KAUNO TECHNOLOGIJOS UNIVERSITETAS

SANDRA ALEKSIENĖ

VIZUALIOSIOS INFORMACIJOS SLĖPIMAS DEFORMUOJAMOSIOSE BEI DVIMATĖSE MUARO GARDELĖSE

Daktaro disertacija
Fiziniai mokslai, Informatika (09P)

2019, Kaunas

Disertacija rengta 2013–2018 metais Kauno technologijos universiteto Matematikos ir gamtos mokslų fakultete Matematinio modeliavimo katedroje.

Mokslinis vadovas:

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

Interneto svetainės, kurioje skelbiama disertacija, adresas:
http://ktu.edu

Redagavo:

Rozita Znamenskaitė (leidykla „Technologija“)

ISBN 978-609-02-1563-0

Leidinio bibliografinė informacija pateikiama Lietuvos nacionalinės Martyno Mažvydo bibliotekos Nacionalinės bibliografijos duomenų banke (NBDB).

TURINYS

ŽENKLŲ, SIMBOLIŲ IR SANTRUMPŲ SĄRAŠAS 5
ĮVADAS 6
1. LITERATŪROS APŽVALGA 8
1.1. Muaro optiniai efektai 8
1.2. Geometrinio muaro taikymai 9
1.3. Tiesinės muaro gardelės 10
1.4. Optinės iliuzijos 11
1.5. Vizualioji kriptografija 14
1.6. Laike vidurkintas geometrinis muaras 16
1.7. Dinaminė vizualioji kriptografija 16
1.7.1. Vienmatė muaro gardelė 16
1.7.2. Nedeformuojamoji muaro gardelė 17
1.7.3. Vaizdo slėpimo schemos įgyvendinimas 19
1.8. Pirmojo skyriaus išvados ir apibendrinimas 21
2. DEFORMUOJAMOJI MUARO GARDELĖ 23
2.1. Optimalaus muaro gardelės periodo parinkimas dinaminės vizualiosios kriptografijos uždaviniuose 23
2.1.1. Optimalaus muaro gardelės periodo parinkimas, kai muaro gardelė yra harmoninė 23
2.1.2. Optimalaus muaro gardelės periodo parinkimas, kai muaro gardelė yra stačiakampė 27
2.2. Deformuojamosios muaro gardelės pritaikymas dinaminei vizualiajai kriptografijai 30
2.2.1. Deformuojamoji muaro gardelė tiesinio deformacijų lauko atveju 30
2.2.2. Deformuojamoji muaro gardelė netiesinio deformacijų lauko atveju 32
2.2.3. Dinaminė vizualioji kriptografija, pagrįsta deformuojamosiomis muaro gardelėmis, remiantis baigtinių elementų metodu 34
2.3. Deformuojamoji Ronči tipo muaro gardelė 38
2.4. Deformuojamoji muaro gardelė su nulinėmis zonomis 44
2.5. Dinaminė vizualioji kriptografija chaotinėse baigtinių elementų gardelėse 46
2.5.1. Harmoniniai svyravimai ir deformuojamoji muaro gardelė 46

2.5.2. Chaotiniai svyravimai ir nedeformuojamoji muaro gardelė 47
2.5.3. Chaotiškai svyruojančios deformuojamosios muaro gardelės optiniai efektai 49
2.5.4. Dinaminė vizualioji kriptografija, pagrįsta chaotiškai svyruojančia deformuojamąja muaro gardele 53
2.5.5. Chaotinės dinaminės vizualiosios kriptografijos eksperimentiniai tyrimai ..63
2.6. Antrojo skyriaus išvados 65
3. DVIMATĖ MUARO GARDELĖ: NEDEFORMUOJAMAS KŪNAS.....66
3.1. Vaizdo slėpimo schema, pagrįsta laike vidurkintais elipsiniais svyravimais 66
3.1.1. Dvimatė muaro gardelė 66
3.1.2. Dvimatės muaro gardelės vienkrypčiai svyravimai.....67
3.1.3. Dvimatė kryžminė gardelė elipsinių svyravimų atveju 69
3.1.4. Vaizdo slėpimas dvimatėje kryžminėje gardelėje 70
3.2. Šifruotų vaizdų dekodavimo eksperimentinis stendas kryžminės dvimatės muaro gardelės atveju 74
3.3. Apskritiminis geometrinis muaras.....77
3.4. Šifruotų vaizdų dekodavimo eksperimentinis stendas apskritiminės muaro gardelės atveju 80
3.5. Trečiojo skyriaus išvados 83
BENDROSIOS IŠVADOS.....84
LITERATŪRA.....85
MOKSLINIŲ PUBLIKACIJŲ DARBO TEMA SĄRAŠAS.....91

ŽENKLŲ, SIMBOLIŲ IR SANTRUMPŲ SĄRAŠAS

MOEMS – mikro–opto–elektromechaninės sistemos;
CGH – kompiuteriu generuotos hologramos;
STEM – skenuojamoji elektroninė mikroskopija;
$F(x)$ – vienmatės muaro gardelės spalvos intensyvumas;
T – ekspozicijos laikas;
λ – muaro gardelės periodas horizontaliąja kryptimi;
ω – harmoninių virpesių dažnis;
φ – fazė;
A – pastovioji virpesių amplitudė;
x – išilginė koordinatė;
J_0 – pirmojo tipo nulinės eilės Beselio funkcija;
r_i – i-toji pirmojo tipo nulinės eilės Beselio funkcijos šaknis;
$F(x,t)$ – deformuojamoji muaro gardelė;
$a(x)$ – deformacija pagal tikrinę formą;
$u(x,t)$ – funkcija, aprašanti muaro gardelės nuokrypį nuo pusiausvyros padėties taške x laiko momentu t;
S – standartinis nuokrypis;
σ_s – atkoduoto vaizdo pilkio tonų standartinis nuokrypis slaptosios informacijos zonoje;
σ_b – atkoduoto vaizdo pilkio tonų standartinis nuokrypis fono zonoje;
δ – slenkstis;
$u(t)$ – trikampė bangos formos svyravimų funkcija;
$F(x,y)$ – dvimatės muaro gardelės spalvos intensyvumas;
μ – muaro gardelės periodas vertikaliąja kryptimi.

ĮVADAS

Dinamine vizualiąja kriptografija paremtos skaitinių vaizdų kodavimo schemos gali būti taikomos įvairiuose mokslo ir inžinerijos uždaviniuose. Žmogaus regos sistemos gebėjimas vidurkinti greitai svyruojančių objektų vaizdus laike gali būti taikomas regos sistemos specifinių ligų nustatymui, žmogaus nuovargio identifikavimui, techninių sistemų optinei diagnostikai [1]. Antra vertus, šios slaptų vaizdų kodavimo schemos turi gana didelį taikymo potencialą MOEMS (mikro–opto–elektromechaninėse sistemose) [2]. Tačiau, formuojant CGH (kompiuteriu generuotų hologramų) optinį fazių profilį, būtina įvertinti, kad projektavimo plokštumoje virpantis vaizdas atsispindi nuo deformuojamo MOEMS elemento. Taigi visi iki šiol pasiūlyti dinamine vizualiąja kriptografija paremti skaitinių vaizdų slėpimo algoritmai yra netinkami, kai šviesos srautas atsispindi nuo deformuojamo kūno paviršiaus. Šios disertacijos pagrindinis tikslas – sukurti teorinius pagrindus ir sukonstruoti atitinkamus algoritmus, leidžiančius modeliuoti dinaminės vizualiosios kriptografijos optinius efektus deformuojamosiose bei dvimatėse muaro gardelėse.

Tyrimo objektas

1. Dinamine vizualiąja kriptografija paremtų skaitinių vaizdų slėpimo algoritmų sudarymas deformuojamosiose harmoninėse muaro gardelėse.
2. Dinamine vizualiąja kriptografija paremtų skaitinių vaizdų slėpimo algoritmų sudarymas deformuojamosiose chaotinėse muaro gardelėse.
3. Dinamine vizualiąja kriptografija paremtų skaitinių vaizdų slėpimo algoritmų sudarymas dvimatėse kryžminėse muaro gardelėse.

Tyrimo tikslas

Sukurti dinaminės vizualiosios kriptografijos principais pagrįstas skaitinių vaizdų slėpimo metodikas deformuojamosiose bei dvimatėse muaro gardelėse.

Tyrimo uždaviniai

Darbo tikslui pasiekti yra iškelti tokie uždaviniai.

1. Sukonstruoti dinaminės vizualiosios kriptografijos schemą deformuojamosiose muaro gardelėse ir pritaikyti šią schemą skaitinių vaizdų slėpimui baigtiniais elementais aprašomose gardelėse.
2. Pritaikyti dinaminės vizualiosios kriptografijos, pagrįstos skaitinių vaizdų slėpimu, schemą chaotinių virpesių atveju.
3. Sukonstruoti skaitinių vaizdų slėpimo schemą dvimatėse kryžminėse muaro gardelėse.
4. Sukonstruoti stendus pristatomų skaitinių vaizdų slėpimo algoritmų eksperimentiniam verifikavimui.

Tyrimų metodika

Deformuojamųjų dvimačių stochastinių muaro gardelių parametrų nustatymo uždaviniai, slapto vaizdo kodavimo bei dekodavimo algoritmai konstruojami ir sprendžiami MATLAB programinėje aplinkoje. Baigtiniais elementais aprašomų deformuojamųjų kūnų paviršiaus dinamikos uždaviniai sprendžiami pasitelkiant

COMSOL programą. Optimalūs modelių parametrai nustatomi taikant apytikslius analitinius metodus.

Darbo mokslinis naujumas ir praktinė reikšmė

1. Darbe pasiūlyti nauji dinaminės vizualinės kriptografijos metodai, kai deformuojama muaro gardelė svyruoja pagal tam tikrą tikrinę formą harmoniškai bei chaotiškai. Šių naujų metodų detalus išnagrinėjimas atveria galimybes taikyti pasiūlytus metodus mikro–opto–elektromechaninių sistemų optinei kontrolei.
2. Svarbiausias šios disertacijos mokslinio naujumo elementas yra dinaminės vizualiosios kriptografijos realizavimas dvimatėse baigtinių elementų gardelėse. Iki šiol žinomuose darbuose dinaminės vizualiosios kriptografijos principu pagrįstas vaizdų slėpimo algoritmas buvo paremtas laike vidurkintų muaro juostų formavimusi vienmatėse muaro gardelėse. Vaizdų kodavimo algoritmų pritaikymas dvimatėms gardelėms smarkiai išplečia pristatomų algoritmų taikymo sritis – tai ir sudaro šios disertacijos praktinę reikšmę.

Darbo rezultatų aprobavimas

Disertacijos tema paskelbti 8 moksliniai straipsniai, iš jų 4 straipsniai Mokslinės informacijos instituto (ISI) pagrindinio sąrašo leidiniuose su citavimo indeksu, 3 straipsniai pristatyti tarptautinėse mokslinėse konferencijose ir atspausdinti konferencijų pranešimų medžiagoje.

Disertacijos struktūra

Disertaciją sudaro įvadas, 3 pagrindiniai skyriai, išvados, literatūros šaltinių sąrašas. Disertacijos apimtis – 92 puslapiai. Disertacijos pagrindinėje dalyje yra 66 paveikslai ir 98 šaltinių cituojamos literatūros sąrašas.

1. LITERATŪROS APŽVALGA

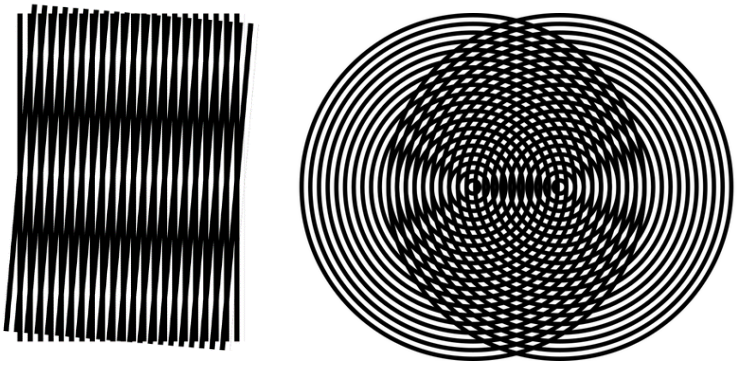
1.1. Muaro optiniai efektai

Žodis „moiré“ yra kilęs iš žodžio „mohair“ – tai audinio, pagaminto iš plonos angorinės ožkos vilnos, rūšis. Audėjai pastebėjo, kad ant šio tipo audinio drabužių matomos keistos ir besikeičiančios juostos.

Taigi muaro interferencines juostas galima pastebėti uždėjus vieną ant kito peršviečiamus panašaus rašto piešinius ar audinius. Kaip ir iš angoros vilnos audinių gauti raštai, geometriniai raštai (tokie kaip apskritimai, lygiagrečios ir radialinės linijos) taip pat suformuoja interferencines juostas, kai sudedami keli šių raštų sluoksniai.

Geometrinis muaras – tai klasikinė optinė eksperimentinė metodika, pagrįsta vizualių raštų susidarymu, kai sudedamos viena ant kitos dvi taisyklingos gardelės, kurios geometriškai interferuoja [3-5]. Gardelės viena ant kitos gali būti uždėtos taikant dvigubos ekspozicijos fotografiją, atspindžio bei šešėlinio muaro metodus, taip pat tiesiogiai uždėjus vieną ant kitos abi gardeles [6, 7]. Muaro metodai taikomi įvertinti tokiems kintamiesiems kaip poslinkiai, kreivumas, pasisukimas bei įtempimas tam tikrame plote. Plokštuminis muaro metodas (angl. *in-plain moiré*) paprastai susijęs su vienodų, lygiagrečių linijų gardelėmis, atspausdintomis ant nagrinėjamo kūno paviršiaus [4, 6].

1.1 paveiksle pavaizduotas geometrinio muaro efektas – sudėjus vieną ant kito du lygiagrečių linijų masyvus arba dvi apskritimines gardeles, susidaro muaro interferencinės juostos.



1.1 pav. Geometrinio muaro efekto iliustracija [8]

Muaro raštų susidarymą galima įgyvendinti naudojantis įvairia programine įranga. G. Cloud aprašė [9], kaip, naudojantis vektorinės grafikos programine įranga, galima sugeneruoti įvairias gardeles ir jomis manipuliuojant išgauti įdomius muaro efekto vaizdus. Jis išsamiai apibūdino programos *CorelDraw* galimybes generuoti muaro gardeles ir apžvelgė standartines funkcijas, taikomas muaro gardelių pasukimui, ištempimui bei kitoms gardelių deformacijoms [9].

Muaro raštų tyrimuose galima pastebėti du pagrindinius tikslus. Pirmasis tikslas – tai eksperimentiškai gautų muaro raštų analizė, paremta postūmiais ar įtempimais muaro interferencinių juostų centruose. Antrasis tikslas – muaro raštų sintezė, kai reikia

sugeneruoti tam tikrą iš anksto nustatytą muaro raštą [10]. Sintezės proceso metu iš dviejų vaizdų gaunamos reikiamos muaro interferencinės juostos, kai pradiniai du vaizdai yra sudedami vienas ant kito. Iš anksto nustatomos sąlygos, užtikrinančios reikalingo muaro rašto išryškėjimą, tačiau šios sąlygos nenusako pradinių dviejų vaizdų. Tam tikri kriterijai, išsprendžiantys šią problemą muaro raštų sintezės analizėje, pasiūlyti [11]. Muaro efektai taip pat taikomi tokiose srityse kaip interferometrija [12, 13], muaro deflektometrija [14-17], muaro topografija [18-20], steganografija [21], navigacija, klastotės prevencija [22], mikroskopija [23, 24].

Mokslinius straipsnius, kuriuose nagrinėjamos muaro interferencinės juostos, galima skirstyti į tris dalis.

1. Tikslingai generuojamos muaro interferencinės juostos, turint tikslą sukurti norimą piešinį. Kaip tipinį pavyzdį galima pateikti projektuotojo kuriamų muaro raštų struktūras, pritaikomas architektūroje [25].
2. Muaro interferencinės juostos atsiranda kaip šalutinis, nepageidaujamas reiškinys ir ieškoma būdų, kaip jas pašalinti [26-28].
3. Iš eksperimentiniais tyrimais gautų muaro juostų vaizdo bandoma spręsti apie stebimo kūno deformacijas [29].

1.2. Geometrinio muaro taikymai

Geometrinio muaro metodai plačiai taikomi optinėje metrologijoje. Čia galima paminėti daugybę įvairiausių taikymų, pradedant nuo mikroskopinių kūnų deformacijų matavimų, baigiant profilometrijos taikymais biomedicinoje.

A. Pofelski su bendraautoriais tyrė dvimačių deformacijų atvaizdavimą remiantis skenuojamąja elektronine mikroskopija (STEM), muaro interferometrija ir geometrinės fazės analizės algoritmais. Šiame straipsnyje teoriškai ir eksperimentiškai aprašoma, kaip pagaminti ir interpretuoti muaro hologramas, sugeneruotas iš STEM skenuojančiųjų gardelių ir kristalinių gardelių. STEM muaro interferometrija, sujungta su geometrinės fazės analizės metodu, yra lengvai įgyvendinamas ir greitas metodas, padedantis gauti santykinius deformacijų žemėlapius su dideliais matomumo laukais (iki kelių mikrometrų) [30].

Y. Tang su bendraautoriais pritaikė projekcinio muaro sistemą trimatės formos geometrijai įvertinti. Kadangi sistemos matavimo tikslumui įtaką daro daug parametrų, reikalingas tikslus projekcinio muaro sistemos kalibravimas [31].

Muaro technikų taikymas matuojant dažnai apima muaro interferencinių juostų padėties nustatymą. Dėl interferencinių juostų intensyvumo kitimo šiuose matavimuose dažnai pasitaiko klaidų. M. Abolhassani pasiūlė formuoti muaro interferencines juostas remiantis erdviniu vidurkinimu [32].

Geometrinė mikromuaro metodika, paremta klasikinio geometrinio muaro metodo ir mikroskopijos principais, yra pristatyta [7]. Geometrinio muaro principai pritaikyti biologinių sistemų mikrodeformacijų matavimui aprašyti [33]. Mechaninės trinties kontrolės metodas atominiame lygyje, pagrįstas geometrinio muaro raštais, susiformuojančiais tarp grafeno sluoksnio ir palaikančiojo kristalo gardelės, pristatytas darbe [34].

P. Pochet ir kiti tyrė van der Waals deformacijas dvimatėse medžiagose. Šios deformacijos yra susijusios ir su įtempimais, ir su muaro raštų posūkiais [35]. Muaro interferencinių juostų susidarymas Mandelbroto orbitų raštuose yra analizuojamas [36].

Femtosekundinio lazerio panaudojimas mikromuaro gardelėms formuoti yra aptartas [37]. Dvimačių Ronči tipo gardelių panaudojimas muaro raštams formuoti yra pristatytas [38]. Elektronų pluoštų generuojamų muaro raštų formavimo metodas aptartas [39]. Virtualiųjų laukų metodas muaro interferometrijos taikymuose medžiagų parametrų indentifikavimo uždaviniams yra pristatytas [40].

Mikro–elektro–mechaninių struktūrų deformacijų matavimas modifikuotu skaitmeniniu muaro metodu aptartas [41]. Polimerų temperatūrų matavimo metodas, pagrįstas fazės žingsnio šešėliniu muaru pristatytas šiame straipsnyje [42]. Muaro juostų išlyginimo metodas mikrolitografijos taikymuose pasiūlytas [43].

Trimačio veido atpažinimo technologija, pagrįsta šešėliniu muaru, pristatyta [44]. Naujas metodas mikro–nano periodinių struktūrų charakterizavimui, paremtas mikroskopine muaro technika, pasiūlytas [45]. Trimačio muaro raštų apdorojimas neraiškiaisiais neuroniniais tinklais žmogaus veido bruožų atpažinimui pristatytas [46].

L. Kunyang ir kiti tyrė spalvotas muaro interferencines juostas, susidarančias dėl vienodo gylio tiesinio Fresnel objektyvo (EDLFL) ir skystųjų kristalų ekranų (LCD) superpozicijos. Jų pasiūlyta schema efektyviai pašalina muaro interferencines juostas iš monitorių, turinčių refrakcines optines plėveles su kvaziperiodinėmis struktūromis [47].

1.3. Tiesinės muaro gardelės

Tiesinė muaro gardelė – „mušimo“ efekto vizualinis pavyzdys, kai dvi tiesinės gardelės, turinčios skirtingus periodus, sudedamos viena ant kitos. Jei vienos gardelės periodas yra λ_1, o kitos gardelės periodas λ_2, tai gautų muaro interferencinių juostų periodą galime paskaičiuoti pagal tokią formulę [48]:

$$\lambda_m = \frac{\lambda_1 \lambda_2}{\lambda_2 - \lambda_1}. \tag{1.1}$$

(1.1) formulė išvedama iš formulės, naudojamos „mušimo“ dažniui nustatyti, kai interferuoja dvi garso bangos $f_m = |f_1 - f_2|$. Jei tartume, kad tiesinės gardelės įstatytos vietoj sinuso ir kosinuso funkcijų, kai tamsios linijos reiškia didžiausią reikšmę, o šviesios – mažiausią, galima pastebėti, kaip susijusios tiesinės muaro gardelės su dviejų garsų sukurtu „mušimo“ dažniu.

Galima parodyti [48], kad muaro interferencinių juostų, susidarančių dėl dviejų gardelių, kurių periodai λ_1 ir λ_2, pavidalas yra tokios formos:

$$\cos\big(\phi_1(x,y) - \phi_2(x,y)\big); \tag{1.2}$$

čia $\phi_1(x,y)$ ir $\phi_2(x,y)$ – dviejų tiesinių gardelių funkcijos. Kai dvi gardelės yra sudedamos viena ant kitos 2α kampu tarp jų, gardelių funkcijos $\phi_1(x,y)$ ir $\phi_2(x,y)$ gali būti aprašytos tokiu būdu:

$$\begin{aligned} \phi_1(x,y) &= \frac{2\pi}{\lambda_1}(x\cos\alpha + y\sin\alpha); \\ \phi_2(x,y) &= \frac{2\pi}{\lambda_1}(x\cos\alpha - y\sin\alpha). \end{aligned} \tag{1.3}$$

Tada supaprastintai užrašę (1.2) sąryšyje esantį kosinuso funkcijos argumentą gauname:

$$\phi_1(x,y) - \phi_2(x,y) = \frac{2\pi}{\lambda_m} x \cos\alpha + \frac{4\pi}{\bar{\lambda}} y \sin\alpha\,; \tag{1.4}$$

čia $\bar{\lambda}$ yra periodų vidurkis [48]. Muaro interferencinių juostų centrų vietos apskaičiuojamos pagal formulę

$$\phi_1(x,y) - \phi_2(x,y) = M2\pi; \tag{1.5}$$

čia M yra interferencinės juostos numeris (sveikasis skaičius, nusakantis interferencinę juostą; pavyzdžiui, pirmosios interferencinės juostos $M = 1$). Creath ir Wyant [48] aprašo du atskirus (1.5) lygties atvejus:

- kai $\lambda_1 = \lambda_2 = \lambda$;
- kai $\alpha = 0$.

Nagrinėkime pirmąjį atvejį. Kai dviejų gardelių periodai yra vienodi, (1.1) lygtyje esantis λ_m tampa begalinis, todėl (1.5) lygties pirmasis dėmuo artės į nulį. Tokiu būdu yra eliminuojama (1.5) lygtyje esanti x komponentė, ir muaro interferencinių juostų pavidalas priklauso tik nuo komponentės y:

$$\phi_1(x,y) - \phi_2(x,y) = \frac{4\pi}{\bar{\lambda}} y \sin\alpha; \tag{1.6}$$

Matematiškai šią problemą galima išspręsti taip: kai abiejų gardelių periodai yra tokie patys, gauname, kad $\bar{\lambda}$ yra lygus λ. Įstatę (1.7) lygtį į (1.6) lygtį ir išsprendę ją interferencinių juostų centro vietose, gausime tokią lygtį:

$$M\lambda = 2y \sin\alpha. \tag{1.7}$$

1.4. Optinės iliuzijos

Optinės iliuzijos leidžia tirti žmogaus vizualinį suvokimą ir jo ribas. Yra žinomos įvairiausios optinių iliuzijų rūšys: judesio bei laiko sukeliamos iliuzijos; apšvietimo bei kontrasto iliuzijos; spalvos iliuzijos; geometrinės bei kampo iliuzijos; erdvės bei dydžio iliuzijos ir kitos. Panagrinėkime kiekvieną optinių iliuzijų rūšį atskirai.

Kaip tipines judesio ir laiko sukeliamas iliuzijas plačiau panagrinėsime šias: „Spine drift“ iliuzija, judesio sukeltas aklumas (angl. *motion induced blindness*), „Sigma motion“ iliuzija.

„Spine drift“ iliuzija. Reguliarioje statinėje gardelėje išskirta centrinė zona, kurioje sudaromųjų elementų ašys yra pasuktos 90° kampu išorinės gardelės atžvilgiu (žr. internetiniame tinklalapyje http://www.michaelbach.de/ot/mot-spineDrift/index.html). Tada stebimas centrinės gardelės dalies „plaukiojimo“ efektas, kurį sukelia akių judesiai. Šis efektas vadinamas Kitaoka „Spine drift“ iliuzija. Kadangi ši iliuzija priklauso nuo akių judėjimo, todėl skirtingi žmonės skirtingai ją mato ir suvokia. Norint aiškiau pamatyti šią iliuziją, reikėtų švelniai sukratyti planšetę ar pakratyti galvą. „Spine drift“ iliuzijos paaiškinimas yra toks: akių judėjimas sukelia judesio išblukimo efektą tinklainėje. Jei nagrinėtume mažiausio rašto elemento judesio sukeltą išblukimą, tai

kiekvienas vaizdo kontrastas smarkiai skirtųsi pagal tinklainės judesio kryptį. Kai tinklainės judesys yra ties 45°, vaizdo kontrastas labai blogas.

Judesio sukeltas aklumas. Sakykim, turime besisukantį mėlynų kryžiukų masyvą ir tris geltonus nejudančius taškus (žr. internetiniame tinklalapyje http://www.michaelbach.de/ot/mot-mib/index.html). Sukoncentravus žvilgsnį į viduryje blyksintį ir besikeičiantį raudoną arba žalią tašką, geltonieji taškai kartkartėmis dingsta: kartais vienas, kartais poromis, kartais visi trys. Tačiau iš tikrųjų šie trys geltoni taškai visada yra. Toks reiškinys vadinamas judesio sukeltu aklumu. Pakeitus fono ar kryžiukų spalvą, taškai taip pat dingsta. Judesio sukelto aklumo paaiškinimas: nuolatinis žvilgsnio fiksavimas į vieną tašką palengvina geltonų taškų išnykimą, o taško mirksėjimas ir spalvos pasikeitimas sukelia geltonų taškų pasirodymą. Šis reiškinys primena Trokslerio efektą, tačiau yra stipresnis ir labiau atsparus akių judėjimui.

Judesio sukelto aklumo iliuzija tiriama ir moksliniuose straipsniuose, susijusiuose su regos tyrimais. Thomas S. A. Wallis ir Derek H. Arnold atlikę du eksperimentus nustatė, kad judesio sukeltas aklumas nepriklauso nuo tinklainės dirginimo greičio [49]. Judesio sukelto aklumo iliuziją sąlygoja žmogaus regos sistemos funkcinė adaptacija, kurios nepastebime kasdieniame gyvenime [50].

„Sigma motion“ iliuzija. Turime sparčiai judančią gardelę (žr. internetiniame tinklalapyje http://www.michaelbach.de/ot/mot-sigma/index.html). Jeigu vestume pirštu išilgai nuo kairiojo krašto iki dešiniojo tokiu greičiu, kad visą atstumą pereitume per dvi sekundes, ir žvilgsnį sukoncentruotume ties pirštu, tai matytume ramų juostų judėjimą dešine kryptimi. Jeigu pirštu vestume atgal ir sektume akimis pirštą, tai matytume tolygų juostų judėjimą kaire kryptimi. Šiek tiek pasipraktikavus galima pakeisti juostų judėjimo kryptį ir nesinaudojant pirštu. „Sigma motion“ iliuzijos paaiškinimas: nors žmogus ir suvokia iliuzinį judesį, jo akys tolygiai seka judesį, kartkartėmis greitai judant akims nuo vieno taško prie kito. Šios iliuzijos priežastis yra greitas fazės pasikeitimas – juodos juostos tampa baltomis, o baltos tampa juodomis. Atsitiktiniai trūkčiojimai būna tik dėl kompiuteryje vykstančių procesų. Šį fenomeną „Sigma motion“ vardu pavadino J. Grüser, nors pirmas jį aprašęs buvo James Pomerantz.

Kaip tipines apšvietimo ir kontrasto iliuzijas plačiau panagrinėsime šias: „Induced grating“ iliuzija, „Craik–O'Brien–Cornsweet“ iliuzija.

„Induced grating“ iliuzija. Šiuo atveju naudojama šviesos gardelė su keturiais šviesiais–tamsiais ciklais (žr. internetiniame tinklalapyje http://www.michaelbach.de/ot/lum-inducedGrating/index.html). Paveikslo viduryje yra horizontali pilka juosta. Įsižiūrėjus į šią juostą atrodo, kad ji keičiasi iš tamsesnės į šviesesnę pagal fono gardelės fazę. Tačiau iš tikrųjų fono gardelė tik sukelia iliuziją, kad horizontali pilka juosta irgi yra gardelė, tik priešinga fono gardelei. Atlikti tyrimai [51] leidžia manyti, kad aprašytasis efektas priklauso nuo mechanizmų, vykstančių smegenų žievėje. Ryškumo fenomenas bei žmogaus regos sistemos galimybės atskirti fizikine prasme nekintančius atspindžius nuo paviršių, kurie skirtingai apšviesti, taip pat tirtas ir [52, 53] straipsniuose.

„Craik–O'Brien–Cornsweet“ iliuzija. Sakykime, kad pilkame fone matomi du tamsiai pilko atspalvio diskai ir geltonas judantis žiedas (žr. internetiniame tinklalapyje http://www.michaelbach.de/ot/lum-cobc/index.html). Judėdamas horizontalia kryptimi į dešinę, o paskui į kairę, geltonasis žiedas atsiduria ties vienu ar kitu disku taip, kad žiedo

kiaurymėje matoma disko spalva. Įdomu tai, kad žiedą pakėlus į viršų abiejų diskų spalva yra identiška (tiesa, ties kairiuoju žiedu matosi ratilas). Tačiau žiedui esant ties dešiniuoju disku kiaurymėje matosi tamsiau pilka disko spalva, kuri aiškiai skiriasi nuo fono pilkos spalvos. Žiedui esant ties kairiuoju disku, kiaurymėje besimatanti disko spalva atrodo lygiai tokia pati, kaip ir fono. „Craik–O'Brien–Cornsweet“ iliuzija parodo, kad žmogaus regos sistema neteisingai perduoda aplinkos apšviestumo lygį smegenims. Tinklainės nerviniai mazgai užkoduoja ateinantį apšvietimą per centro–aplinkos apšvietimo profilį. Tai vyksta žmogaus smegenų žievėje, todėl mes teisingai suvokiame apšviestumą.

Kaip tipines spalvos iliuzijas plačiau panagrinėkime šias: akvarelės iliuzija, raudonų braškių iliuzija.

Akvarelės iliuzija. Turime 3×3 langelių „šachmatų lentą“, kurios kiekvieno langelio linija yra vingiuota ir dviguba – nuspalvinta dviem spalvomis (oranžine ir violetine) (žr. internetiniame tinklalapyje http://www.michaelbach.de/ot/col-watercolor/index.html). Kiekvienas „šachmatų lentos“ kvadratas turi visiškai vienodą baltą foną. Tačiau tų kvadratų, kurių vidinė linija yra oranžinė, o išorinė violetinė, fono spalva atrodo šviesiai gelsva. Priešingai, kvadratų, kurių vidinė linija yra violetinė, o išorinė oranžinė, fono spalva atrodo balta. Akvarelės iliuzijos fenomeną atrado Baingio Pinna 1987 metais. Šis fenomenas pagrįstas spalvų asimiliacijos reiškiniu – šviesesnė kontūro spalva pasklinda į visą uždarą plotą.

Raudonų braškių iliuzija. Naudojamas pyragėlio su braškėmis vaizdas (žr. internetiniame tinklalapyje http://www.michaelbach.de/ot/col-strawbsNotRed/index.html). Ant šio paveikslo uždėta žalsvai mėlyna spalva, tačiau braškės atrodo vis tiek raudonos. Iš tikrųjų šiame paveiksle nėra nė vieno raudono, netgi nė vieno rausvo taško. Jeigu paslėptume didžiąją paveikslo dalį, palikdami tik kelias raudoniausiai atrodžiusias vietas, tai pamatytume, kad raudona spalva dingsta. Raudonų braškių iliuzijos paaiškinimas būtų toks: žmogus automatiškai mato braškes raudonas. Hansen su bendraautoriais įrodė [54], kad tikėjimasis tam tikru laipsniu veikia žmogaus spalvos suvokimą.

Kaip tipines geometrines ir kampo iliuzijas plačiau panagrinėkime šias: pasvirusio stalo iliuzija (angl. *tilted table illusion*), Zöllner iliuzija, Poggendorff iliuzija.

Pasvirusio stalo iliuzija. Nupieštas balansuojantis stalas, kurio viršutinė dalis yra pasvirusi nuo uždėto ant jos mėlyno svarsčio (žr. internetiniame tinklalapyje http://www.michaelbach.de/ot/ang-tiltedTable/index.html). Stalą vaizduojantys stačiakampiai subrūkšniuoti pasvirusiomis lygiagrečiomis linijomis. Nuėmus mėlynąjį svarstį nuo paveikslo paaiškėja, kad stalo pasvirimas yra iliuzinis.

Pasvirusio stalo iliuzija yra patrauklus *Zöllner iliuzijos* variantas. Šitoje iliuzijoje ilgos linijos yra lygiagrečios, nors pažiūrėjus taip neatrodo. Toks vaizdas susidaro dėl trumpų kertančiųjų linijų, kurios yra horizontalios ir vertikalios.

Poggendorff iliuzija. Dvi tiesios linijos dalys, einančios už stačiakampio, rodos, prasilenkia, nors iš tikrųjų jos jungiasi (žr. internetiniame tinklalapyje http://www.michaelbach.de/ot/ang-poggendorff/index.html). Šią iliuziją 1860 metais atrado mokslininkas J. C. Poggendorff. K. Hamburger [55] nagrinėjo įvairias geometrines optines iliuzijas esant skirtingam apšviestumui ir linijų bei fono spalvų kontrastui.

Kaip tipines erdvės ir dydžio iliuzijas plačiau panagrinėkime šias: *T* iliuzija, silueto iliuzija (angl. *silhouette illusion*).

T iliuzija. Nupiešta apversta *T* raidė, kurios vertikaliosios dalies ilgį galima pakeisti (žr. internetiniame tinklalapyje http://www.michaelbach.de/ot/sze-tIllusion/index.html). Pakeitus vertikaliosios dalies ilgį taip, kad vertikaliosios ir horizontaliosios dalies ilgiai atrodytų vienodi, galima įsitikinti, kad vertikaliąją dalį parenkame trumpesnę lyginant su horizontaliosios dalies ilgiu. K. Mikellidou ir P. Thompson [56] sukūrė *ABC* modelį (šiame modelyje *A* – anizotropija, *B* – lietimasis, *C* – susikirtimas), kuris žymiai geriau paaiškina suvokiamą linijos dydį įvairiose su linijų dydžiu susijusiose iliuzijose.

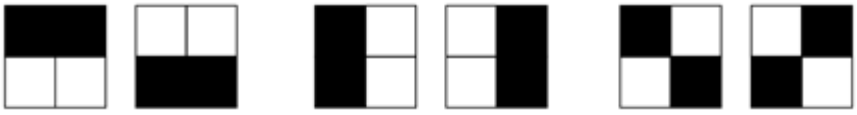
Silueto iliuzija. Šiai iliuzijai naudojamas besisukančios figūros siluetas (žr. internetiniame tinklalapyje http://www.michaelbach.de/ot/sze-silhouette/index.html). Stebint besisukantį siluetą paaiškėja įdomi savybė – sukimosi krypties šališkumas. Vieni žmonės mato besisukančią figūrą pagal laikrodžio rodyklę, kiti prieš laikrodžio rodyklę. N. F. Troje ir M. McAdam pateikė įrodymų, kad sukimosi šališkumas yra susijęs su žmogaus regos sistemos ypatumu dažniau į objektą žiūrėti iš viršaus nei iš apačios [57]. Štai kodėl dauguma žmonių mato laikrodžio rodyklės kryptimi besisukantį siluetą.

Šiame darbe pristatoma *naujo tipo optinė iliuzija*, pagrįsta žmogaus regos sistemos gebėjimu vidurkinti laike aukštuoju dažniu virpančių objektų vaizdus.

1.5. Vizualioji kriptografija

Vizualioji kriptografija – tai kriptografijos technika, leidžianti užšifruoti vaizdinę informaciją (tekstą, paveikslus ir kt.) tokiu būdu, kad iššifravimas būtų atliekamas remiantis tik žmogaus rega, be jokių papildomų skaičiavimų. M. Naor ir A. Shamir laikomi vizualiosios kriptografijos pradininkais [58]. 1994 metais jie pasiūlė naują vaizdinės slaptos informacijos schemą, kai slaptas vaizdas yra suskaidomas į n dalių. Kiekviena dalis išspausdinama ant atskiros permatomos skaidrės. Neturint bent vienos dalies, neįmanoma pamatyti slaptos informacijos. Slepiamas vaizdas gaunamas tik sudėjus vieną ant kitos visas n dalių.

Toks vaizdinės informacijos kodavimo metodas pagrįstas kiekvieno pikselio skaidymu į mažesnes dalis. Norint išlaikyti dekoduoto vaizdo kontrastą, baltų ir juodų dalių skaičius viename pikselyje turi būti vienodas. Jei kiekvienas pikselis suskaidomas į 4 mažesnes dalis, gaunamos 3 poros pikselių blokų būsenų, kurios parodytos 1.2 paveiksle [58]. Šis būdas naudojamas vaizdo kodavimui į dvi skaidres. Pirmoje skaidrėje atsitiktinai parenkama bet kuri koduojamo pikselio būsena. Antroje skaidrėje parenkama priešinga būsena, jei norima išryškinti slaptą informaciją, ir tokia pati, jei slapta informacija nebus išryškinta.



1.2 pav. 3 galimos poros pikselių blokų būsenų skaidant pikselį į 4 dalis [58]

Tokiu būdu gautos skaidrės išspausdinamos ant skaidrios plėvelės. Kiekvieną skaidrę paėmę atskirai (1.3 pav., a) ir 1.3 pav., b)) matysime tik atsitiktinių baltų ir juodų pikselių rinkinį – slaptos informacijos nematysime. Tam, kad pamatytume koduotą vaizdą, reikia abi skaidres sudėti vieną ant kitos (1.3 pav., c)).

a) b)

c)

1.3 pav. Vizualiosios kriptografijos schema: koduojamas vaizdas suskaidomas į dvi permatomas skaidres a) ir b), slaptas vaizdas c) dekoduojamas sudėjus vieną ant kitos abi skaidres

Nuo 1994 metų buvo pasiūlyta įvairių vizualiosios kriptografijos algoritmo modifikacijų.

Yan ir kiti pasiūlė pilkos spalvos pustoniais pagrįstą vizualiosios kriptografijos schemą, kuriai naudojama mažiau papildomų pikselių [59]. Padidintos talpos vizualiosios kriptografijos schema pateikta [60]. Geetha ir kiti pristatė optimalią vizualiosios kriptografijos schemą, pagrįstą kelių skaidrių naudojimu, kuri gali būti pritaikyta multimedijos duomenims apdoroti [61]. Hajiabolhassan ir Cheraghi pateikė teorines vizualiosios kriptografijos schemų taikymo ribas [62].

Lee ir kiti pateikė naują vizualiosios kriptografijos schemą, pagrįstą daugiasluoksniu informacijos kodavimu, kai dekoduotas vaizdas nepadidėja [63]. Hua ir kiti pasiūlė vizualiosios kriptografijos schemą daugiasluoksniams informacijos slėpimo taikymams vizualizuojant slaptus vaizdus kompiuterių tinkle [64]. Shemin ir Vipinkumar pristatė elektroninių mokėjimų sistemą, pagrįstą vizualiąja ir kvantine kriptografija [65]. Pasiūlyta sistema užtikrina didesnį saugumą lyginant su tradicinėmis elektroninių mokėjimų sistemomis.

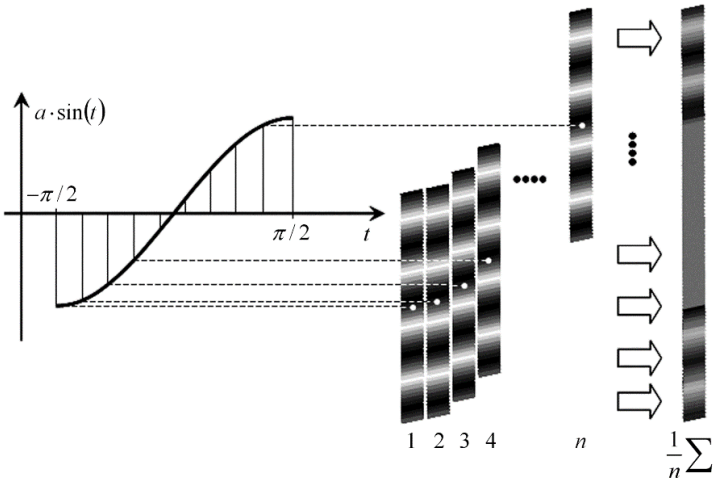
Klasikinės vizualiosios kriptografijos schema yra kriptografiškai gana saugi, nes neturint visų skaidrių neįmanoma atkurti slaptos informacijos. Tačiau šios schemos trūkumas yra didelė sukčiavimo galimybė. Lin ir kiti pristatė vizualiosios kriptografijos schemą, pagrįstą koherentiniais raštais; ji sudaro galimybę išvengti sukčiavimo atvejų [66].

Luo ir kiti pasiūlė vizualiosios kriptografijos schemą, skirtą spalvotiems paveikslams koduoti. Ši schema yra pritaikyta nebrangiems išvesties įrenginiams, tokiems kaip monochrominis spausdintuvas, faksas. Pasiūlyta schema gali būti naudojama vaizdams nuspalvinti [67]. Tharayil ir kiti pristatė vizualiosios kriptografijos schemą, pagrįstą hibridiniu spalvų skaidymo algoritmu [68].

Yang ir kiti pristatė visiškai saugią vizualiosios kriptografijos schemą spalvotiems vaizdams [69]. Dvi vizualiosios kriptografijos schemos spalvotiems vaizdams yra pasiūlytos [70]. Pirmojoje schemoje slaptam vaizdui rekonstruoti reikalingos visos trys skaidrės, antrojoje schemoje – dvi iš trijų. Visos skaidrės padarytos prasmingos, norint padidinti saugumą ir išvengti įtarimo, kad jose kažkas yra paslėpta.

1.6. Laike vidurkintas geometrinis muaras

Laike vidurkintas geometrinis muaras yra dinaminė alternatyva statiniam dvigubos ekspozicijos geometriniam muarui. 1979 metais buvo suformuluoti laike vidurkinto geometrinio muaro principai [71]. Čia, kitaip nei vizualiosios kriptografijos atveju, yra naudojama tik viena muaro gardelė.



1.4 pav. Schema, rodanti laike vidurkinto vaizdo skaitmeninį sukūrimą [72]

Neperšviečiamas gardelės vaizdas yra išspausdinamas ant svyruojančio kūno paviršiaus, vidurkinimo laike metodas taikomas laike vidurkintoms muaro interferencinėms juostoms užfiksuoti [73]. 1.4 pav. parodyta, kaip gaunamas laike vidurkintas vaizdas, kai turime n tokių pačių paslinktų statinių vaizdų.

1.7. Dinaminė vizualioji kriptografija

Vaizdo slėpimo metodika, kai slaptas vaizdas išryškėja laike vidurkintų muaro interferencinių juostų pavidalu, kai svyruoja nedeformuojamas užkoduotas vaizdas, pirmą kartą buvo pasiūlyta [72] straipsnyje. Čia, norint paslėpti slaptą vaizdą viename užkoduotame vaizde, yra naudojama stochastinė muaro gardelė. Slapta informacija dekoduojama plika akimi, kai harmoninių svyravimų amplitudė tiksliai sutampa su iš anksto nustatyta reikšme. Tai, kad plika akimi negalime pamatyti slaptos informacijos iš užkoduoto vaizdo, leidžia daryti išvadą, kad ši vaizdo slėpimo metodika yra panaši į vizualiąją kriptografiją. Tam tikri skaitiniai algoritmai naudojami vaizdui užkoduoti, tačiau dekodavimui jokių algoritmų nereikia – jis yra visiškai vizualus. Skirtingai nei vizualiojoje kriptografijoje, koduojant šiuo būdu reikalingas tik vienas užkoduotas vaizdas, kuriam virpant išryškėja slapta informacija. Nors taip užkoduotas vaizdas nėra kriptografiškai saugus, sujungę vizualiąją kriptografiją ir laike vidurkintą geometrinį muarą gauname naują vaizdo slėpimo metodiką – dinaminę vizualiąją kriptografiją [10, 74].

1.7.1. Vienmatė muaro gardelė

Tarkim, turime vienmatę harmoninę muaro gardelę [75]:

$$F(x) = \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right); \quad (1.8)$$

čia x – išilginė koordinatė; λ – muaro gardelės periodas. Skaitinės funkcijos $F(x)$ reikšmės parodo pilkio lygį taške x: skaitinė reikšmė 0 atitinka juodą spalvą, 1 – baltą spalvą, o visos tarpinės reikšmės atitinka tam tikrą pilkio lygį.

Sakykime, kad muaro gardelė yra formuojama ant vienmačio deformuojamojo kūno paviršiaus. Deformacijos funkciją pusiausvyros padėties atžvilgiu taške x laiko momentu t pažymėkime $u(x,t)$.

Tada deformuojama muaro gardelė gali būti išreikšta tokiu būdu:

$$F(x,t) = \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}\mu(x,t)\right), \quad (1.9)$$

jei nepriklausomasis kintamasis x gali būti išreikštas iš sąryšio

$$x + u(x,t) = z \quad (1.10)$$

tokiu pavidalu:

$$x = \mu(z,t). \quad (1.11)$$

Tarkim, kad funkcija $u(x,t)$ aprašo harmoninius svyravimus apie pusiausvyros padėtį [72]:

$$u(x,t) = a(x)\sin(\omega t + \varphi); \quad (1.12)$$

čia $a(x)$ – tam tikros virpesių tikrinės formos svyravimai; ω ir φ yra harmoninių svyravimų dažnis ir fazė.

Paimkime tašką x_0 ir užrašykime Teiloro eilutę funkcijai $a(x)$:

$$a(x) = a_0 + \dot{a}_0(x - x_0) + O((x - x_0)^2); \quad (1.13)$$

čia $a(x_0) = a_0$, $\left.\frac{da}{dx}\right|_{x=x_0} = \dot{a}_0$, … .

Imdami tik tiesinę šios eilutės dalį ir inžinerine prasme galime parašyti:

$$a(x) \approx a_0 + \dot{a}_0(x - x_0). \quad (1.14)$$

Neprarasdami bendrumo galime tarti, kad $\omega = 1$ ir $\varphi = 0$. Tada aprašytus sąryšius įstatę į (1.10) lygtį gauname:

$$x + (a_0 + \dot{a}_0 x - \dot{a}_0 x_0)\sin t = z, \quad (1.15)$$

$$x = \frac{z - a_0 \sin t + \dot{a}_0 x_0 \sin t}{1 + \dot{a}_0 \sin t}. \quad (1.16)$$

Tada deformuotą muaro gardelę taške x bet kuriuo laiko momentu t galime aprašyti [76]:

$$F(x,t) = \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}\cdot\frac{x + (\dot{a}_0 x_0 - a_0)\sin t}{1 + \dot{a}_0 \sin t}\right). \quad (1.17)$$

1.7.2. Nedeformuojamoji muaro gardelė

Tegul $a(x) = A$ (čia A yra konstanta). Kitais žodžiais tariant, nuokrypis

$$u(x,t) = A\sin(\omega t + \varphi) \tag{1.18}$$

aprašo nedeformuojamojo kūno svyravimą apie pusiausvyros padėtį. Tada muaro gardelės pilkio lygis aprašomas tokia lygtimi:

$$F(x,t) = \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}\cdot\left(x - Asin(\omega t + \varphi)\right)\right). \tag{1.19}$$

Tarkime, kad vidurkinimas laike yra taikomas registruoti harmoniškai svyruojančiai muaro gardelei

$$\begin{aligned}\lim_{T\to\infty}\frac{1}{T}\int_0^T F(x,t)dt &= \frac{1}{2} + \frac{1}{2}\lim_{T\to\infty}\frac{1}{T}\int_0^T \cos\left(\frac{2\pi}{\lambda}x - \frac{2\pi}{\lambda}A\sin t\right)dt = \\ = \frac{1}{2} + \frac{1}{2}\lim_{T\to\infty}\frac{1}{T}\int_0^T &\left[\cos\left(\frac{2\pi}{\lambda}x\right)\cos\left(\frac{2\pi}{\lambda}A\sin t\right) + \sin\left(\frac{2\pi}{\lambda}x\right)\sin\left(\frac{2\pi}{\lambda}A\sin t\right)\right]dt \\ &= \frac{1}{2} + \frac{1}{2}\Big[\cos\left(\frac{2\pi}{\lambda}x\right)\lim_{T\to\infty}\frac{1}{T}\int_0^T \cos\left(\frac{2\pi}{\lambda}A\sin t\right)dt + \\ &\sin\left(\frac{2\pi}{\lambda}x\right)\lim_{T\to\infty}\frac{1}{T}\int_0^T \sin\left(\frac{2\pi}{\lambda}A\sin t\right)dt\Big].\end{aligned} \tag{1.20}$$

Žinoma, kad $\lim_{T\to\infty}\frac{1}{T}\int_0^T \sin\left(\frac{2\pi}{\lambda}A\sin t\right)dt = 0$, nes pointegralinė funkcija nelyginė. Tada (1.20) formulę galime užrašyti taip:

$$\begin{aligned}\lim_{T\to\infty}\frac{1}{T}\int_0^T F(x,t)dt &= \frac{1}{2} + \\ + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)&\left[\lim_{T\to\infty}\frac{1}{T}\int_0^T \cos\left(\frac{2\pi}{\lambda}A\sin t\right)dt + i\lim_{T\to\infty}\frac{1}{T}\int_0^T \sin\left(\frac{2\pi}{\lambda}A\sin t\right)dt\right] = \\ = \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)&\lim_{T\to\infty}\frac{1}{T}\int_0^T \left[\cos\left(\frac{2\pi}{\lambda}A\sin t\right) + i\sin\left(\frac{2\pi}{\lambda}A\sin t\right)\right]dt.\end{aligned} \tag{1.21}$$

Pritaikę Oilerio formulę $e^{ix} = \cos x + i\sin x$ gausime:

$$\lim_{T\to\infty}\frac{1}{T}\int_0^T F(x,t)dt = \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)\lim_{T\to\infty}\frac{1}{T}\int_0^T e^{i\frac{2\pi}{\lambda}A\sin t}dt. \tag{1.22}$$

Tada žinant, kad $J_0(z) = \frac{1}{\pi}\int_0^\pi e^{iz\cos\theta}d\theta$ yra pirmojo tipo nulinės eilės Beselio funkcija, (1.22) lygtį galima perrašyti tokiu būdu [71, 75, 77]:

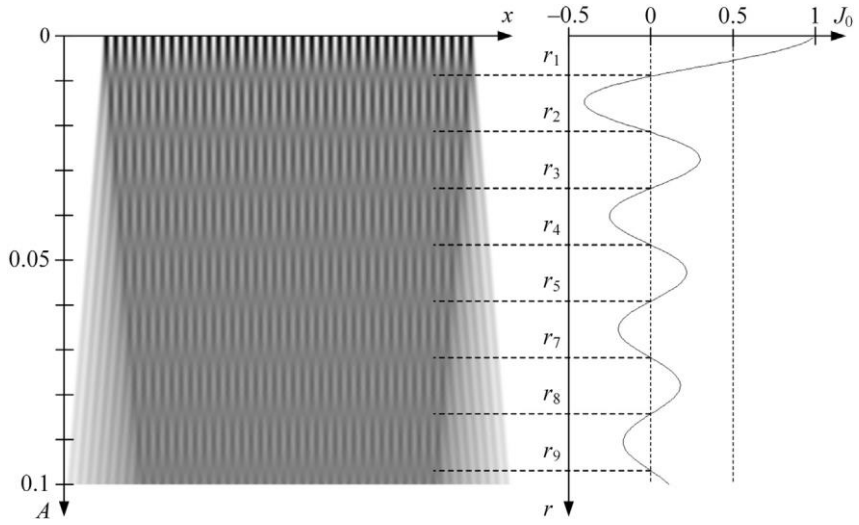
$$\lim_{T\to\infty}\frac{1}{T}\int_0^T F(x,t)dt = \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)J_0\left(\frac{2\pi}{\lambda}A\right). \tag{1.23}$$

Reikia pažymėti, kad pilkio lygio pasiskirstymas laike vidurkintame vaizde nepriklauso nuo harmoninių svyravimų dažnio ir fazės.

Laike vidurkintame vaizde interferencinės juostos formuosis, kai $J_0 = 0$. Taip bus tada, kai virpesių amplitudės reikšmės bus [75, 78, 79]

$$\frac{2\pi}{\lambda}A_k = r_k; \tag{1.24}$$

čia r_k – pirmojo tipo nulinės eilės Beselio funkcijos šaknis; $k = 1, 2, \ldots$. Laike vidurkintų interferencinių juostų formavimasis pavaizduotas 1.5 paveiksle. Šiame paveiksle x ašis atitinka išilginę koordinatę x, o y ašis – amplitudę A.

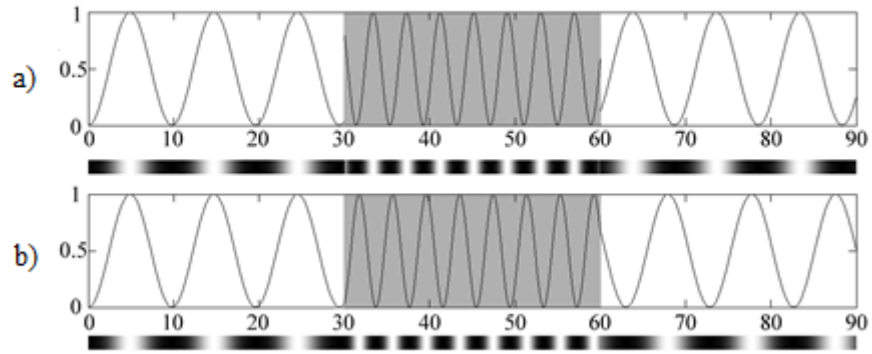


1.5 pav. Vienmatės muaro gardelės harmoniniai svyravimai išryškina laike vidurkintas interferencines juostas (muaro gardelės periodas $\lambda = 0{,}025$). Laike vidurkintas vaizdas parodytas paveikslo kairėje pusėje, funkcijos J_0 grafikas – paveikslo dešinėje pusėje [76]

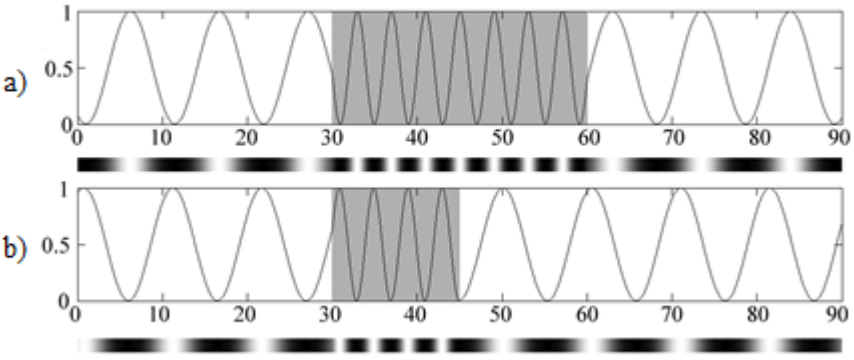
Ryški harmoninė gardelė yra matoma, kai $A = 0$. Pilkos laike vidurkintos interferencinės juostos aiškiai matomos tada, kai amplitudės sutampa su pirmojo tipo nulinės eilės Beselio funkcijos šaknimis r_k. Vienmatė muaro gardelė formuojasi tik tam tikrame intervale – išblukusios zonos intervalo galuose proporcingos harmoninių svyravimų amplitudei (1.5 pav.).

1.7.3. Vaizdo slėpimo schemos įgyvendinimas

Vaizdo kodavimą galima laikyti iš dalies saugiu, jeigu slaptos informacijos nepamatysime plika akimi iš statinio užkoduoto vaizdo. Sakykim, turime slaptą vaizdą, kuris parodytas 1.8(a) paveiksle. Fonui parinkime muaro gardelę, kurios periodas yra $\lambda_b = 0{,}2$, o slaptam vaizdui – muaro gardelę, kurios periodas $\lambda_s = 0{,}15$. Tiesiogiai įterpę slaptą vaizdą į fono muaro gardelę, galime aiškiai interpretuoti slaptą informaciją (paveikslas 1.8(b)). Todėl būtina statinį vaizdą pakeisti taip, kad plika akimi slaptos informacijos nematytume. Tuo tikslu naudojami algoritmai, aprašyti [72] straipsnyje. Tai fazių reguliarizacijos ir atsitiktinių fazės postūmių algoritmai. Šių algoritmų veikimo vienam pikselių stulpeliui principas parodytas 1.6 ir 1.7 paveiksluose.



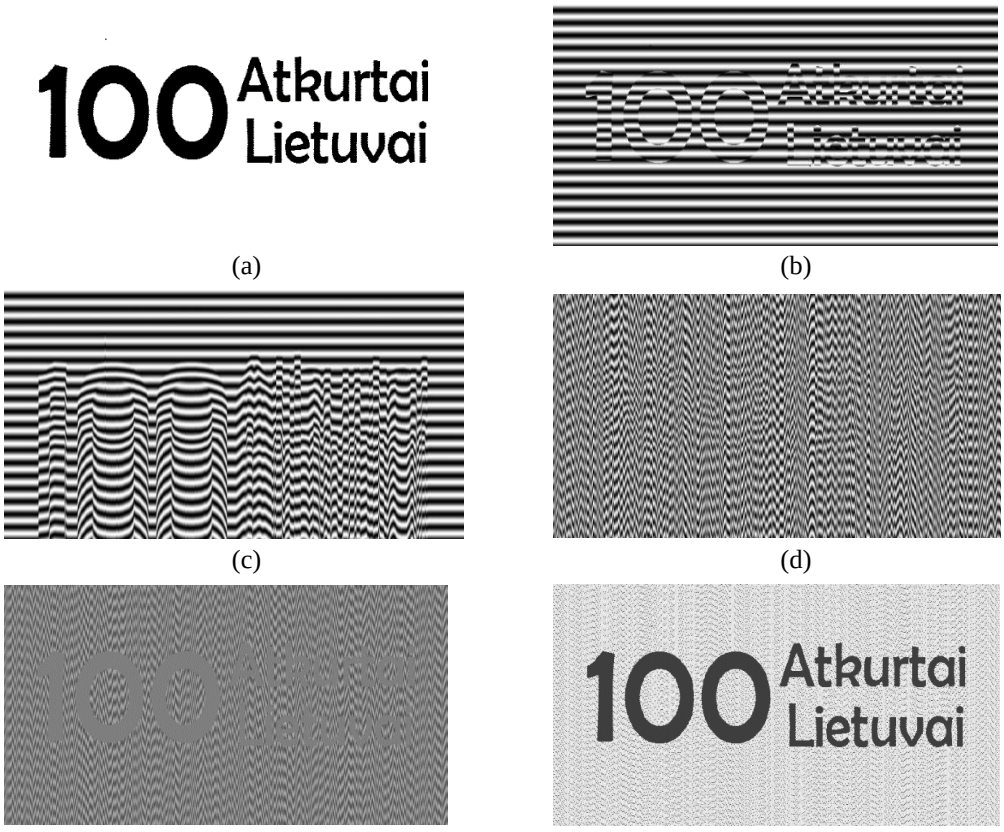
1.6 pav. Fazių reguliarizacija, fono muaro gardelei pereinant į slaptos informacijos gardelę: (a) pilkumo lygio kitimas prieš fazių reguliarizaciją; (b) po fazių reguliarizacijos [72]



1.7 pav. Atsitiktinių fazės postūmių algoritmas [72]

Fazių reguliarizacijos algoritmas pastumia muaro gardelės struktūrą tokiu būdu, kad neliktų pilkio lygio neatitikimų fono ir teksto lūžio vietose. Staigus perėjimas iš šviesios spalvos į tamsią (arba atvirkščiai) išryškina slapto vaizdo kontūrus. 1.6 paveiksle pilkosios sritys atitinka slaptos informacijos zoną, o baltosios sritys – fono gardelę. 1.6(a) paveiksle pavaizduotas pikselių stulpelis prieš pritaikant fazių reguliarizacijos algoritmą, o 1.6(b) paveiksle – pritaikius fazių reguliarizacijos algoritmą. Nesunku pamatyti, kad statinio vaizdo, kuris parodytas 1.8(c) paveiksle, apatinėje dalyje atsiranda fono muaro gardelės netolygumai. Tai yra fazių reguliarizacijos algoritmo pritaikymo pasekmė.

Pritaikius fazių reguliarizacijos algoritmą (1.8(c) pav.), slaptą informaciją interpretuoti darosi sunkiau, bet gautas rezultatas vis dar netenkina tikslo – sukurti visiškai neinterpretuojamą statinį užkoduotą vaizdą. Tam tikslui papildomai taikomas atsitiktinių fazės postūmių algoritmas, kurio veikimas parodytas 1.7 paveiksle. Šiame paveiksle parodytiems dviem gretimiems pikselių stulpeliams (1.7(a) pav. ir 1.7(b) pav.) buvo pritaikyti pradiniai atsitiktiniai fazės postūmiai stulpelių kairėje. Atsitiktinių fazės postūmių algoritmas pritaikytas tik pritaikius fazių reguliarizacijos algoritmą. Abiejų anksčiau minėtų algoritmų pritaikymo rezultatą matome 1.8(d) paveiksle.



1.8 pav. Fazių reguliarizacijos ir atsitiktinių fazės postūmių algoritmų pritaikymas slaptam vaizdui užkoduoti: (a) slaptas vaizdas; (b) slapto vaizdo tiesioginis įterpimas į fono muaro gardelę, fono muaro gardelės periodas $\lambda_b = 0{,}2$, teksto muaro gardelės periodas $\lambda_s = 0{,}15$; (c) užkoduotas statinis vaizdas pritaikius fazių reguliarizacijos algoritmą; (d) užkoduotas statinis vaizdas pritaikius atsitiktinių fazės postūmių algoritmą; (e) dekoduotas vaizdas; (f) dekoduotas paryškintas vaizdas

Statinio užkoduoto vaizdo dekodavimas, atliktas skaitmeniniu būdu, kompiuteriu realizuojant vidurkinimo laike algoritmą, parodytas 1.8(e) paveiksle. Čia laike vidurkintos interferencinės juostos susiformuoja slaptos informacijos zonoje. Tačiau fono muaro gardelė neužpilkėja.

1.8. Pirmojo skyriaus išvados ir apibendrinimas

Dinaminės vizualiosios kritptografijos metodas sukurtas sujungus muaro interferencinių juostų formavimosi efektą, klasikinę vizualiąją kriptografiją ir vidurkinimo laike procedūrą. Kitaip nei klasikinės vizualiosios kriptografijos atveju, kai slaptam vaizdui dekoduoti naudojamos kelios skaidrės, kurios sudedamos viena ant kitos, dinaminės vizualiosios kriptografijos atveju naudojama tik viena skaidrė – dekodavimas atliekamas virpinant užkoduotą vaizdą tiksliai pagal iš anksto nustatytą trajektoriją. Kadangi dinaminės vizualiosios kriptografijos metodas gali būti pritaikytas žmogaus

regos sistemos tyrimams, mikro–opto–elektromechaninėse sistemose, labai svarbu praplėsti šio metodo tyrimus deformuojamosiose bei dvimatėse muaro gardelėse.

Norint sukurti dinaminės vizualiosios kriptografijos principais pagrįstus skaitinių vaizdų slėpimo modelius deformuojamosiose bei dvimatėse muaro gardelėse, reikia išspręsti šiuos uždavinius.

1. Sukonstruoti dinaminės vizualiosios kriptografijos schemą deformuojamosiose muaro gardelėse ir pritaikyti šią schemą skaitiniams vaizdams slėpti baigtiniais elementais aprašomose gardelėse.
2. Pritaikyti dinaminės vizualiosios kriptografijos, pagrįstos skaitinių vaizdų slėpimu, schemą chaotinių virpesių atveju.
3. Sukonstruoti skaitinių vaizdų slėpimo schemą dvimatėse kryžminėse muaro gardelėse.
4. Sukonstruoti stendus pristatomų skaitinių vaizdų slėpimo algoritmų eksperimentiniam verifikavimui.

2. DEFORMUOJAMOJI MUARO GARDELĖ

Šio skyriaus pagrindas yra dinaminės vizualiosios kriptografijos naujų teorinių sąryšių išvedimas ir sukurtų naujų modelių realizavimas (programiškai ir eksperimentiniu būdu). Tai leis siūlomas skaitmeninių vaizdų slėpimo metodikas pritaikyti įvairiose mokslo ir inžinerijos srityse (optinės kontrolės sistemose, mikro–opto–elektromechaninėse sistemose ir kt.).

Skyrių sudaro šios dalys: optimalaus muaro gardelės periodo parinkimas nagrinėjamas 2.1 poskyryje [80]; dinaminės vizualiosios kriptografijos modeliai deformuojamųjų harmoninės bei Ronči tipo gardelių atveju (kai svyravimai harmoniniai) aprašyti 2.2–2.4 poskyriuose [76, 81, 82]; dinaminė vizualioji kriptografija baigtinių elementų gardelėse chaotinių svyravimų atveju nagrinėjama 2.5 poskyryje [83].

2.1. Optimalaus muaro gardelės periodo parinkimas dinaminės vizualiosios kriptografijos uždaviniuose

Dinaminės vizualiosios kriptografijos uždaviniuose svarbios dvi fazės: kodavimo ir dekodavimo. Kiekvienoje iš šių fazių reikia atlikti tam tikrus veiksmus. Toliau pateikti kodavimo bei dekodavimo algoritmai.

Kodavimo algoritmas

1. Muaro gardelės periodo, skirto fonui, λ_b parinkimas.
2. Dėsnio, pagal kurį bus virpinama gardelė, parinkimas.
3. Muaro gardelės periodo, skirto slaptai informacijai, λ_s parinkimas, sprendžiant dviejų kriterijų optimizavimo uždavinį.
4. Slaptos informacijos vaizdo parinkimas.
5. Fazių reguliarizacijos ir pradinės atsitiktinės fazės algoritmų taikymas vaizdui paslėpti stochastinėje muaro gardelėje.

Dekodavimo algoritmas

1. Koduoto vaizdo virpinimas pagal numatytąjį dėsnį laike vidurkinto vaizdo registracijai.

Iš pateiktų algoritmų aprašymų galima matyti, kad kodavimo fazė yra kur kas sudėtingesnė lyginant su dekodavimo faze.

Muaro gardelės periodo, skirto slaptai informacijai, λ_s parinkimo uždavinys iki šiol dar nebuvo spręstas. Skyreliuose 2.1.1, 2.1.2 pateikiamas beveik optimalaus muaro gardelės periodo nustatymas, kai muaro gardelė yra harmoninė ir stačiakampė.

2.1.1. Optimalaus muaro gardelės periodo parinkimas, kai muaro gardelė yra harmoninė[1]

Sprendžiant dinaminės vizualiosios kriptografijos uždavinius labai svarbu optimizuoti slapto vaizdo užkodavimo saugumą bei dekodavimo kokybę. Atliekant tyrimus pastebėta, kad užkoduoto vaizdo saugumą bei dekoduojamo vaizdo ryškumą

[1] *Šiame skyriuje pristatomi rezultatai buvo publikuoti straipsnyje*:
Near-optimal pitch of a moiré grating for image hiding applications in dynamic visual cryptography
Saunorienė L.; Aleksienė S.; Ragulskienė J.

labai veikia muaro gardelių, naudojamų slaptam vaizdui ir fonui užkoduoti, žingsniai. Jeigu šie žingsniai skirsis nedaug – atkoduoto vaizdo kokybė bus prasta, jeigu žingsniai skirsis daug – kokybė bus gera, tačiau nukentės užkodavimo saugumas. Todėl šiame skyrelyje bus analizuojama dinaminės vizualiosios kriptografijos parametrų įtaka užkoduojamo slapto vaizdo saugumui ir atkoduojamo vaizdo kokybei, taip pat išvestos formulės, leidžiančios nustatyti optimalius dinaminės vizualiosios kriptografijos parametrus.

Laike vidurkinto vaizdo, aprašyto (1.23) lygtimi, standartinį nuokrypį galima apskaičiuoti pagal tokią formulę [84]:

$$S\left(F_t(x)\right) = \frac{\left|J_0\left(\frac{2\pi}{\lambda}a\right)\right|}{\sqrt{8}}. \tag{2.1}$$

Laike vidurkinto vaizdo standartinio nuokrypio reikšmė priklauso nuo laike vidurkintos muaro gardelės išblukimo lygio – ryški gardelės struktūra užtikrina pakankamai didelę standartinio nuokrypio reikšmę. Svarbu pažymėti, kad standartinis nuokrypis lygus nuliui laike vidurkintų interferencinių juostų centruose.

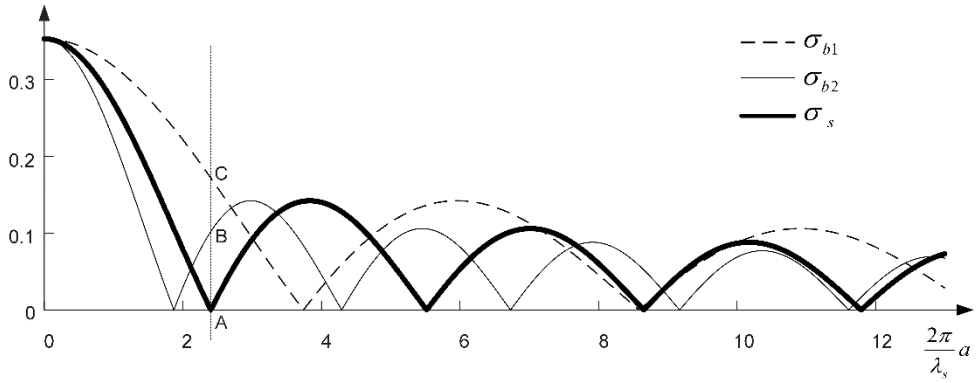
Kaip jau minėta metodologinėje dalyje, pagrindinė idėja dinaminės vizualiosios kriptografijos uždaviniuose yra užkoduoti slaptą informaciją muaro gardelėje: vienoks muaro gardelės periodas naudojamas fonui, kitoks – šiek tiek besiskiriantis periodas naudojamas slaptai informacijai. Pažymėkime slaptos informacijos zonoje periodą λ_s, o fono periodą λ_b. Gardelės periodai λ_s ir λ_b negali pastebimai skirtis $|\lambda_s - \lambda_b| \leq \varepsilon$, nes užkoduotas vaizdas bus matomas plika akimi statiniame vaizde. Tuo pat metu skirtumas tarp λ_s ir λ_b turi užtikrinti pakankamą kontrastą tarp slaptos informacijos ir fono laike vidurkintame vaizde.

Pažymėkime laike vidurkinto vaizdo slaptos informacijos ir fono standartinius nuokrypius atitinkamai σ_s ir σ_b. Reikšmės σ_s ir σ_b pagal (2.1) formulę [84] apskaičiuojamos taip:

$$\sigma_s = \frac{\left|J_0\left(\frac{2\pi}{\lambda_s}a\right)\right|}{\sqrt{8}},\ \sigma_b = \frac{\left|J_0\left(\frac{2\pi}{\lambda_b}a\right)\right|}{\sqrt{8}}. \tag{2.2}$$

Pakankamas kontrastas tarp išryškėjusios slaptos informacijos ir fono laike vidurkintame užkoduotame vaizde gaunamas, jei $|\sigma_s - \sigma_b| \geq \delta$. Taigi optimizavimo uždavinio tikslo funkcija yra $max\,|\sigma_s - \sigma_b|$ su apribojimu $|\lambda_s - \lambda_b| \leq \varepsilon$. Grafinis standartinių nuokrypių σ_s ir σ_b vaizdas parodytas 2.1 paveiksle.

Kaip jau buvo minėta, (1.17) lygtyje, slaptos informacijos zonoje, laike vidurkintas vaizdas tampa vientisai pilkas, kai svyravimų amplitudė lygi $a = \frac{\lambda_s}{2\pi}r_i,\ i = 1, 2, \ldots$. Aišku, kad vientisos pilkos srities standartinis nuokrypis yra lygus 0, todėl $\sigma_s = 0$, jei tiktai svyravimų amplitudė lygi $\frac{\lambda_S}{2\pi}r_1$. Todėl kontrastas tarp slaptos informacijos ir fono priklauso tik nuo σ_b reikšmės (galima pastebėti, kad atstumas AC 2.1 paveiksle yra lygus $|\sigma_{b1} - \sigma_s| = \sigma_{b1}$ ir atstumas AB yra lygus $|\sigma_{b2} - \sigma_s| = \sigma_{b2}$ taške, kai $\frac{2\pi}{\lambda_s}a = r_1$).



2.1 pav. Laike vidurkintų muaro gardelių standartinių nuokrypių priklausomybė nuo svyravimų amplitudės a . Stora vientisa linija žymimi slaptos informacijos standartiniai nuokrypiai σ_s, kai $\lambda_s = 0{,}45$; plona vientisa ir plona brūkšniuota linijomis vaizduojami fono standartiniai nuokrypiai σ_{b1} ir σ_{b2}, kai $\lambda_{b1} = 0{,}7$, $\lambda_{b2} = 0{,}35$ atitinkamai

Sakykime, kad išryškėjusios slaptos informacijos kontrastas laike vidurkintame vaizde pakankamas, jei standartinis nuokrypis σ_b yra lygus ar viršija tam tikrą slenkstį δ:

$$\frac{\left|J_0\left(\frac{2\pi}{\lambda_b}a\right)\right|}{\sqrt{8}} \geq \delta, \tag{2.3}$$

o svyravimų amplitudė parenkama $a = \frac{\lambda}{2\pi}r_1$ ir (2.3) lygtis gali būti užrašyta tokiu pavidalu:

$$\frac{\left|J_0\left(\frac{\lambda_s}{\lambda_b}r_1\right)\right|}{\sqrt{8}} \geq \delta. \tag{2.4}$$

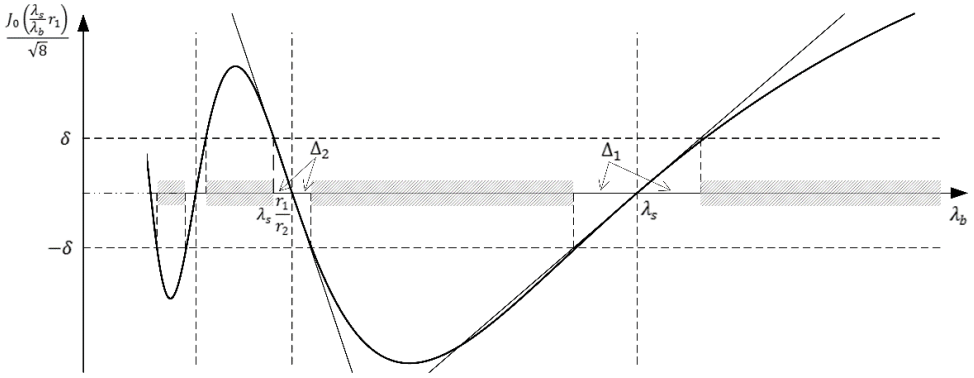
(2.4) nelygybės sprendiniai parodyti 2.2 paveiksle, kai λ_s yra fiksuotas. Brūkšniuoti intervalai rodo tokius λ_b intervalus, kuriose tenkinama nelygybė $\left|J_0\left(\frac{\lambda_s}{\lambda_b}r_1\right)\right|/\sqrt{8} \geq \delta$. Funkcijos $J_0\left(\frac{\lambda_s}{\lambda_b}r_1\right)$ nuliai yra taškuose $\lambda_b = \lambda_s\frac{r_1}{r_i}$, $i = 1, 2, \ldots$.

Funkcija $J_0\left(\frac{\lambda_s}{\lambda_b}r_1\right)$ gali būti aproksimuota jos liestine bet kurios šaknies aplinkoje, kai slenkstis δ yra sąlygiškai mažas. Žinoma, kad $J_0'(x) = -J_1(x)$; čia $J_1(x)$ – pirmojo tipo pirmos eilės Beselio funkcija. Taigi liestinės krypties koeficientas taške $\lambda_b = \lambda_s$ yra $k_1 = J_0'(r_1) = \frac{r_1}{\lambda_s}J_1(r_1)$.

Analogiškai skaičiuojamas krypties koeficientas taške $\lambda_b = \lambda_s\frac{r_1}{r_2}$: $k_2 = J_0{}'(r_2) = \frac{r_2^2}{r_1\lambda_s}J_1(r_2)$. Čia $\Delta_i, i = 1, 2, \ldots$ (2.2 pav.) gali būti aproksimuojama kaip $\Delta_i = \frac{\delta}{k_i}$.

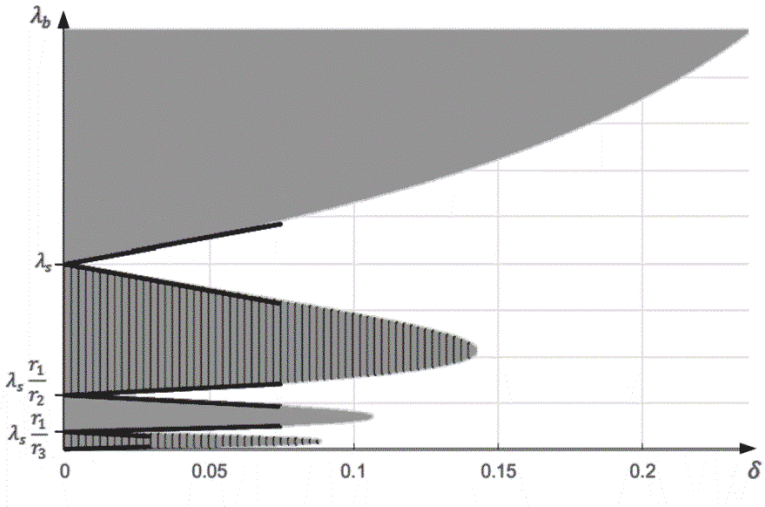
Galiausiai (2.4) nelygybės apytikslis sprendinys, kai δ yra pakankamai mažas, gali būti užrašytas tokiu būdu:

$$\begin{cases} \lambda_b \geq \lambda_s \left(1 + \dfrac{\delta}{r_1 J_1(r_1)}\right), \\ \lambda_s \left(1 - \dfrac{\delta}{r_1 J_1(r_1)}\right) \geq \lambda_b \geq \lambda_s \dfrac{r_1}{r_2}\left(1 + \dfrac{\delta}{r_2 J_1(r_2)}\right). \\ \ldots . \end{cases} \tag{2.5}$$



2.2 pav. Nelygybės $\left|J_0\left(\frac{\lambda_s}{\lambda_b} r_1\right)\right| / \sqrt{8} \geq \delta$ vizualizacija intervale $(0{,}2\lambda_s; 1{,}5\lambda_s)$. Stora vientisa linija vaizduojamas $\left|J_0\left(\frac{\lambda_s}{\lambda_b} r_1\right)\right| / \sqrt{8}$ kitimas; liestinės taškuose λ_s ir $\lambda_s \frac{r_1}{r_2}$ parodytos plonomis linijomis

(2.4) nelygybės apytiksliai sprendiniai, rasti kompiuterinio modeliavimo būdu, yra parodyti 2.3 paveiksle. Visos λ_b reikšmės, išsidėsčiusios vientisoje pilkoje ir brūkšniuotoje pilkoje srityse, tinka nelygybei su iš anksto nustatyta δ reikšme. Juodos linijos rodo (2.5) lygties apytikslio sprendinio ribas.



2.3 pav. Nelygybės $\left|J_0\left(\frac{\lambda_s}{\lambda_b} r_1\right)\right| / \sqrt{8} \geq \delta$ sprendiniai: pilka spalva nurodomos sritys, kuriose $J_0\left(\frac{\lambda_s}{\lambda_b} r_1\right) / \sqrt{8} \geq \delta$, juostuota pilka spalva – sritys, kuriose $J_0\left(\frac{\lambda_s}{\lambda_b} r_1\right) / \sqrt{8} \leq -\delta$, juodomis linijomis nurodomos (2.5) lygties apytikslio sprendinio ribos

Jei norime gauti pakankamą kontrastą tarp slaptos informacijos ir fono sričių ($\sigma_b = \delta$), būtų optimalu išrinkti λ_b reikšmes, esančias ant pilkos ir juostuotos sričių kontūrų 2.3 paveiksle, arba, jei δ reikšmė yra maža, optimalus sprendinys gali būti apskaičiuojamas taip:

$$\lambda_b = \lambda_s \left(1 + \frac{\delta}{r_1 J_1(r_1)}\right) \text{ arba } \lambda_b = \lambda_s \left(1 - \frac{\delta}{r_1 J_1(r_1)}\right). \quad (2.6)$$

Būtina prisiminti, jog skirtumas tarp λ_s ir λ_b reikšmių vis dėlto turi būti pakankamai mažas tam, kad užtikrintume vizualiosios kodavimo schemos saugumą.

2.1.2. Optimalaus muaro gardelės periodo parinkimas, kai muaro gardelė yra stačiakampė[2]

Kaip jau minėta anksčiau, slapta informacija dekoduojama virpinant užkoduotą vaizdą apie pusiausvyros padėtį. Užkoduotas vaizdas gali būti virpinamas eksperimentiniu būdu, tai yra naudojant vibracinį stendą, arba svyravimai gali būti imituojami kompiuterio pagalba naudojant *Adobe Flash Player* ar panašią programinę įrangą. Reikia pažymėti, kad abiem atvejais minimalus svyravimų dažnis turi būti ne mažesnis nei 20 Hz tam, kad būtų galima įžvelgti slaptą informaciją plika akimi. Tačiau imituoti skaitmeninio vaizdo aukštojo dažnio harmoninius svyravimus kompiuteriu yra neįmanoma dėl tam tikrų techninių apribojimų, tokių kaip ribota raiška ir ribotas ekrano atsinaujinimo greitis. Pirmiausia kiekvienas vaizdo poslinkio dydis turi būti pikselio dydžio daugiklis. Be to, harmoniniams svyravimams imituoti reikia 16 kadrų per laiko tarpą. Tuo pat metu svyravimų dažnis turi būti ne mažesnis nei 20 Hz, jei žmogaus regos sistema atlieka vidurkinimą laike. Tai reiškia, kad norint įgyvendinti harmoninius svyravimus kompiuterio ekrane, ekrano atsinaujinimo greitis turi būti 320 Hz. Tačiau tai neįmanoma, nes didžiausias įprasto kompiuterio atsinaujinimo greitis yra 60 Hz. Vienas iš galimų šios problemos sprendimo būdų – taikyti stačiakampę bangos formos funkciją vietoj harmoninių virpesių.

Tarkime, kad muaro gardelė suformuota ant vienmačio nedeformuojamojo kūno paviršiaus, kuris svyruoja apie pusiausvyros padėtį pagal stačiakampę bangos formos funkciją $u(t)$:

$$u(t) = \begin{cases} -a, \quad kai \quad t \in \left[0; \frac{\pi}{\omega}\right); \\ a, \quad kai \quad t \in \left[\frac{\pi}{\omega}; \frac{2\pi}{\omega}\right]; \end{cases} \quad (2.7)$$

čia a – amplitudė, ω – svyravimų dažnis. Vienmatės laike vidurkintos muaro funkcijos taške x pilkio intensyvumas aprašomas pagal formulę:

[2] *Šiame skyriuje pristatomi rezultatai buvo publikuoti straipsnyje*:
Near-optimal pitch for the optical implementation of dynamic visual cryptography
Saunoriene L.; Aleksiene S.; Petrauskiene V., Ragulskiene J.

$$F_t(x) = \lim_{T\to\infty}\frac{1}{T}\int_0^T\left(\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}(x-u(t))\right)\right)dt = \frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)\cos\left(\frac{2\pi}{\lambda}a\right); \tag{2.8}$$

čia T – ekspozicijos trukmė, taikoma vidurkinant laike. Vienmačio laike vidurkinto muaro vaizdo pilkio lygių standartinis nuokrypis aprašomas tokiu būdu:

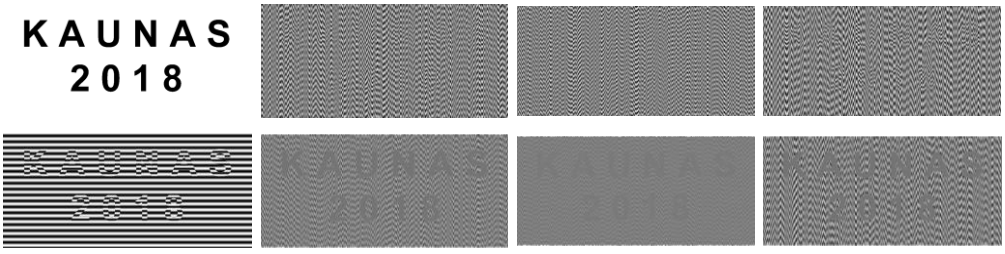
$$\sigma(\lambda, a) = \frac{\left|\cos\left(\frac{2\pi}{\lambda}a\right)\right|}{\sqrt{8}}. \tag{2.9}$$

Laike vidurkintas muaro vaizdas tampa tolydžiai pilkas laike vidurkintų interferencinių juostų centruose. Šis efektas matosi ten, kur yra funkcijos $\cos\left(\frac{2\pi}{\lambda}a\right)$ šaknys, tai yra [29]:

$$\frac{2\pi}{\lambda}a_n = \frac{\pi}{2}(2n-1), \qquad n = 1,2,\dots . \tag{2.10}$$

Be to, vienmačio laike vidurkinto muaro vaizdo pilkio lygio standartinis nuokrypis ties amplitudžių a_n reikšmėmis lygus nuliui.

Dekoduoto slapto vaizdo kontrastas priklauso nuo skirtumo tarp muaro gardelių periodų. Pavyzdžiui, jeigu skirtumas tarp muaro gardelės periodų užkoduotame vaizde yra mažesnis, tai dekoduoto vaizdo kontrastas taip pat yra mažesnis, kaip matyti iš 2.4 paveikslo (c) dalies. Jeigu skirtumas tarp muaro gardelės periodų yra didesnis, tai kontrastas didesnis (2.4 paveikslo (d) dalis), bet tada slaptos informacijos kontūrai matosi stacionariame užkoduotame vaizde (2.4 paveikslo (d) dalies viršuje). Todėl labai svarbu nustatyti sąryšius tarp optimalių λ_s ir λ_b reikšmių, kurios užtikrintų geriausią galimą kontrastą laike vidurkintame vaizde.



a) b) c) d)

2.4 pav. Slaptos informacijos užkodavimas ir dekodavimas, kai $\lambda_s = 0{,}2$: a) slaptas vaizdas (viršuje) ir slaptas vaizdas, tiesiogiai įterptas į muaro gardelę, kai $\lambda_b = 0{,}28$ (apačioje); b) užkoduotas vaizdas, gautas pritaikius fazių reguliarizacijos ir atsitiktinės fazės sumaišymo algoritmus (viršuje) ir dekoduotas vaizdas (apačioje), kai $\lambda_b = 0{,}28$; c) užkoduotas vaizdas (viršuje) ir dekoduotas vaizdas (apačioje), kai $\lambda_b = 0{,}22$; d) užkoduotas vaizdas (viršuje) ir dekoduotas vaizdas (apačioje), kai $\lambda_b = 0{,}38$

2.4 paveikslo (d) dalyje matyti, kad muaro gardelių periodai λ_s ir λ_b negali labai skirtis, t. y. $|\lambda_s - \lambda_b| \le \varepsilon$ (čia ε yra maža teigiamoji konstanta), kitu atveju užkoduotas vaizdas bus matomas plika akimi statiniame užkoduotame vaizde. Tuo pat metu

skirtumas tarp periodų λ_s ir λ_b turi užtikrinti pakankamą kontrastą tarp slaptos informacijos ir fono laike vidurkintame vaizde (paveikslas 2.4 (b)). Pažymėkime slaptos informacijos ir fono laike vidurkintų vaizdų standartinius nuokrypius atitinkamai σ_s ir σ_b. Dydžių σ_s ir σ_b reikšmės skaičiuojamos pagal (2.9) formulę. Pakankamas kontrastas tarp slaptos informacijos ir fono laike vidurkintame užkoduotame vaizde yra gaunamas, jei skirtumas tarp σ_s ir σ_b absoliutiniu didumu yra mažesnis nei slenkstinė reikšmė δ: $|\sigma_s - \sigma_b| \geq \delta$.

Svarbu pažymėti, kad slaptos informacijos sritis laike vidurkintame vaizde tampa tolygiai pilka tik tada, kai svyravimų amplitudė a sutampa su $a_n = \frac{\lambda}{4}(2n-1),\ n = 1, 2, \ldots$. Kaip minėta 2.1.1 skyrelyje, sritis tampa tolygiai pilka, kai pilkio lygio standartinis nuokrypis yra lygus nuliui. Taigi $\sigma_s = 0$, jei svyravimų amplitudė yra lygi $\frac{\lambda}{4}(2n-1),\ n = 1, 2, \ldots$. Todėl kontrastas tarp slaptos informacijos ir fono laike vidurkintame vaizde priklauso tik nuo periodo λ_b reikšmės. Tarkime, kad slapto vaizdo kontrastas laike vidurkintame vaizde yra pakankamas, jei standartinis nuokrypis σ_b ((2.9) lygtyje) yra lygus ar viršija slenkstinę reikšmę δ: $\sigma_s \geq \delta$. Jei svyravimų amplitudė iš anksto nustatyta kaip $a = \frac{\lambda_s}{4}$ (iš (2.10) lygties, kai $n = 1$), tai tenkinama tokia nelygybė:

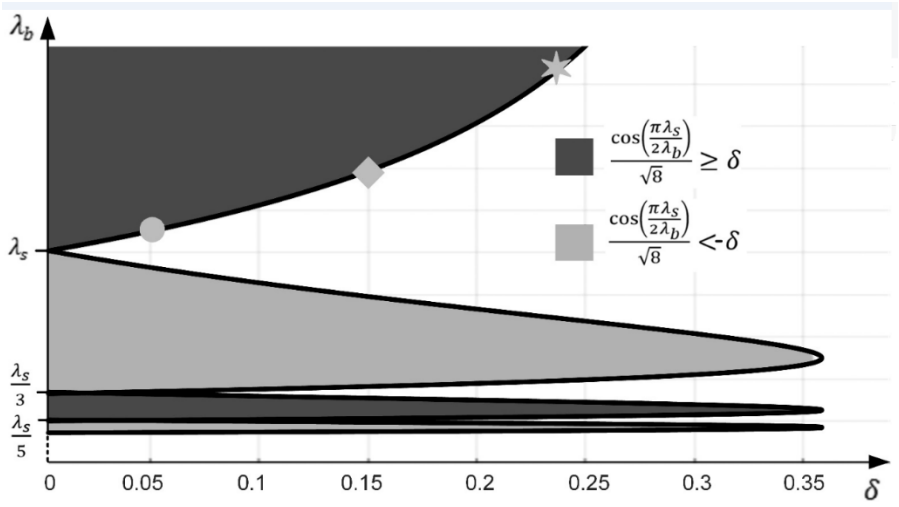
$$\frac{\left|\cos\left(\frac{\pi}{2}\frac{\lambda_s}{\lambda_b}\right)\right|}{\sqrt{8}} \geq \delta. \tag{2.11}$$

(2.11) nelygybės skaitmeniniai sprendiniai yra parodyti 2.5 paveiksle: visos periodo λ_b reikšmės, esančios šviesiai pilkose ir tamsiai pilkose srityse, tenkina (2.11) nelygybę su iš anksto nustatyta reikšme δ. Šių sričių kontūrai, 2.4 paveiksle parodyti stora vientisa linija, aprašomi šiais analitiniais sąryšiais:

$$\lambda_b = \frac{\pi\lambda_s}{2\left(\pi k + \arccos\left(\sqrt{8}\delta\right)\right)},\quad \lambda_b = \frac{\pi\lambda_s}{2\left(\pi(k+1) - \arccos\left(\sqrt{8}\delta\right)\right)},\quad k = 0, 1, 2, \ldots. \tag{2.12}$$

Kadangi skirtumas tarp λ_s ir λ_b reikšmių turi būti pakankamai mažas norint užtikrinti vizualiosios kodavimo schemos saugumą, tai beveik optimalus fono periodas su iš anksto nustatytu kontrastu δ turi būti skaičiuojamas pagal šias formules: $\lambda_b = \frac{\pi\lambda_s}{2\arccos\left(\sqrt{8}\delta\right)}$ ir $\lambda_b = \frac{\pi\lambda_s}{2\left(\pi - \arccos\left(\sqrt{8}\delta\right)\right)}$.

Tarkime, kad muaro gardelės periodas slaptos informacijos srityje yra $\lambda_s = 0{,}2$, o kontrastas δ yra pasirinktas $0{,}05$, $0{,}15$ ir $0{,}24$. Tada pagal (2.12) lygtį apskaičiuotos periodo λ_b reikšmės yra atitinkamai lygios 0,22, 0,28 ir 0,38. Periodo $\lambda_b = 0{,}28$ reikšmė, pažymėta pilku rombu 2.5 paveiksle, atitinka 2.4 paveikslo (b) dalį; periodo $\lambda_b = 0{,}22$ reikšmė, pažymėta pilku apskritimu 2.5 paveiksle, atitinka 2.4 paveikslo (c) dalį; periodo $\lambda_b = 0{,}38$ reikšmė, pažymėta pilka žvaigžde 2.5 paveiksle, atitinka 2.4 paveikslo (d) dalį.



2.5 pav. Nelygybės $\frac{\left|cos\left(\frac{\pi}{2}\frac{\lambda_s}{\lambda_b}\right)\right|}{\sqrt{8}} \geq \delta$ sprendiniai: tamsiai pilka spalva pažymėtos sritys, kuriose $\frac{cos\left(\frac{\pi}{2}\frac{\lambda_s}{\lambda_b}\right)}{\sqrt{8}} \geq \delta$, šviesiai pilka spalva – sritys, kuriose $\frac{cos\left(\frac{\pi}{2}\frac{\lambda_s}{\lambda_b}\right)}{\sqrt{8}} \leq -\delta$. Esant fiksuotai reikšmei $\lambda_s = 0{,}2$, pilkas skritulys žymi $\lambda_b = 0{,}22$ ir $\delta = 0{,}05$, pilkas rombas – $\lambda_b = 0{,}28$ ir $\delta = 0{,}15$, pilka žvaigždė – $\lambda_b = 0{,}38$ ir $\delta = 0{,}24$

2.2. Deformuojamosios muaro gardelės pritaikymas dinaminei vizualiajai kriptografijai[3]

2.2.1. Deformuojamoji muaro gardelė tiesinio deformacijų lauko atveju

Tarkime, kad $a(x) = Ax$. Šiuo atveju nuokrypis nuo pusiausvyros padėties yra proporcingas koordinatei x. Kitaip tariant, harmoninė muaro gardelė gali būti formuojama ant vienmačio kūno paviršiaus jam esant pusiausvyros būsenoje, tačiau muaro gardelė deformuosis, kai kūnas svyruos. Tai yra esminis skirtumas lyginant su nedeformuojamąja muaro gardele, aprašyta 1.7.2 skyrelyje, kai nedeformuojamas vienmatis kūnas svyruoja apie pusiausvyros padėtį, ir muaro gardelė nėra deformuojama.

Šiuo atveju tiesinimas apie tašką x_0 aprašomas:

$$\begin{aligned} a(x) &= Ax_0 + A(x - x_0); \\ a_0 &= Ax_0; \\ \dot{a}_0 &= A. \end{aligned} \tag{2.13}$$

Tada (1.17) lygtis atrodo taip:

$$F(x,t) = \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}\frac{x}{1+A\sin t}\right). \tag{2.14}$$

[3] *Šiame skyriuje pristatomi rezultatai buvo publikuoti straipsnyje*:
Image hiding in time-averaged moire gratings on finite element grids
Vaidelys M.; Ragulskienė J.; Aleksienė S.; Ragulskis M.

Reiškinį $\frac{1}{1+A\sin t}$ skleisdami Teiloro eilute ir įstatę į (2.14) lygtį gauname:

$$F(x,t)=\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi x}{\lambda}\left(1-A\sin t+O(A^2)\right)\right)\approx$$

$$\approx\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x(1-A\sin t)\right)=\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x-\frac{2\pi}{\lambda}Ax\sin t\right)= \qquad (2.15)$$

$$=\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)\cos\left(\frac{2\pi}{\lambda}Ax\sin t\right)+\frac{1}{2}\sin\left(\frac{2\pi}{\lambda}x\right)\sin\left(\frac{2\pi}{\lambda}Ax\sin t\right).$$

Pažymėkime, kad $0<A\ll 1$ (kai $A=1$, gauname singuliarumą). Tada laike vidurkintas vaizdas bus:

$$\lim_{T\to\infty}\frac{1}{T}\int_0^T F(x,t)dt=\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)\lim_{T\to\infty}\frac{1}{T}\int_0^T\cos\left(\frac{2\pi}{\lambda}Ax\sin t\right)dt=$$

$$=\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)\left[\lim_{T\to\infty}\frac{1}{T}\int_0^T\cos\left(\frac{2\pi}{\lambda}Ax\sin t\right)dt \qquad (2.16)$$

$$+i\lim_{T\to\infty}\frac{1}{T}\int_0^T\sin\left(\frac{2\pi}{\lambda}Ax\sin t\right)dt\right].$$

Kadangi $\lim_{T\to\infty}\frac{1}{T}\int_0^T\sin\left(\frac{2\pi}{\lambda}Ax\sin t\right)dt=0,$ tai (2.16) lygtį galime perrašyti tokiu būdu:

$$\lim_{T\to\infty}\frac{1}{T}\int_0^T F(x,t)dt=$$

$$=\tfrac{1}{2}+\tfrac{1}{2}\cos\left(\tfrac{2\pi}{\lambda}x\right)\lim_{T\to\infty}\tfrac{1}{T}\int_0^T\left[\cos\left(\tfrac{2\pi}{\lambda}Ax\sin t\right)+i\sin\left(\tfrac{2\pi}{\lambda}Ax\sin t\right)\right]dt. \qquad (2.17)$$

Pritaikius Oilerio formulę $e^{iz}=\cos z+i\sin z$ gauname:

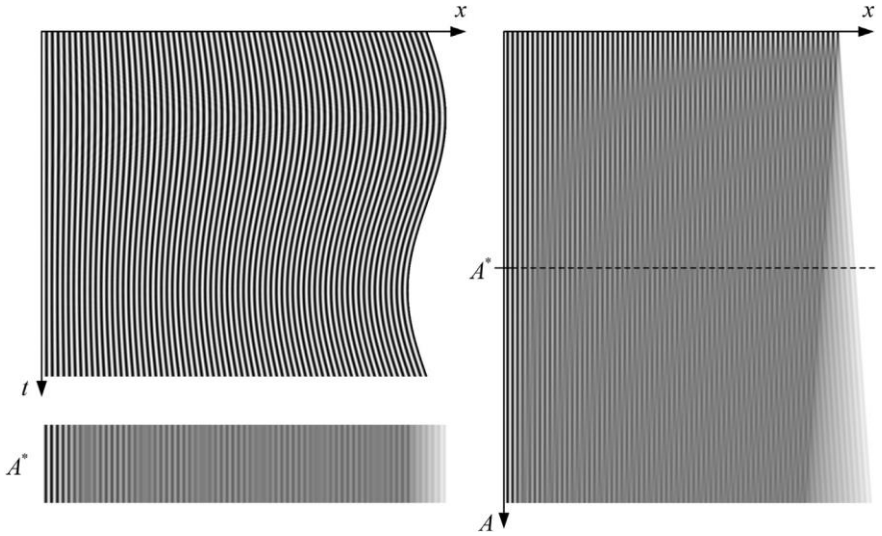
$$\lim_{T\to\infty}\tfrac{1}{T}\int_0^T F(x,t)dt=\tfrac{1}{2}+\tfrac{1}{2}\cos\left(\tfrac{2\pi}{\lambda}x\right)\lim_{T\to\infty}\tfrac{1}{T}\int_0^T e^{i\frac{2\pi}{\lambda}Ax\sin t}dt. \qquad (2.18)$$

Žinome, kad pirmojo tipo nulinės eilės Beselio funkcija aprašoma tokiu būdu: $J_0=\frac{1}{\pi}\int_0^\pi e^{iz\,cos\theta}d\theta$. Tada gausime [10]:

$$\lim_{T\to\infty}\tfrac{1}{T}\int_0^T F(x,t)dt=\tfrac{1}{2}+\tfrac{1}{2}\cos\left(\tfrac{2\pi}{\lambda}x\right)J_0\left(\tfrac{2\pi}{\lambda}Ax\right). \qquad (2.19)$$

Laike vidurkintos muaro juostos formuosis, kai $\frac{2\pi}{\lambda}Ax=r_k;\ k=1,2,\ldots$ [10] (2.6 pav.). Muaro gardelės judesys per vieną periodą pavaizduotas viršutiniame kairiajame 2.6 paveikslo kampe. Vienmatės muaro gardelės kairioji pusė yra pritvirtinta ir nejuda. Dešinė deformuojamosios muaro gardelės pusė svyruoja iš anksto nustatyta amplitude $A^*=0{,}05$, muaro gardelės periodas pusiausvyros padėtyje $\lambda=0{,}015$. Kairiajame apatiniame to paties paveikslo kampe matome vienmatės gardelės laike vidurkintą išdidintą vaizdą, kai $A^*=0{,}05$ – paveiksle aiškiai matyti laike vidurkintos

interferencinės juostos. Dešinėje paveikslo pusėje parodyti vienmačių muaro gardelių laike vidurkinti vaizdai, didėjant amplitudei A. Kuo didesnė harmoninių svyravimų amplitudė, tuo didesnis skaičius muaro interferencinių juostų bus matyti laike vidurkintame vaizde. Horizontalia brūkšniuota linija žymima amplitudė $A^* = 0{,}05$.



2.6 pav. Vienmatės deformuojamosios gardelės ($\lambda = 0{,}015$) harmoniniai svyravimai išryškina laike vidurkintas interferencines juostas. Vienas harmoninių svyravimų periodas pavaizduotas viršutiniame kairiajame kampe; vienmatis laike vidurkintas vaizdas, kai $A^* = 0{,}05$, matomas apatiniame kairiajame kampe; laike vidurkintų interferencinių juostų formavimasis, didėjant amplitudei $A = [0{,}001, 0{,}1]$, matyti dešinėje

2.2.2. Deformuojamoji muaro gardelė netiesinio deformacijų lauko atveju

Šiuo atveju tikslas – sukurti tokią vaizdų slėpimo schemą, kuri būtų pagrįsta deformuojamąja muaro gardele, suformuota baigtinių elementų metodu. Todėl deformacijų laukas $a(x)$ yra netiesinė funkcija. Taigi būtina apsvarstyti ir atvirkštinį uždavinį.

Suformuluokime atvirkštinį uždavinį bendram atvejui, aprašytam (1.17) lygtimi. Kitaip tariant, keliame klausimą, koks turi būti vienmatės muaro gardelės periodo pasiskirstymas $\lambda(x)$, kad laike vidurkintame vaizde išryškėtų interferencinės juostos, kad ir kokia būtų funkcija $a(x)$.

Tarkime, kad $x_0 = 0$. Taip pat apibrėžiame, kad $\bar{a}(x) \approx a_0 + \dot{a}_0 x$. Tada (1.17) lygtis bus:

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

$$= \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}(x - a_0 \sin t)\left(1 - \dot{a}_0 \sin t + O(A^2)\right)\right) \approx$$

$$\approx \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}(x - a_0 \sin t)(1 - \dot{a}_0 \sin t)\right) = \tag{2.20}$$

$$= \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}\left((x + a_0\dot{a}_0\sin^2 t) - (a_0 + \dot{a}_0 x)\sin t\right)\right) =$$

$$= \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}(x + a_0\dot{a}_0\sin^2 t)\right)\cos\left(\frac{2\pi}{\lambda}\bar{a}(x)\sin t\right)$$
$$+ \frac{1}{2}\sin\left(\frac{2\pi}{\lambda}(x + a_0\dot{a}_0\sin^2 t)\right)\sin\left(\frac{2\pi}{\lambda}\bar{a}(x)\sin t\right).$$

Vidurkinant laike reikia pažymėti, kad $\lim_{T\to\infty}\frac{1}{T}\int_0^T \sin\left(\frac{2\pi}{\lambda}(a_0 + \dot{a}_0 x)\sin t\right) = 0$, nes sinuso funkcija yra nelyginė. Taip pat $\lim_{T\to\infty}\frac{1}{T}\int_0^T \sin^2 t dt = 0{,}5$.

Tokiu būdu laike vidurkintas vaizdas aprašomas taip:

$$\lim_{T\to\infty}\frac{1}{T}\int_0^T F(x,t)dt =$$

$$= \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}\left(x + \frac{1}{2}a_0\dot{a}_0\right)\right)\lim_{T\to\infty}\frac{1}{T}\int_0^T \cos\left(\frac{2\pi}{\lambda}\bar{a}(x)\sin t\right)dt =$$

$$= \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}\left(x + \frac{1}{2}a_0\dot{a}_0\right)\right)\lim_{T\to\infty}\frac{1}{T}\int_0^T e^{i\frac{2\pi}{\lambda}a(x)\sin t}dt = \qquad (2.21)$$

$$= \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}\left(x + \frac{1}{2}a_0\dot{a}_0\right)\right)J_0\left(\frac{2\pi}{\lambda}\bar{a}(x)\right).$$

Laike vidurkintos interferencinės juostos formuosis, kai $\frac{2\pi}{\lambda}\bar{a}(x) = r_k; k = 1, 2, \ldots$. Nors ši lygybė gerai atitinka anksčiau aptartus rezultatus, ji toli gražu nėra triviali ir tiesiogiai neišplaukia iš problemos formuluotės. Reikėtų pažymėti, kad tiesinimas atliekamas iš anksto pasirinktai koordinatei x, nors amplitudžių laukas buvo apibrėžtas kaip tiesinis skyrelyje 2.2.1. Norint sėkmingai įgyvendinti dinaminės vizualiosios kriptografijos schemą reikia, kad tam tikra paslėpto vaizdo sritis virstų laike vidurkintomis interferencinėmis juostomis. Vienintelis kontroliuojamas slapto vaizdo parametras yra periodas $\lambda(x)$. Remdamiesi (2.21) lygybe priimkime, kad periodo pasiskirstymas galėtų būti apibrėžtas taip:

$$\lambda(x) = \frac{2\pi}{r_k}\bar{a}(x); k = 1, 2, \ldots . \qquad (2.22)$$

Sąryšyje (2.22) funkcija $\bar{a}(x)$ apibrėžiama kaip tiesinis amplitudžių laukas. Hipotezė, kad $\bar{a}(x)$ gali būti pakeistas į $a(x)$ (2.22) lygybėje, bus patikrinta taikant skaitinius metodus.

Tarkime, kad vienmatė tampri struktūra virpa pagal dėsnį:

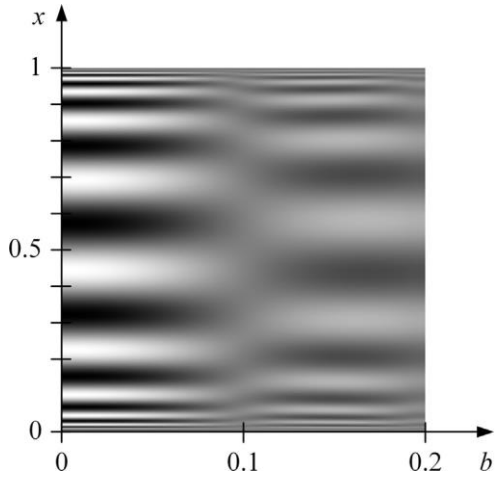
$$u(x,t) = 0{,}1\ \sin(\pi x)\sin(\omega t + \varphi),\ 0 \ll x \ll 1. \qquad (2.23)$$

Pateikta lygybė leidžia manyti, kad laike vidurkintos interferencinės juostos formuosis visoje srityje x, kai stacionarios muaro gardelės periodas yra:

$$\lambda(x) = 0.1\frac{2\pi}{r_1}\sin(\pi x). \quad (2.24)$$

Svyravimai vyks pagal dėsnį, aprašytą (2.23) lygtimi. Parametro k reikšmė parenkama lygi 1, nes šiuo atveju pirmosios laike vidurkintos interferencinės juostos kontrastas yra didžiausias.

Pažymėtina, kad stacionarios muaro gardelės konstravimas pagal (2.24) sąryšį nėra ypatingai sunkus uždavinys, išskyrus sritis, kuriose muaro gardelės periodas greitai artėja į nulį ir pikselis nėra pakankamai mažas tam, kad reprezentuotų gardelės pilkio lygio svyravimus. Tai galima pamatyti kairėje 2.7 paveikslo pusėje.



2.7 pav. Vienmatės muaro gardelės laike vidurkintas vaizdas. Periodo kitimas aprašomas (2.24) lygtimi. Nuokrypio nuo pusiausvyros padėties $u(x,t)$ kitimas aprašomas (2.25) lygtimi

Antra vertus, užuot taikę muaro gardelės svyravimus pagal (2.23) lygtį, nustatykime judėjimo dėsnį remdamiesi išraiška:

$$u(x,t) = b\sin(\pi x)\sin(\omega t + \varphi),\ 0 \ll x \ll 1. \quad (2.25)$$

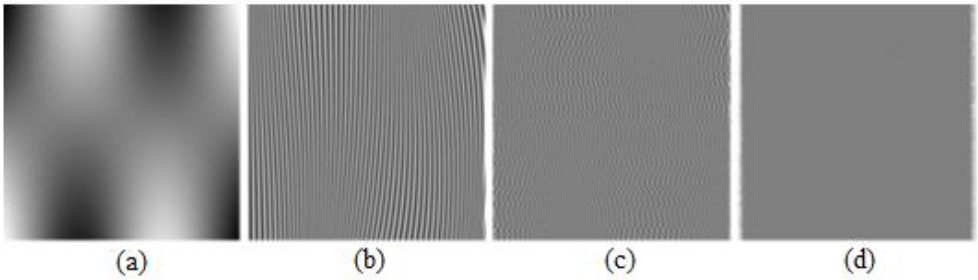
čia parametras b kinta nuo 0 iki 0,2, kaip matyti iš 2.7 paveikslo. Akivaizdu, kad laike vidurkinta interferencinė juosta formuojasi, kai $b = 0{,}1$. Todėl teiginys, kad ištiesintas amplitudžių laukas $\bar{a}(x)$ gali būti pakeistas į $a(x)$ (2.22) lygtyje teisingas net ir esant tokiam sudėtingam netiesiniam judėjimui, aprašytam (2.23) lygtimi.

2.2.3. Dinaminė vizualioji kriptografija, pagrįsta deformuojamosiomis muaro gardelėmis, remiantis baigtinių elementų metodu

Kaip minėta anksčiau, laike vidurkintų juostų formavimuisi bus panaudotas netiesinis deformacijų laukas. Dvimatis deformacijų $a(x;y)$ laukas, sukonstruotas taikant baigtinių elementų metodą, yra sukarpomas horizontaliai. Vienmatis periodo pasiskirstymas skaičiuojamas gretimose muaro gardelėse. Taigi kiekviena dvimatė skaitmeninio vaizdo pikselių eilutė yra interpretuojama kaip vienmatis amplitudžių laukas $a(x)$. Šis procesas atsispindi 2.8 paveiksle.

2.8(a) paveiksle vaizduojama plokštelės dvyliktoji tikrinė formą – juodos zonos reiškia maksimalias deformacijas nuo pusiausvyros padėties, baltos zonos nurodo sritis,

kurios nesvyruoja. Pirmiausia reikia padaryti taip, kad didžiausia svyravimų amplitudė būtų suderinta su didžiausios deformacijos tašku – formos funkcijos reikšmė turi būti padauginta iš konstantos, apibrėžtos iš anksto. Paskui formuojama muaro gardelė. 2.8(a) paveikslo rezoliucija yra 500×500 pikselių. Taigi 2.8(b) paveiksle pavaizduota 500 horizontalių vienmačių muaro gardelių. Periodo kitimas gardelių srityje aprašytas pagal (2.15) formulę. Vienintelis skirtumas tas, kad tiesinis deformacijų laukas $\bar{a}(x)$ yra pakeičiamas į $ka(x) + b$; čia $a(x)$ yra tam tikros gardelės formos funkcijos skaitinė reikšmė, k ir b yra teigiamosios, didesnės už nulį, konstantos. Konstanta b reikalinga tam, kad išvengtume singuliarumo taškų tose vietose, kuriose amplitudės $a(x)$ tampa lygios 0. Konstanta k reikalinga skaitinių amplitudžių reikšmėms kontroliuoti. Nustačius $k = 0{,}0025$ ir $b = 0{,}0075$ tolimesniems skaičiavimams, pradinis tikrinių reikšmių intervalas $[-1;\ 1]$ pakeičiamas į reikalingą amplitudžių intervalą $[0{,}005;\ 0{,}01]$.



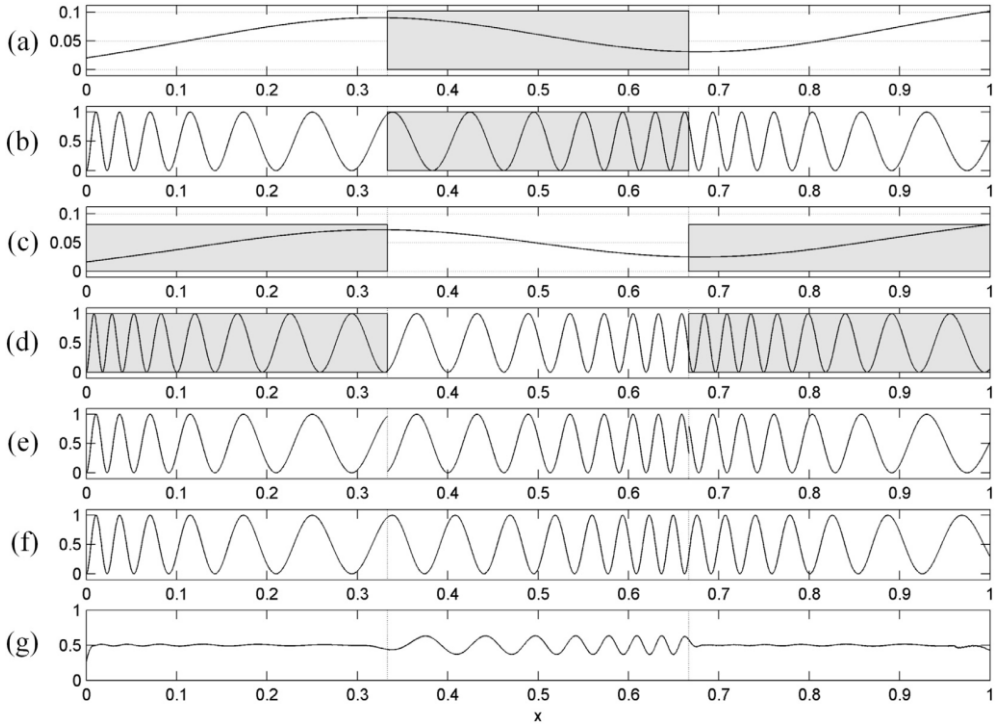
2.8 pav. Stačiakampės plokštelės harmoniniai svyravimai pagal 12-ąją tikrinę formą sukuria pilką dvimatį laike vidurkintą vaizdą: (a) tikrinę formą; (b) stacionarią muaro gardelę (gardelės periodas kinta intervale $\lambda = [0{,}013;\ 0{,}026]$; $\lambda(x) = \frac{2\pi}{r_1} a(x)$; (c) muaro gardelėje užkoduotą vaizdą; (d) laike vidurkintą vaizdą, kai užkoduotas vaizdas virpinamas pagal 12-ąją tikrinę formą

Pažymėtina, kad visų 500 vienmačių gardelių pradinė fazė yra nustatyta 0 – tokiu būdu 2.8(b) paveiksle parodytas interpretuojamas linijų masyvas, kuriame matoma pati formos funkcija. 2.8(c) paveiksle matome vaizdą, gautą pritaikius stochastinį pradinės fazės perstūmimo algoritmą. 2.8(d) paveiksle matyti, kad vienkrypčiai svyravimai x ašies kryptimi suformuoja laike vidurkintas interferencines juostas. Gautas paveikslas yra visiškai pilkas, išskyrus dešinę ir kairę puses, kuriose paveikslas tampa kiek netolygus.

Slapta informacija įterpiama į užkoduotą paveikslą pritaikius fazės reguliarizavimo algoritmą, pateiktą [8] šaltinyje. Šio algoritmo veikimas parodytas 2.9 paveiksle. Tarkime, kad amplitudės $a(x)$ kitimas pavaizduotas 2.9(a) paveiksle. Šį kitimą atitinkantis vienmatės gardelės pilkumo lygis parodytas 2.9(b) paveiksle.

Padarykime prielaidą, kad slapta informacija bus patalpinta vidurinėje gardelės dalyje. Kitais žodžiais tariant, laike vidurkintos muaro interferencinės juostos turi formuotis visur, išskyrus vidurinį intervalą. Harmoninių svyravimų muaro gardelės amplitudžių laukas yra pakeliamas, padauginant jį iš konstantos C, kuri yra kiek mažesnė (arba didesnė) už 1 (kiek mažesnė ar didesnė konstantos C reikšmė, nusako (2.5) nelygybė). 2.9(c) paveiksle parodytas amplitudžių lauko $a(x)$ kitimas yra toks pats, kaip ir 2.9(a) paveiksle, tiktai padaugintas iš $C = 0{,}8$. Toks didelis pokytis parinktas vien tam,

kad 2.9 paveiksle būtų galima plika akimi įžiūrėti amplitudžių lauko pasikeitimus. Kitimą atitinkanti muaro gardelė parodyta 2.9(d) paveiksle.



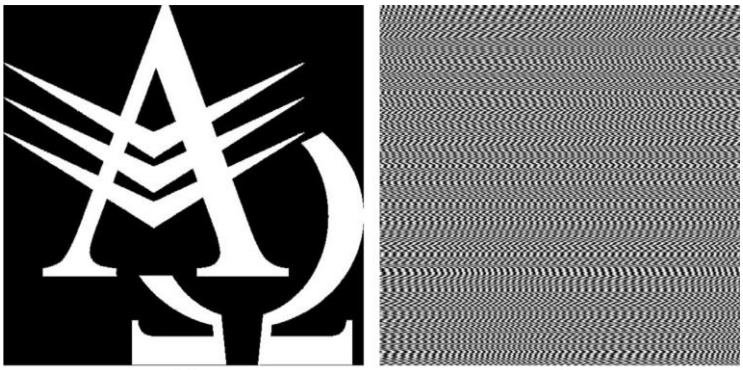
2.9 pav. Scheminė diagrama, kuria iliustruojamas slaptos informacijos užkodavimas vienmatėje muaro gardelėje: (a) amplitudžių laukas, sugeneruotas pagal tam tikrą iš anksto nustatytą tikrinę formą; (b) atitinkama muaro gardelė; (c) amplitudžių laukas, naudojamas slaptos informacijos dalyje; (d) atitinkama muaro gardelė. Sudėtinė muaro gardelė naudoja kairįjį ir dešinįjį trečdalius iš (b) dalies ir vidurinįjį trečdalį iš (d) dalies. Visi kreivės netolydumai iš (e) dalies pašalinami taikant fazių reguliarizavimo algoritmą ((f) dalis). Laike vidurkintas (f) dalies vaizdas parodytas (g) dalyje

Tada kairysis ir dešinysis gardelės trečdaliai iš 2.9(b) dalies yra tiesiogiai perkeliami į 2.9(e) paveikslo kraštus, o vidurinis gardelės trečdalis iš 2.9(d) dalies perkeliamas į 2.9(e) paveikslo vidurį. Tokiu būdu gaunama netolydi gardelė. Šiam trūkumui pašalinti parenkama tinkama fazė – taip pašalinami fazės šuoliai sujungimo taškuose. Svarbu pažymėti, kad šio proceso metu pats periodo kitimas išlieka pastovus. Galiausiai 2.9(f) paveikslo laike vidurkintas vaizdas yra parodytas paveikslo 2.9(g) dalyje, čia svyravimai aprašomi (1.11) formule ir amplitudžių laukas $a(x)$ apibrėžiamas kaip 2.9(a) paveiksle. Laike vidurkintos muaro interferencinės juostos formuojasi kairiajame ir dešiniajame trečdaliuose, be to, aiškiai matyti, kad vidurinis trečdalis nėra tolygiai pilkas.

Štai tokia vaizdo slėpimo schema gali būti efektyviai pritaikyta paslepiant juodai baltą vaizdą į užkoduotą paveikslą. Labai svarbu pažymėti, kad formos funkcija yra traktuojama kaip slaptas raktas vizualiosios informacijos dekodavimui. Kitais žodžiais

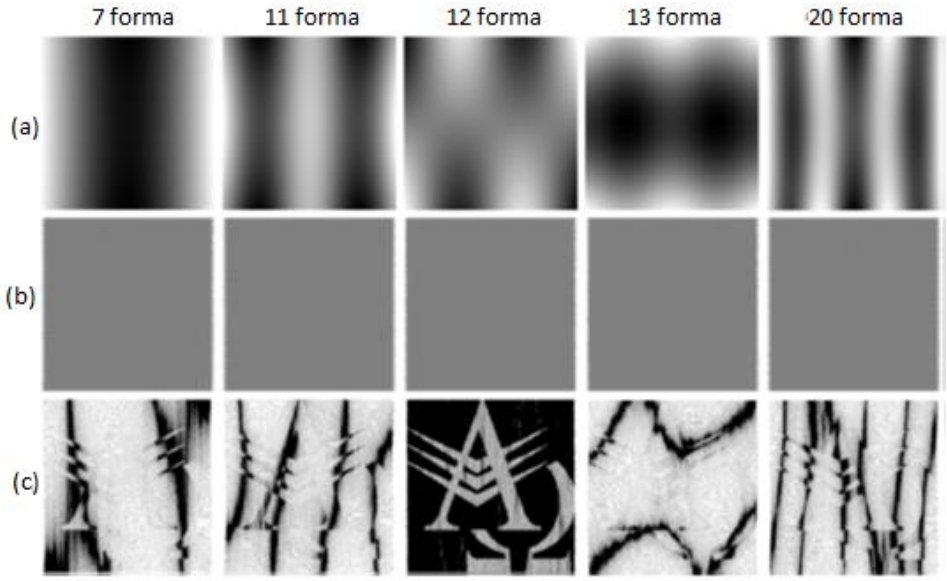
tariant, slapta informacija išryškėja tik tada, kai paveikslas virpinamas pagal tokią formos funkciją, kuria buvo užkoduotas.

Tokios vaizdų slėpimo schemos, pagrįstos dinamine vizualiąja kriptografija, funkcionalumą pademonstruoja skaitinis eksperimentas. Slaptas juodai baltas vaizdas (kaip matyti 2.10(a) paveiksle) yra užkoduojamas (2.10(b) paveikslas), pritaikant 12-ąją stačiakampės plokštelės formos funkciją. Atsitiktinės pradinės fazės ir fazės reguliarizavimo algoritmai pritaikyti tam, kad paslėptų slaptą vaizdą. Iš užkoduoto paveikslo plika akimi neįmanoma atpažinti slapto vaizdo. Maža to – slaptas vaizdas gali išryškėti tik tada, kai deformuojamas užkoduotas vaizdas yra virpinamas pagal tokią formos funkciją, pagal kurią jis buvo užkoduotas.



2.10 pav. Slaptas vaizdas parodytas (a) dalyje; statinis vaizdas su užkoduota slapta informacija (kodavimas atliktas tokiu būdu, kad slapta informacija išryškėja, kai užkoduotas vaizdas virpinamas pagal 12-ąją tikrinę formą) parodytas (b) dalyje. Periodo reikšmės parenkamos intervale nuo 0,013 iki 0,026

Kitais žodžiais tariant, formos funkcija gali būti laikoma vizualiojo dekodavimo procedūros raktu. 2.11 paveiksle matyti vizualiojo dekodavimo rezultatai, gauti užkoduotą paveikslą virpinant pagal skirtingas formos funkcijas. Vaizdo išryškinimo procedūros [85] taikomos tam, kad būtų geriau matomos muaro interferencinės juostos laike vidurkintuose vaizduose.



2.11 pav. Tikrinė forma pritaikoma kaip raktas užkoduotam vaizdui dešifruoti. Pirmoje eilutėje parodytos skirtingos tikrinės formos, antroje eilutėje – laike vidurkinti vaizdai, trečioje eilutėje – paryškinti laike vidurkinti vaizdai

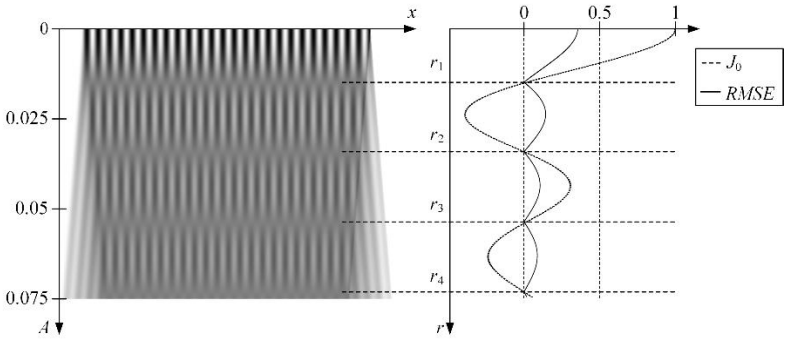
2.3. Deformuojamoji Ronči tipo muaro gardelė[4]

Ronči tipo muaro gardelė yra aprašoma taip:

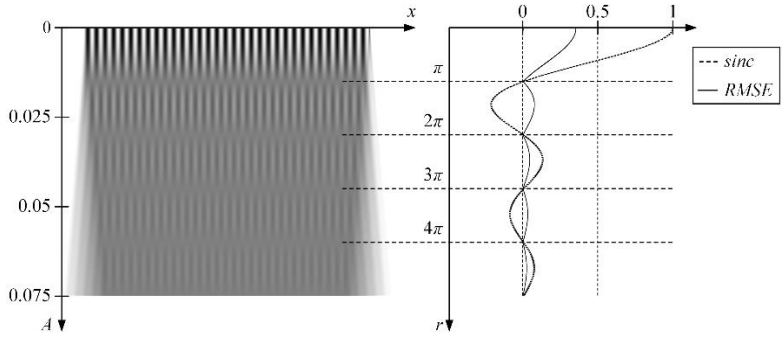
$$F(x) = \frac{1}{2} + \frac{1}{2}\operatorname{sign}\cos\left(\frac{2\pi}{\lambda}x\right). \qquad (2.26)$$

(1.23) sąryšis netinka Ronči tipo muaro gardelei – laike vidurkintos muaro interferencinės juostos nesiformuos, kad ir kokią harmoninių svyravimų [86] amplitudę parinktume (2.12 paveikslas). Ronči tipo muaro gardelė suformuoja laike vidurkintas interferencines juostas tik tada, jei svyravimai yra trikampės bangos formos [86] – ši ypatinga savybė gali būti pritaikoma kaip papildomas saugumo faktorius dinaminės vizualiosios kriptografijos schemoje.

[4] *Šiame skyriuje pristatomi rezultatai buvo publikuoti straipsnyje*:
Dynamic visual cryptography scheme on the surface of a vibrating structure
Vaidelys M.; Aleksienė S., Ragulskienė J.



a)



b)

2.12 pav. Nelanksčios vienmatės muaro gardelės svyravimai suformuoja laike vidurkintas interferencines juostas. Kairėje paveikslo pusėje parodytas laike vidurkintas vaizdas, dešinėje paveikslo pusėje – RMSE paklaidos pusiausvyros padėtyje ir sinc bei Beselio funkcijos grafikai. Laike vidurkintos interferencinės juostos formuosis, jei harmoninis užkoduotas vaizdas virpinamas pagal harmoninį dėsnį (a). Jei užkoduotas vaizdas virpinamas pagal trikampės bangos formos funkciją (b), laike vidurkintos interferencinės juostos taip pat formuosis, tačiau tik tada, kai sutaps su sinc funkcijos šaknimis

Stačiakampėje Ronči tipo gardelėje užkoduotas vaizdas, suformuotas ant deformuojamos struktūros paviršiaus, nesvyruos pagal dėsnį, aprašytą (1.12) formulėje. Apibrėžkime trikampę bangos formos svyravimų funkciją, kurios periodas 2π ir reikšmių intervalas yra $[-1; 1]$:

$$u(t) = \frac{2}{\pi}\left(t - \pi\left|\frac{t}{\pi} + \frac{1}{2}\right|\right)(-1)^{\left|\frac{t}{\pi}+\frac{1}{2}\right|}. \qquad (2.27)$$

Pažymėkime $u(x, t)$ deformaciją nuo pusiausvyros padėties taške x laiko momentu t. Tada muaro gardelės deformaciją aprašysime (1.9)–(1.11) formulėmis.

Nagrinėkime vieną trikampės bangos funkcijos pusperiodį, kai nelanksti konstrukcija juda erdvėje pastoviu greičiu:

$$u(x,t) = a(x) \cdot t. \tag{2.28}$$

Ši formulė paprastu būdu aprašo trikampę bangos formos funkciją, kai $a(x)$ yra tikrinės formos svyravimai, o $t \in [-1;\ 1]$ yra laikas. Amplitudžių laukas $a(x)$ ištiesinamas taško x_0 aplinkoje panašiu būdu kaip ir 1.7.2 skyrelio (1.13)–(1.16) formulėse.

Išveskime vidurkinimo laike formulę nedeformuojamajai muaro gardelei. Tarkime, kad $a(x) = A$ (čia A yra konstanta) ir svyravimai vyksta pagal trikampę bangos formos funkciją. Tai reiškia, kad nedeformuojamojo kūno svyravimų apie pusiausvyros padėtį nuokrypiai yra lygūs $u(x,t) = At$ [72]. Tada muaro gardelės pilkumo lygis laiko momentu t apskaičiuojamas pagal formulę:

$$F(x,t) = \tfrac{1}{2} + \tfrac{1}{2}\cos\left(\tfrac{2\pi}{\lambda}(x - At)\right). \tag{2.29}$$

Vidurkinimo laike technika gali būti taikoma gardelės vaizdui registruoti [72]:

$$\begin{aligned}
&\frac{1}{2}\int_{-1}^{1} F(x,t)dt = \\
&= \frac{1}{2} + \frac{1}{4}\int_{-1}^{1}\left[\cos\left(\frac{2\pi}{\lambda}x\right)\cos\left(\frac{2\pi}{\lambda}A\mathrm{t}\right) + \sin\left(\frac{2\pi}{\lambda}x\right)\sin\left(\frac{2\pi}{\lambda}At\right)\right]dt = \\
&= \frac{1}{2} + \frac{1}{4}\cos\left(\frac{2\pi}{\lambda}x\right)\int_{-1}^{1}\cos\left(\frac{2\pi}{\lambda}A\mathrm{t}\right)dt + 0 = \\
&= \frac{1}{2} + \frac{1}{4}\cos\left(\frac{2\pi}{\lambda}x\right)\frac{\lambda}{2\pi A}\sin\left(\frac{2\pi}{\lambda}At\right) = \\
&= \frac{1}{2} + \frac{1}{4}\cos\left(\frac{2\pi}{\lambda}x\right)\frac{\lambda}{2\pi A}2\sin\left(\frac{2\pi}{\lambda}A\right) = \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)\frac{\sin\left(\frac{2\pi}{\lambda}A\right)}{\frac{2\pi}{\lambda}A} = \\
&= \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)\mathrm{sinc}\left(\frac{2\pi}{\lambda}A\right);
\end{aligned} \tag{2.30}$$

čia $\mathrm{sinc}(x) = \frac{\sin(x)}{x}$ yra sinc funkcija. Svarbu pažymėti, kad pilkumo lygio pasiskirstymas laike vidurkintame vaizde nepriklauso nuo trikampės bangos formos funkcijos (2.28) charakteristikų. Dėl šios priežasties supaprastinta forma gali būti taikoma tolimesniems skaičiavimams.

Pilkos laike vidurkintos muaro interferencinės juostos formuosis, kai $\mathrm{sinc}(x) = 0$ – tai įvyks tada, kai amplitudės bus $\frac{2\pi}{\lambda}A_k = r_k$ (šiuo atveju $r_k = \pi k,\ k = 1, 2, \ldots$ yra funkcijos $\mathrm{sinc}(x)$ šaknys). Tai matyti 2.12(b) paveiksle.

Išveskime laike vidurkintos deformuojamosios muaro gardelės pilkio intensyvumo formulę. Šiuo atveju tarsime, kad $a(x) = Ax$. Tiesinimas taško x_0 aplinkoje aprašomas taip pat, kaip ir 2.2.1 skyrelyje pagal (2.13) formules. Tada

$$F(x,t) = \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}\cdot\frac{x}{1 + \dot{a}_0 t}\right) =$$

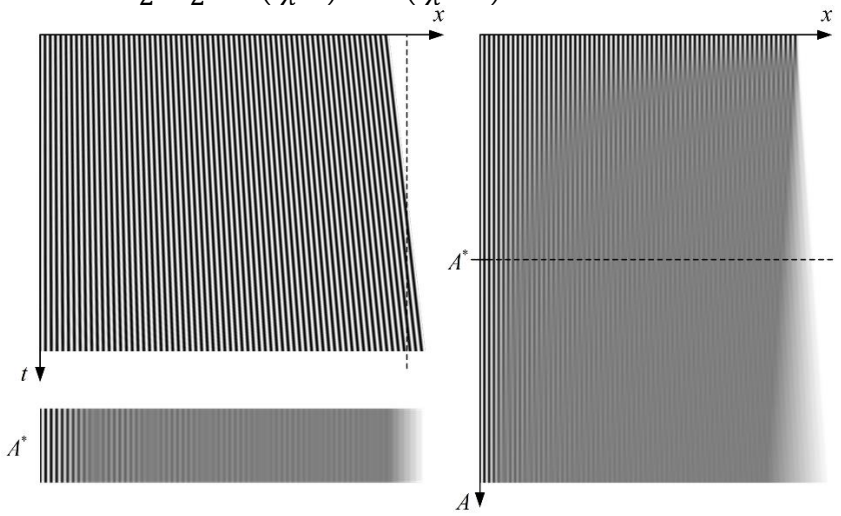
$$= \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}\left(1 - \left(\dot{a}_0 t + O((\dot{a}_0 t)^2 x)\right)\right)\right) \approx \tag{2.31}$$

$$\approx \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x - \frac{2\pi}{\lambda}Axt\right).$$

Būtina pažymėti, kad (2.31) lygtyje, kai $A = 1$, atsiranda singuliarumas. Todėl tariame, kad $0 < A \ll 1$. Tada laike vidurkintas vaizdas aprašomas tokiu būdu:

$$\frac{1}{2}\int_{-1}^{1} F(x,t)dt = \frac{1}{2} + \frac{1}{4}\cos\left(\frac{2\pi}{\lambda}x\right)\frac{\lambda}{2\pi Ax}2\sin\left(\frac{2\pi}{\lambda}Axt\right) = \tag{2.32}$$

$$= \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)\mathrm{sinc}\left(\frac{2\pi}{\lambda}Ax\right).$$



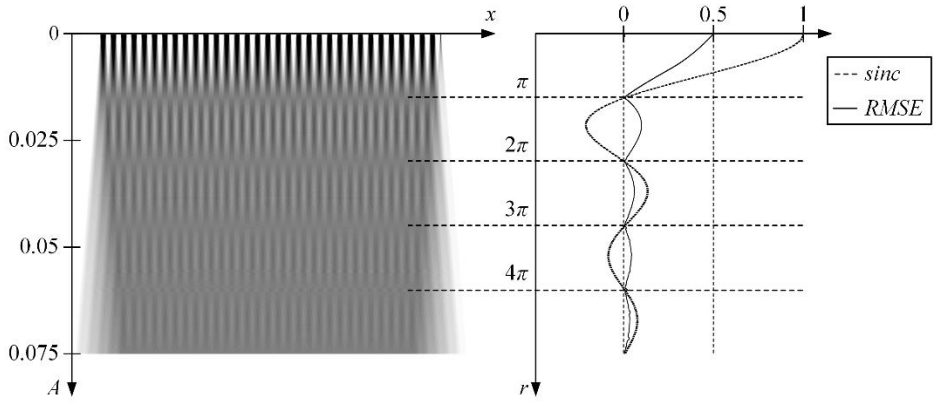
2.13 pav. Deformuojamoji vienmatė muaro gardelė suformuoja laike vidurkintas interferencines juostas tada, kai ji svyruoja pagal trikampę bangos formą. Vienas svyravimų periodas ($t \in [-1;\ 1]$) yra parodytas viršutiniame kairiajame paveiksle. Vienmatis laike vidurkintas vaizdas, kai $A^* = 0{,}05$, pavaizduotas apatiniame kairiajame paveiksle. Laike vidurkintų interferencinių juostų formavimasis, esant skirtingoms amplitudžių reikšmėms, parodytas dešinėje, $A = \overline{0{,}001, 0{,}1}$

Išveskime vidurkinimo laike formules, kai muaro gardelė yra deformuojamoji, o deformacijų laukas netiesinis. Pritaikę samprotavimus, panašius kaip 2.2.2 skyrelyje, laike vidurkintą vaizdą galime aprašyti taip:

$$\frac{1}{2}\int_{-1}^{1} F(x,t)dt = \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)\mathrm{sinc}\left(\frac{2\pi}{\lambda}\bar{a}(x)\right). \tag{2.33}$$

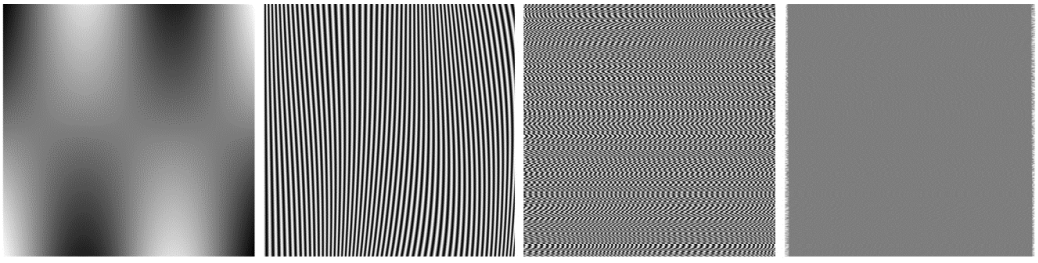
Sukonstruokime vaizdų slėpimo schemą, pagrįstą deformuojamąja Ronči tipo muaro gardele, kai amplitudžių laukas suformuojamas pritaikant baigtinių elementų metodą. Iškelkime hipotezę, kad laike vidurkintos interferencinės juostos formuosis, kai Ronči

tipo muaro gardelė svyruos pagal trikampę bangos formos funkciją. Ši hipotezė gali būti patvirtinta eksperimentiškai tokiu pačiu būdu, kaip tai buvo daryta su harmonine muaro gardele. 2.14 paveiksle matyti, kad laike vidurkintos interferencinės juostos formuosis, kai $r_k = \pi k$, jei Ronči tipo muaro gardelė svyruos pagal trikampę bangos formos funkciją.



2.14 pav. Laike vidurkintos interferencinės juostos susiformuos, jei Ronči tipo muaro gardelė svyruos pagal trikampę bangos formos funkciją. Interferencinės juostos formuosis ties sinc funkcijos šaknimis $r_k = \pi k$

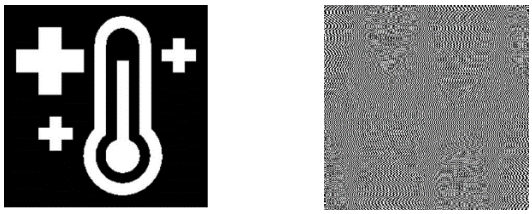
Laike vidurkintos interferencinės juostos formuosis naudojant anksčiau minėtus netiesinius deformacijų laukus. Dvimatis deformacijų laukas turi būti horizontaliai (arba vertikaliai) supjaustytas. Jis apibrėžiamas pritaikant baigtinių elementų metodą. Visas šis procesas parodytas 2.15 paveiksle.



2.15 pav. Ronči tipo muaro gardelės trikampės bangos formos svyravimai pagal 10-ąją tikrinę formą suformuoja pilką dvimatį vaizdą: (a) tikrinė forma; (b) stacionari muaro gardelė (gardelės periodas kinta intervale $\lambda = [0{,}002;\ 0{,}02]$; $\lambda(x) = 2a(x)$); (c) muaro gardelėje užkoduotas slaptas vaizdas; (d) laike vidurkintas vaizdas, kai užkoduotas vaizdas virpinamas pagal 10-ąją tikrinę formą

Pasiūlyta vaizdo slėpimo schema efektyviai paslepia juodai baltą vaizdą užkoduotame vaizde. Norėdami užtikrinti vaizdo slėpimo schemos, pagrįstos dinamine vizualiąja kriptografija, funkcionalumą, paslėpkime juodai baltą slaptą vaizdą (paveikslas 2.16(a)) į užkoduotą vaizdą (paveikslas 2.16(b)). Užkoduotas vaizdas

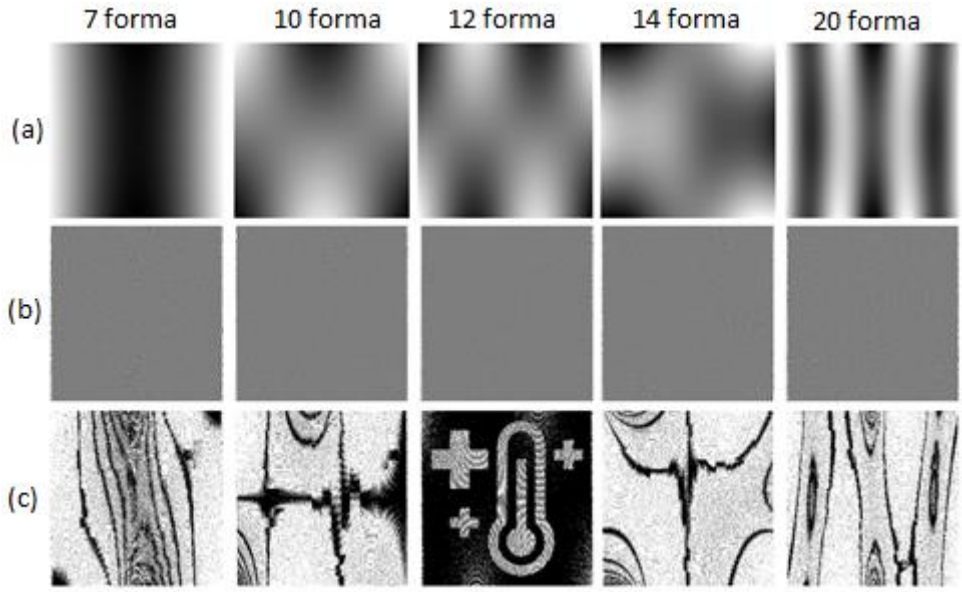
sugeneruotas pasinaudojus 12-ąja tikrine forma. Fazių reguliarizacijos algoritmas pritaikytas norint paslėpti slaptą vaizdą. Plika akimi negalime įžiūrėti slaptos informacijos užkoduotame vaizde.



a) b)

2.16 pav. Slaptas vaizdas parodytas (a) dalyje; slapta informacija, užkoduota naudojantis 12-ąja tikrine forma, parodyta (b) dalyje

Maža to, dekodavimas priklauso nuo pradinės tikrinės formos struktūros, ir tai yra dar vienas saugumo faktorius – slapta informacija neišryškėja užkoduotą vaizdą virpinant pagal neteisingą tikrinę formą. Taigi tikrinę formą galime laikyti raktu vizualiojo dekodavimo procese. Šį faktą galime pademonstruoti 2.17 paveiksle, kai dekodavimui naudojamos skirtingos tikrinės formos. Interferencinėms juostoms išryškinti laike vidurkintame vaizde taikomi kontrasto paryškinimo algoritmai.

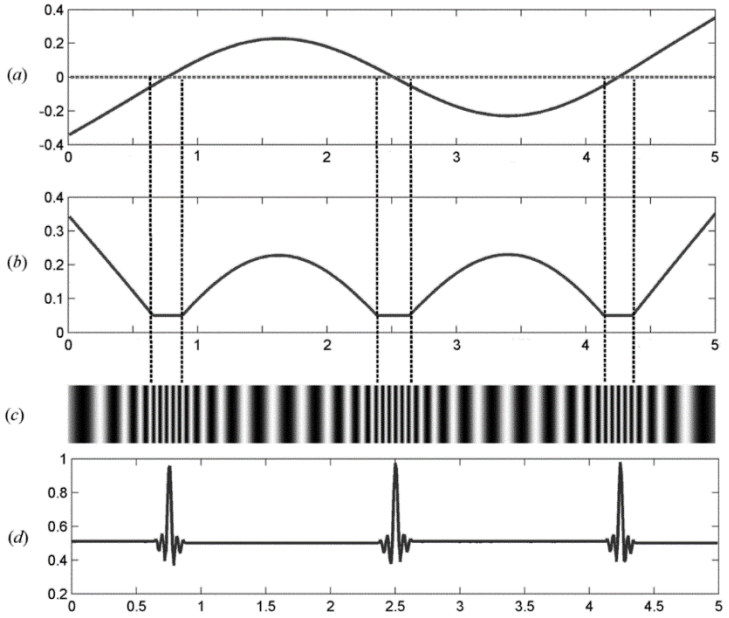


2.17 pav. Tikrinė forma pasitarnauja kaip raktas slaptai informacijai iššifruoti. Pirmoje eilutėje – skirtingos tikrinės formos; antroje eilutėje – laike vidurkinti vaizdai; trečioje eilutėje – laike vidurkinti išryškinti vaizdai

2.4. Deformuojamoji muaro gardelė su nulinėmis zonomis[5]

2.2 skyriuje nagrinėjome atvejį, kai muaro gardelės amplitudžių laukas yra pakeliamas virš *x* ašies. Šis veiksmas buvo atliekamas tam, kad pagal (1.24) lygtį negautume neigiamųjų ir lygių nuliui muaro gardelės periodo reikšmių. Šitame poskyryje taikysime kitokią muaro gardelės periodo konstravimo metodiką lyginant su ankstesniuose skyriuose nagrinėta.

Laikysime, kad muaro gardelės periodas yra proporcingas tikrinės formos reikšmėms, paimtoms absoliučiuoju didumu. Tačiau tam tikruose taškuose tikrinės formos reikšmės tampa lygios nuliui. Šiuose taškuose ir jų aplinkoje nustatome fiksuotą teigiamąją nelygią nuliui mažą reikšmę. Tai galima pagrįsti faktu, kad periodo reikšmės, artimos nuliui, sutankina muaro gardelę – atstumas tarp dviejų gretimų gardelės pikų artėja į nulį. Norint išvengti šio trūkumo, nuliui artimi muaro gardelės periodai yra pakeičiami konstanta 0,05, kaip matyti iš 2.18(b) paveikslo.



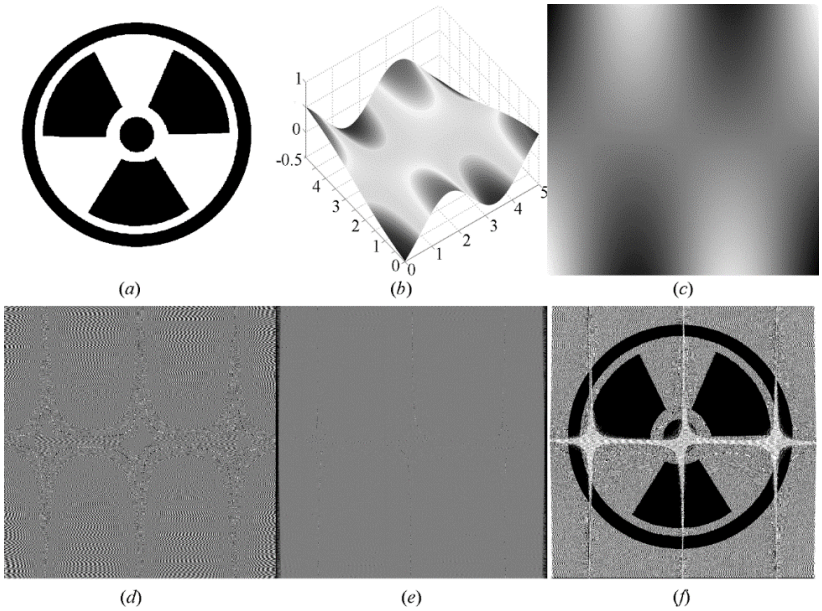
2.18 pav. Grafinė muaro gardelės konstravimo schema vienmačiu atveju: (a) viena iš tikrinės formos eilučių; (b) muaro gardelės periodo reikšmės, atitinkančios paveikslo (a) dalį; (c) muaro gardelės optinė vizualizacija; (d) laike vidurkinta muaro gardelė, esant harmoniniams svyravimams pagal (a) dalyje pateiktą tikrinę formą

Optinė muaro gardelės vizualizacija pateikta 2.18(c) paveiksle. Vertikalios brūkšniuotos linijos, jungiančios 2.18 paveikslo (a), (b), (c) dalis, žymi harmoninių svyravimų amplitudes, kurių reikšmės yra artimos nuliui. Būtina pabrėžti, kad šiuose intervaluose muaro gardelės tankis yra pastovus.

[5] *Šiame skyriuje pristatomi rezultatai buvo publikuoti straipsnyje*:
Dynamic visual cryptography on deformable finite element grids
Aleksienė S.; Vaidelys M.; Aleksa A.; Ragulskis M.

Fazių reguliarizacijos algoritmas [72] taikomas tam, kad išvengtume muaro gardelės netolydumo (paveikslas 2.18(c)). Laike vidurkinta muaro gardelė yra pavaizduota paveiksle 2.18(d). Svarbu pažymėti, kad harmoninių svyravimų amplitudės yra nevienodos skirtingose statinio muaro vaizdo vietose, ir muaro gardelės periodas kiekviename taške yra skaičiuojamas pagal (1.24) lygybę, išskyrus tris nedideles sritis – jose periodas yra pastovus dydis. Šiose srityse laike vidurkintos interferencinės juostos nesiformuoja (paveikslas 2.18(d)), kai struktūra yra virpinama pagal tam tikrą pasirinktą tikrinę formą.

2.19 paveiksle parodytas dvimatis pavyzdys. Slaptas vaizdas (2.19(a) paveikslas) yra užkoduotas į muaro gardelę (paveikslas 2.19(d)) pagal tikrinę formą, vaizduojančią harmoninius svyravimus (paveiksluose 2.19(b) ir 2.19(c) pavaizduota atitinkamai tikrinės formos trimatis vaizdas ir dvimatė projekcija). Tamsios ir baltos tikrinės formos sritys aprašo harmoninių svyravimų didžiausias amplitudes, reikšmės apie 0,5 nurodo sritis, kuriose nėra jokių svyravimų. Tai galima būtų pagrįsti faktu, kad visos tikrinės formos reikšmės yra aprašomos kaip pilkumo lygiai – mažiausia neigiamoji reikšmė reiškia juodą spalvą, didžiausia reikšmė reiškia taip pat juodą spalvą, kaip parodyta 2.19(b) paveiksle.



2.19 pav. (a) Slaptas vaizdas; (b) tikrinės formos trimatis vaizdas; (c) tikrinės formos dvimatė projekcija; (d) slaptas vaizdas, užkoduotas statinėje muaro gardelėje; (e) laike vidurkintas užkoduotas vaizdas; (f) išryškintas laike vidurkintas vaizdas

Jau anksčiau minėta, kad tikrinės formos sritys, artimos nuliui, yra pakeičiamos konstanta, lygia 0,05. Laike vidurkintas vaizdas parodytas 2.19(e) paveiksle. Kontrasto išryškinimo algoritmas, pritaikomas laike vidurkintam vaizdui, yra parodytas 2.19(f) paveiksle. Svarbu pažymėti, kad šviesios horizontalios ir vertikalios sritys, matomos 2.19(f) paveiksle, yra susiformavusios nulinių mazginių taškų aplinkoje, tačiau jos netrukdo identifikuoti slaptą vaizdą.

2.5. Dinaminė vizualioji kriptografija chaotinėse baigtinių elementų gardelėse[6]

Chaotinė dinaminė vizualioji kriptografija buvo nagrinėta [87, 88] straipsniuose. Šiuose darbuose laiko funkcija, apibrėžianti nuokrypį nuo pusiausvyros padėties, parenkama kaip Gauso ergodinis procesas su nuliniu vidurkiu ir iš anksto apibrėžta dispersija. Šioje disertacijoje nagrinėjamas atvejis, kai laiko funkcija apibrėžiama kaip Roslerio netiesinių diferencialinių lygčių sistemos chaotinis sprendinys.

2.5.1. Harmoniniai svyravimai ir deformuojamoji muaro gardelė

Tarkime, kad harmoninė muaro gardelė yra formuojama ant vienmačio deformuojamojo kūno paviršiaus. Tegul taško x poslinkis nuo pusiausvyros padėties yra $u(x,t)$. Tada deformuojamoji muaro gardelė aprašoma pagal (1.9) formulę, o nepriklausomasis kintamasis x gali būti išreikštas iš (1.10) sąryšio į (1.11) formą.

Taip pat tarkime, kad laiko ir erdvės kintamieji poslinkio funkcijoje gali būti atskirti:

$$u(x,t) = a(x) \cdot g(t); \tag{2.34}$$

čia $a(x)$ yra svyravimų formos funkcija, $g(t)$ – laiko funkcija.

Tada funkciją $a(x)$ ištiesinę apie pusiausvyros tašką $x = x_0$, gauname (1.13) sąryšį, kuriame $a_0 = a(x_0)$ ir $\dot{a}_0 = \left.\frac{da(x)}{dx}\right|_{x=x_0}$. Iš (1.10), (2.34), (1.11) formulių galima gauti tokį sąryšį:

$$x \approx \frac{z-(a_0-\dot{a}_0 x_0)g(t)}{1+\dot{a}_0 g(t)}. \tag{2.35}$$

Atitinkamai deformuojamąją muaro gardelę galima aprašyti išraiška:

$$F(x,t) \approx \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda} \cdot \frac{x-(a_0-\dot{a}_0 x_0)g(t)}{1+\dot{a}_0 g(t)}\right). \tag{2.36}$$

Laike vidurkinant, (2.36) formulė keičiasi į

$$F_t(x) \approx \frac{1}{2} + \frac{1}{2}\lim_{T\to\infty}\frac{1}{T}\int_0^T \cos\left(\frac{2\pi}{\lambda} \cdot \frac{x-(a_0-\dot{a}_0 x_0)g(t)}{1+\dot{a}_0 g(t)}\right) dt. \tag{2.37}$$

Pažymėtina, kad tiriamai struktūrai virpant kaip nedeformuojamajam kūnui pagal harmoninį dėsnį, t. y. $a(x) = A = const$ ir $g(t) = \sin(\omega t + \varphi)$, (2.31) formulė sutampa su (1.23). Jeigu deformacijų laukas yra tiesinis ir apibrėžiamas $a(x) = Ax$ [89], tada pilkumo lygio funkciją galime aprašyti (2.14) formule, kurią vidurkindami gauname:

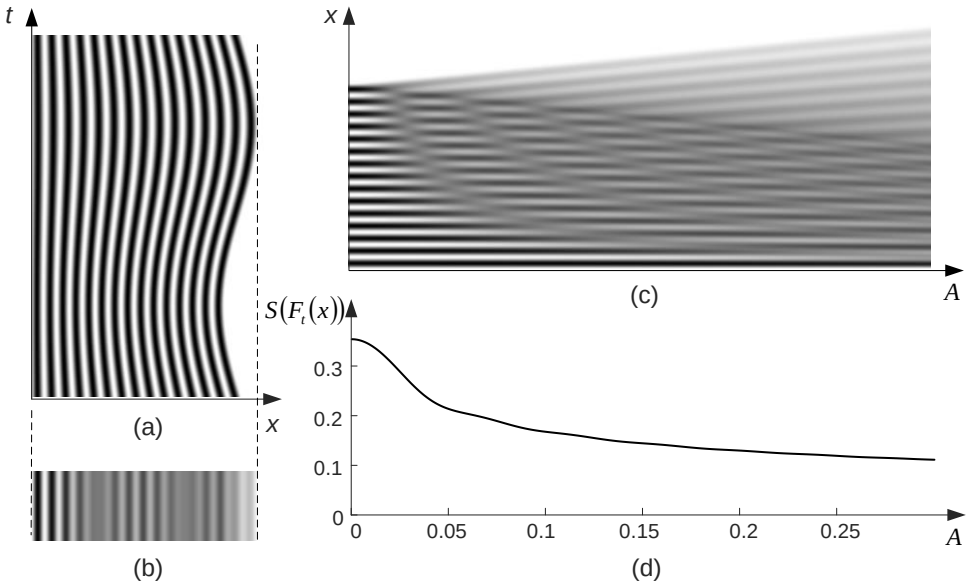
$$F_t(x) \approx \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right) J_0\left(\frac{2\pi}{\lambda}Ax\right). \tag{2.38}$$

Šiuo atveju laike vidurkintos muaro interferencinės juostos formuosis tada, kai $\frac{2\pi}{\lambda}Ax = r_i,\ \ i = 1, 2, \ldots$. Svarbu pastebėti šios formulės skirtumus nuo (1.24) formulės.

---

[6] *Šiame skyriuje pristatomi rezultatai buvo publikuoti straipsnyje*:
Optical image hiding based on chaotic vibration of deformable moiré grating
Lu G., Saunorienė L., Aleksienė S., Ragulskis M.

2.20 paveiksle parodytas laike vidurkintų muaro interferencinių juostų formavimąsis, kai muaro gardelė yra deformuojamoji.



2.20 pav. Vienmatės deformuojamosios muaro gardelės laike vidurkintas vaizdas. Gardelės periodas pusiausvyros padėtyje yra $\lambda = 0{,}2$: (a) vienmatės muaro gardelės judėjimas vieno periodo metu ($A = 0{,}075$); brūkšniuota linija rodo didžiausius poslinkius nuo pusiausvyros padėties; (b) laike vidurkintas (a) dalies vaizdas; (c) vienmatė laike vidurkinta muaro gardelė, didėjant amplitudei A; (d) laike vidurkinto vaizdo standartinis nuokrypis

Gardelės kairioji pusė yra nejudamai įtvirtinta, dešinioji pusė virpa pagal harmoninį dėsnį – stebėjimo lango amplitudė A kinta nuo 0 iki 0,3. Pusiausvyros padėtyje muaro gardelės periodas yra $\lambda = 0{,}2$. 2.20(a) paveiksle pademonstruotas vienmatės deformuojamosios muaro gardelės vienas harmoninio judesio periodas. Laike vidurkintas 2.20(a) paveikslo vaizdas parodytas 2.20(b) paveiksle. 2.20(c) paveikslas rodo vienmates laike vidurkintas muaro gardeles, didėjant amplitudei A – kuo didesnė harmoninių svyravimų amplitudė, tuo daugiau muaro interferencinių juostų susiformuoja laike vidurkintame vaizde.

2.5.2. Chaotiniai svyravimai ir nedeformuojamoji muaro gardelė

Chaotiniai procesai yra taikomi skirtingose optikos srityse. Tačiau optinės technikos taip pat taikomos norint pavaizduoti, interpretuoti ir įvertinti chaotinius reiškinius. Tai paremta faktu, kad netiesiškumas yra būdingas beveik kiekvienai realaus pasaulio sistemai. Gerai žinoma, kad netiesinių sistemų atsakas dažnai būna chaotinis, net jeigu jį lemia harmoninis sužadinimas. Todėl kalbant apie dinaminę vizualiąją kriptografiją, labai svarbu sukurti vaizdų slėpimo schemą deformuojamosiose stochastinėse muaro gardelėse, svyruojančiose chaotiškai, ir šią schemą patikrinti virtualiose optinėse aplinkose.

Tarkim, turime nedeformuojamąją muaro gardelę, virpančią chaotiškai. Jos laike vidurkintas vaizdas bus aprašomas formule:

$$F_t(x) = \frac{1}{2} + \frac{1}{2}\lim_{T\to\infty}\frac{1}{T}\int_0^T \left(\cos\left(\frac{2\pi}{\lambda}(x-\theta(t))\right)\right)dt; \quad (2.39)$$

čia $\theta(t)$ yra laiko funkcija, kuria aprašomi chaotiniai svyravimai aplink pusiausvyros padėtį. Jeigu $\theta(t)$ yra Gauso normalusis ergodinis procesas, aproksimuojamas diskrečiųjų, normaliai pasiskirsčiusių skaičių eilute su vidurkiu 0 ir dispersija σ^2, tada laike vidurkintas vaizdas aprašomas šia išraiška [90]:

$$F_t(x) = \tfrac{1}{2} + \tfrac{1}{2}\cos\left(\tfrac{2\pi}{\lambda}x\right)\exp\left(-\tfrac{1}{2}\left(\tfrac{2\pi}{\lambda}A\sigma\right)^2\right). \quad (2.40)$$

Reikėtų atkreipti dėmesį, kad laike vidurkintos interferencinės juostos chaotinių virpesių atveju nesiformuoja [90].

Laike vidurkinto muaro (2.40 lygtis) pilkio lygio standartinis nuokrypis skaičiuojamas pagal tokią formulę:

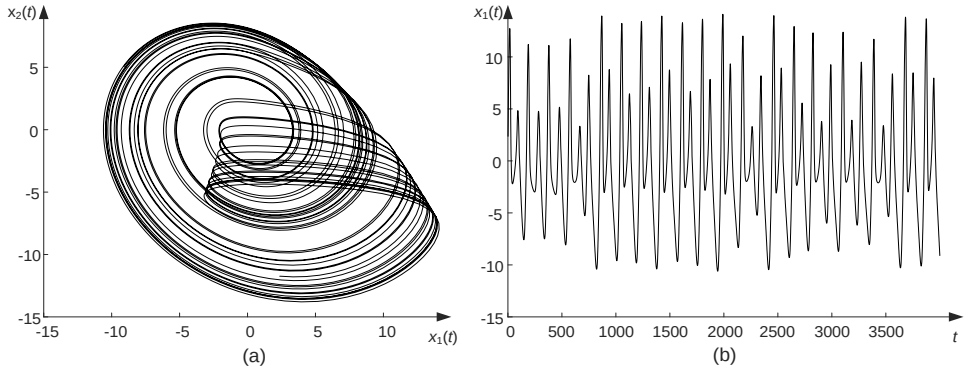
$$S\big(F_t(x)\big) = \tfrac{1}{\lambda}\int_0^{\lambda}\Big(F_t(x) - E\big(F_t(x)\big)\Big)^2 dx = \tfrac{\sqrt{2}}{4}exp\left(-\tfrac{1}{2}\left(\tfrac{2\pi}{\lambda}A\sigma\right)^2\right). \quad (2.41)$$

Visgi yra labai sudėtinga sukonstruoti aiškią fizikinę interpretaciją, kaip tolydžiosios chaotinės funkcijos galėtų būti pakeistos normaliai pasiskirsčiusių skaičių diskrečiąja skaliarine eilute (tačiau toks pakeitimas yra labai naudingas konstruojant teorinius sąryšius). Todėl toliau atlikdami kompiuterinį modeliavimą laikysime, kad $\theta(t)$ yra chaotinio modelio – Roslerio sistemos sprendinys [91]:

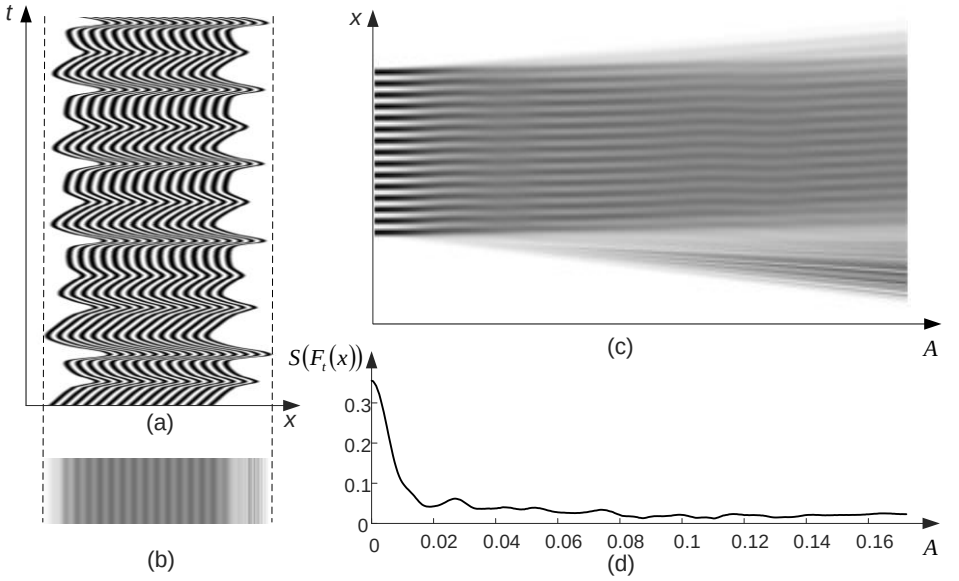
$$\begin{cases} \dfrac{dx_1}{dt} = -x_2 - x_3, \\ \dfrac{dx_2}{dt} = x_1 + ax_2, \\ \dfrac{dx_3}{dt} = bx_1 - cx_3 + x_1x_3; \end{cases} \quad (2.42)$$

čia x_1, x_2, x_3 yra laiko *t* funkcijos, *a*, *b*, *c* – modelio parametrai. Roslerio sistemos elgesys gali būti stacionarus, periodiškas, kvaziperiodiškas ir chaotinis; tai priklauso nuo parametrų reikšmių. 2.21 paveiksle pateiktas Roslerio sistemos chaotinis atraktorius, kai parametrų reikšmės yra šios: $a = 0{,}3$, $b = 0{,}2$, $c = 5{,}7$.

Tarkime, kad analizuojamas vienmatis nedeformuojamasis kūnas svyruoja apie pusiausvyros padėtį pagal laiko funkciją $Ax_1(t)$ ((2.42) lygtis). Čia A yra konstanta. 2.22 paveiksle parodyti vienmatės muaro gardelės chaotiniai svyravimai, kai $A = 0{,}09$. Paveikslo 2.22(a) laike vidurkintas vaizdas pateiktas 2.22(b) paveiksle. Vienmačiai laike vidurkinti vaizdai, didėjant A reikšmei, parodyti 2.22(c) paveiksle.



2.21 pav. Roslerio sistemos sprendinys nusistovėjusioje būsenoje, kai $a = 0{,}3$, $b = 0{,}2$, $c = 5{,}7$; (a) chaotinis atraktorius fazinėje plokštumoje $x_1 - x_2$; (b) $x_1(t)$



2.22 pav. Nedeformuotos vienmatės muaro gardelės chaotiniai svyravimai, kai $\lambda = 0{,}2$: (a) chaotiniai svyravimai pagal laiko funkciją $Ax_1(t)$ ($A = 0{,}09$); brūkšniuota linija rodo didžiausius poslinkius nuo pusiausvyros padėties; (b) laike vidurkintas (a) dalies vaizdas; (c) vienmačiai laike vidurkinti vaizdai, didėjant A reikšmėms; (d) laike vidurkinto vaizdo pilkio pustonių standartinis nuokrypis

2.5.3. Chaotiškai svyruojančios deformuojamosios muaro gardelės optiniai efektai

Šiame skyrelyje išvesime teorinius sąryšius, apibrėžiančius laike vidurkintų interferencinių juostų formavimąsi, kai deformuojamosios gardelės svyruoja chaotiškai.

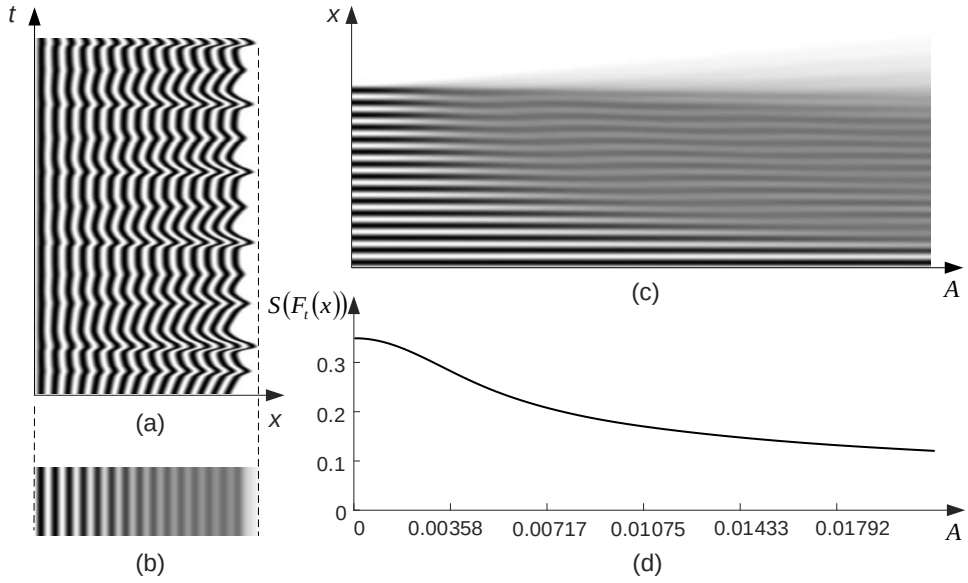
2.5.3.1. Tiesinė funkcija $a(x)$

Nagrinėkime vienmatę deformuojamąją muaro gardelę su pastoviu periodu pusiausvyros padėtyje, $\lambda = 0{,}2$. Tarkime, kad muaro gardelės kairioji pusė yra įtvirtinta,

o dešinioji pusė svyruoja pagal chaotinę laiko funkciją $g(t) = Ax_1(t)$. Be to, padarykime prielaidą, kad svyravimų funkcija yra tiesinė $a(x) = x$. Tada

$$F(x,t) = \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda} \cdot \frac{x}{1 + Ax_1(t)}\right); \tag{2.43}$$

čia parametras A kinta nuo 0 iki 0,02 (2.23 paveikslas). Gauti laike vidurkinti vaizdai yra pateikti 2.23(c) paveiksle. Svarbu pažymėti, kad vaizdo standartinis nuokrypis 2.23(d) paveiksle yra didesnis nei 2.22(d) paveiksle. Tai gali būti paaiškinta faktu, kad kairioji deformuojamosios gardelės pusė yra įtvirtinta ir nejuda.



2.23 pav. Vienmatės deformuojamosios muaro gardelės laike vidurkintas vaizdas, kai $a(x) = x$ ir $g(t) = Ax_1(t)$: (a) vienmatės muaro gardelės judėjimas, kai $A = 0{,}005$; (b) laike vidurkintas (a) dalies vaizdas; (c) vienmatė laike vidurkinta muaro gardelė, esant skirtingoms A reikšmėms; (d) vienmačių laike vidurkintų vaizdų standartinis nuokrypis

2.5.3.2. Netiesinė funkcija $a(x)$

Šiame skyrelyje analizuojamas atvejis, kai funkcija, kuria aprašomi deformuojamojo vienmačio kūno svyravimai, yra netiesinė. (2.37) formule aprašytas kosinuso funkcijos argumentas gali būti pertvarkytas taip:

$$\begin{aligned} \frac{x - (a_0 - \dot{a}_0 x_0)g(t)}{1 + \dot{a}_0 g(t)} &= \big(x - (a_0 - \dot{a}_0 x_0)g(t)\big) \cdot \frac{1}{1 + \dot{a}_0 g(t)} = \\ &= \big(x - (a_0 - \dot{a}_0 x_0)g(t)\big)\big(1 - \dot{a}_0 g(t)\big) + O(\dot{a}_0^2). \end{aligned} \tag{2.44}$$

Pažymėkime, kad $a_0 + \dot{a}_0(x - x_0) = \bar{a}(x)$. Tada deformuojamąją muaro gardelę galima aprašyti taip:

$$F(x,t) \approx \frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}\left(x-(a_0-\dot{a}_0x_0)g(t)-\dot{a}_0xg(t)+(a_0-\dot{a}_0x_0)\dot{a}_0g^2(t)\right)\right)=$$

$$=\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}\left(\left(x+(a_0-\dot{a}_0x_0)\dot{a}_0g^2(t)\right)-(a_0+\dot{a}_0(x-x_0))g(t)\right)\right)= \quad (2.45)$$

$$=\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}\left(x+(a_0-\dot{a}_0x_0)\dot{a}_0g^2(t)\right)\right)\cos\left(\frac{2\pi}{\lambda}\bar{a}(x)g(t)\right)+$$

$$+\frac{1}{2}\sin\left(\frac{2\pi}{\lambda}\cdot\left(x+(a_0-\dot{a}_0x_0)\dot{a}_0g^2(t)\right)\right)\sin\left(\frac{2\pi}{\lambda}\cdot\bar{a}(x)g(t)\right).$$

Vidurkindami (2.45) formulę laike gauname:

$$F_t(x)=\lim_{T\to\infty}\frac{1}{T}\int_0^T F(x,t)dt=\frac{1}{2}+$$

$$+\frac{1}{2}\lim_{T\to\infty}\frac{1}{T}\int_0^T\cos\left(\frac{2\pi}{\lambda}\cdot\left(x+(a_0-\dot{a}_0x_0)\dot{a}_0g^2(t)\right)\right)\cos\left(\frac{2\pi}{\lambda}\cdot\bar{a}(x)g(t)\right)dt+ \quad (2.46)$$

$$+\frac{1}{2}\lim_{T\to\infty}\frac{1}{T}\int_0^T\sin\left(\frac{2\pi}{\lambda}\cdot\left(x+(a_0-\dot{a}_0x_0)\dot{a}_0g^2(t)\right)\right)\sin\left(\frac{2\pi}{\lambda}\cdot\bar{a}(x)g(t)\right)dt.$$

Jeigu padarysime prielaidą, kad laiko funkcija $g(t)$ yra Gauso normalusis ergodinis procesas, tai jį galima aproksimuoti diskrečiųjų, normaliai pasiskirsčiusių skaičių eilute su vidurkiu 0 ir dispersija σ^2:

$$g_i \sim N(0,\sigma),\ i=1,2,\dots,k. \quad (2.47)$$

Tada remiantis [90] straipsniu, galima teigti, kad aprašytos aproksimacijos yra teisingos:

$$\lim_{T\to\infty}\frac{1}{T}\int_0^T\cos\left(\frac{2\pi}{\lambda}\cdot\bar{a}(x)g(t)\right)dt=\exp\left(-\frac{1}{2}\left(\frac{2\pi}{\lambda}\cdot\bar{a}(x)\sigma\right)^2\right);$$
$$\lim_{T\to\infty}\frac{1}{T}\int_0^T\sin\left(\frac{2\pi}{\lambda}\cdot\bar{a}(x)g(t)\right)dt=0. \quad (2.48)$$

Tačiau, jeigu g_i yra normaliai pasiskirstę dydžiai su vidurkiu 0 ir dispersija σ^2, tada žinoma, kad g_i^2 yra pasiskirstę pagal Chi–kvadratų skirstinį ($g_i^2 \sim \chi^2(1)$) ir $Eg_i^2=\sigma^2$ [92]. Tada (2.46) lygtis gali būti pertvarkyta, pakeičiant σ^2 į $g^2(t)$ ir laikant teisingomis (2.48) lygties aproksimacijas:

$$F_t(x)\approx\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}(x+(a_0-\dot{a}_0x_0)\dot{a}_0\sigma^2)\right)\exp\left(-\frac{1}{2}\left(\frac{2\pi}{\lambda}\cdot\bar{a}(x)\sigma\right)^2\right). \quad (2.49)$$

(2.49) lygtyje gautas sąryšis visiškai atitinka (2.40) lygtį. Stochastinių svyravimų atveju laike vidurkintos interferencinės juostos nesiformuoja. Didesnė dispersija ar/ir didesnės svyravimų reikšmės duoda didesnio išblukimo efektą. Tačiau šis sąryšis yra tik apytikslis, išvestas esant prielaidoms, kad $g^2(t)$ gali būti pakeistas į σ^2.

2.5.3.3. Sąryšio (2.49) skaitmeninis validavimas

Norint validuoti (2.49) lygtyje aprašytą apytikslį sąryšį, yra atliekami skaitiniai eksperimentai. Imkime deformuojamąsias vienmates muaro gardeles su kairiosios ir dešiniosios pusės įtvirtinimu stebėjimų lange $0 \leq x \leq L$. Tarkime, kad formos funkcija $a(x)$ vaizduojama deformuojamo vienmačio kūno pirmoji forma:

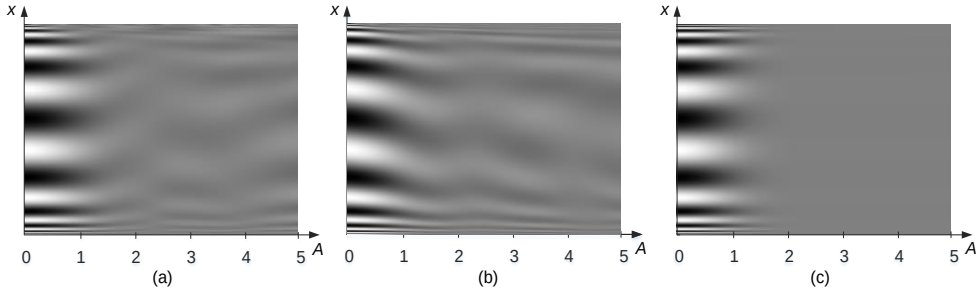
$$a(x) = sin\left(\frac{\pi x}{L}\right). \tag{2.50}$$

Aišku, kad deformuojamoji muaro gardelė su pastoviu periodu negali suformuoti tolygaus laike vidurkinto vaizdo šiame stebėjimo lange, nes skirtingi gardelės taškai svyruoja skirtinga amplitude (žr. paveikslus 2.20 ir 2.23). Todėl tinkamo muaro gardelės periodo pusiausvyros padėtyje parinkimas yra pirmas žingsnis validuojant (2.49) lygtį. Kintantis muaro gardelės periodas turi būti proporcingas formos funkcijai [89]. Tokiu būdu pasirenkame, kad

$$\lambda(x) = 3sin\left(\frac{\pi x}{L}\right). \tag{2.51}$$

Deformuojamoji muaro gardelė pusiausvyros padėtyje yra pavaizduota 2.24 paveikslo (a), (b) ir (c) dalyse, kai $A = 0$. 2.24(a) paveiksle matoma laike vidurkinta vienmatė deformuojamoji muaro gardelė, kai laiko funkcija $g(t)$ yra aproksimuojama pagal Gauso normalųjį ergodinį procesą (lygtis 2.46) su standartiniu nuokrypiu, lygiu 0,7. Diskrečiųjų $g(t)$ reikšmių skaičius, naudojamas vidurkinimui, parenkamas k = 5000.

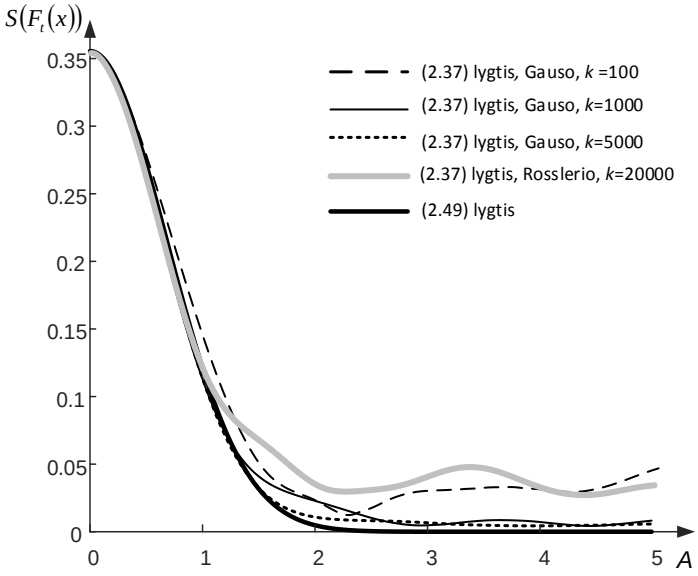
Analogiškai, 2.24(b) paveiksle matyti laike vidurkintas vaizdas, kai laiko funkcija $g(t) = Ax_1(t)$. Diskrečiųjų $g(t)$ reikšmių skaičius, naudojamas vidurkinant laike, yra parenkamas k = 20 000. Galiausiai 2.24 (c) paveiksle matomas laike vidurkintas vaizdas, aprašytas (2.49) lygtimi, kai parametras σ yra parinktas 0,7.



2.24 pav. Vienmatės deformuojamosios muaro gardelės, svyruojančios pagal pirmąją formos funkciją, laike vidurkinti vaizdai: (a) $g(t)$ yra aproksimuojama pagal $g_i \sim A \cdot N(0{,}0.7)$; (b) $g(t) = Ax_1(t)$, čia $x_1(t)$ yra chaotinis Roslerio procesas; (c) (2.49) lygties analizinis rezultatas, kai $\sigma = 0{,}7$

2.24(a) paveikslo laike vidurkinto vaizdo standartinio nuokrypio kitimas yra parodytas 2.25 paveiksle (tanki brūkšniuota linija pavaizduoja atvejį, kai $k = 5000$). Norėdami pademonstruoti vidurkinimo laike optinį efektą pateikiame standartinius nuokrypius, kai $k = 100$ ir $k = 1000$ (2.25 paveikslas). Analogiškai, 2.25 paveiksle yra pavaizduoti 2.24(b) ir 2.24(c) paveikslų standartiniai nuokrypiai. Aiškiai matyti, kad chaotinio proceso aproksimavimas Gauso ergodiniu procesu artėja prie teorinio rezultato,

kai k didėja. Be to, vidurkinimas laike pagal Roslerio chaotinį procesą gerai atitinka (2.49) lygtį. Skirtumai tarp standartinių nuokrypių kitimo kreivių prie didelių parametro A reikšmių gali būti paaiškinti ribotu ekspozicijos laiku, naudojamu sugeneruoti laike vidurkintiems vaizdams.



2.25 pav. Vienmatės muaro gardelės laike vidurkintų vaizdų standartiniai nuokrypiai

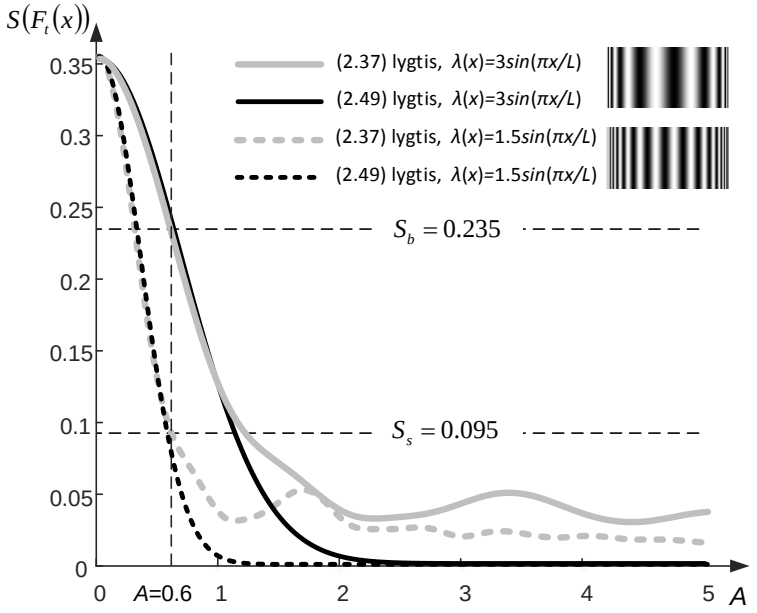
2.5.4. Dinaminė vizualioji kriptografija, pagrįsta chaotiškai svyruojančia deformuojamąja muaro gardele

Vaizdų slėpimo technikos stochastinėse nedeformuojamosiose muaro gardelėse yra pagrįstos juodai balto slapto vaizdo naudojimu [72]. Vienoks muaro gardelės periodas naudojamas fonui, kiek kitoks – slaptai informacijai. Chaotinis fazės sumaišymas taikomas norint paslėpti slaptą informaciją užkoduotame paveiksle. Slapta informacija išryškėja dėl laike vidurkintų interferencinių juostų, kai užkoduotas paveikslas virpinamas pagal tam tikrą iš anksto nustatytą dėsnį.

Vis dėlto, kaip matyti iš anksčiau aprašyto pavyzdžio, laike vidurkintos muaro interferencinės juostos nesiformuoja, kai deformuojamoji muaro gardelė yra virpinama pagal chaotinį dėsnį. Bet kokiu atveju bus naudojamas dichotominis slaptas vaizdas, kai slaptai informacijai ir fonui taikomi skirtingi periodai.

2.5.4.1. Vaizdų slėpimas chaotiškai svyruojančioje deformuojamojoje vienmatėje muaro gardelėje

Taigi grįžkime prie (2.49) lygties validavimo skaitmeninio pavyzdžio. Darome prielaidą, kad vienos deformuojamosios muaro gardelės periodas yra aprašomas $\lambda(x) = 3sin\left(\frac{\pi x}{L}\right)$, o kitos muaro gardelės – $\lambda(x) = 1{,}5sin\left(\frac{\pi x}{L}\right)$. Šių laike vidurkintų muaro gardelių, virpančių pagal chaotinį dėsnį, standartai parodyti 2.26 paveiksle.



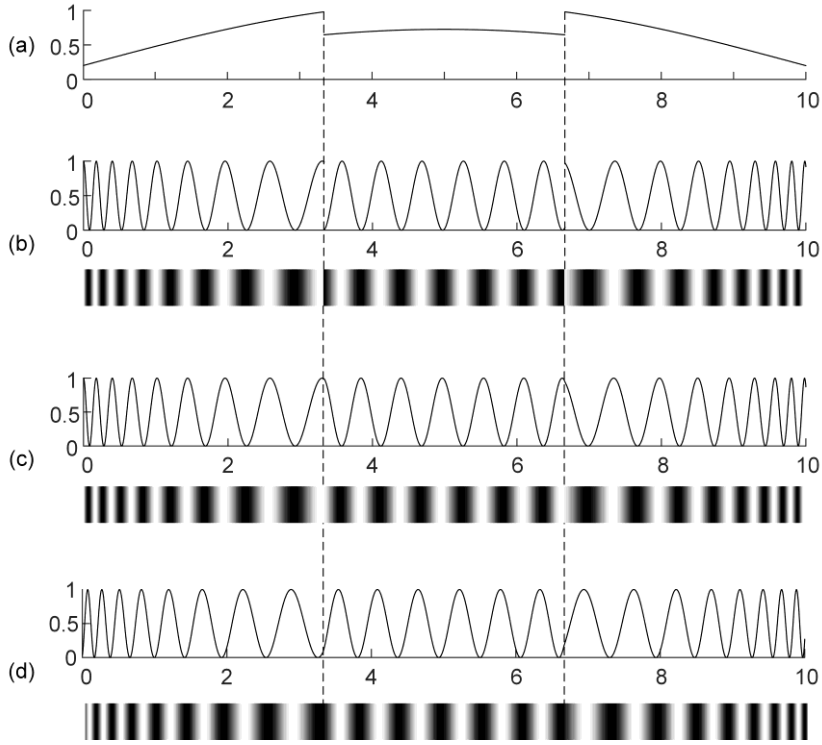
2.26 pav. Vienmatės laike vidurkintos muaro gardelės vaizdų standartiniai nuokrypiai, esant skirtingiems periodams

Mūsų tikslas – parinkti tokią parametro A reikšmę, kad skirtumas tarp abiejų gardelių standartų būtų didžiausias (2.26 paveiksle, kai $A = 0{,}6$). Slapta informacija išryškėja laike vidurkintame vaizde, kai užkoduotas paveikslas yra virpinamas pagal laiko funkciją, aprašančią chaotinį Roslerio atraktorių. Laike vidurkinto vaizdo pilkumo netolygumas skiriasi fono ir slapto vaizdo srityse. Akivaizdu, kad skirtumas tarp slaptos informacijos ir fono laike vidurkintame vaizde turi būti pakankamai didelis, norint užtikrinti reikiamą atkoduoto slapto vaizdo kontrastą.

Jeigu kintantis muaro gardelės periodas slaptos informacijos srityje yra $\lambda_s(x) = 1{,}5sin\left(\frac{\pi x}{L}\right)$, tada standartinis nuokrypis yra $S_s = 0{,}095$, kai $A = 0{,}6$ (laike vidurkinto užkoduoto vaizdo sritys, apimančios slaptą informaciją, yra beveik tolygiai užpilkėjusios). Tačiau, jei fono gardelės periodas yra $\lambda_b(x) = 3sin\left(\frac{\pi x}{L}\right)$, tai laike vidurkintas vaizdas fono srityje yra nelygiai pilkas ($S_b = 0{,}235$). Skirtumas tarp standartinių nuokrypių fone ir slaptos informacijos srityje yra $|S_s - S_b| = 0{,}14$, o tai leidžia užtikrinti pakankamą skirtumą tarp slaptos informacijos ir fono laike vidurkintame vaizde (2.26 paveikslas). Tačiau, jei parametras A būtų didesnis už 1,5, skirtumas tarp standartinių nuokrypių $|S_s - S_b|$ būtų per mažas slaptos informacijos vizualiam interpretavimui (2.26 paveikslas).

2.5.4.2. Informacijos slėpimo schemos aprašymas

Vaizdų slėpimo schemos fizikinis realizavimas susideda iš dviejų žingsnių. Pirmas žingsnis yra fazių reguliarizavimas ties slaptos informacijos ir fono riba. Antrasis žingsnis – chaotinis atsitiktinės fazės parinkimas. Šie abu žingsniai parodyti 2.27 paveiksle.



2.27 pav. Scheminė diagrama, kurioje vaizduojama pasiūlyta vaizdo slėpimo schema. Formos funkcija parodyta (a) dalyje; vienmatė muaro gardelė be ir su fazės reguliarizavimo algoritmo – (b) ir (c) dalyse; vienmatė muaro gardelė su atsitiktinai parinkta pradine faze – (d) dalyje

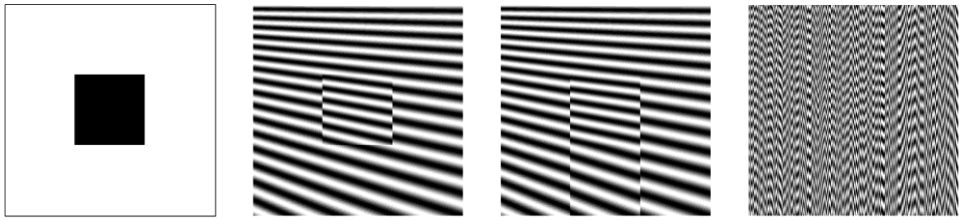
Tarkime, kad vienmatė deformuojamoji muaro gardelė yra apibrėžta netolydžia formos funkcija (2.27(a) paveikslas). Stebėjimų langas $0 \leq x \leq 10$ padalytas į tris dalis. Neprarasdami bendrumo tarkime, kad slapta informacija yra vidurinėje dalyje, o kitos dvi dalys yra fonas.

Anksčiau aprašytiems sąryšiams būtina, kad muaro gardelės kintamas periodas būtų proporcingas formos funkcijai. Tačiau tiesiogiai užkodavę netolydžią formos funkciją, gauname muaro gardelės fazės netolydumą (2.27(b) paveikslas). Toks netolydumas gali sukompromituoti vaizdo slėpimo schemą, nes riba tarp slaptos informacijos ir fono gali būti matoma plika akimi. Todėl būtina pritaikyti fazių reguliarizavimo algoritmą ties šia riba. Toks žingsnis pavaizduotas 2.27(c) paveiksle.

Būtina pažymėti, kad deformuojamosios muaro gardelės fazė kairėje vienmačio vaizdo dalyje yra nepakitusi lyginant su 2.27(b) paveikslu. Tačiau vidurinėje dalyje esanti gardelės pradinė fazė yra priderinta taip, kad gauta muaro gardelė tampa tolydi (2.27(c) paveikslas). Svarbu pabrėžti, kad fazės priderinimas nekeičia muaro gardelės periodo. Tokia pati fazės reguliarizavimo procedūra yra atliekama ir kitame krašte (tarp centrinės ir dešiniosios dalies). Pažymėtina, kad fazės priderinimų skaičiui nėra jokių apribojimų.

Kitas pasiūlytos vaizdo slėpimo technikos žingsnis yra pradinių fazių chaotinis sumaišymas. Nagrinėkime du gretimus juodai baltų pikselių stulpelius. Šiuose stulpeliuose esantys pikseliai bus identiški, jei formos funkcija lėtai keisis. Toks optinis

efektas ir vaizdo slėpimo schema bendruoju atveju yra parodyti 2.28 paveiksle. Paprastumo dėlei tarkime, kad slapta informacija yra juodas kvadratas baltame fone (paveikslas 2.28(a)). Taip pat tarkime, kad dvimatė formos funkcija nėra pastovi stebėjimų lange. Slaptą informaciją įterpus į foną tiesiogiai, plika akimi bus aiškiai matomos skirtingos deformuojamosios muaro gardelės ir riba tarp jų (2.28(b) paveikslas). Fazių reguliarizavimo algoritmas, pritaikytas horizontalioje riboje tarp slaptos informacijos ir fono, eliminuoja netolydumus kiekviename pikselių stulpelyje (paveikslas 2.28(c)). Galiausiai pradinės fazės chaotinis sumaišymas kiekvienam pikselių stulpeliui duoda plika akimi neinterpretuojamą užkoduotą vaizdą (paveikslas 2.28(d)).



2.28 pav. Scheminė diagrama, kurioje pavaizduota informacijos slėpimo schema; periodas $\lambda(x)$ stebėjimo lange kinta intervale [0,2; 0,4]. Tiesioginis slaptos informacijos ((a) dalis) įterpimas į foną parodytas (b) paveiksle. Fazių reguliarizacija pavaizduota (c) dalyje; stochastinis pradinių fazių sumaišymas pavaizduotas (d) dalyje

2.5.4.3. Slaptos informacijos talpa vaizdų slėpimo schemoje

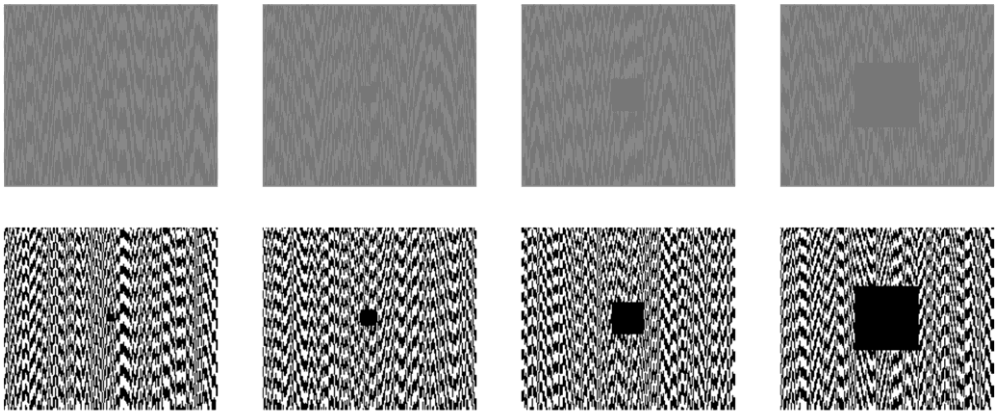
Ankstesniuose skyriuose pademonstruota, kad kintamas periodas $\lambda(x)$ turi būti proporcingas formos funkcijai $a(x)$. Proporcingumas apibrėžiamas, remiantis vidurkinimo laike operatoriaus matematinėmis savybėmis ir chaotinių svyravimų fizikinėmis savybėmis. Tačiau konkretus kintamo periodo parinkimas tiesiogiai priklauso nuo vaizdo slėpimo efekto ir slaptos informacijos talpos vaizdo slėpimo schemoje.

Imkime tokį patį pavyzdį, kuris buvo naudotas 2.28 paveiksle pateiktoje vaizdo slėpimo schemoje. Tik šiuo atveju imsime skirtingus kvadratinio elemento dydžius (2.29 paveikslas). Muaro gardelės periodas yra kintamas stebėjimų lange. Taigi bus naudojamas periodo reikšmių vidurkis ir konstruojami keturi skaitiniai eksperimentai. 2.29(a) paveiksle pavaizduotas kvadratinis elementas, įdėtas į užkoduoto vaizdo vidurį, šio elemento kraštinės ilgis lygus $0{,}25\bar{\lambda}$ ($\bar{\lambda}$ yra periodo vidurkis stebėjimų lange). Viršuje esantis vaizdas – laike vidurkintas užkoduotas vaizdas, kai svyravimai yra chaotiniai pagal iš anksto nustatytą formos funkciją. Apačioje esantis vaizdas – paryškintas laike vidurkintas užkoduotas vaizdas.

Analogiškai skaitinis eksperimentas su kvadratiniu elementu, kurio kraštinės ilgis $0{,}5\bar{\lambda}$, yra pavaizduotas 2.29(b) paveiksle, $\bar{\lambda}$ – 2.29(c) paveiksle ir $2\bar{\lambda}$ – 2.29(d) paveiksle. Vadinasi, galime daryti išvadą, kad mažiausias interpretuojamas elemento dydis laike vidurkintame vaizde turi būti ne mažesnis nei pusė vidutinio muaro gardelės periodo nagrinėjamoje srityje.

Šis apribojimas iš anksto nulemia informacijos talpą vaizdo slėpimo schemoje. Būtina pažymėti, kad užkoduoto vaizdo kintamas periodas $\lambda(x)$ turi būti atidžiai parinktas pagal chaotinių virpesių fizikinius parametrus (formos funkcija nulemia

amplitudžių lauką, pokytis nulemia chaotinio proceso atsitiktinumą). Kai kintamas periodas $\lambda(x)$ yra fiksuotas, galima įvertinti užkoduoto vaizdo informacijos talpą ir sukonstruoti patį slaptą vaizdą.



2.29 pav. Vaizdo slėpimo schemos informacijos talpa. Paveikslai viršutinėje eilutėje vaizduoja deformuojamos muaro gardelės, svyruojančios chaotiškai pagal tam tikrą formos funkciją, naudotą 2.28 paveiksle, laike vidurkintus vaizdus; paveikslai apatinėje eilutėje – atitinkamus paryškintus vaizdus. Slapto kvadratinio elemento kraštinės dydis yra $0{,}25\bar{\lambda}$ ((a) dalis); $0{,}5\bar{\lambda}$ ((b) dalis); $\bar{\lambda}$ ((c) dalis) ir $2\bar{\lambda}$ ((d) dalis), čia $\bar{\lambda}$ yra periodo vidurkis stebėjimo lange

2.5.4.4. Vaizdo slėpimo schemos saugumas

Kaip minėta anksčiau, pasiūlyta vaizdo slėpimo schema priklauso vizualiosios kriptografijos technikų klasei – specialūs algoritmai taikomi vaizdui užkoduoti, tačiau dekodavimui nereikia jokių skaičiavimo įrenginių, ir jis yra visiškai vizualus. Klasikinės vizualiosios kriptografijos schemos pagrįstos slapto vaizdo skaidymu į kelias skaidres. Kiekviena skaidrė yra kriptografiškai saugi – slapta informacija išryškėja tik atidžiai sudėjus skaidres vieną ant kitos. Šiame skyriuje aptartu atveju slaptas vaizdas nėra dalijamas. Naudojamas tik vienas užkoduotas vaizdas, slapta informacija išryškėja tik laike vidurkintame vaizde.

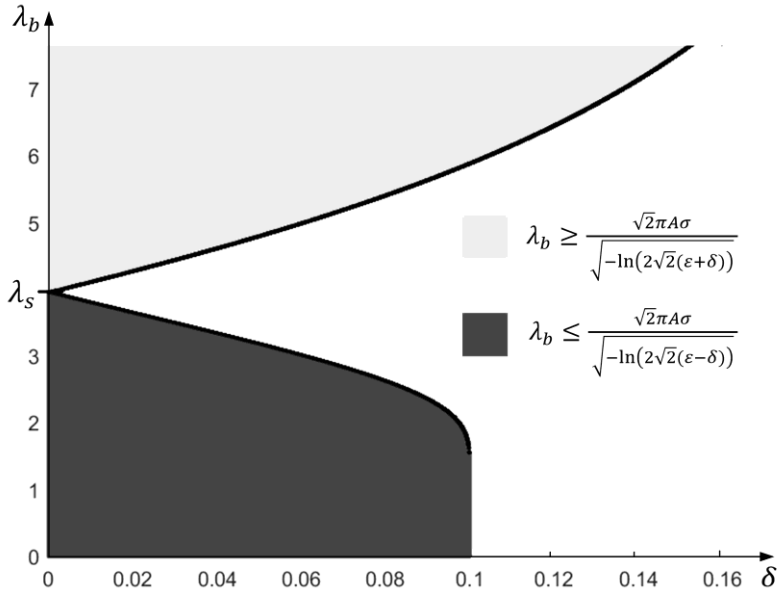
Natūralu, kad kiekviena vaizdo kodavimo schema turi savo privalumų ir trūkumų. Kaip minėta, klasikinė vizualiosios kriptografijos schema yra kriptografiškai saugi, tačiau turėtų būti pritaikyti specialūs algoritmai, sumažinantys sukčiavimo tikimybę [93].

Šiame skyriuje pasiūlyta vaizdo slėpimo schema nėra kriptografiškai griežtai saugi – slaptas vaizdas išryškėja iš vieno užkoduoto vaizdo vidurkinant laike. Be to, formos funkcijos su skirtingais proporcingumo koeficientais yra naudojamos fonui ir slaptos informacijos sričiai.

Panagrinėkime supaprastintą situaciją, kai formos funkcija yra pastovi visame stebėjimų lange. Šiuo atveju turėsime deformuojamąją muaro gardelę su pastoviais periodais pusiausvyros padėtyje. Tarkime, kad slaptos informacijos srityje periodas yra λ_s, o fono periodas – λ_b.

Akivaizdu, kad periodai λ_s ir λ_b negali pastebimai skirtis, nes užkoduotas vaizdas matytųsi plika akimi statiniame užkoduotame vaizde. Antra vertus, skirtumas tarp λ_s ir

λ_b turi užtikrinti pakankamą kontrastą tarp slaptos informacijos ir fono laike vidurkintame vaizde. Būtina pažymėti, kad deformuojamo užkoduoto vaizdo svyravimai yra chaotiniai. Todėl standartinis nuokrypis laike vidurkintame vaizde slaptos informacijos zonoje yra $\sigma_s = \frac{\sqrt{2}}{4} exp\left(-\frac{1}{2}\left(\frac{2\pi}{\lambda_s} A\sigma\right)^2\right)$ ir fone $\sigma_b = \frac{\sqrt{2}}{4} exp\left(-\frac{1}{2}\left(\frac{2\pi}{\lambda_b} A\sigma\right)^2\right)$ (2.41 lygtis).



2.30 pav. Grafinė 2.52 ir 2.53 nelygybių interpretacija, kai $\varepsilon = 0{,}05$, $A = 1$, $\sigma = 1$ (stora vientisa linija reiškia optimalią Pareto ribą)

Slapta informacija išryškėja, kai gaunamas tinkamas kontrastas tarp σ_s ir σ_b laike vidurkintame vaizde. Tarkime, kad laike vidurkintos interferencinės juostos beveik visiškai susiformuoja slaptos informacijos srityje ($\sigma_s = \varepsilon$; čia ε yra mažas teigiamasis skaičius). Tada fono standartinis nuokrypis turi būti kiek galima didesnis: $|\sigma_b - \sigma_s| = |\sigma_b - \varepsilon| \geq \delta$. Būtina pažymėti, kad $\lambda_s = \frac{\sqrt{2}\pi A\sigma}{\sqrt{-\ln(2\sqrt{2}\varepsilon)}}$ (kadangi $\sigma_s = \varepsilon$). Todėl turi būti teisinga tokia nelygybė, kai $\sigma_b > \sigma_s$:

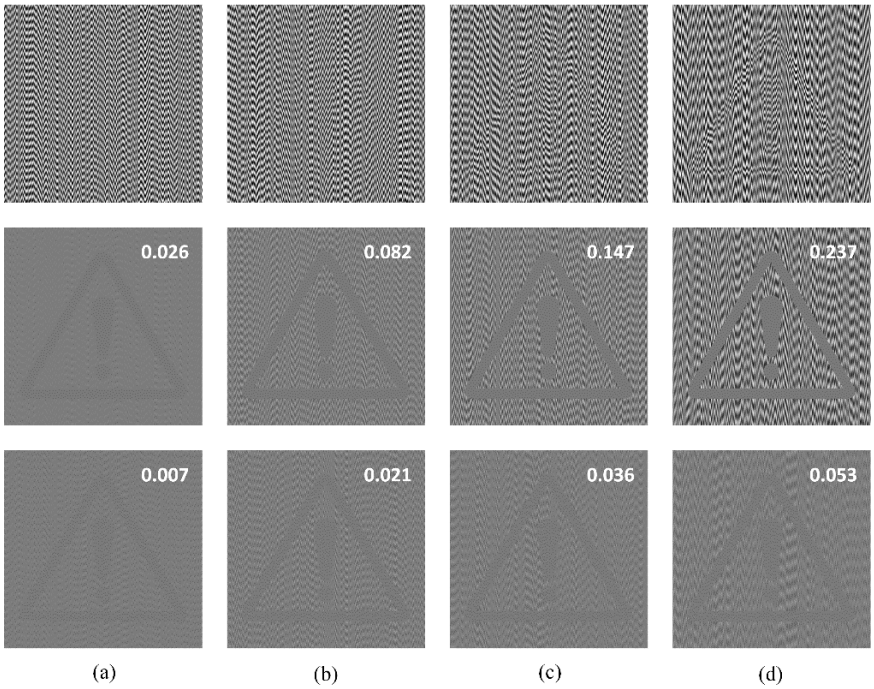
$$\lambda_b \geq \frac{\sqrt{2}\pi A\sigma}{\sqrt{-\ln\left(2\sqrt{2}(\varepsilon+\delta)\right)}}. \tag{2.52}$$

Analogiškai, kai $\sigma_b < \sigma_s$:

$$\lambda_b \leq \frac{\sqrt{2}\pi A\sigma}{\sqrt{-\ln\left(2\sqrt{2}(\varepsilon-\delta)\right)}}. \tag{2.53}$$

Šių nelygybių grafinė interpretacija pateikta 2.30 paveiksle. Tai yra standartinė optimizavimo su apribojimais problema – rasti didžiausią δ (didžiausias skirtumas tarp

laike vidurkintų vaizdų) reikšmę, su kuria būtų mažiausias skirtumas tarp λ_s ir λ_b (mažiausias periodų skirtumas užkoduotuose vaizduose). Pareto optimali riba pavaizduota 2.30 paveiksle stora vientisa linija. Tokiu būdu, jei ε reikšmę nustatysime 0,05, λ_s bus 3,18 mm, skirtumas $|\sigma_b - \sigma_s|$ turi būti ne mažesnis nei 0,1, taigi λ_b turi būti mažesnis nei 4,8 mm (2.30 paveikslas).



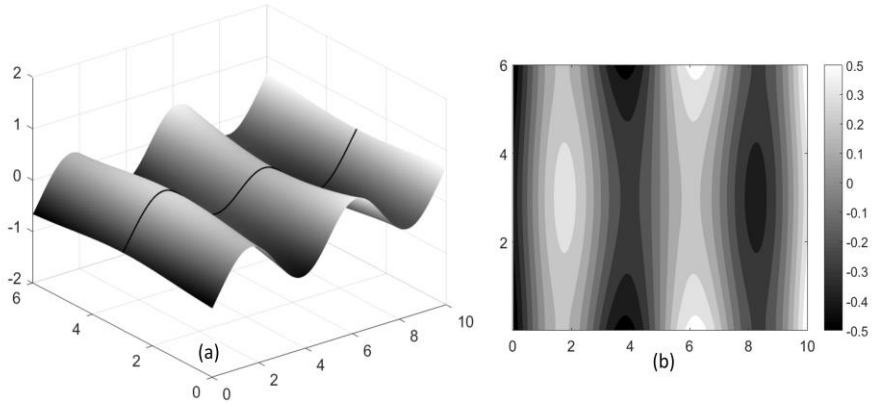
2.31 pav. Slaptos informacijos užkodavimas ir dekodavimas, kai λ_s = 0,33: užkoduoti vaizdai (viršutinė eilutė), dekoduoti vaizdai harmoninių svyravimų atveju (vidurinė eilutė) ir chaotinių svyravimų atveju (apatinė eilutė). Fono periodas λ_b yra skirtingas kiekviename paveikslo stulpelyje (a) λ_b = 0,35; (b) λ_b=0,4; (c) λ_b=0,475; (d) λ_b = 0,66. Kontrasto $|\sigma_s - \sigma_b|$ įverčiai tarp laike vidurkinto slapto vaizdo ir fono sričių yra pateikti kiekviename dekoduoto vaizdo viršutiniame kairiajame kampe [94]

Palyginkime slaptos informacijos dekodavimo rezultatus chaotinių ir harmoninių virpesių atveju, kai yra parenkamos skirtingos muaro gardelių periodų poros. 2.31 paveikslo pirmoje eilutėje pateikti užkoduoti vaizdai, antroje eilutėje – dekoduoti vaizdai harmoninių virpesių atveju, trečioje eilutėje – dekoduoti vaizdai chaotinių virpesių atveju. Muaro gardelės periodas slaptos informacijos zonoje yra parinktas $\lambda_s = 0{,}33$. Muaro gardelės periodas fono zonoje λ_b yra skirtingas kiekviename paveikslo stulpelyje: (a) dalyje $\lambda_b = 0{,}35$; (b) $\lambda_b = 0{,}4$; (c) $\lambda_b = 0{,}475$; (d) $\lambda_b = 0{,}66$. Harmoninių svyravimų amplitudė lygi 0,126 ir Gauso svyravimų standartinis nuokrypis lygus 0,036 visose paveikslo 2.31 dalyse. Kuo mažesnis skirtumas tarp λ_s ir λ_b reikšmių, tuo blogesnis kontrastas matomas laike vidurkintame vaizde (2.31 paveikslo (a) dalis). Teisingas ir priešingas teiginys – kuo didesnis skirtumas tarp λ_s ir λ_b reikšmių, tuo geresnis kontrastas matomas laike vidurkintame vaizde. Deja, didelis skirtumas tarp λ_s

ir λ_b reikšmių sukompromituoja pačią informacijos kodavimo schemą – slaptas vaizdas gali būti matomas plika akimi statiniame užkoduotame vaizde (2.31 paveikslo (d) dalis).

2.5.4.5. Dvimatės muaro gardelės konstravimas ir virtualus optinis eksperimentas

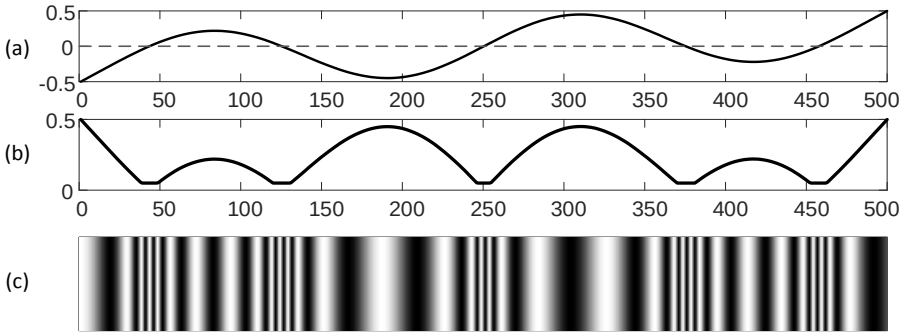
Tarkime, kad yra atliekamas virtualus optinis eksperimentas, kai muaro gardelė suformuojama ant deformuojamos plokštelės, turinčios šviesą atspindintį paviršių. Neprarasdami bendrumo tarkime, kad apšvietimas yra statmenas plokštelės paviršiui pusiausvyros padėtyje. Atsispindintis muaro vaizdas yra iš karto užfiksuojamas. Imkime 17-ąją dvimatę formos funkciją, aprašančią natūralius deformuojamos plokštelės svyravimus (2.32(a) paveikslas).



2.32 pav. Laisvai deformuojamos plokštelės 17-oji tikrinė forma: (a) trimatis vaizdas; (b) lygio linijų žemėlapis

Plokštelės paviršiuje susiformavusi dvimatė muaro gardelė yra formuojama kaip vienmačių lygiagrečių muaro gardelių masyvas. Jeigu visos vienmatės muaro gardelės turėtų tokį patį periodą ir visų vienmačių gardelių pradinė fazė būtų vienoda, tai dvimatis muaro vaizdas būtų sudarytas iš lygiagrečių tamsių ir šviesių juostų, statmenų vienmatės gardelės krypčiai.

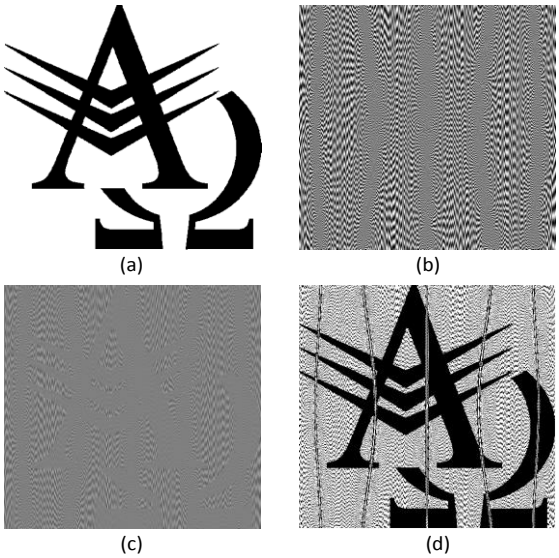
Tačiau, kaip buvo aprašyta 2.5.3.3 skyrelyje, kiekvienos muaro gardelės periodas turi būti kintamas, taip pat turi būti proporcingas formos funkcijai, apibrėžiančiai atitinkamą virpesių pobūdį. Aptarkime muaro gardelės su kintamu periodu konstravimą (2.33 paveikslas). Dvimatės formos funkcijos centrinė linija yra pavaizduota kaip vienmatė funkcija 2.33(a) paveiksle. 2.33(b) paveiksle pateiktos formos funkcijos absoliučiosios reikšmės. Tačiau tiesinis ryšys tarp formos funkcijos modulio ir periodo leidžia numatyti, kad vienmatės muaro gardelės periodas bus lygus nuliui formos funkcijos nuliniuose taškuose. Aišku, kad muaro gardelės su begaliniu periodu fizikinis konstravimas nėra įmanomas. Su tuo tikslu nustatome formos funkcijos absoliučiajai reikšmei minimalią ribą (paveikslas 2.33(b)). Ši riba gali skirtis pagal fizikinius įrankius, naudojamus muaro gardelei generuoti. Vienmatės muaro gardelės optinė vizualizacija pavaizduota 2.33(c) paveiksle. Būtina pažymėti, kad 2.33(c) paveikslo plotis yra dirbtinai padidintas dėl vaizdumo. Tikrasis vienmatės muaro gardelės plotis yra 1 pikselis.



2.33 pav. Scheminė diagrama, kurioje vaizduojamas vienmatės muaro gardelės su kintamu periodu konstravimas: (a) dvimatės formos funkcijos, vaizduojančios 17-ąją tikrinę formą, pjūvis; (b) formos funkcijos absoliučiosios reikšmės pjūvyje; (c) vienmatės muaro gardelės optinė vizualizacija

2.5.4.6. Dinaminė vizualioji kriptografija, pagrįsta chaotiškais svyravimais

Tarkime, kad dviejų spalvų skaitmeninis vaizdas yra parodytas 2.34(a) paveiksle. 2.34(b) paveiksle slaptas vaizdas yra įterptas į stacionarią muaro gardelę.

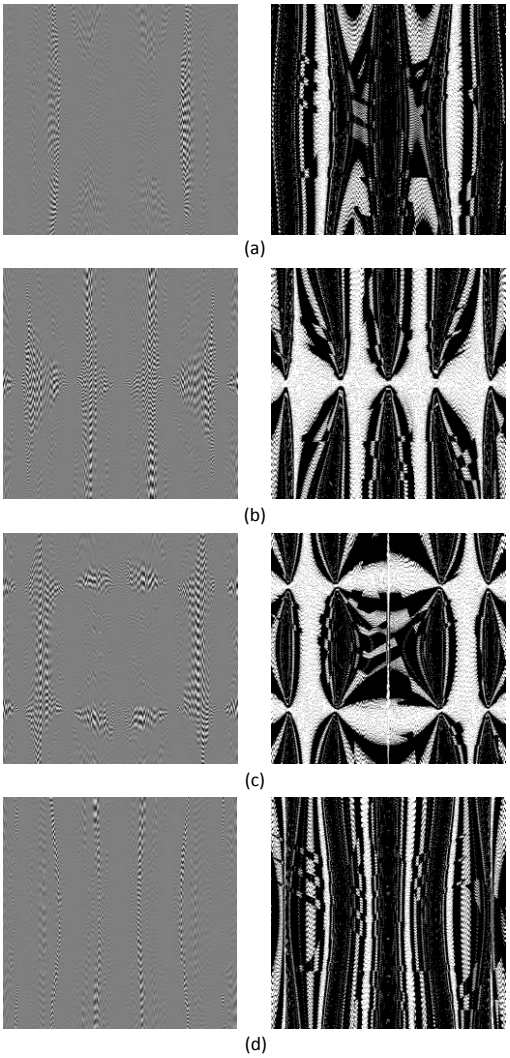


2.34 pav. Slapto vaizdo užkodavimas ir dekodavimas, pagrįstas chaotiniais deformuojamosios gardelės svyravimais: (a) slaptas vaizdas; (b) slaptas vaizdas, užkoduotas su 17-ąja tikrine forma, kintamo gardelės periodo intervalas yra [0,015; 0,350]; (c) vizualiai dekoduotas laike vidurkintas slaptas vaizdas: chaotinių svyravimų amplitudžių laukas kinta pagal 17-ąją tikrinę formą, svyravimų amplitudės intervalas yra [–0,498; 0,740]; (d) paryškintas laike vidurkintas vaizdas

Pažymėtina, kad kintamas periodas $\lambda(x)$ yra parinktas tokiu būdu, kad jis būtų proporcingas absoliučioms 17-osios tikrinės formos reikšmėms, kurios varijuoja intervale nuo 0,015 iki 0,350.Fazių reguliarizacijos algoritmas [72] taikomas slaptam

vaizdui įterpti į stochastinę muaro gardelę – plika akimi slapto vaizdo įžiūrėti neįmanoma statiniame užkoduotame vaizde (paveikslas 2.34(b)).

2.34(c) paveiksle matyti 2.34(b) paveikslo laike vidurkintas vaizdas, kai plokštelė svyruoja pagal laiko funkciją $x_1(t)$ (Roslerio sistemos chaotinius svyravimus). Formos funkcija kinta pagal plokštelės 17-ąją tikrinę formą, svyravimų amplitudė yra intervale nuo –0,498 iki 0,740. Kitais žodžiais tariant, visa chaotinių svyravimų energija yra koncentruota į plokštelės 17-ąją tikrinę formą. Pritaikius kontrasto paryškinimo algoritmą, 2.34(d) paveiksle galima lengvai įžvelgti laike vidurkintą dekoduotą slaptą informaciją.

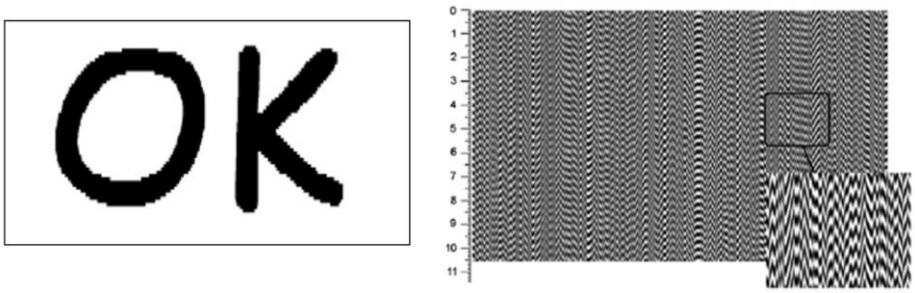


2.35 pav. Laike vidurkinti (kairysis stulpelis) ir paryškinti laike vidurkinti (dešinysis stulpelis) vaizdai. Chaotiniai svyravimai pagal neteisingą tikrinę formą neatskleidžia slaptos informacijos laike vidurkintame vaizde: (a) svyravimai pagal 7-ąją tikrinę formą; (b) 15-ąją tikrinę formą; (c) 18-ąją tikrinę formą; (d) 20-ąją tikrinę formą

Taigi plokštelės forma yra naudojama kaip raktas slaptam vaizdui dekoduoti. Optinis laiko vidurkinimo metodas neatskleidžia slapto paveikslo, jei chaotinių virpesių formos funkcija yra kita plokštelės forma nei ta, su kuria buvo užkoduota. Šis faktas akivaizdžiai matosi 2.35 paveiksle, kai chaotinių virpesių formos funkcijos yra 7-oji, 15-oji, 18-oji ir 20-oji tikrinės formos.

2.5.5. Chaotinės dinaminės vizualiosios kriptografijos eksperimentiniai tyrimai[7]

Eksperimentiniai tyrimai buvo atlikti, norint patikrinti teorinius sąryšius ir patvirtinti kompiuterinio modeliavimo metu gautus rezultatus. Pirmiausia 2.36 paveikslo kairėje esantis vaizdas užkoduojamas muaro gardelėje, taikant fazių reguliarizacijos ir atsitiktinės pradinės fazės algoritmus, aprašytus 1.7.3 skyriuje. Muaro gardelės periodai yra parenkami tokie: $\lambda_s = 2{,}2$ mm ir $\lambda_b = 2{,}8$ mm. Tada užkoduotas vaizdas (2.36 paveikslo dešinėje) yra išspausdinamas su paprastu lazeriniu spausdintuvu.



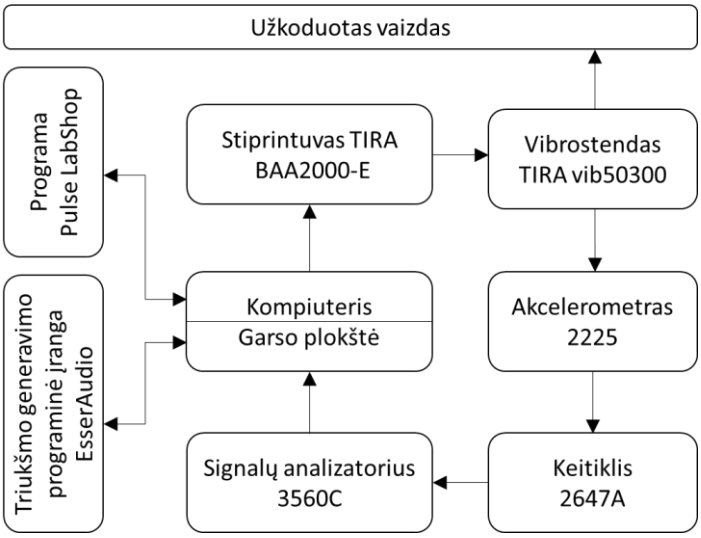
2.36 pav. Slaptas vaizdas (kairėje) ir užkoduotas slaptas vaizdas (dešinėje), kai $\lambda_s = 2{,}2$ mm, $\lambda_b = 2{,}8$ mm [94]

Visa eksperimentinė įranga parodyta 2.37 paveiksle. Eksperimentinės įrangos scheminė diagrama – 2.38 paveiksle.

Vibrostendas *TIRA vib 50300* yra valdomas stiprintuvu *TIRA BAA 200-E*. Triukšmą generuojanti programinė įranga *Esser Audio* naudojama baltajam triukšmui sukurti. Šis triukšmas perleidžiamas per žemojo dažnio filtrą (dažnių diapazonas nustatomas nuo 0 Hz iki 100 Hz). Tada signalas perleidžiamas per stiprintuvą. Užkoduotas išspausdintas vaizdas yra priklijuojamas prie vertikalios plokštumos ir įtvirtinamas ant vibrostendo paviršiaus (2.37 paveikslas). Lengvasvoris pjezoelektrinis akcelerometras *Endevco 2225* (jautrumas 0,07655 pC/m/s^2) pritvirtinamas prie vibrostendo darbinio elemento. Akcelerometro išėjimas yra sujungtas su analizatoriumi *Pulse 3560* per *2647A* tipo krūvio–įtampos keitiklį (stiprinimas 1mV/pC). Programa *Brue&Kjaer Pulse LabShop* kontroliuoja visą procesą. Šitaip atsiranda galimybė nustatyti, stebėti ir keisti chaotinių virpesių parametrus.

[7] *Šiame skyriuje pristatomi rezultatai buvo publikuoti straipsnyje*:
Near-optimal pitch of a moiré grating in dynamic visual cryptography
Saunorienė L., Petraukienė V., Aleksienė S., Ragulskienė J.

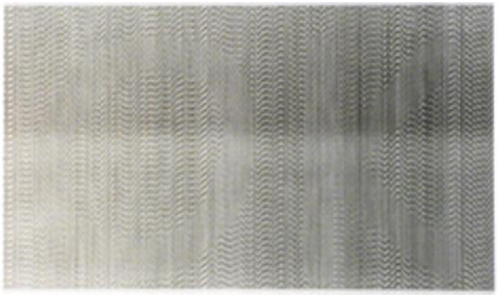
2.37 pav. Vibrostendas



2.38 pav. Eksperimentinės įrangos scheminė diagrama

Pirmiausiai filtruoto triukšmo generatorius sukuria 30 s trukmės baltojo triukšmo signalus, kurie filtruojami žemųjų dažnių filtru. Didžiausias dažnis 30 Hz. Kadangi vibrostendas negali vibruoti 10 kHz dažniu, yra naudojamas žemojo dažnio filtras norint imituoti netiesines mechaninių sistemų vibracijas.

Atliekant eksperimentą, vienintelis kintamas parametras yra kontrolinio signalo stiprumas. Užkoduotas vaizdas lieka stacionarioje padėtyje, kai svyravimų standartinis nuokrypis yra lygus nuliui – slapto vaizdo negalima įžvelgti užkoduotame vaizde. Kai svyravimų standartinis nuokrypis $\sigma = 0{,}6$, slaptas vaizdas išryškėja laike vidurkintame vaizde. 2.39 paveiksle pateiktas laike vidurkintas užkoduotas vaizdas, užfiksuotas naudojant fotoaparatą, kai $T = 0{,}63$ s.



2.39 pav. Eksperimentiškai gautas laike vidurkintas užkoduotas vaizdas, esant chaotiniams svyravimams, kai $\lambda_s = 2{,}2$ mm, $\lambda_b = 2{,}8$ mm, $\sigma = 0{,}6$, $T = 0{,}63$ s

2.6. Antrojo skyriaus išvados

1. Slaptos informacijos užkodavimas ir sėkmingas dekodavimas yra paremtas teisingu muaro gardelės parametrų parinkimu. Todėl buvo pasiūlyta metodika, kuria remiantis galima parinkti optimalius muaro gardelės parametrus tiek harmoninių, tiek chaotinių virpesių atveju. Slaptos informacijos periodas turi užtikrinti pilkos srities atsiradimą laike vidurkintame vaizde (šioje srityje standartinis nuokrypis yra lygus nuliui). Fono periodas turi garantuoti pakankamai didelį standartinį nuokrypį laike vidurkintame vaizde. Toks beveik optimalus muaro gardelių periodų poros parinkimas užtikrina pakankamą dekoduojamo vaizdo kontrastą, taip pat ir faktą, kad slapta informacija nėra matoma statiniame vaizde.
2. Pasiūlyta vaizdo kodavimo schema, kai kintamo periodo muaro gardelė svyruoja pagal tam tikrą tikrinę formą. Slapta informacija išryškėja per laike vidurkintas muaro interferencines juostas, kai užkoduotas vaizdas virpinamas pagal tą pačią tikrinę formą, kuria buvo užkoduotas. Aprašytos schemos efektyvumą iliustruoja skaitiniai pavyzdžiai, kuriuose taikomas baigtinių elementų metodas.
3. Sukurta dinaminės vizualiosios kriptografijos schema, kurioje panaudotos Ronči tipo gardelės ir trikampės bangos formos funkcijos.
4. Pasiūlyta vaizdo kodavimo schema, kai deformuojamoji muaro gardelė svyruoja chaotiškai. Slaptas vaizdas įterpiamas į stacionarią muaro gardelę taip, kad slapta informacija išryškėtų laike vidurkintame vaizde, kai deformuojamasis kūnas virpa chaotiškai pagal tam tikrą tikrinę formą. Nors chaotinių virpesių atveju laike vidurkintos interferencinės juostos nesiformuoja, tačiau slaptas vaizdas yra atkoduojamas dėl fono bei slaptos zonos užpilkėjimų skirtumo laike vidurkintame vaizde.

3. DVIMATĖ MUARO GARDELĖ: NEDEFORMUOJAMAS KŪNAS

Šiame skyriuje pirmą kartą apibrėžiama dvimatė kryžminė muaro gardelė. Slaptai informacijai užkoduoti dvimatėje muaro gardelėje reikalingi visiškai kitokie metodai ir kitokios technikos negu buvo taikomos vienmatėje muaro gardelėje. Kaip jau minėta 1.7.3 skyrelyje, slaptam vaizdui paslėpti vienmatėje muaro gardelėje yra taikomi fazių reguliarizacijos ir pradinės atsitiktinės fazės algoritmai. Jeigu pabandytume slaptą informaciją paslėpti remdamiesi tokiu pačiu principu dvimatėje gardelėje pagal pasirinktą ašį, tai sudarkytume muaro juostų struktūrą stulpeliuose (arba eilutėse), todėl slaptas vaizdas virpinant gardelę nepasirodytų. Todėl 3.1 skyriuje aprašomi pagrindiniai principai, reikalingi norint paslėpti informaciją dvimatėje kryžminėje muaro gardelėje [95].

Taip pat šiame skyriuje yra aprašyti eksperimentiniai stendai ir pristatyti realių eksperimentų rezultatai dvimatės kryžminės (3.2 poskyris) bei apskritiminės (3.4 poskyris [96]) gardelių atveju.

3.1. Vaizdo slėpimo schema, pagrįsta laike vidurkintais elipsiniais svyravimais[8]

3.1.1. Dvimatė muaro gardelė

Ant plokščio paviršiaus susidarantis lygiagrečių baltų ir juodų linijų masyvas gali būti aprašytas šia formule:

$$F(x,y) = \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right); \tag{3.1}$$

čia x yra išilginė koordinatė; λ – muaro gardelės periodas; y ašis sutampa su gardelę sudarančių linijų kryptimi. Panašiai kaip ir vienmatės gardelės atveju, tarkime, kad nedeformuojamojo kūno paviršius svyruoja harmoniškai. Dvimačio nedeformuojamojo kūno paviršiuje vienkrypčiai svyravimai x ašies kryptimi aprašomi taip:

$$\begin{aligned} &\lim_{T\to\infty}\frac{1}{T}\int_0^T F(x - a\sin t, y)dt = \\ &= \lim_{T\to\infty}\frac{1}{T}\int_0^T \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}(x - a\sin t)\right) = \frac{1}{2} + \frac{1}{2}J_0\left(\frac{2\pi}{\lambda}a\right). \end{aligned} \tag{3.2}$$

Laike vidurkintas vaizdas tampa visiškai pilku, kai $a = \frac{\lambda}{2\pi}r_i$. Kitaip tariant, svyravimai išilgai y ašies nekeičia statinio vaizdo:

[8] *Šiame skyriuje pristatomi rezultatai buvo publikuoti straipsnyje*:
Image hiding scheme based on time-averaged elliptic oscillations
Saunorienė L., Aleksienė S.; Maskeliūnas R.; Ragulskis M.

$$\lim_{T\to\infty}\frac{1}{T}\int_0^T F(x,y-a\sin t)dt=\lim_{T\to\infty}\frac{1}{T}\int_0^T\left(\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)\right)= \\ =\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right). \tag{3.3}$$

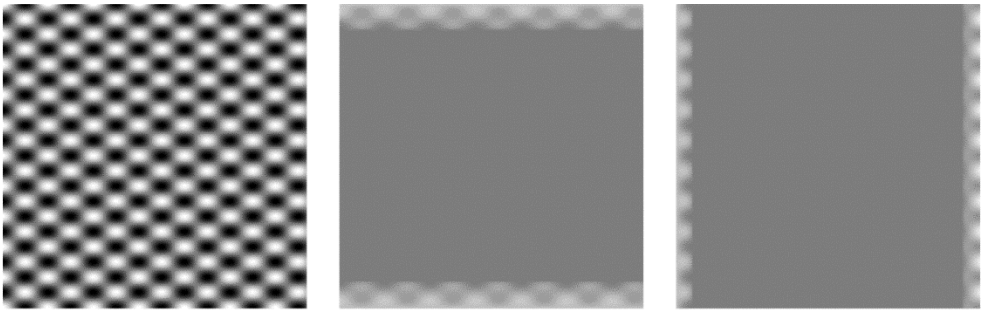
Tai yra gerai žinomas eksperimentinės mechanikos rezultatas, kad deformacijos išilgai gardelę sudarančiųjų linijų nekeičia paviršiaus optinio vaizdo [3, 4].

3.1.2. Dvimatės muaro gardelės vienkrypčiai svyravimai

Statinė dvimatė gardelė gali būti aprašyta tokiu būdu:

$$F_2(x,y)=\tfrac{1}{2}+\tfrac{1}{2}\cos\left(\tfrac{2\pi}{\lambda}x\right)\cos\left(\tfrac{2\pi}{\mu}y\right); \tag{3.4}$$

čia λ – muaro gardelės periodas horizontaliąja kryptimi; μ – muaro gardelės periodas vertikaliąja kryptimi. Dvimatės muaro gardelės pavyzdys, kai $\lambda=0{,}75$ ir $\mu=0{,}5$, pateiktas 3.1(a) paveiksle.



3.1 pav. Dvimatės kryžminės gardelės vienkrypčiai svyravimai: (a) statinis vaizdas, kai $\lambda=0{,}75$, $\mu=0{,}5$; (b) laike vidurkintas vaizdas vertikaliųjų vienkrypčių svyravimų atveju, kai $b=0{,}4393$; (c) laike vidurkintas vaizdas horizontaliųjų vienkrypčių svyravimų atveju, kai $a=0{,}2871$

Jei kryžminė (angl. *cross-grating*) gardelė, aprašyta (3.4) lygtimi, svyruoja išilgai x ir y ašių, gautas laike vidurkintas vaizdas aprašomas taip:

$$\lim_{T\to\infty}\frac{1}{T}\int_0^T F_2(x-a\sin t,y)dt=\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)\cos\left(\frac{2\pi}{\mu}y\right)J_0\left(\frac{2\pi}{\lambda}a\right); \tag{3.5}$$

$$\lim_{T\to\infty}\frac{1}{T}\int_0^T F_2(x,y-b\sin t)dt=\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)\cos\left(\frac{2\pi}{\mu}y\right)J_0\left(\frac{2\pi}{\mu}b\right); \tag{3.6}$$

čia a ir b yra harmoninių svyravimų amplitudės išilgai x ir y ašių.

Kitais žodžiais tariant, kryžminė gardelė tampa visiškai pilka, kai harmoninių svyravimų amplitudė išilgai x ir y ašių yra tokia, kad pirmojo tipo nulinės eilės Beselio funkcija tampa lygia 0. Šie rezultatai parodyti 3.1(b) ir 3.1(c) paveiksluose.

Jeigu vienkrypčiai svyravimai atliekami kampu $\varphi = \arctan\left(\frac{b}{a}\right)$ x ašies atžvilgiu, tai elementarių trigonometrinių pertvarkymų dėka laike vidurkintą vaizdą galima aprašyti taip:

$$\begin{aligned}&\lim_{T\to\infty}\frac{1}{T}\int_0^T F_2(x-a\sin t, y-b\sin t)dt = \\ &= \frac{1}{2}+\frac{1}{4}\cos\left(\frac{2\pi}{\lambda}x\right)\cos\left(\frac{2\pi}{\mu}y\right)\left(J_0\left(\frac{2\pi}{\lambda}a+\frac{2\pi}{\mu}b\right)+J_0\left(\frac{2\pi}{\lambda}a-\frac{2\pi}{\mu}b\right)\right) \\ &\quad+\frac{1}{4}\sin\left(\frac{2\pi}{\lambda}x\right)\sin\left(\frac{2\pi}{\mu}y\right)\left(J_0\left(\frac{2\pi}{\lambda}a-\frac{2\pi}{\mu}b\right)\right. \\ &\quad\left.-J_0\left(\frac{2\pi}{\lambda}a+\frac{2\pi}{\mu}b\right)\right).\end{aligned} \tag{3.7}$$

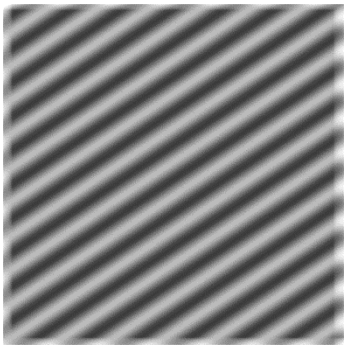
Tada, jeigu vienkrypčių svyravimų parametrai yra apibrėžti lygtimi $\frac{a}{\lambda}=\frac{b}{\mu}$, tai (3.7) lygtis gali būti perrašyta tokiu būdu:

$$\begin{aligned}&\lim_{T\to\infty}\frac{1}{T}\int_0^T F_2\left(x-a\sin t, y-a\frac{\mu}{\lambda}\sin t\right)dt = \\ &= \frac{1}{2}+\frac{1}{4}\cos\left(\frac{2\pi}{\lambda}x\right)\cos\left(\frac{2\pi}{\mu}y\right)\left(J_0\left(\frac{4\pi}{\lambda}a\right)+1\right)+ \\ &\quad+\frac{1}{4}\sin\left(\frac{2\pi}{\lambda}x\right)\sin\left(\frac{2\pi}{\mu}y\right)\left(1-J_0\left(\frac{4\pi}{\lambda}a\right)\right)= \\ &= \frac{1}{2}+\frac{1}{4}\left(\cos\left(\frac{2\pi}{\lambda}x-\frac{2\pi}{\mu}y\right)+\cos\left(\frac{2\pi}{\lambda}x+\frac{2\pi}{\mu}y\right)J_0\left(\frac{4\pi}{\lambda}a\right)\right).\end{aligned} \tag{3.8}$$

Parametrų a ir b tinkamas parinkimas ($a=\frac{\lambda}{4\pi}r_i$ ir $b=\frac{\mu}{4\pi}r_i$, $i=1,2,...$) duoda tokį rezultatą:

$$\lim_{T\to\infty}\frac{1}{T}\int_0^T F_2\left(x-\frac{\lambda}{4\pi}r_i\sin t, y-\frac{\mu}{4\pi}r_i\sin t\right)dt = \frac{1}{2}+\frac{1}{4}\cos\left(\frac{2\pi}{\lambda}x-\frac{2\pi}{\mu}y\right). \tag{3.9}$$

Kitais žodžiais tariant, kryžminė gardelė yra transformuojama į nuožulnių linijų masyvą laike vidurkintame vaizde. Šis įdomus optinis efektas pavaizduotas 3.2 paveiksle.



3.2 pav. Nedeformuojamosios gardelės, pavaizduotos 3.1(a) paveiksle, vienkrypčiai svyravimai virsta į nuožulnių linijų masyvą, kai $a = 0{,}1435$, $b = 0{,}0957$, $\varphi = \frac{\pi}{4}$

3.1.3. Dvimatė kryžminė gardelė elipsinių svyravimų atveju

Tarkime, kad dvimatės kryžminės gardelės nuokrypiai nuo pusiausvyros padėties aprašomi elipsiškai. Pažymėkime elipsės pusašes a ir b. Tada atlikę elementarius trigonometrinius pertvarkymus gauname:

$$\lim_{T\to\infty} \frac{1}{T}\int_0^T F_2(x - a\sin t, y - b\cos t) = \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)\cos\left(\frac{2\pi}{\mu}y\right)J_0(M); \qquad (3.10)$$

čia

$$M = \sqrt{\left(\frac{2\pi}{\lambda}a\right)^2 + \left(\frac{2\pi}{\mu}b\right)^2};\ \varphi = arctan\left(\frac{b\lambda}{a\mu}\right). \qquad (3.11)$$

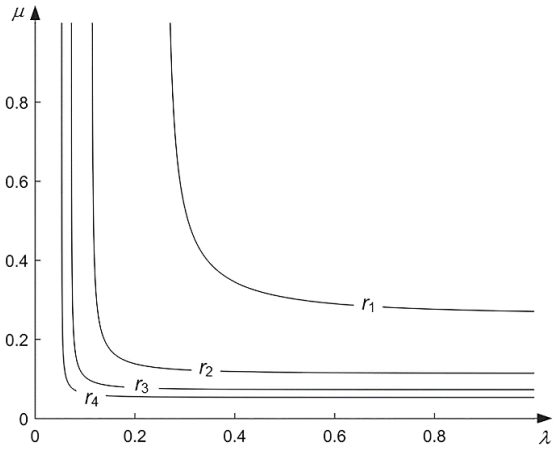
Taigi laike vidurkintas vaizdas tampa visiškai pilkas, kai tenkinama ši lygtis:

$$\left(\frac{2\pi}{\lambda}a\right)^2 + \left(\frac{2\pi}{\mu}b\right)^2 = (r_i)^2;.i = 1, 2, \dots . \qquad (3.12)$$

Jeigu $a = b = A$, tai (3.12) lygtis pavirs tokiu santykiu tarp λ and μ:

$$\lambda = \frac{1}{\sqrt{\left(\frac{r_i}{2\pi A}\right)^2 - \frac{1}{\mu^2}}};\ \mu > \frac{2\pi A}{r_i};\ i = 1, 2, \dots . \qquad (3.13)$$

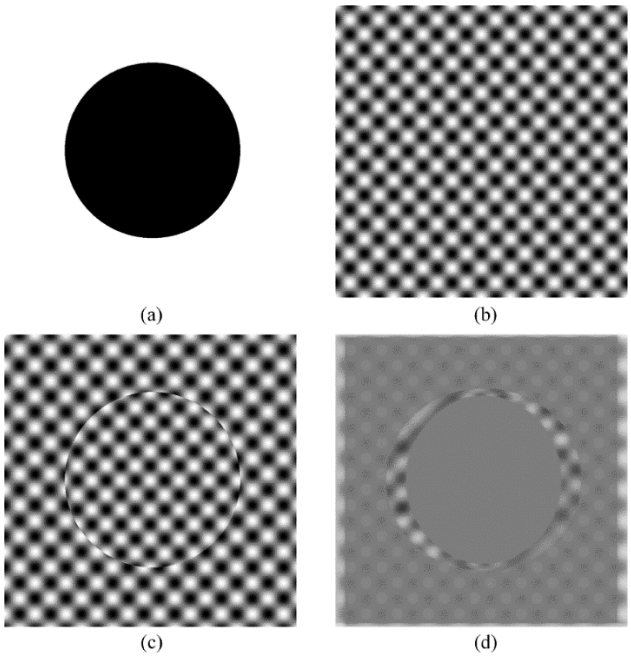
Grafinis (3.13) lygties vaizdas parodytas 3.3 paveiksle.



3.3 pav. Santykis tarp gardelės parametrų λ ir μ, kai $A = 0{,}1$; skirtingos kreivės atitinka skirtingas r_i reikšmes, kai $i = 1, 2, 3, 4$.

3.1.4. Vaizdo slėpimas dvimatėje kryžminėje gardelėje

Tarkime, kad slaptas vaizdas yra juodas apskritimas, pavaizduotas 3.4(a) paveiksle. Sukonstruokime foną, kaip dvimatę kryžminę gardelę su parametrais $\lambda = 1{,}7$ ir $\mu = 1{,}7$ (3.4(b) paveikslas).



3.4 pav. Tiesioginis geometrinės formos įterpimas į foną neduoda tinkamo užkoduoto vaizdo: (a) slaptas vaizdas (juodas skritulys); (b) statinė fono muaro gardelė, kai $\lambda = 1{,}7$, $\mu = 1{,}7$; (c) tiesioginė įterpimo procedūra duoda aiškiai matomą liniją tarp fono ir slaptos informacijos ($\lambda = 1{,}6$, $\mu = 1{,}6$ yra taikomi slaptos informacijos srityje); (d) skaitmeninis dekodavimas, taikant elipsinius svyravimus, kai $a = 0{,}5788$, $b = 0{,}2$

Slaptas vaizdas, t. y. apskritimas, taip pat sukonstruotas kaip dvimatė kryžminė gardelė, tačiau su skirtingais periodais $\lambda = 1{,}6$ ir $\mu = 1{,}6$ (3.4(c) paveikslas). Ribinė linija tarp fono ir slaptos informacijos aiškiai matyti 3.4(c) paveiksle – todėl tokio būdo negalima vadinti informacijos slėpimo technika. Nepaisant to, atitinkamų elipsinio dėsnio parametrų parinkimas ($a = 0{,}5788$; $b = 0{,}2$) suformuoja visiškai pilką sritį, kurioje yra slapta informacija, laike vidurkintame vaizde – tuo metu fone matyti nevisiškai išreikštos laike vidurkintos interferencinės juostos. Būtina pažymėti, kad ribinėje linijoje tarp fono ir slaptos informacijos susiformuoja neišreikštų interferencinių juostų ruožas, kuris atsiranda dėl užkoduoto vaizdo elipsinio judėjimo (3.4(d) paveikslas).

Akivaizdu, kad reikėtų sudėtingesnių vaizdo slėpimo schemų, nei aprašyta 3.4 paveiksle. Deja, stochastinė muaro gardelė negali būti naudojama elipsiniams svyravimams – vadinasi, pradinės atsitiktinės fazės parinkimo algoritmas negali padėti slėpti slaptos informacijos. Vienas iš galimų sprendimų yra sumažinti skirtumą tarp fono ir slaptos informacijos periodų – tačiau skirtumas turi būti pakankamai didelis tam, kad būtų įmanoma atskirti slaptą informaciją ir foną laike vidurkintame vaizde [72].

Taigi pagrindinė slaptos informacijos užkodavimo dvimatėje muaro gardelėje (3.4 lygtis) idėja yra pagrįsta λ ir μ reikšmių didinimu mažais dydžiais λ^* ir μ^*:

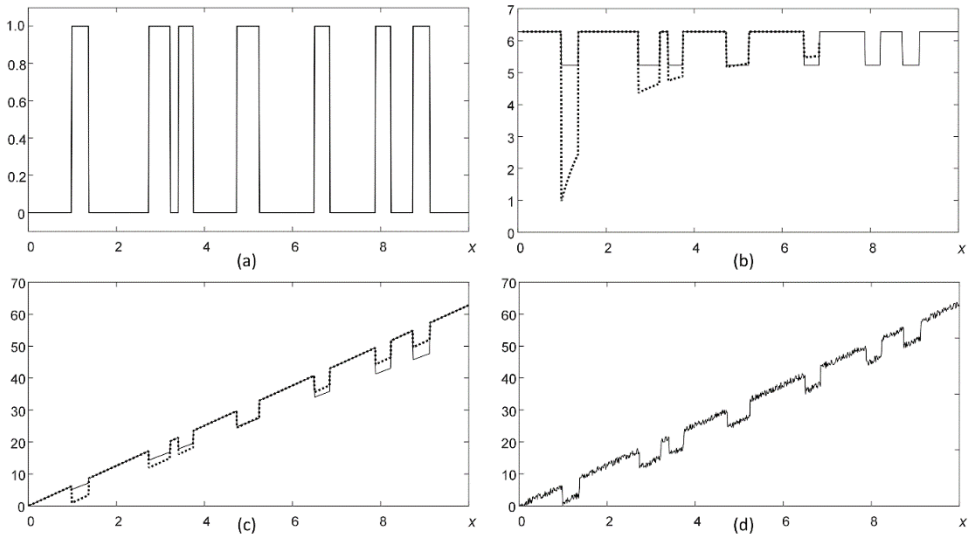
$$F_2(x, y) = \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi x}{\lambda+\lambda^*}\right)\cos\left(\frac{2\pi y}{\mu+\mu^*}\right); \tag{3.14}$$

čia λ^* ir μ^* ($\lambda^* \ll \lambda$ ir $\mu^* \ll \mu$) yra maži teigiamieji skaičiai srityje, apimančioje vaizdą, ir lygūs nuliui fone.

Reikia pažymėti, kad sąlygų λ^* ir μ^* (esančių 3.14 lygtyje) įtaka didėja, kai didėja koordinačių *x* ir *y* reikšmės (kaip matyti 3.5 paveiksle). Vientisa linija 3.5(c) paveiksle rodo šį faktą – skirtumas tarp reikšmių $\frac{2\pi x}{\lambda+\lambda^*}$ ir $\frac{2\pi x}{\lambda}$ didėja, kai didėja *x*. Lygiai taip pat skirtumas tarp reikšmių $\frac{2\pi y}{\mu+\mu^*}$ ir $\frac{2\pi y}{\mu}$ didėja, kai didėja *y*. Todėl reikia surasti tokias funkcijas $\lambda^* = l(x)$ ir $\mu^* = m(y)$, kurios užtikrintų nuolatinį $\frac{2\pi x}{\lambda+\lambda^*}$ ir $\frac{2\pi y}{\mu+\mu^*}$ kitimą su kiekviena *x* ir *y* reikšme:

$$\begin{aligned} &\frac{2\pi x}{\lambda} - \frac{2\pi x}{\lambda + l(x)} = \delta, \qquad 0 \le x \le x_{max}; \\ &\frac{2\pi y}{\mu} - \frac{2\pi y}{\mu + m(y)} = \delta, \qquad 0 \le y \le y_{max}; \end{aligned} \tag{3.15}$$

čia x_{max} ir y_{max} apibrėžia stačiakampio užkoduoto vaizdo maksimalius matmenis; δ yra slenkstinė reikšmė, užtikrinanti mažiausią skirtumą tarp dvimatės muaro gardelės periodų, garantuojanti interpretuojamą skirtumą laike vidurkintame vaizde.



3.5 pav. Vienmatis pavyzdys, iliustruojantis atsitiktinio triukšmo δ reikšmės parinkimo algoritmą: (a) slaptos informacijos scheminis vaizdavimas (reikšmė 1 atitinka slaptą informaciją; 0 atitinka foną); (b) $\frac{2\pi}{\lambda+\lambda^*}$ kitimas (vientisa linija) ir $\frac{2\pi}{\lambda+l(x)}$ kitimas (brūkšniuota linija); (c) $\frac{2\pi x}{\lambda+\lambda^*}$ kitimas (vientisa linija) ir $\frac{2\pi x}{\lambda+l(x)}$ kitimas (brūkšniuota linija); (d) $\frac{2\pi x}{\lambda+l(x)}$ kitimas su atsitiktinai parinkta δ reikšme

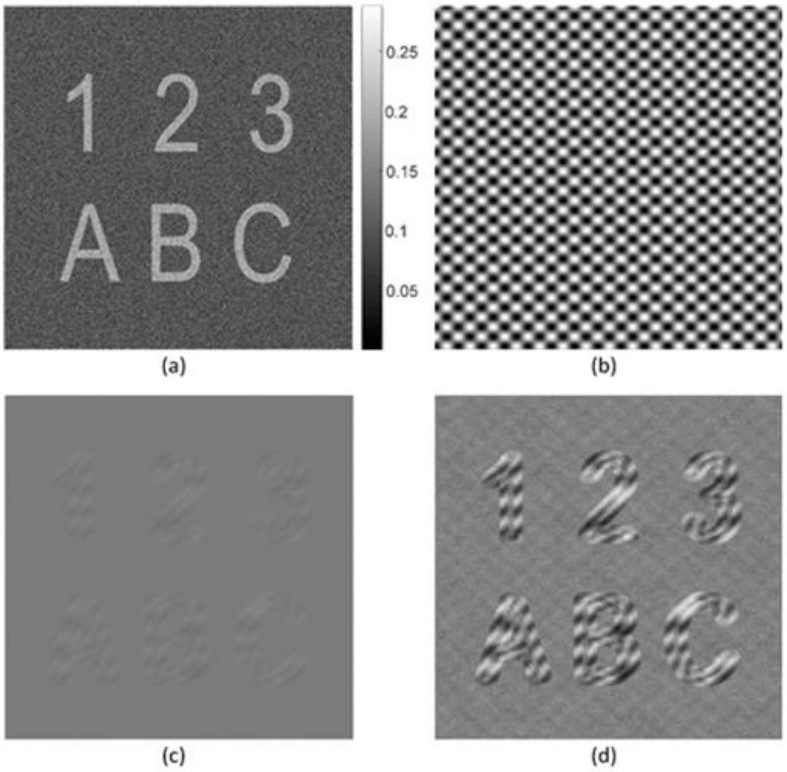
Tarkime, kad δ yra lygi nuliui fone ir lygi iš anksto nustatytam skaičiui slapto vaizdo srityje. Iš (3.15) lygties galime gauti tokias $l(x)$ ir $m(y)$ išraiškas:

$$l(x) = \frac{\lambda\delta}{2\pi x - \delta};$$
$$m(y) = \frac{\mu\delta}{2\pi y - \delta}. \tag{3.16}$$

Punktyrinė linija 3.5(b) ir 3.5(c) paveiksle rodo atitinkamai $\frac{2\pi}{\lambda+l(x)}$ ir $\frac{2\pi x}{\lambda+l(x)}$ kitimą. Šiame pavyzdyje δ reikšmė gaunama iš lygybės $l(\frac{x_{max}}{2}) = \lambda^*$.

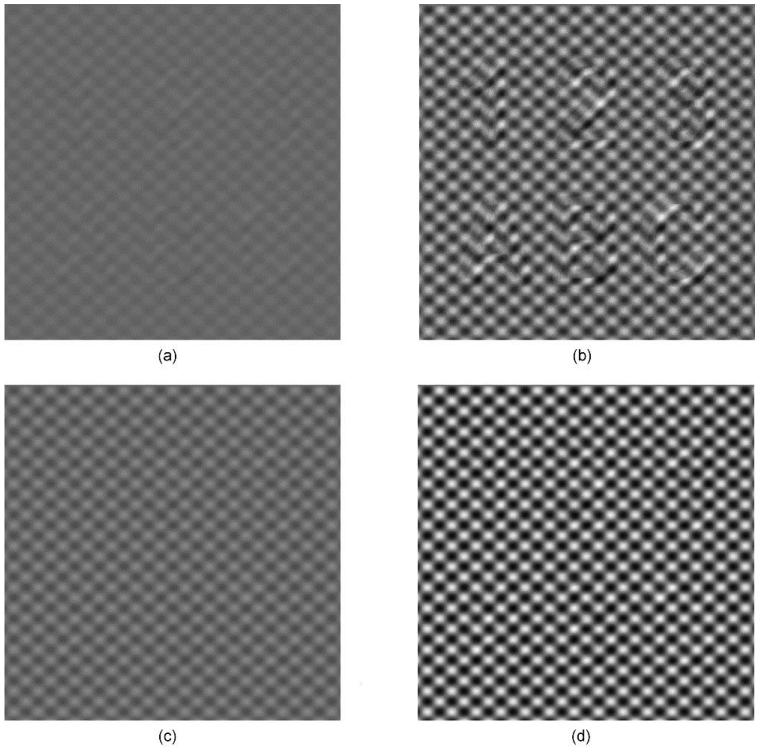
Kaip minėta, visos vaizdų slėpimo schemos, pagrįstos dinamine vizualiąja kriptografija, nėra kriptografiškai saugios. Pagrindinis reikalavimas tas, kad slapta informacija nesimatytų stacionariame užkoduotame vaizde. Būtent todėl pasiūlytos vaizdo slėpimo schemos optinis saugumas gali būti padidintas pridedant atsitiktinį triukšmą prie δ reikšmės. 3.5(d) paveiksle matome $\frac{2\pi x}{\lambda+l(x)}$ kitimą, kai prie δ yra pridėtas atsitiktinis triukšmas.

3.6 paveiksle parodytas vaizdo slėpimo technikos, pagrįstos elipsiniais svyravimais, įgyvendinimas. Slaptas vaizdas sudarytas iš skaičių 1, 2, 3 ir raidžių *A*, *B*, *C*. Simbolių plotis parinktas taip, kad būtų lygus pusei fono kryžminės gardelės periodo. Tai atitinka minimalų kvadratinės formos objekto dydžio įterpimą į stochastinę muaro gardelę vienkrypčiam dekodavimui [10].



3.6 pav. Vaizdų slėpimo schema, paremta elipsiniais svyravimais: (a) $\delta(x, y)$ reikšmės, atitinkančios stacionarų slaptą vaizdą; (b) stacionarus užkoduotas vaizdas, kai $\lambda = 0{,}8$, $\mu = 0{,}68$ (plika akimi neįmanoma interpretuoti slapto užkoduoto vaizdo); (c) užkoduotas laike vidurkintas vaizdas, gautas atlikus elipsinius svyravimus, kai $a = 0{,}25$, $b = 0{,}15$; (d) paryškintame laike vidurkintame vaizde matomi aiškūs slaptos informacijos kontūrai

3.6(a) paveiksle parodytos δ reikšmės, taikomos slaptos informacijos kodavimui. Užkoduotas vaizdas konstruojamas kaip deformuojamoji dvimatė kryžminė gardelė (3.6(b) paveikslas). Tarkime, kad vaizdas yra 12×12 stačiakampis, kurio dvimatės muaro gardelės periodai yra $\lambda = 0{,}8$ ir $\mu = 0{,}68$. Akivaizdu, kad slapta informacija nesimato žiūrint plika akimi į užkoduotą vaizdą (3.6(b) paveikslas). Atkoduotas vaizdas gaunamas virpinant užkoduotą vaizdą elipsiškai amplitudėmis $a = 0{,}25$ ir $b = 0{,}15$. Kaip nagrinėta 3.1.3 skyrelyje, parametrai λ, μ, a ir b turi atitikti (3.12) sąryšį tam, kad išryškėtų laike vidurkintos muaro interferencinės juostos. Originalus ir paryškintas laike vidurkinti vaizdai parodyti 3.6(c) ir 3.6(d) paveiksluose. Gana akivaizdu, kad iššifruoti simboliai laike vidurkintame vaizde (paveikslas 3.6(d)) yra didesni lyginant su užkoduotais simboliais (paveikslas 3.6(a)). Tai atsitinka dėl elipsinių svyravimų – simbolius ribojančios ribos užpilkėja. Kuo didesnės elipsės pusašės, tuo didesnės užpilkėjusios zonos.



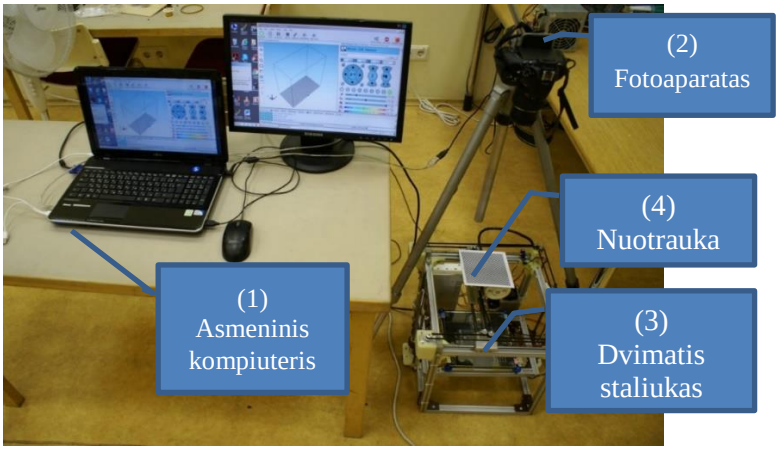
3.7 pav. Netinkamai parinkus elipsinių svyravimų amplitudes slapta informacija neišryškėja: (a) nevisiškai išryškėjusios muaro interferencinės juostos laike vidurkintame vaizde, kai $a = 0{,}26$, $b = 0{,}16$; (b) laike vidurkintam vaizdui (kai $a = 0{,}26$, $b = 0{,}16$) pritaikius kontrasto išryškinimo algoritmą išryškėja neinterpretuojami slaptos informacijos kontūrai; (c) laike vidurkintame vaizde neišryškėja slapta informacija, kai $a = 0{,}29$, $b = 0{,}19$; (d) laike vidurkintam vaizdui (kai $a = 0{,}29$, $b = 0{,}19$) pritaikius kontrasto išryškinimo algoritmą neišryškėja jokie slapto vaizdo kontūrai

3.7 paveiksle parodyta, kaip neišryškėja slapta informacija, esant netinkamoms elipsinių svyravimų amplitudėms. Nevisiškai išryškėjusios muaro interferencinės juostos parodytos 3.7(a) paveiksle, kai elipsinių svyravimų parametrai yra $a = 0{,}26$, $b = 0{,}16$. Laike vidurkintas vaizdas yra visiškai neinterpretuojamas, kai $a = 0{,}29$, $b = 0{,}19$ (3.7(c) paveikslas).

Reikia pažymėti, kad šiame skyrelyje pasiūlytos schemos informacijos talpa (slaptos informacijos kiekis, kuris gali būti įterptas į užkoduotą vaizdą) nėra blogesnė nei informacijos talpa, aprašyta [10] straipsnyje.

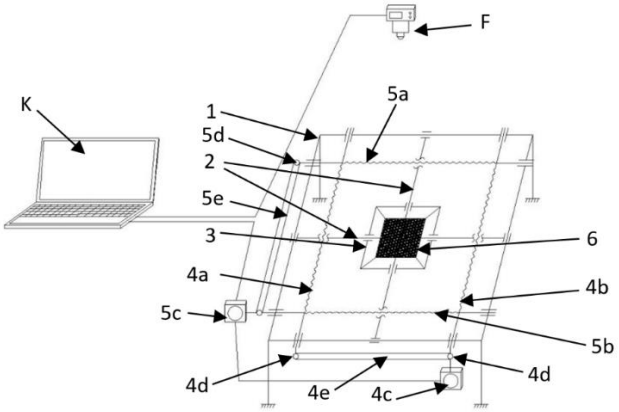
3.2. Šifruotų vaizdų dekodavimo eksperimentinis stendas kryžminės dvimatės muaro gardelės atveju

Eksperimentinis užšifruotų vaizdų dekodavimo stendas (3.8 paveikslas) sudarytas iš kompiuterio (1), kabeliais prijungtais skaitmeniniu fotoaparatu (2) ir skaitmeniniu būdu valdomu staliuku (3) su ant jo pritvirtinta užšifruoto vaizdo nuotrauka (4).



3.8 pav. Eksperimentinio stendo nuotrauka

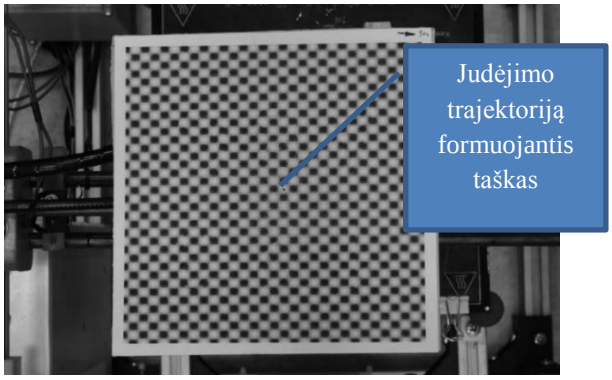
Staliuko konstrukcija (3.9 paveikslas) sudaryta iš korpuso (1) su prie jo pritvirtintomis kreipiančiosiomis (2), kuriomis slysta staliukas (3). Prie staliuko pritvirtinti du dvigubi sraigto–veržlės (4a, 4b) ir (5a, 5b) pavaros mechanizmai su žingsniniais varikliais (4c) ir (5c). Šios dvi sraigto–veržlės pavaros (4a, 4b) ir (5a, 5b) pritvirtintos prie staliuko (3) judamai ir nukreiptos viena kitos atžvilgiu 90° kampu. Sraigtai per krumpliuotus skriemulius (4d) ir (5d) sujungti vienas su kitu krumpliuotais diržais (4e) ir (5e). Ant staliuko (3) priklijuojama nuotrauka (6) su joje užkoduotu vaizdu.



3.9 pav. Eksperimentinio vaizdų dešifravimo stendo principinė schema. K – kompiuteris; F –skaitmeninis fotoaparatas. Staliuko konstrukcija: 1 – korpusas; 2 – kreipiančiosios; 3 – staliukas; 4a ir 4b – *x* ašies valdiklis; 5a ir 5b – *y* ašies valdiklis; 4c ir 5c – žingsniniai varikliai; 4d ir 5d – krumpliuoti skriemuliai; 4e ir 5e – krumpliuoti diržai; 6 – nuotrauka su užkoduotu vaizdu

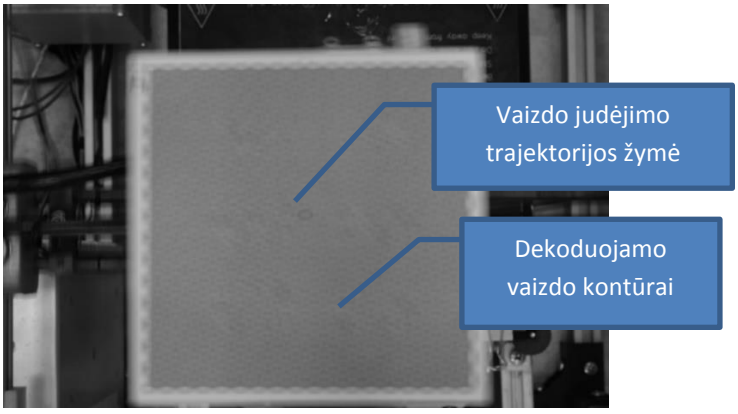
Nuotraukos judėjimo plokštumoje trajektorijos nustatymui jos centre padėtas taškas (3.10 paveikslas), kuris nuotraukai judant nustatyta trajektorija nufotografuotame vaizdo centre suformuoja judesio trajektorijos liniją. Eksperimentas atliekamas pirmiausia nustatant kompiuterio programoje staliuko judesį formuojančių žingsninių variklių pasisukimą vienas kito atžvilgiu per nustatytą laiką pagal iš anksto žinomos (čia

nustatyta trajektorijos forma – elipsė, 3×4 mm) trajektorijos parametrus. Prie staliuko pritvirtinama išspausdinta užkoduoto vaizdo nuotrauka su pažymėtu tašku gerai matomoje jos vietoje, centre. Virš staliuko su nuotrauka pritvirtinamas skaitmeninis fotoaparatas, nustatomas ryškumas ir ekspozicijos laikas (šiuo atveju – 2 s.) Fotoaparatas su kompiuteriu sujungiamas USB kabeliu duomenų perdavimui. Prie kompiuterio prijungiamas ir skaitmeninio valdymo dviejuose matmenyse (*x*, *y* plokštumoje) staliuko mechanizmas.



3.10 pav. Įtvirtinta ant dvimačio staliuko dekoduojama nuotrauka su judėjimo trajektorijos kontrolės žyme – tašku centre

Paleidžiama kompiuterinė staliuko valdymo programa, ir staliukas pradeda judėti pagal nustatytą judėjimo dėsnį sukiojantis žingsniniams varikliams į vieną arba kitą pusę. Staliuko judėjimo metu įjungiamas skaitmeninio fotoaparato fotografavimo režimas, ir taip gaunama 2 s laike vidurkinta skaitmeninė nuotrauka. Iš fotoaparato (3.8 paveikslas) nuotrauka persiunčiama USB kabeliu į kompiuterį, kuriame ją atidarius su nuotraukų peržiūros programa galima pamatyti užšifruotą vaizdą (3.11 paveikslas) anksčiau nematytą plika stebėtojo akimi (3.10 paveikslas).



3.11 pav. Dekoduojamos, laike vidurkintos nuotraukos su staliuko judėjimo trajektorija plokštumoje *x* ir *y* ašių atžvilgiu. Ekspozicijos laikas $T = 2$ s; poslinkis *x* ašimi – 3 mm; poslinkis *y* ašimi – 5 mm

3.3. Apskritiminis geometrinis muaras

Imkime tokį užkoduotą vaizdą, kuris yra sudarytas iš koncentrinių apskritimų apie fiksuotą centro tašką $(x_0;\ y_0)$. Tokiu atveju gardelę galėtume vadinti apskritimine muaro gardele. Kiekvienas apskritimas sudarytas kaip pagal (1.8) formulę apskaičiuotų juodai baltų pikselių rinkinys. Skaičiavimas nuo anksčiau minėtų pavyzdžių skiriasi tuo, kad išilginė koordinatė y yra pakeičiama kampine koordinate φ, tokiu būdu vienkrypčiai svyravimai išilgai y ašies yra pakeičiami kampiniais svyravimais apie centrinį tašką $(x_0;\ y_0)$.

Tardami, kad kampinių harmoninių svyravimų amplitudė a yra konstanta visoje vaizdo srityje, gauname tokią išraišką [97, 98]:

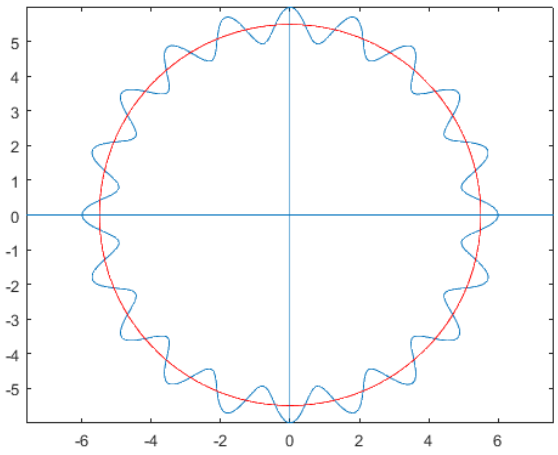
$$F_T(x,y) = \lim_{n\to\infty} \frac{1}{n} \sum_{k=0}^{n-1} \frac{1}{2} \left(1 + \cos\left(\frac{2\pi}{\lambda}\left(\varphi_0 + a\sin\left(\frac{2\pi k}{n}\right)\right)\right)\right); \qquad (3.17)$$

čia n yra diskrečiųjų laiko taškų skaičius viename harmoninių kampinių svyravimų periode, φ_0 yra taško $(x;\ y)$ kampinė koordinatė kampinių svyravimų centrinio taško atžvilgiu [97].

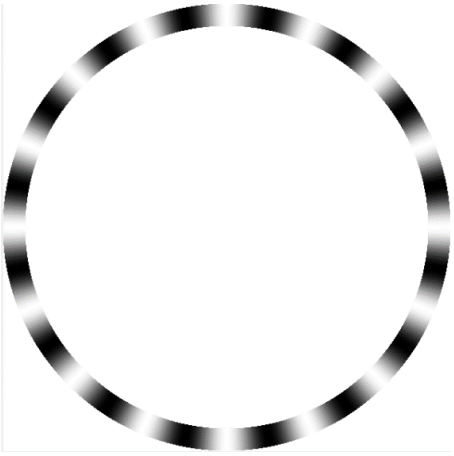
Kampinė koordinatė φ_0 skaičiuojama pagal tokią formulę [97]:

$$\varphi_0 = arctan\left(\frac{y_0 - y}{x - x_0}\right). \qquad (3.18)$$

3.12 paveiksle parodytas statinio koncentrinio apskritimo formavimasis. Vientisa linija paveiksle rodo pilkumo lygio kitimą kampo kryptimi. Šį kitimą atitinkanti optinė vizualizacija pavaizduota kaip žiedas, atitinkantis anksčiau minėtą muaro gardelę (3.13 paveikslas). Parenkant koncentrinę muaro gardelę labai svarbu, kad kampinių periodų skaičius būtų sveikasis, vadinasi, kad atitiktų visą apskritimą.

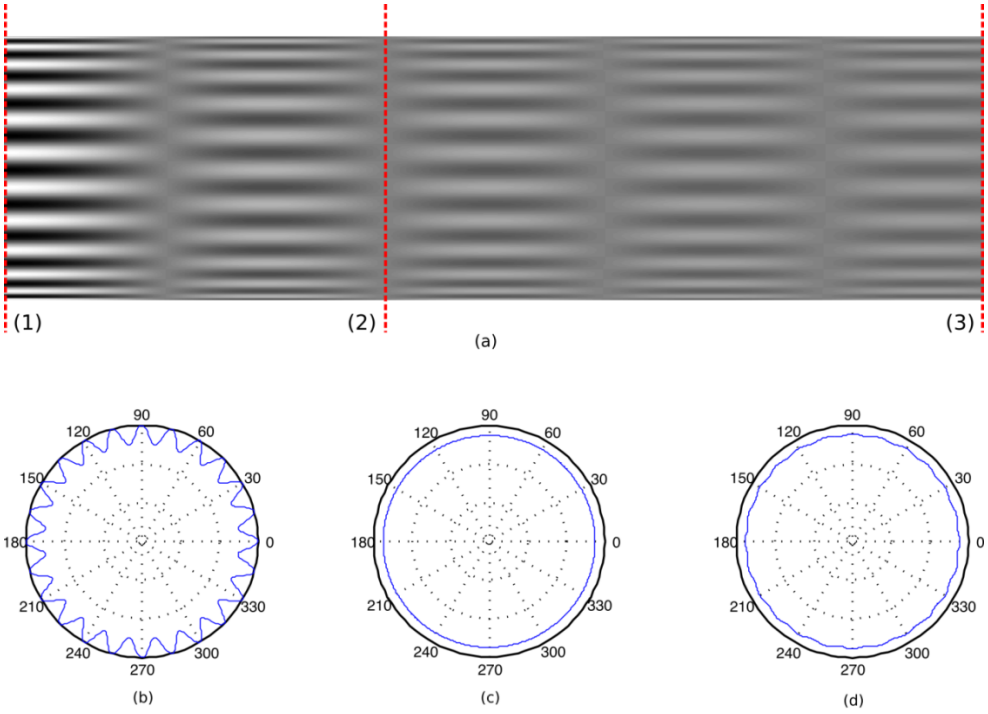


3.12 pav. Apskritiminė muaro gardelė, kurios periodas $\lambda = \pi/10$, pusiausvyros padėtyje



3.13 pav. Optinė apskritiminės muaro gardelės (3.12 paveikslas) vizualizacija

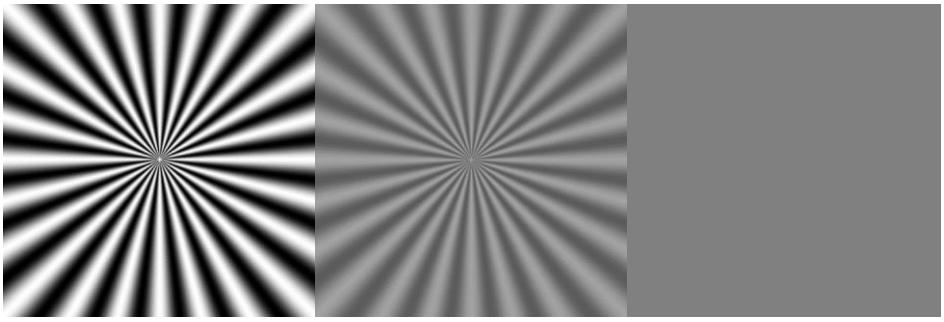
3.14 paveiksle parodyta laike vidurkinta optinė vizualizacija, kai ekspozicijos laikas artėja į begalybę. Kampinių harmoninių svyravimų amplitudė a didėja išilgai horizontaliosios ašies.



3.14 pav. Laike vidurkintų muaro interferencinių juostų, susiformavusių esant kampiniams svyravimams su periodu $\lambda = \pi/12$, skaitmeninis pavyzdys. Laike vidurkintos interferencinės juostos, kai amplitudė a kinta nuo 0 iki 0,6 yra matomos paveikslo (a) dalyje. Pjūviai (1), (2), (3) yra atitinkamai pavaizduoti (b), (c) ir (d) dalyse

3.14 paveikslo (a) dalyje kairėje pusėje, pažymėtoje raudona linija ir skaičiumi (1), amplitudė $a = 0$, skaičiumi (2) – $a = 0{,}23$, skaičiumi (3) – $a = 0{,}6$. Didėjant svyravimų amplitudei procesas netampa monotoniškas, nors laike vidurkintame vaizde didėjant kampinių svyravimų amplitudei matomas judesio sužadintas išblukimas. 3.14(b) paveiksle matome statinį koncentrinį muaro apskritimą, gaunamą, kai $a = 0$. Skaičiumi (2) pažymėtoje vietoje kampinių svyravimų amplitudė parinkta taip, kad iš formulės $a = \frac{\lambda}{2\pi} r_2$ gautume pirmos eilės Beselio funkcijos antrąją šaknį. 3.14 paveiksle skaičiumi (3) pažymėta vieta, kurioje kampinių svyravimų amplitudė nesutampa su jokia Beselio funkcijos šaknimi, o 3.14(d) paveiksle matome svyruojančios apskritiminės muaro gardelės laike vidurkintą vaizdą.

Nagrinėkime apskritiminę geometrinę muaro gardelę su pastoviu kampiniu periodu. Tokia gardelė parodyta 3.15(a) paveiksle.

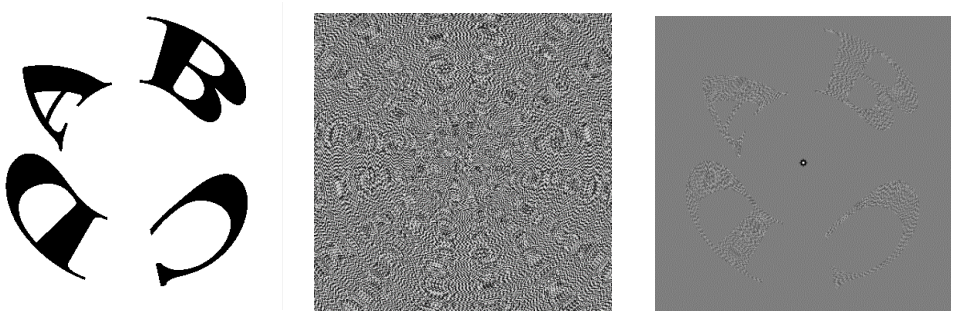


a) b) c)

3.15 pav. Apskritiminės muaro gardelės skaitmeninis pavyzdys. Apskritiminė muaro gardelė pusiausvyros padėtyje parodyta (a) dalyje, nevisiškai susiformavusios kampinių svyravimų laike vidurkintos interferencinės juostos, kai $a = 0{,}276$, yra pavaizduotos (b) dalyje, kampinių svyravimų interferencinės juostos, kai $a = 0{,}23$, yra parodytos (c) dalyje

Žinome, kad atitinkamos harmoninių kampinių svyravimų amplitudės parinkimas suformuos laike vidurkintas interferencines juostas. Tačiau šios juostos susiformuos tik tada, kai harmoninių svyravimų amplitudė sutaps su nulinės eilės pirmojo tipo Beselio funkcijos šaknimi. Skaičiavimai atliekami pagal (1.24) formulę. Antra vertus, laike vidurkintos muaro interferencinės juostos nesiformuos arba bus nevisiškai išreikštos, jei harmoninių svyravimų amplitudė nesutaps su atitinkama nulinės eilės pirmojo tipo Beselio funkcijos šaknimi, kaip matome 3.15(b) paveiksle. 3.15(c) paveiksle matome visame stebėjimo lange susiformavusias laike vidurkinto muaro interferencines juostas. Šiuo atveju visa zona vizualiai yra pilka, ir pilkio lygio reikšmė yra lygi $\frac{1}{2}$.

Panagrinėkime šį kodavimo metodą, remdamiesi konkrečiu pavyzdžiu. Sakykime, reikia užkoduoti raides *ABCD* į apskritiminę muaro gardelę (3.16(a) paveikslas). Tam, kad iš statinio užkoduoto vaizdo negalėtume atpažinti slaptos informacijos, taikomas atsitiktinės fazės postūmio algoritmas. 3.16 (b) paveiksle parodytas užkoduotas vaizdas, pritaikius šį algoritmą. 3.16 (c) paveiksle parodytas dekoduotas laike vidurkintas vaizdas, kai interferencinės juostos yra susiformavusios fone.



a) b) c)

3.16 pav. Slapto vaizdo užkodavimas ir dekodavimas, kai muaro gardelė yra apskritiminė: (a) slaptas vaizdas; (b) užkoduotas slaptas vaizdas, slapto vaizdo muaro gardelės periodas $\lambda_s = 0{,}1$, fono $\lambda_b = 0{,}18$; (c) vizualiai dekoduotas laike vidurkintas slaptas vaizdas

3.4. Šifruotų vaizdų dekodavimo eksperimentinis stendas apskritiminės muaro gardelės atveju[9]

Šifruotų vaizdų, išspausdintų ant popieriaus lapų, dekodavimas atliekamas su stendu, kurio bendras vaizdas pateiktas iliustracijoje (3.17 paveikslas). Eksperimentinio stendo schemoje (3.18 paveikslas) yra pavaizduotos visos jo sudedamosios dalys, tai: žemųjų dažnių generatorius 1 (nuo 2 Hz iki 40 kHz diapazonas), elektromagnetinis vibratorius 2, veleno su disku mechanizmas 3 ir skaitmeninis fotoaparatas 4. Dažnių generatoriuje generuojamo signalo amplitudė yra reguliuojama rankiniu būdu su rankenėle 1a, o signalo dažnis reguliuojamas irgi rankiniu būdu su rankenėle 1b. Išvesties signalo forma yra nekintanti, sinusoidės formos. Dažnių generatorius kabeliu 1c sujungtas su elektromagnetiniu vibratoriumi 2. Šis pritvirtintas keturiais varžtais 2b prie metalinio standaus karkaso 2a. Prie šio karkaso keturiais varžtais 3f pritvirtintas veleno su disku mechanizmas 3. Jis šarnyrais 3r, 3t ir strypu 3s sujungtas su vibratoriaus 2 šerdimi.

Eksperimentas su užkoduoto vaizdo rekonstrukcija atliekamas tokia tvarka. Su lazeriniu spausdintuvu išspausdinamas vienspalvis dekoduojamas vaizdas ant lipnaus arba paprasto popieriaus. Dekoduojamo vaizdo sukimo ašies taškas yra pažymėtas išspausdintame vaizde 1 mm × 1 mm dydžio baltu kvadrato plotu. Toks atspaudas apkerpamas iki tokio dydžio, kad tilptų ant 220 mm skersmens disko 3d. Šiame disko 3d centre išgręžta 0,1 mm skersmens kiaurymė. Plona adata perveriamas atspaudas 3u per jame pažymėtą centrą, ir adatos smaigalys įkišamas į disko 3d centre esančią kiaurymę taip sutapatinant vaizdo sukimosi ašį su disko 3d, pritvirtinto prie veleno 3a, sukimosi ašimi. Popieriaus lapas 3u pritvirtinamas prie disko 3d lipniąja puse taip, kad nesusidarytų raukšlės ir oro burbuliukai, o vaizdo pasukimo nuo atskaitos linijos $3u_0$ galas sutaptų su rodyklės 3e smaile.

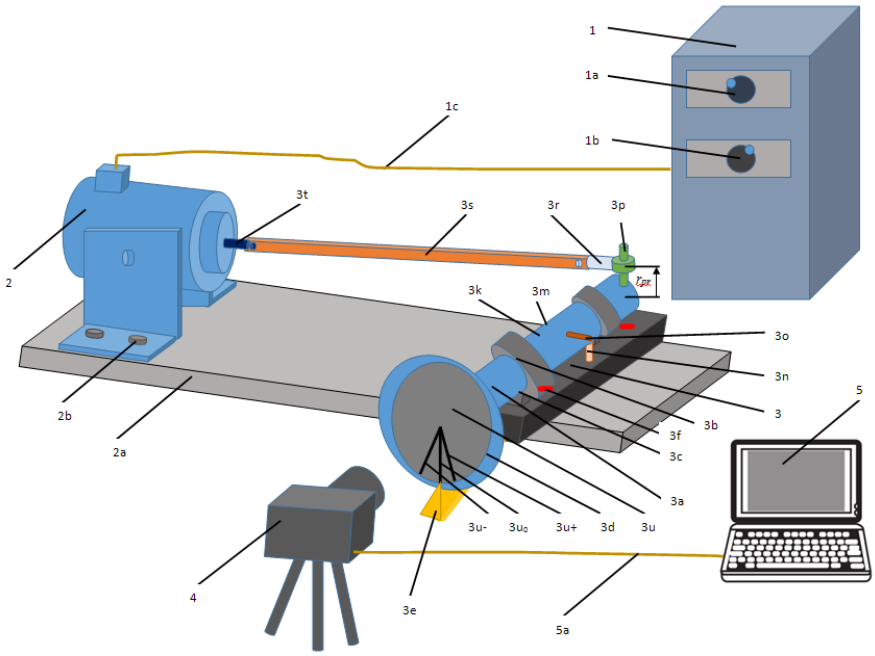
[9] *Šiame skyriuje pristatomi rezultatai buvo publikuoti straipsnyje*:
Experimental approach for optical registration of circular time-averaged moiré images
Lu G.; Maskeliūnas R.; Aleksienė S; Peng W.

3.17 pav. Šifruotų vaizdų dekodavimo eksperimentinis stendas

Centruojanti adata ištraukiama iš popieriaus lapo 3u ir veleno 3a centro. Velenas 3a su prie jo gale pritvirtintu disku 3d yra įtvirtintas dviejuose guoliuose 3b, kurie yra įmontuoti į šio mechanizmo metalinį korpusą 3c, o šitas keturiais varžtais 3f standžiai pritvirtintas prie metalinio karkaso 2a. Veleno 3a su prie jo pritvirtintu disku 3d sukimosi kampai pagal ir prieš laikrodžio rodyklę yra reguliuojami dviem atraminiais varžtais statramsčiais 3k ir 3n, įsuktais į šio mechanizmo korpusą 3c. Į šiuos statramsčius 3k, 3n atsiremia į vieną arba kitą pusę sukamas velenas 3a į jį įsuktais 3m ir 3o varžtais. Tikslus pasukimo kampas sureguliuojamas taip, kad veleną 3a pasukus apie savo ašį prie jo pritvirtintame diske 3d esančios ant popieriaus lapo 3u atspausdintos linijos „3u+“ ir „3u-„ sutaptų su 3e rodyklės smaile, o neutralioje padėtyje su šia smaile sutaptų ir linija „$3u_0$“.

Mechanizmo 3 veleno 3a galas per jame įsuktą varžtą su veržle 3p sujungtas su vibratoriumi 2 per du šarnyrus 3r ir 3t bei 3s strypą taip, kad vibratoriaus elektromagnetinės šerdies ašinė linija sutaptų su šarnyrų 3r, 3t ir strypo 3s ašine linija, kuri sudarytų statųjį kampą su šarnyrą 3r fiksuojančio varžto 3p ašine linija, o ši statmena veleno 3a ašinei linijai. Toks vibratoriaus 2 ir mechanizmo 3 sujungimas užtikrina disko 3d, įtvirtinto ant veleno 3a, pasukimo apie savo ašį į abi puses simetriškumą. Tokio sujungimo metodu vibratoriaus 2 elektromagnetinės šerdies linijinis poslinkis paverčiamas sukamuoju veleno 3a judesiu, kurio pasisukimo kampą galima padidinti arba sumažinti mechaniškai keičiant šarnyro 3r pritvirtinimo vietą ant varžto 3p taip, kad jeigu bus mažinamas spindulys r_{pr}, veleno 3a pasisukimo kampas didės, o didinant r_{pr} veleno 3a pasisukimo kampas mažės esant tiems patiems vibratoriaus 2 elektromagnetinės šerdies linijiniams poslinkiams.

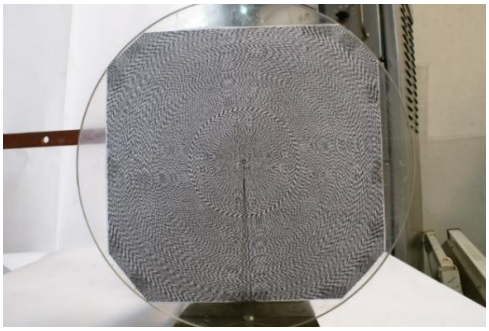
Prieš diską 3d, ant kurio jau yra pritvirtintas užšifruotas ir ant popieriaus išspausdintas vaizdas, 0,3 m atstumu ant trikojo laikiklio pritvirtinamas skaitmeninis fotoaparatas 4 su 12,0 mln. pikselių vaizdo matrica taip, kad jo optinė ašis sutaptų su veleno 3a ašine linija. Fotoaparate 4 nustatomas ryškumas ir kadro dydis bei ekspozicijos laikas, nurodytu atveju tai buvo 1 s. Sureguliuojamas fotografuojamo vaizdo apšvietimas taip, kad nesusidarytų šešėliai ir atspindžiai.



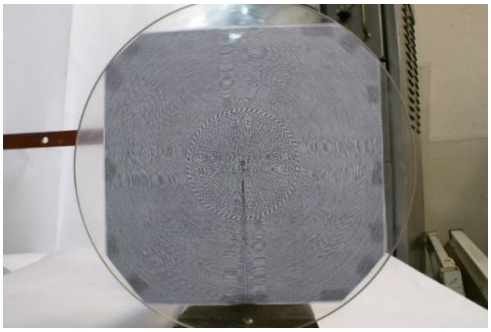
3.18 pav. Šifruotų vaizdų dekodavimo eksperimentinio stendo schema

Po šių paruošiamųjų darbų įjungiamas signalų generatorius 1 ir signalo dažnio reguliatoriumi 1b nustatomas dažnis 15–30 Hz ribose; šio eksperimento atveju buvo pasirinktas 20 Hz dažnis. Signalo, paduodamo į vibratorių 2 kabeliu 1c, amplitudės reguliatoriumi 1a nustatoma tokia amplitudė, kad vibratoriaus 2 elektromagnetinės šerdies linijinis poslinkis per šarnyrus 3r ir 3t bei 3s strypą suteiktų velenui 3a sukamuosius svyravimus atitinkančius 2° kampo amplitudę, nes tokio dydžio kampas yra panaudotas vaizdo užkodavimo algoritme. Didesniu kampu velenas 3a fiziškai nebegalės pasisukti dar ir todėl, kad jo pasisukimo kampą riboja kairės ir dešinės pusės statramsčiai 3k ir 3n, nes į juos atsirems į veleną 3a įsukti varžtai 3m, 3o ir jo pasisukimo kampą ribojantys varžtai. Tinkamai sureguliavus amplitudę neturi būti girdimi ir jaučiami varžtų 3m ir 3o smūgiai į statramsčius 3k ir 3n. Tokiomis sąlygomis atliekant eksperimentą plika akimi galima pamatyti užšifruotą vaizdą. Fotoaparatu 4 fotografuojami vaizdai rankiniu būdu keičiant generatoriaus 1 signalo amplitudę nedidelėse ribose, siekiant gauti kokybiškesnius rekonstruojamus vaizdus. Iš fotoaparato 4 vaizdai perkeliami į kompiuterį 5.

Eksperimento metu gauti vaizdai pateikiami 3.19 paveiksle.



(a)



(b)

3.19 pav. (a) Statinis užkoduotas vaizdas, susidedantis iš apskritiminių muaro gardelių; (b) laike vidurkintas vaizdas, kai vaizdas virpinamas pagal kampinius svyravimus

3.5. Trečiojo skyriaus išvados

1. Pasiūlyta vaizdo kodavimo schema pagrįsta elipsiniais svyravimais. Vaizdui užkoduoti naudojama dvimatė kryžminė gardelė. Slaptas vaizdas išryškėja per laike vidurkintas interferencines juostas, kai užkoduotas vaizdas virpinamas elipsiniu dėsniu.
2. Esminis skirtumas tarp vaizdo slėpimo schemos, pagrįstos vienkrypčiais svyravimais ir elipsiniais svyravimais, yra slaptos informacijos įterpime. Vienmatės eilutės (stulpeliai) gali būti atsitiktinai sumaišytos vaizdo slėpimo schemose, pagrįstose vienkrypčiais svyravimais. Tačiau toks atsitiktinis fazių sumaišymas negali būti taikomas elipsiniams svyravimams. Todėl pasiūlyta nauja vaizdo slėpimo technika, užtikrinanti efektyvų optinį slaptos informacijos dekodavimą.
3. Pasiūlyta vaizdo kodavimo schema, leidžianti optiškai registruoti kampinių svyravimų amplitudes. Ši schema pagrįsta laike vidurkintų interferencinių juostų formavimusi kampinėse muaro gardelėse.
4. Sukurti eksperimentiniai stendai ir atlikti realūs eksperimentai dvimatės kryžminės gardelės bei apskritiminės gardelės atveju.

BENDROSIOS IŠVADOS

1. Sukurta dinaminės vizualiosios kriptografijos schema deformuojamosiose muaro gardelėse. Ši schema leidžia įgyvendinti juodai baltų vaizdų vizualinio slėpimo schemą baigtiniais elementais aprašomų deformuojamųjų kūnų paviršiuose. Tai, savo ruožtu, atveria galimybes taikyti šias schemas mikro–opto–elektromechaninių sistemų optinei kontrolei.
2. Sukurta dinaminės vizualiosios kriptografijos schema chaotiškai svyruojančiose deformuojamosiose muaro gardelėse. Tai leidžia pritaikyti šias schemas netiesinių sistemų optinei kontrolei.
3. Sukurtos dvi dinaminės vizualiosios kriptografijos schemos dvimatėse muaro gardelėse (elipsiniams svyravimams ir apskritiminei muaro gardelei). Tai leidžia pastebimai praplėsti dinaminės vizualiosios kriptografijos taikymo ribas sudėtingoms inžinerinėms sistemoms. Sukurti optiniai stendai suformuotų schemų eksperimentiniam validavimui.

LITERATŪRA

1. Laurutis, V., G. Daunys, and R. Zemblys, *Quantitative analysis of catch-up saccades executed during two-dimensional smooth pursuit.* Elektronika ir Elektrotechnika, 2010. **98**(2): p. 83-86.
2. Palevicius, P. and M. Ragulskis, *Image communication scheme based on dynamic visual cryptography and computer generated holography*. Optics Communications, 2015. **335**: p. 161-167.
3. Sharpe, W.N., *Springer handbook of experimental solid mechanics*. 2008: Springer Science & Business Media.
4. Patorski, K., *Handbook of the moiré fringe technique*. 1993: Elsevier Sci. Publ.
5. Atluri, S. and A. Kobayashi, *Handbook on experimental mechanics*. 1993, Prentice-Hall.
6. Post, D., B. Han, and P. Ifju, *High sensitivity moiré: experimental analysis for mechanics and materials*. 2012: Springer Science & Business Media.
7. Dai, F. and Z. Wang, *Geometric micron-moiré.* OPTICS and Lasers in Engineering, 1999. **31**(3): p. 191-198.
8. Design, H.o.G. *Moiré*. 2017 [cited 2018; Available from: http://www.historygraphicdesign.com/the-age-of-information/postmodern-design/525-moire.
9. Gary, C., *Optical methods in experimental mechanics Part 18: Geometric Moire Phenomena and Simulations.* Experimental Techniques, 2005. **29**(4): p. 15-18.
10. Palivonaite, R., et al., *Image hiding in time-averaged deformable moiré gratings.* Journal of Optics, 2014. **16**(2): p. 025401.
11. Lebanon, G. and A.M. Bruckstein, *Variational approach to moiré pattern synthesis.* JOSA A, 2001. **18**(6): p. 1371-1382.
12. Li, F.-C. and A. Kishen, *Deciphering dentin tissue biomechanics using digital moiré interferometry: A narrative review.* Optics and Lasers in Engineering, 2018. **107**: p. 273-280.
13. Lim, H., et al., *Residual microstrain in root dentin after canal instrumentation measured with digital moiré interferometry.* Journal of endodontics, 2016. **42**(9): p. 1397-1402.
14. Rasouli, S., Y. Rajabi, and H. Sarabi, *Microlenses focal length measurement using Z-scan and parallel moiré deflectometry.* Optics and Lasers in Engineering, 2013. **51**(12): p. 1321-1326.
15. Meidanshahi, F.S., K. Madanipour, and B. Shokri, *Measurement of temperature and electrons density distribution of atmospheric arc plasma by moiré deflectometry technique.* Optics and Lasers in Engineering, 2013. **51**(4): p. 382-387.
16. Trivedi, S., J. Dhanotia, and S. Prakash, *Measurement of focal length using phase shifted moiré deflectometry.* Optics and Lasers in Engineering, 2013. **51**(6): p. 776-782.
17. Juste, G.L. and E.M. Benavides, *Moiré-Fourier deflectometry for local heat transfer measurement over a backward-facing step.* International Journal of Thermal Sciences, 2014. **77**: p. 244-251.

18. Kuroki, H., et al., *School scoliosis screening by Moiré topography–Overview for 33 years in Miyazaki Japan.* Journal of Orthopaedic Science, 2018.
19. Wang, J., et al., *Volume moiré tomography based on projection extraction by spatial phase shifting of double crossed gratings.* Optics Communications, 2018. **407**: p. 311-320.
20. Buytaert, J.A. and J.J. Dirckx, *Phase-shifting Moiré topography using optical demodulation on liquid crystal matrices.* Optics and Lasers in Engineering, 2010. **48**(2): p. 172-181.
21. Jiang, N. and L. Wang, *A novel strategy for quantum image steganography based on moire pattern.* International Journal of Theoretical Physics, 2015. **54**(3): p. 1021-1032.
22. Hu, J., et al., *Design and fabrication of ultrathin lighting responsive security device based on moiré imaging phenomenon.* Optics Communications, 2018. **424**: p. 80-85.
23. Korkh, Y.V., et al., *Moiré pattern of artificial opal crystals investigated by acoustic scanning microscopy.* Applied Acoustics, 2018. **130**: p. 149-155.
24. Su, D. and Y. Zhu, *Scanning moiré fringe imaging by scanning transmission electron microscopy.* Ultramicroscopy, 2010. **110**(3): p. 229-233.
25. Brzezicki, M. *Designer's controlled and randomly generated moiré patterns in architecture*. in *Proceedings of Generative Art*. 2011.
26. Zhuang, Z., et al., *Moiré-reduction method for slanted-lenticular-based quasi-three-dimensional displays.* Optics Communications, 2016. **381**: p. 314-322.
27. Tang, Y., et al., *Beyond the partial light intensity imager: Eliminating Moiré patterns.* Optics Communications, 2015. **355**: p. 143-147.
28. Kong, L., G. Jin, and T. Wang, *Analysis of Moiré minimization in autostereoscopic parallax displays.* Optics express, 2013. **21**(22): p. 26068-26079.
29. Kobayashi, A.S., *Handbook of Experimental Mechanics*. 1998: Wiley-VCH Verlag GmbH. 1072.
30. Pofelski, A., et al., *2D strain mapping using scanning transmission electron microscopy Moiré interferometry and geometrical phase analysis.* Ultramicroscopy, 2017.
31. Tang, Y., et al., *Calibration of an arbitrarily arranged projection moiré system for 3D shape measurement.* Optics and Lasers in Engineering, 2017.
32. Abolhassani, M., *Formulation of moiré fringes based on spatial averaging.* Optik-International Journal for Light and Electron Optics, 2011. **122**(6): p. 510-513.
33. Zhao, Y. and X. Zhang, *Determination of the deformations in polymeric nanostructures using geometric moiré techniques for biological applications.* Sensors and Actuators B: Chemical, 2006. **117**(2): p. 376-383.
34. Liu, J., et al., *Lateral force modulation by moiré superlattice structure: Surfing on periodically undulated graphene sheets.* Carbon, 2017. **125**: p. 76-83.
35. Pochet, P., et al., *Toward Moiré engineering in 2D materials via dislocation theory.* Applied Materials Today, 2017. **9**: p. 240-250.

36. Alcover, P.M., *Moiré interferences in the map of orbits of the Mandelbrot Set.* Communications in Nonlinear Science and Numerical Simulation, 2017. **42**: p. 545-559.
37. Yan, G., et al., *Fabrication of micro-scale gratings for moiré method with a femtosecond laser.* Theoretical and Applied Mechanics Letters, 2016. **6**(4): p. 171-175.
38. Zhang, X., M. Chang, and Y. Hou, *A two crossed Ronchi-gratings quantitative model of Moiré fringe patterns.* Optics Communications, 2015. **344**: p. 27-32.
39. Lang, F., et al., *A novel raster-scanning method to fabricate ultra-fine cross-gratings for the generation of electron beam moiré fringe patterns.* Optics and Lasers in Engineering, 2016. **86**: p. 281-290.
40. Zhou, M., H. Xie, and L. Wu, *Virtual fields method coupled with moiré interferometry: Special considerations and application.* Optics and Lasers in Engineering, 2016. **87**: p. 214-222.
41. Liu, Z., X. Lou, and J. Gao, *Deformation analysis of MEMS structures by modified digital moiré methods.* Optics and Lasers in Engineering, 2010. **48**(11): p. 1067-1075.
42. Hsu, J.-S., et al., *Measuring glass transition temperatures of polymers by using phase-stepping shadow moiré.* Polymer Testing, 2017. **57**: p. 58-66.
43. Zhu, J., et al., *Influence of tilt moiré fringe on alignment accuracy in proximity lithography.* Optics and Lasers in Engineering, 2013. **51**(4): p. 371-381.
44. Lay, Y.-L., et al., *3D face recognition by shadow moiré.* Optics & Laser Technology, 2012. **44**(1): p. 148-152.
45. Wu, D., et al., *A new method for the characterization of micro-/nano-periodic structures based on microscopic Moiré fringes.* Ultramicroscopy, 2014. **136**: p. 1-6.
46. Chiang, W.-C., et al., *The cluster assessment of facial attractiveness using fuzzy neural network classifier based on 3D Moiré features.* Pattern Recognition, 2014. **47**(3): p. 1249-1260.
47. Li, K., et al., *Global control of colored moiré pattern in layered optical structures.* Optics Communications, 2018. **414**: p. 154-159.
48. Creath, K. and J. Wyant, *Moiré and fringe projection techniques.* Optical shop testing, 1992. **2**: p. 653-685.
49. Wallis, T.S. and D.H. Arnold, *Motion-induced blindness is not tuned to retinal speed.* Journal of Vision, 2008. **8**(2): p. 11-11.
50. Wallis, T.S. and D.H. Arnold, *Motion-induced blindness and motion streak suppression.* Current Biology, 2009. **19**(4): p. 325-329.
51. Foley, J.M. and M.E. McCourt, *Visual grating induction.* JOSA A, 1985. **2**(7): p. 1220-1230.
52. Blakeslee, B. and M.E. McCourt, *Nearly instantaneous brightness induction.* Journal of Vision, 2008. **8**(2): p. 15-15.
53. Blakeslee, B. and M.E. McCourt, *A multiscale spatial filtering account of brightness phenomena*, in *Levels of perception*. 2003, Springer. p. 47-72.
54. Hansen, T., et al., *Memory modulates color appearance.* Nature neuroscience, 2006. **9**(11): p. 1367.

55. Hamburger, K., T. Hansen, and K.R. Gegenfurtner, *Geometric-optical illusions at isoluminance.* Vision research, 2007. **47**(26): p. 3276-3285.
56. Mikellidou, K. and P. Thompson, *The vertical-horizontal illusion: assessing the contributions of anisotropy, abutting, and crossing to the misperception of simple line stimuli.* Journal of vision, 2013. **13**(8): p. 7-7.
57. Troje, N.F. and M. McAdam, *The viewing-from-above bias and the silhouette illusion.* i-Perception, 2010. **1**(3): p. 143-148.
58. Naor, M. and A. Shamir. *Visual cryptography*. in *Workshop on the Theory and Application of of Cryptographic Techniques*. 1994. Springer.
59. Yan, X., et al., *Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality*. Digital Signal Processing, 2015. **38**: p. 53-65.
60. Li, P., et al., *Sharing more information in gray visual cryptography scheme.* Journal of Visual Communication and Image Representation, 2013. **24**(8): p. 1380-1393.
61. Geetha, P., V. Jayanthi, and A. Jayanthi, *Optimal visual cryptographic scheme with multiple share creation for multimedia applications.* Computers & Security, 2018. **78**: p. 301-320.
62. Hajiabolhassan, H. and A. Cheraghi, *Bounds for visual cryptography schemes.* Discrete Applied Mathematics, 2010. **158**(6): p. 659-665.
63. Lee, C.-C., et al., *A new visual cryptography with multi-level encoding.* Journal of Visual Languages & Computing, 2014. **25**(3): p. 243-250.
64. Hua, H., et al., *Visual Cryptography Based Multilevel Protection Scheme for Visualization of Network Security Situation.* Procedia computer science, 2018. **131**: p. 204-212.
65. Shemin, P. and K. Vipinkumar, *E–payment system using visual and quantum cryptography.* Procedia Technology, 2016. **24**: p. 1623-1628.
66. Lin, P.-Y., et al., *Prevention of cheating in visual cryptography by using coherent patterns.* Information Sciences, 2015. **301**: p. 61-74.
67. Luo, H., et al., *Color transfer in visual cryptography.* Measurement, 2014. **51**: p. 81-90.
68. Tharayil, J.J., E.K. Kumar, and N.S. Alex, *Visual cryptography using hybrid halftoning.* Procedia engineering, 2012. **38**: p. 2117-2123.
69. Yang, C.-N., et al., *Color transfer visual cryptography with perfect security.* Measurement, 2017. **95**: p. 480-493.
70. Dhiman, K. and S.S. Kasana, *Extended visual cryptography techniques for true color images.* Computers & Electrical Engineering, 2018. **70**: p. 647-658.
71. Liang, C., et al., *Time-averaged moiré method for in-plane vibrational analysis.* Journal of Sound and Vibration, 1979. **62**(2): p. 267-275.
72. Ragulskis, M. and A. Aleksa, *Image hiding based on time-averaging moiré.* Optics Communications, 2009. **282**(14): p. 2752-2759.
73. Lin, C. and F. Chiang, *Time-average in-plane moiré method for the analysis of nonsinusoidal cyclic loading.* Experimental Mechanics, 1982. **22**(2): p. 64-68.
74. Petrauskiene, V., et al., *Dynamic visual cryptography for optical control of vibration generation equipment.* Optics and Lasers in Engineering, 2012. **50**(6): p. 869-876.

75. Ragulskis, M., et al., *Investigation of dynamic displacements of lithographic press rubber roller by time average geometric moiré.* Optics and Lasers in Engineering, 2005. **43**(9): p. 951-962.
76. Vaidelys, M., et al., *Image hiding in time-averaged moiré gratings on finite element grids.* Applied Mathematical Modelling, 2015. **39**(19): p. 5783-5790.
77. Ragulskis, M., R. Maskeliunas, and L. Saunoriene, *Identification of in-plane vibrations using time average stochastic moiré.* Experimental Techniques, 2005. **29**(6): p. 41-45.
78. Ragulskis, M. and L. Saunoriene, *Applicability of Optical Geometric Differentiation for Time-average Geometric Moiré.* Strain, 2006. **42**(3): p. 173-179.
79. Ragulskis, M., *Time-averaged patterns produced by stochastic moiré gratings.* Computers & Graphics, 2009. **33**(2): p. 147-150.
80. Saunoriene, L., S. Aleksiene, and J. Ragulskiene, *Near-optimal pitch of a moiré grating for image hiding applications in dynamic visual cryptography.* Vibroeng. Procedia, 2017. **13**: p. 266-271.
81. Vaidelys, M., S. Aleksiene, and J. Ragulskiene, *1826. Dynamic visual cryptography scheme on the surface of a vibrating structure.* Journal of Vibroengineering, 2015. **17**(8).
82. Aleksiene, S., et al. *Dynamic visual cryptography on deformable finite element grids*. in *AIP Conference Proceedings*. 2017. AIP Publishing.
83. Lu, G., et al., *Optical image hiding based on chaotic vibration of deformable moiré grating.* Optics Communications, 2018. **410**: p. 457-467.
84. Ragulskis, M., L. Saunoriene, and R. Maskeliunas, *THE STRUCTURE OF MOIRÉ GRATING LINES AND ITS INFLUENCE TO TIME-AVERAGED FRINGES.* Experimental Techniques, 2009. **33**(2): p. 60-64.
85. Ragulskis, M., A. Aleksa, and R. Maskeliunas, *Contrast enhancement of time-averaged fringes based on moving average mapping functions.* Optics and Lasers in Engineering, 2009. **47**(7-8): p. 768-773.
86. Ragulskis, M., A. Aleksa, and Z. Navickas, *Image hiding based on time-averaged fringes produced by non-harmonic oscillations.* Journal of Optics A: Pure and Applied Optics, 2009. **11**(12): p. 125411.
87. Petrauskiene, V., et al., *Dynamic visual cryptography based on chaotic oscillations.* Communications in nonlinear science and numerical simulation, 2014. **19**(1): p. 112-120.
88. Petrauskiene, V., et al., *Dynamic visual cryptography for optical assessment of chaotic oscillations.* Optics & Laser Technology, 2014. **57**: p. 129-135.
89. Ragulskis, M. and Z. Navickas, *Time average geometric moiré—back to the basics.* Experimental Mechanics, 2009. **49**(4): p. 439-450.
90. Ragulskis, M., M.A. Sanjuan, and L. Saunoriene, *Applicability of time-average moiré techniques for chaotic oscillations.* Physical Review E, 2007. **76**(3): p. 036208.
91. Hilborn, R.C., *Chaos and nonlinear dynamics: an introduction for scientists and engineers*. 2000: Oxford University Press on Demand.
92. Rao, C.R., *The Concise Encyclopedia of Statistics Springer-Verlag 2008.*

93. Biltta P George, D.M.P., *Cheating Prevention Schemes for Visual Cryptography*..International Journal of Engineering Research & Technology, 2015. **4**(07): p. 324-328.
94. Saunorienė, L., et al., *Near-optimal pitch of a moiré grating in dynamic visual cryptography.* Journal of vibroengineering, 2018: p. 2504-2514.
95. Saunoriene, L., et al., *Image hiding scheme based on time-averaged elliptic oscillations.* Optics and Lasers in Engineering, 2017. **98**: p. 83-88.
96. Lu, G., et al., *Experimental approach for optical registration of circular time-averaged moiré images.* Journal of Vibroengineering, 2017. **14**.
97. Ragulskis, M., A. Aleksa, and J. Ragulskiene, *Image hiding based on circular moire fringes.* 2010: p. 90-99.
98. Palevicius, P., et al., *Circular geometric moiré for degradation prediction of mechanical components performing angular oscillations.* Mechanical Systems and Signal Processing, 2017. **86**: p. 278-285.

MOKSLINIŲ PUBLIKACIJŲ DARBO TEMA SĄRAŠAS

Mokslinės informacijos instituto duomenų bazės „ISI Web of Science“ leidiniuose, turinčiuose citavimo indeksą paskelbti straipsniai:

1. Lu, Guangqing; Saunorienė, Loreta; Aleksienė, Sandra; Ragulskis, Minvydas Kazys. Optical Image Hiding Based on Chaotic Vibration of Deformable Moiré Grating // Optics Communications. Amsterdam : Elsevier. ISSN 0030-4018. eISSN 1873-0310. 2018, Vol. 410, p. 457-467.
2. Saunorienė, Loreta; Aleksienė, Sandra; Maskeliūnas, Rimas; Ragulskis, Minvydas Kazys. Image hiding scheme based on time-averaged elliptic oscillations // Optics and Lasers in Engineering. Oxford : Elsevier. ISSN 0143-8166. eISSN 1873-0302. 2017, Vol. 98, p. 83-88.
3. Vaidelys, Martynas; Ragulskienė, Jūratė; Aleksienė, Sandra; Ragulskis, Minvydas Kazys. Image hiding in time-averaged moire gratings on finite element grids // Applied mathematical modelling. New York : Elsevier. ISSN 0307-904X. 2015, vol. 39, iss. 19, spec. iss. SI, p. 5783-5790
4. Vaidelys, Martynas; Aleksienė, Sandra; Ragulskienė, Jūratė. Dynamic visual cryptography scheme on the surface of a vibrating structure // Journal of vibroengineering. Kaunas : JVE International. ISSN 1392-8716. 2015, vol. 17, iss. 8, p. 4142-4152.

Kituose recenzuojamuose mokslo leidiniuose paskelbti straipsniai:

1. Saunoriene, Loreta; Petrauskiene, Vilma; Aleksiene, Sandra; Ragulskiene, Jurate. Near-optimal pitch of a moiré grating in dynamic visual cryptography // Journal of vibroengineering. Kaunas : JVE International. ISSN 1392-8716. eISSN 2538-8460. 2018, vol. 20, iss. 6, p. 2504-2514.

Konferencijų pranešimų medžiagoje:

1. Aleksienė, Sandra; Vaidelys, Martynas; Aleksa, Algiment; Ragulskis, Minvydas Kazys. Dynamic visual cryptography on deformable finite element grids // AIP Conference proceedings : International conference of numerical analysis and applied mathematics (ICNAAM 2016). Melville, NY : AIP Publishing. ISSN 0094-243X. 2017, vol. 1863, iss. 1, article 440002, p. 1-4.
2. Lu, Guangqing; Maskeliūnas, Rimas; Aleksienė, Sandra; Peng, Wenbin. Experimental approach for optical registration of circular time-averaged moiré images // Vibroengineering Procedia : [28th international conference on vibroengineering, Beijing, China, 19-21 October, 2017]. Kaunas : JVE International. ISSN 2345-0533. 2017, Vol. 14, p. 364-367.
3. Saunorienė, Loreta; Aleksienė, Sandra; Ragulskienė, Jūratė. Near-optimal pitch of a moiré grating for image hiding applications in dynamic visual cryptography // Vibroengineering Procedia : [27th international conference on vibroengineering, Katowice, Poland, 26-28 September, 2017]. Kaunas : JVE International. ISSN 2345-0533. 2017, Vol. 13, p. 266-271.

SL344. 2019-02-07, 11,5 leidyb. apsk. 1. Tiražas 14 egz. Užsakymas 49.
Išleido Kauno technologijos universitetas, K. Donelaičio g. 73, 44249 Kaunas
Spausdino leidyklos „Technologija“ spaustuvė, Studentų g. 54, 51424 Kaunas