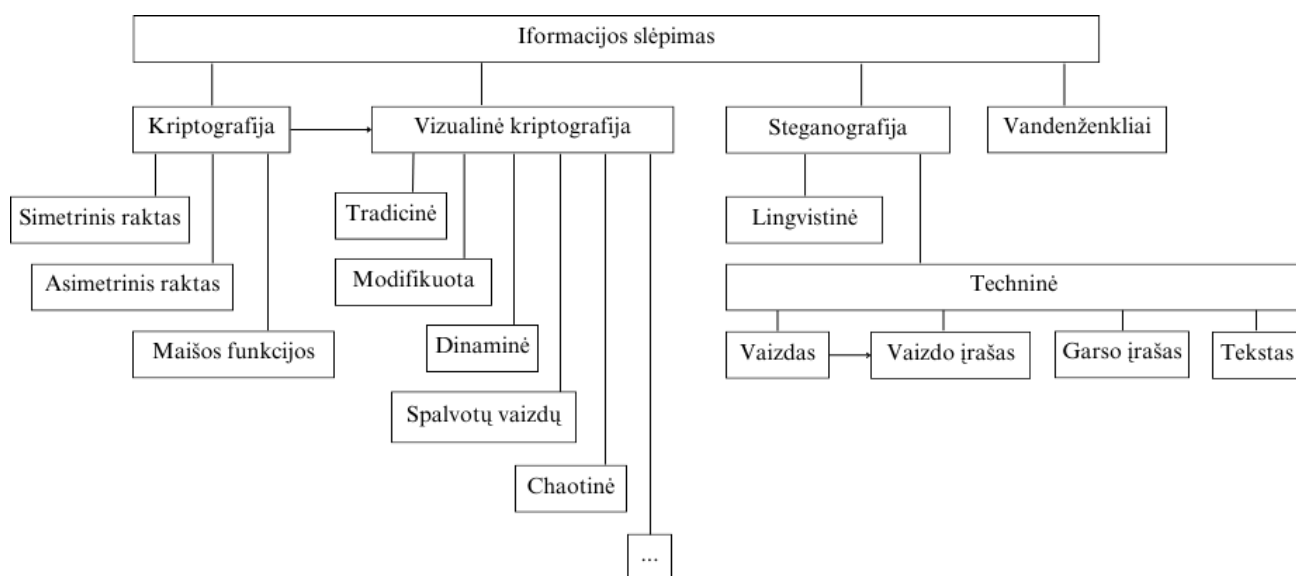
Tikslas. Pasiūlyti dinaminės vizualinės kriptografijos metodiką, skirtą vaizdinei informacijai dvimatėje stochastinėje muaro gardelėje paslėpti.

Uždaviniai.

1. Parengti laike vidurkintos dvimatės stochastinės muaro gardelės sudarymo metodologiją bet kurios krypties harmoninių ar elipsinių virpesių atvejais.
2. Suformuluoti reikalavimus dvimatėms stochastinėms muaro gardelėms taip, kad jos būtų tinkamos vaizdų slėpimui.
3. Suformuluoti ir išspręsti dvimačių stochastinių muaro gardelių, skirtų vaizdų slėpimui, optimizavimo uždavinį.
4. Pademonstruoti pasirinktos vaizdinės informacijos slėpimą dvimatėje optimizuotose muaro gardelėse.

1. Literatūros apžvalga

Informacijos saugumas yra viena didžiausių technologijos amžiaus problemų, kurias sprendžia kriptologijos metodai. Informacijos slėpimo metodikos bendru atveju gali būti išskiriamos į tris grupes: kriptografiją (*angl.* cryptography), steganografiją (*angl.* steganography) ir vandenženklus (*angl.* watermarking) [4]. Vizualinės kriptografijos metodika yra atskira kriptografijos metodikos dalis, skirta informacijos slėpimui vaizduose. Informacijos slėpimo metodikų schema pavaizduota **1 pav.** [4, 5, 6], o 1 lentelė aprašo kriptografijos, vizualinės kriptografijos ir steganografijos palyginimą [4,6-8]. Minėtos metodikos praktikoje yra persipynusios: vizualinė kriptografija yra naudojama vandenženklių sudaryme [4,9], o steganografijos ir kriptografijos metodai papildo vienas kitą ir dažnai yra naudojami kartu [4,10,11] dėl aukštesnio saugos lygio.



1 pav. Informacijos slėpimo metodų schema.

1 lentelė. Kriptografijos, vizualinės kriptografijos ir steganografijos kriterijų palyginimas.

Kriterijus	Kriptografija	Vizualinė kriptografija	Steganografija
Nešėjas	Dažniausiai tekstinis, kartais vaizdų formatas	Vaizdų formatas	Bet koks skaitmeninių medijų formatas
Slapta informacija	Tekstas	Vaizdas	Tekstas, vaizdas, garso ar vaizdo įrašas
Raktas	Būtinas	Nereikalingas	Pasirenkamas
Įvesties failai	Vienas	Du arba daugiau	Du arba daugiau
Tikslas	Duomenų apsauga	Saugus duomenų perdavimas ir saugojimas	Slapta komunikacija
Užkodavimo įrankis	Kompiuteris	Kompiuteris	Kompiuteris
Atkodavimo įrankis	Kompiuteris	Vizualinis arba kompiuteris	Kompiuteris

Komunikacijos saugumas	Priklauso nuo rakto konfidencialumo	Priklauso nuo to, ar vaizdo dalys saugomos kartu	Priklauso nuo įterpimo metodo sudėtingumo ir konfidencialumo
Rezultatas	Šifruotas tekstas	Kelios atsitiktinai atrodančios vaizdo dalys	Vaizdas su įterpta informacija (<i>angl.</i> stego file)
Taikymo sritys	Duomenų saugumas ir privatumas, saugus komunikavimas, autentifikacija ir prieigos kontrolė, skaitmeniniai parašai ir t.t.	Informacijos slėpimas, autentifikacija, balsavimo sistemos, virpesių kontrolės, regos sistemų, biomedicininės sistemų tyrimai	Informacijos slėpimas, duomenų privatumas ir saugumas, autorinių teisių apsauga, slapta komunikacija, autentifikacija ir t.t.

1 lentelėje nėra aprašyta vandenženklių kūrimo metodika, kadangi jos tikslas ir požymiai nėra susiję su tyrimo tematika. Popierinis vandenženklių kūrimas prasidėjo dar XIII amžiuje Italijoje su tikslu identifikuoti popieriaus gamintojus [12] ir autentifikuoti popierių, vėliau šis metodas išplito po visą pasaulį. Popieriaus, pinigų banknotų vandenženklių kūrimas buvo įkvėpimas ir skaitmeninių duomenų vandenženklių sudarymui, kuris kompiuterinėse technologijose atsirado 1988 metais ir skaitmeniniuose vaizduose taikomas nuo 1995 metų [12,13]. Vandenženklių kūrimas yra tokia metodika, kuri matomą arba nematomą ženklą (tekstą, vaizdą ar raštą) įterpia į tokias skaitmenines medijas kaip vaizdai, garso ar vaizdo įrašai, dokumentai. Vandenženklių metodikos tikslas yra identifikuoti intelektualinės nuosavybės savininkus, nuosavybės autentiškumą, bei sustiprinti multimedijos dokumentų saugumą [13].

Kriptografija – informacijos apsaugojimo metodas, naudojantis kodus, kuriuos turint gali būti atskleista slapta informacija. Kriptografija yra pagrįsta paprastuoju ir šifruotuoju tekstu. Užkoduoiant pradinį, t.y. paprastąjį, tekstą gaunamas užšifruotas tekstas, kuris yra siunčiamas per kanalą, gavėjas gautą tekstą iššifruoja ir gauna paprastąjį, pradinį tekstą [4,6]. Šifravimo procese svarbiausias saugą užtikrinantis aspektas yra raktas: simetrinis, asimetrinis ir maišos (*angl.* hash) funkcijos, kurių turėtojai gali tekstą užšifruoti ir iššifruoti. Kriptografija geriausiai pritaikoma paprastiems tekstams, nors gali būti naudojama ir vaizdų šifravimui [4,6]. Plačiau vizualinės kriptografijos metodai ir pritaikymas aprašyti 1.2 skyrelyje. Kriptografijoje yra žinoma, kad slapta informacija yra siunčiama, todėl vis plačiau pradėta analizuoti steganografiją, kuri tiria metodus, slepiančius informaciją vaizduose tokiu būdu, kad stebėtojas neįtaria, jog stebimame vaizde egzistuoja slapta informacija [2]. Taip informacija gali būti perduodama viešais komunikavimo kanalais.

1.1. Steganografija

Steganografija – tai komunikacijos slėpimo metodika, kuri įterpia konfidencialius duomenis (tekstą, vaizdus ar kt.) kitoje neslaptoje informacijos terpėje, dar vadinama nešėju (tekstas, vaizdas, vaizdo ar garso įrašas). [3,14] Terminas „steganografija“ pažodinis vertimas iš graikų kalbos reiškia „uždengtas raštas“ [2,3]. Dabar internetas plačiai naudojamas skaitmeninių medijų mainuose tarp privačių individų, kompanijų, institucijų, dėl to saugumo ir privatumo tema darosi vis aktualesnė [14,15]. Šiame kontekste steganografija sulaukė pripažinimo ir yra naudojama slėpti informaciją taip, kad žmogaus akiai ji būtų nepastebima [3,14,15].

Steganografijos tyrimus galima skirstyti pagal du faktorius: slaptos informacijos prigimtį bei naudojamą slėpimo metodiką [15]. Pagal informacijos prigimtį steganografija gali būti lingvistinė arba skaitmeninė [15]. Vaizdo steganografija taip pat gali būti klasifikuojama pagal informacijos įterpimo sritį: vaizdo steganografija erdvinėje srityje (*angl.* domain) ir vaizdo steganografija dažnio srityje [16,17].

1.1.1. Steganografija erdvinėje srityje

Erdvinės vaizdo srities steganografijos schema slepia informaciją tiesiogiai nešėjo erdvėje, t.y. pagrindinio vaizdo taškuose (*angl.* pixels). Šiame procese steganografijos metodika naudoja vaizdo taškų ryškumo reikšmes bitais, kuriuose užkoduojamas slaptos informacijos bitų reikšmės. Tokios metodikos laikomos paprasčiausiomis informacijos slėpimo steganografijos metodikomis.

Vienas populiariausių šios rūšies steganografijos metodų yra LSB (*angl.* Least Significant Bit) metodas, kuris remiasi informacijos paslėpimu mažiausiai svarbiame vaizdo taško bite (paskutinis vaizdo taško bitas), tokiu būdu taško reikšmę pakeičiant daugiausia 1 vienetu ir padarant slėpimo procesą beveik nepastebimu [16-18]. Tačiau taip paslėpta informacija gali būti lengvai atkoduojama arba pakeičiama, kadangi įsibrovėliui užtenka žinoti, jog egzistuoja slapta informacija, kurią atitinkantys bitai lengvai modifikuojami arba atskleidžiami naudojant standartinę bitų plokštumų analizę [19].

Ilgainiui, dėl saugos lygio didinimo LSB metodas buvo modifikuojamas. Siūloma k -LSB metodika, kuri slaptą vaizdą užkoduoja į k mažiausiai reikšmingų bitų [15,19]. Taip pat naudojamas metodas, kuris originalų vaizdą padalina į atskirus blokus, kuriuose paslepiama informacija bitais. Kiekvienas blokas yra išskiriamas į sluoksnius naudojant vaizdo taškų dvejetainių reikšmių skaitmenis. Tada ieškomi panašiausi originalaus vaizdo ir slaptos informacijos bitai ir pastarieji pakeičia originalius bitus [20]. Taip pat plačiai naudojamas PVD (*angl.* Pixel Value Differencing) metodas, kuris skaičiuoja dviejų vaizdo taškų reikšmių skirtumą. Jeigu reikšmių skirtumas yra didesnis, daugiau slaptos informacijos bitų yra koduojama tuose taškuose. Mažesnio skirtumo taškuose atitinkamai koduojamas mažesnis kiekis slaptos informacijos bitų [17,21].

1.1.2. Steganografija dažnio srityje

Dažnio srities, dar vadinamos transformacijos srities, vaizdo steganografijos schemoje panaudojus įvairias transformacijos metodikas iš erdvinės srities pereinama į dažnių sritį, kurioje yra slepiama slapta informacija. Tokio metodo kodavimo procesas yra sudėtingesnis, todėl sistema laikoma saugesne. Dažnio srities steganografija taiko tokias metodikas kaip diskrečiųjų bangelių transformacija (DBT), diskrečioji Furjė transformacija (DFT), diskrečioji kosinuso transformacija (DKT) ir kt. [17] Šių transformacijų koeficientai atlieka informacijos nešėjo funkciją [22,23].

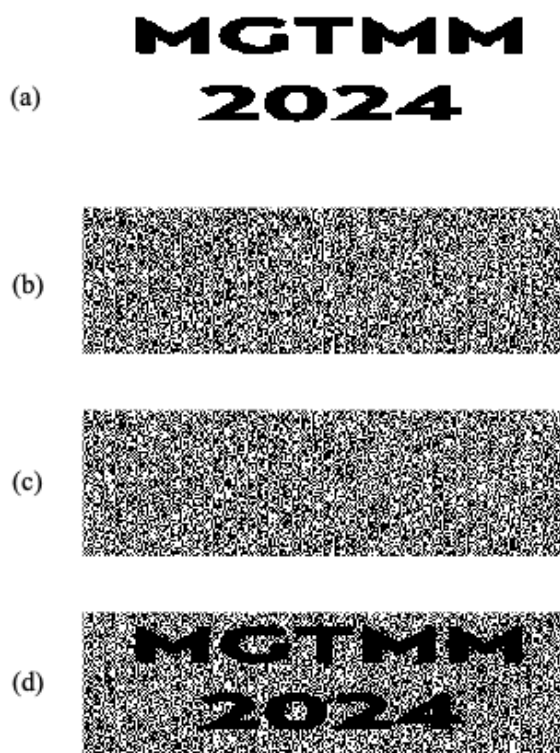
1.2. Vizualinė kriptografija

Vizualinė kriptografija yra Naor'o ir Shamir'o 1994 metais pristatyta kriptografijos metodika, kuri paslepia vaizdinę informaciją tokiu būdu, kad jos atkodavimas atliekamas be jokių skaičiavimų, o pasitelkiant tik žmogaus regą. Klasikinės vizualinės kriptografijos schemoje slaptas vaizdas yra suskaidomas į n dalių tokiu būdu, kad slapta informacija būtų matoma tik turint visas vaizdo dalis [24]. Nuo 1994 metų iki šių dienų vizualinė kriptografija stipriai patobulėjo. Vizualinė kriptografija dabar gali būti naudojama ne tik pilkiems, bet ir spalvotiems vaizdams [25,26,27]. Taip pat ši sritis išplėtota taip, kad slapto vaizdo atkodavimui naudojamos nebūtinai visos n dalys [28], o kai kurie

metodai pagrįsti net kvantinės fizikos principais [29]. Dar vienas svarbus vizualinės kriptografijos išplėtimas – tai dinaminė vizualinė kriptografija [30], pagrįsta muaro gardelių, o ne kelių skaidrių panaudojimu.

1.2.1. Klasikinė vizualinė kriptografija

Klasikinės vizualinės kriptografijos pradininkai Moni Naor'as ir Adi Shamir'as [24] pasiūlė informaciją slėpti ją išskaidant į kelias skaidres, kurias tam tikru būdu sudėjus viena ant kitos išryškėja slaptas vaizdas. Šiame metode slapta informacija yra sudaryta iš juodų (slapta informacija) ir baltų (fonas) vaizdo taškų, kurie padalinami į atskiras skaidres. Kiekviena skaidrė taip pat yra juodų ir baltų taškų rinkinys, kuris vizualiai atrodo atsitiktinis. Slapto vaizdo taškai yra išskaidomi į skaidres, kurias sudėjus išryškėja informacija, kaip pavaizduota **2 pav.** [31]. Matoma, kad vaizdai (b) ir (c) atrodo kaip atsitiktiniai vaizdai iš juodų ir baltų vaizdo taškų bei nutekina slaptos informacijos, pavaizduotos (a) vaizde. Sudėjus (b) ir (c) vaizdus gaunamas (d) vaizdas, kuriame matoma slapta informacija [44].



2 pav. Klasikinio vizualinės kriptografijos metodo demonstracija. Skaidrės, kurios naudojamos informacijos atkodavimui, pavaizduotos (b) ir (c), originalus slaptas vaizdas pavaizduotas (a), o atkodavimo rezultatas pavaizduotas (d) vaizde.

Toks slaptos informacijos kodavimo metodas paremtas slapto vaizdo kiekvieno taško skaidymu į kelias mažesnes dalis, kuriose juodų ir baltų dalių skaičius vienam taškui turi būti vienodas. Autoriai rekomendavo naudoti 4 dalis vienam vaizdo taškui. Tada kiekvienas taškas gali būti išskaidomas į skaidres trimis variantais: horizontaliai, vertikaliai, įstrižai, kaip pavaizduota **3 pav.** [24] Tokiu būdu pirmojoje skaidrėje parenkama bet kuri koduojamo vaizdo taško būseną, o antrojoje skaidrėje naudojama priešinga būseną, jei norima išryškinti slaptą informaciją. Antroje skaidrėje naudojama tokia pati taško būseną, jeigu slapta informacija nebus išryškinama [24].



3 pav. Trys galimos vaizdo taško būsenos skaidrėse, skaidant tašką į keturias dalis. Pirmas ir antras vaizdai atitinka horizontalųjį, 3-4 vertikalųjį, o 5-6 įstrižąjį vaizdo taško skaidymą.

Tokiu principu sudaromos reikalingo dydžio skaidrės, kurios atspausdinamos ant skaidrių plėvelių. Plėvelės sudėjus gaunamas koduotas vaizdas.

1.2.2. Modifikuota vizualinė kriptografija

Nuo 1994 metų vizualinė kriptografija buvo sparčiai tobulinama. Jau 1999 metais Ryo Ito ir kiti pasiūlė patobulintą klasikinės vizualinės kriptografijos schemą, kuri leidžia slėpti vaizdą neskaidant taškų į dar mažesnes dalis [32]. Vėliau pradėti kurti spalvoto slapto vaizdo kodavimo metodai [25,26,27] ir jų patobulinimai, siekiant išvengti spalvų užtamsėjimo [33], naudojant baltų vaizdo taškų rekonstrukciją PRWP (*angl.* Perfect Reconstruction of White Pixel) vietoj įprastai naudojamų juodų taškų [34], bei naudojant ŽPG (*angl.* CMY) spalvų erdvę [35].

2000 metais [36] straipsnyje autoriai aprašo vizualinę kriptografiją skirtingo pilkumo vaizdams. Po dešimtmečio atsirado metodai, leidžiantys formuoti skirtingas slapto vaizdo komponentes naudojant skirtingus parametrus [37]. Naudojant pastarąjį metodą, dedant daugiau skaidrių, matoma daugiau slaptos informacijos. [28] straipsnyje pristatyta tikimybinė k iš n vizualinės kriptografijos schema, naudojama pilkiems ir spalvotiems vaizdams koduoti. Tokiu būdu slapta informacija gali būti atkoduojama naudojant ne visas, bet k ar daugiau skaidrių. 2013 metais pasiūlyta padidintos talpos vizualinė kriptografija, kuri leidžia paslėpti daugiau informacijos pilkame vaizde pasitelkiant jo taškų šešėlius [38]. [39] straipsnyje aprašyta pilkos spalvos pustoniais grįsta vizualinė kriptografija.

Naujausi straipsniai aprašo vizualinės kriptografijos patobulinimus naudojant t paklaidų taisymą (*angl.* t-error correcting capability) [40], vieno vaizdo taško atvaizdavimą (*angl.* SPI single-pixel imaging) [41,42] ar dvejetainį laumžirgio algoritmą (*angl.* binary dragonfly algorithm) [43]. Taip pat vis labiau plėtojama dinaminė vizualinė kriptografija, pagrįsta muaro gardelėmis [44-47].

1.2.3. Dinaminė vizualinė kriptografija

Dinaminės vizualinės kriptografijos (DVK) idėją pasiūlė M. Ragulskis ir bendraautoriai 2009 metais [40]. Vietoje įprastai vizualinėje kriptografijoje naudojamų kelių skaidrių pradėtos naudoti harmoninės muaro gardelės ir tokiu būdu visas slaptas vaizdas paslėpiamas viename vaizde (panašiai, kaip ir steganografijoje) [30,48]. Slapta informacija užkoduotame vaizde nėra matoma plika akimi. Informaciją galima atkoduoti tiesiog vizualiai, stebint virpančią vaizdą, dėl to šis metodas priskiriamas vizualinei kriptografijai. Slaptas vaizdas bus atkoduotas tik tada, kai parenkama iš anksto numatyta harmoninio svyravimo amplitudė, naudota vaizdui paslėpti. Apie dinaminę vizualinę kriptografiją galima detaliau kalbėti tik susipažinus su geometrinio muaro ir laike vidurkinto geometrinio muaro sąvokomis ir pagrindiniais veikimo principais.

1.2.3.1. Harmoninė muaro gardelė

Muaro gardelė pusiausvyros būsenoje gali būti aprašoma harmonine funkcija [49]:

$$M(x) = \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} x\right), \quad (1)$$

čia x – erdvės koordinatė; λ – muaro gardelės periodas, nurodantis atstumą tarp dviejų baltų (arba juodų) gardelės linijų centrų; $M(x)$ – paviršiaus pilkumo lygis taške x , kur reikšmė 0 atitinka juodą spalvą, reikšmė 1 – baltą spalvą, o tarpinės reikšmės atitinkamus pilkus atspalvius [44].

Jeigu gardelė virpinama laike pagal harmoninę funkciją $a \sin(\omega t + \varphi)$ statmenai gardelės linijoms (a, ω, φ atitinkamai žymi harmoninio virpėjimo amplitudę, dažnį ir fazę), tai pilkos spalvos reikšmė taške x laiko momentu t_0 bus apskaičiuojama taip:

$$M(x)|_{t=t_0} = \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda}(x - a \sin(\omega t_0 + \varphi))\right). \quad (2)$$

Jeigu atliekamas vidurkinimas laike, pavyzdžiui, fotografuojant su ilga ekspozicija, tai pilkas laike vidurkintas vaizdas apibūdinamas taip:

$$\bar{M}(x, a) = \lim_{T \rightarrow \infty} \int_0^T M(x - a \sin(\omega t + \varphi)) dt = \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} x\right) J_0\left(\frac{2\pi}{\lambda} a\right), \quad (3)$$

čia J_0 yra nulinės eilės pirmojo tipo Beselio funkcija:

$$J_0(x) = \lim_{T \rightarrow \infty} \int_0^T \exp(i \cdot x \sin(\omega t + \varphi)) dt; \quad i^2 = -1. \quad (4)$$

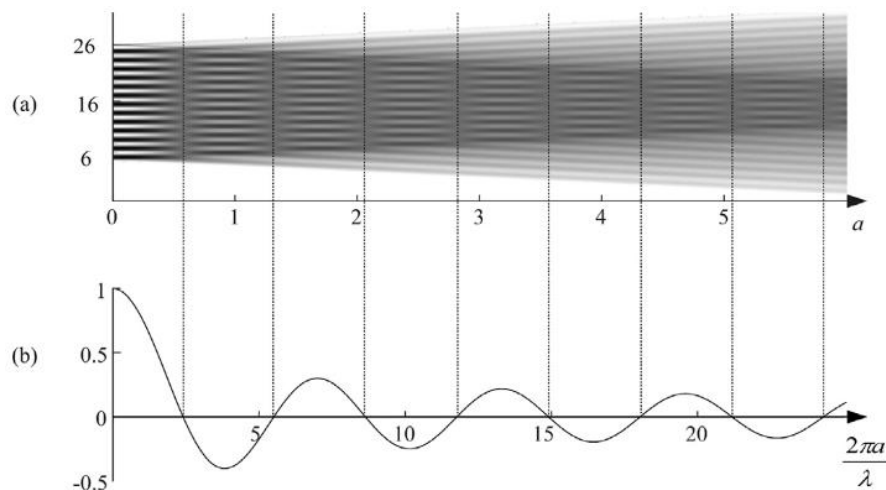
Laike vidurkintos juostos pilnai susiformuoja, kai

$$J_0\left(\frac{2\pi}{\lambda} a\right) = 0, \quad (5)$$

t.y. nulinės eilės Beselio funkcija yra lygi nuliui. Tada sąryšis tarp laike vidurkintų juostų eilės, harmoninių svyravimų amplitudės ir gardelės periodo aprašomas [49]:

$$\frac{2\pi}{\lambda} a_i = r_i, \quad (6)$$

čia r_i žymi i -tąją J_0 šaknį; a_i yra svyravimų amplitudė i -tosios laike vidurkintos juostos centre. Šis optinis efektas, t.y. laike vidurkintų juostų formavimasis, yra pavaizduotas **4 pav.** [50]. Kairėje (a) vaizdo pusėje (kai $a = 0$) matoma stacionari vienmatė muaro gardelė. Laike vidurkintas vaizdas, kuris gaunamas judinant vienmatę muaro gardelę, matomas kiekviename vaizdo taškų stulpelyje, kai amplitudės reikšmė yra diskreti. Funkcijos $J_0\left(\frac{2\pi}{\lambda} a\right)$ grafikas yra parodytas **4 pav.** (b), kur punktyrinės vertikalios linijos nurodo J_0 šaknų vietas. Grafike aiškiai matoma, kad laike vidurkintų muaro juostų centrai sutampa su pirmojo tipo nulinės eilės Beselio funkcijos J_0 šaknimis.



4 pav. Laike vidurkintų juostų formavimasis, kai $\lambda = 1.5$: (a) vienmačių pilkos spalvos tonų vidurkinti vaizdai didinant harmoninio vaizdo judinimo amplitudę; (b) nulinės eilės Beselio funkcijos reikšmių priklausomybė nuo $2\pi a/\lambda$ [50].

Harmoninės muaro gardelės vaizdų slėpimui taikomos taip, kad suvidurkintas fonas kuo tolygiau užpilkėtų, o suvidurkintas slaptas vaizdas būtų kuo margsnis (Beselio nulinės eilės funkcijos reikšmės nebūtų artimos nuliui).

1.2.3.2. Ronči tipo muaro gardelė

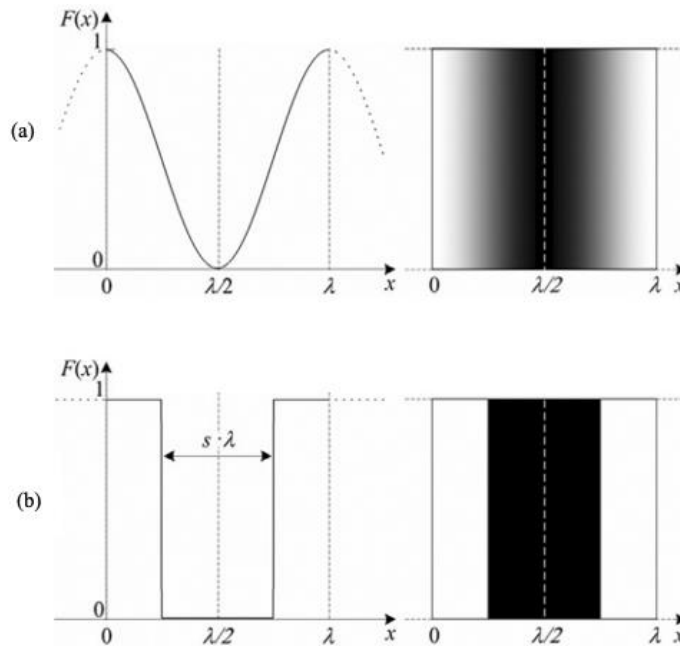
Dinaminėje vizualinėje kriptografijoje be harmoninės muaro gardelės gali būti naudojama ir Ronči tipo muaro gardelė, dar vadinama stačiakampe muaro gardele. Ši gardelė generuoja laike vidurkintas interferencines juostas tik tada, kai yra teisingai parinktas judesio dėsnis, pavyzdžiui, svyravimai trikampės bangos formos [51]. Tokia muaro gardelė pasirenkama dėl aukštesnio saugumo lygio. [51] straipsnyje autoriai pasirenka naudoti Ronči tipo muaro gardelę:

$$F(x) = \begin{cases} 1, & \text{kai } x \in \left[\lambda j; \frac{(1-s)\lambda}{2} + \lambda j \right] \cup \left[\frac{(1+s)\lambda}{2} + \lambda j; \lambda(j+1) \right] \\ 0, & \text{kai } \left(\frac{(1-s)\lambda}{2} + \lambda j; \frac{(1+s)\lambda}{2} + \lambda j \right) \end{cases}, \quad (7)$$

čia $j = 0, \pm 1, \pm 2, \dots$, parametras s žymi muaro gardelės santykį tarp baltų ir juodų juostų pločio; λ – gardelės periodas. Pati gardelė $F(x)$ gali būti išskleista Furjė eilute su tokiais koeficientais:

$$F(x) = \begin{cases} a_0 = 2(1-b) \\ a_k = \frac{\sin(k\pi(1-s)) - \sin(k\pi(1+s))}{k\pi} \\ b_k = \frac{\cos(k\pi(1+s)) - \cos(k\pi(1-s))}{k\pi} \end{cases}, \quad (8)$$

čia $k = 1, 2, \dots$. Harmoninė ir Ronči tipo muaro gardelės pavaizduotos **5 pav.**, kai gardelės juostų plotis vienodas, o jų santykis $s = 0.5$.



5 pav. Harmoninė (a) ir Ronči tipo (b) muaro gardelė. Diagramos kairėje iliustruoja vienmatės gardelės funkciją, dešinėje esančios diagramos rodo pilkos spalvos reikšmių pasiskirstymą vaizde [51].

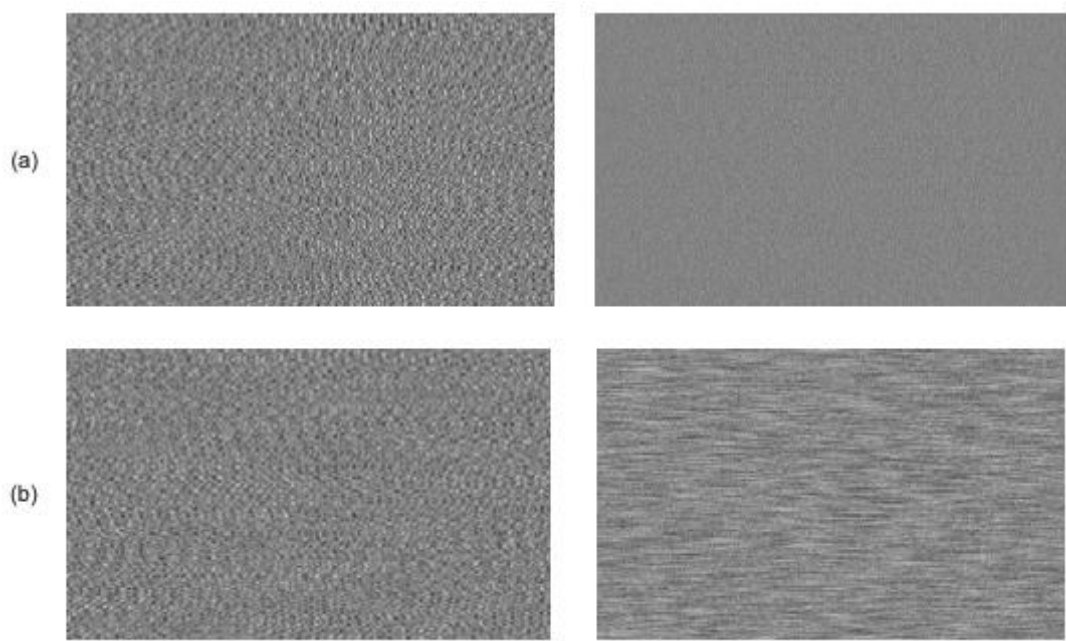
Ronči tipo, laiptuotą gardelę judinant trikampė forma („zig-zag“ tipo) pastebima, kad egzistuoja tokios parametro s reikšmės, prie kurių laike vidurkinto vaizdo funkcijos antras ir tolimesni Furjė eilutės nariai bus lygūs nuliui. Priešingai, tą pačią gardelę judinant harmoniškai, nerandamos tokios parametro s reikšmės, prie kurių liktų tik pirmasis eilutės narys ir laike vidurkintame vaizde nesusidarys laike vidurkintos juostos. Slapta informacija galės būti atkoduojama tik pritaikius trikampės formos svyravimus, tokiu būdu suteikiant didesnę saugumo lygį [51].

1.2.3.3. Stochastinė muaro gardelė

Šiame tyrime naudojama gardelė nėra nei harmoninė, nei Ronči tipo, tačiau yra atsitiktinės reikšmės turinti dvimatė gardelė, todėl yra vadinama atsitiktine arba stochastine gardele. Dinaminės vizualinės kriptografijos, naudojančios harmoninę gardelę principas yra pagrįstas Beselio funkcijų ir jų šaknų savybėmis, o stochastinei gardelei sudaryti ir įvertinti naudojamos naujos metodikos.

Algoritmas vaizdo užkodavimui ir atkodavimui naudojant stochastines muaro gardeles yra pristatytas [48]. Stochastinė muaro gardelė yra deformuojama pagal slapto vaizdo pilkos spalvos ryškumo reikšmės. Atkodavimas vykdomas naudojant slapto ir originalaus vaizdo taškų koreliaciją. [52] straipsnio autoriai taip pat pasiūlė beveik optimalią periodinę stochastinę muaro gardelę. Vienam gardelės periodui parenkamos optimalios spalvos, t.y. sukuriama optimalumo tikslo funkcija, kuri optimizuojama naudojant evoliucinius optimizavimo algoritmus.

2023 m. [44] straipsnyje buvo pristatyta DVK schema, leidžianti slėpti informaciją vienmatėse neperiodinėse stochastinėse muaro gardelėse. Skaitmeninių vaizdų reikšmių atsitiktinumui įvertinti siūloma naudoti Wada indeksą [44,53]. Siekiant slėpti informaciją stochastiniame vaizde, naudojant DVK, reikalingos dvi gardelės: viena – slaptos informacijos, kita – fono kodavimui. Pirmasis reikalavimas stochastinių gardelių panaudojimo schemai yra pradiniam vaizde paslėpti informaciją taip, kad ji nebūtų matoma plika akimi. Antrasis reikalavimas – slapta informacija turi tapti matoma laike vidurkintame vaizde, kai pradinis vaizdas svyruoja pagal iš anksto nustatytą virpesių amplitudę. Tokių gardelių sudarymui naudojamas Wada indeksas, kuris abejoms stacionarioms gardelėms turi būti beveik identiškas, o laike vidurkintoms gardelėms, kuo labiau skirtis [44]. Laikoma, kad dvimatį vaizdą sudaro 180 skirtingų vienmačių stochastinių gardelių, kurios judinamos horizontalia kryptimi ir į vaizdą sudedamos eilutėmis. **6 pav.** pavaizduoti du vaizdai, sudaryti iš stochastinių gardelių. Pirmojo vaizdo gardelės vidurkinamos taip, kad būtų kuo pilkesnės, o laike suvidurkinus antrojo vaizdo gardeles, gaunamas kuo margesnis vaizdas. Pusiausvyros būsenoje abu vaizdai turi būti kuo panašesni. Šių reikalavimų rezultatas matomas **6 pav.**, kur taip pat matoma virpėjimo (horizontali) kryptis [44].



6 pav. Pirmasis (a) ir antrasis (b) DVK schemas vaizdai, sudaryti iš 180 skirtingų beveik optimalių vienmačių muaro gardelių, sudėtų horizontaliai [44].

1.2.3.4. Gardelės svyravimai laike

Atkodavimas dinaminėje vizualinėje kriptografijoje yra pagrįstas muaro gardelių svyravimais, taip imituojuant vidurkinimo, „susiliejo“ efektą. Literatūroje daugiausia aprašyti tyrimai, kuriuose atliekami harmoniniai gardelės svyravimai, kurie gali būti vertikalūs [40, 62], horizontalūs [44] ar elipsiniai [50]. Vertikalūs ir horizontalūs harmoniniai svyravimai aprašomi harmonine funkcija:

$$u(t) = a \sin(\omega t + \varphi), \quad (9)$$

čia a yra harmoninių svyravimų amplitudė, ω – dažnis, o φ – fazė. Elipsiniai svyravimai atliekami naudojant dvi statmenai sudėtas muaro gardeles. Vidurkintų juostų formavimąsi aprašo nulinės eilės Beselio funkcijos. Taip pat [55] pademonstruota, kad galima naudoti atsitiktinius gardelės svyravimus, kurie remiasi Gauso procesu:

$$u(t) \sim N(0, \sigma^2). \quad (10)$$

Šiuo atveju, laike vidurkinto vaizdo spalvą moduliuoja nykstančioji eksponentinė funkcija $\exp(-\frac{1}{2}(\omega\sigma^2))$, čia σ yra atsitiktinumo standartinis nuokrypis, o ω – svyravimų dažnis [55]. Dar viena, jau minėta, gardelės svyravimo funkcija gali būti trikampė arba “zig-zag” tipo funkcija [51]. Laike vidurkinto vaizdo spalvą moduliuoja funkcija $\frac{\sin(\omega a)}{\omega a}$, kurios argumentai svyravimų dažnis ir amplitudė. [56] straipsnio autoriai atliko “stačiakampius” (*angl.* rectangular waveform) svyravimus dėl praktinio svyravimų realizavimo. Minėtame straipsnyje autoriai pademonstravo, kaip žmogus plika akimi gali atkoduoti vaizdą, kai vaizdo svyravimai atliekami pakankamai aukštu dažniu. Dėl tyrimui reikalingo aukšto dažnio, pasirinkta naudoti paprastesnė, t.y. “stačiakampių” svyravimo funkcija, kuri apibrėžiama taip:

$$u(t) = \begin{cases} -a, & \text{kai } t \in \left[-\frac{\pi}{2\omega}; 0\right]; \\ a, & \text{kai } t \in \left[0; \frac{\pi}{2\omega}\right]. \end{cases} \quad (11)$$

Tada laike vidurkinto vaizdo moduliuojančioji funkcija įgyja funkcijos $\frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} a\right)$ formą [56].

Šiame tyrime naudojamas metodas turi steganografijos požymių: slaptas vaizdas nėra skaidomas į dalis bei užkodavimui naudojama kompiuterinė technika. Nepaisant šių požymių, tyrimo metodas priskiriamas vizualinei kriptografijai, kadangi atkodavimas gali būti atliekamas pasitelkiant tik žmogaus regą. Metodas priskiriamas specifiškai DVK, kadangi slaptas vaizdas sudarytas tik iš vienos dalies. Literatūroje tokio tipo tyrimai priskiriami dinaminei vizualinei kriptografijai [30,44,56,57].

1.2.3.5. Dinaminės vizualinės kriptografijos taikymai

Vizualinė kriptografija yra pritaikoma daugelyje informatikos bei optikos inžinerijos mokslinių tyrimų sričių. Pirmiausia, vizualinė kriptografija yra pritaikoma informacijos slėpime [24], o tokios modifikacijos kaip DVK pritaikomos optikos kontrolės įrankiams, kurie gali būti naudojami įvairiuose su virpesiais susijusiuose pritaikymuose [45,58]. [45] straipsnio autoriai pristato DVK pritaikymą harmoninių virpesių sistemoms bei virpesių generavimo įrangai. Tačiau periodinis judėjimas pritaikomas netiesinėms sistemoms gali sukelti chaotinį atsaką. Tokios sistemos gali būti biologinės, cheminės ir techninės. Todėl [58] straipsnio autoriai atliko chaotinės dinaminės vizualinės kriptografijos tyrimą, kuris gali būti pritaikomas chaotinių virpesių kontrolei ar chaotinių procesų vertinimui.

DVK optikoje taip pat taikoma ir regos sistemos tyrimuose [56]. Kadangi DVK remiasi vaizdo laike vidurkinimo procesu, atliktas eksperimentas, kurio tikslas ištirti žmogaus regos sistemą, atliekančia laike vidurkinimą [56]. Šalia pritaikymų optikoje, DVK taip pat taikyta biomediciniui sistemų tyrimams [59]. DVK, paremta laike vidurkintomis muaro gardelėmis, kartu su Gerchberg-Saxton algoritmu ir trimatės mikrosandaros kūrimo metodika, panaudotos optinei schemai sukurti [59].

1.3. Išvados

Taigi, informacijos slėpimo tematikoje yra atlikta daug mokslinių tyrimų, plėtojama dinaminės vizualinės kriptografijos metodika. Dinaminėje vizualinėje kriptografijoje naudojamos harmoninės, Ronči tipo ar stochastinės muaro gardelės, kurios gali būti judinamos harmoniniais, stochastiniais ar kitokiais dėsniais.

Muaro gardelių metodika sėkmingai buvo pritaikyta informacijos slėpime. Vaizdo kodavimo metodika, paremta slapto vaizdo įterpimu geometriniame muare, aptarta [60]. Deja, pritaikius šį metodą, slapto vaizdo detalės yra matomos net plika akimi. Todėl patobulintas algoritmas vaizdo užkodavimui ir atkodavimui naudojant stochastines muaro gardeles yra pristatytas [48]. Čia autoriai slaptą informaciją slepia deformuodami stochastinę muaro gardelę pagal slapto vaizdo pilkos spalvos ryškumo reikšmes. Atkodavimas vykdomas naudojant slapto ir originalaus vaizdo taškų reikšmių koreliaciją.

2023 m. buvo pristatyta DVK schema, leidžianti slėpti informaciją vienmatėse neperiodinėse stochastinėse muaro gardelėse [44]. Tokia schema pasižymi didesniu atsparumu statistinės analizės algoritmams lyginant su DVK schemomis, pagrįstomis informacijos kodavimu periodinėse muaro gardelėse. Deja, slaptai informacijai užkoduoti bei atkoduoti šioje DVK schemoje įmanoma panaudoti tik horizontalios ar vertikalios krypties harmoninius virpesius. Įvairių krypčių harmoninių ar netgi elipsinių virpesių panaudojimas tokio tipo schemoje ne tik padidintų įterpiamos informacijos saugumą, bet ir išplėstų DVK taikymo galimybes. Todėl šio tyrimo pagrindinis tikslas yra pasiūlyti DVK schemą, pagrįstą neperiodinėmis stochastinėmis muaro gardelėmis ir skirtingų krypčių harmoniniais bei elipsiniais virpesiais. Šiam tikslui pasiekti bus naudojamos dvimatės stochastinės neperiodinės muaro gardelės.

2. Tyrimo metodai

Dinaminėje vizualinėje kriptografija galioja tam tikri vaizdų slėpimo principai. Pirmiausia, slapta informacija pradiname vaizde plika akimi neturi būti matoma. Antra, laike vidurkintame vaizde slapta informacija turi būti atskleidžiama, kai pradinis vaizdas yra judinamas iš anksto nustatyta tam tikra harmoninių svyravimų amplitudė. Gardelės reikalavimų atitikimas yra vertinamas vizualiai, Wada indekso bei standartinio nuokrypio reikšmėmis.

2.1. Wada indeksas gardelės vertinime

Skaitmeninių vaizdų taškų atsitiktinumui vertinti dažnai naudojama Šenono entropija (*angl.* Shannon entropy), dar vadinama informacijos entropija [61,62]. 2021 metais buvo pristatytas svorinės apdorotos Šenono entropijos panaudojimas Wada ribų nustatyme [53]. Šis matas buvo pavadintas Wada indeksu. Taip pat pasiūlyta Wada indeksą naudoti matuojant spalvų pasiskirstymą dvimatėje fazinėje plokštumoje. Tokia savybė buvo pritaikyta vaizdų analizėje nustatant skirtingus pilkumo lygius stacionarioje bei laike vidurkintoje gardelėje [44].

Norint apibrėžti dvimatį Wada indeksą, kuris naudojamas vaizdo kompleksiskumo nustatyme, pirmiausia, aprašomi naudojami žymėjimai [44]:

- s – stebėjimo lango ilgis taškais, kai $s \geq 2$. Tyrime tai yra dvimatis vaizdas.
- c – skirtingų pilkos spalvos intensyvumo reikšmių stebėjimo lange skaičius, $c \geq 1$.
- $v_k, k = 1, 2, \dots, c$ – k -tojo vaizdo taško pilkos spalvos intensyvumo reikšmė stebėjimo lange.
- $p_k = \frac{v_k}{s^2}, k = 1, 2, \dots, c$ – k -tojo vaizdo taško pilkos spalvos reikšmės tikimybė stebėjimo lange.
- $1_2^{(s)} = \begin{cases} 1, c \geq 2, \\ 0, c = 1 \end{cases}$ – indikatoriaus funkcija, kuri lygi 1, jeigu skirtingų pilkos spalvos intensyvumo reikšmių skaičius stebėjimo lange yra didesnis arba lygus 2.
- $1_3^{(s)} = \begin{cases} 1, c \geq 3, \\ 0, c \leq 2 \end{cases}$ – indikatoriaus funkcija $1_3^{(s)}$ lygi 1, jeigu skirtingų pilkos spalvos intensyvumo reikšmių skaičius stebėjimo lange yra didesnis arba lygus 3.
- Pilkos spalvos intensyvumo reikšmių Šenono entropija stebėjimo lange s :

$$e^{(s)}(p_1, p_2, \dots, p_c) = -\sum_{k=1}^c p_k \log(p_k). \quad (12)$$

Tada Wada indeksas $\omega_1^{(s)}$ stebėjimo lange s apibrėžiamas taip [63]:

$$\omega_1^{(s)}(p_1, p_2, \dots, p_c) = \frac{c}{\log(c)} 1_3^{(s)} e^{(s)} = \begin{cases} 0, c < 3, \\ -\frac{c}{\log(c)} \sum_{k=1}^c p_k \log(p_k), c \geq 3. \end{cases} \quad (13)$$

Jeigu laikome, kad N stebėjimo langų sudaro visą vaizdą, tada viso vaizdo Wada indeksas yra apibrėžiamas taip [53]:

$$W_1^{(s)} = \frac{\sum_{k=1}^N \omega_{1,k}^{(s)}}{\sum_{k=1}^N 1_{2,k}^{(s)}}, \quad (14)$$

čia $\omega_{1,k}^{(s)}$ ir $1_{2,k}^{(s)}$ atitinkamai yra Wada indeksas ir indikatoriaus funkcija k -tajame stebėjimo lange. Tolimesniuose tyrimuose didžiausia stacionarios gardelės $M_1(x)$ Wada indekso reikšmė visame stebėjimo lange bus žymima $\omega_{max}^{(1)}$ ir atitinkamai gardelės $M_2(x)$ didžiausia Wada indekso reikšmė žymima $\omega_{max}^{(2)}$, o šių laike vidurkintų gardelių atitinkamai didžiausios Wada indekso reikšmės žymimos $\bar{\omega}_{max}^{(1)}$ ir $\bar{\omega}_{max}^{(2)}$.

2.2. Reikalavimai stochastinėms gardelėms

Sudarant dvi stochastines gardeles $M_1(x, y)$ ir $M_2(x, y)$, turi būti tenkinami tam tikri reikalavimai, kad būtų gautos beveik identiškos statinės gardelės ir kuo labiau besiskiriančios laike vidurkintos gardelės. Šiam tikslui pasiekti, pirmąją $M_1(x, y)$, t.y. fono stacionarią gardelę siekiama sugeneruoti kuo magesnę, o tą pačią suvidurkintą gardelę – kuo pilkesnę. Reikalavimai pirmajai gardei $M_1(x, y)$ [44]:

1. Stacionariosios gardelės $M_1(x, y)$ standartinis nuokrypis turi būti kuo didesnis, taip užtikrinant plačiausią vaizdo taškų ryškumo diapazoną gardelėje.
2. Vidurkis ir standartinis nuokrypis visose $M_1(x, y)$ dalyse turėtų būti panašus, taip užtikrinant gardelės vientisumą.
3. Skirtumas tarp vaizdo taškų ryškumo suvidurkintoje gardelėje $\bar{M}_1(x, y, a)$ ir vidutinės vaizdo ryškumo reikšmės 127.5 turi būti kaip įmanoma mažesnis, taip užtikrinant, kad suvidurkintas vaizdas būtų kuo panašesnis į vientisą pilką vaizdą.

Gardelė $M_2(x, y)$, kuri bus naudojama slaptai informacijai užkoduoti, tiek stacionarioje, tiek vidurkintoje būsenoje siekiama gauti kuo magesnę. Be to stacionari gardelė $M_2(x, y)$ turėtų būti kuo panašesnė į gardelę $M_1(x, y)$, o laike vidurkinta gardelė $\bar{M}_2(x, y, a)$ turėtų kiek įmanoma daugiau skirtis nuo pirmosios gardelės $\bar{M}_1(x, y, a)$ [44]:

1. Stacionari gardelė $M_2(x, y)$ turi būti kuo panašesnė į $M_1(x, y)$ gardelę.
2. Stacionarios gardelės $M_2(x, y)$ vidurkis turi būti apytiksliai lygus $M_1(x, y)$ gardelės vidurkiui, kad slaptas vaizdas stacionariame užkoduotame vaizde nebūtų matomas.
3. Stacionarios gardelės $M_2(x, y)$ standartinis nuokrypis turi būti apytiksliai lygus $M_1(x, y)$ gardelės standartiniui nuokrypiui, taip pat dėl slaptos informacijos saugumo.
4. Stacionarios gardelės $M_2(x, y)$ Wada indeksas turi būti apytiksliai lygus $M_1(x, y)$ gardelės Wada indeksui. 2, 3 ir 4 reikalavimai užtikrina slaptos informacijos ir fono gardelių panašumą.
5. Laike vidurkintos gardelės $\bar{M}_2(x, y, a)$ standartinis nuokrypis turi būti kuo didesnis, kad laike vidurkintas vaizdas nebūtų visiškai pilkas, t.y., kad skirtųsi nuo $\bar{M}_1(x, y, a)$.
6. Kiekviename laike vidurkintos gardelės $\bar{M}_2(x, y, a)$ segmente vidurkis, standartinis nuokrypis ir Wada indeksas turėtų būti kuo panašesni. Šis reikalavimas užtikrina slapto vaizdo vientisumą vidurkintoje būsenoje.

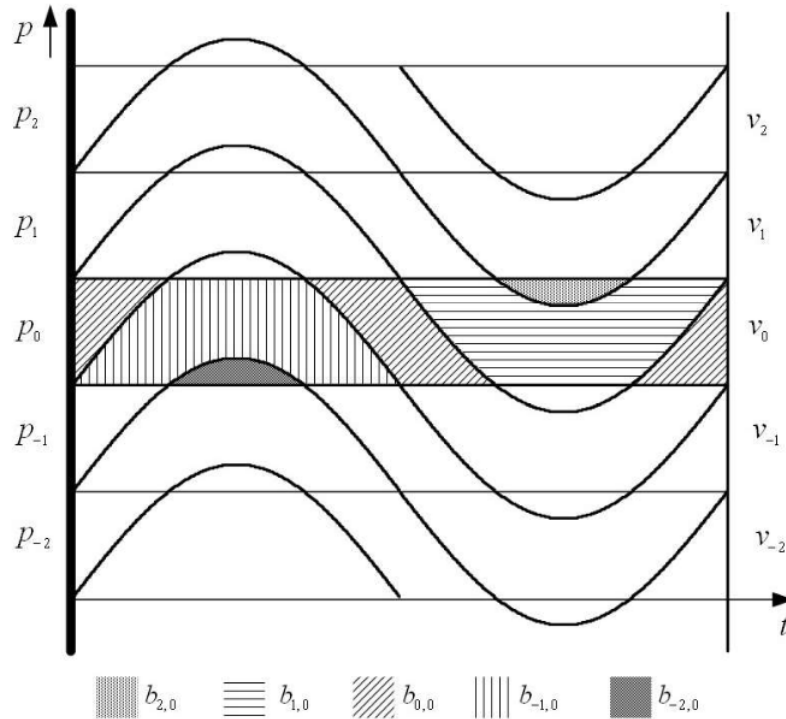
Informacijos slėpime slapta informacija bus koduojama naudojant pirmąją $M_1(x, y)$ gardelę, o fonas koduojamas naudojant antrąją $M_2(x, y)$ gardelę. Toliau tyrime slaptos informacijos gardelę vadinsime pirmąja gardele, o vaizdo fono gardelę – antrąja.

2.3. Laike vidurkinta gardelė

Kadangi tyrime nagrinėjama schema yra priskiriama dinaminei vizualinei kriptografija, tai vaizdo atkodavimą turi būti įmanoma atlikti plika akimi. Šiame tyrime slapta informacija yra atkoduojama laike vidurkinant stacionarų vaizdą. Tai gali būti atliekama tiesiog stebint plika akimi vaizdą, virpinamą pagal tam tikrus dėsnius, arba laike vidurkintą vaizdą generuoti kompiuterio pagalba (imituojant virpesių procesą). Atkreipiame dėmesį, kad šiame tyrime laike vidurkinta gardelė gaunama pasitelkiant skaitinius metodus.

Laikome, kad tyrime naudojami vaizdai su diskrečiomis taškų reikšmėmis. Kad būtų paprasčiau, pirmiausia tiriamo vienmatės vertikalios gardelės vidurkinimo procesą. Vaizdo pilkos spalvos intensyvumo reikšmės vienmatėje gardelėje pažymime $p_0, p_1, p_{-1}, p_2, p_{-2}$ ir t.t. Atitinkamai laike vidurkintos gardelės tų pačių taškų pilkos spalvos reikšmės žymimos $v_0, v_1, v_{-1}, v_2, v_{-2}$ ir t.t. [63]

Virpėjimo metu vienos gardelės i -tasis taškas juda svyravimo kryptimi p ašimi taip, kaip pavaizduota **7 pav.** Tada plotą, kurį užima i -tasis taškas j -tojo taško erdvėje pažymėsime b_{ij} . Kuo didesnė judėjimo amplitudė a , tuo taškas p_i pasiekia daugiau kaimyninių taškų. Jeigu amplitudė a yra lygi nuliui, tai sakome, kad vienmatė gardelė pusiausvyros būsenoje bus ta pati kaip ir laike vidurkinta gardelė: $p_i = v_i, i = 0, 1, -1, 2, -2, \dots$



7 pav. Vienmatės gardelės taškų judėjimas pagal harmoninę funkciją [63].

Tada laike vidurkintos gardelės j -tojo taško pilkos spalvos intensyvumas bus skaičiuojamas pagal kaimyninių taškų reikšmes ir j -tojo taško užimamus plotus juose, t.y. vieno taško pilkos spalvos intensyvumo reikšmė apibrėžiama svertine kitų taškų reikšmių suma:

$$v_j = \sum_{i=j-M}^{j+M} p_i b_{ij}, \quad -\infty < j < \infty, \quad (15)$$

čia v_i nurodo laike vidurkinto i -tojo taško pilkos spalvos intensyvumo reikšmę; p_i nurodo i -tojo taško pilkos spalvos intensyvumo reikšmę pusiausvyros būsenoje; b_{ij} yra svertinis koeficientas, rodantis i -tojo taško užimamą normalizuotą plotą j -tojo taško vietoje. Kuo kaimyniniame taške pagrindinis taškas praleidžia daugiau laiko, tuo svertinis koeficientas yra didesnis. M nurodo aplankomų

kaimyninių taškų kiekį per pusę bangos ilgio (per vieną bangos ilgį vienas taškas aplanko $2M$ vaizdo taškus).

Diskrečiuoju atveju laike vidurkintam vaizdui V pilkos spalvos intensyvumo reikšmės bus apskaičiuojamos taip:

$$V = B \cdot P, \quad (15)$$

čia

$$V = \begin{pmatrix} \dots \\ v_2 \\ v_1 \\ v_0 \\ v_{-1} \\ v_{-2} \\ \dots \end{pmatrix}, B = \begin{pmatrix} \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & b_{2,2} & b_{1,2} & b_{0,2} & b_{-1,2} & b_{-2,2} & \dots \\ \dots & b_{2,1} & b_{1,1} & b_{0,1} & b_{-1,1} & b_{-2,1} & \dots \\ \dots & b_{2,0} & b_{1,0} & b_{0,0} & b_{-1,0} & b_{-2,0} & \dots \\ \dots & b_{2,-1} & b_{1,-1} & b_{0,-1} & b_{-1,-1} & b_{-2,-1} & \dots \\ \dots & b_{2,-2} & b_{1,-2} & b_{0,-2} & b_{-1,-2} & b_{-2,-2} & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix}, P = \begin{pmatrix} \dots \\ p_2 \\ p_1 \\ p_0 \\ p_{-1} \\ p_{-2} \\ \dots \end{pmatrix} \quad (16)$$

Matricos B koeficientai gali būti suskaičiuojami analitiniu arba skaitmeniniu būdu. Svariai b_{ij} bus lygūs nuliui kiekvienam j tada, kai $i < j - M$ arba $i > j + M$. Tada kiekviename taške i vektorius $(b_{i+M,i} \dots b_{i+1,i} b_{i,i} b_{i-1,i} \dots b_{i-M,i})$ įgis tas pačias reikšmes. Šį vektorių pažymime B^* ir jį laikysime vidurkinimo laike transformacijos operatoriumi. Toliau taško i reikšmę laikysime lygią nuliui, kadangi kiekviename taške B^* reikšmės vienodos:

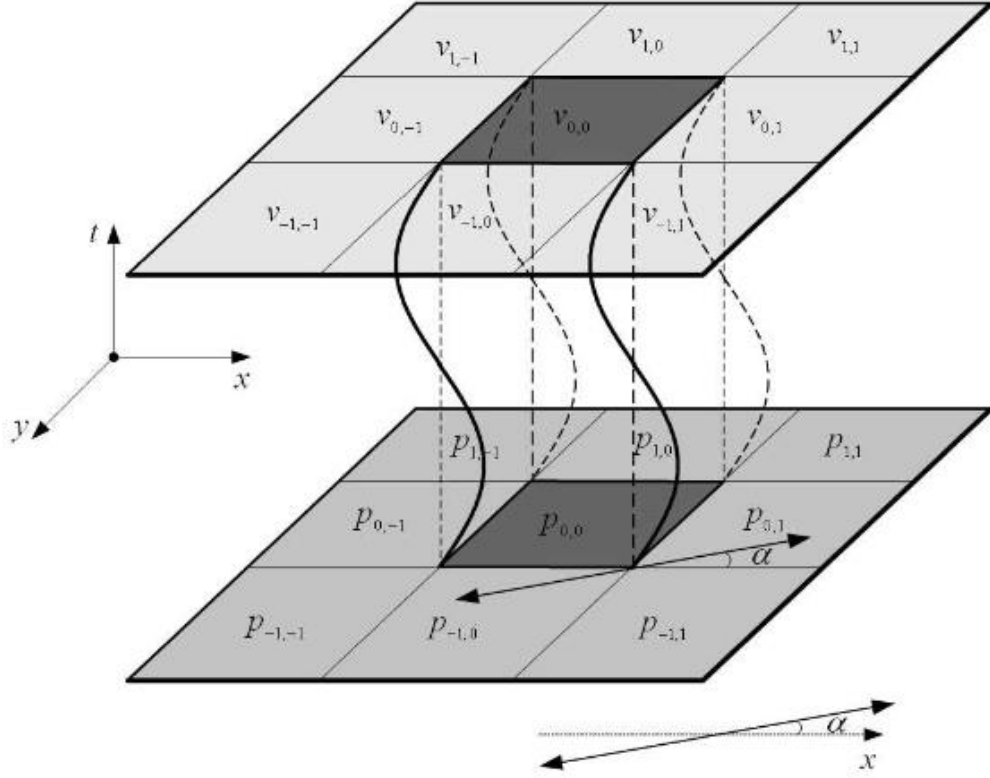
$$B^* = (b_{M,0} \dots b_{1,0} b_{0,0} b_{-1,0} \dots b_{-M,0}). \quad (17)$$

Analogiškai vienmačiu atveju atlikti skaičiavimai gali būti pritaikyti dvimatėms gardelėms.

Taigi, siekiant nustatyti vaizdo taškų pilkos spalvos intensyvumo reikšmes laike vidurkintam vaizdui, kuris yra judinamas harmoniškai, yra pritaikoma ta pati vidurkinimo metodika. Judėjimo kryptis x ašimi yra žymima raide α , kaip parodyta **8 pav.** Tada spalvos intensyvumo reikšmės statiniame vaizde P ir laike vidurkintame vaizde V bus apibrėžiamos matricomis [63]:

$$P = \begin{pmatrix} \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & p_{2,2} & p_{2,1} & p_{2,0} & p_{2,-1} & p_{2,-2} & \dots \\ \dots & p_{1,2} & p_{1,1} & p_{1,0} & p_{1,-1} & p_{1,-2} & \dots \\ \dots & p_{0,2} & p_{0,1} & p_{0,0} & p_{0,-1} & p_{0,-2} & \dots \\ \dots & p_{-1,2} & p_{-1,1} & p_{-1,0} & p_{-1,-1} & p_{-1,-2} & \dots \\ \dots & p_{-2,2} & p_{-2,1} & p_{-2,0} & p_{-2,-1} & p_{-2,-2} & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix}, \quad (18)$$

$$V = \begin{pmatrix} \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & v_{2,2} & v_{2,1} & v_{2,0} & v_{2,-1} & v_{2,-2} & \dots \\ \dots & v_{1,2} & v_{1,1} & v_{1,0} & v_{1,-1} & v_{1,-2} & \dots \\ \dots & v_{0,2} & v_{0,1} & v_{0,0} & v_{0,-1} & v_{0,-2} & \dots \\ \dots & v_{-1,2} & v_{-1,1} & v_{-1,0} & v_{-1,-1} & v_{-1,-2} & \dots \\ \dots & v_{-2,2} & v_{-2,1} & v_{-2,0} & v_{-2,-1} & v_{-2,-2} & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix}$$



8 pav. Dvimačio vaizdo harmoninio judėjimo vieną periodą schemą.

Kaip pavaizduota **8 pav.**, kiekvienas vaizdo taškas keliauja kryptimi α tokiu būdu aplankydamas kaimyninius taškus. Jeigu laikome, kad judėjimo metu (i,j) -tasis taškas užima (k,l) -tają vietą, tada užimamas plotas žymimas $b_{i,j;k,l}$. Spalvos intensyvumo reikšmės (i,j) -tajame vidurkinamo vaizdo taške bus lygios jo kaimyninių taškų spalvų intensyvumo reikšmių statiniame vaizde svertinei sumai:

$$v_{i,j} = \sum_{k=i-M}^{i+M} \sum_{l=j-M}^{j+M} p_{k,l} \cdot b_{k,l;i,j}, \quad -\infty < i, j < \infty, \quad (19)$$

Čia $v_{i,j}$ – laike vidurkinto (i,j) -tojo vaizdo taško spalvos intensyvumas; $p_{i,j}$ – statinio vaizdo (i,j) -tojo taško spalvos intensyvumas; $b_{k,l;i,j}$ – svertinis koeficientas, kuris gali būti randamas analitiškai arba skaitiniu būdu. Kiekvienam taškui i ir j svarių matrica

$$\begin{pmatrix} b_{i+M,j+M;i,j} & \dots & b_{i+M,j;i,j} & \dots & b_{i+M,j-M;i,j} \\ \dots & \dots & \dots & \dots & \dots \\ b_{i,j+M;i,j} & \dots & b_{i,j;i,j} & \dots & b_{i,j-M;i,j} \\ \dots & \dots & \dots & \dots & \dots \\ b_{i-M,j+M;i,j} & \dots & b_{i-M,j;i,j} & \dots & b_{i-M,j-M;i,j} \end{pmatrix} \quad (20)$$

bus ta pati.

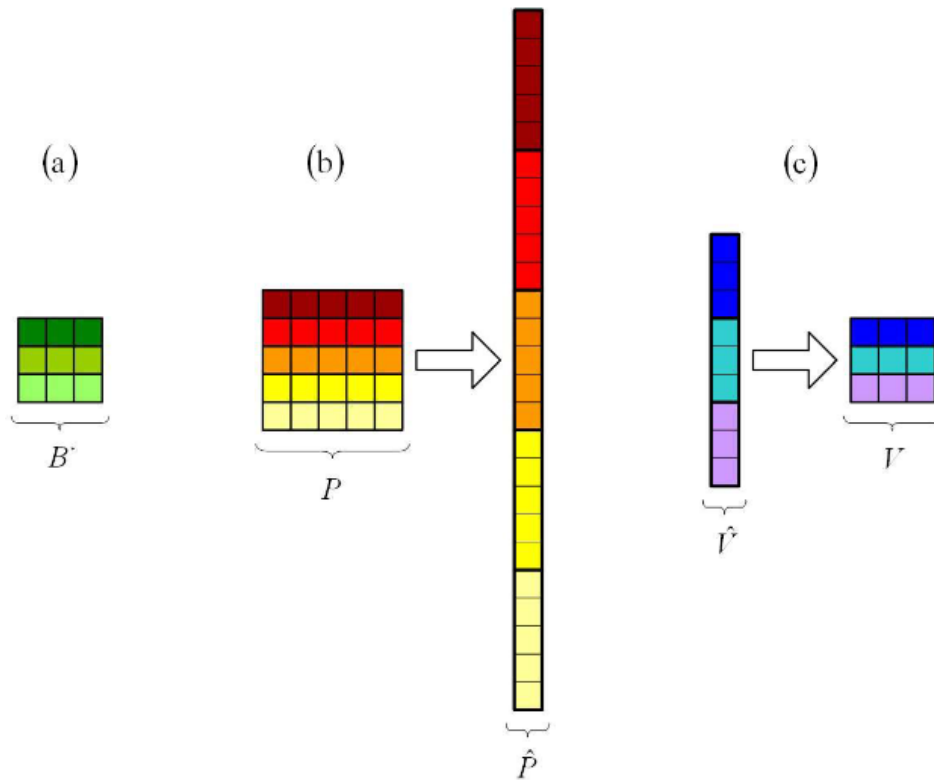
Šią matricą pažymime B^* ir ją laikysime vidurkinimo laike transformacijos operatoriumi dvimačiu atveju. Toliau taško i ir j reikšmes laikysime lygias nuliui, kadangi kiekviename taške B^* reikšmės vienodos:

$$B^* = \begin{pmatrix} b_{M,M;0,0} & \dots & b_{M,0;0,0} & \dots & b_{M,-M;0,0} \\ \dots & \dots & \dots & \dots & \dots \\ b_{0,M;0,0} & \dots & b_{0,0;0,0} & \dots & b_{0,-M;0,0} \\ \dots & \dots & \dots & \dots & \dots \\ b_{-M,M;0,0} & \dots & b_{-M,0;0,0} & \dots & b_{-M,-M;0,0} \end{pmatrix}. \quad (21)$$

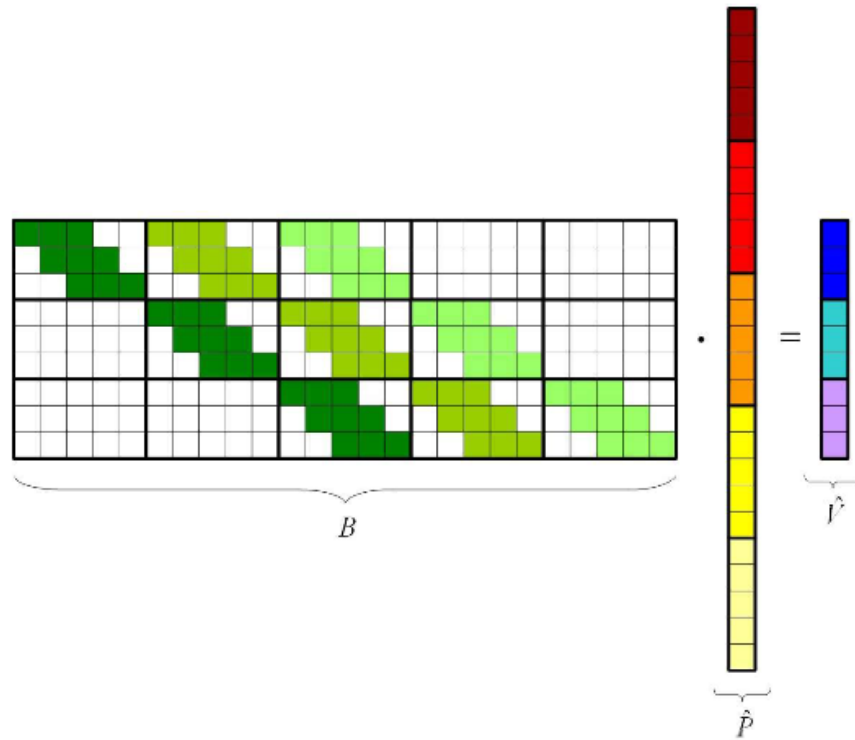
Tada laike vidurkinto vaizdo spalvų intensyvumo reikšmės V bus apskaičiuojamos taip:

$$\hat{V} = B \cdot \hat{P}, \quad (21)$$

Čia $\hat{P}$ ir $\hat{V}$ yra vektoriai, kurie gaunami matricų P ir V eilutes sudėjus į stulpelį, kaip pavaizduota **9 pav.** Tada iš transformacijos matricos B^* sudaroma matrica B taip, kaip pavaizduota **10 pav.**



9 pav. Matricų vertimo į vektorius schema. Paveikslai (a) ir (b) grafiškai vaizduoja, kaip iš matricos gaunamas vektorius ir atvirkščiai [63].



10 pav. Vaizdo taškų spalvos intensyvumo reikšmių skaičiavimo formulės $B \cdot \hat{P} = \hat{V}$ grafinė interpretacija [63].

Taigi, tyrime laike vidurkintas vaizdas yra gaunamas remiantis aprašyta schema, kai sukurama transformacijos operatoriaus matrica su svoriniais koeficientais kaimyniniams vaizdo taškams. Tada stacionarusis vaizdas yra padauginamas iš sudarytos transformacijos matricos ir tokiu būdu gaunamas suvidurkintas vaizdas.

2.4. Tikslų funkcijos F_1 sudarymas

Tarkime, kad erdvės koordinatės x, y yra apribotos intervale $0 \leq x, y \leq L$. Tada, darome prielaidą, kad stebėjimo langas apima $n \times n$ vaizdo taškų ir koordinatės $(x_i; y_j)$ ($1 \leq i, j \leq n$) yra $(i; j)$ -tojo taško centras. Skaidome stebėjimo langą į tokius $q \times q$ segmentus (segmentai tarsi atitinka vaizdo „langelius“), kad kiekvienas segmentas apimtų $d \times d$ vaizdo taškų ($q^2 d^2 = n^2$).

Tikslų funkcijos $F_1(M_1)$ formulė, skirta gauti stochastinę gardelę $M_1(x, y)$, atitinkančią aukščiau aprašytus reikalavimus, yra tokia:

$$F_1(M_1) = k_1 \left(\frac{127.5}{\sigma^{(1)}} - 1 \right) + k_2 \sqrt{\frac{1}{q^2} \sum_{i=1}^q \sum_{j=1}^q (m^{(1,i,j)} - m^{(1)})^2} + k_3 \sqrt{\frac{1}{q^2} \sum_{i=1}^q \sum_{j=1}^q \left(\sigma^{(1,i,j)} - \frac{1}{q^2} \sum_{k=1}^q \sum_{l=1}^q \sigma^{(1,k,l)} \right)^2} + \bar{\mu}_4^{(1)}, \quad (22)$$

čia k_1, k_2, k_3 yra realūs teigiami svoriniai koeficientai. Kuo didesnis vaizdo $M_1(x, y)$ standartinis nuokrypis pusiausvyros būsenoje, tuo mažesnė $\frac{127.5}{\sigma^{(1)}} - 1$ reikšmė, kadangi didžiausia įmanoma standartinio nuokrypio reikšmė yra 127.5 (kai pusė vaizdo taškų yra juodos, o kita pusė – baltos spalvos), čia $\sigma^{(1)}$ yra vaizdo $M_1(x, y)$ ryškumo standartinis nuokrypis visame stebimame intervale, apibrėžiamas taip:

$$\sigma^{(1)} = \sqrt{\frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n (M_1(x_i, y_j) - m^{(1)})^2}. \quad (23)$$

Formulės (22) dalys $\sqrt{\frac{1}{q^2} \sum_{i=1}^q \sum_{j=1}^q (m^{(1,i,j)} - m^{(1)})^2}$ ir $\sqrt{\frac{1}{q^2} \sum_{i=1}^q \sum_{j=1}^q \left(\sigma^{(1,i,j)} - \frac{1}{q^2} \sum_{k=1}^q \sum_{l=1}^q \sigma^{(1,k,l)} \right)^2}$ artėja prie nulio, kai ryškumo vidurkis ir standartinis nuokrypis visose dalyse yra apytiksliai toks pat; čia $m^{(1)}$ yra muaro gardelės $M_1(x, y)$ vidutinis ryškumas visame stebėjimo intervale ir apibrėžiamas taip:

$$m^{(1)} = \frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n M_1(x_i, y_j), \quad (24)$$

o parametrai $m^{(1,i,j)} = \frac{1}{d^2} \sum_{k=1}^d \sum_{l=1}^d M_1(x_{(i-1)d+k}, y_{(j-1)d+l})$ ir $\sigma^{(1,i,j)} = \sqrt{\frac{1}{d^2} \sum_{k=1}^d \sum_{l=1}^d (M_1(x_{(i-1)d+k}, y_{(j-1)d+l}) - m^{(1,i,j)})^2}$ atitinkamai žymi ryškumo vidurkį ir standartinį nuokrypį (i, j) -tajame segmente. $\bar{\mu}_4^{(1)}$ bus tuo artimesnis 0, kuo laike vidurkinta gardelė $\bar{M}_1(x)$ bus pilkesnė (visų vaizdo taškų ryškumas yra arti 127.5 reikšmės):

$$\bar{\mu}_4^{(1)} = \frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n \left(\bar{M}_1(x_i, y_j, a) - \bar{m}^{(1)} \right)^4. \quad (25)$$

čia 4-asis laipsnis reikalingas tam, kad išvengtume didelių svyravimų nuo 127.5 reikšmės. Laike vidurkintos gardelės parametrai (vidutinis ryškumas bei ryškumo standartinis nuokrypis visame stebėjimo intervale) skaičiuojami taip pat kaip ir stacionarios gardelės parametrai:

$$\bar{m}^{(1)} = \frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n \bar{M}_1(x_i, y_j, a), \quad (26)$$

$$\bar{\sigma}^{(1)} = \sqrt{\frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n (\bar{M}_1(x_i, y_j, a) - \bar{m}^{(1)})^2}. \quad (27)$$

Laike vidurkintos gardelės $\bar{M}_1(x, y, a)$ vidurkis ir standartinis nuokrypis i -tajame segmente taip pat apibrėžiami kaip ir stacionariai gardelei: $\bar{m}^{(1,i,j)} = \frac{1}{d^2} \sum_{k=1}^d \sum_{l=1}^d \bar{M}_1(x_{(i-1)d+k}, y_{(j-1)d+l}, a)$ ir $\bar{\sigma}^{(1,i,j)} = \sqrt{\frac{1}{n^2} \sum_{k=1}^d \sum_{l=1}^d (\bar{M}_1(x_{(i-1)d+k}, y_{(j-1)d+l}, a) - \bar{m}^{(1,i,j)})^2}$.

2.5. Tikslų funkcijos F_2 sudarymas

Antrosios stacionarios gardelės $M_2(x, y)$ charakteristikos atitinkamai žymimos $m^{(2)}$, $m^{(2,i,j)}$, $\sigma^{(2)}$, $\sigma^{(2,i,j)}$, o laike vidurkintos gardelės $\bar{M}_2(x, y, a)$ charakteristikos žymimos $\bar{m}^{(2)}$, $\bar{m}^{(2,i,j)}$, $\bar{\sigma}^{(2)}$, $\bar{\sigma}^{(2,i,j)}$, $\bar{\mu}_4^{(2)}$, kurios analogiškai apibrėžiamos pagal (23)-(27) formules.

Remiantis gardelės sudarymo reikalavimais, aprašytais 2.2 skyrelyje, antroji stacionari gardelė $M_2(x)$ turėtų būti kuo panašesnė į pirmąją stacionariąją gardelę $M_1(x, y)$. Todėl tyrime antroji gardelė sudaroma dviem būdais: su *Matlab* atsitikinių dydžių generavimo funkcija *randn()* naudojant pirmosios gardelės standartinio nuokrypio ir vidurkio reikšmes, bei antrąją gardelę apibrėžiant kaip pirmąją gardelę su tam tikra nuokrypių matrica ε [44]:

$$M_2(x, y) = M_1(x, y) + \varepsilon \quad (28)$$

ir sudarant tikslo funkciją. $F_2(M_1, \varepsilon)$, kuri apibrėžiama taip:

$$\begin{aligned} F_2(M_1, \varepsilon) = & \frac{1}{n^2} \sqrt{\sum_{i=1}^n \sum_{j=1}^n |\varepsilon_{ij}|} + |m^{(1)} - m^{(2)}| + |\sigma^{(1)} - \sigma^{(2)}| + |\omega_{max}^{(1)} - \\ & \omega_{max}^{(2)}| + \frac{k_1}{\bar{\sigma}^{(2)}} + k_2 \sqrt{\frac{1}{q^2} \sum_{i=1}^q \sum_{j=1}^q \left(\bar{m}^{(2,i,j)} - \bar{m}^{(2)} \right)^2} + \\ & k_3 \sqrt{\frac{1}{q^2} \sum_{i=1}^q \sum_{j=1}^q \left(\bar{\sigma}^{(2,i,j)} - \frac{1}{q^2} \sum_{k=1}^q \sum_{l=1}^q \bar{\sigma}^{(2,k,l)} \right)^2} + \\ & k_4 \sqrt{\frac{1}{q^2} \sum_{i=1}^q \sum_{j=1}^q \left(\bar{\omega}_{max}^{(2,i,j)} - \frac{1}{q^2} \sum_{k=1}^q \sum_{l=1}^q \bar{\omega}_{max}^{(2,k,l)} \right)^2}, \end{aligned} \quad (29)$$

čia k_1, k_2, k_3, k_4 yra realūs teigiami svoriniai koeficientai. Kuo mažesnės nuokrypių matricos ε reikšmės tikslo funkcijoje, tuo mažesnė funkcijos nario $\frac{1}{n^2} \sqrt{\sum_{i=1}^n \sum_{j=1}^n |\varepsilon_{ij}|}$ reikšmė. Narių $|m^{(1)} - m^{(2)}|, |\sigma^{(1)} - \sigma^{(2)}|$ ir $|\omega_{max}^{(1)} - \omega_{max}^{(2)}|$ reikšmės artėja prie nulio, kai abiejų $M_1(x, y)$ ir $M_2(x, y)$ gardelių vidurkiai, standartiniai nuokrypiai ir Wada indeksai tampa panašūs. Laike vidurkintos gardelės $\bar{M}_2(x, y)$ margumas bus tuo didesnis, kuo standartinis nuokrypis $\bar{\sigma}^{(2)}$ bus aukštesnis. Analogiškai, nario $\frac{1}{\bar{\sigma}^{(2)}}$ reikšmė bus mažesnė.

Funkcijos nariai $\sqrt{\frac{1}{q^2} \sum_{i=1}^q \sum_{j=1}^q \left(\bar{m}^{(2,i,j)} - \bar{m}^{(2)} \right)^2}, \sqrt{\frac{1}{q^2} \sum_{i=1}^q \sum_{j=1}^q \left(\bar{\sigma}^{(2,i,j)} - \frac{1}{q^2} \sum_{k=1}^q \sum_{l=1}^q \bar{\sigma}^{(2,k,l)} \right)^2},$
 $\sqrt{\frac{1}{q^2} \sum_{i=1}^q \sum_{j=1}^q \left(\bar{\omega}_{max}^{(2,i,j)} - \frac{1}{q^2} \sum_{k=1}^q \sum_{l=1}^q \bar{\omega}_{max}^{(2,k,l)} \right)^2}$ artės prie nulio, kai vidutinis ryškumas, standartinis nuokrypis ir didžiausia Wada indekso reikšmė visuose laike vidurkinto vaizdo $\bar{M}_2(x, y)$ segmentuose bus kuo panašesnės.

Kadangi antrasis vaizdas yra pirmojo vaizdo optimizavimo rezultatas, tai parenkamos specifinės korekcijų ε ribos. Įprastai vaizdo taškai gali įgauti reikšmes nuo 0 iki 255. Tyrime antrasis vaizdas optimizuojamas koreguojant pirmąjį, todėl optimizavimo procese sprendinių ribos nebus nuo 0 iki 255, tačiau esamos pirmojo vaizdo reikšmės bus koreguojamos, t.y. mažinamos arba didinamos pagal nurodytą tikslo funkciją. Pavyzdžiui, korekcijos gali būti atliekamos $[-50; 50]$ intervale, tai reiškia, kad norint gauti antrojo vaizdo taškų reikšmes, pirmojo vaizdo taškų reikšmės bus didinamos ir mažinamos iki 50 vienetų.

2.6. Stochastinės gardelės optimizavimas

Sugeneruoti du stochastinius vaizdus, kurie pusiausvyros būsenoje būtų panašūs, o, suvidurkinus laike, akivaizdžiai skirtingi, nėra paprasta. Šiame tyrime tikslo funkcijų optimizavimui pasirinkta naudoti dalelių spiečiaus optimizavimo algoritmą (*angl.* particle swarm optimization, PSO) dėl greito konvergavimo savybės [64]. Dalelių spiečiaus optimizavimo algoritmas yra populiacija paremtas evoliucinis optimizavimo metodas sukurtas remiantis socialiniu paukščių ir žuvų elgesiu. Algoritmą 1995 metais pasiūlė J. Kennedy ir R. Eberhart [65,66]. Nuo to laiko pristatyta nemažai skirtingų PSO algoritmo modifikacijų ir patobulinimų [67].

PSO algoritme dalelių populiacija keliauja per kelių matavimų paieškos erdvę ir ieško optimalių sprendinių optimizavimo uždaviniui. Kiekviena dalelė yra potencialus sprendinys. Kiekvienoje iteracijoje dalelės keičia savo pozicijas remdamasi asmenine patirtimi bei bendromis spiečiaus žiniomis. Tokiu būdu dalelės suranda vis geresnius tikslo funkcijos sprendinius.

Jau 1998 metais pasiūlyta prie originalaus PSO algoritmo mechanizmo pridėti dar vieną parametą – inercijos svorinį koeficientą [68]. M. Clerc pasiūlė PSO algoritmo modifikaciją siekiant pagerinti algoritmo konvergavimą ir stabilumą [69], t.y. sukurtas ribojimo faktorius (*angl.* constriction factor), kuris užtikrina, kad dalelės greitis yra apribotas. Tokiu būdu, algoritmas apsisaugo nuo nesuvaldomų svyravimų. Būtent [44] straipsnyje vaizdų optimizavime dinaminėje vizualinėje kriptografijoje naudojamas dalelių spiečiaus optimizavimo algoritmas su ribojimu (*angl.* Constricted PSO), todėl ir šiame tyrime pasirinkta naudoti PSO su ribojimu.

Informacija apie dalelę i saugojama vektoriuose $P_i, Lger_i$ ir V_i , kurie atitinkamai žymi dalelės esamą poziciją, buvusią geriausią poziciją (lokaliai geriausia pozicijos reikšmė) ir esamą greitį. Vektorius $Gger$ nurodo geriausios dalelės poziciją (globaliai geriausia pozicijos reikšmė). Kiekvienoje j -tojoje iteracijoje, dalelė i atnaujinama savo poziciją ir greitį pagal šias formules:

$$V_{ij} = \chi \left(V_{ij} + c_1 * r_{1j} * (Lger_{ij} - P_{ij}) + c_2 * r_{2j} * (Gger_j - P_{ij}) \right), j=1,2,\dots \quad (30)$$

$$P_{ij} = P_{ij} + V_{ij},$$

čia c_1 ir c_2 yra pažintinio ir socialinio mokymosi faktoriai, koeficientas c_1 traukia dalelę link pozicijos, kurioje yra geriausia tikslo funkcijos reikšmė, o per tą laiką koeficientas c_2 stumia dalelę link dalelės su turimu geriausiu rezultatu; r_1 ir r_2 – nepriklausomi, tolygiai pasiskirstę atsitiktiniai skaičiai (0,1) intervale; $Lger_{ij}$ – geriausias lokalus sprendinys, $Gger_t$ – geriausias globalus sprendinys, o ribojimo koeficientas $\chi = \frac{2\kappa}{|2-c-\sqrt{c^2-4c}|}$; $c_1 + c_2 > 4, 0 < \kappa \leq 1$, čia κ parametras kontroliuoja spiečiaus gebėjimą tyrinėti ir išnaudoti erdvę (*angl.* exploration and exploitation). Jeigu κ yra arti nulio, tai konvergavimas vyksta greičiau ir geriausias sprendinys ieškomas pagal turimą informaciją, vykdomas lokalus išnaudojimas. Kai parametras κ yra arti 1, tada vyksta lėtas konvergavimas, tačiau atliekamas erdvės tyrinėjimas, bandomi ne tik jau žinomi, bet ir nauji potencialių sprendinių variantai [67]. Kai parametrai c_1 ir c_2 suma $c = 4.1$, konvergavimas yra greitas ir užtikrintas [44,67]. Tada parametrai c_1 ir c_2 laikomi lygiais ($c_1 = c_2 = 2.05$) [44,67]. Šiame tyrime parametras κ parenkamas eksperimentiškai. Atsižvelgiant į algoritmo darbo greitį ir tikslumą visi pateikti rezultatai gaunami naudojant $\kappa = 0.8$, tad ribojimo koeficientas $\chi \approx 0.5839$.

Kiekvienoje iteracijoje dalelės pagal (30) formules atnaujinama savo greičius ir pozicijas. Greitis yra atnaujinamas pagal ribojimo koeficientą, kuris leidžia dalelėms išlaikyti jų kryptį, kognityvinę komponentę, kuri nukreipia daleles link jų asmeninio geriausio rezultato ir socialinę komponentę, kuri pakreipia daleles link globalaus geriausio rezultato. Dalelių spiečiaus optimizavimo algoritmas yra žinomas dėl savo efektyvumo bei gebėjimo surasti beveik optimalius sprendinius skirtinguose optimizavimo uždaviniuose. Šis algoritmas turi geras konvergavimo savybes, todėl pasirinktas naudoti stochastinių gardelių sudaryme [44].

Visi skaičiavimai atliekami programine įranga *Matlab*, kur taip pat gaunami ir skaitiniai bei grafiniai rezultatai. Programavimo kalba ir interaktyvi aplinka *Matlab* yra naudojama įvairiose srityse: vaizdų ir signalų apdorojime, kontrolinėse sistemose, finansų modeliavime ir t.t. [69]. Pastaraisiais metais *Matlab* pagrindiniai patobulinimai atlikti skaičiavimo aplinkoje, įskaitant ir patobulinius objektų ir grafinėse sistemose, lygiagrečių skaičiavimų palaikyme [56]. Ši programinė įranga turi intuityvią sintaksę, interaktyvią aplinką, platų dokumentacijų pasirinkimą, plačią įrangos naudojimo bendruomenę, todėl vartotojui yra patogi naudojimui. Taip pat tyrime naudojami *Matlab* esantys lygiagretūs skaičiavimai siekiant taupyti laiko resursus ieškant geriausių sprendinių. Tyrime naudojamos didelės matricos, kurios vizualizuojamos grafiškai, o *Matlab* padeda tai padaryti, kadangi turi galingas vizualizavimo galimybes.

Tyrimo eiga:

1. Pasirenkami šie parametrai: amplitudės dydis, svyravimų kryptis, vaizdo dydis.
2. Skaičiuojama transformacijos matrica B^* ir vidurkinimo matrica B .
3. Pasirenkamos optimizavimo algoritmo parametrų reikšmės. Tada vykdomas pirmosios gardelės tikslo funkcijos F_1 , aprašytos 2.4 skyrelyje optimizavimas (ieškomas minimumas) naudojant 2.6 skyrelyje aprašytą dalelių spiečiaus optimizavimo algoritmą su apribojimu. Taip gaunama pirmoji stacionarioji gardelė M_1 .
4. Skaičiuojama pirmoji laike vidurkinta gardelė $\overline{M}_1$ (optimizavimo metu gautas geriausias sprendinys (stacionari gardelė) dauginamas iš vidurkinimo matricos B).
5. Antroji stacionarioji gardelė skaičiuojama dviem būdais:
 - a. Vykdomas antrosios gardelės tikslo funkcijos F_2 , aprašytos 2.5 skyrelyje, optimizavimas (ieškomas minimumas) naudojant 2.6 skyrelyje aprašytą dalelių spiečiaus optimizavimo algoritmą su apribojimu bei pirmąją gardelę M_1 . Tada antroji stacionarioji gardelė M_2 skaičiuojama taip: prie pirmosios gardelės pridedamas optimizuotas sprendinys.
 - b. Kuriama gardelė iš atsitiktinai sugeneruotų reikšmių, panaudojant pirmosios gardelės standartinio nuokrypio ir vidurkio reikšmes (funkcija *randn()*).
6. Skaičiuojama antroji laike vidurkinta gardelė $\overline{M}_2$ (antroji stacionarioji gardelė M_2 dauginama iš vidurkinimo matricos B).
7. Kiekvienai stacionariai ir laike vidurkintai gardelei skaičiuojamas Wada indeksas.
8. Grafiškai pavaizduojami gauti rezultatai.

3. Tyrimų rezultatai ir jų aptarimas

Šio tyrimo ypatumas yra dvimatė gardelė. Iki šiol dinaminėje vizualinėje kriptografijoje buvo naudojamos vienmatės gardelės, kurios galėjo būti sudedamos į dvimatį vaizdą. Šiame tyrime naudojamos stochastinės dvimatės gardelės, dėl to galime analizuoti naujus virpesių dėsnius tam tikru kampu, ar elipsinius virpesius.

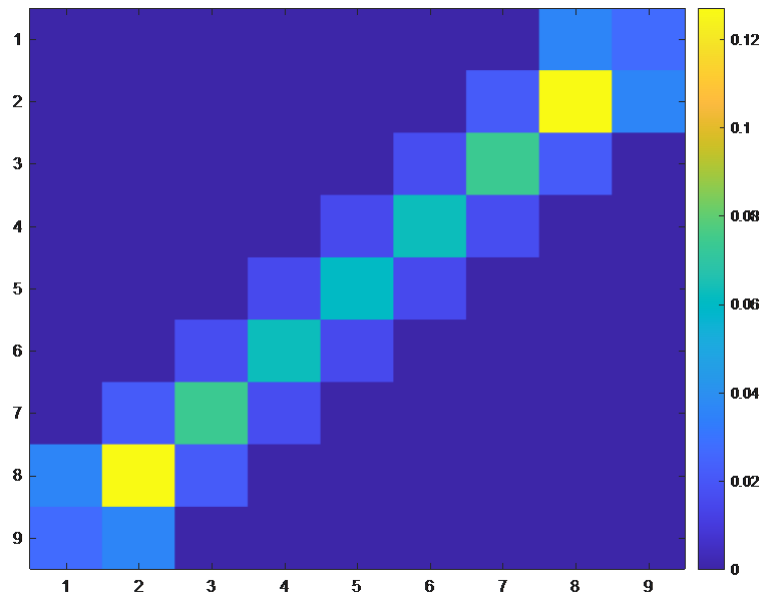
3.1. Pirmojo optimalaus vaizdo sudarymas

Pirmiausia, siekiama sugeneruoti pirmąjį vaizdą taip, kad stacionari dvimatė gardelė M_1 būtų kuo margesnė, o laike vidurkinta dvimatė gardelė $\overline{M_1}$ kuo pilkesnė. Tyrime vaizdas judinamas dvejais būdais: harmoniniais ir elipsiniais virpesiais.

3.1.1. Harmoninis svyravimas kampu

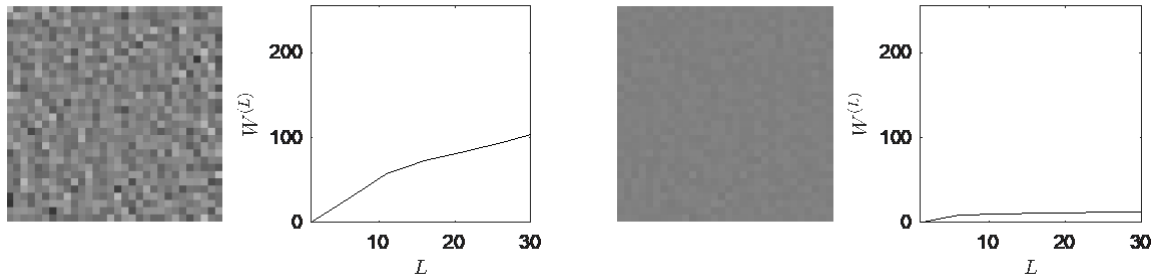
Pirmąją gardelę judinant kampu, pirmiausia, parenkamas pasvirimo kampas α , kuriuo yra atliekamas harmoniniai svyravimai. Tada parenkamas svyravimų amplitudės dydis a . Pagal šiuos parametrus sudaroma gardelės transformacijos matrica. Pavyzdžiui, jeigu parenkame parametrus tokius: $a = 5$ ir $\alpha = \frac{\pi}{4}$, tai transformacijos matrica grafiškai atrodys kaip **11 pav.**, o matematiškai bus užrašoma taip:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.0361 & 0.0269 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.0216 & 0.1272 & 0.0316 \\ 0 & 0 & 0 & 0 & 0 & 0.0166 & 0.0739 & 0.0216 & 0 \\ 0 & 0 & 0 & 0 & 0.0152 & 0.0629 & 0.0166 & 0 & 0 \\ 0 & 0 & 0 & 0.0152 & 0.0603 & 0.0152 & 0 & 0 & 0 \\ 0 & 0 & 0.0166 & 0.0629 & 0.0152 & 0 & 0 & 0 & 0 \\ 0 & 0.0216 & 0.0739 & 0.0166 & 0 & 0 & 0 & 0 & 0 \\ 0.0361 & 0.1271 & 0.0216 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.0269 & 0.0361 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$



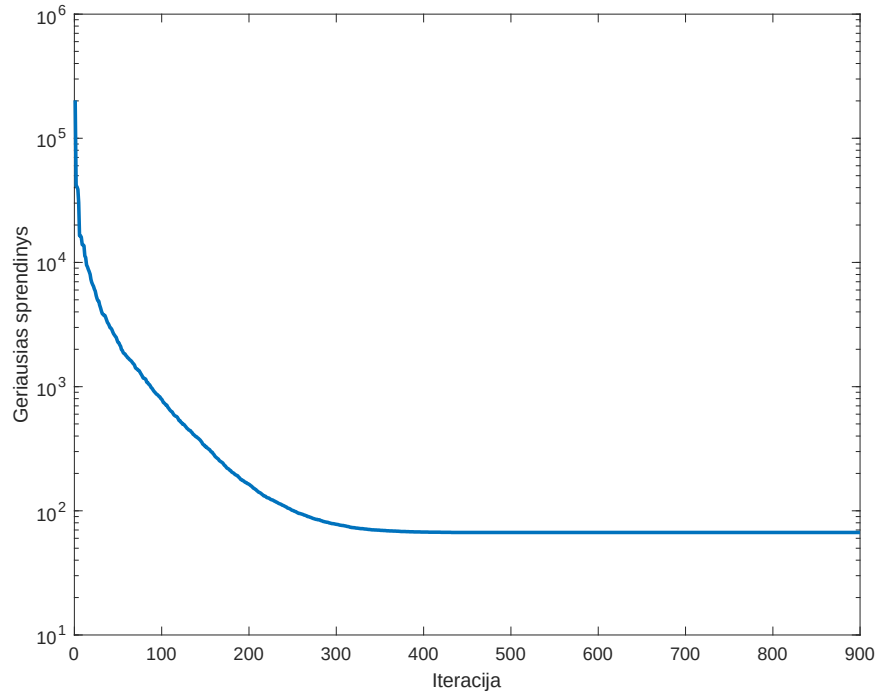
11 pav. Gardelės transformacijos matricos B^* grafinis atvaizdavimas, kai gardelės svyravimo parametrai yra tokie: $a = 5, \alpha = \frac{\pi}{4}$.

Įstrižai judinamas vaizdas (kampas lygus $\frac{\pi}{4}$) amplitudė $a = 2$ pusiausvyros ir laike vidurkinto vaizdo būsenoje parodytas **12 pav.** Čia matomi vaizdų taškų pilkos spalvos atspalviai, kurių įvairovei vertinti naudojamas Wada indeksas. Atitinkamai pirmosios gardelės abiejų būsenų Wada indeksai grafiškai pavaizduoti taip pat **12 pav.**



12 pav. Pirmoji stochastinė stacionari (pirmas vaizdas) ir laike vidurkinta (trečias vaizdas) gardelė, kai svyravimai atliekami $\frac{\pi}{4}$ kampu, amplitudė lygi 2, vaizdo dydis 30x30. Antrajame ir ketvirtajame vaizduose atitinkamai parodyti gardelių Wada indeksai. F_1 optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 34x34, nežinomų sprendinių skaičius $34^2 = 1156$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 900, populiacijos dydis – 600 dalelių, tikslo funkcijos F_1 koeficientų reikšmės: $k_1 = k_2 = k_3 = 1$.

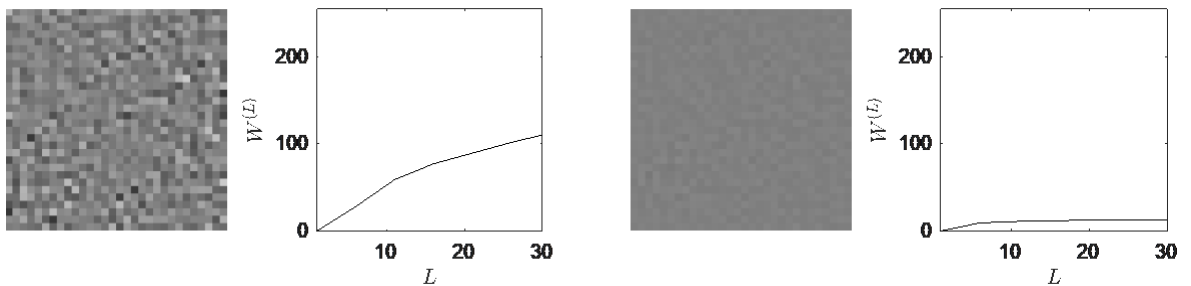
12 pav. matoma, kad stacionarioje gardelėje Wada indekso grafike maksimali reikšmė yra didesnė ($\omega_{\max}^{(1)} = 103.57$), nei laike vidurkintoje gardelėje ($\bar{\omega}_{\max}^{(1)} = 12.29$). Vizualiai, stacionarioji gardelė atrodo marga, o laike vidurkinta gardelė – pilka, tai parodo ir standartinio nuokrypio reikšmės: stacionarios gardelės taškų reikšmių sklaida yra didesnė ($\sigma^{(1)} = 20.88$), lyginant su laike vidurkinta gardele, kurios dauguma taškų įgijo artimą reikšmę pilko taško reikšmei – 127.5 (standartinis nuokrypis $\bar{\sigma}^{(1)} = 2.36$). Optimizavimo rezultatų konvergavimo grafikas yra pateiktas **13 pav.** Matoma, kad beveik optimalus sprendinys optimizavimo procese buvo rastas. Toliau vaizduojant optimizavimo rezultatus, gautus gardelę vidurkinant su amplitudė $a = 2$, sprendinių konvergavimo grafikai nebus pateikiami, kadangi visais atvejais konvergavimas panašus į **13 pav.**, kur matoma kreivės „uodega“, nurodanti į nusistovėjusią beveik optimalaus sprendinio reikšmę. Taip pat dėl aiškesnio vaizdo taškų vaizdavimo bei optimizavimo resursų taupymo tolimesniuose skaičiavimuose grafiniai rezultatai pateikiami 30x30 dydžio vaizdams.



13 pav. Pirmosios gardelės optimizavimo konvergavimo grafikas: kiekvienoje iteracijoje rasto geriausio sprendinio reikšmė, kai svyravimai atliekami $\frac{\pi}{4}$ kampu, amplitudė lygi 2, vaizdo dydis 30x30. F_1 optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 34x34, nežinomų sprendinių skaičius $34^2 = 1156$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 900, populiacijos dydis – 600 dalelių, tikslo funkcijos F_1 koeficientų reikšmės: $k_1 = k_2 = k_3 = 1$.

Optimizavimo tikslo funkcija apibrėžiama (22) formule, kai visi koeficientai $k_1 = k_2 = k_3 = 1$. Vizualiai matoma, kad **12 pav.** laike vidurkintas vaizdas nėra visiškai pilkas (matomi skirtingi pilkos spalvos atspalviai), todėl toliau tikslo funkcija yra keičiama taip, kad vaizdo margumas būtų mažesnis, t.y. funkcijos dalis $\left(\frac{127.5}{\sigma^{(1)}} - 1\right)$ neturėtų didelio svorio optimizavime, o funkcijos dalis $\overline{\mu}_4^{(1)}$ turėtų didesnę svarbą.

Taigi, tyrime toliau atliekamas optimizavimas 900 iteracijų su tokiais pačiais parametrais, tačiau tikslo funkcijoje paliekamas tik $\overline{\mu}_4^{(1)}$ narys, kuris laike vidurkintą gardelę padaro kuo pilkesnę. Tokios funkcijos optimizavimo rezultatas pavaizduotas **14 pav.**

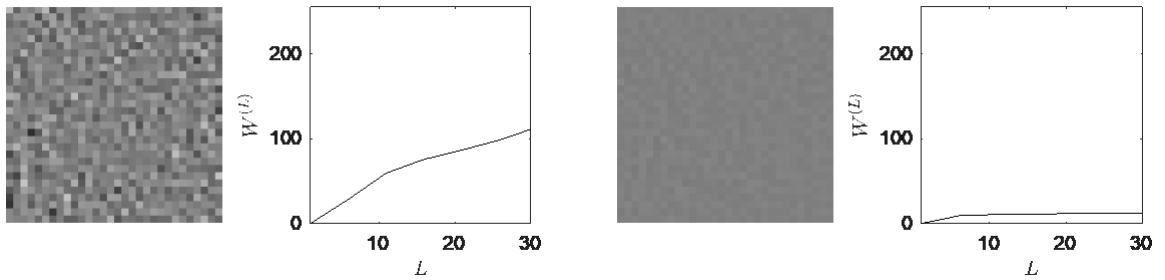


14 pav. Pirmoji stochastinė stacionari (pirmas vaizdas) ir laike vidurkinta (trečias vaizdas) gardelė, kai svyravimai atliekami $\frac{\pi}{4}$ kampu, amplitudė lygi 2, vaizdo dydis 30x30. Antrajame ir ketvirtajame vaizduose atitinkamai parodyti gardelių Wada indeksai. F_1 optimizavimo algoritmo parametrai: optimizuojamas vaizdo

dydis 34x34, nežinomų sprendinių skaičius $34^2 = 1156$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 900, populiacijos dydis – 600 dalelių, tikslo funkcijos F_1 koeficientų reikšmės: $k_1 = k_2 = k_3 = 0$.

14 pav. matoma, kad stacionarioje gardelėje tiek maksimali Wada indekso reikšmė yra didesnė ($\omega_{max}^{(1)} = 110.42$), nei laike vidurkintoje gardelėje ($\bar{\omega}_{max}^{(1)} = 13.23$), tiek standartinių nuokrypių reikšmės skiriasi ($\sigma^{(1)} = 22.31$ ir $\bar{\sigma}^{(1)} = 2.55$). Tikslo funkcijos $F_1(M_1) = \bar{\mu}_4^{(1)}$ optimizavimas abu vaizdus (stacionarią ir laike vidurkintą gardelę) užpilkino. Toliau ieškomos optimalios tikslo funkcijos koeficientų reikšmės didinant gardelių standartinį nuokrypį, kad stacionari gardelė būtų margesnė, t.y. grąžinamas tikslo funkcijos narys $\left(\frac{127.5}{\sigma^{(1)}} - 1\right)$, kuris lemia stacionarios gardelės standartinio nuokrypio dydį. Toliau optimizuojama tikslo funkcija apibrėžiama (32) formule, o jos optimizavimo rezultatai pateikiami **15 pav.**

$$F_1(M_1) = \left(\frac{127.5}{\sigma^{(1)}} - 1\right) + \bar{\mu}_4^{(1)} \quad (32)$$

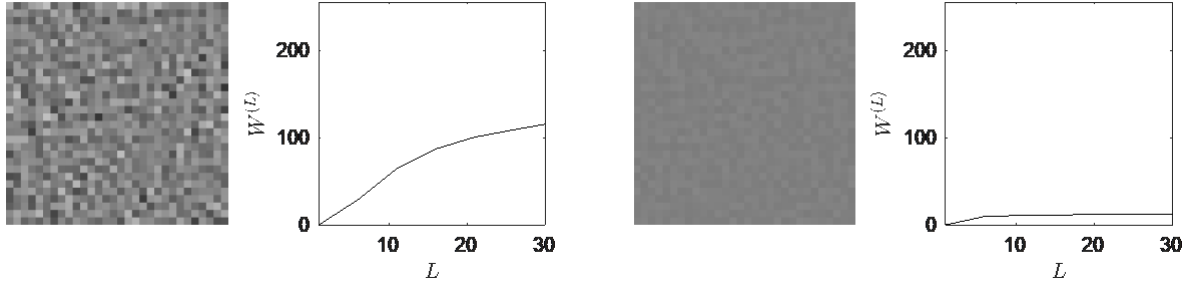


15 pav. Pirmoji stochastinė stacionari (pirmas vaizdas) ir laike vidurkinta (trečias vaizdas) gardelė, kai svyravimai atliekami $\frac{\pi}{4}$ kampu, amplitudė lygi 2, vaizdo dydis 30x30. Antrajame ir ketvirtajame vaizduose atitinkamai parodyti gardelių Wada indeksai. F_1 optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 34x34, nežinomų sprendinių skaičius $34^2 = 1156$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 900, populiacijos dydis – 600 dalelių, tikslo funkcijos F_1 koeficientų reikšmės: $k_1 = 1$, $k_2 = k_3 = 0$.

15 pav. pateiktuose rezultatuose vaizdai atitinka tokias aukščiausias Wada indekso reikšmes: $\omega_{max}^{(1)} = 110.99$ ir $\bar{\omega}_{max}^{(1)} = 12.09$, bei standartinio nuokrypio reikšmes: $\sigma^{(1)} = 21.9$ ir $\bar{\sigma}^{(1)} = 2.55$.

Tyrime toliau bandoma padidinti stacionarios gardelės pilkų taškų spalvų kontrastą didinant tikslo funkcijos $\left(\frac{127.5}{\sigma^{(1)}} - 1\right)$ nario įtaką optimizavime. Eksperimentiniu būdu išbandomos skirtingos koeficiento k_1 reikšmės ir nuspręsta, kad geriausiai optimizavimas atliekamas, kai $k_1 = 100$, o $k_2 = k_3 = 1$, tokiu būdu išlaikant spalvų pasiskirstymą panašų visose gardelės dalyse. Taigi tikslo funkcijos, aprašytos (33) formule, rezultatai pateikiami **16 pav.**

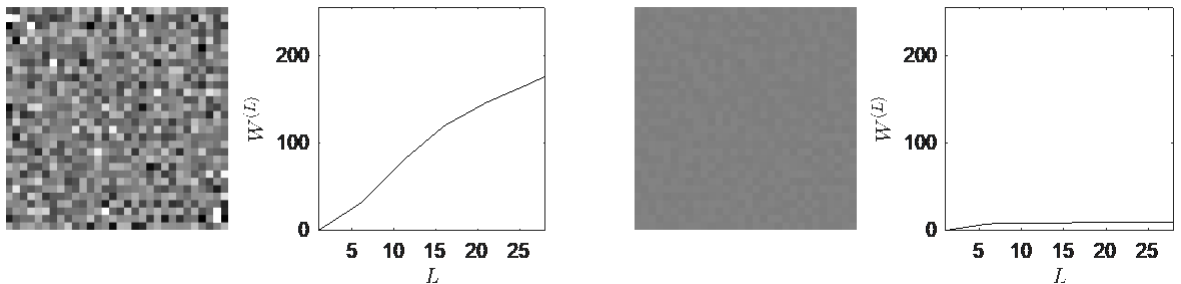
$$F_1(M_1) = 100 \left(\frac{127.5}{\sigma^{(1)}} - 1 \right) + \sqrt{\frac{1}{q^2} \sum_{i=1}^q \sum_{j=1}^q (m^{(1,i,j)} - m^{(1)})^2} + \sqrt{\frac{1}{q^2} \sum_{i=1}^q \sum_{j=1}^q \left(\sigma^{(1,i,j)} - \frac{1}{q^2} \sum_{k=1}^q \sum_{l=1}^q \sigma^{(1,k,l)} \right)^2} + \bar{\mu}_4^{(1)} \quad (33)$$



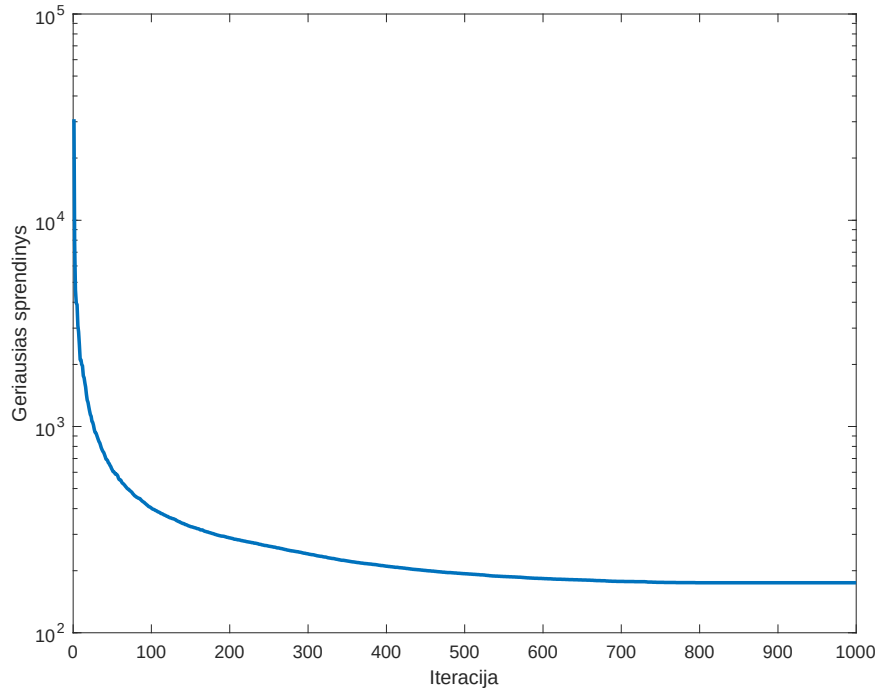
16 pav. Pirmoji stochastinė stacionari (pirmas vaizdas) ir laike vidurkinta (trečias vaizdas) gardelė, kai svyravimai atliekami $\frac{\pi}{4}$ kampų, amplitudė lygi 2, vaizdo dydis 30x30. Antrajame ir ketvirtajame vaizduose atitinkamai parodyti gardelių Wada indeksai. F_1 optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 34x34, nežinomų sprendinių skaičius $34^2 = 1156$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 900, populiacijos dydis – 600 dalelių, tikslo funkcijos F_1 koeficientų reikšmės: $k_1 = 100$, $k_2 = k_3 = 1$.

Gautuose rezultatuose matoma, kad Wada indeksas pasiekia aukščiausias reikšmes būtent optimizuojant (33) tikslo funkciją (stacionarios gardelės $\omega_{max}^{(1)} = 115.32$). Laike vidurkintos gardelės aukščiausia Wada indekso reikšmė yra žemiausia lyginant su anksčiau gautais rezultatais ($\bar{\omega}_{max}^{(1)} = 11.95$). Standartinio nuokrypio reikšmės (33) funkcijos optimizavime atitinkamai yra $\sigma^{(1)} = 24.55$ ir $\bar{\sigma}^{(1)} = 2.84$. Tolesniuose skaičiavimuose naudojama būtent ši (33) tikslo funkcija.

Taip pat matoma, kad paskutiniuose rezultatuose **16 pav.** laike vidurkintas vaizdas vizualiai nėra visiškai pilkas, tai galėjo lemti amplitudės dydis. Pirmieji rezultatai gauti, kai gardelė vidurkinta amplitudė 2. Todėl toliau skaičiuojami ir vizualizuojami rezultatai, kai gardelė vidurkinama su amplitudė lygia 5. Kadangi padidėjus amplitudei vidurkinimo procese atliekamas didesnis veiksmų kiekis tarp vaizdo taškų, optimizavimas vykdomas 1000 iteracijų. (33) formule aprašyta tikslo funkcija yra optimizuojama, kai $a = 5$. Gauti rezultatai pateikti **17 pav.**, o optimizuoto sprendinio konvergavimo grafikas **18 pav.**



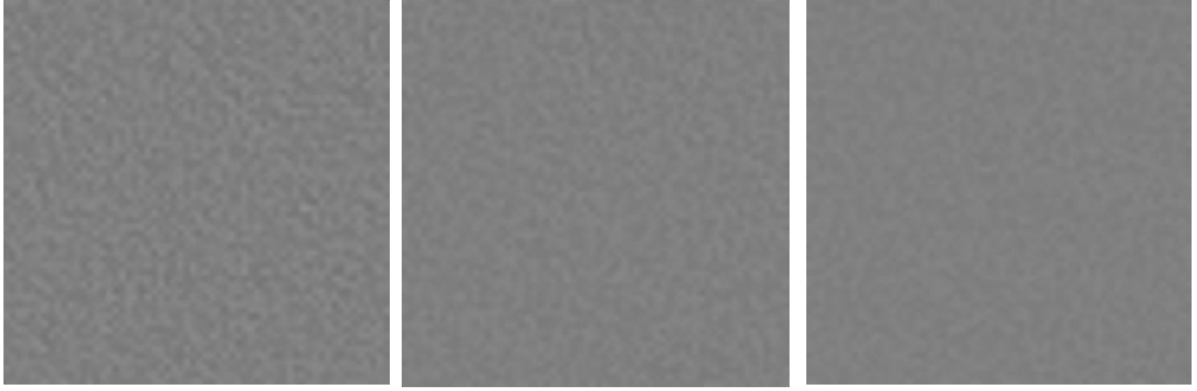
17 pav. Pirmoji stochastinė stacionari (pirmas vaizdas) ir laike vidurkinta (trečias vaizdas) gardelė, kai svyravimai atliekami $\frac{\pi}{4}$ kampu, amplitudė lygi 5, vaizdo dydis 30x30. Antrajame ir ketvirtajame vaizduose atitinkamai parodyti gardelių Wada indeksai. F_1 optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 38x38, nežinomų sprendinių skaičius $38^2 = 1444$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos F_1 koeficientų reikšmės: $k_1 = 100$, $k_2 = k_3 = 1$.



18 pav. Pirmosios gardelės optimizavimo konvergavimo grafikas: kiekvienoje iteracijoje rasto geriausio sprendinio reikšmė, kai svyravimai atliekami $\frac{\pi}{4}$ kampu, amplitudė lygi 5, vaizdo dydis 30x30. F_1 optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 38x38, nežinomų sprendinių skaičius $38^2 = 1444$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos F_1 koeficientų reikšmės: $k_1 = 100$, $k_2 = k_3 = 1$.

Kai amplitudė padidinama, optimizavimo rezultatai vizualiai atrodo geresni (statinė gardelė magesnė, o laike vidurkinta gardelė pilkesnė). Taip pat ir stacionarios gardelės Wada indekso reikšmė didesnė ($\omega_{max}^{(1)} = 175.93$), o laike vidurkintos gardelės aukščiausia Wada indekso reikšmė yra mažesnė ($\bar{\omega}_{max}^{(1)} = 8.96$). Standartinis nuokrypis taip pat rodo geresnius optimizavimo rezultatus: $\sigma^{(1)} = 43.9$ ir $\bar{\sigma}^{(1)} = 2.22$.

Žinoma, kad didesnė amplitudės reikšmė laike vidurkintą vaizdą padaro pilkesnį, lyginant su vidurkinimu mažesne amplitudė. Skirtingomis amplitudėmis laike vidurkintų gardelių vaizdai pateikti **19 pav.**



19 pav. Pirmoji laike vidurkinta gardelė, kai svyravimai atliekami $\frac{\pi}{4}$ kampu, tokiomis amplitudėmis: $a = 2$ (kairėje), $a = 5$ (viduryje), $a = 8$ (dešinėje), kai vaizdo dydis 60x60. F_1 optimizavimo algoritmo parametrai: sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1100, populiacijos dydis – 600 dalelių, tikslo funkcijos F_1 koeficientų reikšmės: $k_1 = 100$, $k_2 = k_3 = 1$.

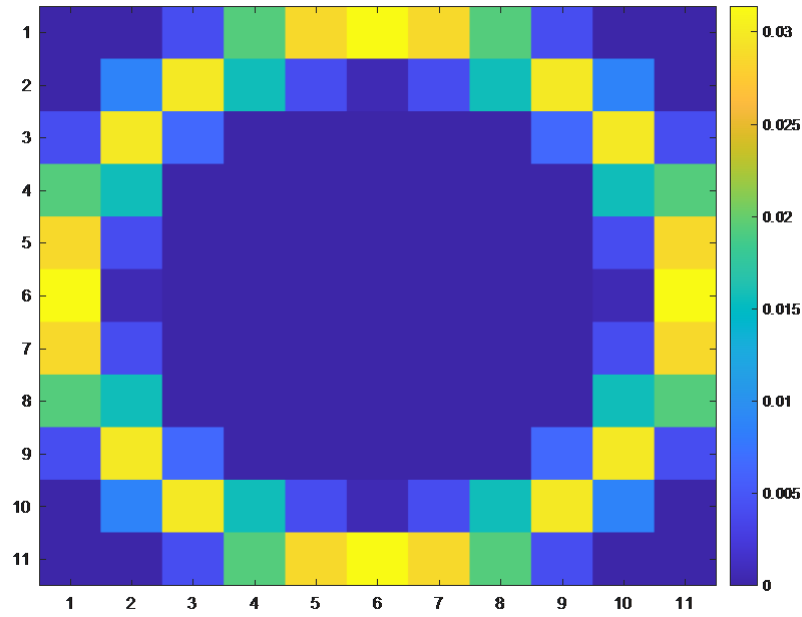
Kai amplitudės dydis yra 2, 5 ir 8, laike vidurkintų gardelių taškų reikšmių standartinis nuokrypis atitinkamai yra $\bar{\sigma}^{(1)} = 3.8$, $\bar{\sigma}^{(1)} = 3$ ir $\bar{\sigma}^{(1)} = 2.3$, o vidurkių reikšmės: $\bar{m}^{(1)} = 128.06$, $\bar{m}^{(1)} = 128$, $\bar{m}^{(1)} = 127.98$.

Iš **19 pav.** matoma, kad norint vaizdą padaryti kuo pilkesnį, amplitudę reikėtų pasirinkti kuo didesnę. Atlikus tuos pačius skaičiavimus su amplitude $a = 8$, gauti tokie rezultatai: $\omega_{\max}^{(1)} = 195.97$, $\bar{\omega}_{\max}^{(1)} = 8.06$, $\sigma^{(1)} = 59.84$ ir $\bar{\sigma}^{(1)} = 1.99$. Tačiau naudojant didesnę gardelę, reikalingas didesnis kiekis iteracijų ir sunaudojama daugiau laiko bei energijos resursų. Taip pat vėliau bus pastebėta, kad informacijos slėpime didelės amplitudės judesys iškreipia informacijos vaizdą, todėl bus ieškoma optimali amplitudė, su kuria pirmosios gardelės laike vidurkintas vaizdas būtų pilkas, o paslėpta informacija nebūtų iškraipoma. Optimalia amplitude pasirinkta laikyti $a = 5$, todėl tolesniuose rezultatuose pateikiamos gardelės, judinamos būtent šio dydžio amplitude.

3.1.2. Elipsinis svyravimas

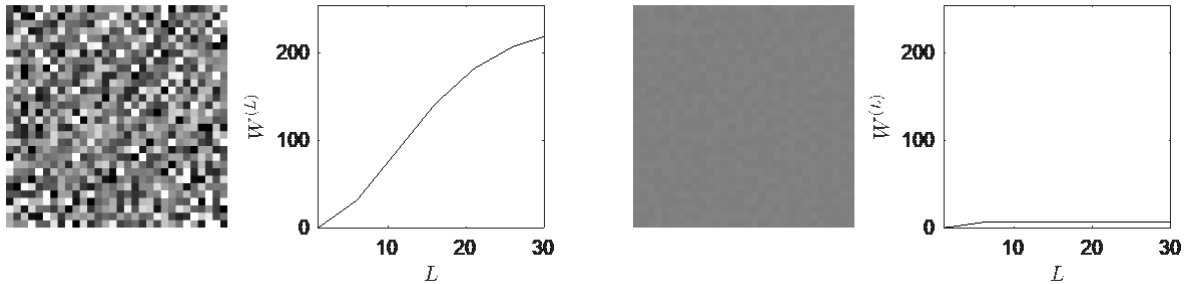
Elipsiniams svyravimams aprašyti reikalingos dviejų amplitudžių (horizontalios ir vertikalios ašies) parametrai a ir b . Pavyzdžiui, jeigu vaizdas judinamas apskritimu, tai parenkame vienodus elipsės amplitudžių parametrus $a = b = 5$, tada gardelė yra judinama apskritimu ir transformacijos matrica grafiškai atrodo kaip **20 pav.**, o matematiškai aprašoma taip:

$$\begin{pmatrix} 0 & 0 & 0.0041 & 0.0193 & 0.0287 & 0.0314 & 0.0287 & 0.0193 & 0.0041 & 0 & 0 \\ 0 & 0.0086 & 0.0298 & 0.0156 & 0.0039 & 0.0005 & 0.0039 & 0.0156 & 0.0298 & 0.0086 & 0 \\ 0.0041 & 0.0298 & 0.0065 & 0 & 0 & 0 & 0 & 0 & 0.0065 & 0.0298 & 0.0041 \\ 0.0193 & 0.0156 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.0156 & 0.0193 \\ 0.0287 & 0.0039 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.0039 & 0.0287 \\ 0.0314 & 0.0005 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.0005 & 0.0314 \\ 0.0287 & 0.0039 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.0039 & 0.0287 \\ 0.0193 & 0.0156 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.0156 & 0.0193 \\ 0.0041 & 0.0298 & 0.0065 & 0 & 0 & 0 & 0 & 0 & 0.0065 & 0.0298 & 0.0041 \\ 0 & 0.0086 & 0.0298 & 0.0156 & 0.0039 & 0.0005 & 0.0039 & 0.0156 & 0.0298 & 0.0086 & 0 \\ 0 & 0 & 0.0041 & 0.0193 & 0.0287 & 0.0314 & 0.0287 & 0.0193 & 0.0041 & 0 & 0 \end{pmatrix}.$$



20 pav. Gardelės transformacijos matricos B^* grafinis atvaizdavimas, kai gardelė judinama elipsiniais svyravimais su tokiais parametrais: $a = 5, b = 5$.

Naudojant šiuos parametrus ($a = 5, b = 5$) laike vidurkinama pirmoji stacionari gardelė, gauti rezultatai pateikti **21 pav.**

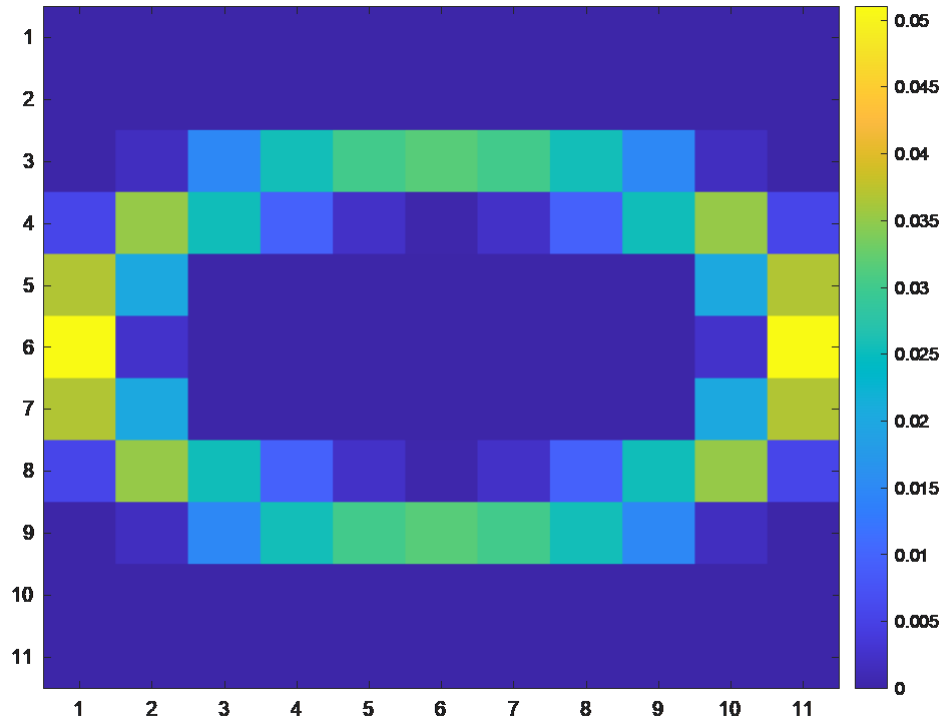


21 pav. Pirmoji stochastinė stacionari (pirmas vaizdas) ir laike vidurkinta (trečias vaizdas) gardelė, kai atliekami elipsiniai svyravimai, amplitudės lygios 5 ir 5, vaizdo dydis 30x30. Antrajame ir ketvirtajame vaizduose atitinkamai parodyti gardelių Wada indeksai. F_1 optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 40x40, nežinomų sprendinių skaičius $40^2 = 1600$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos F_1 koeficientų reikšmės: $k_1 = 100$, $k_2 = k_3 = 1$.

Gardelės, judinamos elipsiniais virpesiais (apskritimu) vidurkinimo procesas davė geresnius optimizavimo rezultatus, nei gardelės vidurkinimas harmoniniais svyravimais (**17 pav.**). Matoma, kad stacionari gardelė marga, o laike vidurkinta gardelė – pilka. Stacionarios gardelės parametru reikšmės po optimizavimo: $\omega_{max}^{(1)} = 218.92$, $\sigma^{(1)} = 67.79$. Laike vidurkintos gardelės parametru reikšmės po optimizavimo: $\bar{\omega}_{max}^{(1)} = 7.13$, $\bar{\sigma}^{(1)} = 1.77$.

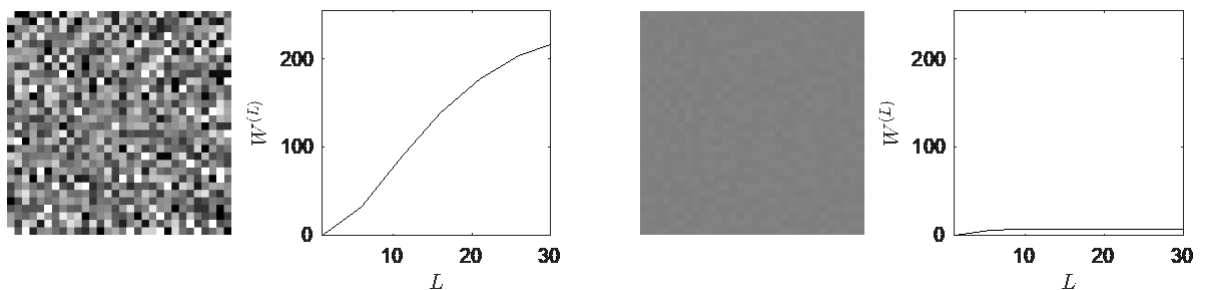
Jeigu vaizdas judinamas elipse, tai parenkami skirtingi amplitudžių parametrai. Pavyzdžiui, $a = 5$, $b = 3$, tada transformacijos matrica atrodo taip:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.0017 & 0.0148 & 0.0256 & 0.0303 & 0.0316 & 0.0303 & 0.0256 & 0.0148 & 0.0017 & 0 \\ 0.0055 & 0.0351 & 0.0254 & 0.0094 & 0.0024 & 0.0003 & 0.0024 & 0.0094 & 0.0254 & 0.0351 & 0.0055 \\ 0.0368 & 0.0202 & 0.0001 & 0 & 0 & 0 & 0 & 0 & 0.0001 & 0.0202 & 0.0368 \\ 0.0510 & 0.0025 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.0025 & 0.0510 \\ 0.0368 & 0.0202 & 0.0001 & 0 & 0 & 0 & 0 & 0 & 0.0001 & 0.0202 & 0.0368 \\ 0.0055 & 0.0351 & 0.0254 & 0.0094 & 0.0024 & 0.0003 & 0.0024 & 0.0094 & 0.0254 & 0.0351 & 0.0055 \\ 0 & 0.0017 & 0.0148 & 0.0256 & 0.0303 & 0.0316 & 0.0303 & 0.0256 & 0.0148 & 0.0017 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$



22 pav. Gardelės transformacijos matricos B^* grafinis atvaizdavimas, kai gardelė judinama elipsiniais svyravimais su tokiais parametrais: $a = 5$, $b = 3$.

Naudojant **22 pav.** parametrus ($a = 5$, $b = 3$) laike vidurkinama pirmoji stacionari gardelė, gauti rezultatai pateikti **23 pav.**



23 pav. Pirmoji stochastinė stacionari (pirmas vaizdas) ir laike vidurkinta (trečias vaizdas) gardelė, kai atliekami elipsiniai svyravimai, amplitudės lygios 5 ir 3, vaizdo dydis 40x40. Antrajame ir ketvirtajame vaizduose atitinkamai parodyti gardelių Wada indeksai. F_1 optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 40x40, nežinomų sprendinių skaičius $40^2 = 1600$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$,

iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos F_1 koeficientų reikšmės: $k_1 = 100$, $k_2 = k_3 = 1$.

Optimizavimo rezultatai, kai gardelė svyruoja pagal elipsinį dėsnį, vizualiai yra panašūs į rezultatus, kai gardelė svyruoja apskritimu. **23 pav.** parodytuose rezultatuose gardelių Wada indekso ir standartinio nuokrypio parametrai tai pat parodo panašius rezultatus, kaip **21 pav.** Stacionarios gardelės parametrų reikšmės po optimizavimo: $\omega_{\max}^{(1)} = 216.52$, $\sigma^{(1)} = 62.86$. Laike vidurkintos gardelės parametrų reikšmės po optimizavimo: $\bar{\omega}_{\max}^{(1)} = 6.68$, $\bar{\sigma}^{(1)} = 1.68$.

Taigi, galime daryti išvadą, kad pirmojo vaizdo sudaryme amplitudės dydis turi įtaką: kuo didesnė amplitudė, tuo laike vidurkinta gardelė yra pilkesnė. Dvimatė gardelė gali būti judinama tiek harmoniniais, tiek elipsiniais svyravimais. Pirmosios gardelės optimizavime, elipsiniu dėsniu svyruojama gardelė davė geresnius rezultatus, sukuriant statinį vaizdą kuo margesnį, o laike vidurkintą vaizdą kuo pilkesnį. Tačiau informacijos slėpime svarbu atitinkamai gerai suoptimizuoti antrąjį vaizdą, todėl antroji skyriaus dalis aptars būtent šį procesą.

3.2. Antrojo optimalaus vaizdo sudarymas

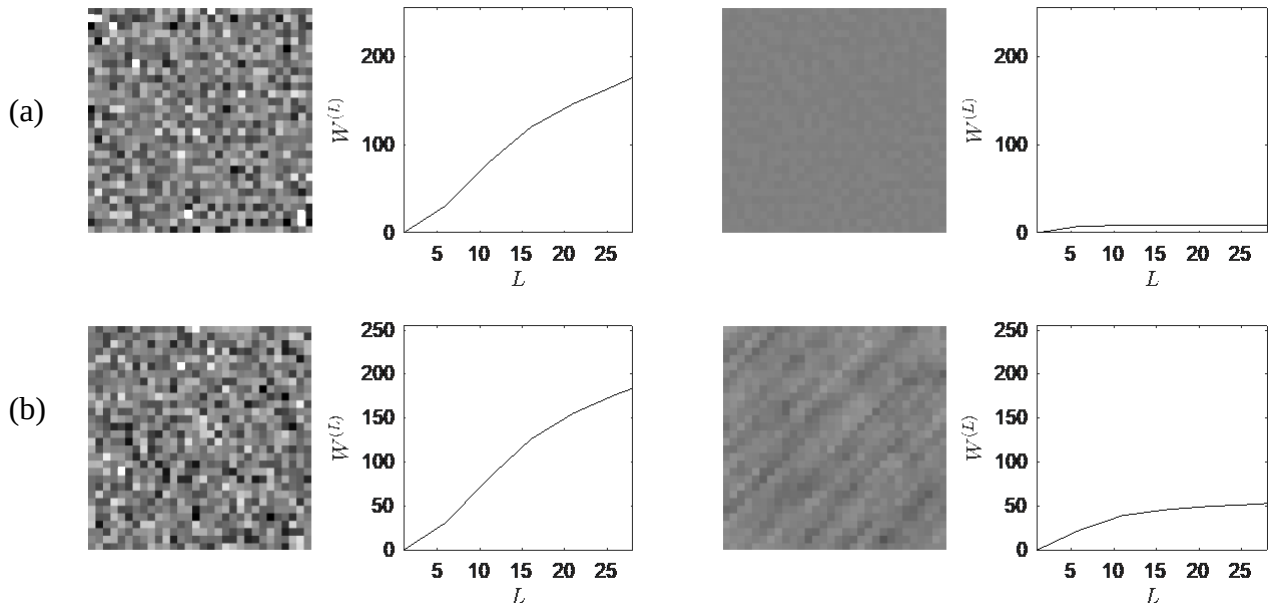
Generuojant antrąjį vaizdą siekiama, kad stacionari dvimatė gardelė M_2 būtų kuo panašesnė į pirmąją stacionarią gardelę M_1 , o laike vidurkinta dvimatė gardelė $\bar{M}_2$ kuo labiau skirtųsi nuo pirmosios laike vidurkintos gardelės $\bar{M}_1$, t.y. gardelė $\bar{M}_2$ būtų kuo margesnė. Taigi, antroji gardelė yra sudaroma naudojant pirmąją gardelę. Tai atliekama dvejais būdais: sudarant atsitiktinių reikšmių gardelę arba naudojant optimizavimą.

3.2.1. Atsitiktinių reikšmių gardelės sudarymas

Antroji stacionari gardelė gali būti sudaryta pagal pirmąją stacionarią gardelę naudojant įprastą atsitiktinių reikšmių generatorių *randn()* *Matlab* aplinkoje. Atsitiktinių reikšmių generavimo funkcijai nurodomas pirmosios gardelės vidurkis ir standartinis nuokrypis, pagal kuriuos sukuriamą į pirmąją gardelę panaši atsitiktinių reikšmių gardelė. Funkcija *randn()* originaliai sukuria atsitiktinius dydžius, kurių vidurkis yra 0, o standartinis nuokrypis lygus 1. Norint sukurti panašius atsitiktinius dydžius į pirmosios gardelės reikšmes, sugeneruotos reikšmės yra dauginamos iš pirmosios gardelės standartinio nuokrypio reikšmės ir pridamos vidurkio reikšmės:

$$M_2 = randn(0,1) \cdot \sigma^{(1)} + m^{(1)} \quad (34)$$

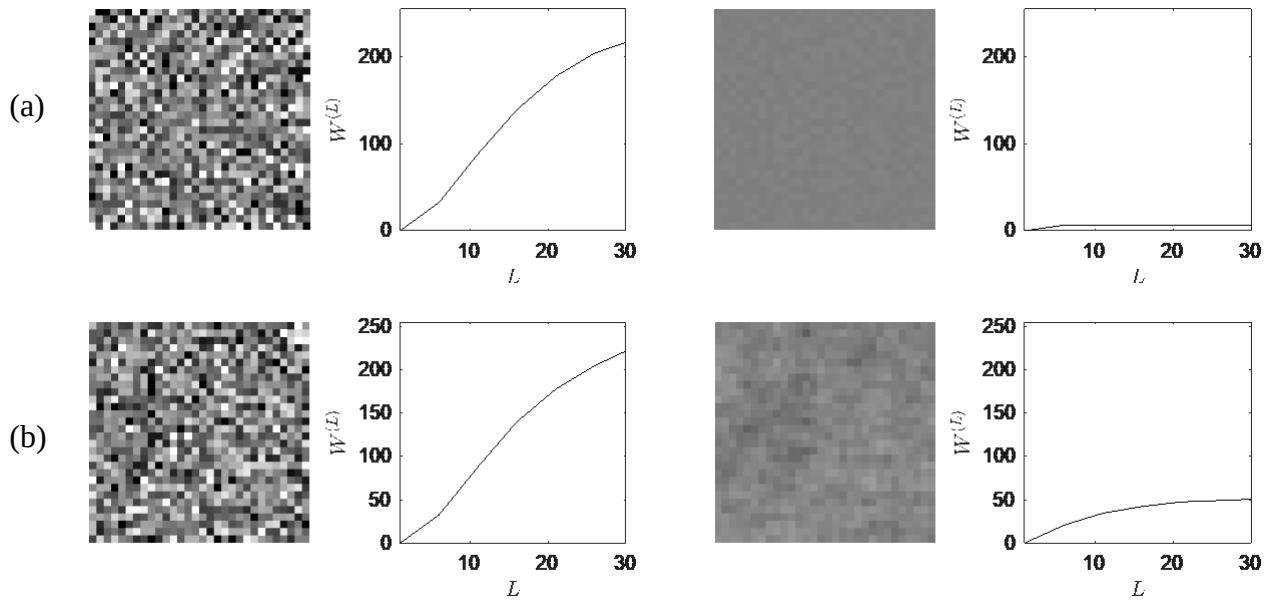
Sugeneruota antroji gardelė yra paveikiama transformacijos matricos ir taip gaunama antroji laike vidurkinta gardelė. Judėjimas atliekamas harmoniniu būdu su amplitude $a = 5$ ir pasvirimo kampų $\alpha = \frac{\pi}{4}$. Su šiais parametrais pirmoji ir antroji gardelė, bei jų Wada indeksų grafikai atrodo kaip **24 pav.**



24 pav. Pirmoji (a) ir antroji (b) stochastinė stacionari (pirmas vaizdas) ir laike vidurkinta (trečias vaizdas) gardelė, kai svyravimai atliekami $\frac{\pi}{4}$ kampų, amplitudė lygi 5, vaizdo dydis 30x30. Antrajame ir ketvirtajame vaizduose atitinkamai parodyti gardelių Wada indeksai. F_1 optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 38x38, nežinomų sprendinių skaičius $38^2 = 1444$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos F_1 koeficientų reikšmės: $k_1 = 100$, $k_2 = k_3 = 1$.

Iš **24 pav.** grafikų matoma, kad abi stacionarios gardelės atrodo atsitiktinės ir panašios ($\sigma^{(1)} = 43.9$ ir $\sigma^{(2)} = 44.04$), o laike vidurkintos gardelės skiriasi ($\bar{\sigma}^{(1)} = 2.22$ ir $\bar{\sigma}^{(2)} = 10.61$). Wada indekso reikšmės vizualiai matosi grafike: stacionarios pirmojo ir antrojo vaizdo gardelės Wada indekso reikšmės panašios, o laike vidurkintos gardelės reikšmės skiriasi. Taip pat antroje gardelėje vizualiai matoma virpėjimo kryptis ($\frac{\pi}{4}$), kai atliekami elipsiniai gardelės svyravimai, virpėjimo kryptis nėra taip aiškiai matoma (vaizdo taškai „prasilenkia“ ir „susimaišo“). Tokios gardelės optimizavimo rezultatai pateikti **25 pav.**

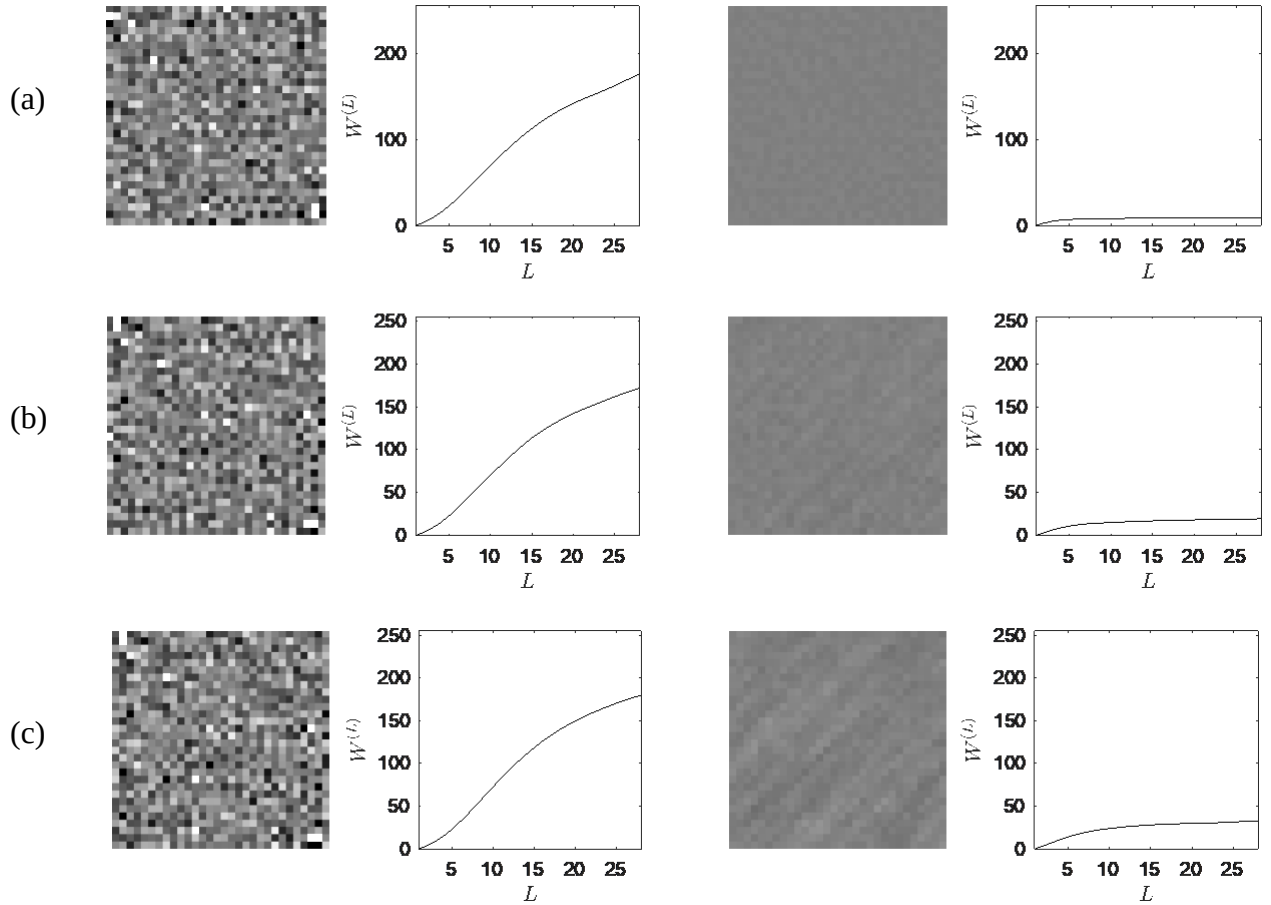
Kai gardelė svyruoja pagal elipsinį dėsnį, o antroji gardelė sudaroma iš atsitiktinių reikšmių pagal pirmosios gardelės parametrus. Tada antrosios gardelės standartinio nuokrypio reikšmės yra $\sigma^{(2)} = 60.17$, $\bar{\sigma}^{(2)} = 9.62$, kai pirmosios gardelės standartinio nuokrypio reikšmės $\sigma^{(1)} = 62.86$, $\bar{\sigma}^{(1)} = 1.68$. Gauti rezultatai (**24 pav.** ir **25 pav.**) atitinka pagrindinius stochastinių gardelių sudarymo reikalavimus (2.2 skyrelis), todėl antrosios gardelės sudarymo būdas naudojant atsitiktines reikšmes, bus naudojamas ir toliau tyrime, t.y. informacijos slėpimo procese.



25 pav. Pirmoji (a) ir antroji (b) stochastinė stacionari (pirmas vaizdas) ir laike vidurkinta (trečias vaizdas) gardelė, kai atliekami elipsiniai svyravimai, amplitudės lygios 5 ir 3, vaizdo dydis 30x30. Antrajame ir ketvirtajame vaizduose atitinkamai parodyti gardelių Wada indeksai. F_1 optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 40x40, nežinomų sprendinių skaičius $40^2 = 1600$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos F_1 koeficientų reikšmės: $k_1 = 100$, $k_2 = k_3 = 1$.

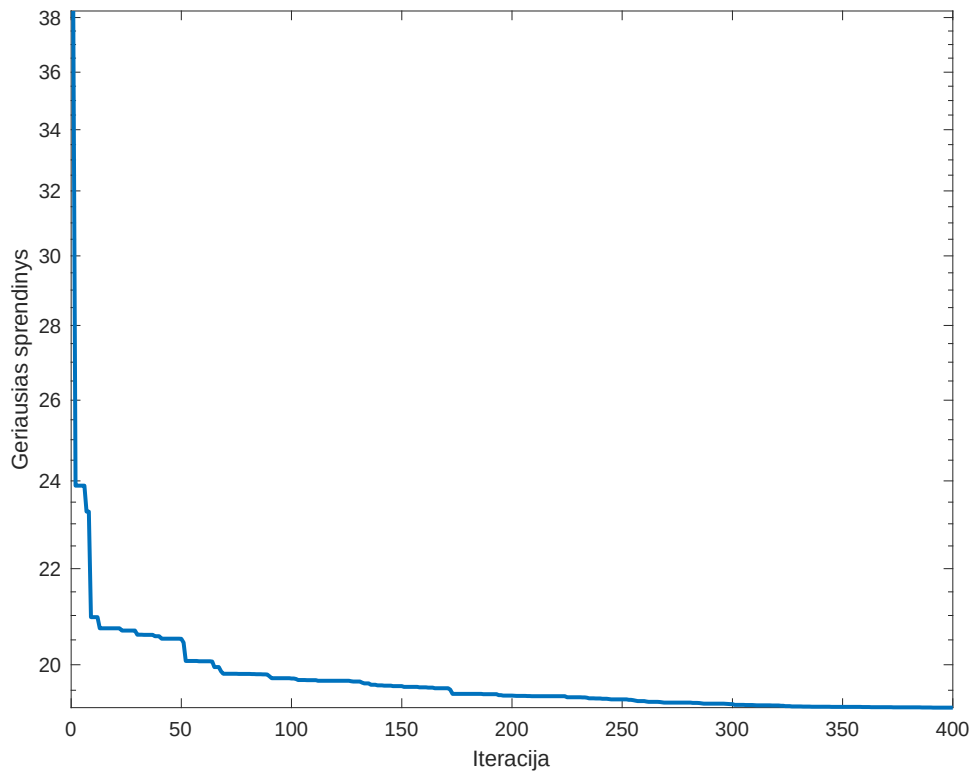
3.2.2. Optimizuotos gardelės sudarymas

Antrąją gardelę galime sudaryti ne tik atsitiktiniu būdu, tačiau taikant optimizavimo metodus. Optimizavimo tikslo funkcija F_2 aprašyta 2.5 skyrelyje. Ji optimizuojama 2.6 skyrelyje aprašytu dalelių spiečiaus optimizavimo algoritmu su apribojimu. Algoritmas skaičiuoja pirmosios gardelės korekcijas, kurios pridedamos ir gaunama antroji optimizuota stacionarioji gardelė M_2 . Gautoji gardelė paveikiama transformacijos matrica ir taip gaunama antroji laike vidurkinta gardelė. Pirmiausia, parenkamos optimizavimo sprendinių ribos, t.y. pirmosios gardelės korekcijų ribos. Šios ribos nurodo, kiek pirmoji stacionari gardelė bus koreguojama kuriant antrąją stacionariąją gardelę. Eksperimentiškai bandomi įvairūs korekcijų ribų intervalai. Rezultatai, gauti, kai ribos yra nuo -50 iki 50 ir nuo -85 iki 85, pateikti **26 pav.**, čia pirmosios gardelės svyravimai yra harmoniniai su amplitudė $a = 5$ ir pasvirimo kampu $\alpha = \frac{\pi}{4}$.



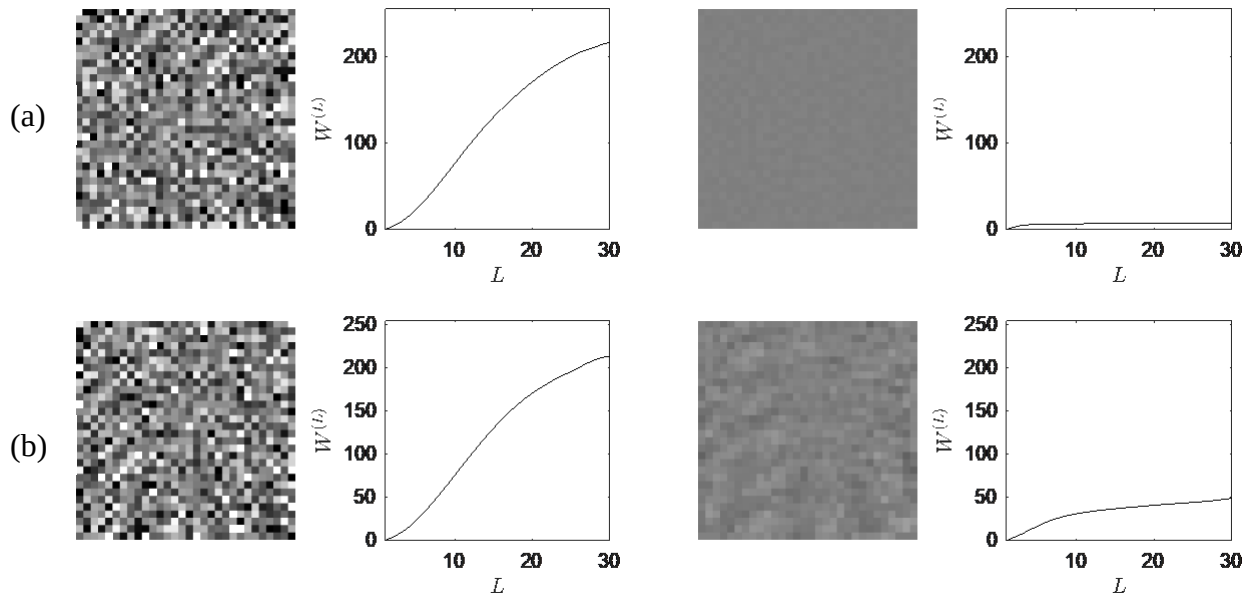
26 pav. Pirmoji (a) ir antroji (b,c) stochastinė stacionari (pirmas stulpelis) ir laike vidurkinta (trečias stulpelis) gardelė, kai svyravimai atliekami $\frac{\pi}{4}$ kampų, amplitudė lygi 5, vaizdo dydis 30x30. Antrajame ir ketvirtajame vaizduose atitinkamai parodyti gardelių Wada indeksai. F_1 optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 38x38, nežinomų sprendinių skaičius $38^2 = 1444$, sprendinių reikšmių ribos [0;255], $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių. Antroji gardelė sudaryta optimizuojant pirmąją gardelę. F_2 optimizavimo algoritmo parametrai: (b) vaizdo optimizavimo sprendinių ribos [-50;50], (c) vaizdo optimizavimo sprendinių ribos [-85;85], $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 400, populiacijos dydis – 500 dalelių, tikslo funkcijos F_1 koeficientų reikšmės: $k_1 = 100$, $k_2 = k_3 = 1$.

Antrosios stacionarios gardelės, gautos optimizavus pirmąją gardelę su sprendinių ribomis [-50;50] (**26 pav. (b)**), aukščiausia Wada indekso reikšmė lygi $\omega_{\max}^{(2)} = 171.69$, o standartinis nuokrypis $\sigma^{(2)} = 44.63$. Šią gardelę suvidurkinus, gaunama aukščiausia Wada indekso reikšmė $\bar{\omega}_{\max}^{(2)} = 19.51$ ir standartinis nuokrypis $\bar{\sigma}^{(2)} = 3.68$. Antrosios stacionarios gardelės, gautos optimizavus pirmąją gardelę su sprendinių ribomis [-85;85] (**26 pav. (c)**), aukščiausia Wada indekso reikšmė $\omega_{\max}^{(2)} = 1$, o standartinis nuokrypis $\sigma^{(2)} = 46.78$. Šią gardelę suvidurkinus, gaunama aukščiausia Wada indekso reikšmė $\bar{\omega}_{\max}^{(2)} = 32.56$ ir standartinis nuokrypis $\bar{\sigma}^{(2)} = 6.31$. Kadangi antrosios laike vidurkintos gardelės standartinis nuokrypis yra didesnis, kai optimizavimo sprendinių apribojimas yra nuo -85 iki 85 (tada $\bar{\sigma}^{(2)} = 6.31$), nei optimizavimo rezultatų su apribojimais nuo -50 iki 50 ($\sigma^{(2)} = 3.68$), tolesni rezultatai pateikiami optimizuotos antrosios gardelės su [-85;85] korekcijomis. Su šiais parametrais gautų rezultatų konvergavimo grafikas parodytas **27 pav.**

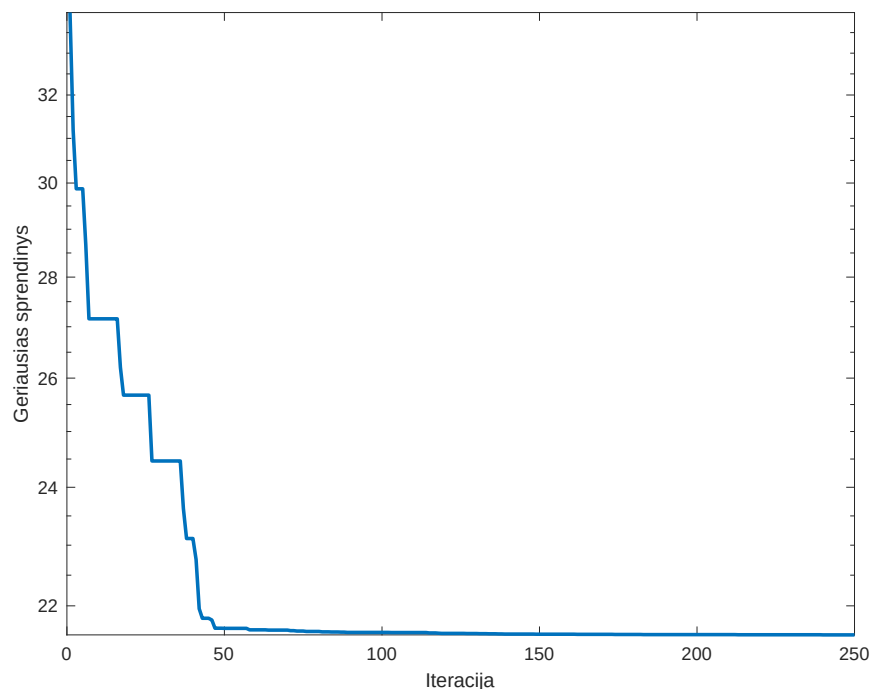


27 pav. Antrosios gardelės optimizavimo konvergavimo grafikas: kiekvienoje iteracijoje rasto geriausio sprendinio reikšmė, kai svyravimai atliekami $\frac{\pi}{4}$ kampu, amplitudė lygi 5. F_1 optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 38×38 , nežinomų sprendinių skaičius $38^2 = 1444$, sprendinių reikšmių ribos $[0; 255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos F_1 koeficientų reikšmės: $k_1 = 100$, $k_2 = k_3 = 1$. Antroji gardelė sudaryta optimizuojant pirmąją gardelę. F_2 optimizavimo algoritmo parametrai: vaizdo optimizavimo sprendinių ribos $[-85; 85]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 400, populiacijos dydis – 500 dalelių.

Toliau atliekamas antrosios gardelės optimizavimo procesas, kai pirmoji gardelė judinama elipsiniais virpesiais. Pirmosios ir antrosios gardelės optimizavimo rezultatai pateikti **28 pav.**, o konvergavimo grafikas pateiktas **29 pav.**



28 pav. Pirmoji (a) ir antroji (b) stochastinė stacionari (pirmas stulpelis) ir laike vidurkinta (trečias stulpelis) gardelė, kai atliekami elipsiniai svyravimai, amplitudės lygios 5 ir 3, vaizdo dydis 30x30. Antrajame ir ketvirtajame vaizduose atitinkamai parodyti gardelių Wada indeksai. F_1 optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 40x40, nežinomų sprendinių skaičius $40^2 = 1600$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos F_1 koeficientų reikšmės: $k_1 = 100$, $k_2 = k_3 = 1$. Antroji gardelė sudaryta optimizuojant pirmąją gardelę. F_2 optimizavimo algoritmo parametrai: (b) vaizdo optimizavimo sprendinių ribos $[-50;50]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 250, populiacijos dydis – 500 dalelių.



29 pav. Antrosios gardelės optimizavimo konvergavimo grafikas: kiekvienoje iteracijoje rasto geriausio sprendinio reikšmė, kai atliekami elipsiniai svyravimai, amplitudės lygios 5 ir 3, vaizdo dydis 30x30. F_1 optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 40x40, nežinomų sprendinių skaičius $40^2 = 1600$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$,

inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos F_1 koeficientų reikšmės: $k_1 = 100$, $k_2 = k_3 = 1$. Antroji gardelė sudaryta optimizuojant pirmąją gardelę. F_2 optimizavimo algoritmo parametrai: (b) vaizdo optimizavimo sprendinių ribos $[-50;50]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 250, populiacijos dydis – 500 dalelių.

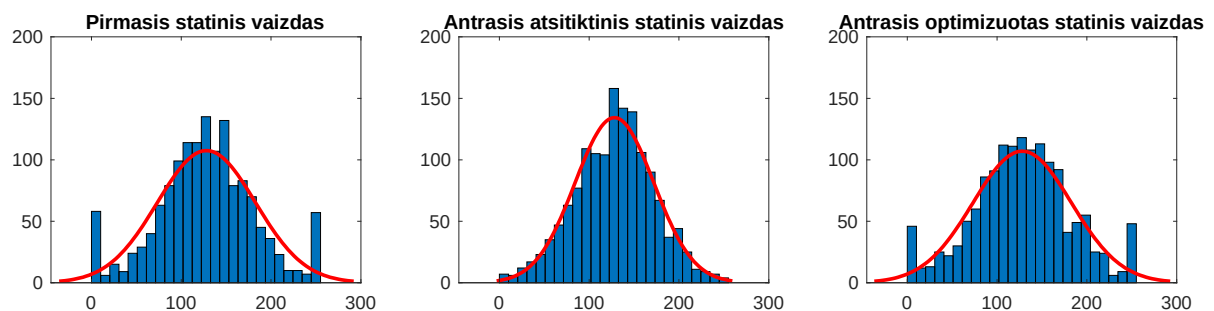
Taigi, antroji gardelė gali būti sudaroma dvejais būdais: naudojant atsitiktinių dydžių funkciją ir pirmosios gardelės parametrus, arba optimizuojant pirmąją gardelę pagal tikslo funkciją F_2 , aprašytą 2.5 skyrelyje. Šių antrosios gardelės sudarymo būdų ir kitų optimizavimui įtaką darančių parametru palyginimas pateiktas 2 lentelėje. Čia optimizuota gardelė sudaryta su pirmosios gardelės korekcijomis $[-85;85]$ intervale, kai svyravimai yra harmoniniai ir $[-50;50]$, kai svyravimai – elipsiniai.

2 lentelė. Atsitiktinai ir optimizavimo būdu sudarytos antrosios gardelės parametru reikšmės prie skirtingų pirmosios gardelės parametru.

Parametrai							Atsitiktinė antroji gardelė				Optimizuota antroji gardelė			
a	b	α	$\sigma^{(1)}$	$\bar{\sigma}^{(1)}$	$\omega_{max}^{(1)}$	$\bar{\omega}_{max}^{(1)}$	$\sigma^{(2)}$	$\bar{\sigma}^{(2)}$	$\omega_{max}^{(2)}$	$\bar{\omega}_{max}^{(2)}$	$\sigma^{(2)}$	$\bar{\sigma}^{(2)}$	$\omega_{max}^{(2)}$	$\bar{\omega}_{max}^{(2)}$
5	-	$\frac{\pi}{4}$	43.9	2.2	175.9	9	44	10.6	183.7	53.9	46.8	6.3	179.7	32.6
8	-	$\frac{\pi}{4}$	59.8	2	196	8.1	59.8	11.2	208.1	56	61	6	197.7	32.5
5	5	$\frac{\pi}{3}$	67.8	1.8	218.9	7.1	63.8	9.6	219.7	51.4	68.9	2.8	219.6	15.3
5	3	$\frac{\pi}{3}$	62.9	1.7	216.5	6.7	60.2	9.6	221.7	50.6	62.9	9.3	213.7	48.9

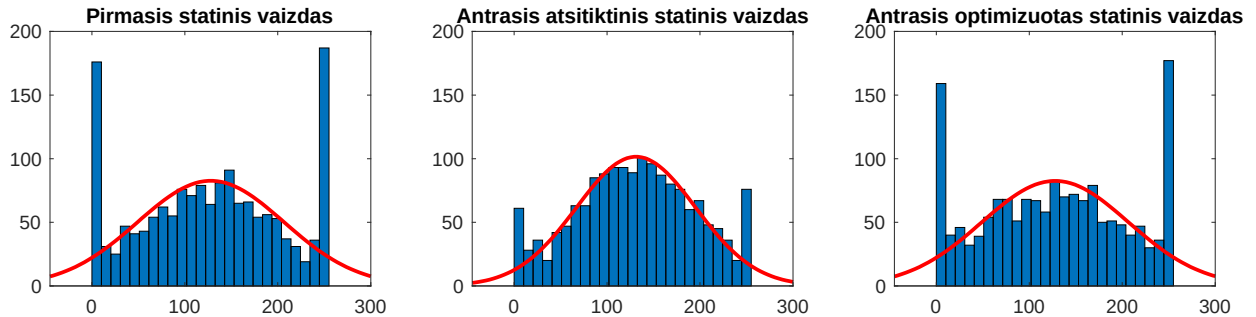
2 lentelė parodo, kad atsitiktinai sudaryta antroji gardelė siūlo panašius (kartais netgi geresnius) rezultatus, kaip optimizuotoji antroji gardelė, ypač laike vidurkintam vaizdui. Fonui ir slaptam vaizdui koduoti skirtos stacionarios gardelės turi būti kuo panašesnės. Kai slaptos informacijos kodavimo gardelė sudaroma naudojant atsitiktines normaliojo skirstinio reikšmes, stacionarios gardelės **24 pav.** ir **25 pav.** neatrodo tokios panašios, kaip **26 pav.** ir **28 pav.** stacionarios gardelės, kur slaptos informacijos kodavimui skirta gardelė sudaryta optimizavimo būdu.

Todėl reikalinga kita metodika, įvertinti optimizuotos ir atsitiktinai sudarytos gardelės tinkamumą informacijos slėpimui. Toliau braizomi stacionariųjų gardelių reikšmių skirstinių grafikai skirti įvertinti, kuris stacionarios gardelės sudarymo būdas (atsitiktinių reikšmių ar optimizavimo) yra tinkamesnis kuriant kuo panašesnę gardelę į pirmąją, fonui koduoti skirtą gardelę. **30 pav.** ir **31 pav.** parodyti stacionariųjų gardelių reikšmių pasiskirstymai.



30 pav. Stacionariųjų gardelių reikšmių pasiskirstymo grafikai: pirmoji stacionari gardelė (kairėje), antroji atsitiktinai sudaryta gardelė (viduryje) ir antroji optimizuota gardelė (dešinėje), kai svyravimai atliekami $\frac{\pi}{4}$ kampu, amplitudė lygi 5. F_1 optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 38×38 ,

nežinomų sprendinių skaičius $38^2 = 1444$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos F_1 koeficientų reikšmės: $k_1 = 100$, $k_2 = k_3 = 1$. Antroji gardelė sudaryta optimizuojant pirmąją gardelę. F_2 optimizavimo algoritmo parametrai: vaizdo optimizavimo sprendinių ribos $[-85;85]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 400, populiacijos dydis – 500 dalelių.



31 pav. Stacionarių gardelių reikšmių pasiskirstymo grafikai: pirmoji stacionari gardelė (kairėje), antroji atsitiktinai sudaryta gardelė (viduryje) ir antroji optimizuota gardelė (dešinėje), kai atliekami elipsiniai svyravimai, amplitudės lygios 5 ir 3, vaizdo dydis 30×30 . F_1 optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 40×40 , nežinomų sprendinių skaičius $40^2 = 1600$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos F_1 koeficientų reikšmės: $k_1 = 100$, $k_2 = k_3 = 1$. Antroji gardelė sudaryta optimizuojant pirmąją gardelę. F_2 optimizavimo algoritmo parametrai: (b) vaizdo optimizavimo sprendinių ribos $[-85;85]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 250, populiacijos dydis – 500 dalelių.

Kai gardelė yra judinama harmoniniais virpesiais ($\frac{\pi}{4}$ kampų), matoma, kad optimizuotos antrosios gardelės skirstinys yra panašesnis į pirmosios gardelės skirstinį, nei atsitiktinai sudarytos antrosios gardelės skirstinys (**30 pav.**). Kai gardelė judinama pagal elipsinį dėsnį, optimizuota statinė gardelė taip pat įgijo panašesnes reikšmes pirmajai statinei gardelei, nei atsitiktinai sudaryta antroji gardelė (**31 pav.**). Šie antrosios gardelės sudarymo būdai bus palyginti informacijos slėpimo etape.

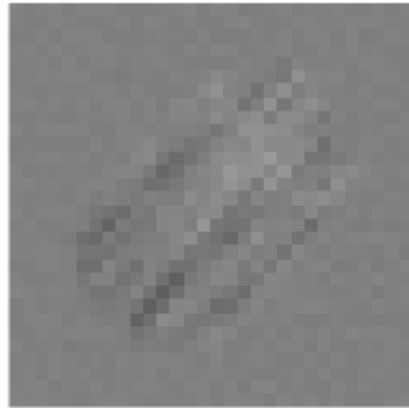
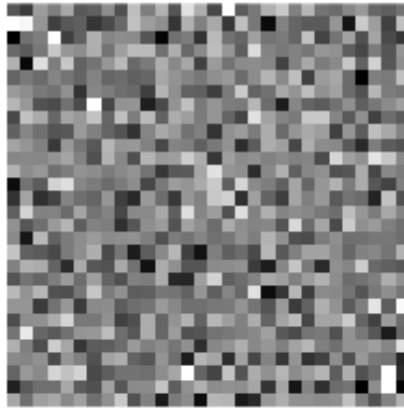
3.3. Informacijos slėpimas

Šiame skyrelyje pateikiami rezultatai, kai abu optimizuoti vaizdai yra sudedami į slaptos informacijos vaizdą. Pirmiausia, pasirenkamas juodas vaizdas baltame fone (gali būti atvirkščiai). Juodi slaptos informacijos vaizdo taškai pakeičiami antrosios gardelės taškais, o fono balti taškai – pirmosios gardelės taškais (taip pat, gali būti atvirkščiai). **32 pav.** parodyta slapta informacija – juodas skritulys, kuris slepiamas antrojoje gardelėje, kai stacionari pirmoji gardelė judinama amplitude $a = 5$, kampų $\frac{\pi}{4}$. Galutiniuose rezultatuose pateikiami užkoduoti ir atkoduoti vaizdai su nukirptu „rėmeliu“, kuris susidaro reikšmių vidurkinimo metu. Kraštiniuose vaizdo taškuose gardelė „užsibūna“ ilgiau ir vidurkinimas didesnis taškų kiekis, todėl atkoduotame vaizde matomas tamsus susidaręs rėmas. Patektuose grafiniuose rezultatuose, atkoduotų vaizdų kraštai yra apkerpami ir pateikiami be susidariusių rėmelių.

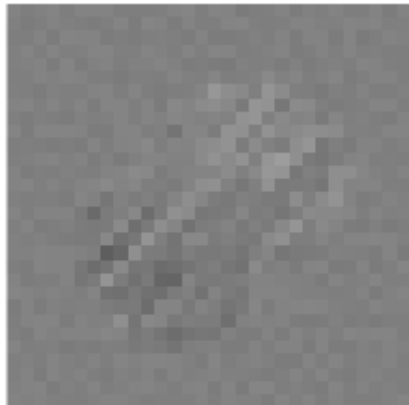
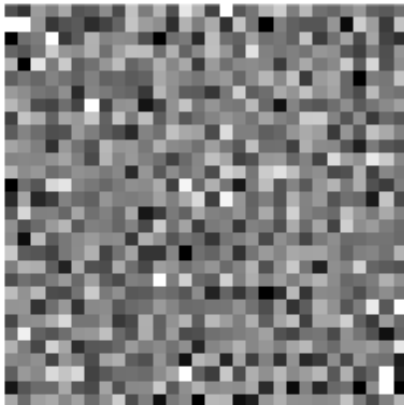
(a)



(b)

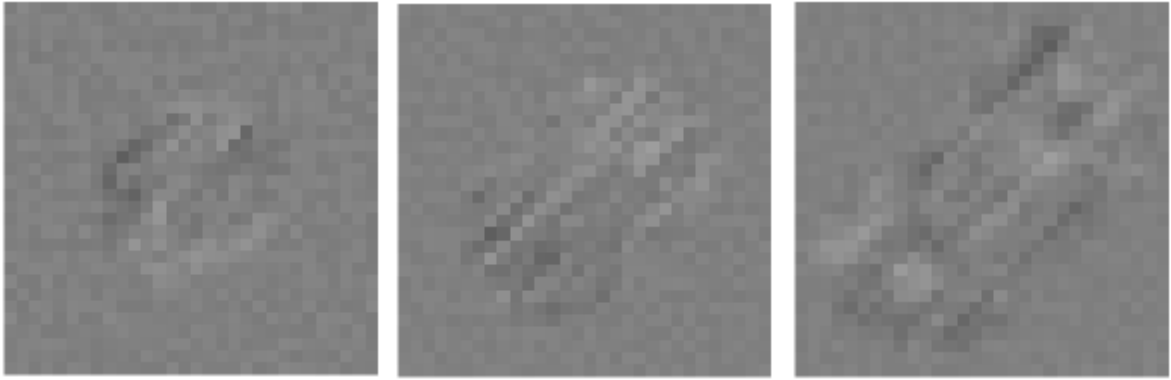


(c)



32 pav. Slaptos informacijos slėpimas dvimatėse muaro gardelėse: slaptos informacijos vaizdas (a), slaptas vaizdas dvimatėje statinėje (kairėje) ir laike vidurkintoje (dešinėje) muaro gardelėje, kai antroji gardelė sudaryta atsitiktinai (b), slaptas vaizdas dvimatėje statinėje (kairėje) ir laike vidurkintoje (dešinėje) gardelėje, kai antroji gardelė sudaryta optimizuojant (c). F_1 optimizavimo algoritmo parametrai: amplitudė lygi 5, svyravimų kampas $\frac{\pi}{4}$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, o vaizdo dydis yra 30x30, optimizavimo algoritmo parametrai: optimizuojamas vaizdo dydis 40x40, nežinomų sprendinių skaičius $40^2 = 1600$, sprendinių reikšmių ribos [0;255], $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, tikslo funkcijos F_1 koeficientų reikšmės: $k_1 = 1$, $k_2 = k_3 = 1$. F_2 optimizavimo algoritmo parametrai: (c) vaizdo optimizavimo sprendinių ribos [-85;85], $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 250, populiacijos dydis – 500 dalelių, tikslo funkcijos koeficientų reikšmės: $k_1 = 1$, $k_2 = k_3 = 1$.

Gautuose rezultatuose pastebima, kad **32 pav.** pradinėje užkoduotoje gardelėje slapta informacija nėra matoma, o laike vidurkintoje atkoduotoje gardelėje slapta informacija išryškėja. Tačiau atkoduotos informacijos vaizdas gardelėje atrodo sulietas, vizualiai matoma svyravimų kryptis. Kai skaičiavimai atliekami su didesne amplitude, slaptos informacijos vaizdas dar labiau suliejamas, kaip pavaizduota **33 pav.**, čia slepiamas tas pats juodas skritulio vaizdas (**32 pav.** (a)).



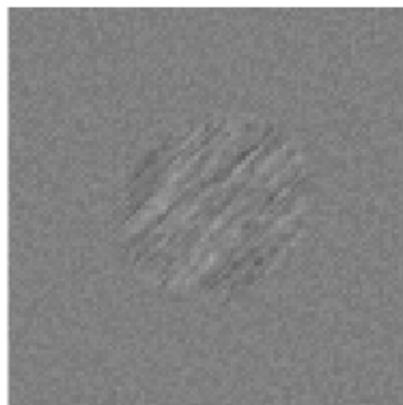
33 pav. Slaptos informacijos slėpimas dvimatėse muaro gardelėse: laike vidurkinta slapta informacija, kai svyravimų amplitudė lygi 2 (kairėje), 5 (viduryje) ir 8 (dešinėje), o svyravimų kryptis yra kampas $\frac{\pi}{4}$.

33 pav. matoma, kad judinant vaizdus su maža amplitude slapta informacija atkoduotame vaizde yra geriau matoma, tačiau fonas (pirmoji gardelė) yra mažiau pilkas, lyginant su didesne amplitude judintų vaizdų. Kuo didesnė amplitudė naudojama, tuo labiau atkoduotame vaizde slapta informacija yra suliejama, todėl toliau informacijos slėpimo procese naudojama svyravimų amplitudė sudaro ne daugiau nei 7 procentus vaizdo kraštinės ilgio. Iki šiol visi skaičiavimai atliekami 30 taškų pločio ir 30 taškų ilgio dydžio vaizdams. Didesniuose vaizduose (vaizdo dydis 100x100) suliejimo efektas nėra taip ryškiai matomas, kai svyravimų amplitudė $a = 5$, kaip parodyta **34 pav.**

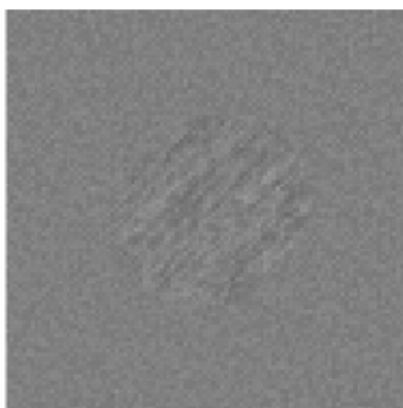
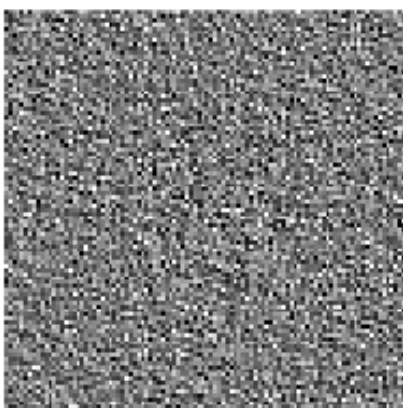
(a)



(b)



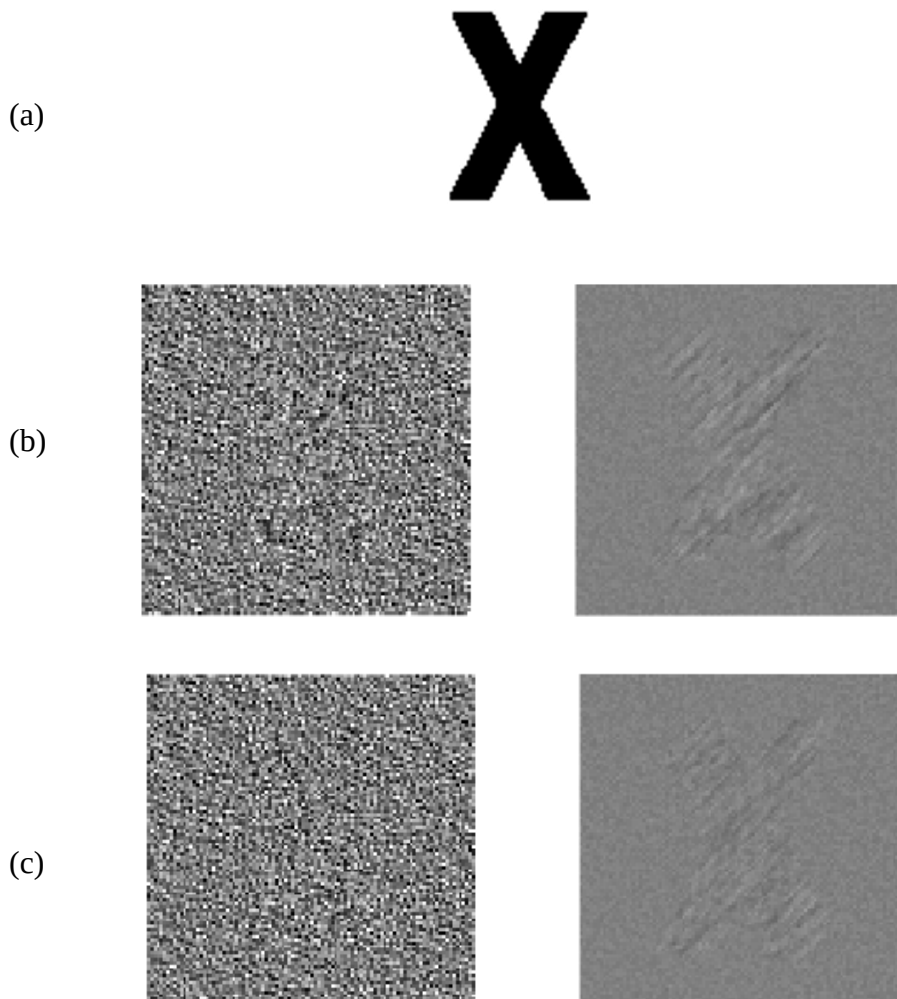
(c)



34 pav. Slaptos informacijos slėpimas dvimatėse muaro gardelėse: slaptos informacijos vaizdas (a), slaptas vaizdas dvimatėje statinėje (kairėje) ir laike vidurkintoje (dešinėje) muaro gardelėje, kai antroji gardelė sudaryta atsitiktinai (b), slaptas vaizdas dvimatėje statinėje (kairėje) ir laike vidurkintoje (dešinėje) gardelėje, kai antroji gardelė sudaryta optimizuojant (c). F_1 optimizavimo algoritmo parametrai: amplitudė lygi 5, svyravimų kampas $\frac{\pi}{4}$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, o vaizdo dydis yra 100x100, optimizuojamas vaizdo dydis 108x108, nežinomų sprendinių skaičius $108^2 = 11664$, sprendinių reikšmių ribos [0;255], $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, tikslo funkcijos F_1 koeficientų reikšmės: $k_1 = 100$, $k_2 = k_3 = 1$. F_2 optimizavimo algoritmo parametrai: (c) vaizdo optimizavimo sprendinių ribos [-85;85], $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 250, populiacijos dydis – 500 dalelių, tikslo funkcijos F_1 koeficientų reikšmės: $k_1 = 1$, $k_2 = k_3 = 1$.

Didesniuose vaizduose, kaip **34 pav.**, matoma, kad atsitiktinėmis reikšmėmis sudaryta antroji stacionari gardelė (**34 pav. (b)**) pilnai nepaslepia informacijos (matomi slaptos informacijos kraštai), nors atkoduotame vaizde slapta informacija vizualiai atrodo ryškesnė. Kai antroji gardelė yra optimizuojama (**34 pav. (c)**), informacijos slėpime užkoduotame vaizde slaptos informacijos

nesimato, o atkoduotame vaizde ji išryškėja, nors ji ne tokia ryški kaip **34 pav.** (b) vaizde. Toliau bandomas informacijos slėpimas su kitu slaptu vaizdu, gauti rezultatai parodyti **35 pav.**



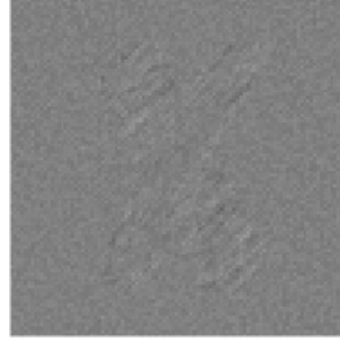
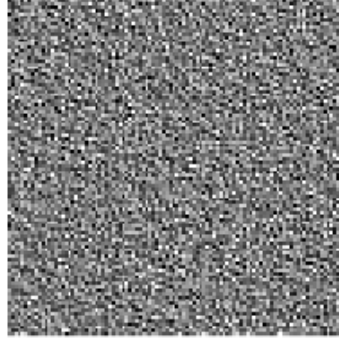
35 pav. Slaptos informacijos slėpimas dvimatėse muaro gardelėse: slaptos informacijos vaizdas (a), slaptas vaizdas dvimatėje statinėje (kairėje) ir laike vidurkintoje (dešinėje) muaro gardelėje, kai antroji gardelė sudaryta atsitiktinai (b), slaptas vaizdas dvimatėje statinėje (kairėje) ir laike vidurkintoje (dešinėje) gardelėje, kai antroji gardelė sudaryta optimizuojant (c). F_1 optimizavimo algoritmo parametrai: amplitudė lygi 5, svyravimų kampas $\frac{\pi}{4}$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, o vaizdo dydis yra 100x100, optimizuojamas vaizdo dydis 108x108, nežinomų sprendinių skaičius $108^2 = 11664$, sprendinių reikšmių ribos [0;255], $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, tikslo funkcijos koeficientų reikšmės: $k_1 = 100$, $k_2 = k_3 = 1$. F_2 optimizavimo algoritmo parametrai: (c) vaizdo optimizavimo sprendinių ribos [-85;85], $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 250, populiacijos dydis – 500 dalelių, tikslo funkcijos koeficientų reikšmės: $k_1 = 1$, $k_2 = k_3 = 1$.

Slepiant kitą informaciją, grafiniai rezultatai išlieka panašūs: naudojant atsitiktinai sudarytą gardelę, užkoduojamas slaptas vaizdas yra matomas, o naudojant optimizuotą gardelę, slapta informacija nėra matoma. Todėl laikome, kad optimizuota antroji gardelė yra labiau tinkama slėpti informacijai stochastinėje gardelėje. **34 pav.** ir **35 pav.** antroji funkcija yra optimizuojama su korekcijomis [-85;85] intervale. Taip pat bandomas [-50;50] korekcijų intervalas ir gauti rezultatai pateikiami **36 pav.**

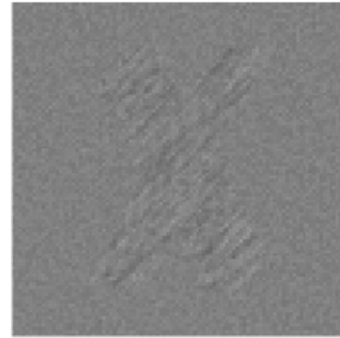
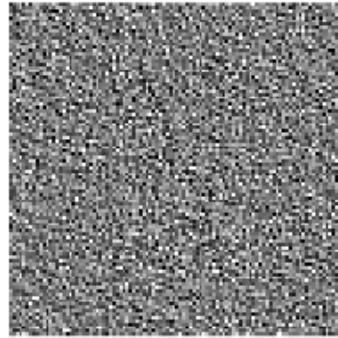
(a)



(b)



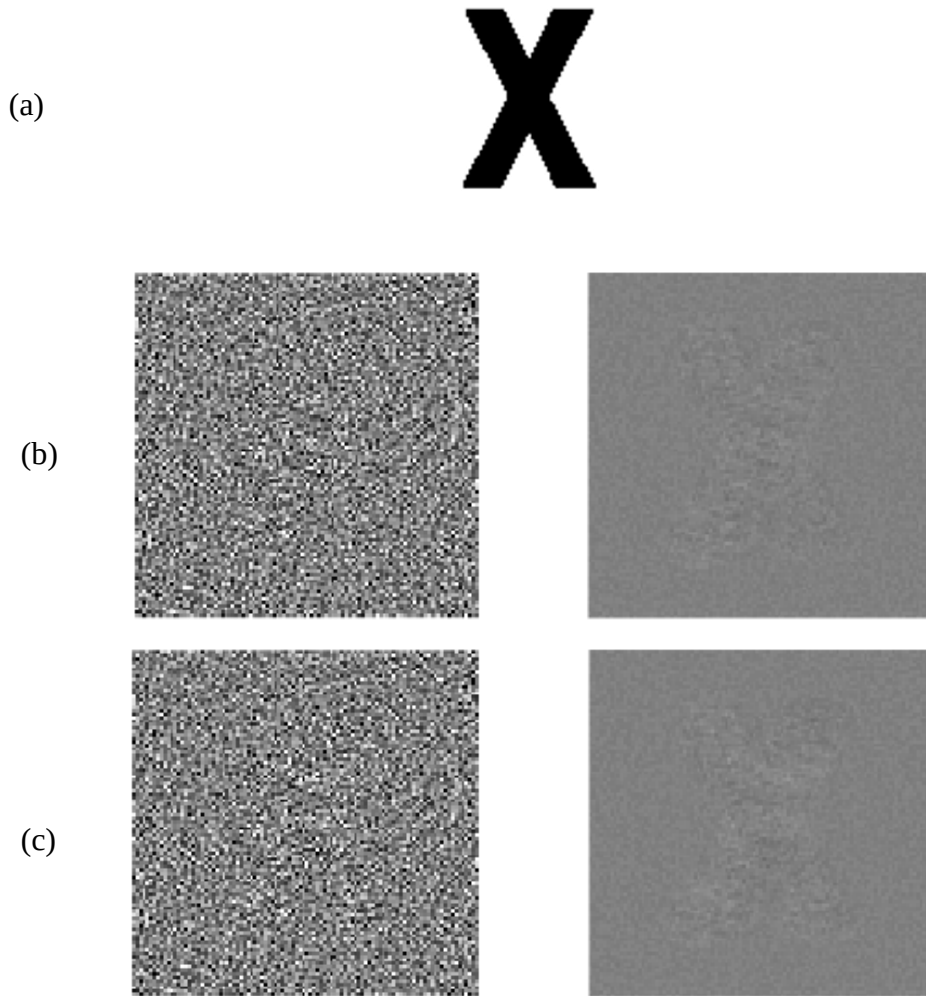
(c)



36 pav. Slaptos informacijos slėpimas dvimatėse muaro gardelėse: slaptos informacijos vaizdas (a), slaptas vaizdas dvimatėje statinėje (kairėje) ir laike vidurkintoje (dešinėje) muaro gardelėje, kai antroji gardelė sudaryta optimizuojant su $[-50;50]$ korekcijomis (b) ir $[-85;85]$ korekcijomis (c). F_1 optimizavimo algoritmo parametrai: amplitudė lygi 5, svyravimų kampas $\frac{\pi}{4}$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, o vaizdo dydis yra 100×100 , optimizuojamas vaizdo dydis 108×108 , nežinomų sprendinių skaičius $108^2 = 11664$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, tikslo funkcijos koeficientų reikšmės: $k_1 = 100$, $k_2 = k_3 = 1$. F_2 optimizavimo algoritmo parametrai: $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 250, populiacijos dydis – 500 dalelių, tikslo funkcijos koeficientų reikšmės: $k_1 = 1$, $k_2 = k_3 = 1$

36 pav. matoma, kad vizualiai ryškesnis atkoduojamas vaizdas gaunamas, kai antrosios gardelės optimizavimas atliekamas su pirmosios gardelės korekcijomis $[-85;85]$ intervale (**36 pav.** (c)), nei $[-50;50]$ intervale (**36 pav.** (b)). Tai rodo ir standartinio nuokrypio reikšmės: laike vidurkintame vaizde foną koduojančios gardelės standartinis nuokrypis yra nuokrypis $\bar{\sigma}^{(1)} = 3.84$. Slaptą informaciją koduojančios laike vidurkintos gardelės standartinis nuokrypis turi būti kuo didesnis. Kai ši gardelė sudaroma naudojant $[-50;50]$ korekcijų ribas, $\bar{\sigma}^{(2)} = 4.87$. Kai gardelė sudaroma naudojant $[-85;85]$ korekcijų ribas, $\bar{\sigma}^{(2)} = 6.39$. Taigi, geresni informacijos slėpimo rezultatai gaunami, kai antroji gardelė optimizuojama naudojant $[-85;85]$ korekcijų ribas.

Tie patys skaičiavimai atliekami gardelei svyruojant pagal elipsinį dėsnį. Antrosios gardelės optimizavime naudojamos pirmosios gardelės korekcijos šiuose intervaluose: $[-35;35]$ ir $[-50;50]$. **37 pav.** pateikiami informacijos slėpimo rezultatai.

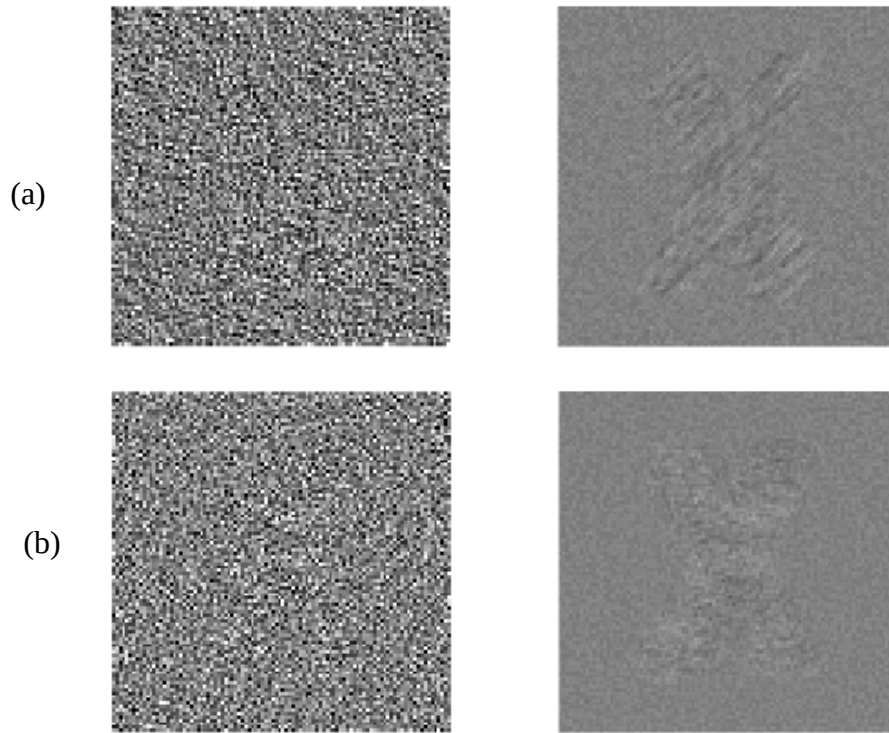


37 pav. Slaptos informacijos slėpimas dvimatėse muaro gardelėse: slaptos informacijos vaizdas (a), slaptas vaizdas optimizuotoje dvimatėje statinėje (kairėje) ir laike vidurkintoje (dešinėje) muaro gardelėje, kai antroji gardelė sudaryta optimizuojant su $[-35;35]$ korekcijomis (b) ir $[-50;50]$ korekcijomis (c). F_1 optimizavimo algoritmo parametrai: elipsinių svyravimų amplitudės lygios 5 ir 3, iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, o vaizdo dydis yra 100×100 , optimizuojamas vaizdo dydis 110×110 , nežinomų sprendinių skaičius $110^2 = 12100$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, tikslo funkcijos koeficientų reikšmės: $k_1 = 100$, $k_2 = k_3 = 1$. F_2 optimizavimo algoritmo parametrai: $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 300, populiacijos dydis – 300 dalelių, tikslo funkcijos koeficientų reikšmės: $k_1 = 1$, $k_2 = k_3 = 1$.

Kai gardelės svyravimai elipsiniai, antrajai gardelei optimizuoti tinkamesnės yra pirmosios gardelės korekcijos didesniame intervale, t.y. $[-50;50]$, nei mažesniame $[-35;35]$. Laike vidurkintos gardelės, koduojančios slapto vaizdo foną (pirmoji gardelė), reikšmių standartinis nuokrypis $\bar{\sigma}^{(1)} = 2.75$. Slaptą informaciją koduojančios laike vidurkintos gardelės standartinis nuokrypis turi būti kuo didesnis. Kai ši gardelė sudaroma naudojant $[-35;35]$ korekcijų ribas, $\bar{\sigma}^{(2)} = 4.96$. Kai gardelė

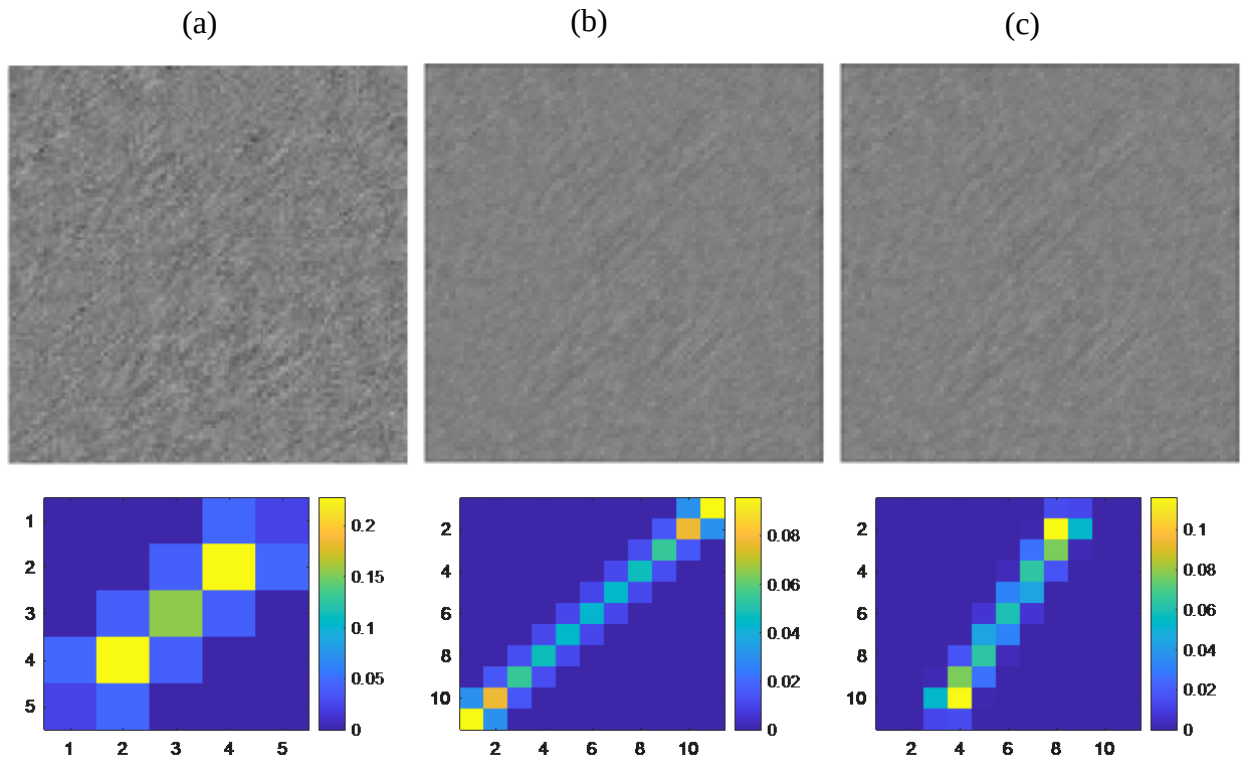
sudaroma naudojant $[-50;50]$ korekcijų ribas, $\overline{\sigma}^{(2)} = 5.32$. Taigi, geresni informacijos slėpimo rezultatai gaunami, kai antroji gardelė optimizuojama naudojant $[-50;50]$ korekcijų ribas.

Taigi, galutiniuose rezultatuose (**38 pav.**) pateikiamas informacijos slėpimas, kai užkoduota gardelė yra judinama harmoniniais ir elipsiniais svyravimais atitinkamai su antrosios gardelės korekcijų ribomis: $[-85;85]$ ir $[-50;50]$.



38 pav. Informacijos slėpimo rezultatai: užkoduotos informacijos vaizdas (kairėje) ir atkoduotos informacijos vaizdas (dešinėje), kai dvimatė stochastinė gardelė svyruoja harmoniniais svyravimais su amplitudė 5 (a) ir elipsiniais svyravimais su amplitudėmis 5 ir 3 (b). F_1 optimizavimo algoritmo parametrai: iteracijų skaičius 1000, populiacijos dydis – 600 dalelių, o vaizdo dydis yra 100×100 , optimizuojamas vaizdo dydis 110×110 , nežinomų sprendinių skaičius $110^2 = 12100$, sprendinių reikšmių ribos $[0;255]$, $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, tikslo funkcijos koeficientų reikšmės: $k_1 = 100$, $k_2 = k_3 = 1$. F_2 optimizavimo algoritmo parametrai: $\kappa = 0.8$, $c = 4.1$, inercijos koeficientas $\chi = 0.5839$, inercijos slopinimo koeficientas $w = 1$, iteracijų skaičius 250 (b) ir 300 (c), populiacijos dydis – 250 (b) ir 300 (c) dalelių, tikslo funkcijos koeficientų reikšmės: $k_1 = 1$, $k_2 = k_3 = 1$.

Gauti rezultatai parodo, kad informacijos slėpimas ir atkodavimas yra galimas naudojant dvimates stochastines muaro gardeles. Atkodavimas vykdomas atliekant konkrečius gardelės svyravimus su tam tikra svyravimų amplitudė ir kryptimi. Jeigu svyravimai atliekami ne ta kryptimi, arba ne ta amplitudė, informacijos atkoduoti neįmanoma. Atkoduotas vaizdas, kai parenkami kiti parametrai, nei panaudoti vaizdo užkodavime, pateiktas **39 pav.**, kuriame slapta informacija beveik nematoma. Atkodavimui sukurama nauja transformacijos matrica su kitais parametrais (svyravimų amplitudės ar krypties), nei buvo naudojami gardelės užkodavime. Užkodavime naudotos matricos grafinė iliustracija pateikta **11 pav.**, o atkodavime naudojamos matricų iliustracijos pateiktos **39 pav.** antroje eilutėje.



39 pav. Informacijos atkodavimo vaizdai (pirmoje eilutės) ir jų transformacijos operatorių vaizdai (antroje eilutėje), kai naudojami šie vidurkinimo parametrai: $a = 2, \alpha = \frac{\pi}{4}$ (a), $a = 7, \alpha = \frac{\pi}{4}$ (b) ir $a = 5, \alpha = \frac{\pi}{3}$ (c).

Informacijos slėpimas pradinėje gardelėje atliktas su šiais vidurkinimo parametrais: $a = 5, \alpha = \frac{\pi}{4}$.

Slapta informacija negali būti atkoduojama, jeigu nėra naudojami tie patys vidurkinimo parametrai, kokie buvo naudojami informacijos užkodavime, kaip parodyta **39 pav.** Ši dinaminės vizualinės kriptografijos schema savybė parodo, kad pasiūlyta informacijos slėpimo schema dvimatėse stochastinėse muaro gardelėse gali būti naudojama slaptai informacijai paslėpti. Kadangi šioje schemoje yra naudojamas didesnis parametrų kiekis, ji gali būti laikoma saugesne informacijos slėpimo schema, nei vienmatės muaro gardeles naudojanti schema [32].

Išvados

1. Bet kurio taško ryškumas laike vidurkintoje dvimatėje gardelėje priklauso nuo kaimyninių taškų ryškumo reikšmių ir gali būti apskaičiuotas panaudojant vidurkinimo transformacijos operatorių. Vidurkinimo transformacijos operatorius yra matrica, kurios formatas ir reikšmės priklauso nuo svyravimų dėsnio (harmoninis, elipsinis) bei parametrų (svyravimo kampas, amplitudė). Kuo didesnė svyravimų amplitudė, tuo didesnis vidurkinimo operatoriaus formatas. Jeigu dvimatė gardelė svyruoja kaip nesideformuojantis kūnas, tai vidurkinimo operatorius bet kuriam vaizdo taškui yra vienas ir tas pats. Visų laike vidurkinto vaizdo taškų ryškumą vienu metu galima apskaičiuoti panaudojus vidurkinimo matricą, kurioje tam tikra tvarka yra išdėstytos atskiros vidurkinimo operatoriaus eilutės.
2. Dvimatė stochastinė muaro gardelė, skirta fonui užkoduoti, stacionarioje būsenoje turi būti kuo margsnė, o suvidurkinta laike - kuo pilkesnė. Dvimatė stochastinė muaro gardelė, skirta slaptai informacijai užkoduoti, stacionarioje būsenoje turi būti kuo panašesnė į fonui koduoti skirtą gardelę. Slaptai informacijai koduoti skirta dvimatė stochastinė muaro gardelė vidurkintoje būsenoje turi kuo labiau skirtis nuo laike vidurkintos fonui koduoti skirtos gardelės (t.y. slaptai informacijai koduoti naudojama gardelė, suvidurkinus ją laike, turi būti kuo margsnė).
3. Optimalioms dvimatėms stochastinėms muaro gardelėms generuoti yra sukonstruotos specialios tikslo funkcijos. Pastebėta, kad slaptai informacijai koduoti skirtą gardelę tikslinga generuoti kaip optimaliai pakoreguotą fono kodavimui skirtą gardelę. Geriausi rezultatai gauti, kai fono kodavimui skirtai gardelei optimizuoti naudojamos tikslo funkcijos koeficientai yra tokie: $k_1 = 100$, $k_2 = 1$, $k_3 = 1$, o antrosios gardelės optimizavimui naudojamos tikslo funkcijos koeficientai yra tokie: $k_1 = 1$, $k_2 = 1$, $k_3 = 1$, $k_4 = 1$. Šioms funkcijoms optimizuoti parinktas dalelių spiečiaus optimizavimo algoritmas. Kai optimizuojamos gardelės svyravimai ne didesni nei 7 procentai jos dydžio, optimaliai informaciją slepiančiai gardelei, sugeneruoti prireikė 500 dalelių ir 250 iteracijų. Optimaliai foną koduojančiai stochastinei gardelei, sudarančiai 30x30 taškų, sugeneruoti prireikė 600 dalelių ir 700 iteracijų, gardelei, sudarytai iš 100x100 taškų, sugeneruoti prireikė 600 dalelių ir 1000 iteracijų.
4. Vizualiai atkoduoto slapto vaizdo ir fono kontrastas yra didesnis tuo atveju, kai stochastinėms gardelėms generuoti ir slaptai informacijai užkoduoti yra naudojami harmoniniai virpesiai, tačiau skirtumas tarp laike vidurkinto vaizdo ir fono standartinių nuokrypių yra 0.02 vienetais didesnis, kai slaptai informacijai užkoduoti yra naudojamos stochastinės gardelės, sugeneruotos taip, kad būtų virpinamos pagal elipsinį dėsnį. Tiek fono, tiek ir slaptos informacijos užkodavimui būtina naudoti optimizuotas gardeles. Jeigu slaptos informacijos užkodavimui naudotume atsitiktinę, ne optimizuotą gardelę, užkoduotame vaizde slapta informacija bus matoma tiesiog plika akimi. Rezultatai parodė, kad atkodavimas įmanomas tik tada, kai užkodavimui ir atkodavimui naudojami vidurkinimo parametrai (svyravimų amplitudė ir kryptis) yra tokie patys. Jeigu atkoduoti bandoma su kitokiais parametrais, slapta informacija yra beveik nematoma.

Literatūros sąrašas

1. SPEIER, H. The Communication of Hidden Meaning. *Social Research*, 1977, 44(3), 471–501. Prieiga per internetą: <http://www.jstor.org/stable/40970295>
2. KAHN, D. The history of steganography. In: *Anderson, R. (eds) Information Hiding. Lecture Notes in Computer Science*, 1996, 1174. Prieiga per: doi:10.1007/3-540-61996-8_27
3. RAHMAN S. A Comprehensive Study of Digital Image Steganographic Techniques. *IEEE*, 2023, vol. 11, pp. 6770-6791. Prieiga per: doi: 10.1109/ACCESS.2023.3237393.
4. VAIDELYS, Martynas. *Self-organizing patterns in information hiding applications: daktaro disertacija* [interaktyvus]. Kauno technologijos universitetas, 2018. Prieiga per: <https://epubl.ktu.edu/object/elaba:30765661/>
5. ALTAAY, A. A. J., SAHIB, S. B., ZAMANI, M. An introduction to image steganography techniques. In: *2012 international conference on advanced computer science applications and technologies (ACSAT)*. *IEEE*, 2012, 122-126. Prieiga per: doi: 10.1109/ACSAT.2012.25.
6. CHANDRA, S. A comparative survey of symmetric and asymmetric key cryptography. In: *2014 international conference on electronics, communication and computational engineering (ICECCE)*. *IEEE*, 2014, 83-93. Prieiga per: doi: 10.1109/ICECCE.2014.7086640.
7. CHEDDAD, A. Digital image steganography: Survey and analysis of current methods. *Signal processing*, 2010, 90(3), 727-752. Prieiga per: doi.org/10.1016/j.sigpro.2009.08.010.
8. ZIELINSKA, E., MAZURCZYK, W., SZCZYPIORSKI, K. Trends in Steganography. *Communications of the ACM*, 2014, 57(3), 86-95. Prieiga per: doi:10.1145/2566590.2566610
9. WEIR, J., YAN, W. *Visual Cryptography and Its Applications*, 2012. ISBN 978-87-403-0126-7.
10. ABOUD, G., MAREAN, J., YAMPOLSKIY, R. V. Steganography and visual cryptography in computer forensics. In: *2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*. *IEEE*, 2010, 25-32. Prieiga per: DOI: [10.1109/SADFE.2010.14](https://doi.org/10.1109/SADFE.2010.14).
11. MARWAHA, P., MARWAHA, P. Visual cryptographic steganography in images. In: *2010 Second international conference on computing, communication and networking technologies*. *IEEE*, 2010, 1-6. Prieiga per: doi: 10.1109/ICCCNT.2010.5591730.
12. HARTUNG, F., KUTTER, M. Multimedia watermarking techniques. *Proceedings of the IEEE*, 1999, 87(7) 1079-1107. Prieiga per: doi: [10.1109/5.771066](https://doi.org/10.1109/5.771066)
13. BEGUM, M, UDDIN, M, S. Digital image watermarking techniques: a review. *Information*, 2020, 11(2) 110. Prieiga per: doi: [10.3390/info11020110](https://doi.org/10.3390/info11020110)
14. GHOUL, S., SULAIMAN, R., SHUKUR, Z. A review on security techniques in image steganography. *International Journal of Advanced Computer Science and Applications*, 2023, 14(6). Prieiga per: doi: [10.14569/IJACSA.2023.0140640](https://doi.org/10.14569/IJACSA.2023.0140640)
15. SUBRAMANIAN, N., ELHARROUSS, O., AL-MAADEED, S., BOURIDANE, A. Image Steganography: A Review of the Recent Advances, *IEEE Access*, 2021, 9, 23409-23423. Prieiga per: doi: 10.1109/ACCESS.2021.3053998.

16. EVSUTIN, O., MELMAN, A., MESHCHERYAKOV, R. Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions, *IEEE Access*, 2020, 8, 66589-166611. Prieiga per: doi: [10.1109/ACCESS.2020.3022779](https://doi.org/10.1109/ACCESS.2020.3022779).
17. KAUR, S., SINGH, S., KAUR, M., LEE, H. A Systematic Review of Computational Image Steganography Approaches. *Archives of Computational Methods in Engineering*, 2022, 29(3). Prieiga per: doi: [10.1007/s11831-022-09749-0](https://doi.org/10.1007/s11831-022-09749-0)
18. CHANDRAMOULI, R., MEMON, N. Analysis of LSB based image steganography techniques. In: *Proceedings 2001 international conference on image processing (Cat. No. 01CH37205)*. IEEE, 2001, 3, 1019-1022. Prieiga per: doi: [10.1109/ICIP.2001.958299](https://doi.org/10.1109/ICIP.2001.958299).
19. WAYNER, Peter, *Disappearing Cryptography and Watermarking (The Morgan Kaufmann Series in Software Engineering and Programming)*, (trečias leidimas), 337–353, Boston, 2009, ISBN: 9780080922706.
20. KURTULDU, O., ARICA, N. A new steganography method using image layers. In: *2008 23rd International Symposium on Computer and Information Sciences*. IEEE, 2008, 1-4. Prieiga per: doi: [10.1109/ISCIS.2008.4717893](https://doi.org/10.1109/ISCIS.2008.4717893).
21. HUSSAIN, M., RIAZ, Q., SALEEM, S., GHAFOR, A.. Enhanced adaptive data hiding method using LSB and pixel value differencing. *Multimedia Tools and Applications*, 2021, 80, 20381-20401. Prieiga per: doi: [10.1007/s11042-021-10652-2](https://doi.org/10.1007/s11042-021-10652-2).
22. FAKHREDANESH, M., RAHMATI, M., SAFABAKHSH, R. Steganography in discrete wavelet transform based on human visual system and cover model. *Multimedia Tools and Applications*, 2019, 78, 18475-18502. Prieiga per: doi: [10.1007/s11042-019-7238-8](https://doi.org/10.1007/s11042-019-7238-8).
23. SONI, A., JAIN, J., ROSHAN, R. Image Steganography using Discrete Fractional Fourier Transform. *2013 International Conference on Intelligent Systems and Signal Processing (ISSP)*, 2013, 97-100. Prieiga per: doi: [10.1109/ISSP.2013.6526882](https://doi.org/10.1109/ISSP.2013.6526882).
24. NAOR, M., SHAMIR, A. Visual cryptography. In: *Advances in Cryptology—EUROCRYPT'94: Workshop on the Theory and Application of Cryptographic Techniques Perugia*, 1995, 950, 1-12. Prieiga per: doi: [10.1007/BFb0053419](https://doi.org/10.1007/BFb0053419).
25. VERHEUL, E. R., VAN TILBORG, H. Constructions and properties of k out of n visual secret sharing schemes. *Designs, Codes and Cryptography*, 1997, 11, 179-196. Prieiga per: doi: [10.1023/A:1008280705142](https://doi.org/10.1023/A:1008280705142).
26. YANG, C., LAI, C. New colored visual secret sharing schemes. *Designs, Codes and cryptography*, 2000, 20, 325-336. Prieiga per: doi: [10.1023/A:1008382327051](https://doi.org/10.1023/A:1008382327051).
27. HOU, Y. Visual cryptography for color images. *Pattern recognition*, 2003, 36(7), 1619-1629. Prieiga per: [https://doi.org/10.1016/S0031-3203\(02\)00258-3](https://doi.org/10.1016/S0031-3203(02)00258-3).
28. WANG, D., YI, F., LI, X. Probabilistic visual secret sharing schemes for greyscale images and color images, *Information Sciences*, 2011, 181(11), 2189–2208. Prieiga per: <https://doi.org/10.1016/j.ins.2011.01.019>.
29. ZHAO, MY., YAN, B., PAN, JS. Quantum meaningful visual cryptography. *Quantum Inf Process*, 2023, 22(312). <https://doi.org/10.1007/s11128-023-04066-2>.

30. RAGULSKIS, M., ALEKSA, A. Image hiding based on time-averaging moiré. *Optics Communications*, 2009, 282(14) 2752-2759. Prieiga per: <https://doi.org/10.1016/j.optcom.2009.04.007>.
31. PALEVIČIUS, Paulius. *Optical interferometry based methods for investigations of dynamical processes in microsystems: daktaro disertacija* [interaktyvus]. Kauno technologijos universitetas, 2015. Prieiga per: <https://epubl.ktu.edu/object/elaba:11566131/>.
32. ITO, R., KUWAKADO, H., TANAKA, H. Image size invariant visual cryptography. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 2000, 82(10), 2172-2177, ISSN 0916-8508. Prieiga per: https://www.researchgate.net/publication/2823555_Image_Size_Invariant_Visual_Cryptography.
33. CIMATO, S., DE PRISCO, R., DE SANTIS, A. Colored visual cryptography without color darkening. In: *Security in Communication Networks: 4th International Conference, SCN 2004*. 2005, 235-248. Prieiga per: doi: [10.1007/978-3-540-30598-9_17](https://doi.org/10.1007/978-3-540-30598-9_17).
34. MOHAN, A., BINU, V. P. Quality improvement in color extended visual cryptography using ABM and PRWP. In: *2016 International Conference on Data Mining and Advanced Computing (SAPIENCE)*. IEEE, 2016, 273-278. Prieiga per: doi: [10.1109/SAPIENCE.2016.7684159](https://doi.org/10.1109/SAPIENCE.2016.7684159).
35. DAHAT, A. V., CHAVAN, P. V. Secret sharing based visual cryptography scheme using CMY color space. *Procedia Computer Science*, 2016, 78, 563-570. Prieiga per: doi: [10.1016/j.procs.2016.02.103](https://doi.org/10.1016/j.procs.2016.02.103).
36. BLUNDO, C., DE SANTIS, A., NAOR, M. Visual cryptography for grey level images. *Information Processing Letters*, 2000, 75(6) 255-259. Prieiga per: [https://doi.org/10.1016/S0020-0190\(00\)00108-3](https://doi.org/10.1016/S0020-0190(00)00108-3).
37. WANG, R.-Z., LAN, Y.-C., LEE, Y.-K., HUANG, S.-Y., SHYU, S.-J., CHIA, T.-L., Incrementing visual cryptography using random grids, *Optics Communications*, 2010, 283(21), 4242–4249. Prieiga per: doi: [10.1016/j.optcom.2010.06.042](https://doi.org/10.1016/j.optcom.2010.06.042).
38. LI, P., YANG, C.-N., KONG, Q., MA, Y., LIU, M. Sharing more information in gray visual cryptography scheme. *Journal of Visual Communication and Image Representation*, 2013, 24(8), 1380-1393. Prieiga per: <https://doi.org/10.1016/j.jvcir.2013.09.010>.
39. YAN, X., WANG, S., NIU, X., YANG, C.-N. Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality. *Digital Signal Processing*, 2015, 38, 53-65. Prieiga per: <https://doi.org/10.1016/j.dsp.2014.12.002>.
40. YANG, C.-N. YANG, Y.-Y. On the analysis and design of visual cryptography with error correcting capability. *IEEE Transactions on Circuits and Systems for Video Technology*, 2020, 31(6), 2465-2479. Prieiga per: doi: [10.1109/TCSVT.2020.3017126](https://doi.org/10.1109/TCSVT.2020.3017126).
41. EDGAR, M. P., GIBSON, G. M.; PADGETT, M. J. Principles and prospects for single-pixel imaging. *Nature photonics*, 2019, 13(1), 13-20. Prieiga per: <https://doi.org/10.1038/s41566-018-0300-7>.
42. JIAO, S., FENG, J., GAO, Y., LEI, T., YUAN, X. Visual cryptography in single-pixel imaging, *Optics Express*, 2020, 28, 7301-7313. Prieiga per: <https://doi.org/10.1364/OE.383240>.

43. IBRAHIM, D. R., ABDULLAH, R., TEH, J.S. An enhanced color visual cryptography scheme based on the binary dragonfly algorithm. *International Journal of Computers and Applications*, 2022, 44(7) 623-632. Prieiga per: <https://doi.org/10.1080/1206212X.2020.1859244>.
44. SAUNORIENE, L., SAUNORIS, M., RAGULSKIS, M. Image Hiding in Stochastic Geometric Moiré Gratings. *Mathematics* 2023, 11, 1763. Prieiga per: <https://doi.org/10.3390/math11081763>
<https://www.mdpi.com/2227-7390/11/8/1763>
45. PETRAUSKIENE, V., ALEKSA, A., FEDARAVICIUS, A., RAGULSKIS, M. Dynamic visual cryptography for optical control of vibration generation equipment. *Optics and Lasers in Engineering*, 2012, 50(6), 869-876. Prieiga per: <https://doi.org/10.1016/j.optlaseng.2012.01.013>.
46. PALIVONAITE, R., ALEKSA, A., PAUNKSNIS, A., GELZINIS, A. Image hiding in time-averaged deformable moiré gratings. *Journal of Optics*, 2014, 16(2), 025401. Prieiga per: DOI 10.1088/2040-8978/16/2/025401.
47. VAIDELYS, M., RAGULSKIENE, J., ALEKSIENE, S., RAGULSKIS, M. Image hiding in time-averaged moiré gratings on finite element grids. *Applied Mathematical Modelling*, 2015, 39(19), 5783-5790. Prieiga per: <https://doi.org/10.1016/j.apm.2015.01.056>
48. RAGULSKIS, M., ALEKSA, A. SAUNORIENE, L. Improved algorithm for image encryption based on stochastic geometric moiré and its application. *Optics communications*, 2007, 273(2) 370-378. Prieiga per: <https://doi.org/10.1016/j.optcom.2007.01.055>.
49. RAGULSKIS, M., MASKELIUNAS, R., RAGULSKIS, L., TURLA, V. Investigation of dynamic displacements of lithographic press rubber roller by time average geometric moiré. *Optics and Lasers in Engineering*, 2005, 43(9), 951-962. Prieiga per: <https://doi.org/10.1016/j.optlaseng.2004.10.004>.
50. SAUNORIENE, L., ALEKSIENE, S., MASKELIUNAS, R., RAGULSKIS, M. Image hiding scheme based on time-averaged elliptic oscillations. *Optics and Lasers in Engineering*, 2017, 98, 83-88. Prieiga per: <https://doi.org/10.1016/j.optlaseng.2017.06.009>.
51. RAGULSKIS, M., ALEKSA, A., NAVICKAS, Z. Image hiding based on time-averaged fringes produced by non-harmonic oscillations. *Journal of Optics A: Pure and Applied Optics*, 2009, 11(12) 125411. Prieiga per: doi: 10.1088/1464-4258/11/12/125411.
52. SAKYTE, E., PALIVONAITE, R., ALEKSA, A., RAGULSKIS, M. Image hiding based on near-optimal moire gratings. *Optics Communications*. ISSN 0030-4018, Elsevier. 2011, 284, 3954-3964. Prieiga per: <https://doi.org/10.1016/j.optcom.2011.04.039>.
53. SAUNORIENE, L., ragulskis, M., CAO, J. Wada index based on the weighted and truncated Shannon entropy. *Nonlinear Dyn*, 2021, 104, 739–751. Prieiga per: <https://doi.org/10.1007/s11071-021-06261-1>.
54. LU, G., SAUNORIENE, L., GELZINIS, A., PETRAUSKIENE, V., RAGULSKIS, M. Visual integration of vibrating images in time. *Optical Engineering*, 2018, 57(9), 093107-093107. Prieiga per: <https://doi.org/10.1117/1.OE.57.9.093107>.
55. PETRAUSKIENE, V., PALIVONAITE, R., ALEKSA, A., RAGULSKIS, M. Dynamic visual cryptography based on chaotic oscillations. *Communications in nonlinear science and numerical simulation*, 2014, 19(1) 112-120. Prieiga per: <https://doi.org/10.1016/j.cnsns.2013.06.002>.
56. MOLER, C., LITTLE, J. A history of MATLAB. *Proceedings of the ACM on Programming Languages*, 2020, 4, 1-67. Prieiga per: <https://doi.org/10.1145/3386331>.

57. ALEKSIENĖ, Sandra. *Vizualiosios informacijos slėpimas deformuojamosiose bei dvimatėse muaro gardelėse: daktaro disertacija*. 2019. Kauno technologijos universitetas. Prieiga per: epubl.ktu.edu.
58. PETRAUSKIENE, V., SURVILA, A., FEDARAVICIUS, A., RAGULSKIS M. Dynamic visual cryptography for optical control of chaotic oscillations. *Optics & Laser Technology, Elsevier*. 2014, 57(7), 129-135, ISSN: 0030-3992. Prieiga per: doi: [10.1016/j.optlastec.2013.10.015](https://doi.org/10.1016/j.optlastec.2013.10.015).
59. PALEVICIUS, A., JANUSAS, G., RAGULSKIS, M., PALEVICIUS, P. Design, Analysis and Application of Dynamic Visual Cryptography for Visual Inspection of Biomedical Systems. Chapter 17. NATO Science for Peace and Security Series A: Chemistry and Biology, 2018, 223-232. Prieiga per: https://doi.org/10.1007/978-94-024-1304-5_17.
60. MUNOZ-RODRÍGUEZ, J.A., RODRÍGUEZ-VERA, R. Image encryption based on moiré pattern performed by computational algorithms. *Optics Communications*, 2004, 236, 295–301. Prieiga per: <https://doi.org/10.1016/j.optcom.2004.03.089>.
61. WU, Y., ZHOU, Y., SAVERIADES, G., AGAIAN, S. Local Shannon entropy measure with statistical tests for image randomness. *Information Sciences*, 2013, 222, 323-342. Prieiga per: <https://doi.org/10.1016/j.ins.2012.07.049>.
62. MCCONNELL, B. S. Entropy: Measuring Order and Randomness. In: *The Alien Communication Handbook*, 2021, 127-132. Prieiga per: doi: https://doi.org/10.1007/978-3-030-74845-6_8.
63. SAUNORIENE, L. *Analysis and investigation of time-averaged moiré images of dynamical systems: daktaro disertacija*, 2007. Kauno technologijos universitetas.
64. GAD, A.G. Particle Swarm Optimization Algorithm and Its Applications: A Systematic Review. *Arch Computat Methods Eng*, 2022, 2531–2561. Prieiga per: <https://doi.org/10.1007/s11831-021-09694-4>.
65. KENNEDY, J, EBERHART, R. Particle swarm optimization (pso). In: *Proceedings of IEEE international conference on neural networks*, 1995, 4, 1942–1948. Prieiga per: doi: 10.1109/ICNN.1995.488968.
66. EBERHART, R., KENNEDY, J. A new optimizer using particle swarm theory. In: *MHS'95. Proceedings of the sixth international symposium on micro machine and human science. IEEE*, 39–43. Prieiga per: doi: 10.1109/MHS.1995.494215.
67. JAIN, M., SAIHPAL, V., SINGH, N., SINGH, S.B. An overview of variants and advancements of PSO algorithm. *Applied Sciences*, 2022, 12(17), 8392. Prieiga per: <https://doi.org/10.3390/app12178392>.
68. SHI, Y., EBERHART, R. A modified particle swarm optimizer. In: *1998 IEEE international conference on evolutionary computation proceedings. IEEE world congress on computational intelligence (Cat. No. 98TH8360)*. IEEE, 1998, 69-73. Prieiga per: doi: 10.1109/ICEC.1998.699146.
69. SHARMA, G., MARTIN, J. MATLAB®: a language for parallel computing. *International Journal of Parallel Programming*, 2009, 37, 3-36. Prieiga per: <https://doi.org/10.1007/s10766-008-0082-5>.