KAUNO TECHNOLOGIJOS UNIVERSITETAS

VILMA PETRAUSKIENĖ

VIZUALINĖS KRIPTOGRAFIJOS SISTEMOS PAGRĮSTOS NETIESINIAIS VIRPESIAIS

Daktaro disertacija
Technologijos mokslai, mechanikos inžinerija (09T)

2015, Kaunas

Disertacija rengta 2010–2014 metais Kauno technologijos universitete, Matematikos ir gamtos mokslų fakultete, Matematinio modeliavimo katedroje, remiant Lietuvos valstybiniam mokslo ir studijų fondui ir Lietuvos mokslo tarybai.

Mokslinis vadovas:
Prof. habil. dr. **Minvydas Kazys Ragulskis** (Kauno technologijos universitetas, technologijos mokslai, mechanikos inžinerija – 09T).

TURINYS

Ženklų, simbolių ir santraukų sąrašas 5
ĮVADAS 7
1. LITERATŪROS APŽVALGA 10
1.1. Interferencinių juostų formavimosi optiniai efektai 10
1.2. Metodų pagrįstų muaro gardele taikymas 11
1.3. Muaro efektų kompiuterinė realizacija 12
1.4. Vizualinė kriptografija 13
1.5. Dinaminės vizualinės kriptografijos metodas 16
1.5.1. Laike vidurkinimo efektai harmoninėje muaro gardelėje 16
1.5.2. Laike vidurkinimo efektai stačiakampėje muaro gardelėje 22
1.6. Žmogaus regos sistemos tyrimai 25
1.7. Skyriaus išvados 25
2. BEVEIK OPTIMALI DINAMINĖS VIZUALINĖS KRIPTOGRAFIJOS LAIKO FUNKCIJA 27
2.1. Optimizavimo uždavinio konstravimas 29
2.2. Optimizavimo uždavinio sprendimas naudojant genetinius algoritmus 30
2.3. Slapto vaizdo kodavimo algoritmas 37
2.4. Skaitiniai eksperimentai 39
2.5. Skyriaus išvados 41
3. DINAMINĖS KRIPTOGRAFIJOS PANAUDOJIMAS VIBRUOJANČIOS ĮRANGOS KONTROLEI 42
3.1. Teorinis pagrindimas 42
3.2. Eksperimentinė įranga 44
3.3. Eksperimentinė realizacija 46
3.4. Metodo jautrumas 49
3.5. Neharmoniniai virpesiai 51
3.6. Metodo jautrumas fazės pokyčiams 54
3.7. Skyriaus išvados 55
4. DINAMINĖ VIZUALINĖ KRIPTOGRAFIJA PAGRĮSTA CHAOTINIAIS VIRPESIAIS 56
4.1. Optinis pagrindimas 56
4.2. Teoriniai sąryšiai 57
4.2.1. Chaotinių virpesių skaičiavimų pateikimas 58
4.2.2. Pasvarstymai apie pikselio dydį 59
4.2.3. Pasvarstymai apie standartinį nuokrypį σ 61
4.2.4. Realių chaotinių virpesių modeliavimas kompiuterio ekrane 62
4.3. Chaotinių virpesių panaudojimas dinaminėje kriptografijoje 63
4.3.1. Slapto vaizdo dekodavimas 63
4.3.2. Kompiuteriniai eksperimentai 64
4.4. Dinaminės kriptografijos panaudojimas optiniam chaotinių virpesių vertinimui 66
4.4.1. Eksperimentinė realizacija kompiuterio ekrane 69

4.4.2.Praktiniai eksperimentai 71
4.4.3.Eksperimento rezultatai 76
4.5.Skyriaus išvados 78
5.DINAMINĖS VIZUALINĖS KRIPTOGRAFIJOS TAIKYMAS ŽMOGAUS REGOS SISTEMOS TYRIMAMS 80
5.1.Problemos susijusios su ekrano atnaujinimo dažniu 80
5.2.Dinaminės vizualinės kriptografijos pagrindu funkcionuojančio žmogaus regos sistemos tyrimo maketo trumpas aprašymas 82
5.3.Eksperimentiniai žmogaus regos sistemos tyrimai 83
5.5.Skyriaus išvados 89
IŠVADOS 91
LITERATŪRA 92
MOKSLINIŲ PUBLIKACIJŲ DISERTACIJOS TEMA SĄRAŠAS 98
PRIEDAI 99

Ženklų, simbolių ir santraukų sąrašas

$F(x)$ – muaro gardelė
t – laiko momentai
T – ekspozicijos laikas
$\xi_s(t)$ – funkcija aprašanti dinaminį nuokrypį nuo pusiausvyros padėties
λ – muaro gardelės periodas
ω – harmoninių virpesių dažnis
φ – fazė
s – virpesių amplitudė
x – išilginė koordinatė
J_0 – pirmojo tipo nulinės eilės Beselio funkcija
r_i – i-toji pirmojo tipo nulinės eilės Beselio funkcijos šaknis
$E_m(s)$ – gaubiančioji funkcija
m – diskretinių kadrų skaičius viename virpesių periode
a_0, a_k, b_k – Furjė eilutės koeficientai
H_s – laike vidurkinimo operatorius
$\sigma(s)$ – laike vidurkintų interferencinių juostų standartinio nuokrypio funkcija
$E(H_s)$ – laike vidurkintos muaro gardelės vidurkis
$p_s(x)$ – tankio funkcija
$(\gamma_1, \gamma_2,...,\gamma_n)$ – svorių vektorius, γ_i – i-tojo stulpelio plotas
$P_s(\Omega)$ – funkcijos $p_s(x)$ Furjė transformacija
H – chromosomos suma
μ – mutacijos koeficientas
κ – kryžminimo koeficientas
N – populiacijos dydis
mean fit – tikslo funkcijos vidurkis
k – geriausio sprendinio pasikartojimų skaičius
$\delta_{x_0}(x)$ – impulsinė delta funkcija
h – impulsinės funkcijos tankio funkcijos parametras, nurodantis jos plotį
$u(t)$ – funkcija aprašanti harmoninį dėsnį
$z(t)$ – „zig-zag“ bangos formos funkcija
σ_c^2 – fazės triukšmą charakterizuojantis periodo kitimas
M – periodo numeris
τ_n – n-tojo periodo ilgis
τ_{avg} – visų periodų ilgių vidurkis
$\xi_\sigma(t)$ – Gauso normalusis ergodinis procesas
σ^2 – dispersija
ε – pikselio aukštis
$\theta(t)$ – diskretūs atsitiktiniai dydžiai
$h_\varepsilon(k)$ – diskrečios tikimybes nenukrypti nuo pusiausvyros padėties
$\widetilde{P}_\sigma(\omega)$ – diskrečioji tankio funkcijos $p_\sigma(x)$ Furjė transformacija

Φ – Laplaso funkcija
EX – vidurkis
SD^2 – dispersija
SD – standartinis nuokrypis
Me – mediana
M_0 – moda
Min – minimali reikšmė
Max – maksimali reikšmė
IP – imties plotis
H_0 – nulinė hipotezė
H_a – alternatyvioji hipotezė
$\chi^2_{imt.}$ – imties statistikos reikšmė
$\chi^2_{krit.}$ – kritinė imties statistikos reikšmė
n – imties tūris
α – reikšmingumo lygmuo
$t_{1-\frac{\alpha}{2};n-1}$, $t_{\frac{\alpha}{2};n-1}$ – Stjudento skirstinio kvantiliai
$\chi^2_{1-\frac{\alpha}{2},n-1}$, $\chi^2_{\frac{\alpha}{2},n-1}$ – Chi kvadrato skirstinio kvantiliai

ĮVADAS

Temos aktualumas

Vizualinės kriptografijos sistemos apima tokius kompleksinius klausimus kaip laike vidurkintų muaro interferencinių juostų susidarymas, blogai sąlygoti atvirkštiniai uždaviniai bei chaotinių atraktorių valdymas. Šia tema reikalingus atlikti tyrimus sąlyginai būtų galima sugrupuoti į muaro optikos, kriptografijos, chaotinių sistemų analizės, bei eksperimentinių tyrimų sritis. Visos šios tyrimų kryptys yra gana glaudžiai persipynusios tarpusavyje, jas visas vienija tyrinėjami procesai netiesinių virpesių kontekste.

Dinaminės vizualinės kriptografijos metodas ir jos algoritminis realizavimas pasiūlytas 2009 metais [1]. Specialūs kodavimo algoritmai naudojami įterpti slaptą vaizdą į stochastinę muaro gardelę, tačiau informacijos dekodavimui kompiuterio nereikia – slaptas vaizdas pasimato tuomet, kai užkoduotas vaizdas yra virpinamas pagal tam tikrą nustatytą dėsnį. Aktualu buvo tęsti pradėtus tyrimus dinaminės vizualinės kriptografijos srityje ir juos perkelti į eksperimentinį lygmenį. Darbai dinaminės vizualinės kriptografijos srityje tampriai susiję su laike vidurkintomis optinių metodų realizacijomis. Šios realizacijos išnaudojamos konstruojant eksperimentinius optinius muaro įrenginius dinaminei vizualinei kriptografijai realizuoti.

Aktualu buvo atlikti ne tik tokius tyrimus kurie pagrįsti fiziniu užkoduoto vaizdo virpinimu, naudojant vibrostendą su galimybe užtikrinti reikiamus virpesių parametrus, bet ir atlikti vaizdo dekodavimą kompiuterio ekrane. Tam įgyvendinti išspręstos svarbios teorinės problemos, išvesti teoriniai sąryšiai, aprašantys laike vidurkintų interferencinių juostų formavimąsi stochastinėse muaro gardelėse, kai užkoduoto vaizdo dinaminius atsilenkimus nuo pusiausvyros padėties aprašančios funkcijos yra laiptuotos, trūkios, o pati sistema baigtinius laiko intervalus praleidžia tik maksimalių atsilenkimų pozicijose. Taip pat įvertinti ir stochastinių muaro gardelių vizualizavimo ypatumai kompiuterio ekrane. Nagrinėjama tema atlikti darbai ženkliai praplečia pasiekimus netiesinių dinaminių sistemų ir virpesių teorijos bei taikymų srityje, bei sudaro sąlygas tolimesniems tyrimams dinaminės vizualinės kriptografijos srityje.

Tyrimų objektas – laike vidurkintų muaro metodų optinės eksperimentinės realizacijos, skirtos dinaminės vizualinės kriptografijos taikymams.

Darbo tikslas – sukurti ir eksperimentiškai realizuoti dinaminės vizualinės kriptografijos koncepciją pagrįstą netiesinių sistemų virpesiais.

Suformuluotam tikslui pasiekti darbe yra sprendžiami tokie uždaviniai:

1. Atlikti teorinius tyrimus, ieškant būdų dinaminės vizualinės kriptografijos saugumui padidinti panaudojant netiesinių sistemų virpesius.
2. Suformuluoti tikslo funkciją optimalios dekodavimo trajektorijos nustatymui, suformuluotam optimizavimo uždaviniui spręsti panaudoti genetinius algoritmus.
3. Sukonstruoti atitinkamas vibracijų generavimo ir valdymo bei optines priemones padidinto saugumo vizualinės kriptografijos eksperimentinei realizacijai.

4. Ištirti ir eksperimentiškai patikrinti galimybę dinaminės vizualinės kriptografijos efektus realizuoti panaudojant chaotinius virpesius.
5. Sukurti dinaminės vizualinės kriptografijos principu funkcionuojantį eksperimentinį įrenginį, skirtą žmogaus regos sistemos diagnostikai.

Tyrimo metodai programinės priemonės:

- Tyrimuose naudojama optinio muaro metodo teorija, ji praplečiama ir toliau vystoma.
- Dinaminės vizualinės kriptografijos, pagrįstos netiesiniais virpesiais, koncepcijos sukūrimui ir realizavimui naudojami informacijos vizualizavimo ir apdorojimo metodai, kurie yra pagrįsti matematine bei statistine analize, skaitmeninių vaizdų apdorojimo principais.
- Tyrimams atlikti naudojamos programinės priemonės parašytos Matlab R2009b terpėje, vaizdų analizavimui ir apdorojimui panaudotos Matlab sistemos įrankinės.
- Eksperimentinio kompiuterinio įrenginio sukūrimui panaudotos Adobe kompanijos programinės priemonės (Adobe Flach Profesional CS8).
- Gauti eksperimentų rezultatai apdorojami matematinės statistikos metodais pasinaudojant IBM SPSS Statistics programa.

Darbo mokslinis naujumas ir praktinė svarba:

- Surasta beveik optimali laiko funkcija ir patobulinti vaizdo kodavimo muaro gardelėje metodai leido padidinti dinaminės vizualinės kriptografijos saugumą.
- Vibruojančių sistemų patikimumui nustatyti pasiūlyta bekontaktė optinė tyrimo metodika, leidžiantis tiesiogiai, be papildomų priemonių nustatyti gedimus atsirandančius vibruojančiose konstrukcijose.
- Optiniam chaotinių virpesių intensyvumui vertinti pasiūlyta naudoti metodikas, pagrįstas dinaminės vizualinės kriptografijos efektais.
- Išvesti sąryšiai, susiejantys pikselio išmatavimus, judesio parametrus, ekrano fizines charakteristikas, laike vidurkinto vaizdo vizualinį interpretavimą, leido sukonstruoti naują žmogaus regos sistemos tyrimo įrenginį įgalinantį registruoti žmogaus regos sistemos gebėjimą interpretuoti laike vidurkintus vaizdus.

Gynimui pateikiama:

1. Rasta beveik optimali laiko funkcija, leidžianti padidinti dinaminės vizualinės kriptografijos saugumą.
2. Sukurtas vibrostendų patikimumo tyrimo metodas pagrįstas laike vidurkintomis muaro juostomis.
3. Dinaminės vizualinės kriptografijos metodai pritaikyti optiniam chaotinių virpesių vertinimui.
4. Sukonstruotas dinaminės vizualinės kriptografijos pagrindu funkcionuojantis žmogaus regos sistemos tyrimo įrenginys.

Darbo rezultatų aprobavimas:

Eksperimentai buvo atlikti Kauno technologijos universiteto Gynybos technologijų instituto laboratorijoje ir Lietuvos sveikatos mokslų universiteto ligoninės Akių ligų klinikoje. Rezultatai panaudoti atliekant Lietuvos mokslo fondo

projektą „Dinaminė vizualinė kriptografija žmogaus regos sistemos tyrimams“. Projekto laikotarpis – 2012–2014 m.

Pagrindiniai disertacijos darbo rezultatai paskelbti 4 publikacijose, 3 iš jų mokslinės informacijos instituto (ISI) pagrindinio sąrašo leidiniuose su citavimo indeksais, vienas paskelbtas tarptautinės duomenų bazės leidinyje. Disertacijoje nagrinėjama tematika buvo pristatyta 2 tarptautinėse ir 1 respublikinėje konferencijose. Parodoje-konkurse „KTU Technorama 2014“ pristatytas darbas „Dinaminės vizualinės kriptografijos taikymas žmogaus regos sistemos tyrimams“ buvo apdovanotas užėmus trečiąją vietą. Pagal kompanijos *Wolfram* kvietimą sukurtas demonstracinis projektas „*Stochastic Time-Averaged Moiré Fringes*“ ir patalpintas Wolfram Demonstrations Project bibliotekoje. Straipsnis „Dynamic visual cryptography for optical control of vibration generation equipment“ apžvelgtas Kanados internetinėje duomenų bazėje „Advances in Engineering“, pristatančioje paskutinius mokslo atradimus bei naujienas.

Darbo apimtis ir struktūra:

Daktaro disertaciją sudaro įvadas, 5 pagrindiniai skyriai, išvados, literatūros sąrašas ir autoriaus publikacijų sąrašas. Disertacijos apimtis yra 113 puslapių. Disertacijos pagrindinėje dalyje, apimančioje 85 puslapius yra 62 paveikslai, 6 lentelės, 88 šaltinių cituojamos literatūros sąrašas.

1. LITERATŪROS APŽVALGA

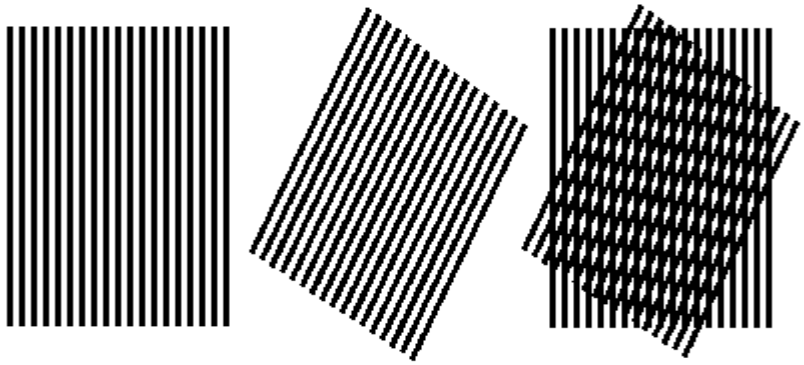
1.1. Interferencinių juostų formavimosi optiniai efektai

Atliekant optinius eksperimentus, tyrimams dažnai pasitelkiami įvairūs metodai pagrįsti interferencinių juostų formavimusi. Metodus pagal skirtingus požymius galima suskirstyti į atskiras grupes. Vienas iš skaidymo į grupes požymių gali būti priklausomybė nuo to, kaip tiriamas eksperimentinis laukas: ar analizė atliekama visam laukui, ar yra atliekama daug skirtingų taškinių matavimų. Taip pat tyrimo metodus galime suskirstyti priklausomai nuo interferencinio vaizdo gavimo principo. Muaro [2] ar fototamprumo [3] metoduose vaizdas yra gaunamas pasitelkus baltos šviesos šaltinius, o vidurkintoje laike lazerinėje holografijoje [4] – naudojama koherentinė spinduliuotė. Vieni metodai skirti tirti procesams vykstantiems kūnų paviršiuose, kiti – kūnų viduje. Matuojant vidinius įtempius galima taikyti fototamprumo metodą.

Šiame darbe bus nagrinėjami muaro eksperimentinės optikos analizės metodai. Šiems metodams reikalingas baltos šviesos šaltinis, yra tiriamas visas eksperimentinis kūnas, jie yra priskiriami prie neardančios kontrolės metodų. Pagrindinė šių metodų savybė yra kūno paviršiuje susiformuojančios interferencinės juostos. Dėl galimybės pastebėti paviršiaus deformacijas, muaro metodai plačiai taikomi įvairiose technologijų ir mokslo srityse. Šiame darbe nenagrinėjamos kūno paviršiaus deformacijos, o modeliuojami optiniai efektai, kurie yra taikomi kriptografijoje, bei informacijai koduoti.

Žodis muaras kildinamas iš prancūzų kalbos, ten taip yra vadinama tam tikru būdu austa šilkinė juostelė. Juostelėje šilkas supresuojamas dviem audinio sluoksniams. Audinio sluoksniams pasislinkus vienas kito atžvilgiu pastebimos interferencinės juostos. Natūraliai susiformavusias muaro juostas galime pastebėti ir kasdieniniame gyvenime žiūrint į reguliarios struktūros užuolaidų audinį ar lygiagrečių laidų tinklelį.

Skelbiama, kad lordas Rayleigh pirmasis susidomėjo muaro juostų reiškiniu. Nuo tada imta muaro juostas tyrinėti. Šiuo metu yra žinoma daug šio efekto panaudojimo galimybių. Nustatyta, kad stebint muaro juostų judėjimą, galima nustatyti dviejų gardelių santykinį poslinkį. Weller ir Shepherd [5] pirmieji pritaikė muarą kūno deformacijoms nustatyti. Tiksli muaro juostų teorija atsirado tik penkto dešimtmečio viduryje. Ligtenberg [6] bei Guid [7] muaro juostas pritaikė įtempimų tyrimuose. Taip pat muaras buvo pritaikytas topografijos matavimams [8, 9, 10]. Der Hovanesian ir Gasvik muarą pritaikė virpesių teorijoje [11, 12]. Eksperimentinėje optikoje žinomas geometrinio muaro metodas (1.1 pav.). Šio metodo esmė yra ta, kad tiriamojo kūno paviršiuje yra suformuojama periodinė gardelė, ji gali būti nupiešiama arba nubraižoma ant kūno paviršiaus [13, 14]. Taip pat gali būti suformuojama atominio mikroskopo mikrogembės pagalba [15]. Be geometrinio muaro yra žinomi projekcinio muaro, atspindžio muaro, šešėlinio muaro ir kiti metodai.



1.1 pav. Geometrinio muaro efekto pavyzdys

1.2. Metodų pagrįstų muaro gardele taikymas

Yra žinoma nemažai metodų, kurie pagrįsti muaro gardele. Norint gerai suprojektuoti ir valdyti mikro-elektromechaninių struktūrų sistemas reikia atlikti kiekybinę sistemų deformacijų analizę. Šioms deformacijoms nustatyti galima panaudoti Zhanwei L. pasiūlytus skaitmeninio muaro modelius. Aukštos mikrometrinės skyros deformacijoms nustatyti pritaikyti principai aprašyti [14]. Vienas jų Gauso dėsnio išplovimo algoritmas, atliekamas kartu su fazės postūmiu. Mikro-elektromechaninės sistemos paviršius, formuojant muaro gardelę yra subraižomas sufokusuotų jonų srautu. Ši suformuota gardelė yra pradinė muaro gardelė, kompiuterio pagalba yra formuojama dar viena – papildoma skaitmeninė muaro gardelė. Sudėjus šias dvi gardeles yra gaunamos muaro juostos. Tikslesnėms deformacijoms gauti papildomai yra panaudojamas Gauso dėsnio išplovimo algoritmas, fazės postūmis, pagaliau yra gaunama interferencinių juostų struktūra, iš kurios galime spręsti apie deformacijas.

Kodavimo požymių užmaskavimui holografmose, A. K. Aggarwal pritaikė muaro raštų formą, šiuo atveju dekodavimui naudojamas holografmos raktas [16].

Panaudojęs šešėlinio muaro metodą A. Del Taglia suformavo šviesias ir tamsias interferencines juostas, kurių pagalba galima nustatyti kūno gylį skaitmeniniame trimačiame televizijos kameros vaizde. Šią informaciją galima panaudoti erdvinio objekto formų nustatymui [17].

R. A. Braga nagrinėjo trimačių vaizdų generavimą panaudojant muaro metodus [18]. Ant nagrinėjamo objekto projektuojant muaro struktūrą, dėl nepakankamai gero apšviestumo, gaunamas vaizdas su pašaliniu šešėlio efektu. Jis trukdo nustatyti tikslias nagrinėjamo kūno formas. Norint išvengti šešėlio efekto, muaras projektuojamas skirtingiems projektavimo kampams. Sulyginus gautus vaizdus gaunamos kūno formos.

Muaro gardelę vaizdų kodavimui panaudojo Munoz-Rodriguez. Vaizdų kodavimas ir dekodavimas eksperimentiškai atliekamas virtualioje aplinkoje. Iš nedeformuotos muaro gardelės, ją papildant atspindžio vaizdo pilkio lygiu yra gaunama deformuota muaro gardelė. Dekoduojant sudėjus abi muaro gardeles matomas išblukęs slaptas vaizdas. Šis metodas aprašomas [19].

Nano skyros eilės interferencinių muaro gardelių sutapatinimo algoritmas paremtas interferencinėmis muaro juostomis yra pristatytas [20] darbe.

Muaro juostomis pagrįsti kūnų formos identifikacijos uždaviniai randa pritaikymą ir biomedicinoje [21]. Pavyzdžiui kai sprendžiame klausimą apie mentikaulio išnirimą arba tam tikrų raumenų grupių paralyžių. Projekcinio muaro pagrindu, interferencinių juostų formavimasis apie vidurkį gali padėti objektyviai nustatyti paralyžuotų raumenų zonas ar išnirusių kaulų deformacijų ypatybes. Tam muaro juostos projektoriumi projektuojamos ant mentikaulio, gautas vaizdas fotografuojamas, tai pat fotografuojamas ir vaizdas gautas pakėlus ranką. Gauti vaizdai analizuojami tam skirta programine įranga. Muaro juostų projektavimas leidžia atlikti neinvazinius skaitmeninius 3D mentikaulio matavimus. Šio metodo privalumas – jo paprastumas.

Laike vidurkintu optiniu interferenciniu būdu gautų vaizdų panaudojimas virpančių kūnų deformacijų analizei pristatytas [22] darbe. Jame analizuojama kaip laike vidurkintų interferencinių juostų vaizdas atspindėtas nuo veidrodinio paviršiaus moduliuojamas su harmoninės muaro gardelės vaizdu leidžia eksperimentiškai nustatyti virpančių kūnų charakteristikas.

Muaro interferencinius optinius metodus taip pat galima panaudoti ir trūkių laminatuose eksperimentinei detekcijai. Apie tai rašoma [23] darbe.

1.3. Muaro efektų kompiuterinė realizacija

Muaro efekto pagalba gauti vaizdai gali susiformuoti savaime arba gali būti sukuriami žmogaus. Šiuo atveju yra analizuojami patys gauti raštai, ieškomos įvairios charakteristikos, konstruojamos lygtys, kuriomis aprašomos muaro raštų struktūros, atliekama gauto muaro rašto analizė.

Dažnai reikia sukonstruoti tokias muaro struktūras, kurias sujungus būtų gaunamas norimas muaro raštas. Tai jau kita muaro raštų analizavimo sritis.

Muaro gardelių sudarymui ir jų sudėjimui gali būti panaudota vektorinės grafikos programinė įranga, pvz. CorelDrav paketas. Vienas tokių muaro gardelių formavimo pavyzdžių yra aprašytas [24] darbe. Čia gardelės deformavimui (ištempimui, posūkiui ir kt.) yra naudojamas standartinis funkcijų rinkinys, kuris leidžia greitai ir be papildomų priemonių formuoti norimas muaro gardeles.

Konstruojant muaro efektus naudojant programinius paketus gaunama vaizdi mokymo priemonė. Tačiau moksliniams tyrimams toks muaro struktūrų formavimas nėra geras, be to naudojant vektorinės grafikos programinę įrangą ne visada galima pavaizduoti sudėtingas muaro sistemas ar laike vidurkintus interferencinius raštus.

Tokiais atvejais geriau naudoti techninę programinę įrangą, tai galėtų būti Matlab, Mathcad ar kita įranga galinti pavaizduoti grafinius vaizdus. Taip konstruojant muaro raštus sudaromas skaitmeninis modelis. Toliau pateikti kompiuterinio modeliavimo pritaikymo pavyzdžiai.

Tolimojo lauko muaro interferencinių optinių metodų analizė paremta skaliarinių difrakcinių laukų teorija pateikta [25] darbe. Čia muaro metodo kompiuteriniam modeliavimui ir slaptai informacijai aprašyti yra naudojamas baigtinių elementų metodas.

Muaro interferencinių juostų panaudojimas kaip pristatymo įrankis, kompiuterinėmis priemonėmis atkurti kompozicinių medžiagų modeliavimo rezultatus, pateiktas [26] publikacijoje.

J. R. Berger muaro laukų nevienalytėse anizotropinėse medžiagose tyrimui panaudojo kraštinių elementų metodą [27].

J. F. Cárdenas-García [28] darbe pateikė optinį skylių įtempių tyrimo metodą pagrįstą skylių gręžimo būdu validuojamu optiniais muaro metodais ir kompiuteriniais baigtinių elementų metodo skaičiavimais.

1.4. Vizualinė kriptografija

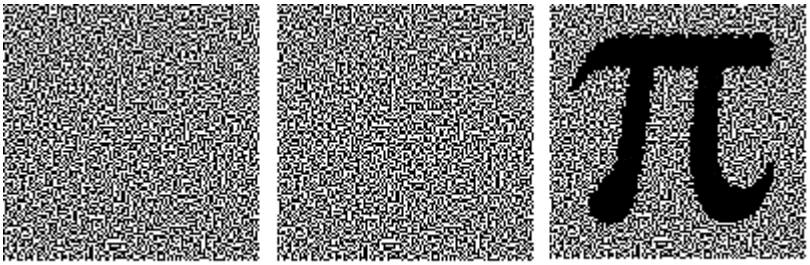
Vizualinė kriptografija, tai šifravimo metodas, kai vaizdinė informacija (nuotraukos, tekstas ir panašiai) užšifruojama taip, kad dekodavimas gali būti atliekamas žmogaus regos sistemos pagalba, net neturint kompiuterio.

Klasikinė vizualinė kriptografija pradėta plėtoti Moni Naor ir Adi Shamir 1994 metais [29]. Jų plėtota vizualinė kriptografija pagrįsta slapto vaizdo skaidymu į *n* sudaromųjų dalių taip, kad tik turint visas *n* dalių, gaunamas originalus slaptas vaizdas. Kiekviena dalis spausdinama atskirai ir yra skirtingo skaidrumo. Kai visos *n* dalys sudedamos, matomas originalus vaizdas.

Vaizdo kodavimas pagrįstas koduojamos informacijos skaidymu į mažesnes dalis. Dekoduoto vaizdo kontrasto išlaikymui kiekvienoje suskaidytoje dalyje turi būti toks pat juodų ir baltų pikselių kiekis. Paprasčiausia yra kiekvieną pikselį skaidyti į dvi dalis, kurios sudarytų dviejų pikselių bloką, bet šis metodas iškreips ne tik užkoduotą, bet ir dekoduotą vaizdą. Geriau pikselį skaidyti į 4 pikselių bloką, kaip 2 iš 2 metode. Taip susidarys 3 poros pikselių blokų būsenų, kurios naudojamos slapto vaizdo kodavimui dviejuose skaidrėse (1.2 pav.). Pikseliui esančiam pirmoje skaidrėje gali būti parenkama bet kuri atsitiktinė būsena, tačiau antroje skaidrėje pikselis turės tokią pačią arba tai porai priešingą būseną, priklausomai nuo to ar pikselyje slepiama slapta informacija bus išryškinta ar ne.

1.2 pav. Pikselio skaidymas į 4 pikselių bloką

Gautos skaidrės yra atspausdinamos ant skaidrios plėvelės. Jei nagrinėtume kiekvieną skaidrę atskirai (1.3A ir 1.3B paveikslai), tai matytumėme tik baltus ir juodus pikselius, koduoto vaizdo pamatyti nepavyktų. Norint pamatyti koduotą vaizdą reikia antrą skaidrę uždėti ant pirmos (1.3C pav.) [29].



1.3 pav. Sudėjus koduotos informacijos A ir B dalis išryškėja slapta informacija C

M. Naor ir A. Shamir [29] pasiūlė ir *k* iš *n* vizualinės kriptografijos metodą. Koduojant šiuo metodu vaizdas skaidomas į *n* dalių, o dekoduoti galima turint *k* dalių t.y. slapta informacija išryškės jei viena ant kitos sudėsime *k* skaidrių. Trūkstant nors vienos skaidrės matysime tik baltus ir juodus pikselius – slapta informacija neišryškės.

Nuo 1994 m. vizualinė kriptografija pažengė į priekį. Buvo pristatyta vizualinės kriptografijos schema naudojama spalvoto slapto vaizdo kodavimui ir vizualiniam dekodavimui [30, 31], šioje schemoje išvengiama spalvų užtamsėjimo efekto [32]. Tikimybinė *k* iš *n* vizualinės kriptografijos schema pilkiems ir spalvotiems paveikslams koduoti pristatyta [33] darbe. Dar viena slapto vaizdo kodavimo schema įgalinanti natūralių spalvotų vaizdų dekodavimą yra pristatyta [34]. Vizualinės kriptografijos metodas skirtingo pilkio lygio paveikslams yra aprašytas [35] darbe.

Atvirkštinės vizualinės kriptografijos idealaus kontrasto schema pristatyta [36]. Vizualinė kriptografija įgalinanti prie skirtingų parametrų reikšmių formuoti skirtingas slapto vaizdo komponentes aprašyta [37]; t.y. sudėjus dvi skaidres matysime vieną slapto vaizdo komponentę, pvz. raidę A, uždėjus trečią skaidrę matoma raidė A, bet atsiranda ir raidė B ir t.t.

Nauja efektyvi vizualinės kriptografijos saugumo schema panaudojant pikselio išplėtimą aptarta [38, 39]. Papildyta vizualinės kriptografijos schema *n* paveikslų kodavimui aprašyta [40], be to čia po to kai pradiniai vaizdai yra užkoduojami, jie išlieka reikšmingi, nes vartotojas paveikslą gali atpažinti pagal skaidrumą.

Vizualinė kodavimo schema kai keletas slaptų vaizdų yra koduojama į du apskritimus aprašoma [41]. Jei skaidrės nagrinėjamos atskirai, tai matome atsitiktinai išsidėsčiusius baltus ir juodus pikselių rinkinius. *N* slaptų vaizdų gaunama paėmus vieną koduotą paveikslą ant jo uždėjus kitą dalį ir ją pasukus *n* skirtingais kampais. Kelių slaptų paveikslų kodavimas atsitiktinėje apskritiminėje gardelėje pristatomas [42] straipsnyje.

Apibendrinta daugelio slaptų vaizdų vizualinės kriptografijos schema aprašyta [43, 44, 45, 46]. Dar vienas naujas pažangus metodas paveikslo kodavimui yra aprašomas [47].

C.N. Yang ir C.B. Ciou pristatė [48] du-viename slaptos informacijos kodavimo schemą, panaudojant vizualinės kriptografijos principus ir slapto vaizdo paskirstymo daugianarių pagrindu schemą. Daugelio slaptų vaizdų slėpimo schema

remiantis Bulio logikos operatoriumi pristatyta [49] straipsnyje, siūlomas metodas ne tik slepia slaptus vaizdus, tačiau taip pat padidina kelių slaptų vaizdų slėpimo galimybes.

Naujus algoritmus naudojančius atsitiktines gardeles pilkų ir spalvotų slaptų vaizdų kodavimui ir vizualiniam dekodavimui S. J. Shyu pristatė [50, 51].

Vizualinės kriptografijos schema su daugelio lygių kodavimo principais pristatyta [52] darbe. Šis kodavimo algoritmas pasižymi tuo, kad tiek slapto vaizdo tiek fono vietose sumažinamas pilkio lygių variabilumas ir padidinamas rekonstruoto vaizdo aiškumas.

Vizualinė kriptografija paremta atsitiktinių pikselių muaro gardelėmis, kuriose dar papildomai yra koduojami tam tikri vizualiniai požymiai yra aprašyta [53] darbe. Pasiekiamas aukštas dekoduojamo vaizdo ryškumas ir užtikrinamas reikalavimas, kad šita sistema būtų atspari bandymams „gudrauti“. Paėmus dvi skaidres ir jas sudėjus viena ant kitos gaunama slapta informacija, tačiau jei yra žinoma koks pikselių išsidėstymas pirmojoje skaidrėje kas nors gali bandyti padirbti (sugeneruoti) antrą skaidrę taip, kad jas sudėjus būtų matoma visai kita informacija, skirtinga tikrajai. Ši priemonė yra su papildomais optiniais žymekliais, reikalingais apgavysčių prevencijos sistemai.

K iš *k* išplėstinė vizualinės kriptografijos schemą T. Guo ir kiti pristatatė [54] darbe. Čia eliminuojamas pikselio išsiplėtimo efektas, pagerinama rekonstruojamo vaizdo kokybė. Panašūs rezultatai yra aprašyti ir [55] publikacijoje, čia slaptos informacijos pikselių blokas yra keičiamas tam tikru metodu užkoduotų pikselių bloku taip išsaugant koduoto ir dekoduojamo paveikslo originalų dydį.

Vizualinės kriptografijos taikymų galimybės aptartos [16] darbe. Aptarta pikselio išsiplėtimo, kontrasto praradimo problematikos ir įvertinamos apatinės kontrasto ribos. Taip pat aptariami įvairiausi pikselio kodavimo algoritmai.

Vizualinės kriptografijos schemos pagalba dekoduojamo slapto vaizdo kontrasto apibrėžimas yra pateikiamas [56] darbe. Yra žinoma, kad dekoduojamas slaptas vaizdas pasirodo pilko vaizdo nereguliarioje pikselių gardelėje. Kontrastas tarp slapto vaizdo informacijos vietos ir fono leidžia vizualiai interpretuoti užkoduotą vaizdą. To kontrasto apibrėžimas yra svarbus vertinant gaunamą dekoduojamo vaizdo kokybę.

Naudojantis šiuolaikinėmis technologijomis yra gana paprasta dalintis, kopijuoti ir platinti skaitmeninius duomenis (paveikslus, nuotraukas ir pan.). Tokiu būdu nesunkiai gali būti pažeistos autorinės teisės. Pasitelkus vizualinės kriptografijos metodus [57] straipsnyje pasiūlyta metodika, leidžianti skaitmeniniuose dokumentuose įdėti slaptus duomenis, kurie užtikrintų autorinių teisių apsaugą.

Straipsnyje [58] siūloma apsaugoti skaitmeninius vaizdus naudojantis skaitmeninių vandens ženklų technika, kuri lestų užtikrinti turinio vientisumą ir įrodytų nuosavybės teisę tuo atveju jei būtų panaudoti neteisėtai.

Asmens biometriniai bruožai yra saugomi duomenų bazėje. Taip saugoti duomenis nėra saugu: nekoduoti duomenys gali būti nesunkiai surasti ir pakeisti. Straipsnyje [59] pasiūlytas vizualine kriptografija pagrįstas metodas, kai saugomi duomenys yra užkoduojami. Tokiu būdu jie išlieka saugūs.

Vizualinės kriptografijos metodai taip yra siūlomi naudoti elektroninių asmens sveikatos įrašų saugumui užtikrinti. Straipsnyje [60] aptariama metodika kaip informaciniuose sveikatos tinkluose galima išlaikyti saugius įrašus apie pacientų sveikatą.

1.5. Dinaminės vizualinės kriptografijos metodas

Vizualinėje kriptografijoje informacijos kodavimui buvo panaudota muaro gardelė [61][62], o dekodavimas vykdomas geometrinės superpozicijos principu. Vėliau pasiūlyta gaminti du vaizdus, kurie gaunami panaudojus muaro gardelės sintezę, o šifruotas vaizdas išryškėja, kai šie vaizdai persipina [63]. Muaro gardelės sintezė ir analizė yra glaudžiai susijusios.

Atsiradus dinaminės vizualinės kriptografijos sąvokai, pasiūlytas metodas pagrįstas laike vidurkintomis muaro juostomis [1]. Šis metodas remiasi ne atskirų paveikslų superpozicijos principu, o laike vidurkintu geometriniu muaru vienam koduotam paveikslui Tai vieno vaizdo metodas, informacija nėra skaidoma į sudėtines dalis. Slapta informacija yra užkoduojama į stochastinę muaro gardelę statiniame vaizde. Ji gali būti vizualizuojama laike vidurkintų muaro interferencinių juostų pavidalu, jei tik užkoduotas vaizdas virpinamas pagal griežtai nustatytą kryptį ir amplitudę. Slapto vaizdo kodavimui naudojami sudėtingi skaitiniai algoritmai; dekodavimui kompiuterio nereikia. Šio metodo saugumo trūkumas yra tas, kad jei trečioji šalis žino kuria kryptimi reikia virpinti vaizdą, ji gali atlikinėti eksperimentus tol, kol pasirodys slapta informacija. Todėl buvo pasiūlytas metodas [1, [64], kuriuo sukonstruota muaro gardelė generuos laike vidurkintas muaro interferencines juostas ne tik virpinant patį vaizdą reikiama kryptimi ir amplitude, bet dar ir papildomai užtikrinant, kad laiko funkcija, pagal kurią virpinamas vaizdas, atitiktų specialius reikalavimus. Slaptą informaciją galima dekoduoti tik virpinant pagal nustatytą dėsnį.

1.5.1. Laike vidurkinimo efektai harmoninėje muaro gardelėje

Šiame skyrelyje nagrinėjamas laike vidurkintų muaro juostų formavimasis. Parenkama muaro gardelė, kuri aprašoma kaip harmoninė funkcija $F(x)=\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)$, o nuokrypio nuo pusiausvyros padėties laiko momentu t funkcija yra $\xi(t)=s\cdot\sin(\omega t+\varphi)$, čia λ – muaro gardelės periodas, ω – harmoninių virpesių dažnis, φ – fazė, s – harmoninių virpesių amplitudė, x – išilginė koordinatė. Laike vidurkinimo operatorių galima rasti taip [65][66]:

$$\begin{aligned}&\lim_{T\to\infty}\frac{1}{T}\int_0^T\left(\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}\left(x-s\sin\left(\omega t+\varphi\right)\right)\right)\right)dt=\\&=\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}(x-b)\right)\lim_{T\to\infty}\frac{1}{T}\int_0^T\cos\left(\frac{2\pi}{\lambda}s\sin\left(\omega t+\varphi\right)\right)dt+\\&+\frac{1}{2}\sin\left(\frac{2\pi}{\lambda}(x-b)\right)\lim_{T\to\infty}\frac{1}{T}\int_0^T\sin\left(\frac{2\pi}{\lambda}s\sin\left(\omega t+\varphi\right)\right)dt\end{aligned}\qquad(1.1)$$

Kadangi

$\int_0^T \sin\left(\frac{2\pi}{\lambda} s\sin(\omega t+\varphi)\right)dt = 0$, tai šį narį padauginus iš kompleksinio skaičiaus *i*, o $\sin\left(\frac{2\pi}{\lambda} x\right)$ pakeitus į $\cos\left(\frac{2\pi}{\lambda} x\right)$, lygybė išliks ir tada gaunama:

$$\begin{aligned}
&\lim_{T\to\infty}\frac{1}{T}\int_0^T\left(\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}\left(x-s\sin(\omega t+\varphi)\right)\right)\right)dt = \\
&=\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)\lim_{T\to\infty}\frac{1}{T}\int_0^T\cos\left(\frac{2\pi}{\lambda}s\sin(\omega t+\varphi)\right)dt+ \\
&+i\cdot\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)\lim_{T\to\infty}\frac{1}{T}\int_0^T\sin\left(\frac{2\pi}{\lambda}s\sin(\omega t+\varphi)\right)dt=\frac{1}{2}+ \\
&+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)\lim_{T\to\infty}\frac{1}{T}\int_0^T\left(\cos\left(\frac{2\pi}{\lambda}s\sin(\omega t+\varphi)\right)+i\cdot\sin\left(\frac{2\pi}{\lambda}s\sin(\omega t+\varphi)\right)\right)dt= \\
&=\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)\lim_{T\to\infty}\frac{1}{T}\int_0^T e^{\frac{2\pi}{\lambda}s\sin(\omega t+\varphi)}dt=\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)J_0\left(\frac{2\pi}{\lambda}s\right)
\end{aligned} \tag{1.2}$$

čia J_0 yra pirmojo tipo nulinės eilės Beselio funkcija [67]:

$$J_0(x)=\lim_{T\to\infty}\frac{1}{T}\int_0^T e^{\frac{2\pi}{\lambda}x\sin(\omega t+\varphi)}dt$$

Kitu atveju, jei muaro gardelė yra aprašoma tuo pačiu dėsniu $F(x)=\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)$, bet nuokrypio nuo pusiausvyros padėties laiko momentu *t* funkcija yra $\xi(t)=s\sin(\omega t+\varphi)+b$, čia λ – muaro gardelės periodas, ω – harmoninių virpesių dažnis, φ – fazė, ir *s* – harmoninių virpesių amplitudė, *b* – pastovus skaičius (konstanta), tai laike vidurkintas pilkio lygis bus:

$$\begin{aligned}
&\lim_{T\to\infty}\frac{1}{T}\int_0^T\left(\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}\left(x-s\sin(\omega t+\varphi)\right)-b\right)\right)dt= \\
&=\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)\lim_{T\to\infty}\frac{1}{T}\int_0^T\cos\left(\frac{2\pi}{\lambda}s\sin(\omega t+\varphi)\right)dt+ \\
&+\frac{1}{2}\sin\left(\frac{2\pi}{\lambda}x\right)\lim_{T\to\infty}\frac{1}{T}\int_0^T\sin\left(\frac{2\pi}{\lambda}s\sin(\omega t+\varphi)\right)dt
\end{aligned} \tag{1.3}$$

Kadangi

$\int_0^T \sin\left(\frac{2\pi}{\lambda} s\sin(\omega t+\varphi)\right)dt = 0$, tai šį narį padauginus iš kompleksinio skaičiaus i, o $\sin\left(\frac{2\pi}{\lambda}(x-b)\right)$ pakeitus į $\cos\left(\frac{2\pi}{\lambda}(x-b)\right)$, lygybė išliks ir tada gaunama:

$$\begin{aligned}
&\lim_{T\to\infty}\frac{1}{T}\int_0^T\left(\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}\left(x-s\sin(\omega t+\varphi)\right)\right)\right)dt = \\
&=\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}(x-b)\right)\lim_{T\to\infty}\frac{1}{T}\int_0^T\cos\left(\frac{2\pi}{\lambda}s\sin(\omega t+\varphi)\right)dt + \\
&+i\cdot\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}(x-b)\right)\lim_{T\to\infty}\frac{1}{T}\int_0^T\sin\left(\frac{2\pi}{\lambda}s\sin(\omega t+\varphi)\right)dt=\frac{1}{2}+ \qquad (1.4)\\
&+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}(x-b)\right)\lim_{T\to\infty}\frac{1}{T}\int_0^T\left(\cos\left(\frac{2\pi}{\lambda}s\sin(\omega t+\varphi)\right)+i\cdot\sin\left(\frac{2\pi}{\lambda}s\sin(\omega t+\varphi)\right)\right)dt = \\
&=\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}(x-b)\right)\lim_{T\to\infty}\frac{1}{T}\int_0^T e^{\frac{2\pi}{\lambda}s\sin(\omega t+\varphi)}dt=\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}(x-b)\right)J_0\left(\frac{2\pi}{\lambda}s\right)
\end{aligned}$$

Šiais dviem atvejais moduliuojanti funkcija išlieka ta pati, laike vidurkinimo funkcijos poslinkis jos neįtakoja. Ši formulė aprašo laike vidurkintų interferencinių juostų susidarymą, ji yra taikoma eksperimentinėje mechanikoje [61] [68].

Laike vidurkintos interferencinės juostos susiformuos tada, kai nulinės eilės Beselio funkcijos šaknys įgys reikšmes lygias nuliui $J_0\left(\frac{2\pi}{\lambda}s\right)=0$, pilkio lygis interferencinės juostos centre bus lygus 0.5. Apvalkalo funkcija, aprašanti pilkio kitimą originaliame vaizde, bus $\frac{1}{2}\pm\frac{1}{2}J_0\left(\frac{2\pi}{\lambda}s\right)$.

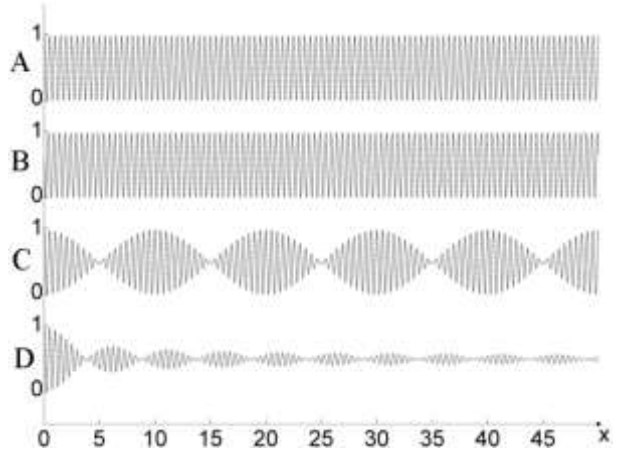
Ryšys tarp muaro gardelės periodo, harmoninių virpesių amplitudės ir laike vidurkintos interferencinės juostos eilės yra randama pagal formulę:

$$s_i=\frac{\lambda}{2\pi}r_i,\ i=1,2,... \qquad (1.5)$$

Formulėje i – interferencinės juostos eilė; r_i – i-toji pirmojo tipo nulinės eilės Beselio funkcijos šaknis, s_i – virpesių amplitudės.

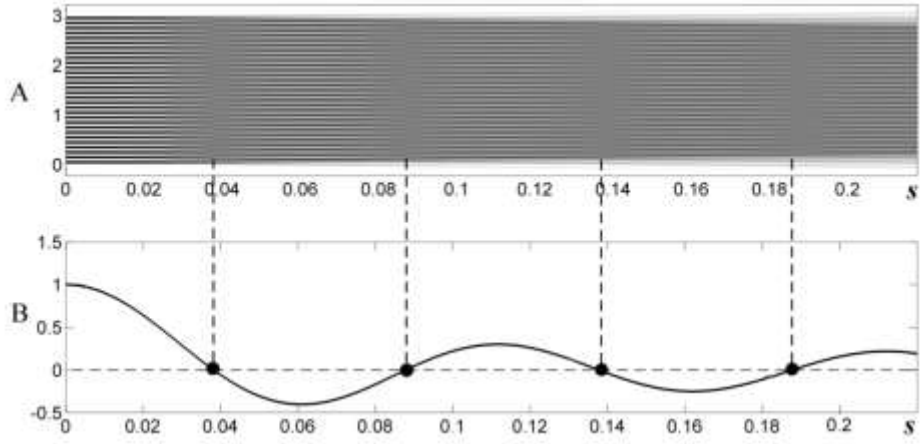
Dvigubos ekspozicijos ir laike vidurkintų interferencinių juostų formavimasis pavaizduotas 1.4 pav. Čia pateiktas rekonstruotas vienmatis muaro gardelės atvejis. 1.4A paveikslo dalyje pavaizduota muaro gardelė pusiausvyros būsenoje; 1.4B paveiksle pavaizduota deformuota muaro gardelė, kai $s(x) = kx$; $k = 0.05$, čia $s(x)$ – harmoninių virpesių amplitudė taške x; 1.4C pav. pavaizduota deformuotos ir pusiausvyros padėtyje esančios muaro gardelės sudedamoji superpozicija; 1.4D pav. matomas laike vidurkintų interferencinių muaro juostų formavimasis, kai dinaminiai nuokrypiai nuo pusiausvyros padėties kinta laike.

Paveiksle galima pastebėti, kad tiek laike vidurkinimo atveju, tiek sudedamosios superpozijos atveju, pilkio lygis interferencinių juostų centruose yra lygus 0.5. Augant virpesių amplitudei, vidurkintos muaro struktūros pilkio reikšmės neinterferencinėse juostose taip pat tampa artimos 0.5. Taip atsitinka dėl pirmojo tipo nulinės eilės Beselio funkcijos savybių: $\lim_{x\to+\infty} J_0(x)=0$.



1.4 pav. Laike vidurkintų interferencinių juostų formavimasis. A – muaro gardelė pusiausvyroje, B – deformuota muaro gardelė, C – muaro juostos gautos sudedamosios superpozicijos būdu, D – laike vidurkintos muaro juostos

Harmoninės muaro gardelės laike vidurkintų interferencinių juostų formavimasis pavaizduotas 1.5A paveiksle. Horizontalioje ašyje pavaizduotos harmoninių judesių amplitudės *s,* vertikalioje – harmoninė gardelė. Paveiksle matomos susidariusios laike vidurkintos interferencinės juostos. Juostų centrai atitinka pirmojo tipo nulinės eilės Beselio funkcijos šaknis (1.5B pav).

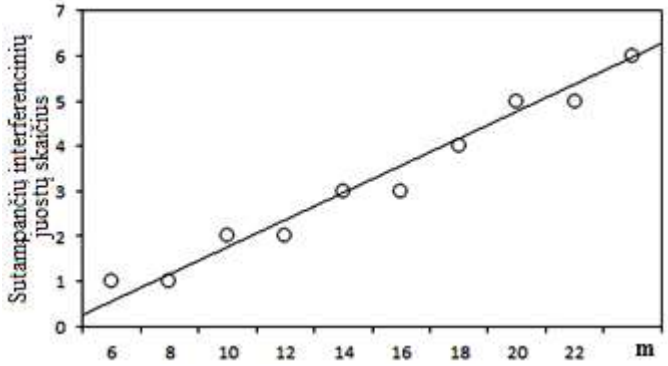


1.5 pav. Harmoninės muaro gardelės, kurios periodas λ=0.1, laike vidurkintų interferencinių juostų susidarymas esant harmoniniams virpesiams pavaizduota A dalyje. B – parodo pirmojo tipo nulinės eilės Beselio funkcijos šaknis ir funkcijos grafiką

Norint kompiuterio ekrane pavaizduoti muaro juostų formavimąsi, konstruojami skaitiniai laike vidurkinti vaizdai, kuriuose gaubiančiosios funkcijos išraiška $\frac{1}{2}\pm\frac{1}{2}J_0\left(\frac{2\pi}{\lambda}s\right)$ keičiama skaičiuojant atitinkamas sumas:

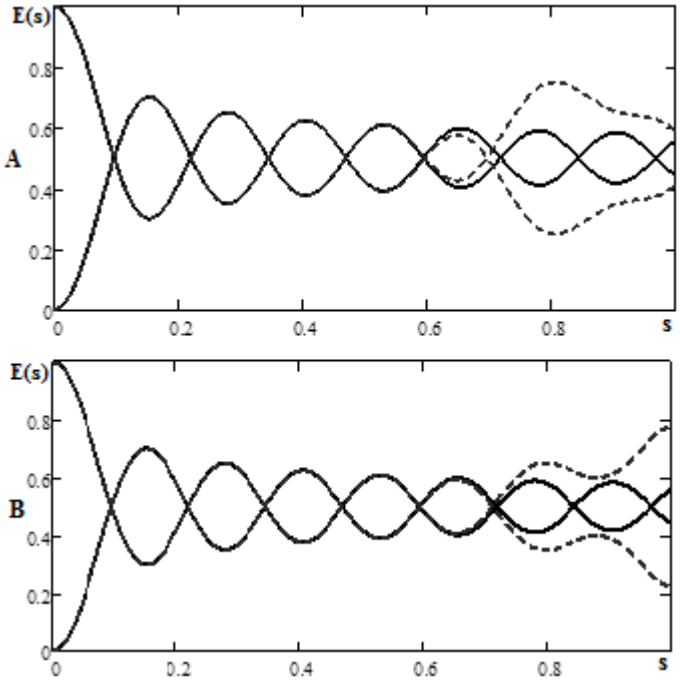
$$E_m(s)=\begin{cases}\frac{1}{m}\sum_{i=1}^{m}\left(\cos^2\left(\frac{\pi}{\lambda}\sin\left(\frac{2\pi}{m}\right)(i-1)/s\right)\right)\\ \frac{1}{m}\sum_{i=1}^{m}\left(\sin^2\left(\frac{\pi}{\lambda}\sin\left(\frac{2\pi}{m}\right)(i-1)/s\right)\right)\end{cases} \tag{1.6}$$

Nustatoma kiek skaitmeniškai gautų gaubiančiosios funkcijos reikšmių sutampa su tikrosiomis gaubiančiosios funkcijos šaknimis, esant skirtingam *m* skaičiui (*m* – diskretinių kadrų skaičius viename virpesių periode). Paveiksle (1.6 pav.) pateikti rezultatai, apskaičiuoti kai amplitudė yra pastovi ir muaro gardelės periodas λ lygus 0.25. Horizontalioje ašyje – pasirinktas diskretinių kadrų skaičius *m*; vertikalioje ašyje – sutampančių interferencinių juostų skaičius, esant harmoniniams virpesiams [66].



1.6 pav. Ryšys tarp teisingai rekonstruotų muaro interferencinių juostų skaičiaus ir parametro *m*

1.7 paveiksle pateikti gaubiančiosios funkcijos ir apytiksliai apskaičiuotos sumos grafikai prie skirtingų *m* reikšmių. Juoda vientisa linija vaizduoja tikslią gaubiančiąją funkciją $\frac{1}{2}\pm\frac{1}{2}J_0\left(\frac{2\pi}{\lambda}s\right)$, o punktyrais pavaizduota apytikslė integralinė suma prie skirtingų *m* reikšmių.



1.7 pav. Gaubiančiosios funkcijos ir ją pakeitusios apytikslės funkcijos grafikai. A – kai kadrų skaičius m lygus 20; B – kai m lygus 22

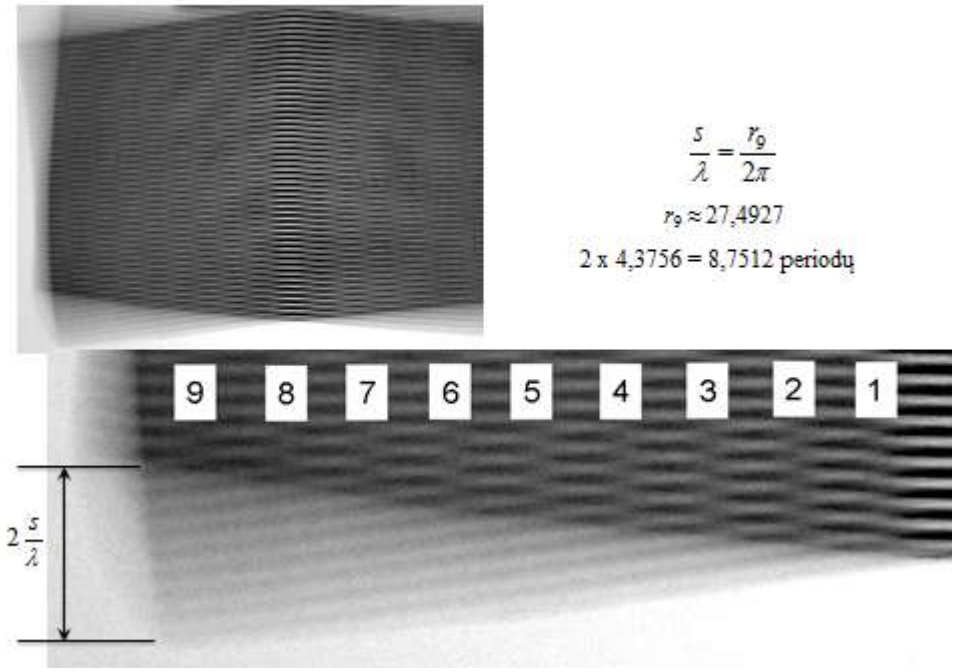
Realiai kai modeliuojami laike vidurkinimo efektai kompiuteryje, tai periodas skaidomas į kelias tarpines būsenas. Šis tyrimas svarbus tuo, kad leidžia nustatyti kaip tarpinių pozicijų skaičius periode įtakoja teisingai rekonstruotų interferencinių juostų skaičių.

Eksperimentinė realizacija

Norint patvirtinti gautus teorinius laike vidurkinto muaro analizės metodus buvo atliktas eksperimentas [66]. Ant guminio paviršiaus buvo įrėžtos tamsios ir baltos spalvos linijos sudarančios muaro gardelę. Guma pritvirtinta ant vibrostendo. Gardelės žingsnis 1 mm, linijos plotis – pusė žingsnio, vibrostendo judėjimo dažnis 51 Hz, kas atitinka antrą rezonansinę gumos bandinio virpesių formą. Pastebėta, kad muaro gardelė aiškiausiai matoma nejudančioje guminio bandinio zonoje. Esant dinaminei deformacijai, lengvai galima identifikuoti susiformavusias laike vidurkintas muaro juostas, kurios gali būti identifikuojamos plika akimi, kuo aukštesnė interferencinės juostos eilė, tuo ji matoma blogiau. Pavyzdžiui, 1.8 pav., kairėje nuo nejudančios bandinio zonos, matome devynias susiformavusias interferencines muaro juostas. Tai reiškia, kad didžiausias dinaminis guminio mėginio poslinkis krašte, vertikalia kryptimi yra $\frac{s}{\lambda}=\frac{r_9}{2\pi}$, šiuo atveju $r_9 \approx 27.4927$. Didžiausias dinaminis nuokrypis nuo pusiausvyros padėties yra 4,3756 muaro

gardelės periodų, arba 8,7512 periodų nuo didžiausio poslinkio žemyn ir didžiausio poslinkio aukštyn vertikalia kryptimi.

1.8 paveikslėlyje pavaizduotos eksperimento metu gautos laike vidurkinto geometrinio muaro interferencinės juostos. Nesunku suskaičiuoti kiek muaro gardelės periodų telpa laike vidurkintame eksperimentiniame vaizde maksimalių poslinkių zonoje t.y. gumos bandinio pačiame gale (išplautoje vaizdo vietoje), kur virpesių amplitudė pati didžiausia. Šių periodų suskaičiuojama apie 8. Tai rodo idealų sutapimą tarp eksperimentinių ir skaitinių rezultatų.



1.8 pav. Laike vidurkinto geometrinio muaro eksperimentinis validavimas

1.5.2. Laike vidurkinimo efektai stačiakampėje muaro gardelėje

Nagrinėjama stochastinė muaro gardelė, kuri generuoja laike vidurkintas interferencines juostas tik tada kai teisingai parinktas judesio dėsnis (pav. „zig-zag“ tipo virpesiai), kryptis ir amplitudė [64].

Paimta laiptuota muaro gardelė:

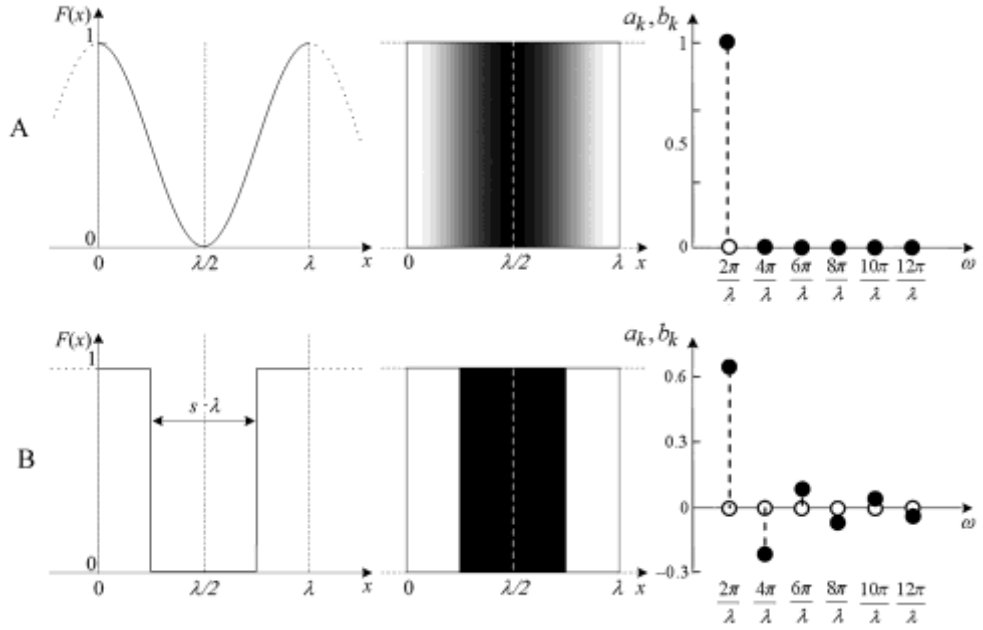
$$F(x)=\begin{cases}1,\ \text{kai}\ x\in\left[\lambda j;\dfrac{(1-b)\lambda}{2}+\lambda j\right]\cup\left[\dfrac{(1+b)\lambda}{2}+\lambda j;\lambda(j+1)\right]\\ 0,\ \text{kai}\ x\in\left(\dfrac{(1-b)\lambda}{2}+\lambda j;\dfrac{(1+b)\lambda}{2}+\lambda j\right)\end{cases} \tag{1.7}$$

čia $j = 0, \pm 1, \pm 2, \ldots$, parametras b parodo muaro gardelės santykį tarp juodų ir baltų juostų. Gardelės periodas λ. Funkciją $F(x)$ galima išskleisti Furjė eilute, kurios koeficientai bus:

$$F(x) = \begin{cases} a_0 = 2(1-b) \\ a_k = \dfrac{\sin(k\pi(1-b)) - \sin(k\pi(1+b))}{k\pi} \\ b_k = \dfrac{\cos(k\pi(1+b)) - \cos(k\pi(1-b))}{k\pi} \end{cases} \tag{1.8}$$

čia $k = 1, 2, \ldots$.

Paveiksle 1.9 pavaizduotos harmoninė ir laiptinė muaro gardelės; skaitinės koeficientų a_k ir b_k reikšmės apskaičiuotos esant gardelės juostų santykiui $b = 0.5$ (juodos ir baltos juostos yra vienodo pločio).

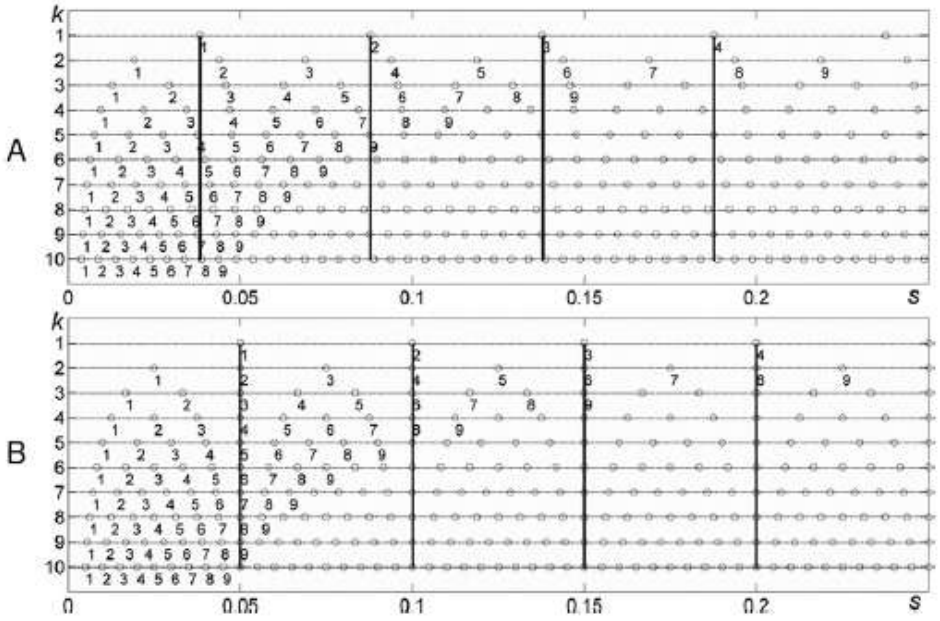


1.9 pav. Harmoninė – A ir laiptuota muaro gardelė – B. Kairysis stulpelis iliustruoja vienmatę gardelę, vidurinysis iliustruoja pilkio pasiskirstymą vaizde ir dešinysis stulpelis parodo Furjė a_k (balti skrituliai) ir b_k (juodi skrituliai) koeficientus

Jeigu laiptuotą pilkio funkcija paveikiama „zig-zag“ tipo nuokrypiais nuo pusiausvyros padėties, tai laike vidurkintas vaizdas yra apibrėžiamas taip:

$$H_s\left(x \mid F; \hat{\zeta}_s\right) = \frac{a_0}{2} + \sum_{k=1}^{+\infty}\left(a_k \cos\frac{k2\pi x}{\lambda} + b_k \sin\frac{k2\pi x}{\lambda}\right)\frac{\sin\left(\frac{k2\pi}{\lambda}s\right)}{\left(\frac{k2\pi}{\lambda}s\right)} \qquad (1.9)$$

Parenkamas gardelės periodas $\lambda = 0.1$ ir tiriama funkcijos $\frac{\sin\left(\frac{k2\pi}{\lambda}s\right)}{\left(\frac{k2\pi}{\lambda}s\right)}$ šaknis, prie skirtingų *k* reikšmių. Jei *k* = 1 šis reiškinys bus lygus nuliui tada, kai $s_j = \frac{j\lambda}{2}$; $j = 1,2,....$ 1.10 paveikslo B dalyje aukščiausioje paveikslo atkarpoje pažymėtos šios funkcijos šaknys. Pastebima, kad šiuo atveju funkcijos šaknys gaunamos kai amplitudė yra lygi 0.05, 0.1, 0,15 ir t.t. Jei *k* = 2 tada funkcijos šaknys gaunamos, kai $s_j = \frac{j\lambda}{4}$; $j = 1,2,....$ Jos taip pat atidėtos 1.10 paveikslo B dalyje šiek tiek žemiau. Dabar šaknys randamos, kai amplitudė yra lygi 0.025, 0.05, 0.075, 0.1 ir t.t. Tai yra dvigubai tankiau. Kai *k* = 3 tada šaknys išsidėsto trigubai tankiau ir t.t. Sekančiose paveikslo 1.10 atkarpose atidedamos funkcijos šaknys prie skirtingo sumos narių skaičiaus *k*. Amplitudės atitinkamai lygios $s_j = \frac{j\lambda}{2k}$, $j = 1,2,....$



1.10 pav. Laike vidurkintų interferencinių juostų centrų pasiskirstymas skirtingiems muaro gardelės Furjė skleidinio koeficientams: A – harmoniniai virpesiai, B – „zig-zag“ tipo virpesiai. Gardelės periodas λ=0.1

Pastebima, kad egzistuoja tokios virpesių amplitudės *s* reikšmės, prie kurių (1.9) formulės begalinė suma lygi nuliui, nepriklausomai nuo to kokia *k* reikšmė (šios reikšmės pažymėtos vertikaliomis paryškintomis atkarpomis (1.10B pav.)). Furjė skleidinyje prie žemiausio dažnio komponentės esanti šaknis bus kartotinė visoms aukštesnėms harmonikoms ir todėl susiformuos interferencinė juosta.

Jeigu laiptuota pilkio funkcija yra virpinama harmoniškai, tai laike vidurkintas vaizdas apibrėžtas taip:

$$H_s\left(x \mid F;\tilde{\zeta}\right)=\frac{a_0}{2}+\sum_{k=1}^{+\infty}\left(a_k\cos\frac{k2\pi x}{\lambda}+b_k\sin\frac{k2\pi x}{\lambda}\right)J_0\left(\frac{k2\pi}{\lambda}s\right) \qquad (1.10)$$

Harmoninių virpesių amplitudės pažymimos: $s_j=\frac{\lambda r_j}{2\pi k}$; čia $j=1,2,...,$ prie kurių *k*-asis Furjė eilutės sumos dėmuo lygus nuliui. Tačiau pirmojo tipo nulinės eilės Beselio funkcijos šaknys tarpusavyje yra nekartotinės ir taip išsidėsto, kad pirmoji harmonika prie atitinkamos amplitudės *s* turi šaknį, o jokia aukštesnė harmonika prie tos pačios amplitudės šaknies neturi, todėl nėra tokios harmoninių virpesių amplitudės *s*, prie kurios begalinė suma virstu nuliu (1.10A pav.). Taigi, jeigu muaro gardelės funkcijos skleidinys Furjė eilute sudarytas iš daugiau nei vieno harmoninio elemento tai tokiu atveju laike vidurkintame vaizde nesusidarys interferencinės juostos. Tai papildomo saugumo įrankis, jeigu vaizdas užkoduotas neharmoninėje muaro gardelėje, tai kokiu harmoniniu dėsniu būtų virpinama, kokia bebūtų amplitudė niekur nesusiformuos muaro interferencinės juostos: slapta informacija nepasirodys niekada. Slapta informacija formuojasi stačiakampėje muaro gardelėje tik tuomet kai ji virpinama pagal „zig-zag“ dėsnį.

1.6. Žmogaus regos sistemos tyrimai

Žmogaus regos sistemos tyrimų srityje yra pasiekta nemažai rezultatų tiek Lietuvoje, tiek ir užsienyje. Čia pirmiausia reiktų paminėti plačius J. Jankauskienės darbus akių mikro judesių tyrimų srityje [69] [70]. Ženklių rezultatų tiek žmogaus akių judesių tyrime, tiek judančių objektų sekimo srityje yra pasiekusi V. Lauručio grupė Biomedicinos inžinerijos centre Šiaulių Universitete [71]. Tarptautinėje plotmėje reiktų paminėti tokius mokslinius žurnalus kaip Perception, Vision Reseach, Nature grupės leidžiamas žurnalas Eye, kuriuose pagrindinis dėmesys kaip tik yra sutelktas į įvairius žmogaus regos sistemos aspektus; čia būtų galima vardinti daugelį žymių mokslininkų darbų tiek judesio detekcijos, tiek regos (frontalinės bei periferinės) tyrimų srityje.

1.7. Skyriaus išvados

Apžvelgus atliktus darbus dinaminės vizualinės kriptografijos ir žmogaus regos sistemos tyrimų srityje disertacijos objektu buvo pasirinktos laike vidurkintos optinių muaro metodų realizacijos, skirtos dinaminės vizualinės kriptografijos tyrimui. Darbe siekta sukurti ir eksperimentiškai realizuoti dinaminės vizualinės kriptografijos koncepciją pagrįstą netiesinių sistemų virpesiais. Buvo nuspręsta atlikti tyrimus bei juos realizuoti eksperimentiškai, panaudoti sistemų parametrų

identifikacijai ir kontrolei. Šioje disertacijoje bus rasta optimali laiko funkcija, leidžianti užtikrinti optimalų koduoto vaizdo saugumą. Parodyta, kad dinaminės vizualinės kriptografijos optinius efektus galima realizuoti naudojantis eksperimentinėmis priemonėmis, pagrįstomis virpesių generavimo įrenginiais ir valdymo technika. Disertacijoje nagrinėjamos chaotinės dinaminės kriptografijos galimybės. Panaudojus optinius efektus skaitmeninių kompiuterių ekranuose sukurtas dinaminės vizualinės kriptografijos principu funkcionuojantis įrenginys, įgalinantis vertinti žmogaus regos sistemos funkcionalumą.

2. BEVEIK OPTIMALI DINAMINĖS VIZUALINĖS KRIPTOGRAFIJOS LAIKO FUNKCIJA

Literatūros apžvalgoje buvo nagrinėtas skirtingomis muaro gardelėmis koduoto paveikslo dekodavimas virpinant vaizdą reikiama kryptimi ir amplitude. Norint užtikrinti didesnį koduoto paveikslo saugumą šiame skyriuje sprendžiamas uždavinys: nustatyti optimalią dekodavimo trajektoriją, t.y. rasti svyravimų dėsnį, kuriuo dekoduojant slaptas vaizdas išryškėtų esant nedideliems amplitudės nuokrypiams apie teorinę amplitudės reikšmę. Skyriaus pradžioje aptariami teoriniai sąryšiai, kuriais remiantis vėliau konstruojamas optimizavimo uždavinys. Pasitelkus genetinius algoritmus gauta beveik optimali laiko funkcija. Taip pat skyriuje aprašomas slapto vaizdo kodavimo algoritmas ir atliekami skaitiniai eksperimentai patvirtinantys gautus rezultatus.

Nagrinėjama vienmatė stochastinė laiptuota muaro gardelė [64]:

$$F(x)=\begin{cases}1,\ kai\ x\in\left[\lambda j;\lambda\left(j+\dfrac{1}{2}\right)\right]\\ 0,\ kai\ x\in\left[\lambda\left(j+\dfrac{1}{2}\right);\lambda(j+1)\right]\end{cases},\quad j=0,\pm1,\pm2,\ldots \tag{2.1}$$

čia λ – muaro gardelės žingsnis.

Apibrėžimas 1. Laike vidurkinimo operatorius H_s apibrėžiamas [72]:

$$H_s(F;\zeta_s)=\lim_{T\to\infty}\frac{1}{T}\int_0^T F(x-\xi_s(t))dt \tag{2.2}$$

čia t – laikas, T – ekspozicijos laikas, $\xi_s(t)$ – funkcija aprašanti dinaminį nuokrypį nuo pusiausvyros padėties, $s\geq 0$ – realus parametras, $x\in\mathrm{R}$.

Apibrėžimas 2. Laike vidurkintų interferencinių juostų standarto funkcija apibrėžiama [64]:

$$\sigma(s)=\sigma(H_s(F(x),\xi_s))=\sqrt{\frac{1}{\lambda}\int_0^\lambda (H_s(F(x),\xi_s)-E(H_s(F(x),\xi_s)))^2} \tag{2.3}$$

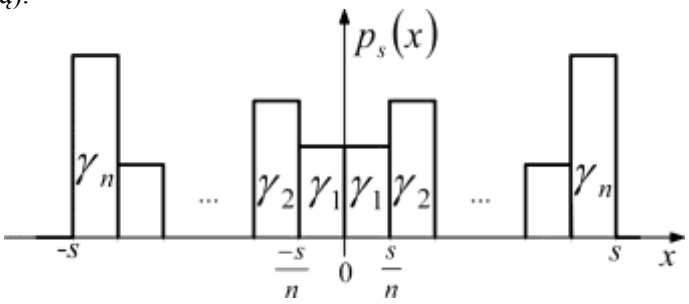
čia $E(H_s(x|F,\xi_s))=\dfrac{1}{\lambda}\int_0^\lambda H_s(x|F,\xi_s)dx$ – laike vidurkintos muaro gardelės vidurkis.

Nagrinėjama dalimis tiesinės funkcijos $\xi_s(t)$ – kintamojo ξ_s realizacijos – kurių atitinkamos tankio funkcijos $p_s(x)$ tenkina tokius du reikalavimus:

a) $p_s(x)=0$ kai $|x|>s;\quad s>0;$

b) $p_s(x)=p_s(-x)$ visiems $x\in\mathrm{R}$.

Laikoma, kad tankio funkcija $p_s(x)$ sudaryta iš 2*n* vienodo pločio stulpelių, simetriškai išsidėsčiusių intervale [-*s*; *s*] (pav. 2.1). Pagal tankio funkcijos reikalavimus, ji turi būti simetrinė ordinačių ašies atžvilgiu, stulpeliai kairėje koordinačių pusplokštumėje yra lygūs atitinkamiems stulpeliams dešinėje pusplokštumėje. Tam, kad būtų išlaikytas simetriškumas nagrinėjamas svorių vektorius (γ_1, γ_2,...,γ_n), kuris atitinka dešiniąją tankio funkcijos pusę (γ_i žymi *i*-tojo stulpelio plotą).



2.1 pav. Dalimis tolygi tankio funkcija sudaryta iš 2*n* vienodo pločio stulpelių. Čia funkcija yra aprašoma stulpelių svorių vektoriumi (γ_1, γ_2,...,γ_n), kur γ_i yra kiekvieno stulpelio plotas

Teiginys 1. Atkarpomis tiesinės tankio funkcijos $p_{s,n}(x)$ Furjė transformacija yra:

$$P_s(\Omega) = \frac{2n}{\Omega \cdot s} \cdot p_1(\Omega);. \tag{2.4}$$

kur

$$p_1(\Omega) = (\gamma_1 - \gamma_2)\sin\left(\frac{s\Omega}{n}\right) + (\gamma_2 - \gamma_3)\sin\left(\frac{2s\Omega}{n}\right) + \ldots + (\gamma_{n-1} - \gamma_n)\sin\left(\frac{(n-1)s\Omega}{n}\right) +$$

$$+ n\gamma_n \sin(s\Omega).$$

Furjė transformacijos $P_s(\Omega)$ išvestinė amplitudės *s* atžvilgiu gali būti užrašoma taip:

$$P_s'(\Omega) = \frac{2}{s} \cdot p_2(\Omega) - \frac{2n}{\Omega s^2} \cdot p_1(\Omega); \tag{2.5}$$

kur

$$p_2(\Omega) = (\gamma_1 - \gamma_2)\cos\left(\frac{s\Omega}{n}\right) + (\gamma_2 - \gamma_3)\cos\left(\frac{2s\Omega}{n}\right) + \ldots + (\gamma_{n-1} - \gamma_n)\cos\left(\frac{(n-1)s\Omega}{n}\right) +$$

$$+ n\gamma_n \sin(s\Omega).$$

Teiginys 2. Jei periodinę pilkio funkciją galima išskleisti Furjė eilute:

$$F(x) = \frac{a_0}{2} + \sum_{k=1}^{\infty}\left(a_k \cos\frac{2k\pi x}{\lambda} + b_k \sin\frac{2k\pi x}{\lambda}\right),\ a_k,\ b_k \in \mathrm{R},\ k = 1,2,\ldots \tag{2.6}$$

tai, pagal [64] muaro gardelės, kurios periodas λ, virpinamos dėsniu $\zeta_s(t)$ vidurkinimo operatorius bus:

$$H\left(F(x),\zeta_s(t)\right)=\frac{a_0}{2}+\sum_{k=1}^{\infty}\left(a_k\cos\frac{2k\pi x}{\lambda}+b_k\sin\frac{2k\pi x}{\lambda}\right)P_s\left(\frac{2k\pi}{\lambda}\right) \tag{2.7}$$

Elementarių pertvarkymų pagalba nustatyta, kad laike vidurkintos pilkio funkcijos vidurkis lygus:

$$E\left(H\left(F(x),\zeta_s(t)\right)\right)=\frac{a_0}{2} \tag{2.8}$$

jo standartas:

$$\sigma\left(H_s\left(F(x),\zeta_s\right)\right)=\frac{\sqrt{2}}{2}\sqrt{\sum_{k=1}^{\infty}\left(a_k^2+b_k^2\right)\cdot P_s^2\left(\frac{2k\pi}{\lambda}\right)} \tag{2.9}$$

o standarto išvestinė, kuri vėliau naudojama įvertinti kodavimo saugumą, lygi:

$$\sigma_s'\left(H_s\left(F(x),\zeta_s\right)\right)=\frac{\sqrt{2}}{2}\frac{\sum_{k=1}^{\infty}\left(a_k^2+b_k^2\right)\cdot P_s\left(\frac{2k\pi}{\lambda}\right)\cdot P_s'\left(\frac{2k\pi}{\lambda}\right)}{\sqrt{\sum_{k=1}^{\infty}\left(a_k^2+b_k^2\right)\cdot P_s^2\left(\frac{2k\pi}{\lambda}\right)}} \tag{2.10}$$

2.1. Optimizavimo uždavinio konstravimas

Yra žinoma [64], kad laike vidurkintos interferencinės juostos nesusiformuoja, kai laiptinė muaro gardelė (2.1) yra virpinama harmoniškai. Tačiau, virpinant tą pačią laiptinę muaro gardelę pagal laiko funkciją, kurios tankio funkcija tolygi, interferencinės juostos formuojasi. Ryškiausia juosta susiformuoja vaizdą virpinant amplitude, atitinkančia pirmąją tankio funkcijos Furjė transformacijos šaknį [64]. Tolydaus tankio atveju, pirmoji interferencinė juosta susiformuoja prie amplitudės $s=\lambda/2$: tada muaro gardelės standartas yra lygus nuliui. Dalimis tolygaus tankio funkcijos Furjė transformacijos šaknys taip pat išsidėsčiusios periodiškai (2.4). Taigi kyla klausimas, kuri tankio funkcija – tolygi ar dalimis tolygi – yra geresnė informacijos kodavimo prasme? Standarto funkcijos išvestinės modulį, apskaičiuotą esant amplitudei, atitinkančiai pirmąją muaro interferencinę juostą, galima panaudoti kaip kodavimo saugumo įvertį. Galima pasiekti didesnį jautrumą amplitudės nustatymui. Kokiame intervale gali būti amplitudė, kad formuotųsi slapta informacija? Jei standarto „frontai“ iš kairės ir dešinės yra glotnūs, tai amplitudės intervalas gali būti ir platesnis. Jei standarto išvestinės modulis prie tam tikros amplitudės, staiga iš abiejų pusių krinta žemyn, tada reikia labai tiksliai nustatyti virpesių amplitudę, nes kitaip koduotas vaizdas nesimatys, ten kur standartas lygus nuliui, ten yra interferencinės juostos centras. Kuo didesnis standarto funkcijos išvestinės modulis prie pirmos interferencinės juostos, tuo funkcija šaknies aplinkoje

greičiau kinta, todėl kuo tiksliau turi būti nustatyta amplitudės reikšmė, norint pamatyti slaptą informaciją, tokiu būdu gaunamas dar vienas saugumo parametras.

Taigi nagrinėjamas toks kombinatorinio optimizavimo uždavinys: surasti vektorių (γ_1, γ_2,...,γ_n), maksimizuojantį tikslo funkciją:

$$\left|\sigma'\left(s=\frac{\lambda}{2}\right)\right| = \left| \frac{\sqrt{2}}{2} \frac{\sum_{k=1}^{\infty}\left(a_k^2+b_k^2\right)\cdot P_s\left(\frac{2k\pi}{\lambda}\right)\cdot P_s'\left(\frac{2k\pi}{\lambda}\right)}{\sqrt{\sum_{k=1}^{\infty}\left(a_k^2+b_k^2\right)\cdot P_s^2\left(\frac{2k\pi}{\lambda}\right)}} \right| \tag{2.11}$$

su apribojimais $\sum_{i=1}^{n}\gamma_i = \frac{1}{2}$ ir $\gamma_i > 0$, $i = 1,2,\ldots,n$.

Norint sumažinti skaičiavimo apimtis, nagrinėtas sveikaskaitinio programavimo uždavinys, ieškoma sveikųjų γ_1, γ_2,...,γ_n reikšmių ir tada jos normalizuojamos $2\sum_{i=1}^{n}\gamma_i$ atžvilgiu: $\frac{1}{2\sum_{i=1}^{n}\gamma_i}(\gamma_1,\gamma_2,\ldots,\gamma_n)$. Fiksuojama suma $H = \sum_{i=1}^{n}\gamma_i$ ir dalimis tolydžios tankio funkcijos pusės stulpelių skaičius *n*. Tada

$$\left|\sigma'\left(s=\frac{\lambda}{2}\right)\right| = \left| \frac{\sqrt{2}}{2} \frac{\sum_{k=1}^{\infty}\left(a_k^2+b_k^2\right)\cdot P_s\left(\frac{2k\pi}{\lambda}\right)\cdot P_s'\left(\frac{2k\pi}{\lambda}\right)}{\sqrt{\sum_{k=1}^{\infty}\left(a_k^2+b_k^2\right)\cdot P_s^2\left(\frac{2k\pi}{\lambda}\right)}} \right| \to \max, \tag{2.12}$$

kai $\sum_{i=1}^{n}\gamma_i = H$; (2.13)

$\gamma_i > 0$, $i = 1,2,\ldots,n$. (2.14)

čia γ_i, $i = 1,2,\ldots,n$ ir *H* yra sveikieji natūralieji skaičiai.

Pastebima, kad dalimis tolydžios tankio funkcijos stulpelių skaičius ir dydis *H* nusako sveikaskaitinio programavimo uždavinio apimtį: vektorių (γ_1, γ_2,...,γ_n), tenkinančių (2.13) ir (2.14) apribojimus, skaičius lygus $N_\gamma = (H-n+1)(H-n+2)/2$.

Uždavinio (2.12-2.14) sprendimui naudojami genetiniai algoritmai.

2.2. Optimizavimo uždavinio sprendimas naudojant genetinius algoritmus

Sprendžiant sukonstruotą optimizavimo uždavinį genetinių algoritmų pagalba pirmiausia suformuojama pradinė fiksuoto dydžio sprendinių aibė, kuri yra vadinama *populiacija*. Kiekvienas populiacijos elementas vadinamas *chromosoma* ir yra užkoduotas tikslo funkcijos sprendinys. Kodavimo sistemos tikslas yra kiekvieną

sprendinį paversti *genų* rinkiniu – chromosoma. Visa populiacija susideda iš *n* chromosomų, chromosoma – iš genų. Nagrinėjamu atveju kiekviena chromosoma atitinka vektorių (γ_1, γ_2,...,γ_n). Chromosomos ilgis (pusės stulpelių skaičius) yra lygus 12, o suma $H = 60$, t.y. genai gali įgyti reikšmes tarp 1 ir 49. Tankio funkcijos stulpelių plotis yra fiksuotas, taigi geno reikšmė yra proporcinga atitinkamo stulpelio aukščiui. Chromosomos optimalumas įvertinamas pagal $\left|\sigma'\left(s=\frac{\lambda}{2}\right)\right|$ reikšmę.

Pradinė populiacija turi *N* atsitiktinai sugeneruotų chromosomų. Kiekviena chromosoma pradinėje populiacijoje sugeneruojama taip, kad galiotų 2.13 ir 2.14 apribojimai. Visos chromosomos (γ_1, γ_2,...,γ_n) yra hiperplokštumos, apibrėžtos 2.13 lygybe ir 2.14 nelygybėmis, taškai. Chromosomų generavimo procedūra vykdoma taip:

1) sugeneruojamas sveikasis skaičius γ_1, tolygiai pasiskirstęs intervale $[1; H-n+1]$.

2) sugeneruojamas sveikasis skaičius γ_2, tolygiai pasiskirstęs intervale $[1; H-n+1-\gamma_1]$.

3) sugeneruojamas sveikasis skaičius γ_3, tolygiai pasiskirstęs intervale $[1; H-n+1-\gamma_1-\gamma_2]$.

n-1) sugeneruojamas sveikasis skaičius γ_{n-1}, tolygiai pasiskirstęs intervale $\left[1; H-n+1-\sum_{i=1}^{n-2}\gamma_i\right]$.

n) suskaičiuojamas genas $\gamma_n = H-n+1-\sum_{i=1}^{n-1}\gamma_i$.

Pradinėje populiacijoje gali būti ir pasikartojančių chromosomų. Todėl kiekvienos jų patekimo į populiaciją tikimybė yra vienoda ir lygi $\frac{1}{H-n+1}\cdot\frac{1}{H-n}\cdot\ldots\cdot\frac{1}{2}\cdot 1=\frac{1}{(H-n+1)!}$.

Kitas žingsnis – *atranka*. Jos tikslas yra iš esamos populiacijos išrinkti tas chromosomas, kurios geriausiai tinka duotai problemai spręsti ir iš jų suformuoti naują tėvų populiaciją, kurios genais bus nauji sprendiniai. Kiekvienai chromosomai apskaičiuojama tikslo funkcijos reikšmė ir lyginis skaičius chromosomų iš pradinės populiacijos atrenkamas į tėvų populiaciją bei suskirstomos atsitiktinėmis poromis. Ši populiacija yra tokio pat dydžio kaip ir pradinė. Chromosomų atrinkimui naudojamas *ruletės* principas – tikimybė patekti į tėvų populiaciją yra proporcinga tikslo funkcijos reikšmei. Ši strategija garantuoja, kad geresni individai tėvais taps daug dažniau nei kiti. Galimos kelios tos pačios chromosomos kopijos. Baigus tėvų atranką, chromosomos suskirstomos į atsitiktines poras. Toliau atliekamas *kryžminimas*. Kryžminimo metu iš atskirų chromosomų, sukuriama nauja labai gera chromosoma, kuri turi visus populiacijoje esančius gerus genus. Taip išgryniname populiaciją ir iš gerų chromosomų sukuriame labai geras. Genetiniuose algoritmuose

kryžminimo metu atrinktoje populiacijoje du šalia esantys tėvai apsikeičia genais ir suformuoja dvi naujas chromosomas – vaikus. Kryžminimas atliekamas su visomis poromis: naudojamas *vieno taško* kryžminimo metodas kai atsitiktinai parenkamas taškas per kurį chromosoma padalinama į dvi dalis ir apatinės dalys sukeičiamos vietomis. Kryžminimo koeficientas κ parodo tikimybę, kad chromosomų pora apsikeis genais, t.y. įvyks kryžminimas. Po kryžminimo galimi tokie chromosomų rinkiniai, kurie netenkina (2.13) sąlygos. Todėl visi tokie genų rinkiniai normuojami pagal 2.15 formulę.

$$\left(\gamma_1', \gamma_2', \ldots, \gamma_n'\right) = \left(\text{round}\left(\frac{H \cdot \gamma_1}{\sum_{i=1}^{n} \gamma_i} \right), \text{round}\left(\frac{H \cdot \gamma_2}{\sum_{i=1}^{n} \gamma_i} \right), \ldots, \text{round}\left(\frac{H \cdot \gamma_n}{\sum_{i=1}^{n} \gamma_i} \right) \right) \quad (2.15)$$

Jei rinkinys $\left(\gamma_1', \gamma_2', \ldots, \gamma_n'\right)$ netenkina (2.14) sąlygos, tai jis suapvalinamas iki (2.14) sąlygą tenkinančio artimiausio mažesnio (H–n+1) n skilčių skaičiaus, jei $\sum_{i=1}^{n} \gamma_i' > H$, arba iki artimiausio didesnio (H–n+1) skaičiaus, jei $\sum_{i=1}^{n} \gamma_i' < H$.

Siekiant išvengti sprendinio konvergavimo į lokalųjį sprendinį, vykdoma *mutacijos* procedūra, kuri į sprendinių aibę įneša naujos informacijos. Mutacijos koeficientas μ ($0<\mu<1$) yra tikimybė, kad chromosoma mutuos. Šiai procedūrai atsitiktinai atrenkama *round*($\mu \cdot N$) chromosomų. Tada jomis pakeičiamas atsitiktinai parinktas genas pridedant prie esamos reikšmės intervale $[1; H-n+1]$ pasiskirsčiusį skaičių. Mutavusioms chromosomoms, kaip ir po kryžminimo, atliekama normavimo procedūra.

Genetiniam algoritmui reikalinga parinkti tokius parametrus: kryžminimo koeficientą κ, mutacijos koeficientą μ ir populiacijos dydį N. Norint parinkti optimalias šių parametrų reikšmes, užtikrinančias geriausius genetinio algoritmo sprendinius, konstruojamas dirbtinis uždavinys: ieškoma geriausia tankio funkcija, susidedanti iš 6 stulpelių (chromosomos ilgis yra 3), ir fiksuojamas dydis $H = 15$. Optimalus šio uždavinio sprendinys, gautas atlikus pilną perrinkimą, yra vektorius (1; 1; 13), o jo tikslo funkcijos reikšmė yra $\left|\sigma_s'\left(s = \frac{\lambda}{2}\right)\right| = 0{,}6565067$. Tada tam pačiam uždaviniui pritaikomi genetiniai algoritmai. Imama populiacija, kurios dydis yra N=20 chromosomų. Tai sudaro $\frac{N}{N_\gamma} = \frac{20 \cdot 2}{(15-3+1)(15-3+2)} = \frac{40}{182} \approx 22.99\%$ visų chromosomų.

Evoliucija vykdoma 5 generacijas po 3 nepriklausomus bandymus. Kryžminimo ir mutacijos koeficientus parenkame pagal tai, kiek kartų populiacijoje pasikartoja geriausias sprendinys (sėkmingų bandymų skaičius), ir pagal visos evoliucionavusios populiacijos tikslo funkcijos vidurkį (mean fit) (2.1 – 2.3 lent.).

2.1 lentelė. Geriausio sprendinio pasikartojimų skaičius (k) ir populiacijos fitnesų vidurkis, kai μ=0.01, N=20

κ	0.5		0.6		0.7		0.8		0.9		1	
	mean fit	*k*	mean fit	*k*	mean fit	*k*	mean fit	*k*	mean fit	*k*	mean fit	*k*
1	0.5146	1	0.5266	10	0.5562	4	0.4916	8	0.4362	3	0.6042	14
2	0.6003	1	0.6502	19	0.6001	7	0.6377	17	0.5793	8	0.6461	18
3	0.6170	1	0.6565	20	0.6399	12	0.6502	18	0.6378	15	0.6544	19
4	0.6170	1	0.6565	20	0.6544	19	0.6544	19	0.6482	18	0.6565	20
5	0.6191	3	0.6565	20	0.6565	20	0.6565	20	0.6523	19	0.6565	20
1	0.5794	1	0.5690	1	0.5824	11	0.5773	0	0.6065	9	0.4267	0
2	0.6066	0	0.5899	0	0.6523	19	0.5752	1	0.6398	16	0.4434	0
3	0.6107	0	0.6086	0	0.6565	20	0.6065	1	0.6565	20	0.4683	0
4	0.6149	0	0.6149	0	0.6565	20	0.6086	0	0.6565	20	0.4850	0
5	0.6149	0	0.6149	0	0.6565	20	0.6149	0	0.6565	20	0.4892	0
1	0.6295	11	0.4720	5	0.5711	0	0.5521	4	0.4899	0	0.5729	0
2	0.6482	17	0.6149	0	0.6045	0	0.5563	4	0.5088	0	0.5729	0
3	0.6565	20	0.6149	0	0.6128	0	0.5959	7	0.5150	0	0.5729	0
4	0.6565	20	0.6149	0	0.6149	0	0.6252	14	0.5192	0	0.5729	0
5	0.6565	20	0.6149	0	0.6149	0	0.6565	20	0.5254	0	0.5729	0

2.2 lentelė. Geriausio sprendinio pasikartojimų skaičius (k) ir populiacijos fitnesų vidurkis, kai μ=0.05, N=20

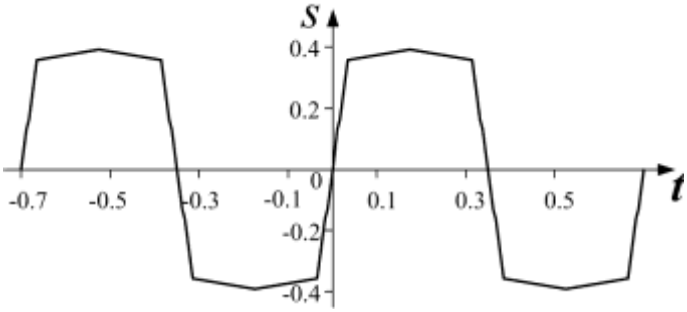
κ	0.5		0.6		0.7		0.8		0.9		1	
	mean fit	*k*	mean fit	*k*	mean fit	*k*	mean fit	*k*	mean fit	*k*	mean fit	*k*
1	0.3461	0	0.5324	10	0.5731	9	0.4661	0	0.6168	16	0.5176	5
2	0.4855	0	0.6232	15	0.6377	18	0.5058	0	0.6356	14	0.6210	12
3	0.5146	0	0.6397	19	0.6481	19	0.5438	0	0.6482	18	0.6270	17
4	0.5229	0	0.6482	19	0.6440	18	0.5500	0	0.6523	19	0.6312	19
5	0.5271	0	0.6312	19	0.6523	19	0.5562	0	0.6440	19	0.6312	19
1	0.4486	4	0.5731	6	0.4894	2	0.5313	1	0.4916	0	0.4047	0
2	0.6082	16	0.6085	8	0.5166	1	0.5538	2	0.5751	3	0.3867	0
3	0.6312	19	0.6229	15	0.5501	2	0.5750	3	0.5919	6	0.4098	0
4	0.6312	19	0.6377	18	0.5877	6	0.5854	5	0.6126	12	0.4065	0
5	0.6481	19	0.6461	19	0.6356	15	0.5980	8	0.6503	18	0.3591	0
1	0.5458	6	0.5686	9	0.5522	7	0.5054	6	0.5042	2	0.5710	9
2	0.6022	11	0.6399	17	0.6148	11	0.6294	14	0.5689	2	0.6149	14
3	0.6440	19	0.6544	19	0.6419	16	0.6377	17	0.6086	4	0.6503	19
4	0.6482	19	0.6544	19	0.6293	16	0.6440	17	0.6211	9	0.6312	19
5	0.6482	19	0.6482	19	0.6355	19	0.6481	19	0.6189	11	0.6461	19

2.3 lentelė. Geriausio sprendinio pasikartojimų skaičius (k) ir populiacijos fitnesų vidurkis, kai μ=0.1, N=20

κ	0.5		0.6		0.7		0.8		0.9		1	
	mean fit	k	mean fit	k	mean fit	k	mean fit	k	mean fit	k	mean fit	k
1	0.5362	7	0.1521	0	0.1816	0	0.4953	3	0.3910	0	0.5227	5
2	0.5685	8	0.3786	0	0.2362	0	0.5458	1	0.4834	0	0.6023	11
3	0.5981	10	0.5562	0	0.2508	0	0.5916	3	0.5271	0	0.6273	16
4	0.5958	15	0.5962	0	0.2926	0	0.6044	4	0.5247	0	0.6186	18
5	0.6271	18	0.5749	0	0.3282	0	0.6021	10	0.5270	0	0.6461	18
1	0.5750	6	0.5353	10	0.4725	2	0.4431	3	0.3345	0	0.4018	0
2	0.5894	12	0.6356	18	0.5433	6	0.5795	6	0.4192	0	0.4209	0
3	0.6104	16	0.6399	18	0.5917	10	0.5997	16	0.4228	0	0.4419	0
4	0.6251	18	0.6144	18	0.6273	16	0.6146	17	0.4359	0	0.4732	0
5	0.6335	18	0.6146	17	0.6314	18	0.6378	16	0.4358	0	0.4918	0
1	0.6084	14	0.1943	0	0.5732	9	0.5123	1	0.6064	10	0.4142	0
2	0.6187	18	0.1936	0	0.6105	11	0.5523	2	0.6315	15	0.4215	0
3	0.6334	18	0.2378	0	0.6210	14	0.5836	4	0.6038	17	0.4389	0
4	0.6059	18	0.2690	0	0.6336	18	0.5980	8	0.6378	18	0.4578	0
5	0.6357	18	0.4150	0	0.6187	18	0.6399	14	0.61020	18	0.4641	0

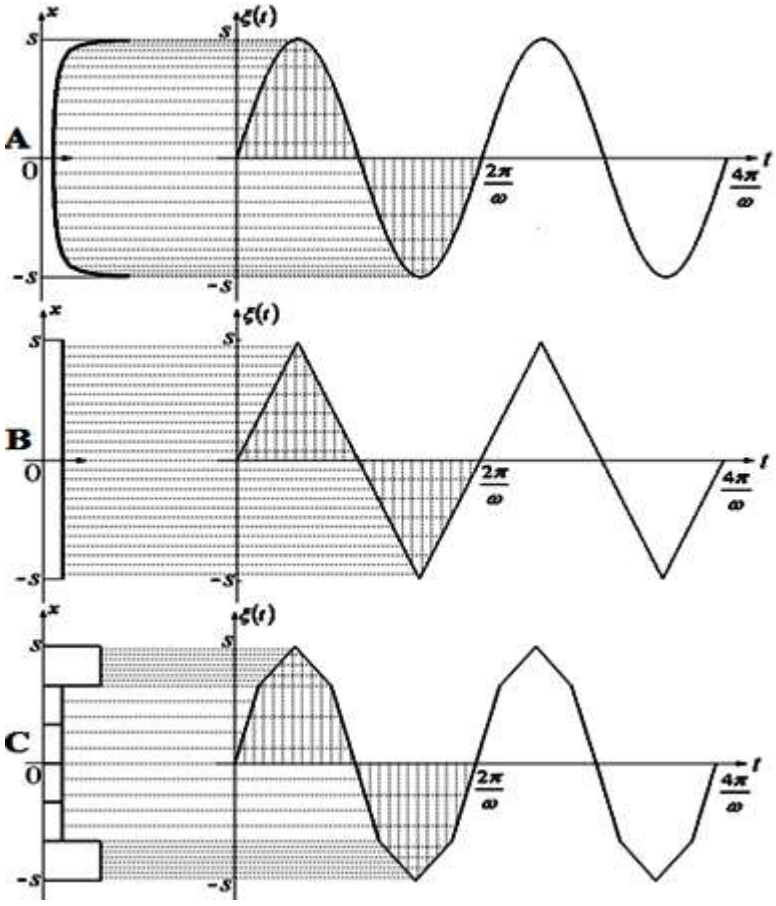
Didžiausias sėkmingų bandymų skaičius ir chromosomų tikslo funkcijos vidurkis gautas, kai κ=0.6 ir μ=0.05 (2.2 lent.). Tokios parametrų reikšmės naudojamos optimalios 24 stulpelių dalimis tolygios tankio funkcijos kai H=60 parinkimo uždavinyje. Tokios apimties uždavinį nerealu išspręsti naudojant pilną perrinkimą: galimų sprendinių kiekis yra $N_\gamma = \frac{(60-12+1)(60-12+2)}{2} = 1225.$

Populiacijos dydis bus 300 chromosomų. Tai sudaro $\frac{N}{N_\gamma} = \frac{300}{1225} \approx 24.49\%$ visų galimų chromosomų skaičiaus. Optimalus sprendinys atrenkamas po 50 generacijų atlikus 5 nepriklausomus bandymus. Beveik optimali svorių γ_i, $i = 1,2,\ldots,n$ aibė yra tokia: $[1;1;1;1;1;1;1;1;2;1;1;48]/120$, atitinkama beveik optimali laiko funkcija $\xi(t)$ pavaizduota 2.2 paveiksle.



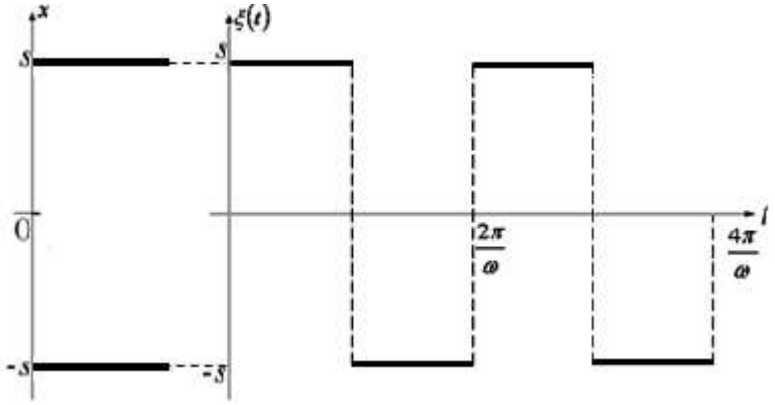
2.2 pav. Beveik optimalios tankio funkcijos, turinčios 24 stulpelius ir H=60, realizacija – laiko funkcija $\xi(t)$

Konstruotas optimizavimo uždavinys apie kodavimo saugumo padidinimą ir gauta, kad geriausias kodavimo saugumas gaunamas kai maksimali būsenų koncentracija yra apie maksimalių atsilenkimų regionus, tada tikslo funkcijos reikšmė yra lygi 0,6565067, o atitinkantis sprendinys (1; 1; 13), harmoninės tankio funkcijos, tikslo funkcijos reikšmė lygi 0,2796672, atitinkantis sprendinys (2; 5; 8), tolydžiojo dydžio tankio funkcijos tikslo funkcijos reikšmė lygi 0,46812697, sprendinys – (5; 5; 5). Paveiksle 2.3 matome skirtingo tipo funkcijų $\xi_s(t)$ ir atitinkamų tankio funkcijų $p_s(x)$ realizacijas.



2.3 pav. Skirtingo tipo funkcijų $\xi_s(t)$ ir atitinkamų tankio funkcijų $p_s(x)$ realizacijos: (A) harmoninė tankio funkcija, (B) tolydaus tankio funkcija, (C) dalimis tolydi tankio funkcija

Geriausias rezultatas gaunamas, kai daugiausia laiko procesas praleidžia maksimalių atsilenkimų zonoje, galima teigti, kad geriausias rezultatas bus tada, kai virpesių dėsnis bus stačiakampio bangos formos signalas (2.4 pav).



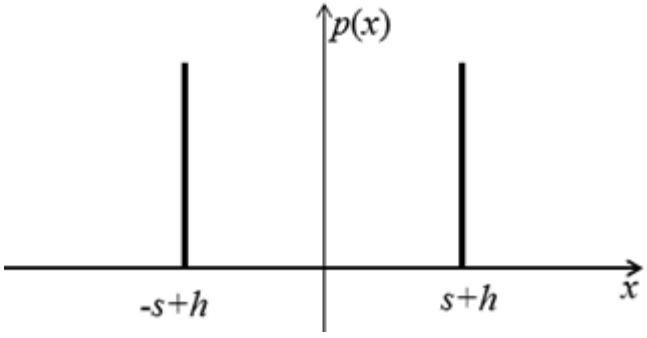
2.4 pav. Stačiakampio bangos formos signalas

Skaičiavimai parodė, kad optimali tankio funkcija įgyja maksimalias reikšmes, kai $x = s$ ir $x = -s$. Ribinė tankio funkcija tada yra tokia:

$$p(x) = \frac{1}{2} \cdot \delta_{-s}(x) + \frac{1}{2} \cdot \delta_s(x) \tag{2.16}$$

čia $\delta_{x_0}(x)$ – impulsinė delta funkcija, tenkinanti reikalavimus:

$$\delta_{x_0}(x) = \begin{cases} +\infty, \text{ kai } x = x_0; \\ 0, \text{ kitaisatvejais} \end{cases} \text{ ir } \int_{-\infty}^{\infty} \delta(x) = 1. \tag{2.17}$$



2.5 pav. Impulsinės delta funkcijos tankio funkcija

Paveikslėlyje 2.5 pavaizduota tankio funkcija, kuri susideda iš dviejų stulpelių, kurių kiekvieno aukštis $y = \frac{1}{2h}$ priklauso nuo parametro *h*, $h \to 0$, kai $y \to +\infty$. Tokios funkcijos Furjė transformacija yra randama:

$$\int_{-s}^{-s+h} e^{-i\Omega x}\cdot\frac{1}{2h}dx+\int_{s-h}^{s} e^{-i\Omega x}\cdot\frac{1}{2h}dx=-\frac{1}{2hi\Omega}\left(e^{-i\Omega x}\Big|_{-s}^{-s+h}+e^{-i\Omega x}\Big|_{s-h}^{s}\right)=$$

$$=-\frac{e^{i\Omega s}}{2i\Omega}\cdot\frac{e^{-i\Omega h}-1}{h}-\frac{e^{-i\Omega s}}{2i\Omega}\cdot\frac{1-e^{i\Omega h}}{h}$$

Skaičiuojama riba kai $h\to 0$:

$$-\frac{e^{i\Omega s}}{2i\Omega}\lim_{h\to 0}\frac{e^{-i\Omega h}-1}{h}-\frac{e^{-i\Omega s}}{2i\Omega}\lim_{h\to 0}\frac{1-e^{i\Omega h}}{h}=-\frac{e^{i\Omega s}}{2i\Omega}\left(-i\Omega\right)-\frac{e^{-i\Omega s}}{2i\Omega}\left(-i\Omega\right)=$$

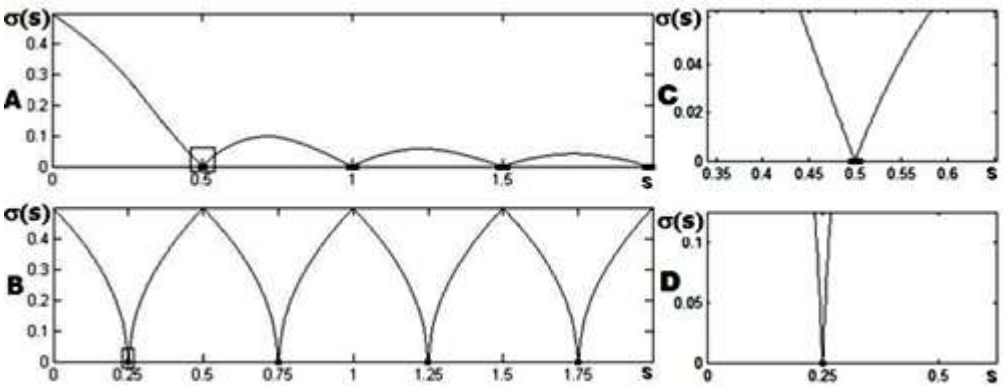
$$=\frac{e^{i\Omega s}+e^{-i\Omega s}}{2}=\cos(s\cdot\Omega)$$

Taigi ribinės tankio funkcijos Furjė transformacija yra

$$P_s(\Omega)=\int_{-\infty}^{+\infty}\left(\frac{1}{2}\cdot\delta_{-s}(x)+\frac{1}{2}\cdot\delta_s(x)\right)e^{-ix\Omega}dx=\cos(s\cdot\Omega) \qquad (2.18)$$

ir pirmoji interferencinė juosta susiformuoja, kai $s=\lambda/4$.

Laike vidurkintų interferencinių juostų formavimosi standarto funkcijų esant „zig-zag“ tipo ir stačiakampio formos virpesiams palyginimas pateiktas 2.6 paveiksle. Juodais storais brūkšniais, pažymėtos sritys, kuriose formuojasi interferencinės juostos. Aiškiai matoma, kad amplitudės nuokrypio intervalas yra siauresnis esant stačiakampio formos virpesiams. Vadinasi šiuo atveju informacija yra slepiama geriau.

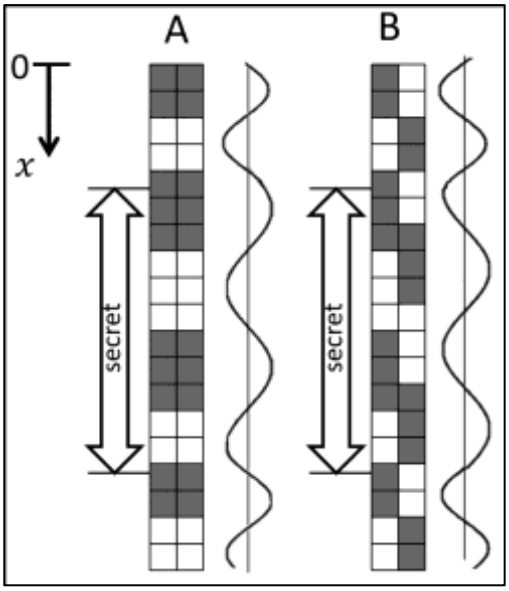


2.6 pav. Laike vidurkintų interferencinių juostų formavimosi standarto funkcijų grafikai. (A) – „zig-zag‘ tipo virpesiai, (B) – stačiakampio formos virpesiai, (C) – išdidintas intervalas kuriam esant dar formuojasi interferencinės juostos, esant „zig-zag“ formos virpesiams, (D) – intervalas kuriam esant dar formuojasi interferencinės juostos, esant stačiakampio formos virpesiams

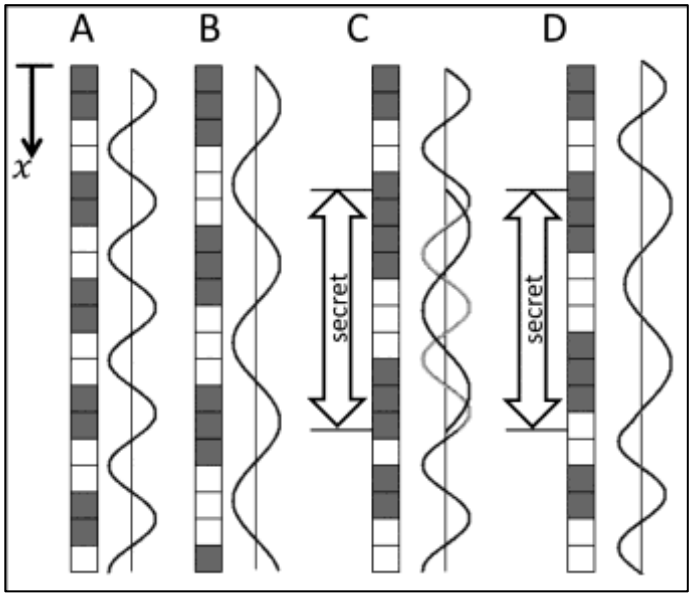
2.3. Slapto vaizdo kodavimo algoritmas

Slaptų vaizdų kodavimas atliekamas atsižvelgiant į gardelės funkciją 0.5 + 0.5cos(*x*). Ši funkcija tinka tiek fono gardelei, tiek slaptosios informacijos

gardelei aprašyti. Be to šią funkciją labai lengva transformuoti į juodai – baltų pikselių gardelę. Pirmiausiai parenkamas slaptasis vaizdas kurį reikia užkoduoti. Nustatoma koks gardelės periodas bus naudojamas fonui λ_1 ir koks slaptam vaizdui λ_2. Vaizdas yra koduojamas atskiruose vaizdo stulpeliuose – visi stulpeliai sudaro dvimatį užkoduotą paveikslą. Kiekvieno vaizdo stulpelio pradžioje pridedame po atsitiktinį dydį (atliekamas stochastinis pradinės fazės postūmio algoritmas). Šis dydis reikalingas tam, kad nebūtų galima vizualiai, be jokių virpesių matyti užkoduoto vaizdo. Tokiu būdu yra „išdarkomas“ visas dvimatis paveikslas, išnyksta fono ir slaptojo vaizdo sandūros kontūrai. Paprastai kodavimas pradedamas įterpiant fono gardelę. Šio reikalavimo galima būtų ir nepaisyti, jei tik koduojamas vaizdas paveikslo pakraščiuose būtų „riebus“, priešingu atveju, dėl virpesių „išsiplautų“ smulkios slaptojo vaizdo detalės. 2.7 paveiksle pateikta pradinių fazių stochastinio postūmio algoritmo iliustracija. Paveikslo A dalyje pavaizduoti du koduoti pikselių stulpeliai, išskirta sritis kurioje įterpta slapta informacija, ji koduojama parinkus gardelės žingsnį λ_2. Taip užkoduotame vaizde gali išryškėti slepiamas vaizdas. 2.7 pav. B dalyje matomi du koduoti pikselių stulpeliai jau po postūmio: pirmasis stulpelis liko savo vietoje, o antrasis buvo paslinktas per dvi pozicijas. Taip koduojant paveikslui esant statinėje padėtyje jokios informacijos nebus galima įžvelgti. Papildomai yra naudojamas ir fazių reguliarizacijos algoritmas (2.8 pav.), kuriame įvertinamas funkcijos fazių neatitikimas kai yra pereinama iš fono į slaptąjį vaizdą ir atvirkščiai. Šis algoritmas yra būtinas, kadangi jo nepritaikius iš karto matosi vietos, kuriose įterptas slaptasis vaizdas.



2.7 pav. Pradinių fazių stochastinio postūmio algoritmo iliustracija: A – stulpeliai prieš postūmį, B – stulpeliai po postūmio



2.8 pav. Fazių reguliarizacijos algoritmo iliustracija. A – stulpelis skirtas fonui koduoti, B – slaptam vaizdui, C – koduoto vaizdo stulpelis, D – koduoto vaizdo stulpelis po fazių reguliarizacijos algoritmo

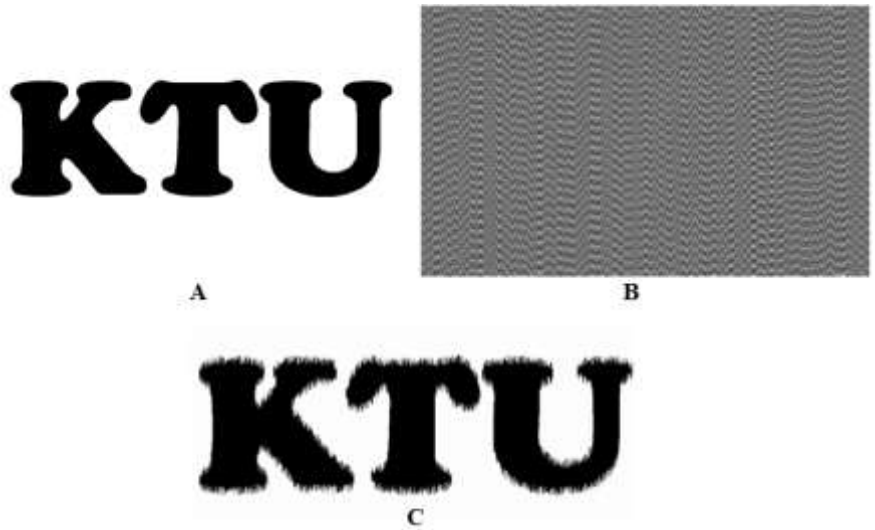
2.8 paveikslo A dalyje pavaizduotas vertikalus pikselių stulpelis skirtas fonui koduoti ($\lambda_1 = 2$), o B dalyje matomas pikselių stulpelis skirtas slaptai informacijai koduoti ($\lambda_1 = 3$). 2.8C pav. į fono stulpelį įterptas slaptas vaizdas, atsiranda pikselių nesuderinamumas ir dėlto gali išsiskirti vietos kuriose įterptas slaptas vaizdas. Atliekamas fazių reguliarizacijos algoritmas ir 2.8D paveiksle pavaizduotas koduotas pikselių stulpelis atlikus algoritmą.

2.4. Skaitiniai eksperimentai

Skaitiniai rezultatai, gauti panaudojant dinaminės kriptografijos schemą su gauta laiko funkcija, realizuojami naudojant 2.9A paveiksle pateiktą informaciją. Slaptas vaizdas užkoduojamas laiptuota muaro gardele (2.9B pav.), kurios žingsnis 1.56 mm, naudojant fazių reguliarizacijos ir stochastinio postūmio algoritmus. Fonui koduoti parenkama muaro gardelė, kurios žingsnis 1.42 mm.

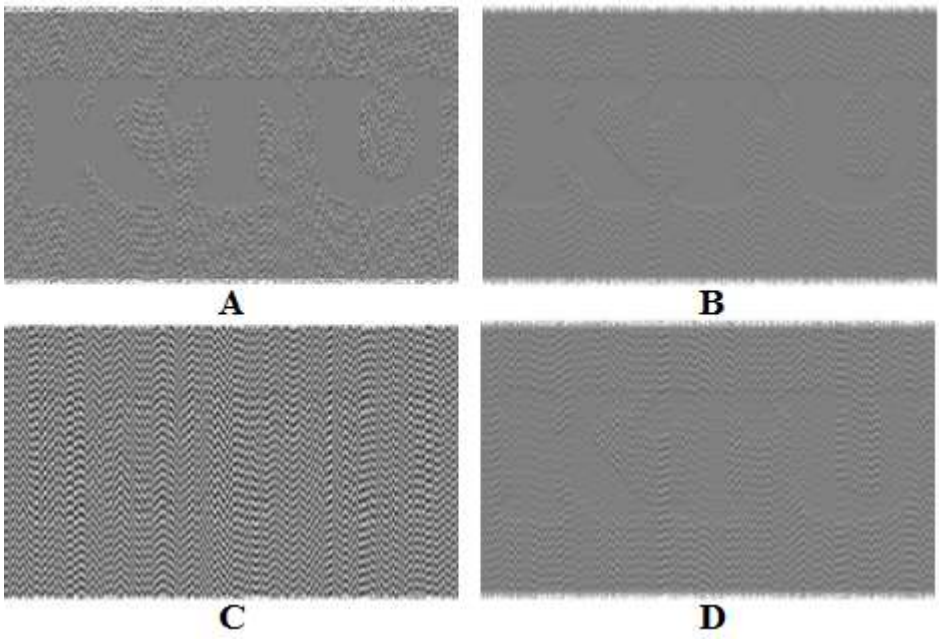
Slaptas vaizdas dekoduojamas naudojant optimalią laiko funkciją, parodytą 2.2 paveiksle, ir virpesių amplitudę $s = \lambda / 4 = 0.39\text{mm}$ (dekoduotam vaizdui paryškinti naudotas kontrasto didinimo algoritmas [73]), išryškintas dekoduotas vaizdas matomas 2.9C paveiksle.

Jei koduotas paveikslas virpinamas tangentine kryptimi atžvilgiu jo paviršiaus, esant virpesių amplitudei $s = 0.78$ mm „zig-zag“ (2.10B pav.) ir stačiakampio formos (2.10A pav.) virpesiais ($s = 0.39$ mm), tai slapta informacija išryškėja.



2.9 pav. Slaptas vaizdas (A), slaptas vaizdas užkoduotas laiptuota muaro gardele (B), dekoduotas išryškintas vaizdas (C)

Tačiau vienodu dydžiu pakeitus „zig-zag“ formos ir stačiakampio formos virpesių amplitudes, slaptas vaizdas vis dar bus matomas virpinant „zig-zag“ (2.10D pav.) virpesiais ($s = 0.80$ mm). Nors ir nedaug pakitus stačiakampio formos virpesių amplitudei ($s = 0.41$ mm) slaptos informacijos pamatyti nepavyks (2.10C).



2.10 pav. Koduoto paveikslo dekodavimas: A virpinama tinkamos amplitudės stačiakampiais virpesiais; B – „zig-zag” tipo virpesiais, tinkama amplitude; C – stačiakampiais virpesiais, bloga amplitude; D – „zig-zag” tipo virpesiai, amplitudė vis dar tinkama

2.5. Skyriaus išvados

Remiantis dinaminės vizualizacijos metodais, panaudojus genetinius algoritmus rasta optimali laiko funkcija, užtikrinanti užkoduoto paveikslo saugumą. Optimalumo kriterijus čia pagrįstas suvidurkinto paveikslo standarto išvestine. Parodyta, kad ekstremalių nuokrypių nuo pusiausvyros padėties sąveika gali būti laikoma beveik optimalia laiko funkcijos realizacija ir tuo pačiu panaudojama skaitiniuose dinaminės vizualinės kriptografijos eksperimentuose. Atlikus skaitinius eksperimentus įsitikinta, kad vaizdą jo paviršiaus atžvilgiu virpinant tangentine kryptimi, stačiakampio formos virpesiais esant net nedideliam virpesių amplitudės pokyčiui slapta informacija koduotame vaizde neišryškės. Gautas virpesių dėsnis nesunkiai gali būti realizuotas skaitmeniniuose kompiuterių ekranuose ir panaudotas penktame skyriuje aprašytam žmogaus regos sistemos tyrimų įrenginiui konstruoti.

3. DINAMINĖS KRIPTOGRAFIJOS PANAUDOJIMAS VIBRUOJANČIOS ĮRANGOS KONTROLEI

Dinaminės kriptografinės sistemos veikimas nepriklauso nuo virpesių dažnių, nors dažnis turi būti pakankamai didelis, kad į ekspozicijos intervalą tilptų pakankamas virpesių periodų skaičius. Ši metodika gali būti taikoma optinei trumpalaikių virpesių kontrolei, jei tik tų virpesių amplitudė yra pastovi. Pavyzdžiui, viena iš tokių situacijų gali susidaryti sukantis turbinai, kai sukimosi dažnis palaipsniui didėja. Pagrindinai veiksniai lemiantis laike vidurkintų interferencinių muaro juostų formavimąsi yra virpesių amplitudė ir signalo generuojama virpesių bangos forma. Ši sistema būtų gera, jei virpesių amplitudė viso proceso metu būtų pastovi.

Šiame skyriuje nagrinėjama nesudėtinga, bet efektyvi optinė metodika, kuri gali būti panaudota prietaisų ar įrengimų parametrų kontrolei įvertinti. Užšifruotas vaizdas matomas plika akimi kai vibrostendas dirba reikiamu režimu. Toks nesudėtingas vaizdinis patikrinimas yra pakankamas judesio amplitudės ir virpesių dėsnio nustatymui. Skyriuje aptariami teoriniai sąryšiai, aprašoma eksperimente naudojama įranga, eksperimento realizacija ir rezultatai esant skirtingo tipo virpesiams.

3.1. Teorinis pagrindimas

Interferencinių juostų formavimasis nagrinėjamas vienmačio pavyzdžio pagalba. Muaro gardelę pusiausvyros būsenoje galima interpretuoti kaip pasikartojančią baltos ir juodos spalvų variaciją:

$$F(x)=\frac{1}{2}+\frac{1}{2}\sin\left(\frac{2\pi}{\lambda}x\right) \tag{3.1}$$

čia x – išilginė koordinatė; $F(x)$ yra pilkio spalvos lygis taške x; λ – gardelės žingsnis; reikšmė 0 atitinka juodą spalvą; reikšmė 1 atitinka baltą spalvą; tarpinės reikšmės – atitinkamo pilkio lygio spalvas.

Laike vidurkintas geometrinis muaras yra optinis eksperimentinis metodas kai muaro gardelė formuojama ant vibruojančio kūno paviršiaus. Paviršiui vibruojant susiformuoja laike vidurkintos interferencinės juostos [65]. Muaro gardelės nuokrypis nuo pusiausvyros padėties laike kinta pagal harmoninį dėsnį:

$$u(t)=s\sin(\omega t+\varphi) \tag{3.2}$$

čia ω yra dažnis, φ – fazė, s – virpesių amplitudė. Šiuo atveju vienmatis laike vidurkintas vaizdas yra aprašomas pagal formulę [61][64]:

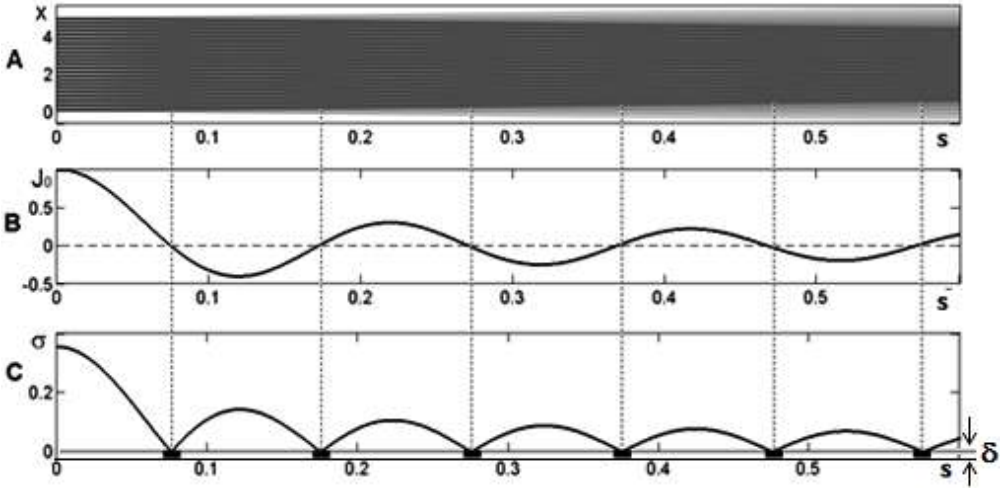
$$H_S(x|F;u)=\lim_{T\to\infty}\frac{1}{T}\int_0^T F(x-s\sin(\omega t+\varphi))dt=\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)J_0\left(\frac{2\pi}{\lambda}s\right) \tag{3.3}$$

čia H_s yra laike vidurkinimo operatorius [64], J_0 – pirmojo tipo nulinės eilės Beselio funkcija.

Laike vidurkintos interferencinės muaro juostos formuosis tada kai amplitudės s reikšmė bus lygties $J_0(2\pi s/\lambda)=0$ sprendinys. Taigi, sąryšis tarp interferencinės juostos eilės, harmoninių virpesių amplitudės ir muaro gardelės žingsnio yra:

$$\frac{2\pi}{\lambda}s_i = r_i;\ i=1,2,\ldots \tag{3.4}$$

čia r_i žymi nulinės eilės pirmo tipo Beselio funkcijos i-ją šaknį; s_i yra virpesių amplitudė i-tosios interferencinės juostos centre. Laike vidurkintų interferencinių juostų formavimasis pavaizduotas 3.1 paveiksle. Daroma prielaida, kad $s(x) = x$; muaro gardelė formuojama intervale kai $0 \le y \le 5$ ir $x = 0$, paveiksle pateikto vaizdo muaro gardelės žingsnis lygus 0.2. Muaro gardelė aiškiai matoma kairėje laike vidurkinto vaizdo pusėje, kuri užpilkėja prie tokios harmoninių virpesių amplitudės, kada moduliuojama pirmo tipo nulinės eilės Beselio funkcija įgyja pirmąją šaknį, tai gaunama remiantis (3.3) formule. Laike vidurkintos interferencinės juostos formuojasi maždaug tose srityse kai virpesių amplitudė tinka (3.4) formule aprašytai lygčiai. Virpesių dažnis neturi įtakos laike vidurkintų juostų formavimuisi be to ekspozicijos laikas turėtų būti pakankamai ilgas, kad jame tilptų pakankamai daug virpesių periodų.



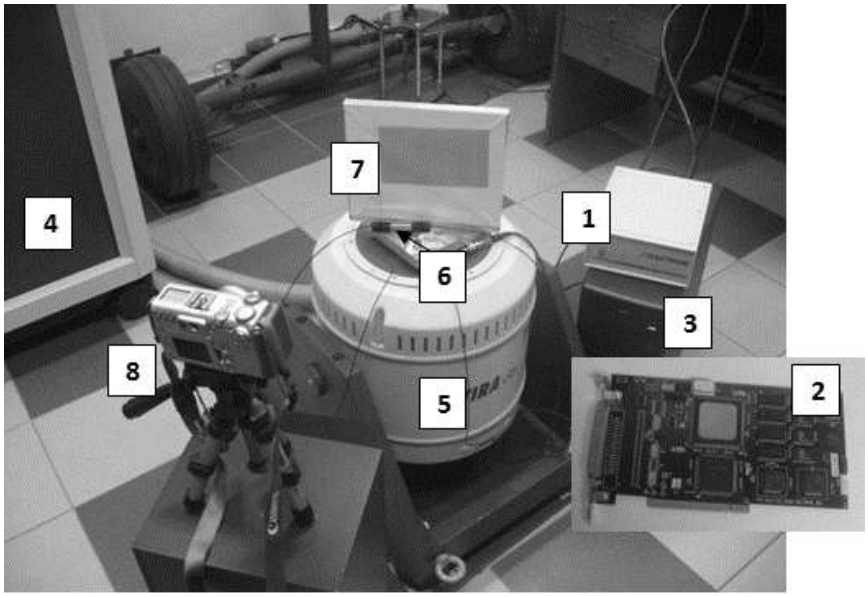
3.1 pav. Susiformavusios laike vidurkintos interferencinės juostos (A); pirmo tipo nulinės eilės Beselio funkcija (B); laike vidurkintų muaro interferencinių juostų standarto funkcija (C); gardelės žingsnis λ=0.2

Galimybė interpretuoti interferencines muaro juostas plika akimi yra naudojama kodavimo metode, paremtame vizualines kriptografijos principais ir laike vidurkintomis geometrinėmis muaro juostomis [1, [64]. Slaptas vaizdas užkoduojamas panaudojant harmoninę muaro gardelę. Panaudojant fazių reguliarizacijos algoritmą panaikinamos ribos tarp fono ir slapto vaizdo koduotame paveikslėlyje. Pritaikius pradinės stochastinių fazės postūmių algoritmą gaunamas vienas paveikslas, kuriame užkoduota informacija, ji išryškės paveikslą virpinant nustatyta kryptimi ir žinant tikslią amplitudės reikšmę. Teoriškai reiktų, kad

poveikis truktų ilgą laiką, praktiškai užtenka, kad laiko intervale tilptų pakankamas virpesių periodų skaičius [61] [66]. Šiuo atveju virpesių dažnis neturi įtakos laike vidurkintų interferencinių juostų formavimuisi, nepaisant to, reiktų naudoti pakankamai aukšto dažnio virpesius, kad žmogaus akis spėtų sekti vibruojančio vaizdo judesius.

3.2. Eksperimentinė įranga

Praktiniam eksperimentui atlikti buvo naudojama virpesių generavimo įranga, kurios schema pavaizduota 3.2 paveiksle. Skaičiais pažymėtos pagrindinės įrangos dalys.



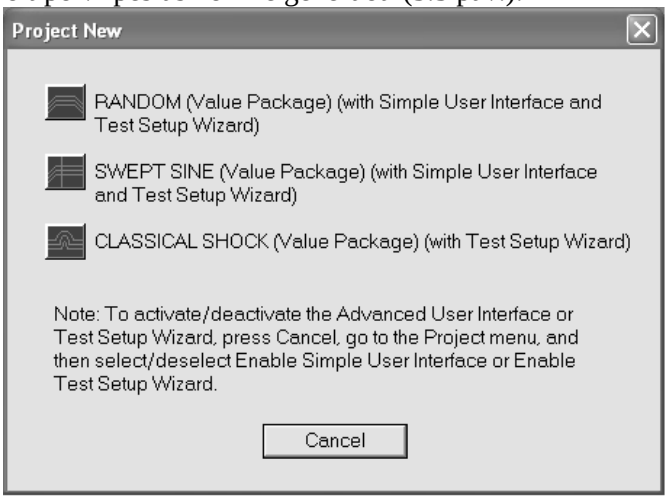
3.2 pav. Virpesių generavimo įrangos schema

1. Valdiklio *DACTRON COMET DSP* signalo išėjimo ir įėjimo įrenginys.
2. DSP plokštė, kuri montuojama į kompiuterį.
3. Personalinis kompiuteris.
4. Vibrostendo valdymo skydas (*TYRA*).
5. Vibrostendas (*TYRA).*
6. Akcelerometras.
7. Eksperimente naudojamas koduotas paveikslėlis.
8. Skaitmeninis fotoaparatas rezultatams fiksuoti.

Kontroleris Dactron *COMET* susideda iš trijų dalių: *DSP* signalo išėjimo ir įėjimo įrenginio, *PCI DSP* plokštės ir *Windows* aplinkai pritaikytos programinės įrangos. Virpesių generavimą, matavimą, analizę ir registravimą atlieka *DSP* įrenginys. Ryšį tarp kompiuterio ir *DSP* įrenginio palaiko *PCI DSP* plokštė, kuri įmontuota kompiuterio viduje. Windows aplinkoje veikiančios programinės įrangos pagalba parenkami pradiniai duomenys, jie siunčiami į signalų išėjimo *DSP* įrenginį, vaizduojami ekrane, saugomi kompiuteryje. Programinė įranga tikrina sistemos veikimą ir esant nesklandumams stabdo darbą. Vartotojo pasirinkti signalai

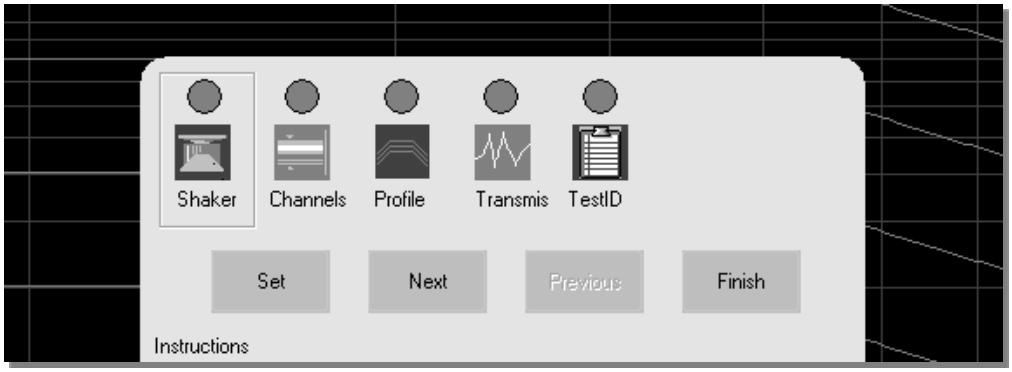
DSP signalų išėjimo įrenginio pagalba siunčiami į vibrostendo valdymo skydą, ten apdorojami ir siunčiami į vibrostendą. Taip gaunami virpesiai, kurių reikia eksperimentui atlikti. Eksperimento rezultatai fiksuojami skaitmeniniu fotoaparatu. Akcelerometras reikalingas kontrolei, norint įsitikinti, kad vibrostendas tikrai vibruoja pagal pasirinktą dėsnį. Jis siunčia signalus į *DSP* signalų įrenginį, juos gavusi programinė įranga patikrina gautus duomenis ir ekrane pavaizduoja rezultatus.

Kontroleris gali generuoti, valdyti, apdoroti harmoninius, atsitiktinius ir smūginius signalus. Prieš sukuriant naują projektą reikia programos dialogo lange pasirinkti kokio tipo virpesius norime generuoti (3.3 pav.).



3.3 pav. Atsitiktinių, harmoninių ar smūginių signalų pasirinkimo langas

Prieš pradedant darbą su kontroleriu reikia nustatyti bendrus programos parametrus, kurie panašūs visiems skirtingo tipo virpesiams (3.4 pav.).



3.4 pav. Penki žingsniai iki projekto sukūrimo.

Parametrų nustatymas susideda iš penkių etapų:

- Shaker (stendo parametrai);
- Channels (įvesties ir išvesties kanalų parametrai);
- Profile (vaizdo parametrai);

- Transmissibility signals (perdavimų signalai);
- TestID (testo identifikacija);

Stendo parametrų dialogo lange leidžiama nustatyti saugias darbo ribas, kad nuo pažeidimų ir perkrovos būtų apsaugota vibrostendo sistema. Visi nustatyti parametrai bus patikrinti prieš atliekant bandymą, jei parametrai viršys leidžiamas vibrostendo ribas, bandymas nebus atliekamas arba vykdymas bus automatiškai nutrauktas. Skirtingiems virpesiams (atsitiktiniams, harmoniniams ar smūginiams) parenkami skirtingi įverčiai, atitinkantys nustatytas ribas.

Po stendo parametrų nustatomi signalų įvesties ir išvesties kanalų parametrai. Jie bus naudojami atliekamuose eksperimentuose.

Toliau gaunama *Profile* (vaizdo) kortelė. Joje pateikiama dažnių – pagreičių diagrama, kurią esant poreikiui galima pakeisti, taip pat šiame etape parenkamos profilio ribinės reikšmės ir apibūdinamas reikšmių spektras.

Ketvirtame etape gauname kortelę *Transmissibility signals*. Šiame etape apibrėžiami perdavimo signalai. Galima pasirinkti įvesties kanalą ir kontrolę.

Paskutinis etapas skirtas testo identifikavimui ir dokumentacijai. Platesnis eksperimentinės įrangos naudojimo aprašas, esant skirtingo tipo virpesiams pateiktas 1 priede.

3.3. Eksperimentinė realizacija

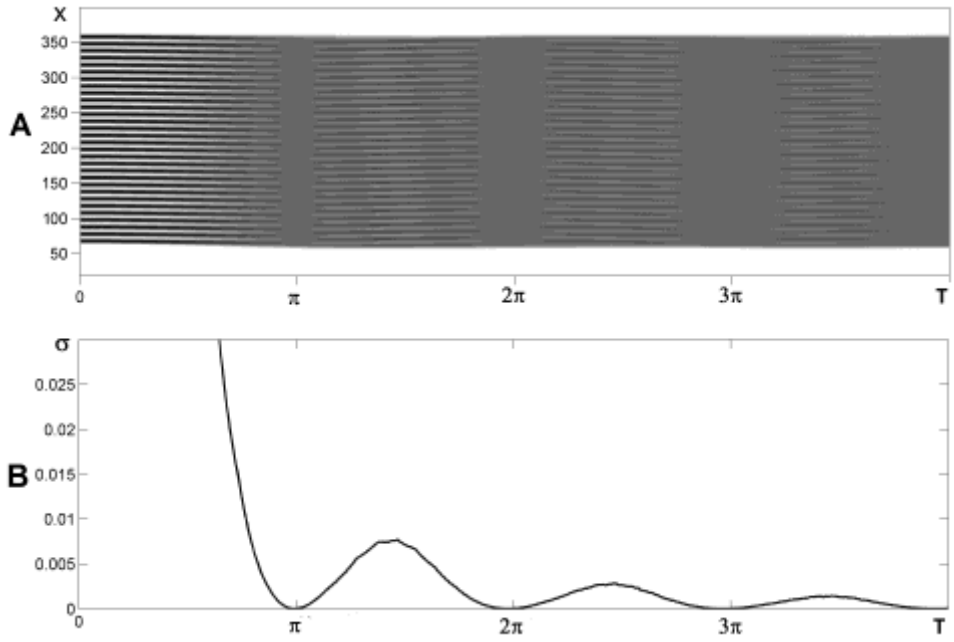
Virpinamo slapto vaizdo dekodavimas pagrįstas optiniu laike vidurkinimo metodu. Koduotas paveikslas gali būti tvirtinamas ant tvirto nesideformuojančio kūno paviršiaus, kuris veikiamas periodiniais virpesiais. Šiam eksperimentui reikalingą įrangą sudaro vibrostendas ir paprastas skaitmeninis fotoaparatas (3.5 pav.).

3.5 pav. Bendras eksperimento vaizdas.

Koduotas vaizdas yra atspausdinamas paprastu skaitmeniniu spausdintuvu ir užklijuojamas ant tvirtos konstrukcijos, kuri pritvirtinta prie vibrostendo. Svarbu patikrinti, kad konstrukcija būtų tvirta ir ją virpinant neatsirastų pašalinių nepageidaujamų virpesių, vizualinis dekodavimas pagrįstas plokštuminiais periodiniais virpesiais.

Kaip rodo teoriniai rezultatai, virpesių dažnis neturi įtakos laike vidurkintų juostų susiformavimui. Vis dėl to šis parametras svarbus norint plika akimi pamatyti susiformavusias interferencines juostas. Fiksuojant dekoduotą vaizdą skaitmenine fotokamera reikia, kad ekspozicijos laike tilptų pakankamas virpesių periodų skaičius.

Pilkio lygių standarto $\sigma(H_s F(x))$ laike vidurkintame paveikslėlyje sąvoka aprašyta [68] straipsnyje, yra svarbi interferencinių juostų formavimosi paaiškinimui. Laike vidurkinto vaizdo standartinis nuokrypis yra svarbus ir kaip baigtinio ekspozicijos laiko sukeltų galimų klaidų įvertinimas. Tam nustatoma amplitudės reikšmė, prie kurios formuojasi pirmoji interferencinė juosta: $s_1 = r_1 \frac{\lambda}{2\pi}$. Pagal (3.3) formulę apskaičiuojamo vidurkinimo operatoriaus reikšmė $H_{s_1}(x|F;u) = 0.5$, kur funkcija $F(x)$ yra gaunama pagal (3.1) formulę, o ekspozicijos laikas artėja į begalybę. Apskaičiuojamas apibrėžtinis integralas $\frac{1}{T}\int_0^T F(x - s_1 \sin(\omega t + \varphi))dt$ ir prie skirtingų ekspozicijos laiko T reikšmių gauti rezultatai pavaizduojami 3.6 paveiksle.



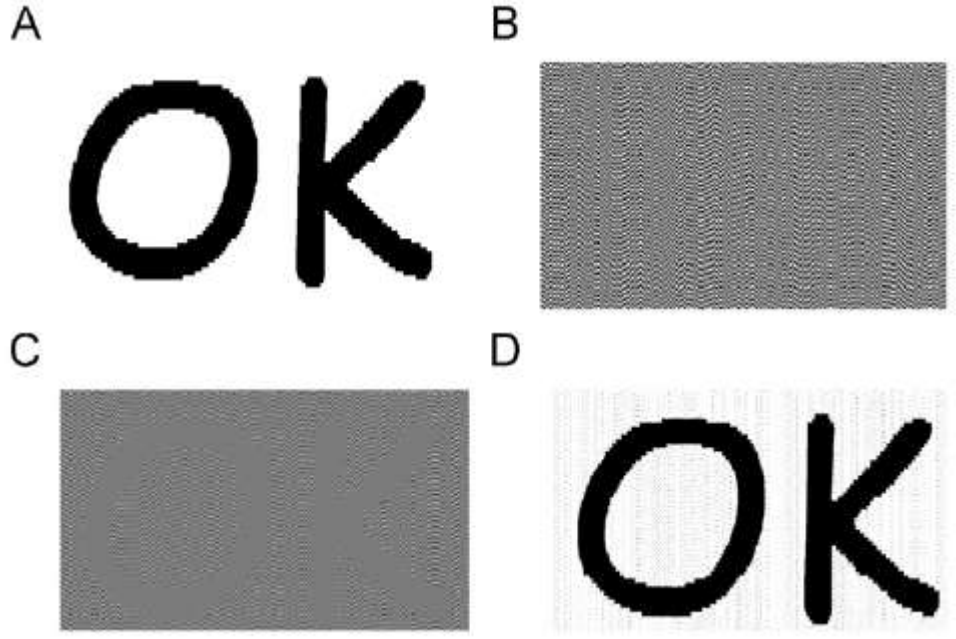
3.6 pav. Laike vidurkintų interferencinių juostų susidarymas (A) ir pilkio lygio standartinis nuokrypis (B) laikui artėjant į begalybę.

Tampa aišku, kad dėl baigtinio ekspozicijos laiko atsirandantys netikslumai mažėja, jei ekspozicijos laike T telpa daugiau nei 10 harmoninių virpesių periodų.

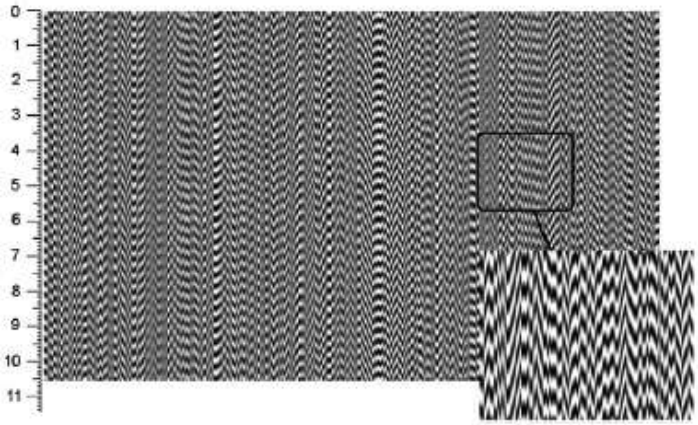
Parenkamas virpesių dažnis lygus 60 Hz, o ekspozicijos laikas T=1/15 s. Į šį ekspozicijos laiką telpa maždaug 4 virpesių periodai. Ekspozicijos laiko intervalo

pradžioje ar pabaigoje galimas nežymus virpesių periodo nuokrypis, tačiau jis neturi jokios reikšmės pačiam vidurkinimo procesui. Slaptas vaizdas pavaizduotas 3.7A paveiksle; harmonine muaro gardele užkoduotas paveikslas pavaizduotas 3.7B paveiksle. Skaitmeniniu būdu dekoduotas vaizdas matomas 3.7 paveikslo C dalyje, koduotas paveikslas buvo virpinamas harmoniniu dėsniu $u(t)$. laike vidurkintos interferencinės juostos aiškiai matomos slapto vaizdo vietose. 3.7 paveikslo D dalyje pateiktas skaitmeniniu būdu išryškintas (panaudojus kontrasto didinimo algoritmą) dekoduotas vaizdas.

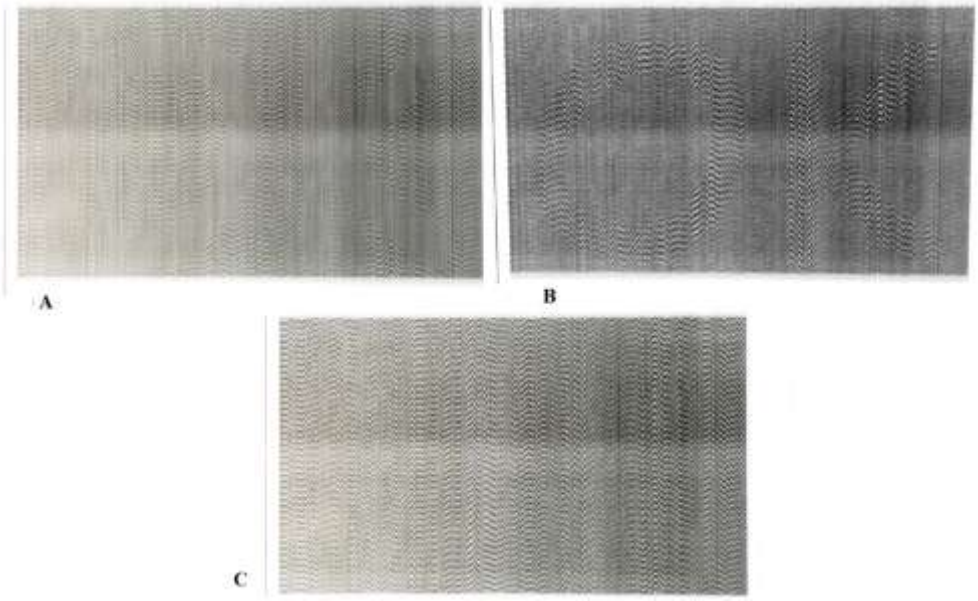
Spausdintuvu atspausdintas koduotas vaizdas, kuris tvirtinamas ant vibrostendo pagrindo pavaizduotas 3.8 paveiksle. Fono kodavimui parinkta muaro gardelė, kurios žingsnis 0.2292 mm; slaptas vaizdas koduojamas naudojant muaro gardelę, kurios žingsnis 0.2645 mm. Laike vidurkinti vaizdai, gauti praktinio eksperimento metu, kai vibrostendas generuoja harmoninius virpesius, kurių amplitudės yra s=0.1012 mm $\left(J_0\left((2\pi/0.2645)\cdot 0.1012\right)=J_0\left(r_1\right)=0\right)$ ir s=0.0877 mm $\left(J_0\left((2\pi/0.2292)\cdot 0.0877\right)=J_0\left(r_1\right)=0\right)$, pavaizduoti 3.9A ir 3.9B paveiksluose; slaptas vaizdas abiejuose vaizduose matomas plika akimi. Plika akimi matomi vaizdai yra ryškesni nei užfiksuoti skaitmenine kamera, taip yra dėl palyginus trumpo ekspozicijos laiko. Parinkus netinkamą amplitudę (s=0.0938 mm) slaptas vaizdas neišryškės, interferencinės juostos nesiformuoja (3.9C pav.).



3.7 pav. Koduojamas slaptas vaizdas (A); vaizdas užkoduotas panaudojus muaro gardelę (B); skaitmeniniu būdu dekoduotas slaptas vaizdas (C) ir panaudojus kontrasto padidinimo algoritmą gautas slaptas vaizdas (D)



3.8 pav. Atspausdintas koduotas vaizdas (išdidintoje paveikslo dalyje matoma muaro gardelės struktūra)



3.9 pav. Laike vidurkintas paveikslas: muaro interferencinės juostos susiformavo žodyje „OK“ (A); interferencinės juostos susiformavo fone (B); blogai parinkta amplitudė, vaizdas nesimato (C)

3.4. Metodo jautrumas

Šio metodo jautrumas priklauso nuo tai, koks muaro gardelės žingsnis parinktas fonui, o koks slaptai informacijai koduoti. Fonui parenkama muaro gardelė, kurios periodas λ_0, o slaptam vaizdui λ_1 (nagrinėjamas atvejis, kai koduojamas tik vienas slaptas vaizdas). Tada, laike vidurkintos interferencinės juostos formuosis fone, kai koduotas paveikslas virpinamas harmoniniais virpesiais, o virpesių amplitudė yra viena iš diskrečių reikšmių tenkinančių lygybę:

$$s_i = r_i \frac{\lambda_0}{2\pi}; i = 1,\ 2, \ldots \tag{3.5}$$

Atitinkamai, laike vidurkintos interferencinės juostos formuosis slaptame vaizde, kai paveikslas bus virpinamas harmoniniais virpesiais, o virpesių amplitudė bus viena iš reikšmių:

$$b_i = r_i \frac{\lambda_1}{2\pi}; i = 1,\ 2, \ldots \tag{3.6}$$

Geriausiai slapta informacija būtų užkoduota jei λ_1 būtų beveik lygus λ_0. Tačiau, tokiu atveju optinis slapto vaizdo dekodavimas taptų sudėtingas, o gal ir neįmanomas. Vietoj to, nagrinėjama kitokia situacija, kai λ_1 reikšmė yra kiek įmanoma toliau nuo λ_0 reikšmės. Dekoduojant tokį paveikslą, tarp slapto vaizdo ir fono gaunamas didžiausias kontrastas. Yra žinoma, kad nulinės eilės pirmo tipo Beselio funkcijos šaknys yra neperiodinės. Tačiau, tai nesvarbu, jei b_1 reikšmė imama iš intervalo $[s_1; s_2]$ vidurio. Tada $b_1 = 0.5(s_1 + s_2)$, kai:

$$\lambda_1 = \frac{r_1 + r_2}{r_1} \lambda_0 \tag{3.7}$$

Kitaip sakant, efektyviausias amplitudės pokytis Δs yra toks kai aiškiai pastebima, kada laike vidurkintos interferencinės juostos formuojasi fone, o kada jau slapto vaizdo vietoje. Ši reikšmė yra lygi:

$$\Delta s \approx b_1 - s_1 = \frac{r_2}{2\pi} \lambda_0 \approx 0.878 \lambda_0 \tag{3.8}$$

Įprasti skaitmeniniai spausdintuvai kokybiškai spausdina muaro gardeles, kai milimetre telpa iki dviejų linijų (didesnė kokybė būtų pasiekiama specializuotose spausdintuvuose). Nėra sunku pasiekti, kad Δs būtų mažesnis nei 0.5 mm.

Šis metodas yra grindžiamas vizualinės kriptografijos principais. Vadinasi, turi būti tiksliai nustatyta virpesių amplitudė, kad galėtumėme vizualiai dekoduoti paveikslą. Geriausias santykis tarp harmoninių virpesių amplitudės ir standartinio nuokrypio laike vidurkintame paveiksle, kai kodavimui parinkta harmoninė muaro gardelė, aprašytas [68] (3.1C pav.):

$$\sigma\left(H_s\left(x|F;u\right)\right) = \frac{\left|J_0\left(\frac{2\pi}{\lambda} s\right)\right|}{\sqrt{8}} \tag{3.9}$$

Slaptas vaizdas išryškėja jei standartinis nuokrypis yra nedidesnis nei 0.01. (3.1C pav. pavaizduota punktyrine linija). Amplitudės intervalai kuriuose dar būtų galima vizualiai dekoduoti slaptą informaciją 3.1C paveiksle *s* ašyje pažymėti storais juodais brūkšniais. Pirmo tipo nulinės eilės Beselio funkcijos pirmos šaknies intervalo plotis yra apie 10 kartų mažesnis nei Δs (3.1C pav.). Lengvai pasiekiamas

metodo jautrumas yra lygus 0.05 mm. Kitaip sakant, šis optinės kontrolės metodas atskiria virpesių amplitudės pokyčius didesnius nei 0.05 mm. Tą galima pasiekti spausdinant koduotą paveikslą įprastu skaitmeniniu spausdintuvu be jokio specialaus spausdinimo paviršiaus paruošimo. Jei reikia, metodo jautrumas gali būti sumažintas kodavimo metu pasirinkus didesnį muaro gardelės žingsnį.

3.5. Neharmoniniai virpesiai

Dekodavimo saugumas padidinamas kodavimui naudojant tokią stochastinę muaro gardelę, kuri generuoja laike vidurkintas interferencines muaro juostas virpinant vaizdą reikiama kryptimi ir reikiama amplitude, bet dar ir papildomai užtikrina, kad laiko funkcija, pagal kurią yra virpinamas vaizdas, atitiktų specialius reikalavimus [64]. Šie reikalavimai yra parinkti taip, kad užkoduotą vaizdą virpinant harmoniškai bet kokia kryptimi ir bet kokia amplitude, slapta informacija niekada nepasirodytų, tai yra niekada nesusiformuotų laike vidurkintos interferencinės juostos. Harmoninė muaro gardelė keičiama į stačiakampę periodinę muaro gardelę.

Muaro gardelę $F(x)$ sudaro stačiakampė periodinė funkcija – gardelė formuojama iš baltų ir juodų reikšmių masyvo:

$$F(x)=\begin{cases}1, \text{ kai } x\in\left[\lambda_j;\lambda(j+0.5)\right]\\ 0, \text{ kai } x\in\left(\lambda(j+0.5);\lambda(j+1)\right)\end{cases}\quad j\in Z \tag{3.10}$$

λ - stačiakampės muaro gardelės žingsnis. (3.10) formule aprašytos muaro gardelės Furjė eilutė:

$$F(x)=\frac{\alpha_0}{2}+\sum_{k=1}^{\infty}\left(\alpha_k\cos\frac{2\pi kx}{\lambda}+\beta_k\sin\frac{2\pi kx}{\lambda}\right) \tag{3.11}$$

$$\text{kur } \alpha_0=1;\ \alpha_1,\alpha_2,\alpha_3,\ldots=0;\ \beta_k=\frac{1+(-1)^{k+1}}{k\pi};\ k=1,2,\ldots \tag{3.12}$$

Tada, virpinant harmoniniais virpesiais laike vidurkinimo operatorius [64] aprašomas lygtimi:

$$H_s(x|F;u)=\frac{1}{2}+\sum_{k=1}^{\infty}\left(\frac{1+(-1)^{k+1}}{k\pi}\sin\frac{2\pi kx}{\lambda}\right)J_0\left(\frac{2\pi k}{\lambda}s\right) \tag{3.13}$$

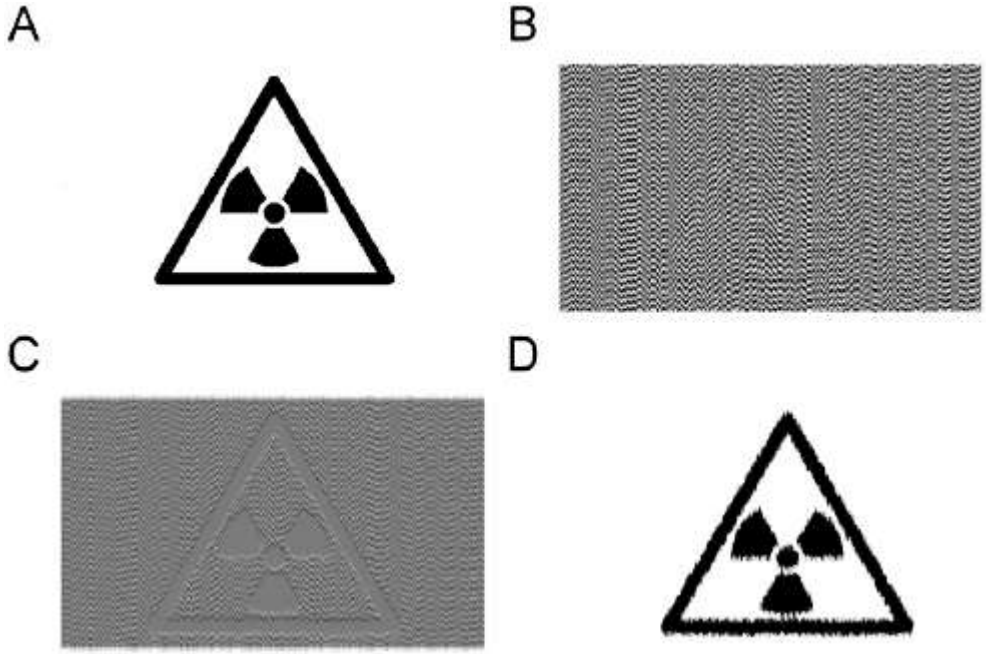
Šiuo atveju laike vidurkintos interferencinės juostos nesiformuos, nes nulinės eilės pirmo tipo Beselio funkcijos šaknys yra neperiodinės. Toliau nagrinėjama neharmoninė funkcija, aprašanti svyravimus nuo pusiausvyros padėties, šiuo atveju „zig-zag“ bangos formos funkcija $z(t)$, aprašoma (3.14) formule (didžiausias nuokrypis nuo pusiausvyros padėties s ir virpesių dažnis ω išlieka toks pat kaip (3.2) formulėje).

$$z(t)=\begin{cases}\dfrac{2s\omega}{\pi}\left(t-\left(\dfrac{2\pi}{\omega}j-\dfrac{\pi}{2\omega}\right)\right)-a, \text{ kai } \left(\dfrac{2\pi}{\omega}j-\dfrac{\pi}{2\omega}\right)\le t<\left(\dfrac{2\pi}{\omega}j+\dfrac{\pi}{2\omega}\right)\\ -\dfrac{2s\omega}{\pi}\left(t-\left(\dfrac{2\pi}{\omega}j+\dfrac{\pi}{2\omega}\right)\right)+a, \text{ kai } \left(\dfrac{2\pi}{\omega}j+\dfrac{\pi}{2\omega}\right)\le t<\left(\dfrac{2\pi}{\omega}j+\dfrac{3\pi}{2\omega}\right)\end{cases} \quad (3.14)$$

Tada pagal [64] straipsnį, vidurkinimo operatorius bus:

$$H_s\left(x|F;z\right)=\frac{1}{2}+\sum_{k=1}^{\infty}\left(\frac{1+(-1)^{k+1}}{k\pi}\sin\frac{2\pi kx}{\lambda}\right)\frac{\sin\left(\dfrac{2\pi k}{\lambda}s\right)}{\left(\dfrac{2\pi k}{\lambda}s\right)}$$

Taip garantuojamas laike vidurkintų interferencinių juostų susidarymas, nes funkcija $\dfrac{\sin(y)}{y}$ yra periodinė funkcija.



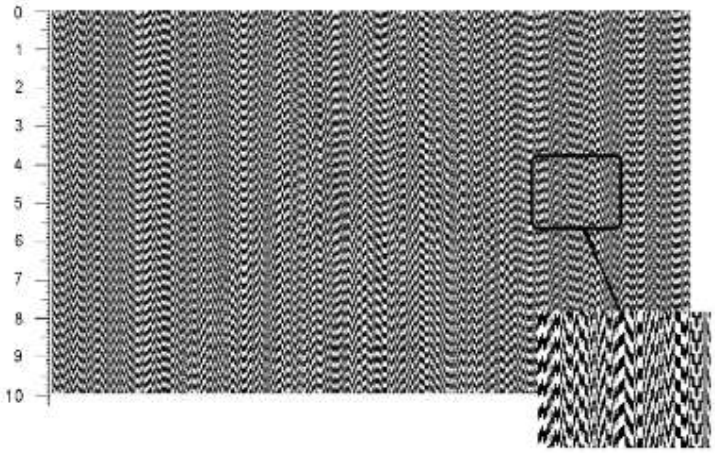
3.10 pav. Koduojamas slaptas vaizdas (A); informacija užkoduota pasinaudojus stačiakampe muaro gardele (B); skaitmeniniu būdu dekoduota informacija (C) ir išryškintas dekoduotas vaizdas (D)

Eksperimentinis slapto vaizdo dekodavimas „zig-zag“ tipo virpesiais yra atliekamas panašiai kaip ir harmoninių virpesių atveju. Tačiau yra vienas esminis skirtumas. Ryšys tarp laike vidurkintos interferencinės juostos eilės, „zig-zag“ bangos formos virpesių amplitudės ir muaro gardelės žingsnio užrašomas:

$$s_i=\frac{\lambda}{2}i;\ i=1,2,\ldots \quad (3.15)$$

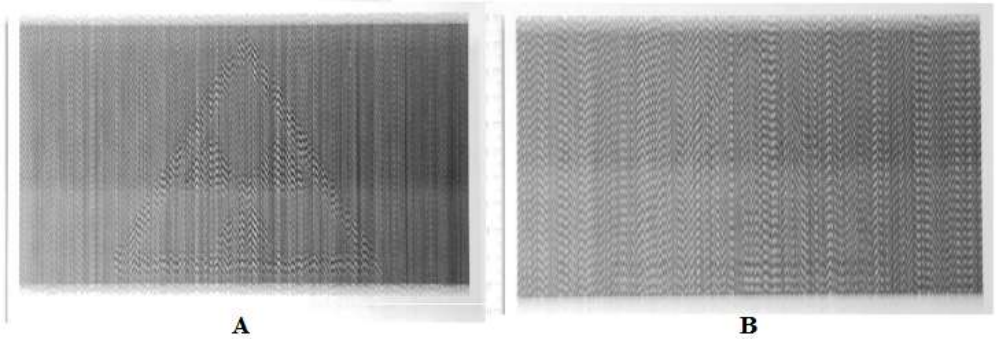
Atliekami skaitiniai eksperimentai, tik dabar vaizdui koduoti panaudota didesnio saugumo stačiakampė stochastinė gardelė (3.10 pav.).

Atspausdintas koduotas vaizdas, kuris tvirtinamas ant vibrostendo paviršiaus pavaizduotas 3.11 paveiksle. Išdidintoje paveikslo vietoje matoma, kad informacijai koduoti parinkta ne harmoninė, o stačiakampė muaro gardelė. Muaro gardelės, naudojamos fonui koduoti, žingsnis lygus 0.2821 mm; slaptai informacijai koduoti – 0.3174 mm.



3.11 pav. Slapta informacija užkoduota panaudojus stačiakampę muaro gardelę, išdidintoje dalyje matoma muaro gardelės struktūra

Laike vidurkintas paveikslas, kai „zig-zag“ formos virpesių amplitudė s=0.14105 mm $(\sin((2\pi/0.2821)\cdot 0.14105) = \sin(\pi) = 0)$ pavaizduotas 3.12A pav. Slaptas vaizdas matomas plika akimi. Slapta informacija neišryškės, jei dekoduojama virpinant harmoniniais virpesiais. 3.12B paveiksle pavaizduota, kad interferencinės juostos nesiformuoja, kai virpinama harmoniniais virpesiais, kurių amplitudė lygi 0.1080 mm (nors $J_0((2\pi)/(0.2821)\cdot 0.1080) = J_0(r_1) = 0$).



3.12 pav. Laike vidurkintos interferencinės muaro juostos, kai slapta informacija užkoduota panaudojus stačiakampę muaro gardelę, susiformavusios fone (A); slapta informacija neišryškėja kai virpinama harmoniniais virpesiais (B)

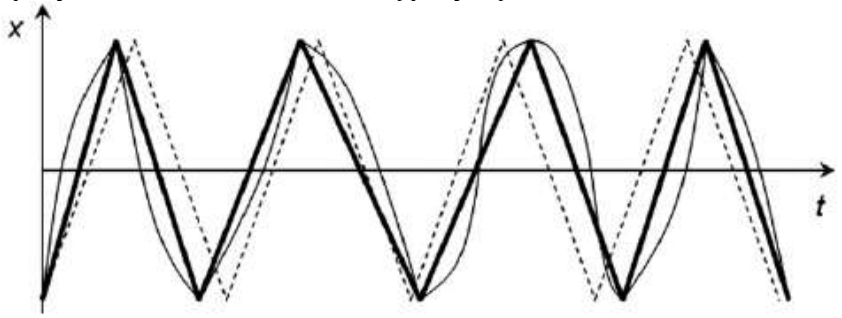
3.6. Metodo jautrumas fazės pokyčiams

Kitas svarbus aspektas kiek šis metodas yra jautrus fazės pokyčiams, net jeigu vidutinis dažnis (virpesių skaičius per minutę) yra griežtai pastovus. Fazės pokytis yra statistinis įvertis kuris vertina užtriukšmintą virpesių procesą, kada kiekvienas virpesių periodas šiek tiek skiriasi dėl triukšmo įvedamų paklaidų. [74][75]. Fazės triukšmas gali būti charakterizuojamas periodo kitimu σ_c^2 [76][77]. Tai reiškia, kad kiekvieno periodo kitimas, vidutinio periodo virpesių atžvilgiu, užrašomas taip:

$$\sigma_c^2 = \lim_{M\to\infty}\left(\frac{1}{M}\sum_{n=1}^{M}\left(\tau_n - \tau_{avg}\right)^2\right) \tag{3.16}$$

kur M yra periodo numeris, τ_n – n-tojo periodo ilgis, τ_{avg} visų periodų ilgių vidurkis, virpesių dažnių vidurkis yra $1/\tau_{avg}$.

„Zig-zag“ virpesių formos fazių iškraipymai pavaizduoti 3.13 paveiksle. Punktyrinė linija rodo stacionarius virpesius be fazės iškraipymo. Stora ištisinė linija vaizduoja „zig-zag“ bangos formos virpesius su fazės iškraipymais, vienas virpesių periodas įvyksta greičiau, kitas lėčiau. Plona ištisinė linija vaizduoja pačios virpesių formos pokyčius atsirandančius dėl fazių pokyčių.



3.13 pav. „Zig-zag“ bangos formos virpesių fazių pokyčiai. Punktyrinė linija pavaizduoti virpesiai be fazių iškraipymų; stora ištisine linija – su fazių pokyčiai; plona ištisine – atsiradę virpesių formos pokyčiai

Kaip minėta anksčiau, laike vidurkintų muaro juostų formavimą apibrėžia laiko funkcija, kuri parodo atsilenkimą nuo pusiausvyros padėties. Daroma prielaida, kad muaro gardelės Furjė skleidinys yra apibrėžtas (3.11) formule, o bangos formos $w(t)$ tankio funkcija yra $p_s(x)$. Taip pat, be kitų tankio funkcijos savybių, reikalaujama, kad funkcija $p_s(x)$ būtų lyginė ir $p_s(x)=0$ kai $x < -s$ ir $x > s$. Tada laike vidurkintas vaizdas formuojasi pagal formulę:

$$H_s(x \mid F; w) = \frac{\alpha_0}{2} + \sum_{k=1}^{\infty}\left(\alpha_k \cos\frac{2\pi kx}{\lambda} + \beta_k \sin\frac{2\pi kx}{\lambda}\right) P_s\left(\frac{2\pi k}{\lambda}s\right) \tag{3.17}$$

čia P_s žymi tankio funkcijos $p_s(x)$ Furjė transformaciją. Šis teorinis rezultatas leidžia priimti išvadą, kad nagrinėjamas metodas nėra jautrus fazės pokyčiams. Kitaip sakant, laiko proceso tankio funkcijos pavaizduota stora ištisine linija ir punktyrine

linija (3.13 pav.) yra tos pačios funkcijos iliustracijos. Taip gali būti apibrėžta atsitiktinio kintamojo tankio funkcija tolygiai pasiskirsčiusi intervale [–*s*; *s*]. tankio funkcijos Furjė transformacija yra $\sin(2\pi/\lambda)s/(2\pi/\lambda)s$ [64].

Situacija tampa daug sudėtingesnė jei dėl fazės pokyčių yra deformuojama pati bangos forma (3.13 pav. - plona ištisinė linija). Situacija kai virpesiai yra chaotiniai išnagrinėta [78] straipsnyje.

3.7. Skyriaus išvados

Eksperimentinė dinaminės vizualinės kriptografijos realizacija buvo aptarta esant skirtingo tipo: harmoniniams ir „zig-zag“ tipo virpesiaims. Iš principo šis metodas gali būti taikomas bet kokiam periodiniam signalui, tam reiktų rasti tankio funkciją atitinkančią tikrąjį signalą ir išvesti jos Furjė transformaciją.

Pagrindinė šio optinio metodo esmė, kad vaizdo kodavimui naudojami sudėtingi kompiuteriniai įrankiai, o dekodavimo procesui kompiuterio nereikia – slaptas vaizdas formuojasi interferencinių juostų rašto forma, kai užkoduotasis vaizdas yra virpinamas tiksliai nustatytu dėsniu. Matematiniai sąryšiai, aprašantys interferencinių muaro juostų formavimąsi, nepriklauso nuo virpesių dažnio. Tačiau žmogaus regos sistema pradeda matyti slaptą vaizdą tik tuomet, kai akis nebegali sekti greitai svyruojančio objekto [79], vizualinės informacijos srautas per akies obuolius, tinklaines, regos nervus patenka į regos centrą smegenų žievėje, ir žmogaus smegenyse susiformuoja slaptasis užkoduotasis vaizdas. Tuo tikslu, šiam metodui yra nustatoma virpesių dažnių žemutinė riba, jei virpesių dažnis būtų gana mažas (pvz. 0.5 Hz) akis spėtų sekti koduotą paveikslą ir smegenyse nesiformuotų slaptasis vaizdas.

Eksperimentiniai vaizdai aiškiau matomi kai stebimi plika akimi nei užfiksuoti fotoaparatu. Atkreipiamas dėmesys, kad nėra tikimasi jog laike vidurkintos interferencinės juostos pilnai susiformuos. Kitaip šio metodo taikymas būtų gana abejotinas – virpesių amplitudė turėtų būti tiksli be galo maža reikšmė. Vietoj to yra nustatoma maksimali pilkio lygių standarto reikšmė – kai interferencinės juostos beveik susiformuoja. Ši maksimali standartinio nuokrypio reikšmė yra susijusi su galimybe išskirti slaptą vaizdą ir foną. Todėl eksperimento nuotraukose slapta informacija nėra idealiai tolygiai pilka, nors pats slaptos informacijos vaizdas yra suprantamas. Standartinio nuokrypio reikšmė yra tiesiogiai susijusi su žmogaus regos sistemos savybėmis [79].

Taigi, šiame skyriuje aptarta paprasta optinė vibruojančių įrenginių kontrolės metodika. Slaptas vaizdas įterptas į stochastinę muaro gardelę gali būti stebimas plika akimi kai virpesių amplitudė patenka į iš anksto nustatytą įverčių intervalą, kuris kiekvienu atveju parenkamas individualiai. Tokia kontrolės metodika gali būti pritaikoma pramonėje ar technologijų srityje (pavyzdžiui, laboratorinis vibrostendas skirtas nustatytos suspensijos skysčiui išmaišyti). Galima atspausdinti koduotą vaizdą ir priklijuoti ant vibruojančio paviršiaus. Slaptas vaizdas bus matomas tik kai konstrukcija vibruos pagal nustatytą rėžimą. Šis metodas nereikalauja jokių papildomų sąnaudų. Be to, jį galima taikyti bet kokioje skaidrioje aplinkoje: vakuume ar skysčiuose.

4. DINAMINĖ VIZUALINĖ KRIPTOGRAFIJA PAGRĮSTA CHAOTINIAIS VIRPESIAIS

Dinaminės vizualinės kriptografijos schema paremta chaotiniais virpesiais gali būti laikoma saugesne paveikslo slėpimo schema lyginant su analogiškomis skaitmeninėmis technikomis kur slaptas vaizdas gali būti vizualiai dekoduotas kai šifruotas vaizdas yra virpinamas harmoniniais, laiptuotais ar dalimis tolydžiais virpesiais. Šiame skyriuje pateiktas vaizdo slėpimo algoritmas, kai koduotame vaizde, virpinant harmoniniais virpesiais bet kokia kryptimi ir bet kokia amplitude slapto vaizdo nepamatysime. Aprašytas metodas vaizdo slėpimui reikalauja sudėtingų kodavimo algoritmų, bet dekodavimas vyksta vizualiai ir nereikalauja kompiuterio, taip pat gali būti pritaikytas chaotinių virpesių vizualinei kontrolei. Yra žinoma, kad sudėtingose netiesinėse sistemose atsiranda chaotiniai virpesiai net esant harmoninėms apkrovoms. Be to, sudėtingos apkrovos, taikomos aviacijoje, retai kada sukelia harmoninės struktūros virpesius. Todėl tiesioginė chaotinių virpesių vizualinės interpretacijos galimybė yra patraukli alternatyva kitiems kontrolės metodams.

Šiame skyriuje nagrinėjamos chaotinės dinaminės kriptografijos galimybes, kai laike vidurkinto vaizdo poslinkio nuo pusiausvyros padėties laiko funkcija yra Gauso dėsnis su nuliniu vidurkiu ir iš anksto nustatyta dispersija.

4.1. Optinis pagrindimas

Nagrinėjama vienmatė muaro gardelę. Imkime stačiakampę pilkio funkciją, kuri apibrėžiama taip:

$$F(x) = 0.5 + 0.5 sign\left(\sin\left(\frac{2\pi}{\lambda} x \right) \right) \tag{4.1}$$

kur λ yra muaro gardelės žingsnis; reikšmė 0 atitinka juodą spalvą; 1 atitinka baltą spalvą, o visos tarpinės reikšmės (atsirandančios laike vidurkintame paveiksle) atitinka tam tikrą pilkio lygį. Funkcija $F(x)$ išskleidžiama Furjė eilute:

$$F(x) = \frac{a_0}{2} + \sum_{k=1}^{+\infty} \left(a_k \cos\left(\frac{2\pi k x}{\lambda} \right) + b_k \sin\left(\frac{2\pi k x}{\lambda} \right) \right) \tag{4.2}$$

kur $a_k, b_k \in R$; $a_0 = 1$; $a_1, a_2, a_3, \ldots = 0$; $b_k = \frac{1 + (-1)^{k+1}}{k\pi}$; $k = 1,2,\ldots$

Imkime situaciją, kada aprašyta vienmatė muaro gardelė yra virpinama x ašies kryptimi ir taikant laike vidurkinimo metodiką yra gaunamas laike vidurkintas vaizdas. Laike vidurkinimo operatorius H_s aprašantis pilkio lygį laike vidurkintame vaizde yra aprašytas [72]:

$$H_s\left(x \mid F; \xi_s\right) = \lim_{T \to \infty} \frac{1}{T} \int_0^T F\left(x - \xi_s(t)\right) dt \tag{4.3}$$

kur t yra laikas; T – ekspozicijos laikas; $\xi_s(t)$ – funkcija aprašanti dinaminį nuokrypį nuo pusiausvyros padėties (kai $\xi = 0$ paviršius yra pusiausvyros būsenoje; t – laikas); $s \geq 0$ – reali reikšmė; $x \in R$. Yra žinoma [64], kad laiko funkcijos $\xi_s(t)$ tankio funkcija $p_s(x)$ tenkina sąlygas:

$$p_s(x) = 0 \text{ kai } |x| > s;\ p_s(x) = p_s(-x) \text{ visiems } x \in R;\ s > 0 \qquad (4.4)$$

Kitaip sakant $p_\xi(x)$ aprašo statistinį nuokrypį nuo pusiausvyros padėties. Tada laike vidurkinto vaizdo, kai muaro gardelė virpa pagal laiko funkciją $\xi_s(t)$ (ekspozicijos laikas T artėja į begalybę) formavimasis yra pagrįstas lygybe:

$$H_s(x \mid F; \xi_s) = \frac{a_0}{2} + \sum_{k=1}^{+\infty} \left(a_k \cos\left(\frac{2\pi k x}{\lambda}\right) + b_k \sin\left(\frac{2\pi k x}{\lambda}\right) \right) P_s\left(\frac{2\pi k s}{\lambda}\right) \qquad (4.5)$$

kur P_s yra tankio funkcijos $p_s(x)$ Furjė transformacija. Kitaip sakant, laike vidurkintas vaizdas gali būti interpretuojamas kaip statinio vaizdo (muaro gardelės) ir taškų sklaidos funkcijos, aprašančios pradinio vaizdo virpesius, sąsuka [80][81].

Kaip minėta skyriaus pradžioje, tikslas yra sukonstruoti algoritmą paveikslo kodavimui, remiantis dinaminės vizualinės kriptografijos principais, kur dekodavimui naudojama laiko funkcija būtų chaotiniai virpesiai.

Kitaip sakant, slapto vaizdo dekodavimas vyktų vizualiai, tačiau jį galima atlikti tik kai koduotas vaizdas virpinamas chaotiškai. Atkreipiamas dėmesys, kad harmoniniai virpesiai negali būti naudojami paveikslo dekodavimui, jei jis užkoduotas panaudojus stačiakampę muaro gardelę, taip yra dėl nulinės eilės Beselio funkcijos pirmos šaknies neperiodiškumo [1].

4.2. Teoriniai sąryšiai

Yra žinoma, kad fiksuojant judantį objektą (pavyzdžiui fotografuojant) vaizdas susilieja, „išplaukia" [82][83].

Gausinis suliejimas yra vienas iš dažnai paplitusių faktorių veikiančių fiksuojamų vaizdų kokybę optinėje sistemoje [84]. Ir nors skaitmeninis suliejimo panaikinimas (debluring) užtriukšmintuose vaizduose yra gana gerai ištirtas, pažiūrėkime į šį klausimą kriptografiniu požiūriu. Gausinis suliejimas bus naudojamas šifruotiems paveikslams dekoduoti. Reikia ištirti kas vyksta, kai koduoto vaizdo suliejimas gaunamas esant chaotiniams virpesiams. Tam faktui ištirti reikia atlikti išsamią laike vidurkinimo procesų analizę, kad išsiaiškinti kas sukelia Gausinį suliejimą; toks supaprastintas požiūris, kai pikseliai nuo esamo pikselio esantys už 3σ intervalo ribų yra ignoruojami, negali būti taikomas esamiems kompiuterio nustatymams. Tarkime, kad $\xi_\sigma(t)$ – Gauso normalusis ergodinis procesas, kai vidurkis lygus nuliui, o dispersija σ^2. Atkreipiamas dėmesys, kad standartinis nuokrypis σ yra naudojamas vietoje apatinio indekso s (4.5) lygtyje. Tada, tankio funkciją $p_\sigma(x)$ bus tokia:

$$p_\sigma(x) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left(-\frac{x^2}{2\sigma^2} \right) \tag{4.6}$$

o funkcijos $p_\sigma(x)$ Furjė transformacija užrašoma:

$$P_\sigma(\omega) = \int_{-\infty}^{+\infty} p_\sigma(x) e^{-i\omega x} dx = \exp\left(-\frac{1}{2}(\omega\sigma)^2 \right) \tag{4.7}$$

Tada, laike vidurkintas vaizdas, kai muaro gardelė virpa pagal funkciją, kurios atsilenkimus nuo pusiausvyros padėties aprašo Gauso normalinis tikimybinis dėsnis, gaunamas naudojantis šia išraiška [26]:

$$H(x \mid F; \xi_\sigma) = \frac{1}{2} + \sum_{k=1}^{+\infty} \left(a_k \cos\left(\frac{2\pi k x}{\lambda} \right) + b_k \sin\left(\frac{2\pi k x}{\lambda} \right) \right) \exp\left(-\frac{1}{2} \left(\frac{2\pi k \sigma}{\lambda} \right)^2 \right) \tag{4.8}$$

(4.8) lygtimi aprašomas laike vidurkinto vaizdo formavimąsi, kai ekspozicijos laikas artėja į begalybę, o muaro gardelė virpa priklausomai nuo funkcijos $\xi_\sigma(t)$. Tačiau reiktų nepamiršti, kad eksperimentiškai atliekant šiuos virpesius, dėl skaitmeninio kompiuterio ekrano savybių gali kilti tam tikrų problemų. Visų pirma, skaitmeniniai ekranai sudaryti iš pikselių masyvo – taigi nuokrypis nuo pusiausvyros padėties turi būti pikselio dydžio kartotinis. Antra, skaitmeniniai ekranai turi baigtinį atnaujinimo dažnį – taigi, negali būti begalinės poveikio trukmės. Taigi, optinių efektų modeliavimas, panaudojant chaotinius virpesius yra daug sudėtingesnis nei efektų modeliavimas naudojant harmoninius (ar periodinius) virpesius, kur ribotas žingsnių skaičius virpesių periode gerai aproksimuoja vidurkinimo laike procesą [1]. Todėl, prieš slapto vaizdo kodavimo algoritmo aptarimą, atliekamas išsamus laike vidurkinimo proceso pagrįsto chaotiniais virpesiais tyrimas.

4.2.1. Chaotinių virpesių skaičiavimų pateikimas

Gauso procesas gali būti aproksimuojamas diskrečiais pagal normalųjį dėsnį pasiskirsčiusiais skaičiais:

$$\theta(t_j) \sim N(0, \sigma^2), \quad j = 1,2,\ldots \tag{4.9}$$

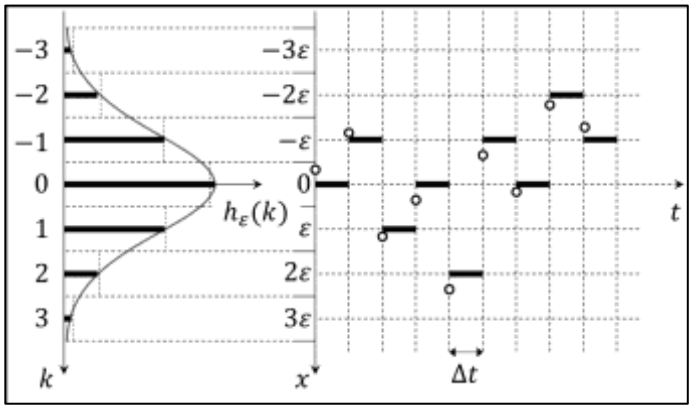
Gauso skirstinio tankio funkcija yra aprašoma (4.6) formule. Kaip buvo paminėta anksčiau, stačiakampę muaro gardelę paslinkti iš pusiausvyros padėties galima tik per sveiką pikselių skaičių. Pikselių dydis pažymimas ε ($\varepsilon > 0$). Tarkime, kad skaitmeninio ekrano atnaujinimo dažnis gali būti *m* Hz. Tada, kiekvienas paslinktos muaro gardelės momentinis vaizdas bus parodytas per $\Delta t = \frac{1}{m}$ sekundžių. 4.1 paveiksle. pavaizduota diskrečių chaotinių virpesių realizacijos schema, kur *t* žymi laiką; *x* – vienmatės muaro gardelės išilginę koordinatę; tuščiaviduriai apskritimai rodo skirstinio $\theta(t_j)$ pasiskirstymą (naujas atsitiktinis dydis yra generuojamas kiekvieno diskretaus laiko intervalo pradžioje); ε parodo

pikselio aukštį; stora ištisinė linija dešinėje paveikslo pusėje rodo muaro gardelės poslinkį nuo pusiausvyros padėties; stulpeliai $h_\varepsilon(k)$ iliustruoja diskrečias tikimybes nenukrypti nuo pusiausvyros padėties.

Kadangi $\theta(t_j)$ yra Gauso skirstinys, *k*-tojo stulpelio $h_\varepsilon(k)$ aukštis nustatomas pagal formulę:

$$h_\varepsilon(k)=\frac{1}{\sqrt{2\pi}\sigma}\int_{k\varepsilon-\frac{\varepsilon}{2}}^{k\varepsilon+\frac{\varepsilon}{2}}\exp\left(-\frac{x^2}{2\sigma^2}\right)dx \tag{4.10}$$

Pastebėkime, kad $h_\varepsilon(k)=h_\varepsilon(-k)$. Taigi, diskrečiojo atsitiktinio dydžio skirstinio reikšmė, aprašanti atsitiktinį nuokrypį nuo pusiausvyros padėties yra lygi nuliui, išskyrus taškus $k\varepsilon$; $k\in Z$.



4.1 pav. Diskrečių chaotinių virpesių realizacijos schema

Norėdami gauti laike vidurkintą vaizdą, turime apskaičiuoti $p_\sigma(x)$ diskrečiąją Furjė transformaciją, kai muaro gardelė virpinama pagal Gauso dėsnį. Taigi,

$$\begin{aligned}\widetilde{P}_\sigma(\omega)&=\sum_{k=-\infty}^{+\infty}h_\varepsilon(k)\exp(-i\omega k\varepsilon)=\sum_{k=-\infty}^{+\infty}h_\varepsilon(k)(\cos(\omega k\varepsilon)+i\sin(\omega k\varepsilon))=\\&=h_\varepsilon(0)+2\sum_{k=1}^{+\infty}h_\varepsilon(k)\cos(\omega k\varepsilon)\end{aligned} \tag{4.11}$$

čia $\widetilde{P}_\sigma(\omega)$nurodo diskretų $P_\sigma(\omega)$ atitikmenį. ((7) formulė). Išraiškai gauti pasinaudota Oilerio formule $e^{ix}=\cos(x)+i\sin(x)$.

4.2.2. Pasvarstymai apie pikselio dydį

Toliau nagrinėjama, kokie galimi rezultatai priklausantys nuo pikselio dydžio. Pirmiausia ištiriami (4.11) formulėje esantys sąryšiai, kai pikselio dydis artėja į nulį ($\varepsilon\to 0$) , o standartinis nuokrypis pastovus.

Tam pasinaudojama vidurinės reikšmės teorema apibrėžtiniam integralui:

$$h_\varepsilon(k)=\frac{1}{\sqrt{2\pi}\sigma}\int\limits_{k\varepsilon-\frac{\varepsilon}{2}}^{k\varepsilon+\frac{\varepsilon}{2}}\exp\left(-\frac{x^2}{2\sigma^2}\right)dx=\frac{\varepsilon}{\sqrt{2\pi}\sigma}\exp\left(-\frac{(k\varepsilon)^2}{2\sigma^2}\right)+o(\varepsilon) \qquad (4.12)$$

kai $\lim\limits_{\varepsilon\to 0}\frac{o(\varepsilon)}{\varepsilon}=0$.

Taigi,

$$\begin{aligned}\widetilde{P}_\sigma(\omega)&=\sum_{k=-\infty}^{+\infty}\left(\frac{\varepsilon}{\sqrt{2\pi}\sigma}\exp\left(-\frac{(k\varepsilon)^2}{2\sigma^2}\right)+o(\varepsilon)\exp(-i\omega k\varepsilon)\right)=\\&=\frac{\varepsilon}{\sqrt{2\pi}\sigma}\sum_{k=-\infty}^{+\infty}\exp\left(-\frac{(k\varepsilon)^2}{2\sigma^2}-i\omega k\varepsilon\right)+\sum_{k=-\infty}^{+\infty}o(\varepsilon)\exp(-i\omega k\varepsilon)\end{aligned} \qquad (4.13)$$

bet,

$$\lim_{\varepsilon\to 0}\sum_{k=-\infty}^{+\infty}\exp(-i\omega k\varepsilon)\varepsilon\cdot\frac{o(\varepsilon)}{\varepsilon}=\lim_{A\to+\infty}\int_{-A}^{A}\exp(-i\omega x)dx\cdot\lim_{\varepsilon\to 0}\frac{o(\varepsilon)}{\varepsilon}=0 \qquad (4.14)$$

kadangi $|\exp(-i\omega k\varepsilon)|=1$ ir $\left|\int\limits_{-A}^{A}\exp(-i\omega x)dx\right|<+\infty$

(atkreipiamas dėmesys, kad

$$\left|\int_{-A}^{A}\exp(-i\omega x)dx\right|\le\sqrt{\left(\int_{-A}^{A}\cos(\omega x)dx\right)^2+\left(\int_{-A}^{A}\sin(\omega x)dx\right)^2}<M<+\infty$$ su visais A).

Taigi,

$$\begin{aligned}\lim_{\varepsilon\to 0}\widetilde{P}_\sigma(\omega)&=\frac{\varepsilon}{\sqrt{2\pi}\sigma}\sum_{k=-\infty}^{+\infty}\exp\left(-\frac{(k\varepsilon)^2}{2\sigma^2}-i\omega k\varepsilon\right)=\\&=\frac{1}{\sqrt{2\pi}\sigma}\int_{-\infty}^{+\infty}\exp\left(-\frac{x^2}{2\sigma^2}-i\omega x\right)dx=\exp\left(-\frac{\omega^2\sigma^2}{2}\right)\end{aligned} \qquad (4.15)$$

Tai svarbus rezultatas parodantis, kad $\widetilde{P}_\sigma(\omega)$ konverguoja į $P_\sigma(\omega)$ kai pikselio dydis artėja į nulį.

Nepaisant to, yra svarbu aptarti ε reikšmę, tai ypač svarbu tada kai chaotiniai virpesiai imituojami kompiuterio ekrane.

Tuo tikslu patikrinami priešingi apribojimai, kai $\varepsilon\to+\infty$ (σ fiksuotas).

Akivaizdu, kad $\lim\limits_{\varepsilon\to+\infty}h_\varepsilon(0)=1$ ir $\lim\limits_{\varepsilon\to+\infty}h_\varepsilon(k)=0$ visiems $k=\pm1,\pm2,\ldots$. Taigi,

$$\lim_{\varepsilon\to+\infty}\widetilde{P}_\sigma(\omega)=\lim_{\varepsilon\to+\infty}\sum_{k=-\infty}^{+\infty}h_\varepsilon(k)\exp(-i\omega k\varepsilon)=1 \qquad (4.16)$$

Visi sugeneruoti diskretieji atsitiktiniai dydžiai $\theta(t_j)$ pateks į stacionarios muaro gardelės centrinį pikselį, esantį koordinačių pradžios taške, jei pikselio dydis yra didelis lyginant su standartiniu nuokrypiu σ. Tada muaro gardelė išliks pastovioje pusiausvyros padėtyje ir laike vidurkintas paveikslas bus stacionarios gardelės paveikslas (charakteringosios funkcijos moduliuojančios laike vidurkintas interferencines juostos šiuo atveju bus lygios vienetui).

4.2.3. Pasvarstymai apie standartinį nuokrypį σ

Priklausomai nuo standartinio nuokrypio σ dydžio galimos skirtingos situacijos Pirmiausiai aptariama situacija, kai $\sigma \to 0$ (pastovus ε).

Tokiu atveju $\lim\limits_{\sigma\to 0} p_\sigma(x) = \delta_0(x)$, kai $\delta_0(x) = \begin{cases} +\infty, & x = 0 \\ 0, & x \neq 0 \end{cases}$ ir $\int\limits_{-\infty}^{\infty} \delta_0(x)dx = 1.$

Taigi,

$$\lim_{\sigma\to 0} \widetilde{P}_\sigma(\omega) = \int_{-\infty}^{\infty} \delta_0(x)\exp(-i\omega x)dx = \exp(-i\omega 0) = 1 \qquad (4.17)$$

Muaro gardelė nebus išstumta iš pusiausvyros padėties jei standartinis nuokrypis σ yra toks mažas, kad visi atsitiktiniai dydžiai pateks šalia stacionarios gardelės centrinio pikselio.

Toliau nagrinėjama situacija, kai $\sigma \to +\infty$ (ε fiksuotas). Šiuo atveju,

$$\lim_{\sigma\to+\infty} h_\varepsilon(k) = \lim_{\sigma\to+\infty} \frac{1}{\sqrt{2\pi}\sigma} \int_{k\varepsilon-\frac{\varepsilon}{2}}^{k\varepsilon+\frac{\varepsilon}{2}} \exp\left(-\frac{x^2}{2\sigma^2}\right)dx = 0 \qquad (4.18)$$

Taigi, $\lim\limits_{\sigma\to+\infty} \widetilde{P}_\sigma(\omega) = 0.$ Momentinis muaro gardelės postūmis iš pusiausvyros padėties bus labai didelis. Taigi muaro gardelė bus tolygiai susiliejusi išilgai visoje poslinkio ašyje ir laike vidurkintas paveikslas taps pilkas ($\lim\limits_{\sigma\to+\infty} H_\sigma(x \mid F; \xi_\sigma) = 0.5$).

Galima dar kitokia situacija, kai ir $\sigma\to\infty$ ir $\varepsilon\to\infty$. Čia bus reikalinga Laplaso funkcija

$$\Phi(s) = \frac{1}{\sqrt{2\pi}} \int_0^s e^{-\frac{x^2}{2}} dx, \text{ kai } s \geq 0 \text{ ir } \Phi(0) = 0, \text{ bei } \lim_{s\to\infty} \Phi(s) = \frac{1}{2}. \qquad (4.19)$$

Šiuo atveju $\widetilde{P}_\sigma(\omega) = h_\varepsilon(0)$, nes $\lim\limits_{\varepsilon\to+\infty} h_\varepsilon(k) = 0$ kai k=±1, ±2, ...

Taigi

$$h_\varepsilon(0) = \frac{1}{\sqrt{2\pi}\sigma} \int_{-\frac{\varepsilon}{2}}^{\frac{\varepsilon}{2}} e^{-\frac{x^2}{2\sigma^2}} dx = \frac{1}{\sqrt{2\pi}} \int_{-\frac{\varepsilon}{2}}^{\frac{\varepsilon}{2}} e^{-\frac{\left(\frac{x}{\sigma}\right)^2}{2}} d\left(\frac{x}{\sigma}\right) \qquad (4.20)$$

Pažymima $\frac{x}{\sigma}=z$, tada kai $x_0=-\frac{\varepsilon}{2}$, tai $z_0=-\frac{\varepsilon}{2\sigma}$, o kai $x_1=\frac{\varepsilon}{2}$, tai $z_1=\frac{\varepsilon}{2\sigma}$.

Tada

$$h_\varepsilon(0)=\frac{1}{\sqrt{2\pi}}\int\limits_{-\frac{\varepsilon}{2\sigma}}^{\frac{\varepsilon}{2\sigma}} e^{-\frac{z^2}{2}}dz=\frac{2}{\sqrt{2\pi}}\int\limits_{0}^{\frac{\varepsilon}{2\sigma}} e^{-\frac{z^2}{2}}dz=2\Phi\left(\frac{\varepsilon}{2\sigma}\right). \tag{4.21}$$

Jeigu $\lim\limits_{\varepsilon,\sigma\to+\infty}\frac{\varepsilon}{2\sigma}=\alpha$, tai $\lim\limits_{\varepsilon,\sigma\to+\infty}h_\varepsilon(0)=2\Phi(\alpha)$, čia $0\le\alpha\le+\infty$. Vadinasi

$$\tilde{P}_\sigma(\omega)=2\Phi(\alpha),\ \text{kai}\ \lim_{\varepsilon,\sigma\to+\infty}\frac{\varepsilon}{2\sigma}=\alpha,\ \text{čia}\ 0\le 2\Phi(\alpha)\le 1. \tag{4.22}$$

Šiuo atveju kai nagrinėjama stambi gardelė bei dideli gardelės postūmiai iš pusiausvyros padėties, pilko lygiai išsibarstys bet kaip po visa sritį.

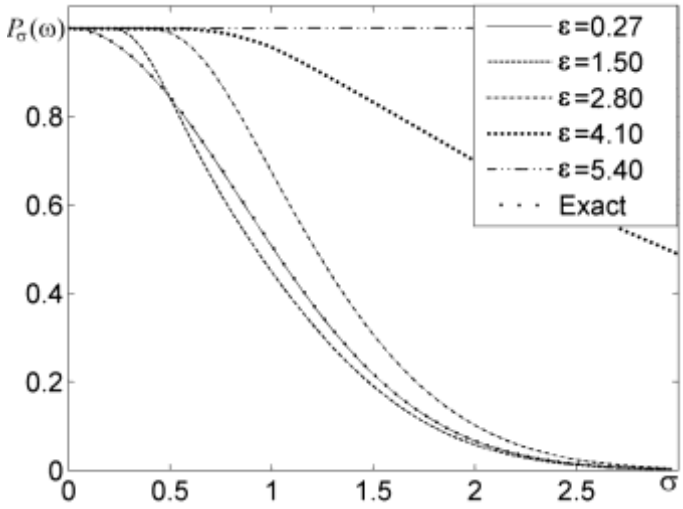
4.2.4. Realių chaotinių virpesių modeliavimas kompiuterio ekrane

Buvo atliekami bandymai norint patikrinti ar teoriniai skaičiavimai galioja chaotinius virpesius modeliuojant kompiuterio ekrane. Buvo naudojamas HP ZR24w tipo skaitmeninis monitorius; šiuo atveju pikselio aukštis yra 0.27 mm (vienmatė muaro gardelė yra vertikalioje padėtyje). Muaro gardelės periodo pavaizdavimui naudojama 20 pikselių (10 pikselių yra juodi ir 10 pikselių yra balti).

Taigi, vienmatės muaro gardelės periodas yra 5,4 mm vertikalia kryptimi. Teorinė gaubiančioji funkcija, kuri moduliuoja muaro gardelės pirmąjį užpilkėjimą yra aprašyta (4.7) formule. Gaubiančiosios funkcijos $\tilde{P}_\sigma(\omega)$ formos imitavimui panaudojama (4.13) formulė, reiktų atkreipti dėmesį, kad ω keičiamas į $\frac{2\pi}{\lambda}$ pirmam muaro gardelės užpilkėjimui atitinkančiam muaro gardelės pagrindinį periodą:

$$\tilde{P}_\sigma\left(\frac{2\pi}{\lambda}\right)=h_\varepsilon(0)+2\sum_{k=1}^{+\infty}h_\varepsilon(k)\cos\left(\frac{2\pi}{\lambda}k\varepsilon\right) \tag{4.23}$$

Gaubiančiosios funkcijos $\tilde{P}_\sigma(\omega)$ forma skaitmeniniu būdu pavaizduota 4.2 paveiksle kai $\varepsilon=0.27,\ 1.5,\ 2.8,\ 4.1$ ir 5.4. Skaičiavimai yra atlikti kai $\lambda=5.4=20\varepsilon$. Plika akimi negalima pamatyti skirtumo tarp gaubiančiosios funkcijos $\tilde{P}_\sigma(\omega)$ ir teorinės gaubiančiosios funkcijos kai $\varepsilon=0.27$ (4.2 pav.).



4.2 pav. Skaitmeniniu būdu gauta gaubiančioji funkcija $\tilde{P}_\sigma(\omega)$ gauta prie skirtingų pikselio reikšmių: ε = 0.27, 1.5, 2.8, 4.1, 5.4

Gautas $\left|P_\sigma(\omega)-\tilde{P}_\sigma(\omega)\right|=0.00191$ skirtumas kai $\varepsilon=0.27$ ir $\sigma=1$ leidžia daryti išvadą, kad $\varepsilon=0.27$ yra pakankamai mažas pikselio dydis norint modeliuoti imituojamus chaotinius virpesius kompiuterio ekrane, jeigu gardelės periodas λ yra nemažesnis nei 20ε.

4.3. Chaotinių virpesių panaudojimas dinaminėje kriptografijoje

Dinaminės kriptografijos idėja remiasi laike vidurkintų muaro juostų formavimusi srityse kurias užima slaptas vaizdas, kai koduotas paveikslas yra virpinamas pagal iš anksto numatytą judesio dėsnį.

Ši idėja negali būti eksploatuojama dinaminei vizualinei kriptografijai pagrįstai chaotiniais virpesiais dėl to, kad laike vidurkintos muaro juostos nesiformuoja, kai koduotas paveikslas yra virpinamas chaotiniais virpesiais ((4.8) formulė) – paveikslėlis tolygiai susilieja standartui σ didėjant.

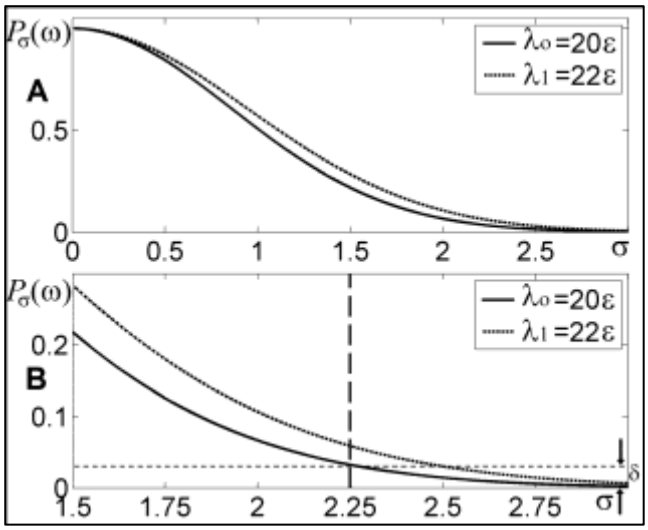
Reikia taikyti kitus metodus, kurie leistų dekoduoti slaptą vaizdą. Parenkamas šifravimo metodas aprašytą [64] straipsnyje, kur fono užimamai sričiai koduoti yra naudojama muaro gardelė, kurios žingsnis $\lambda_0=20\varepsilon=5.4$ mm, o slapto vaizdo sričiai koduoti imama gardelė, kurios žingsnis $\lambda_1=22\varepsilon=5.94$. Parenkama koduoto vaizdo nuokrypių nuo pusiausvyros padėties kryptis – visi poslinkiai turi būti vienos krypties ir ši kryptis turi sutapti su išilgine vienmatės muaro gardelės ašimi. Slaptam vaizdui užkoduoti pritaikomi stochastinio fazės postūmio bei fazių reguliarizacijos metodai.

4.3.1. Slapto vaizdo dekodavimas

Kaip ir minėta anksčiau, chaotiniai virpesiai negeneruoja laike vidurkintų muaro juostų, vaizdas susilieja didėjant standartiniam nuokrypiui, bet Gausinio susiliejimo procesą reguliuojančios gaubiančiosios funkcijos forma priklauso nuo

muaro gardelės žingsnio (4.3A pav.). Taigi, galima rasti tokį standartinį nuokrypį σ prie kurio $P_\sigma(\omega)$ reikšmė bus žemiau nei δ, kai $\lambda_0 = 20\varepsilon$, bet išliks aukščiau δ, kai $\lambda_1 = 22\varepsilon$ (4.3B pav.).

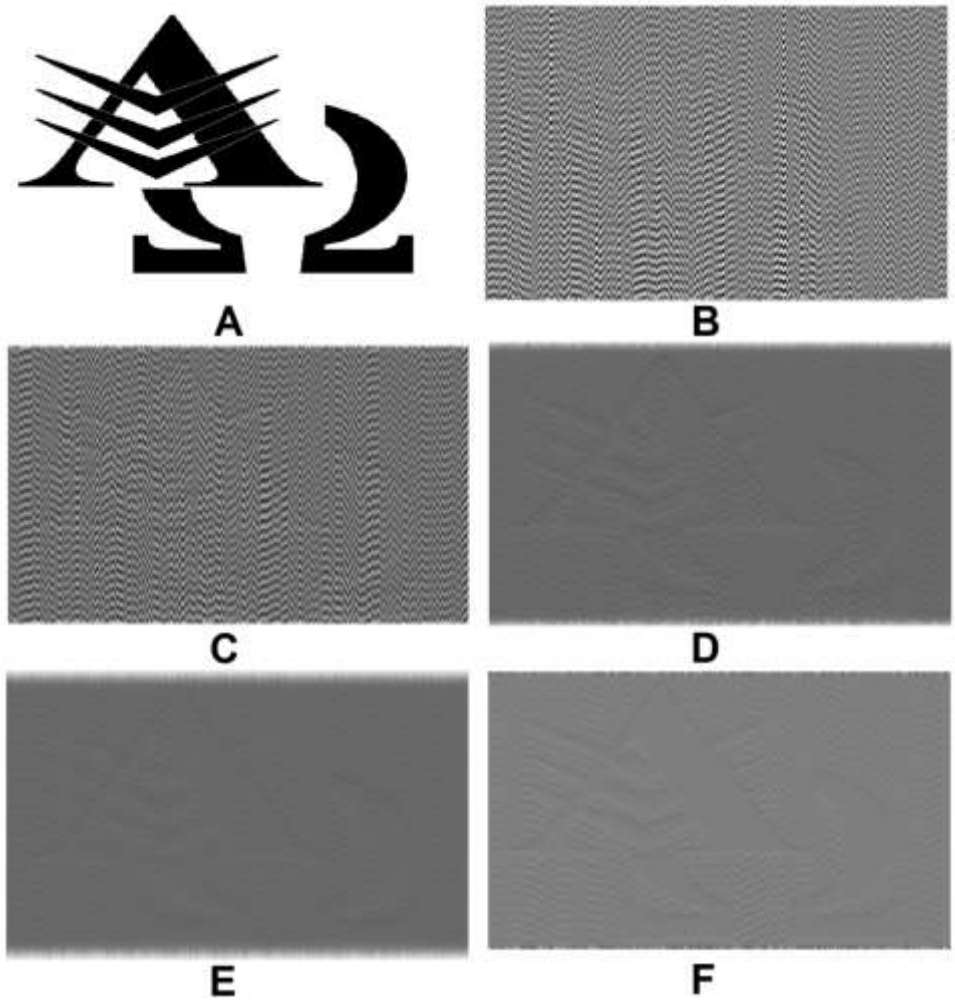
Dydžiu δ aprašoma tokia situacija, kai plika akimi laike vidurkintame vaizde matome beveik pilnai susiformavusias laike vidurkintas interferencines juostas. Kitaip sakant, δ reikšmė turi būti parenkama individualiai ir ji priklauso nuo daugelio skirtingų faktorių, tokių kaip eksperimento struktūra bei statinės muaro gardelės savybės. Šiuo atveju parinkta ribinė δ=0.03 reikšmė, kuri yra pakankama laike vidurkintų muaro juostų interpretacijai. Vertikali brūkšninė linija 4.3B paveiksle nurodo optimalią standartinio nuokrypio σ reikšmę, prie kurios geriausiai dekoduojamas slaptas vaizdas, jei koduotas paveikslas virpinamas chaotiškai. Slapta informacija interpretuojama laike vidurkintomis juostomis, kol fone jos dar nėra susiformavusios.



4.3 pav. Paveikslo kodavimas remiantis chaotiniais virpesiais (A); išdidintoje paveikslo dalyje (B) pavaizduota optimali standartinio nuokrypio reikšmė, prie kurios geriausiai dekoduojama slapta informacija

4.3.2. Kompiuteriniai eksperimentai

Pirmiausiai parenkamas slaptas vaizdas, kuris bus koduojamas panaudojant stačiakampę muaro gardelę (4.4A pav.).

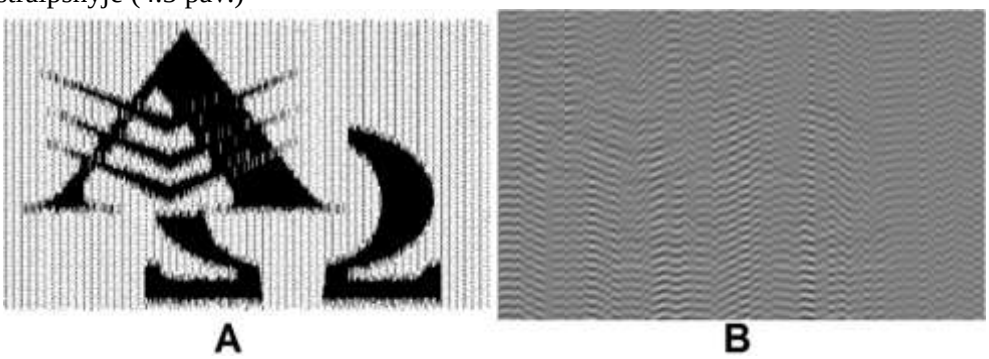


4.4 pav. Koduojama informacija (A); statinis užkoduotas vaizdas (B); dekoduotas vaizdas prie skirtingų σ reikšmių: (C) – σ = 1.2; (D) – σ = 2.25; (E) – σ = 3.1; dekoduotas vaizdas, kai ekspozicijos laikas artėja į begalybę (F)

Panaudojus kodavimo algoritmą gautas statinis vaizdas pavaizduotas 4.4B pav. Vaizdo dekodavimui generuojami diskretūs atsitiktiniai dydžiai $\theta(t_j) \sim N(0,\sigma^2)$ ir gaunami laike vidurkinti vaizdai prie skirtingų σ reikšmių: $\sigma = 1.2$ (4.4C pav.) – standartinis nuokrypis yra per mažas slapto vaizdo dekodavimui, $\sigma = 2.25$ (4.4D pav.) yra optimalus standartinis nuokrypis slapto vaizdo dekodavimui ir $\sigma = 3.1$ (4.4E pav.) standartinis nuokrypis jau per didelis slapto vaizdo dekodavimui.

Pastebime, kad 4.4D pav. matomas slaptas vaizdas susiformuoja ne laike vidurkintų interferencinių juostų pagalba. Šis optinis efektas gali būti paaiškinamas tuo, kad ekspozicijos laikas ribojamas 1 sekunde (trukmė kada diskretūs atsitiktiniai dydžiai veikia laike vidurkintą vaizdą lygi 60). Slaptas vaizdas tampa gerai matomas

stochastinės muaro gardelės fone, kai ekspozicijos laikas artėja į begalybę (4.4F pav.), diskrečių atsitiktinių dydžių poveikio trukmė yra 6000. Dekoduotas vaizdas gali būti išryškintas panaudojus skaitmeninį metodą aprašytą [78] straipsnyje (4.5 pav.)



4.5 pav. Išryškintas dekoduotas vaizdas (A); bandymas dekoduoti naudojant izotropinį Gausinį suliejimą (B)

Galima pastebėti, kad standartiniai suliejimo skaičiavimo metodai (standartinių paveikslėlių redagavimo funkcijos tokios kaip Adobe Photoshop programoje) negali būti naudojami slaptam vaizdui dekoduoti. Pasirinkus $3\sigma = 6.75$ izotropinį Gausinį suliejimą (4.5B pav.) –sulietame vaizde koduoto vaizdo negauname, kadangi proceso metu yra pažeidžiama muaro gardelės struktūra.

4.4. Dinaminės kriptografijos panaudojimas optiniam chaotinių virpesių vertinimui

Šiame skyrelyje nagrinėjama vienmatė harmoninė muaro gardelė:

$$F(x) = \frac{1}{2} + \frac{1}{2}\sin\left(\frac{2\pi}{\lambda}x\right) \tag{4.24}$$

čia x – išilginė koordinatė, λ - muaro gardelės žingsnis, 1 atitinka baltą spalvą, 0 – juodą spalvą, o visos tarpinės – atitinkamą pilkio lygį. Ši gardelė virpinama x ašies kryptimi, o laike vidurkinimo operatorius aprašomas (4.3) formule. Periodinė muaro gardelė skleidžiama Furjė eilute pagal (4.2) formulę. Jei muaro gardelę virpinama pagal laiko funkciją $\xi_s(t)$ laike vidurkintas vaizdas formuojasi pagal (4.5) lygtį. Tokiu atveju kai laiko funkcija aprašanti stochastinius atsilenkimus nuo pusiausvyros padėties yra chaotiniai virpesiai, jos Furjė transformacija yra:

$$P_\sigma\left(\frac{2\pi k}{\lambda}\right) = \exp\left(-\frac{1}{2}\left(\frac{2\pi k\sigma}{\lambda}\right)\right) \tag{4.25}$$

Čia σ yra Gauso normaliojo dėsnio standartinis nuokrypis.

Harmoninė muaro gardelė sudaryta iš masyvo lygiagrečių linijų. Jos Furjė koeficientai, rasti remiantis (4.24) formule yra: $a_0 = 1$; $a_1 = 0{,}5$; $a_{2,3} = 0$; $b_{1,2} = 0$. Gaubiančiąją funkciją charakterizuojančią Gausinio suliejimo procesą galime aprašyti taip:

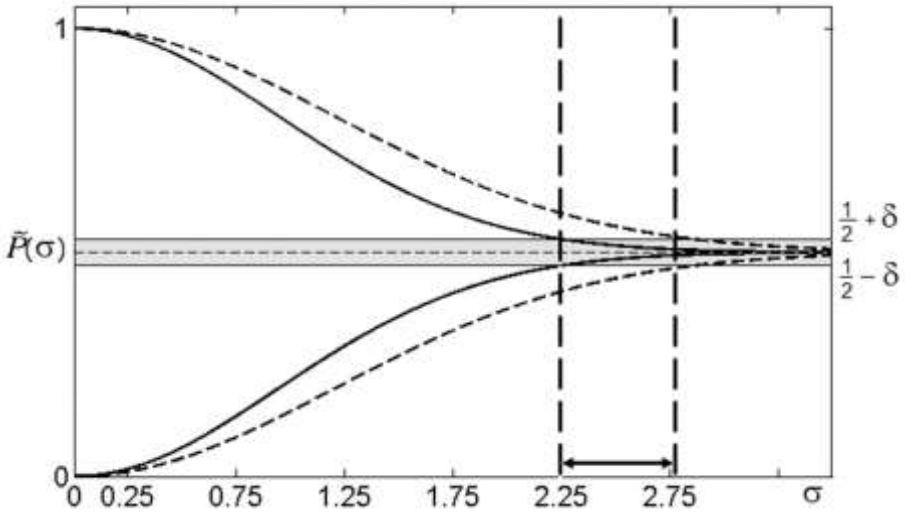
$$\tilde{P}(\sigma)=\frac{1}{2}\pm\frac{1}{2}\exp\left(-\frac{1}{2}\left(\frac{2\pi\sigma}{\lambda}\right)\right) \tag{4.26}$$

Esant chaotiniams virpesiams laike vidurkintos interferencinės juostos formuojasi priklausomai nuo standartinio nuokrypio reikšmės, jam didėjant muaro gardelė periodiškai pilkėja. (4.6 pav.) Ir tikrai, harmoninė muaro gardelė aiškiausiai yra matoma kai $\sigma = 0$:

$$H(x)\big|_{\sigma=0}=\frac{1}{2}+\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right) \tag{4.27}$$

Ir laike vidurkintas vaizdas visiškai užpilkėja kai $\sigma\to\infty$

$$H(x)\big|_{\sigma\to\infty}=\frac{1}{2} \tag{4.28}$$



4.6 pav. Chaotinės vizualinės kriptografijos eksperimentinis realizavimas.

Kaip jau minėta, dinaminės vizualinės kriptografijos idėja remiasi laike vidurkintų interferencinių muaro juostų formavimusi slaptame vaizde kai koduotas vaizdas yra virpinamas pagal iš anksto numatytą judesį (muaro gardelės žingsnis yra skirtingas slaptam vaizdui ir fonui). Judesio dėsniu $\xi(t)$ šiuo atveju pasirenkamas Gauso dėsnis. Parenkamos dvi gaubiančiosios funkcijos $\tilde{P}(\sigma)$ prie skirtingų λ reikšmių: $\lambda_0 = 22\varepsilon = 5.94$ mm ir $\lambda_1 = 20\varepsilon = 5.4$ mm, kurios iliustruotos 4.6 pav., atitinkamai plona punktyrine linija ir plona ištisine linija. (ε yra pikselio dydis ir jis lygus 0.27 mm.) horizontali punktyrinė linija yra nubrėžta per 0.5 reikšmę ir žymi laike vidurkintų muaro juostų centrą. (laike vidurkintos muaro interferencinės juostos visiškai susiformuoja kai $\sigma\to\infty$). Paveiksle pavaizduota 2δ pločio šviesiai pilka juosta abipus 0.5 reikšmės (δ atitinka pilkio lygį) vaizduoja sritį kurioje žmogaus akis gali pamatyti susiformavusias interferencines juostas. Kitaip sakant σ sritis tarp dviejų punktyrinių vertikalių linijų yra pritaikoma kriptografijai pagrįstai

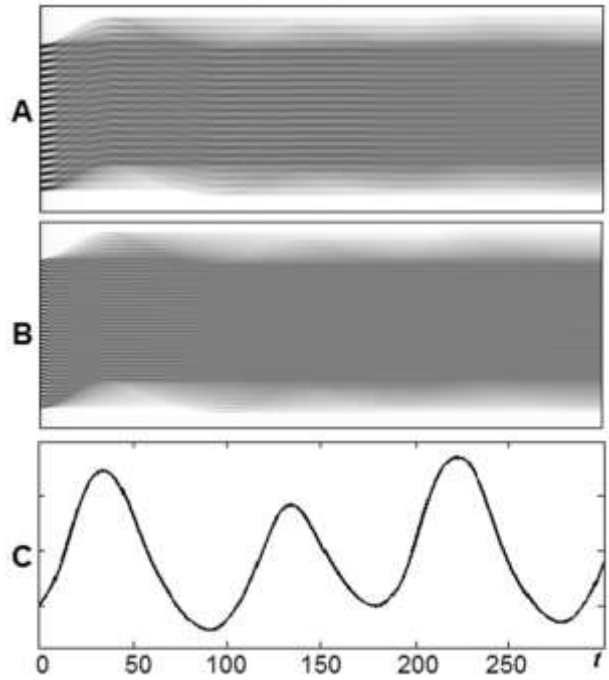
chaotiniais virpesiais. Laike vidurkintame vaizde muaro interferencinės juostos pastebimos kai gardelės žingsnis λ_0, o kai gardelės žingsnis λ_1 juostos dar neidentifikuojamos esant toje σ srityje.

Šis slapto vaizdo identifikavimo būdas chaotinėje vizualinėje kriptografijoje skiriasi nuo dinaminėje kriptografijoje naudojamo vaizdo identifikavimo, kai atliekami periodiniai virpesiai. Esant periodiniams virpesiams slaptą vaizdą nuo fono skiriame dėl dviejų skirtingų lygių. Laike vidurkintos muaro juostos susiformuoja slapto vaizdo vietose, o fone jos nesiformuoja. Arba atvirkščiai, interferencinės juostos formuojasi fone, o nesiformuoja slaptame vaizde, tai priklauso nuo harmoninių virpesių amplitudės. Tačiau chaotinėje vizualinėje kriptografijoje taip nėra. Jei muaro gardelės žingsnis slaptame vaizde yra didesnis nei fone, tai interferencinės juostos formuosis tik fone. Jei interferencinės juostos susiformuos slaptame vaizde, tai neišvengiamai jos jau bus susiformavusios ir fone, dėl to niekaip negalėsime iššifruoti slapto vaizdo.

Kaip jau minėta, virpinant harmoniniais virpesiais virpesių dažnis neturi jokios įtakos interferencinių juostų formavimuisi. Nepaisant to, šis dažnis turi būti pakankamai didelis, jei dekodavimas atliekamas plika akimi (žmogaus regos sistema interpretuoja interferencines juostas, kai akis nebespėja sekti greit svyruojančio koduoto paveikslėlio). Kita vertus, jei norime slaptą vaizdą fiksuoti fotokamera, jos ekspozicijos laikas turi būti pakankamai ilgas, kad fotokamera (analoginė ar skaitmeninė) spėtų užfiksuoti pakankamą harmoninių virpesių periodų skaičių.

Visai kita situacija kai virpesiai yra chaotiniai. Nebėra jokių virpesių periodų. Laike vidurkintos interferencinės juostos visiškai nesiformuos, jei koduotas vaizdas yra veikiamas vienkrypčiais chaotiniais virpesiais.

4.7 paveiksle iliustruotas skaičiavimų pavyzdys, kai judesio suliejimas gaunamas esant chaotiniams virpesiams. Tipinis netiesinės švytuoklės modelis su harmoniniu sužadinimu panaudojamas chaotiniams virpesiams iliustruoti (4.7C pav). 4.4 paveikslo A ir B dalyse pavaizduotos dvi skirtingo žingsnio muaro gardelės; ekspozicijos trukmė šiuo atveju kinta nuo 0 iki 300 diskretinių laiko žingsnių, ji vaizduojama horizontalioje ašyje. Skirtumus tarp muaro gardelių galima pastebėti kairėje laike vidurkinto vaizdo pusėje. Poveikio laikui artėjant į begalybę abu vaizdai (A ir B) užpilkėja, tačiau šis procesas skirtingom gardelėm vyksta skirtingu laiku, nors netiesinių virpesių laiko realizacija yra vienoda.



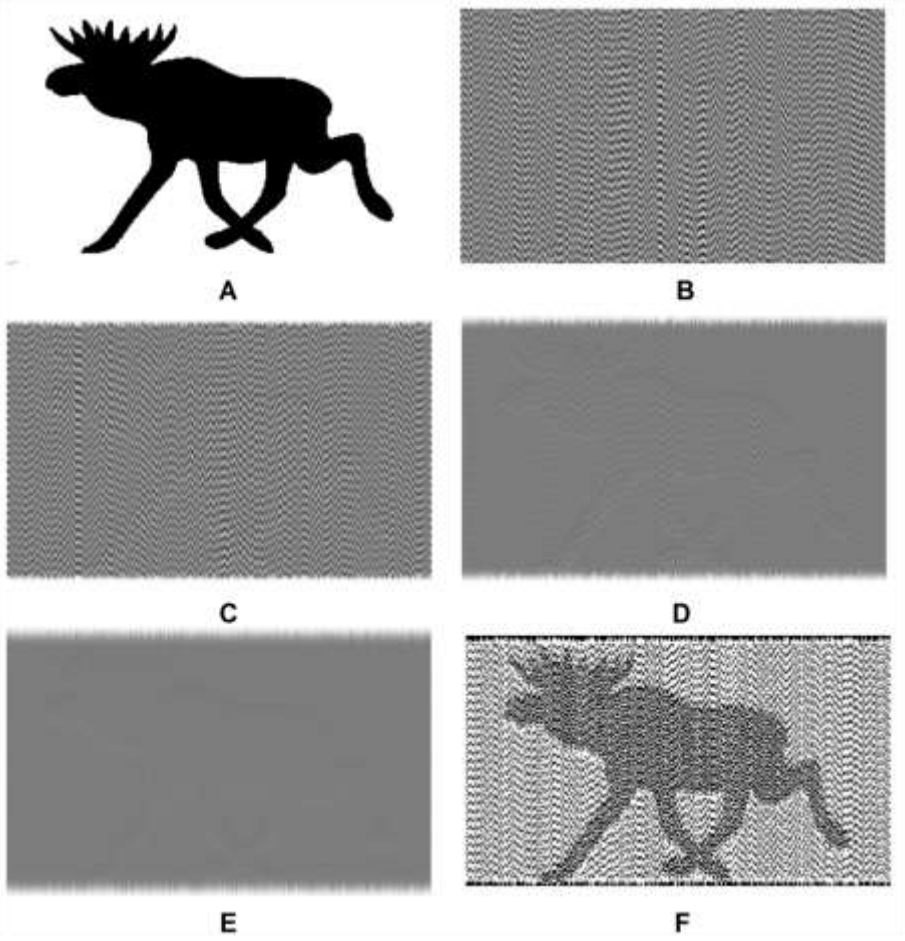
4.7 pav. Judesio sukeltas suliejimo efektas, kurį sukelia chaotiniai virpesiai skirtingoms muaro gardelėms.

Remiantis 4.7 paveikslo vaizdu galima suformuoti du svarbius pastebėjimus. Pirmasis remiasi 4.6 paveikslo rezultatais – judesio suliejimas, kurį sukelia chaotiniai virpesiai yra skirtingas skirtingoms muaro gardelėms. Kitas svarbus pastebėjimas – ribotas ekspozicijos laikas padeda pritaikyti chaotinę vizualinę kriptografiją praktikoje.

4.4.1. Eksperimentinė realizacija kompiuterio ekrane

Slapto vaizdo kodavimas stochastinėje muaro gardelėje atliekamas panaudojant fazių reguliarizavimo ir pradinių fazių stochastinio postūmio algoritmus. Vienmatė muaro gardelė kurios žingsnis $\lambda_0 = 20\varepsilon = 5.4$ mm yra naudojama fonui koduoti, o muaro gardelė, kurios žingsnis $\lambda_1 = 22\varepsilon = 5.94$ mm – slaptam vaizdui koduoti. Tokia kodavimo schema leidžia paslėpti slaptą vaizdą koduotame paveikslėlyje. Reikia paminėti, kad koduoto paveikslėlio atsilenkimai nuo pusiausvyros padėties turi būti vienpusiai ir kryptis turi sutapti su vienmatės muaro gardelės horizontalia ašimi.

Vaizdas, kuris bus koduojamas, pavaizduotas 4.8A paveiksle, statinėje muaro gardelėje užkoduotas vaizdas matomas 4.8B pav. Užkoduotam paveikslui esant nejudančioje padėtyje slapta informacija nepastebima. Atliekami keli skaitiniai eksperimentai, kada koduotas vaizdas virpinamas pagal atsitiktinę laiko funkciją $\xi(t)$. Prie skirtingų standartinio nuokrypio σ reikšmių gaunami skirtingi laike vidurkinti vaizdai (4.8C, 4.8D, 4.8E pav).



4.8 pav. Užkoduotas ir vizualiai dekoduotas slaptas vaizdas. Pradinė informacija vaizduojama A dalyje; koduotas vaizdas – B dalyje; dekoduotas vaizdas prie skirtingų standartinio nuokrypio reikšmių – C, D ir E dalyse; išryškintas vaizdas – F dalyje

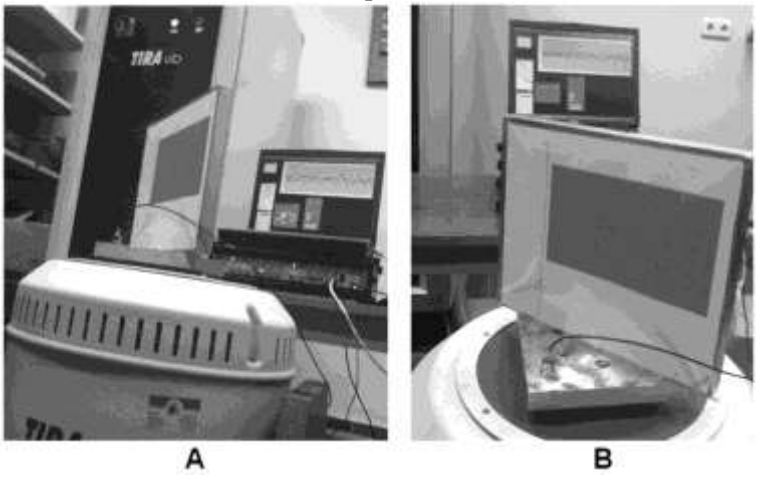
Atsitiktinių skaičių generatoriumi yra generuojami skaičiai pasiskirstę pagal Gauso dėsnį su nuliniu vidurkiu ir standartiniu nuokrypiu σ. Kiekvienas atsitiktinis skaičius apibrėžia koduoto paveikslo nuokrypio nuo pusiausvyros padėties dydį kryptimi statmena gardelės sudaromųjų linijų krypčiai. Parinktas ekspozicijos laikas yra 1000 diskretinių laiko momentų – vidurkintame vaizde pateikta 1000 kadrų, kuriuose užkoduotas vaizdas buvo pastumtas skirtingais atstumais nuo pusiausvyros padėties. Tai pavaizduota 4.8 pav. C, D ir E dalyse. Slaptas vaizdas neišryškėja 4.8C paveiksle – standartinis nuokrypis σ=1,75 yra per mažas (laike vidurkintos interferencinės juostos nesusidaro nei fone nei slapto vaizdo vietose). Situaciją galime paaiškinti 4.6 pav. gautais rezultatais – gaubiančiosios funkcijos $\tilde{P}(1.75)$ reikšmė nepapuola į δ sritį kai σ = 1.75. Slaptas vaizdas išryškėja 4.8D pav. čia interferencinės juostos susiformavo fone, bet nepilnai susiformavo slapto vaizdo vietoje, šiuo atveju σ = 2.5. Taip yra dėl to, kad muaro gardelės žingsnis, kuria

užkoduotas slaptas vaizdas yra didesnis nei muaro gardelės žingsnis fone ($\lambda_0 < \lambda_1$). Gaubiančiosios funkcijos slopimo greitis yra atvirkščiai proporcingas gardelės žingsniui. Standarto reikšmė $\sigma = 2.5$ patenka į chaotinei vizualinei kriptografijai tinkamą sritį (4.6 pav.). Paveiksle 4.8D matomos fone beveik susiformavusias interferencinės juostos, slaptos informacijos vietose taip pat matomas užpilkėjimas, tačiau šiose vietose laike vidurkintos muaro juostos nesiformuoja ir vaizdo šiurkštumas yra žymiai didesnis lyginant su vaizdo šiurkštumu fono vaizde. Pagaliau, slaptas vaizdas neišryškėja kai $\sigma = 3.25$, laike vidurkintos interferencinės muaro juostos susiformuoja ir fone ir slapto vaizdo vietose (4.8E pav.).

4.8D paveiksle gautas dekoduotas vaizdas yra išryškinamas remiantis [73] aprašyta metodika ir gautas rezultatas pateiktas 4.8F paveiksle. Jei, remiantis šia metodika būtų bandoma išryškinti slaptą vaizdą paėmus 4.8B paveikslą, bandymas nepavyktų – informacija nepasirodytų.

4.4.2. Praktiniai eksperimentai

Kaip jau minėta anksčiau chaotinėje vizualinėje kriptografijoje naudojami specialūs paveikslėlio kodavimo būdai, bet dekodavimas yra grynai vizualinis būdas, kuriam kompiuteris nebūtinas. Koduotas paveikslas gali būti pritvirtinamas ant paviršiaus kuris sukelia chaotinius virpesius.



4.9 pav. Bendras eksperimento vaizdas pavaizduotas A dalyje; lengvasvoris pjezoelektrinis akcelerometras reikalingas vibrostendo vibracijai stebėti matomas B dalyje

Eksperimentinei dekodavimo įrangai reikalingi du pagrindiniai elementai: vibrostendas ir skaitmeninė kamera. (4.9 pav.) Koduotas paveikslas yra atspausdinamas įprastiniu skaitmeniniu spausdintuvu ir priklijuojamas ant tvirto konstrukcijos paviršiaus, kuris pritvirtinamas ant vibrostendo. Yra svarbu patikrinti, kad konstrukcija būtų tvirta ir nevibruotų savaisiais dažniais tuo metu, kai pati konstrukcija yra žadinama tam tikru dėsniu. Svarbu paminėti, kad vizualinė dekodavimo procedūra yra pagrįsta judesiais plokštumoje, o ne judesiais iš plokštumos. Struktūriniai parazitiniai konstrukcijos virpesiai atsirandantys dėl prasto tvirtinimo, tam tikrų vidinių konstrukcijų įtrūkimų ar laisvumų, gali sukelti paties

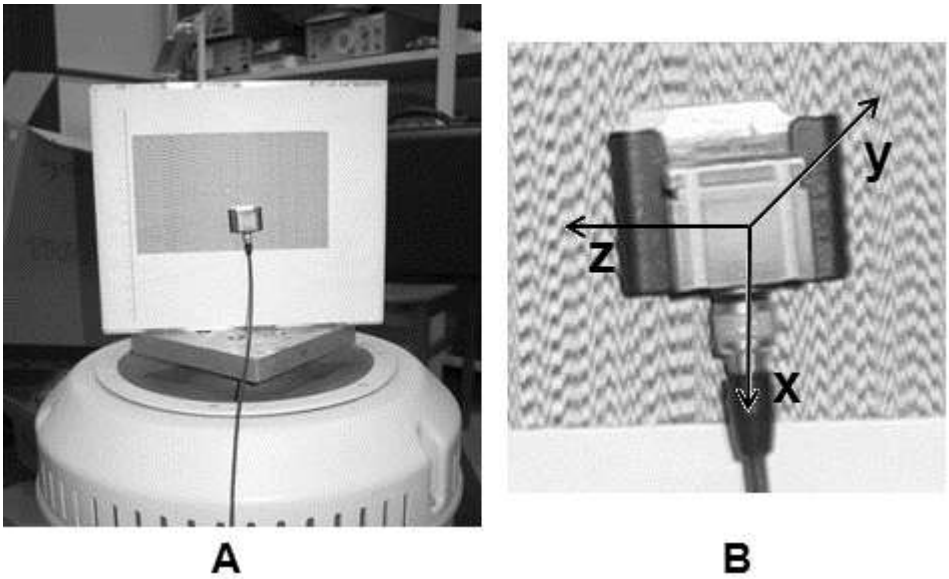
rėmelio nepageidautinus virpesius, kurie gali trukdyti kokybiškam vizualiniam dekodavimui.

Konstrukcijos tikrinės reikšmės

Norint išsiaiškinti kokios yra laikančiosios konstrukcijos tikrinės reikšmės buvo atliktas eksperimentas. Eksperimento įranga: virpesių generatorius, vibrostendas, rėmelis ant kurio tvirtinamas akcelerometras, signalo analizatorius, signalo stiprintuvas pavaizduoti 4.10 paveiksle.

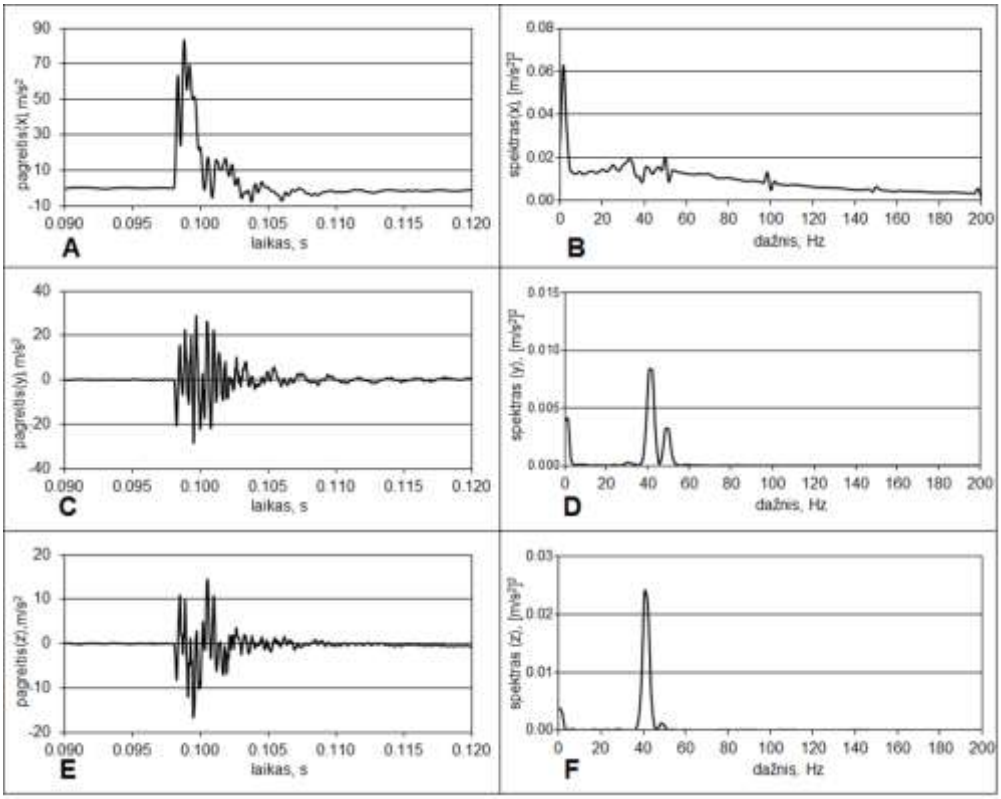
4.10 pav. Eksperimentinė įranga konstrukcijos patikimumui patikrinti

Prie konstrukcijos pritvirtintas trimatis akcelerometras (4.11 pav.), kuris fiksuoja judesius trimis kryptimis: *x* ašyje – iš viršaus į apačią, *y* ašyje – statmenai plokštelei, *z* – ašyje iš dešinės į kairę.



4.11 pav. Tikrinių reikšmių nustatymui naudojamas trimatis akcelerometras (A); akcelerometro kryptys (B)

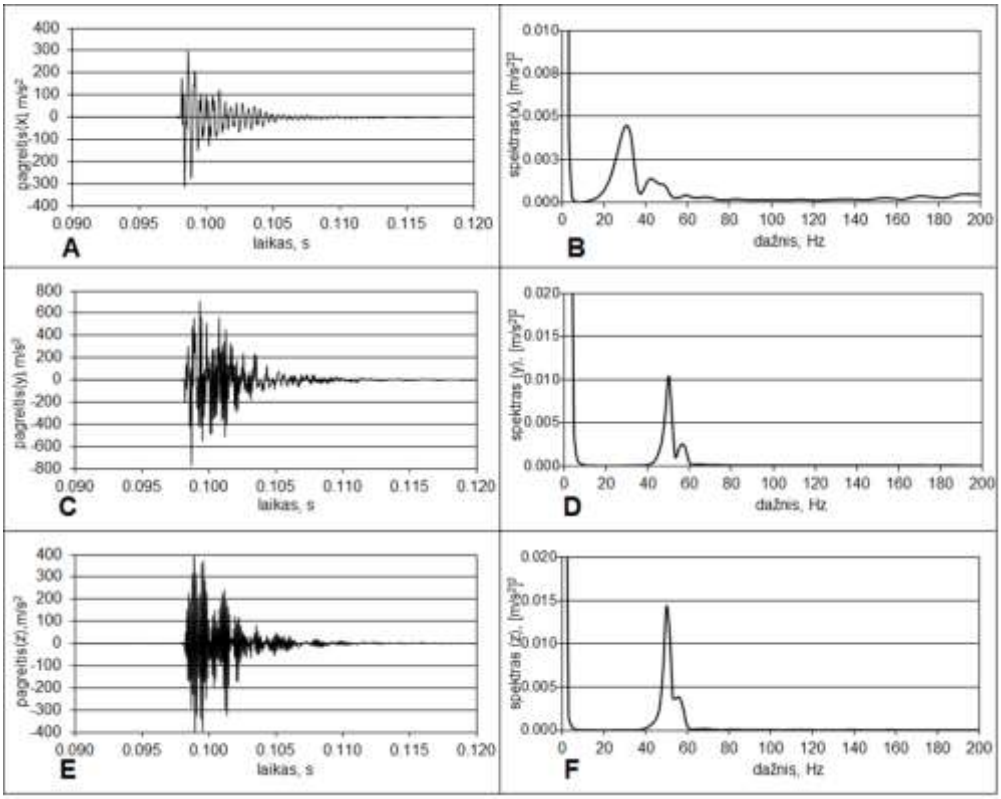
Generatoriumi Agilent 33220A buvo generuojami stačiakampio formos impulsai, kurių dažnis 1 Hz, o trukmė iki 200 ms, kadangi impulsai žadinami *x* ašies kryptimi, tai šia kryptimi gauti akcelerometro parodymai (4.12 pav.) nėra labai tikslūs. Eksperimentui pasirinkti stačiakampiai judesiai tam, kad būtų lengviau sužadinti tikrines įrangos formas ir tikrinius dažnius. Impulso Furjė transformacija apima visus dažnius ir atvirkščiai balto triukšmo transformacija yra vienas impulsas. Tam, kad nebūtų vien tik impulsinės charakteristikos yra paduodamas stačiakampis signalas, vadinasi nuolat atliekamas balto triukšmo sužadinimas, žadiname visas dažnio komponentes kurios yra šioje konstrukcijoje. Tokiu būdu „turtingiau“ suskambės užslėpti konstrukcijos dažniai, kurie yra susiję su kokiais tai konstrukcijos trūkiais, netobulumais suvirinimo taškuose ar konstrukcijos laisvumais, kurie gali iššaukti nepageidautinus virpesius, pvz. skersine kryptimi. Signalo realizacija laike pavaizduota 4.12 paveikslo A, C, E dalyse.



4.12 pav. Stačiakampio formos signalo realizacija laike ir prie atitinkamų dažnių atsiradusios amplitudės *x*, *y* ir *z* kryptimis

4.12 paveikslo B, D ir F dalyse parodoma atėjusio signalo prie atitinkamų dažnių atsiradusios amplitudės *x*, *y* ir *z* kryptimis. T.y. sužadinamas signalas matomas *x* kryptimi, kurio amplitudė šia kryptimi didelė, o *y* ir *z* kryptimis beveik lygi nuliui. Matome, kad konstrukcija yra patikima: *x* ašimi svyruoja, o kitomis kryptimis signalo beveik nėra. Pagrindinės Furjė spektro amplitudės *x* ašies kryptimi yra susikoncentravusios prie žemų dažnių, t.y. prie tokių dažnių kuriais ir yra žadinama konstrukcija. Rezonansiniai dažniai *y* ir *z* kryptimis gaunami toliau nuo spektro pradžios. Konstrukcija turi aukštesnių parazitinių dažnių, bet jie yra pakankamai toli nuo mus dominančių reikšmių. Jei eksperimentas atliekamas dažniams esant iki 30 Hz, tai šie dažnai yra prie 300 Hz. Taigi, tas visiškai nekenkia vizualinei kriptografijos dekodavimo sistemai.

Konstrukciją paveikus formų žadinimo plaktuku, tuo momentu aiškiai pastebima reakcija visomis trimis kryptimis (4.13 pav. A, C, E dalys). Šiuo atveju konstrukcija „suskambėjo“ visomis ašimis, taip atsitinka esant aukštiems dažniams, kas netrukdo registracijos kokybei: amplitudės yra pakankamai mažos (4.13 pav. B, D, F dalys), matome, kad šie virpesiai gana greit užgęsta vadinasi konstrukcijos slopinimas yra didelis. Galima teigti, kad konstrukcija yra tinkama planuojamiems eksperimentams atlikti.



4.13 pav. Formų žadinimo plaktuku sukelto signalo realizacija laike ir prie atitinkamų dažnių atsiradusios amplitudės *x*, *y* ir *z* kryptimis

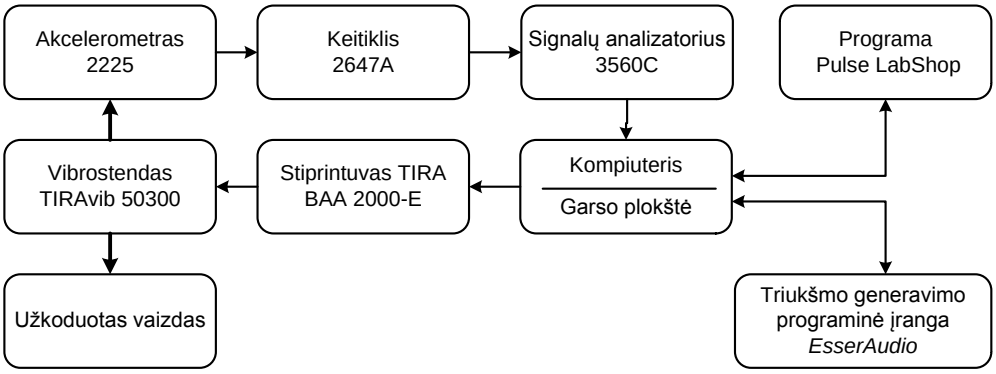
Kaip matoma savi dažniai atsiranda prie 40 Hz, bet jų amplitudės yra mažos, todėl konstrukcijai įtakos beveik neturi.

Šis tyrimas buvo atliktas tam, kad patikrinti konstrukcijos tinkamumą vizualinės kriptografijos tyrimams. Jeigu vizualinės kriptografijos schemos būtų taikomos prietaisų kontrolei inžineriniuose pramoniniuose taikymuose tai nereiškia, kad visą konstrukciją reiks prie kažko tai prisukti, tiesiog ant virpančios konstrukcijos paviršiaus bus klijuojamas koduotas vaizdas. Tarkim, stebimi kokio nors vamzdžio svyravimai, ar kokios nors platformos chaotiniai virpesiai, tai ant lipnios plėvelės atspausdintas koduotas vaizdas tiesiogiai klijuojamas ant to paviršiaus. Tada jau nebebus jokių parazitinių savųjų dažnių ar savųjų formų. Šis tyrimas atliktas tik tam, kad validuoti eksperimentinės įrangos specialiąją laikančiąją konstrukciją, kuri tvirtinama prie vibrostendo.

Dinaminės vizualinės kriptografijos pagrįstos chaotiniais virpesiais eksperimentinė realizacija

Eksperimento schema pavaizduota 4.14 pav. Vibrostendas TIRAvib 50300 yra valdomas stiprintuvu TIRA BAA 200-E. Triukšmo generavimo programinė įranga EsserAudio generuoja baltą triukšmą, jį perleidžia per žemo dažnio filtrą (nustatomas diapazonas nuo 0 iki 100 Hz) ir signalas siunčiamas į stiprintuvą. Užkoduotas vaizdas yra klijuojamas ant rėmelio prie kurio pritvirtinamas

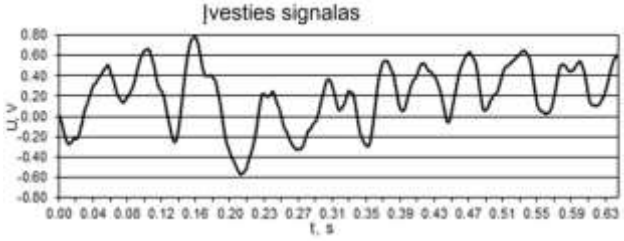
lengvasvoris pjezoelektrinis akcelerometras Endevco 2225, kurio jautrumas 0,07655 pC/m/s^2. Pati konstrukcija montuojama ant vibrostendo darbinio paviršiaus, tuo tarpu akcelerometro išėjimas yra prijungiamas prie analizatoriaus „Pulse Multi-analyzer system Type 3560“ per krūvio-įtampos keitiklį tipo 2647A, kurio stiprinimas yra 1mV/pC; visas procesas yra kontroliuojamas Bruel&Kjaer Pulse LabShop. Taigi, yra ne tik sukuriami žemų dažnių chaotiški virpesiai, bet ir kontroliuojama vibrostendą veikiančių virpesių bangos forma. Kitaip sakant yra galimybė nustatyti, stebėti ir kontroliuoti chaotinių virpesių parametrus.



4.14 pav. Eksperimento schema

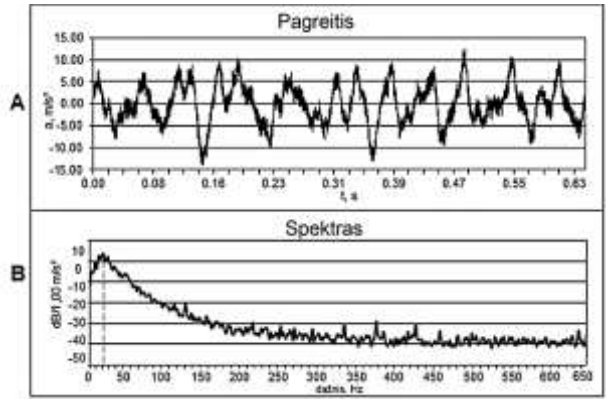
4.4.3. Eksperimento rezultatai

Koduotas paveikslėlis, kuris pavaizduotas 4.8B paveiksle yra priklijuojamas ant vertikalios plokštės pritvirtintos ant vibrostendo pagrindo (4.9 pav). Filtruoto triukšmo generatorius yra nustatomas generuoti 30 s trukmės balto triukšmo signalus ir juos filtruoja žemų dažnių filtru (dažnis prie kurio pasiekiamas amplitudės maksimumas yra lygus 30 Hz). Žemo dažnio filtras naudojamas siekiant imituoti netiesiniais chaotiniais mechaninių sistemų vibracijas. Vibrostendas negalėtų vibruoti 10 kHz dažniu. Įvesties signalo paduodamo į TYRA stiprintuvą momentinis vaizdas yra pateiktas 4.15 pav.



4.15 pav. Paduodamo signalo momentinis vaizdas

Vibrostendo generuojami virpesiai yra registruojami pjezoelektriniu akcelerometru (4.9 pav.). Signalo realizacija laike pavaizduota 4.16A pav.

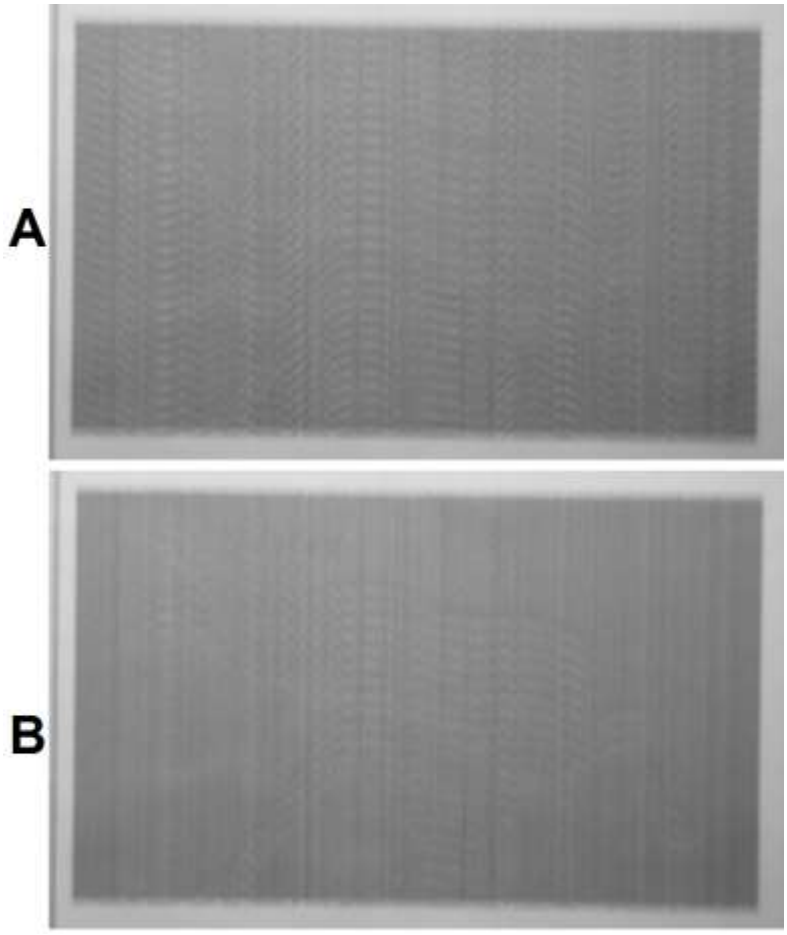


4.16 pav. Signalo realizacija laike

Įrašytas signalo spektras yra parodytas 4.16B pav. – galima aiškiai pamatyti, kad maksimali signalo spektro reikšmė pasiekiama kai dažnis yra 22 Hz, tai beveik atitinka didžiausią žemų dažnių filtro reikšmę.

Dinaminės vizualinės kriptografijos pritaikymas periodinių virpesių kontrolei yra aprašytas 3 skyriuje. Verta priminti, kad harmoninių virpesių dažnis neturi jokios įtakos muaro interferencinių juostų formavimuisi, tik ekspozicijos laikas turi būti pakankamai ilgas, kad jame tilptų bent keli harmoninių virpesių periodai. Kaip jau buvo pastebėta 25-30 Hz yra pakankamas dažnis plika akimi interpretuoti koduotą vaizdą veikiamą harmoniniais virpesiais. Tas taip pat paaiškina dinaminės vizualinės kriptografijos taikymą chaotiniams virpesiams. Chaotinė vizualinė kriptografija neveiktų jei chaotinių virpesių spektro reikšmės telktųsi pavyzdžiui apie 0,1 Hz dažnį – žmogaus plika akis negalėtų dekoduoti lėtai judančio koduoto vaizdo. Laike vidurkintas vaizdas formuojasi kai akis nespėja sekti greitai vibruojančio koduoto paveikslo.

Tas pats tinka ir skaitmeniniam fotoaparatui. Ekspozicijos trukmė turi būti pakankamai ilga, kad joje tilptų pakankamas virpesių proceso intervalų skaičius. 4.16A paveiksle ekspozicijos trukmė lygi 0,63 s nėra pakankama tipiniai chaotinių virpesių bangos formai pavaizduoti, bet pakankama, kad galėtume interpretuoti slaptą vaizdą, pastebime, kad plika akimi vaizdas yra ryškesnis nei gaunamas fotoaparatu (4.17 pav), taip yra dėl trumpo ekspozicijos laiko.



4.17 pav. Slaptos informacijos dekodavimas chaotiniais virpesiais

Eksperimento metu įvesties signalo parametrai nesikeitė – vienintelis parametras kuris kito kontrolinio signalo stiprinimas. Koduotas vaizdas lieka pradinėje padėtyje, kai atsilenkimas nuo pusiausvyros padėties lygus nuliui – slaptas vaizdas koduotame paveiksle nematomas. Atsitiktinių chaotinių virpesių reikšmių standartas padidėja kai stiprinimas padidinamas. Slaptą vaizdą galime įžvelgti 4.17 pav. A dalyje, bet interferencinės juostos nėra susiformavusios nei slapto vaizdo nei fono vietose. Slaptas vaizdas ryškiau matomas (4.17B pav.), kai stiprinimas yra didesnis – interferencinės juostos fone dar nėra pilnai susiformavusios.

4.5. Skyriaus išvados

Šiame skyriuje gautas naujas rezultatas, kai dinaminė vizualinė kriptografija taikyma chaotiniams virpesiams. Teorinė analizė rodo, kad chaotiniai virpesiai neformuoja laike vidurkintų interferencinių juostų – laike vidurkintas paveikslas visada užpilkėjęs jei chaotinių virpesių intensyvumas yra padidėjęs. Bet pilkio rodiklis yra jautrus koduoto paveikslo muaro gardelės žingsniui. Šis optinis efektas

leidžia konstruoti vizualinės kriptografijos sistemą, kai slaptą informaciją galime pamatyti koduotą vaizdą virpinant chaotiškai. Be to, muaro gardelės žingsnį koduotame paveiksle, galime iš anksto parinkti tokį, kad slaptas vaizdas išryškėtų esant atitinkamam chaotinių virpesių intensyvumui, kurį galime reguliuoti vibrostendo maitinimo ir valdymo bloko pagalba.

Fone ir slapto vaizdo vietose laike vidurkintų muaro juostų skirtingą formavimąsi apsprendžia skirtingas jų gaubiančiųjų funkcijų slopimo greitis.

Yra žinoma, kad judesio sukeltas užpilkėjimas, gali būti naudojamas tam judesiui identifikuoti [85][86]. Šis metodas nesiremia pilkio dekodavimo ar trajektorijos atstatymo metodais. Chaotiniais virpesiais tiesiogiai optiškai interpretuojame laike vidurkintą vaizdą. Be to žinoma, kad optiniai metodai gali būti naudojami siekiant iliustruoti ar modeliuoti chaotinius procesus. Tipinis pavyzdys gali būti fraktalinės geometrijos optinis demonstravimas [87]. Šiame skyriuje nagrinėjamame optiniame metode nėra naudojami jokie veidrodžiai ar sudėtingi vaizdai. Tai yra optinis metodas kuris gali būti efektyviai panaudotas įvertinant chaotinius procesus plika akimi. Galima atspausdinti koduotą vaizdą ir priklijuoti ant paviršiaus, kurio virpesius norime kontroliuoti. Slapto vaizdo nesimatys jei paviršius nejudės. Skaitmeninio vaizdo dekodavimo schema gali būti parinkta tokiu būdu, kad slaptas vaizdas pasirodys kai chaotinių virpesių parametrai pateks į iš anksto nustatytą priimtinų reikšmių intervalą.

5. DINAMINĖS VIZUALINĖS KRIPTOGRAFIJOS TAIKYMAS ŽMOGAUS REGOS SISTEMOS TYRIMAMS

Šiame disertacijos skyriuje bus parodyta, kad dinaminės vizualinės kriptografijos optinius efektus galima realizuoti panaudojant optinius efektus skaitmeninių kompiuterių ekranuose. Tam buvo sukurtas dinaminės vizualinės kriptografijos principu funkcionuojantis įrenginys, įgalinantis vertinti žmogaus regos sistemos funkcionalumą. Šio įrenginio pagrindą sudaro nešiojamasis arba planšetinis kompiuteris su specializuota programine įranga, įgalinančia kompiuterio ekrane realizuoti dinaminės vizualinės kriptografijos efektus. Dinaminės vizualinės kriptografijos skiriamasis bruožas yra tas, kad informacijos kodavimui naudojami specialūs algoritmai, tuo tarpu slapto vaizdo dekodavimui kompiuterio nereikia – slaptas vaizdas formuojasi interferencinių juostų rašto forma, kai užkoduotasis vaizdas virpinamas tiksliai nustatytu dėsniu. Tačiau žmogaus regos sistema pradeda matyti slaptą vaizdą tik tuomet, kai akis nebegali sekti greitai svyruojančio objekto, ir žmogaus smegenyse susiformuoja slaptasis užkoduotasis vaizdas [79]. Šį kritinį dažnį (kai žmogus pamato slaptą informaciją) nesunku nustatyti individualiai kiekvienam žmogui tolygiai didinant virpesių dažnį. Šis kritinis dažnis gali tarnauti kaip svarbi diagnostinė regos sistemos charakteristika bei pasitarnauti įvertinant žmogaus nuovargį.

Norint sukurti šį įrenginį, teko išspręsti visą eilę svarbių teorinių ir praktinio realizavimo problemų, buvo išvesti sąryšiai, susiejantys pikselio išmatavimus, judesio parametrus, ekrano fizines charakteristikas bei dinaminės vizualinės kriptografijos būdu formuojamo laike vidurkinto vaizdo vizualinį interpretavimą, bei leidžiantys efektyviai koduoti slaptą vaizdą stochastinėse muaro gardelėse. Taip pat buvo įvertini stochastinių muaro gardelių vizualizavimo ypatumai kompiuterio ekrane.

5.1. Problemos susijusios su ekrano atnaujinimo dažniu

Dinaminėje vizualinėje kriptografijoje vaizdas dekoduojamas virpinant statinį užkoduotą vaizdą pagal iš anksto žinomus virpesių parametrus bei virpinimo dėsnį. Jei dekodavimo procedūra atliekama naudojant vibrostendą, būtina sąlyga susiformuoti laike vidurkintoms juostoms, kurias matys žmogaus akis – pakankamas virpesių dažnis. Šis dažnis turi būti toks, kad žmogaus regos sistema nepajėgtų sekti judančio vaizdo. Taigi gauname, kad dažnis turėtų būti bent 20 Hz. Realiame eksperimente, pavyzdžiui naudojant harmoninius virpesius, gaunama, kad tarpinių vaizdų skaičius viename virpesių periode artėja iki begalybės. Nors atskirų mažai paslinktų vaizdų regos sistema nefiksuoja, tačiau esant pakankamam dažniui suvidurkina visą vaizdą – matomos susiformavusios laike vidurkintos juostos.

Tokį patį eksperimentą galima atlikti ne tik vibrostendo pagalba, bet ir kompiuterio ekrane. Tačiau šiuo atveju susiduriama su visa eile problemų. Jei vibrostendo stalas juda tolygiai, tai vaizdas rodomas kompiuterio ekrane yra kilnojamas netolygiai. Tai yra dėl to, kad monitorius yra sudarytas iš baigtinio skaičiaus taškų – pikselių. Kiekvienas mažiausias statinio vaizdo postūmis gali būti atliekamas vieno pikselio ribose. Vieno pikselio riba nevienintelė pikselių dydžio

problema, kadangi virpinant vaizdą pavyzdžiui pagal harmoninį dėsnį atskirais laiko momentais turime statinį vaizdą perkelti nebūtinai per sveiką pikselių skaičių. Tokiu atveju reikia vaizdo postūmį apvalinti iki sveikosios reikšmės. Kita problema susidaro dėl baigtinio ekrano atnaujinimo dažnio. Daugumos standartinių ekranų atnaujinimo dažnis yra 60 Hz. Net ir padidinus dažnį iki 100 Hz problema nebūtų išspręsta, kadangi pavyzdžiui harmoninių virpesių periodas turi būti sudarytas bent iš 32 postūmių. Gauname vos daugiau nei tris virpesių periodus. Tokio dažnio nepakanka, kad žmogaus regos sistema pradėtų sulieti virpantį vaizdą, kadangi vis dar pajėgtų sekti besikilnojantį paveikslą. Kaip jau buvo minėta, harmoninio tipo virpesiams reikia bent 32 kadrų postūmių per periodą. Įvertinus būtiną mažiausią 20 Hz dažnį gaunama, kad ekrano dažnis turi būti 640 kadrų per sekundę. Remiantis šiais skaičiavimais galime teigti, kad šios virpesių rūšies tiesiog negalime realizuoti kompiuterio ekrane.

Problemą galima spręsti koreguojant virpesių dėsnį. Žinomi būdai, kaip suformuoti statinį vaizdą, kad virpesiai būtų „pjūklo“ ar „zig-zag“ tipo. Bendru atveju, kaip ir esant harmoniniams virpesiams, čia taip pat susiduriama su poslinkių per nepilną pikselį problema. Tačiau ši problema nėra tokia ryški, kadangi lengva pareikalauti, kad postūmiai būtų atliekami reikiamu pikselių skaičiumi. Šie virpesių dėsniai dėkingesni už harmoninį tuo, kad šiuo atveju galima išvengti didelio kadrų skaičiaus viename virpesių periode. Jei harmoninių virpesių atveju reikalavome, kad virpesių periodas būtų sudarytas bent iš 32 poslinkių, tai duotuoju atveju minimalus poslinkių skaičius yra 4. Be abejo šis mažiausias skaičius iššaukia ir eilę apribojimų: amplitudė neturėtų būti didelė, kadangi tai iššauktų „grubius“ užkoduoto statinio vaizdo poslinkius, muaro gardelė, atitinkanti mažas virpesių amplitudes, turi būti sudaryta iš nedidelio pikselių skaičiaus. Šis trūkumas tiesiogiai įtakoja statinio užkoduotą vaizdo kokybę. Pakankamas postūmių skaičius būtų 12 kadrų eilės, tačiau ir šis kadrų skaičius, įvertinant reikiamą 20 Hz dažnį generuoja 240 kadrų per sekundę.

Riboto kompiuterio ekrano dažnio problemą galima išspręsti įvedant ribinius užkoduoto statinio vaizdo atsilenkimus. Šis metodas reikalauja tik dviejų poslinkių – kadrų per periodą. Gauname, kad standartinis 60 Hz dažnio kompiuterio ekranas sugeba atvaizduoti 30 virpesių periodų per sekundę. Šio virpesių dažnio paprastai pakanka, norint sėkmingai vizualizuoti virpančius vaizdus.

Atsižvelgiant į aukščiau aprašytus samprotavimus, susijusius su slapto vaizdo dekodavimo funkcijų parinkimu, įrenginio konstravimui nuspręsta naudoti stochastinių muaro gardelių metodiką, kai užkoduotas vaizdas yra maksimaliai deformuojamas kraštinių atsilenkimų būsenose, o vaizdo įterpimui į stochastinę muaro gardelę naudojami fazių reguliarizacijos ir pradinės fazės stochastizacijos algoritmai.

Charakteringosios funkcijos, aprašančios laike vidurkintų interferencinių juostų formavimąsi laiptuoto diskretinio dėsnio atveju, kai stochastinė muaro gardelė gali būti perstumiama nuo pusiausvyros padėties tik per sveiką pikselių skaičių, teoriniai matematiniai tyrimai aprašyti šios disertacijos antrajame skyriuje. Toliau aprašomas dinaminės vizualinės kriptografijos principu funkcionuojančio žmogaus regos sistemos funkcionalumą įvertinančio įrenginio maketo aprašymas.

5.2. Dinaminės vizualinės kriptografijos pagrindu funkcionuojančio žmogaus regos sistemos tyrimo maketo trumpas aprašymas

Realizuojant dinaminės vizualinės kriptografijos optinius efektus buvo sukurtas pilnai funkcionuojantis kompiuterinis įrenginys, skirtas žmogaus regos sistemos tyrimui.

Pagrindinė ir esminė maketo dalis – tai slapto vaizdo kodavimas stochastinėje muaro gardelėje (panaudojant fazių reguliarizavimo ir pradinių fazių chaotizavimo algoritmus), bei užkoduoto vaizdo virpinimas kompiuterio ekrane pagal nustatytą dėsnį. Svarbiausia maketo savybė – tai galimybė sudaryti norimą virpesių dėsnį ir reguliuoti slapto vaizdo virpesių dažnį, kai jis juda pagal nustatytąjį dėsnį. Dažnis didinamas tol, kol žmogus sugeba perskaityti užkoduotąjį vaizdą.

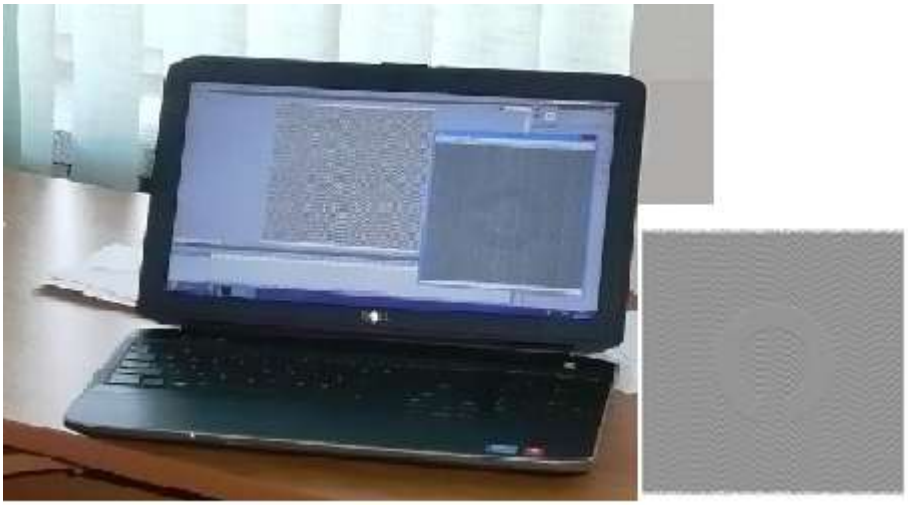
Pats slapto vaizdo kodavimo procesas reikalauja specialių algoritmų pritaikymo – su įrenginiu dirbančiam žmogui pateikiama jau paruošta užkoduotųjų vaizdų biblioteka.

Žmogaus regos sistemos tyrimams naudojami įvairūs slapti vaizdai, kuriuos galima pasirinkti iš standartinių iš anksto paruoštų (ir užkoduotų) vaizdų bibliotekos. Galima naudoti ir standartinius simbolius (apskritimo lankus) ar tekstą, susidedantį tiek iš didžiųjų, tiek ir iš mažųjų raidžių.

Tyrimo metu pastebėta, kad geriausiai pacientų regos sistemų diagnostikai, naudojantis dinaminės vizualinės kriptografijos principais, tinka vaizdai kuriuose nėra smulkių užraitymų, taškų, vertikalių plonų linijų, tolimesniuose tyrimuose rekomenduojama naudoti geometrines figūras, tokias kaip trikampis, kvadratas ir panašiai. Formuojant kiekvieną slaptą vaizdą atsižvelgiama į stochastinės muaro gardelės struktūrą, judesio dėsnį, slaptos informacijos kiekį, kurį galima išsaugoti konkrečioje koduotoje gardelėje. Bibliotekoje saugomi jau užkoduotieji vaizdai, o kiekvienam užkoduotam vaizdui priskiriama dekodavimo funkcija – dėsnis pagal kurį tas vaizdas turi būti virpinamas.

Taigi, norint vaizdą dekoduoti, reikia jį virpinti žinomu dėsniu ir amplitude (iš principo dekodavimui kompiuteris nereikalingas). Šiuo atveju naudojamas ne vibrostendas, o Adobe Flash Professional CS6 programa, kuri optimaliai išnaudoja kompiuterinius resursus statinio vaizdo virpinimui pagal nustatytą dėsnį ir dažnį.

Įrenginio nuotrauka darbiniame režime, bei susiformuojantis laike vidurkintas vaizdas, kuriame išryškėja užkoduotasis slaptasis vaizdas, pavaizduoti 5.1 paveiksle.



5.1 pav. Dekoduojamas slaptas vaizdas virpesių, kompiuterio ekrane, būdu

Sukurtas maketas yra pilnai funkcionalus ir gali būti naudojamas žmogaus regos sistemos funkcijų tyrimui. Platesnis sukurtos programinės įrangos, kuri veikia LMSU Akių klinikoje aprašymas pateikiamas 2 priede.

Atlikti eksperimentiniai žmogaus regos sistemos tyrimai ir gautų rezultatų analizė aprašomi kitame skyrelyje.

5.3. Eksperimentiniai žmogaus regos sistemos tyrimai

Naudojantis sukurtu eksperimentiniu įrenginiu buvo atliktas eksperimentas. Juo siekiama nustatyti faktorius nuo kurių priklauso kritinio dažnio, prie kurio akis atpažįsta slaptą vaizdą, reikšmė. Siekta nustatyti kokia turi būti virpesių dažnio reikšmė: pakankamai didelė ar žmogaus akis vaizdą geba atpažinti ir jo nevirpinant. Šio eksperimento metu buvo tirtas žmogaus regos sistemos gebėjimas atpažinti užkoduotus vaizdus priklausomai nuo respondento lyties, amžiaus, paros laiko.

Eksperimento metu buvo naudojami užkoduoti raidžių deriniai, dekodavimas vyko plika žmogaus akimi, ekrane atpažįstant slaptąjį vaizdą. Šiame tyrime dalyvavo 60 skirtingo amžiaus respondentų. Kiekvienam iš jų teko atpažinti dešimt dinaminės vizualinės kriptografijos metodu užkoduotų vaizdų, tokiu būdu buvo bandoma tiksliai nustatyti virpesių dažnį prie kurio respondento akis geba identifikuoti slaptą vaizdą, o ne jį atspėja. Surinkus duomenis atlikta jų statistinė analizė.

5.4. Duomenų statistinė analizė

Gauti duomenys lyginami tarpusavyje, tiriama nuo ko priklauso gauta virpesių dažnio reikšmė. Eksperimente dalyvavo šešiasdešimt žmonių: 27 – moterys bei 33 – vyrai (5.1 lent.).

5.1 lentelė. Respondentų amžiaus lentelė

Lytis	Moterys	Vyrai
Respondentų skaičius	27	33

Respondentų amžiaus 5.2 lentelėje pateikta informacija apie tiriamų asmenų amžių. Jauniausias tyrimo dalyvis 18 metų amžiaus, vyriausias – 54 metų. Daugiausia respondentų patenka į amžiaus grupę nuo 18 iki 24 metų. Vidutinis respondentų amžius buvo 30 metų.

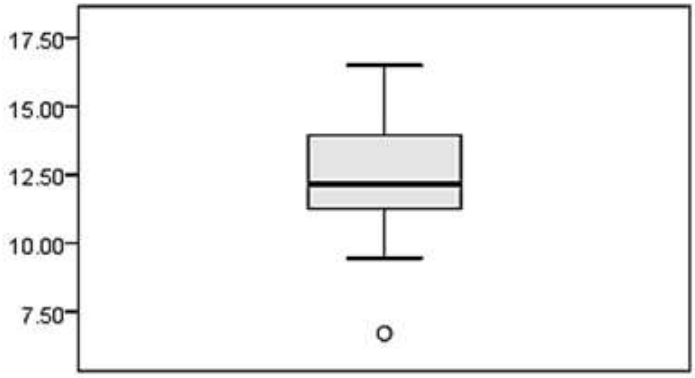
5.2 lentelė. Respondentų amžiaus lentelė

Amžius	Nuo 18 iki 24	Nuo 24 iki 30	Nuo 30 iki 36	Nuo 36 iki 42	Nuo 42 iki 48	Nuo 48 iki 54
Respondentų skaičius	26	8	8	9	4	5

Kiekvienam respondento dekoduotam paveikslui nustatytas individualus virpesių dažnis, prie kurio regos sistema geba atpažinti tikrąjį vaizdą, pagal gautus duomenis apskaičiuotas virpesių dažnio vidurkis kiekvienam tiriamam žmogui. Nustatytos visų duomenų bendros skaitinės charakteristikos: vidurkis (*EX*), dispersija (SD^2)standartinis nuokrypis (*SD*), mediana (*Me*), moda (M_0), minimumas (*Min*), maksimumas (*Max*), imties plotis (*IP*). Rezultatai pateikti 5.3 lentelėje, 5.3 paveiksle pateikta virpesių dažnių vidurkio stačiakampė diagrama.

5.3 lentelė. Duomenų skaitinės charakteristikos

EX	SD^2	*SD*	*Me*	M_0	*Min*	*Max*	*IP*
12.42	3.378	1.822	12.15	11.7	6.7	16.5	9.8

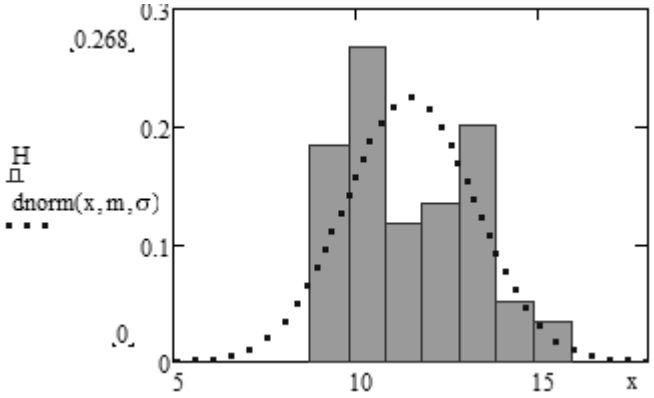


5.3 pav. Virpesių dažnių vidurkio stačiakampė diagrama

Remiantis Chi kvadrato suderinamumo kriterijumi buvo patikrinta neparametrinė hipotezė apie gautų duomenų skirstinio tipą. Suformuluotos hipotezės:

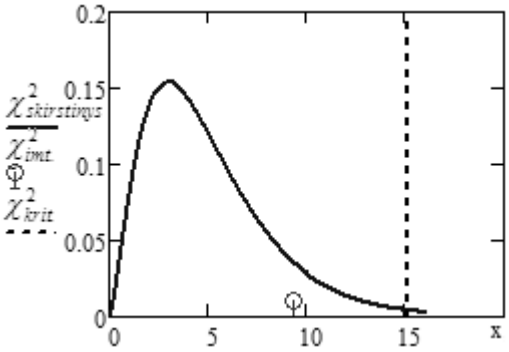
$$H_0 : X \sim N(\mu, \sigma)$$
$$H_a : X \neq N(\mu, \sigma) \quad (5.1)$$

Imtis sudaryta iš 60 reikšmių, todėl pasirinkti 7 grupavimo intervalai. Jau anksčiau rastas imties vidurkis ir standartinis nuokrypis.



5.4 pav. Duomenų histograma ir normaliojo skirstinio tankio funkcija

Visi duomenys priskiriami atitinkamiems intervalams, nubraižoma duomenų histograma ir normaliojo skirstinio tankio funkcijos grafikas (5.4 pav.). Gauta histograma nevisiškai sutampa su normaliojo skirstinio tankio kreive, bet ir labai nesiskiria, galima daryti prielaidą, kad virpesių dažnis gali būti pasiskirstęs pagal normalųjį skirstinį. Reikšmingumo lygmuo parenkamas lygus $\alpha = 0.01$. Randama imties statistikos reikšmė $\chi^2_{imt.} = 9.368$. Randamas kritinis Chi kvadrato suderinamumo kriterijaus taškas $\chi^2_{krit..} = 13.277$. Kadangi $\chi^2_{imt.} < \chi^2_{krit.}$, hipotezė H_0 neatmetama, su 99% tikimybe galima teigti, kad virpesių dažnio skirstinys pasiskirstęs pagal normalųjį dėsnį. Gauti rezultatai pavaizduoti 5.5 paveiksle.



5.5 pav. Neparametrinės hipotezės apie skirstinio normalumą grafiniai rezultatai

Kai jau žinoma, kad virpesių dažnių skirstinys pasiskirstęs pagal normalųjį dėsnį, galima rasti skirstinio vidurkio pasikliautinąjį intervalą. Pasikliautinojo intervalo radimui parenkame statistiką (5.2), kuri turi Stjudento skirstinį su *n*-1 laisvės laipsnių:

$$\frac{EX - m}{SD}\sqrt{n} \qquad (5.2)$$

Vidurkio pasikliautinasis intervalas randamas pagal formulę (5.3).

$$\left(EX - t_{1-\frac{\alpha}{2};n-1} \frac{SD}{\sqrt{n}};\quad EX - t_{\frac{\alpha}{2};n-1} \frac{SD}{\sqrt{n}} \right) \tag{5.3}$$

$t_{1-\frac{\alpha}{2};n-1}$, $t_{\frac{\alpha}{2};n-1}$ žymi Studento skirstinio $\alpha/2$ ir $1-\alpha/2$ lygmens kvantilius, n – imties tūris. Šiuo atveju vidurkio pasikliautinasis intervalas yra (11.78; 13.05), vadinasi su 99% tikimybe galima teigti, kad vidutinis virpesių dažnis prie kurio žmogaus akis atpažįsta slaptą vaizdą, yra nuo 11.78 iki 13.05.

Ieškant dispersijos pasikliautinojo intervalo parenkama statistika, kuri turi Chi kvadrato skirstinį su n-1 laisvės laipsnių:

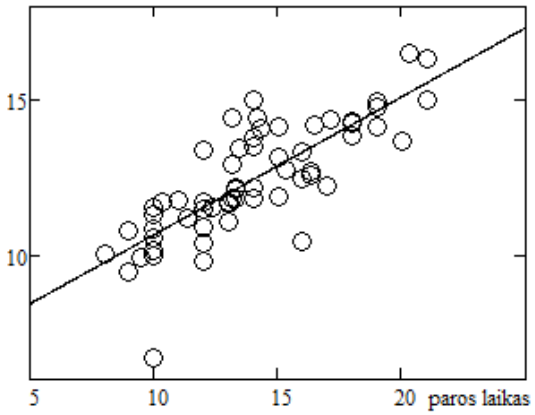
$$\frac{SD^2 \cdot (n-1)}{\sigma^2} \tag{5.4}$$

Dispersijos pasikliautinasis intervalas randamas pagal formulę (5.5):

$$\left(\frac{(n-1) \cdot SD^2}{\chi^2_{1-\frac{\alpha}{2},n-1}};\quad \frac{(n-1) \cdot SD^2}{\chi^2_{\frac{\alpha}{2},n-1}} \right) \tag{5.5}$$

$\chi^2_{1-\frac{\alpha}{2},n-1}$, $\chi^2_{\frac{\alpha}{2},n-1}$ žymi chi kvadrato skirstinio $\alpha/2$ ir $1-\alpha/2$ lygmens kvantilius. Surastas dispersijos pasikliautinasis intervalas, kuris lygus (2.197; 5.731), su 99% tikimybe galima teigti, kad virpesių dažnio dispersija yra intervale nuo 2.197 iki 5.73.

Tirta, ar individuali žmogaus virpesių dažnio vidurkio reikšmė, prie kurios atpažįstamas slaptas vaizdas priklauso nuo paros laiko. Tuščiaviduriai rutuliukai (5.6 pav.) tai taškai kurių *x* koordinatė paros laikas, *y* koordinatė virpesių dažnio vidurkis. Matoma, kad jie grupuojasi aplink tiesę. Spėjama, kad tarp kintamųjų gali būti tiesinis ryšys. Apskaičiavus Pirsono koreliacijos koeficientą gauta, kad jis lygus 0.792, bei atsižvelgiant į šią priklausomybę galima paaiškinti 62.6% duomenų. Vadinasi, galima teigti, kad tarp paros laiko ir virpesių dažnių vidurkio egzistuoja stiprus tiesinis ryšys.



5.6 pav. Regresijos tiesė, parodanti priklausomybę tarp virpesių dažnio reikalingo žmogaus akiai dekoduoti slaptą informaciją ir paros laiko, apie ją grupuojasi regresijos taškai

Kuo vėlesnis paros metas, tuo spėjama, kad žmogus labiau pavargęs, dėlto reikalingas didesnis virpesių dažnis prie kurio akis vidurkintų koduotą vaizdą ir pamatytų užslėptą informaciją. Surasti regresijos tiesės koeficientai ir užrašyta regresijos tiesės lygtis:

$$\textit{Virpesių dažnių vidurkis} = 0.445 \cdot \textit{paros laikas} + 6.206$$

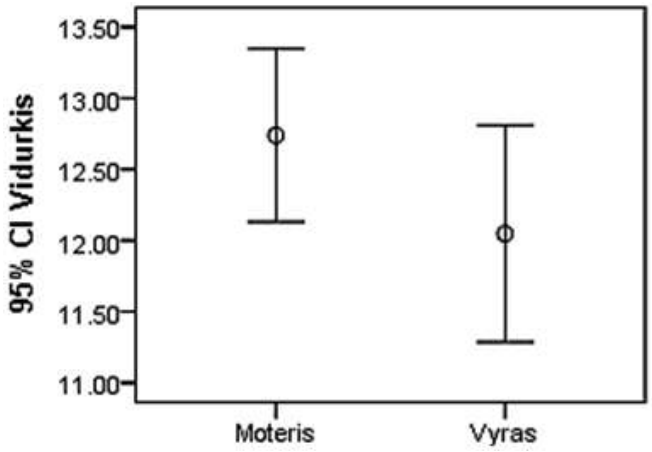
Regresijos tiesė pavaizduota 5.6 paveiksle ištisine linija. Taip pat tirta virpesių dažnio vidurkio reikšmės priklausomybė nuo respondento amžiaus. Pirsono koreliacijos koeficientas gautas lygus 0.308 ir amžiumi paaiškinama tik 9.5% duomenų, tiesinė priklausomybė egzistuoja tačiau ji nėra stipri. Regresijos lygtis būtų:

$$\textit{Virpesių dažnių vidurkis} = 0.0505 \cdot \textit{respondento amžius} + 10.906$$

Ištyrus, kad virpesių dažnių vidurkis priklauso nuo paros laiko ir nuo amžiaus, nagrinėta, o kaip šie faktoriai kartu veikia virpesių dažnio vidurkio reikšmę, pasirodo atsižvelgiant ir į paros laiką ir į respondento amžių koreliacijos koeficientas lygus 0.841 ir šiais dviem dydžiais galima paaiškinti 70.8% visų gautų duomenų. Regresijos lygtis būtų:

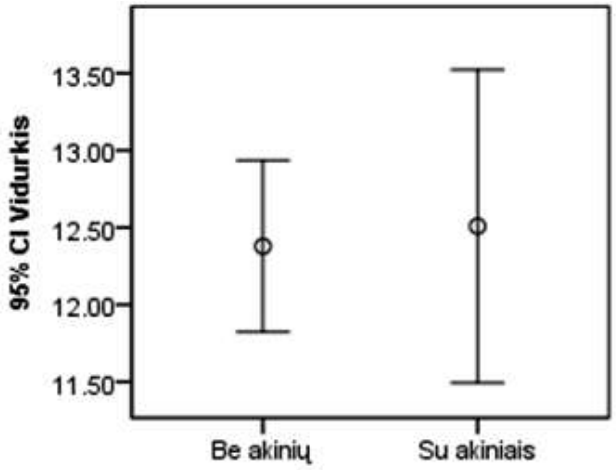
$$\textit{Virpesių dažnių vidurkis} = 0.44 \cdot \textit{paros laikas} + \\ + 0.047 \cdot \textit{respondento amžius} + 4.873$$

Norint išsiaiškinti, ar virpesių dažnių vidurkio reikšmė skiriasi priklausomai nuo lyties, nubrėžti vidurkių pasikliautinieji intervalai, duomenis sugrupavus pagal lytį: atskirai moterims ir atskirai vyrams (5.7 pav.). galima pastebėti, kad vidurkio pasikliautinieji intervalai statistiškai reikšmingai nesiskiria, galima teigti, kad virpesių dažnio reikšmė, prie kurio žmogaus akis atpažįsta slaptą vaizdą nepriklauso nuo lyties, bet vyrams ji šiek tiek mažesnė.



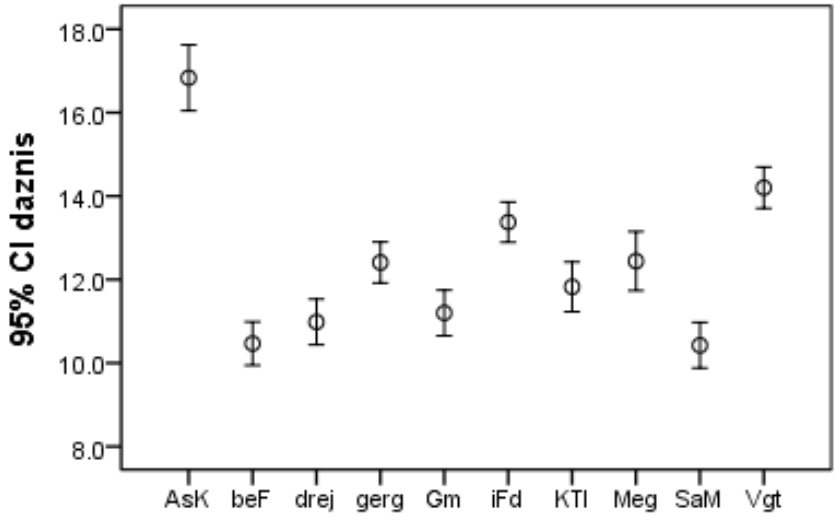
5.7 pav. Virpesių dažnių vidurkių pasikliautinieji intervalai priklausomai nuo lyties

Taip pat buvo siekta išsiaiškinti ar virpesių dažnių vidurkio reikšmė skiriasi priklausomai nuo to ar respondentas nešioja akinius. Nubrėžus vidurkių pasikliautinuosius intervalus atskirai žmonėms nešiojantiems akinius ir nenešiojantiems pastebima, kad statiškai reikšmingo skirtumo nėra, virpesių dažnių reikšmė nepriklauso ar respondentas su akiniais ar be jų (5.8 pav.).



5.8 pav. Virpesių dažnių vidurkių pasikliautinieji intervalai priklausomai nuo to ar respondentas nešioja akinius

Nubrėžus kiekvieno paveikslo virpesių dažnių, prie kurių buvo dekoduotas slaptas vaizdas, pasikliautinuosius intervalus (5.9 pav.), galima pastebėti, kad pirmo paveikslėlio (AsK) virpesių dažnis statistiškai reikšmingai skiriasi nuo kitų paveikslų. Taip gali būti dėl to, kad eksperimento pradžioje respondentai nežino kaip tas dekoduotas paveikslas turi atrodyti, akių regos sistema „apsimoko“ atpažinti slaptąjį vaizdą.



5.9 pav. Vidurkio pasikliautinieji intervalai kiekvienam koduotam paveikslui

5.5. Skyriaus išvados

Atliktu tyrimu siekta parodyti, kad dinaminės vizualinės kriptografijos optinius efektus galima realizuoti panaudojant optinius efektus skaitmeninių kompiuterių ekranuose ir tikrai kompiuterinis vizualinės kriptografijos optinių efektų realizavimas kompiuterių ekranuose yra įmanomas ir įgyvendintas.

Dinaminės vizualinės kriptografijos principu funkcionuojantis žmogaus regos sistemos funkcionalumą įvertinančio įrenginio sukonstravimas yra nepaprastai aktualus tiek medicinine, tiek ir žymiai platesne galimų taikymų prasme. Pirmiausia tokio įrenginio aktualumą apsprendžia nauja galimybė tirti žmogaus regos sistemos gebėjimą registruoti ir interpretuoti laike vidurkintus vaizdus. Tai holistinis priėjimas prie žmogaus regos sistemos tyrimo – žmogaus regos sistema pradeda matyti slaptą vaizdą tik tuomet, kai akis nebegali sekti greitai svyruojančio užkoduotojo vaizdo, vizualinės informacijos srautas per akies obuolius, tinklaines, regos nervus patenka į regos centrą smegenų žievėje, ir žmogaus smegenyse susiformuoja slaptasis vaizdas interferencinių juostų rašto pavidale. Šis kritinis dažnis, prie kurio žmogus jau gali interpretuoti slaptą informaciją, yra svarbus faktorius leidžiantis nustatyti tiek regos sistemos būklę, tiek įvertinti žmogaus nuovargį. Panaudojus sukurtą dinaminės vizualinės kriptografijos principu veikiantį įrenginį, buvo nustatytas virpesių dažnių, prie kurių žmogaus regos sistema atpažįsta slaptą vaizdą, vidurkių pasikliautinasis intervalas, nustatyta virpesių dažnio priklausomybė nuo paros laiko ir respondento amžiaus. Galima teigti, kad nepavargęs žmogus slaptą vaizdą dekoduoja prie žemesnių dažnių. Tęsiant pradėtus eksperimentus įrengta darbo vieta LSMU Akių ligų klinikoje, kur galima tirti pacientų regos sistemas naujai pasiūlytu būdu. Tačiau tokio kritinio dažnio (kai pacientas jau gali perskaityti užkoduotą informaciją) nustatymas turi žymiai platesnę taikomąją perspektyvą. Šis kritinis dažnis neša informaciją apie tiriamojo žmogaus regos sistemos (ir ne tik) nuovargio būklę. Kas svarbiausia, šis kritinio dažnio

nustatymo testas eliminuoja žmogiškąjį faktorių (virpesių dažnis didinamas tol, kol pacientas perskaito užkoduotą tekstą). Taigi, kritinio dažnio nustatymo testas gali būti objektyvus įrankis, leidžiantis įvertinti žmogaus būseną.

Iš tikrųjų, lengva nustatyti vairuotojo girtumo laipsnį naudojant portatyvinį iškvepiamojo oro alkotesterį. Sunkiau nustatyti ar vairuotojas apsvaigęs nuo narkotinių medžiagų – kraujo ar šlapimo mėginius reikia gabenti į laboratoriją ištyrimui. Tuo tarpu galima svarstyti kas pavojingesnis – blaivus sunkvežimio vairuotojas, sėdintis už vairo visą parą be perstojo, ar šiek tiek išgėręs vairuotojas (aišku, pavojingi abu). Tačiau objektyvaus testo vairuotojo nuovargiui nustatyti nėra. Dinaminės vizualinės kriptografijos principu funkcionuojančio portatyvinio įrenginio, leidžiančio nustatyti kritinį dažnį, prie kurio vairuotojas gali perskaityti užkoduotą informaciją, sukūrimas įgalintų padaryti perversmą šioje srityje. Toks tyrimas būtų svarbus ne tik vairuotojams – tai būtų aktualu įvairių atsakingų profesijų atstovams (pvz. atominių elektrinių operatoriams). Tokio įrenginio sukūrimas leidžia pradėti išsamius tolimesnius biomedicininius tyrimus.

Siūloma žmogaus regos sistemos tyrimo metodika pagrįsta optinių iliuzijų vizualine interpretacija. Optinių iliuzijų (ypač judesio sukeltų optinių iliuzijų) srityje dirba kelios rimtos tyrimų grupės, atskirai vertėtų paminėti Bach tyrimų grupę Universitetinėje akių klinikoje Freiburge Vokietijoje [88]. Reikia pažymėti, kad sukurtas dinaminės vizualinės kriptografijos algoritmas – tai nauja optinė iliuzija, o šios optinės iliuzijos dekodavimo fazės sukūrimas atveria naujas taikymų ir tyrimų galimybes.

IŠVADOS

1. Sukonstruotas ir panaudojus genetinius algoritmus išspręstas optimizavimo uždavinys parodė, kad optimalus kodavimo saugumas gaunamas, kai daugiausia laiko procesas praleidžia maksimalių atsilenkimų zonoje, t.y. kai virpesių dėsnis artėja prie stačiakampio bangos formos signalo.
2. Sukurti kompiuteriniai algoritmai realizuojantys dinaminės vizualinės kriptografijos optinius efektus ir palyginantys juos su eksperimentinėmis priemonėmis realizuojamais dekodavimo efektais, pasiūlyta nauja dinaminės vizualinės kriptografijos taikymų sritis – virpančių konstrukcijų vizualinio monitoringo metodika.
3. Sukonstruota dinaminės vizualinės kriptografijos optinė schema pagrįsta chaotiniais virpesiais. Nors chaotiniai virpesiai neformuoja laike vidurkintų interferencinių juostų, koduotas paveikslas visada užpilkėjęs jei chaotinių virpesių intensyvumas padidėjęs, bet pilkio rodiklis jautrus koduoto paveikslo muaro gardelės žingsniui. Šis efektas lemia tai, kad slaptas vaizdas pasirodys kai chaotinių virpesių parametrai pateks į iš anksto nustatytą priimtinų reikšmių intervalą.
4. Išvesti teoriniai sąryšiai, susiejantys pikselio išmatavimus, judesio parametrus, ekrano fizines charakteristikas bei formuojamo vidurkinto vaizdo vizualinį interpretavimą, parodė, kad dinaminės vizualinės kriptografijos optinius efektus galima realizuoti skaitmeninių kompiuterių ekranuose.
5. Sukonstruotas dinaminės vizualinės kriptografijos principu funkcionuojantis įrenginys skirtas žmogaus regos sistemos tyrimui. Svarbiausia įrenginio savybė – tai galimybė sudaryti norimą virpesių dėsnį ir reguliuoti slapto vaizdo virpesių dažnį, kai jis juda pagal nustatytąjį dėsnį. Dažnis didinamas tol, kol pacientas sugeba perskaityti užkoduotąjį vaizdą.
6. Atlikus statistinę analizę nustatyta, kad vidutinis virpesių dažnis prie kurio žmogaus akis sugeba identifikuoti slaptą vaizdą yra nuo 11.78 iki 13.05 Hz. Galima teigti, kad jo reikšmė priklauso nuo žmogaus nuovargio. Mažiau pavargęs žmogus slaptą vaizdą pamatys prie mažesnio virpesių dažnio, nors tai ir priklauso nuo konkretaus žmogaus fiziologinių savybių (pvz. akių ligų).

LITERATŪRA

1. M. Ragulskis and A. Aleksa, Image hiding based on time-averaging moiré, *Optics Communications*, vol. 282, no. 14, pp. 2752–2759, Jul. 2009.
2. X. Huimin, D. Fulong, P. Dietz, A. Schmidt, and Z. Wei, 600°C creep analysis of metals using the Moiré interferometry method, *Journal of Materials Processing Technology*, vol. 88, no. 1–3, pp. 185–189, Apr. 1999.
3. Z. Lei, H. Yun, D. Yun, and Y. Kang, Numerical analysis of phase-stepping interferometric photoelasticity for plane stress separation, *Optics and Lasers in Engineering*, vol. 45, no. 1, pp. 77–82, Jan. 2007.
4. G. Pedrini, S. Schedin, and H. J. Tiziani, Pulsed digital holography combined with laser vibrometry for 3D measurements of vibrating objects, *Optics and Lasers in Engineering*, vol. 38, no. 3–4, pp. 117–129, Sep. 2002.
5. Weller R. and Shepherd B. M., Displacement measurement by mechanical interferometry, *Proccedings of Society of Experimental Stress Analysis*, vol. 6, no. 1, pp. 35–38, 1948.
6. Lightenberg F. K., The Moire Method, *Proccedings of Society of Experimental Stress Analysis*, vol. 12, no. 2, pp. 83–98, 1995.
7. Guid J., The Interference Systems of Crossed Diffraction Gratings, *Clarendon Press, Oxford*, p. 152, 1956.
8. M. D. M. Allen J. B. and Johnson W. O., Generation of Surface Contours by Moire Patterns, *Applied Optics*, vol. 9, no. 4, pp. 942–947, 1970.
9. Takasaki H., Moire Topography, *Applied Optics*, vol. 9, no. 6, pp. 1467–1472, 1970.
10. Wasowski J., Moire Topographic Maps, *Optics Communications*, vol. 2, no. 7, pp. 321–323, 1970.
11. D. H. J. Yung Y. Y., Moire Contour - Sum Contour - Difference and Vibration Analysis of Arbitrary Objects, *Applied Optics*, vol. 10, no. 12, pp. 2734–2738, 1971.
12. Gasvik K. J., *Optical Metrology*. Wiley, Chichester, 1987.
13. Y. Zhao and X. Zhang, Determination of the deformations in polymeric nanostructures using geometric moiré techniques for biological applications, *Sensors and Actuators B: Chemical*, vol. 117, no. 2, pp. 376–383, Oct. 2006.
14. Z. Liu, X. Lou, and J. Gao, Deformation analysis of MEMS structures by modified digital moiré methods, *Optics and Lasers in Engineering*, vol. 48, no. 11, pp. 1067–1075, Nov. 2010.
15. H. Xie, A. Asundi, C. G. Boay, L. Yunguang, J. Yu, Z. Zhaowei, and B. K. A. Ngoi, High resolution AFM scanning Moiré method and its application to the micro-deformation in the BGA electronic package, *Microelectronics Reliability*, vol. 42, no. 8, pp. 1219–1227, Aug. 2002.
16. A. K. Aggarwal, S. K. Kaura, D. P. Chhachhia, and A. K. Sharma, Concealed moiré pattern encoded security holograms readable by a key hologram, *Optics & Laser Technology*, vol. 38, no. 2, pp. 117–121, Mar. 2006.

17. A. Del Taglia, A. Paolucci, and M. Santochi, The Shadow-Moiré Method Applied to 3D Model Copying, *CIRP Annals - Manufacturing Technology*, vol. 44, no. 1, pp. 497–500, Jan. 1995.
18. R. A. Braga, B. S. Oliveira, R. M. Costa, A. C. L. Lino, and I. M. Dal Fabbro, Suppression of border effects in moiré techniques using three-dimensional methods, *Biosystems Engineering*, vol. 102, no. 1, pp. 1–8, Jan. 2009.
19. J. A. Muñoz-Rodríguez and R. Rodríguez-Vera, Image encryption based on moiré pattern performed by computational algorithms, *Optics Communications*, vol. 236, no. 4–6, pp. 295–301, Jun. 2004.
20. E. E. Moon, 15 - Mask-substrate alignment via interferometric moiré fringes, in *Nanolithography*, Elsevier, 2014, pp. 466–502.
21. P. F. Gomes, M. Sesselmann, C. D. C. M. Faria, P. A. Araújo, and L. F. Teixeira-Salmela, Measurement of scapular kinematics with the moiré fringe projection technique, *Journal of Biomechanics*, vol. 43, no. 6, pp. 1215–1219, Apr. 2010.
22. S. Prakash, I. P. Singh, and C. Shakher, Display of tilt information of vibrating object in time average mode using lateral shearing interferometry and interferometric grating, *Optics & Laser Technology*, vol. 33, no. 2, pp. 117–120, Mar. 2001.
23. D. Mollenhauer, E. V. Iarve, R. Kim, and B. Langley, Examination of ply cracking in composite laminates with open holes: A moiré interferometric and numerical study, *Composites Part A: Applied Science and Manufacturing*, vol. 37, no. 2, pp. 282–294, Feb. 2006.
24. Cloud G., Back to basics: geometric moiré phenomena and simulations, *Experimental Techniques*, vol. 29, no. 3, pp. 191–198, 2005.
25. B. Chen and C. Basaran, Far-field modeling of Moiré interferometry using scalar diffraction theory, *Optics and Lasers in Engineering*, vol. 50, no. 8, pp. 1168–1176, Aug. 2012.
26. J. McKelvie and K. E. Perry, Moiré interferometry as a detailed validator for computational modelling of composites, *Composite Structures*, vol. 42, no. 4, pp. 299–305, Aug. 1998.
27. J. R. Berger and V. K. Tewary, Boundary element analysis of moiré fields in anisotropic materials, *Engineering Analysis with Boundary Elements*, vol. 18, no. 4, pp. 317–325, Dec. 1996.
28. J. F. Cárdenas-García and S. Preidikman, Solution of the moiré hole drilling method using a finite-element-method-based approach, *International Journal of Solids and Structures*, vol. 43, no. 22–23, pp. 6751–6766, Nov. 2006.
29. Shamir A. and Naor M., Visual cryptography, *Lecture Notes in Computer Science*, vol. 950, pp. 1–12, 1994.
30. Y.-C. Hou, Visual cryptography for color images, *Pattern Recognition*, vol. 36, no. 7, pp. 1619–1629, Jul. 2003.
31. R. De Prisco and A. De Santis, Color visual cryptography schemes for black and white secret images, *Theoretical Computer Science*, vol. 510, pp. 62–86, Oct. 2013.

32. S. Cimato, R. De Prisco, and A. De Santis, Colored visual cryptography without color darkening, *Theoretical Computer Science*, vol. 374, no. 1–3, pp. 261–276, Apr. 2007.
33. D. Wang, F. Yi, and X. Li, Probabilistic visual secret sharing schemes for grey-scale images and color images, *Information Sciences*, vol. 181, no. 11, pp. 2189–2208, Jun. 2011.
34. D.-S. Tsai, G. Horng, T.-H. Chen, and Y.-T. Huang, A novel secret image sharing scheme for true-color images with size constraint, *Information Sciences*, vol. 179, no. 19, pp. 3247–3254, Sep. 2009.
35. C. Blundo, A. De Santis, and M. Naor, Visual cryptography for grey level images, *Information Processing Letters*, vol. 75, no. 6, pp. 255–259, Nov. 2000.
36. S. Cimato, A. De Santis, A. L. Ferrara, and B. Masucci, Ideal contrast visual cryptography schemes with reversing, *Information Processing Letters*, vol. 93, no. 4, pp. 199–206, Feb. 2005.
37. R.-Z. Wang, Y.-C. Lan, Y.-K. Lee, S.-Y. Huang, S.-J. Shyu, and T.-L. Chia, Incrementing visual cryptography using random grids, *Optics Communications*, vol. 283, no. 21, pp. 4242–4249, Nov. 2010.
38. S. J. Shyu, Efficient visual secret sharing scheme for color images, *Pattern Recognition*, vol. 39, no. 5, pp. 866–880, May 2006.
39. Y.-C. Chen, D.-S. Tsai, and G. Horng, A new authentication based cheating prevention scheme in Naor–Shamir's visual cryptography, *Journal of Visual Communication and Image Representation*, vol. 23, no. 8, pp. 1225–1233, Nov. 2012.
40. G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, Extended capabilities for visual cryptography, *Theoretical Computer Science*, vol. 250, no. 1–2, pp. 143–161, Jan. 2001.
41. S. J. Shyu, S.-Y. Huang, Y.-K. Lee, R.-Z. Wang, and K. Chen, Sharing multiple secrets in visual cryptography, *Pattern Recognition*, vol. 40, no. 12, pp. 3633–3651, Dec. 2007.
42. T.-H. Chen and K.-C. Li, Multi-image encryption by circular random grids, *Information Sciences*, vol. 189, pp. 255–265, Apr. 2012.
43. C.-N. Yang and T.-H. Chung, A general multi-secret visual cryptography scheme, *Optics Communications*, vol. 283, no. 24, pp. 4949–4962, Dec. 2010.
44. J.-B. Feng, H.-C. Wu, C.-S. Tsai, Y.-F. Chang, and Y.-P. Chu, Visual secret sharing for multiple secrets, *Pattern Recognition*, vol. 41, no. 12, pp. 3572–3581, Dec. 2008.
45. S. J. Shyu and K. Chen, Visual multiple secret sharing based upon turning and flipping, *Information Sciences*, vol. 181, no. 15, pp. 3246–3266, Aug. 2011.
46. K.-H. Lee and P.-L. Chiu, A high contrast and capacity efficient visual cryptography scheme for the encryption of multiple secret images, *Optics Communications*, vol. 284, no. 12, pp. 2730–2741, Jun. 2011.
47. W.-P. Fang, Friendly progressive visual secret sharing, *Pattern Recognition*, vol. 41, no. 4, pp. 1410–1414, Apr. 2008.

48. C.-N. Yang and C.-B. Ciou, Image secret sharing method with two-decoding-options: Lossless recovery and previewing capability, *Image and Vision Computing*, vol. 28, no. 12, pp. 1600–1610, Dec. 2010.
49. T.-H. Chen and C.-S. Wu, Efficient multi-secret image sharing based on Boolean operations, *Signal Processing*, vol. 91, no. 1, pp. 90–97, Jan. 2011.
50. S. J. Shyu, Image encryption by random grids, *Pattern Recognition*, vol. 40, no. 3, pp. 1014–1031, Mar. 2007.
51. S. J. Shyu, Image encryption by multiple random grids, *Pattern Recognition*, vol. 42, no. 7, pp. 1582–1596, Jul. 2009.
52. C.-C. Lee, H.-H. Chen, H.-T. Liu, G.-W. Chen, and C.-S. Tsai, A new visual cryptography with multi-level encoding, *Journal of Visual Languages & Computing*, vol. 25, no. 3, pp. 243–250, Jun. 2014.
53. X. Wu and W. Sun, Improved tagged visual cryptography by random grids, *Signal Processing*, vol. 97, pp. 64–82, Apr. 2014.
54. T. Guo, F. Liu, and C. Wu, k out of k extended visual cryptography scheme by random grids, *Signal Processing*, vol. 94, pp. 90–101, Jan. 2014.
55. Y.-F. Chen, Y.-K. Chan, C.-C. Huang, M.-H. Tsai, and Y.-P. Chu, A multiple-level visual secret-sharing scheme without image size expansion, *Information Sciences*, vol. 177, no. 21, pp. 4696–4710, Nov. 2007.
56. F. Liu, C. Wu, and X. Lin, A new definition of the contrast of visual cryptography scheme, *Information Processing Letters*, vol. 110, no. 7, pp. 241–246, Mar. 2010.
57. S. Singh and T. J. Siddiqui, Robust Image Data Hiding Technique for Copyright Protection:, *International Journal of Information Security and Privacy*, vol. 7, no. 2, pp. 44–56, 32 2013.
58. Muraharirao, Siva Charan and Manik Lal Das. 'Securing Digital Image with Authentication Code.' Computer Vision and Image Processing in Intelligent Systems and Multimedia Technologies. IGI Global, 2014. 203-215. Web. 13 Jan. 2015. doi:10.4018/978-1-4666-6030-4.ch011, .
59. P. P. Paul and M. L. Gavrilova, Cancelable Fusion of Face and Ear for Secure Multi-Biometric Template:, *International Journal of Cognitive Informatics and Natural Intelligence*, vol. 7, no. 3, pp. 80–94, 33 2013.
60. Elkhodr, Mahmoud, Seyed Shahrestani and Hon Cheung. 'Preserving the Privacy of Patient Records in Health Monitoring Systems.' Theory and Practice of Cryptography Solutions for Secure Information Systems. IGI Global, 2013. 499-529. Web. 13 Jan. 2015. doi:10.4018/978-1-4666-4030-6.ch019, .
61. Kobayashi A.S., *Handbook on Experimental Mechanics.*, 2nd Edition. SEM Bethel, CT, 1993.
62. Patorski K. and Kujawinska M., *Handbook of the Moiré Fringe Technique.* Amsterdam: Elsevier, 1993.
63. Y. Desmedt and T. van Le, Moiré cryptography, presented at the Seventh ACM Conference on Computer and Communications Security, 2000, pp. 116–124.
64. M. Ragulskis, 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*, vol. 11, no. 12, p. 125411, Dec. 2009.

65. C. Y. Liang, Y. Y. Hung, A. J. Durelli, and J. D. Hovanesian, Time-averaged moire method for in-plane vibrational analysis, *Journal of Sound and Vibration*, vol. 62, no. 2, pp. 267–275, Jan. 1979.
66. M. Ragulskis, R. Maskeliunas, L. Ragulskis, and V. Turla, Investigation of dynamic displacements of lithographic press rubber roller by time average geometric moiré, *Optics and Lasers in Engineering*, vol. 43, no. 9, pp. 951–962, Sep. 2005.
67. Watson G.N., *A Treatise on Theory of Bessel Functions.* Cambridge: Cambridge University Press, 1995.
68. M. Ragulskis, L. Saunoriene, and R. Maskeliunas, The structure of moire grating lines and its influence to time-averaged fringes, *Experimental Techniques*, vol. 33, no. 2, pp. 60–64, Mar. 2009.
69. Jankauskiene, Investigation of eye micromovements in patients with Graves' ophthalmopathy, in *VISION RESEARCH*, vol. 36, THE BOULEVARD, LANGFORD LANE, KIDLINGTON, OXFORD, ENGLAND OX5 1GB: PERGAMON-ELSEVIER SCIENCE LTD, 1996, pp. 350–350.
70. Jankauskiene J, Assessment of visual sensitivity in patients with Graves' optic neuropathy, in *VISION RESEARCH*, vol. 36, THE BOULEVARD, LANGFORD LANE, KIDLINGTON, OXFORD, ENGLAND OX5 1GB: PERGAMON-ELSEVIER SCIENCE LTD, 1996, pp. 1441–1441.
71. Laurutis, V, (paskutinis), Daunys, G, and Zemblys, R, Quantitative Analysis of Catch-up Saccades Executed during Two-dimensional Smooth Pursuit, *Electronics \& Electrical Engineering*, no. 98, 2010.
72. Ragulskis M. and Navickas Z., Hash functions construction based on time average moire, *Discrete and Continuous Dynamical Systems-Series B*, vol. 8, no. 4, pp. 1007–1020, 2007.
73. M. Ragulskis, A. Aleksa, and R. Maskeliunas, Contrast enhancement of time-averaged fringes based on moving average mapping functions, *Optics and Lasers in Engineering*, vol. 47, no. 7–8, pp. 768–773, Jul. 2009.
74. A. Demir, A. Mehrotra, and J. Roychowdhury, Phase noise in oscillators: a unifying theory and numerical methods for characterization, *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 47, no. 5, pp. 655–674, May 2000.
75. F. Herzel and B. Razavi, A study of oscillator jitter due to supply and substrate noise, *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 46, no. 1, pp. 56–62, Jan. 1999.
76. A. Hajimiri, S. Limotyrakis, and T. H. Lee, Jitter and phase noise in ring oscillators, *IEEE Journal of Solid-State Circuits*, vol. 34, no. 6, pp. 790–804, Jun. 1999.
77. A. A. Abidi, Phase Noise and Jitter in CMOS Ring Oscillators, *IEEE Journal of Solid-State Circuits*, vol. 41, no. 8, pp. 1803–1816, Aug. 2006.
78. M. Ragulskis, M. Sanjuan, and L. Saunoriene, Applicability of time-average moiré techniques for chaotic oscillations, *Physical Review E*, vol. 76, no. 3, Sep. 2007.

79. L. Reeves and J. McCoun, *Binocular Vision : Development, Depth Perception, and Disorders*. Hauppauge, N.Y.: Nova Science Publishers, 2009.
80. H. Fujii and T. Asakura, Effect of the point spread function on the average contrast of image speckle patterns, *Optics Communications*, vol. 21, no. 1, pp. 80–84, Apr. 1977.
81. J. J. M. Braat, S. van Haver, A. J. E. M. Janssen, and P. Dirksen, Chapter 6 Assessment of optical systems by means of point-spread functions, in *Progress in Optics*, vol. 51, Elsevier, 2008, pp. 349–468.
82. Z. Peng, N. Guo-Qiang, and X. Ting-Fa, Image restoration for interlaced scan CCD image with space-variant motion blurs, *Optics & Laser Technology*, vol. 42, no. 6, pp. 894–901, Sep. 2010.
83. T. Meyer, Basic Animation, in *Creating Motion Graphics with After Effects*, Elsevier, 2008, pp. 42–67.
84. M. Vairy and Y. V. Venkatesh, Deblurring Gaussian blur using a wavelet array transform, *Pattern Recognition*, vol. 28, no. 7, pp. 965–976, Jul. 1995.
85. X. Ting-Fa and Z. Peng, Object's translational speed measurement using motion blur information, *Measurement*, vol. 43, no. 9, pp. 1173–1179, Nov. 2010.
86. X. Deng, Y. Shen, M. Song, D. Tao, J. Bu, and C. Chen, Video-based non-uniform object motion blur estimation and deblurring, *Neurocomputing*, vol. 86, pp. 170–178, Jun. 2012.
87. Sweet David, Edward Ott, and James A. Yorke, Topology in chaotic scattering, *Nature 399*, pp. 315–316, 1999.
88. Bach tyrimų grupė Universitetinėje akių klinikoje Freiburge, Vokietijoje, *http://www.uniklinik-freiburg.de/augenklinik/augenklinik/mitarbeiter/bach.html*.

MOKSLINIŲ PUBLIKACIJŲ DISERTACIJOS TEMA SĄRAŠAS

STRAIPSNIAI

Mokslinės informacijos instituto (ISI) pagrindinio sąrašo leidiniuose su citavimo indeksais

1. Petrauskienė V.; Aleksa A.; Fedaravičius A.; Ragulskis M. Dynamic visual cryptography for optical control of vibration generation equipment // Optics and Lasers in Engineering. Oxford: Elsevier Ltd. ISSN 0143-8166. 2012, vol. 50, Issues 6, p. 869-876. [ISI Web of Science].

2. Petrauskienė V.; Palivonaitė R.; Aleksa A.; Ragulskis M. Dynamic visual cryptography based on chaotic oscillations // Communications in Nonlinear Science and Numerical Simulation. Amsterdam : Elsevier Science. ISSN 1007-5704. 2014, vol. 19, Issues 1, p. 112-120. [Science Citation Index Expanded (Web of Science)].

3. Petrauskienė V.; Survila A.; Fedaravičius A.; Ragulskis M. Dynamic visual cryptography for optical assessment of chaotic oscillations // Optics and Laser Technology. Oxford : Elsevier. ISSN 0030-3992. 2014, vol. 57, p. 129-135. [Science Citation Index Expanded (Web of Science)].

Kitų tarptautinių duomenų bazių leidiniuose Konferencijų pranešimų medžiagoje

1. Petrauskienė V.; Ragulskienė J.; Šakytė E.; Ragulskis M. Near-optimal time function for secure dynamic visual cryptography // Advances in Visual Computing : 7th International Symposium, ISVC 2011, September 26-28, 2011, Las Vegas, USA: proceedings. Part 2. Heidelberg, Dordrecht, London, New York : Springer, 2011. (Lecture Notes in Computer Science, vol. 6939, ISSN 0302-9743). ISBN 9783642240270. p. 300-309. [SpringerLINK] .

Demonstracinis projektas

1. Aleksa A.; Petrauskienė V.; Ragulskis M. Stochastic Time-Averaged Moiré Fringes. WOLFRAM Demonstration Project.
http://demonstrations.wolfram.com/StochasticTimeAveragedMoireFringes/

PRIEDAI

1 priedas. Eksperimentinės virpesių generavimo įrangos naudojimo aprašymas

Eksperimentinę virpesių įrangą sudaro:

1. Kontrolerio DACTRON COMET DSP signalo išėjimo ir įėjimo įrenginys.
2. DSP plokštė, kuri montuojama į kompiuterį.
3. Personalinis kompiuteris.
4. Vibrostendo valdymo skydas (TYRA).
5. Vibrostendas (TYRA).
6. Akcelerometras.
7. Eksperimente naudojamas koduotas paveikslėlis.
8. Fotoaparatas rezultatams fiksuoti.

Kontroleris Dactron COMET susideda iš trijų dalių: DSP signalo išėjimo ir galutinio įrenginio, PCI DSP plokštės ir Windows aplinkai pritaikytos programinės įrangos. Virpesių generavimą, matavimą, analizę ir registravimą atlieka DSP įrenginys. Ryšį tarp kompiuterio ir DSP įrenginio palaiko PCI DSP plokštė, kuri įmontuota kompiuterio viduje. Windows aplinkoje veikiančios programinės įrangos pagalba parenkami pradiniai duomenys, jie siunčiami į signalų išėjimo DSP įrenginį, vaizduojami ekrane, saugomi kompiuteryje. Programinė įranga tikrina sistemos veikimą ir esant nesklandumams stabdo darbą. Vartotojo pasirinkti signalai DSP signalų išėjimo įrenginio pagalba siunčiami į vibrostendo valdymo skydą, ten apdorojami ir siunčiami į vibrostendą. Gaunami virpesiai, kurie reikalingi eksperimentui atlikti. Eksperimento rezultatai fiksuojami fotoaparatu. Akcelerometras reikalingas tam, kad patikrinti ar vibrostendas tikrai vibruoja pagal pasirinktą dėsnį. Jis siunčia signalus į DSO signalų įrenginį, juos gavusi programinė įranga patikrina gautus duomenis ir ekrane pavaizduoja rezultatus.

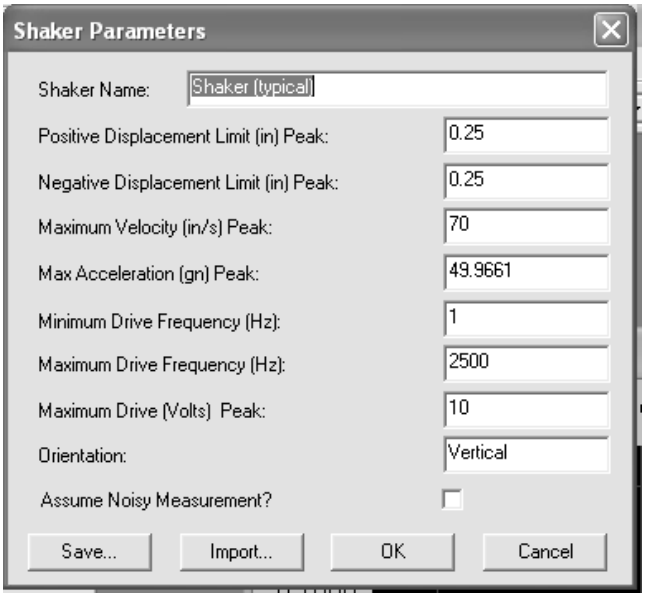
Kontroleris gali generuoti, valdyti, apdoroti harmoninių, atsitiktinių ir smūginius signalus. Prieš sukuriant naują projektą turime programos dialogo lange pasirinkti kokio tipo virpesius norime generuoti, parinkti bendrus programos parametrus, kurie panašūs visiems skirtingo tipo virpesiams.

Parametrų nustatymas susideda iš penkių etapų:

- Shaker (stendo parametrai);
- Channels (įvesties ir išvesties kanalų parametrai);
- Profile (vaizdo parametrai);
- Transmissibility signals (perdavimų signalai);
- TestID (testo identifikacija);

Stendo parametrai

Šiame parametrų dialogo lange (1 pav.) leidžiama nustatyti saugias darbo ribas, kad nuo pažeidimų ir perkrovos būtų apsaugota vibrostendo sistema. Reikiami parametrai nurodomi dialogo lange. Visi nustatyti parametrai bus patikrinti prieš atliekant bandymą, jei parametrai viršys leidžiamas vibrostendo ribas, bandymas nebus atliekamas arba vykdymas bus automatiškai nutrauktas.



1 pav. Stendo parametrai

Skirtingiems virpesiams (atsitiktiniams, harmoniniams ar smūginiams) parenkami skirtingi įverčiai, atitinkantys nustatytas ribas. Stendo parametrų lange turime užpildyti tokius laukus:

Shaker Name **(**stendo vardas**)** – neprivalomas teksto laukas, naudojamas tik dokumentacijos tikslais, čia galime įrašyti modelio ar serijos numerį.`

Positive and Negative Displacement Limits – nurodoma didžiausia ir mažiausia galimos bandymo metu poslinkio ribos.

Maximum Velocity – nurodomas didžiausias leistinas bandymo greitis.

Maximum Acceleration - nurodomas didžiausias leistinas bandymo pagreitis.

Minimum and Maximum Drive Frequency – įvedama mažiausia ir didžiausia dažnio reikšmė, siekiant apsaugoti vibrostendą nuo sugadinimo ir užtikrinant, kad daviklio signalai bus teisingi.

Maximum Drive – apribojama didžiausia leistina įtampa.

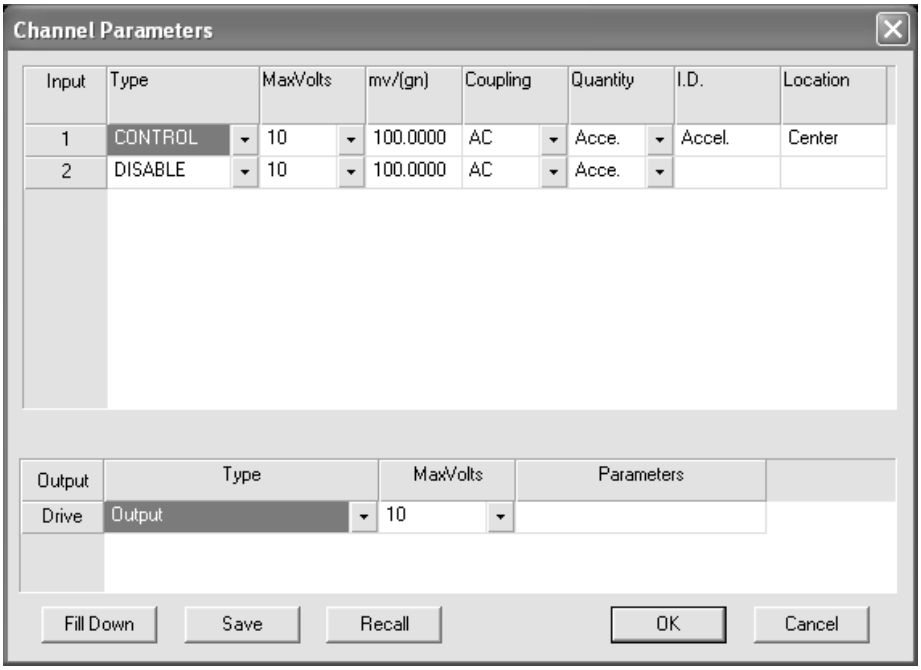
Orientation – neprivalomas teksto laukas, naudojamas tik dokumentacijos tikslais. Čia gali būti įrašoma stendo padėtis (pvz. Vertikali, horizontali, 45°).

Measurement Noisy (triukšmas) – pasirenkamas ar signalas bus veikiamas triukšmo ar nebus. Jei uždedame varnelę, pažymime, kad valdymo jutiklio signalas turės didelį foninį triukšmą.

Save ir ***Import*** – čia galima išsaugoti parametrų rinkinį ar importuoti anksčiau išsaugotą.

Kanalų parametrai

Po stendo parametrų turime nustatyti signalų įvesties ir išvesties kanalų parametrus. Jie bus naudojami atliekamuose eksperimentuose.



2 pav. Kanalų parametrai

Lange (2 pav.) esančiais mygtukais galima atlikti tokius veiksmus:

Fill Down mygtukas kopijuoja langelyje esančią informaciją į to paties stulpelio žemiau esančius langelius. Pasirinkus ***Save*** ir ***Recall*** mygtukus galima išsaugoti ar importuoti pasirinktą parametrų rinkinį.

Pirmiausia šiame lange aprašomi ***Input Channels (Įvesties kanalai).*** Skirtinguose stulpeliuose nurodoma reikalaujama informacija:

Type stulpelyje leidžiama pasirinkti kiekvieno įėjimo tipą. Galime rinktis tarp kontrolės, stebėjimo ar kanalo išjungimo. Jei visus įėjimus pasirinksime kaip kontrolę, tai jie visi ir bus panaudoti vykdymo procese, priklausomai nuo to kokie nurodyti kontrolės parametrai dialogo lange. Jei visi įėjimai pasirinkti stebėjimui, tai procesas bus stebimas, informacija išsaugoma, bet jie nedalyvaus vykdymo procese. Jei visus kanalus išjungsime, tai jie bus sistemos ignoruojami.

Max Volts stulpelyje įvedama didžiausia amplitudė, kokią tikėtina perduos įvesties kanalo daviklis. Programinė įranga elektronikai taikys pilną spektrą reikšmių iš ± Max Volts intervalo. Max Volts turėtų būti didžiausia laukiama įtampa bandymo metu, o ne daviklio aukščiausia riba. Reikia įvertinti, kad dauguma atsitiktinių bandymų energijos grafikų bus žemiau 3 sigma (99,7 % viso laiko) atsitiktinio triukšmo, ir tik kartais viršys 3 sigma taisyklę.

mv/(acceleration unit) stulpelis naudojamas norint parinkti įvesties kanalo daviklio jautrumą. (mv - milivoltai). Jis nurodomas akcelerometro gamintojo kalibravimo specifikacijose. Pagreičio matavimo vienetai tokie kokie parinkti naudoti programinėje įrangoje.

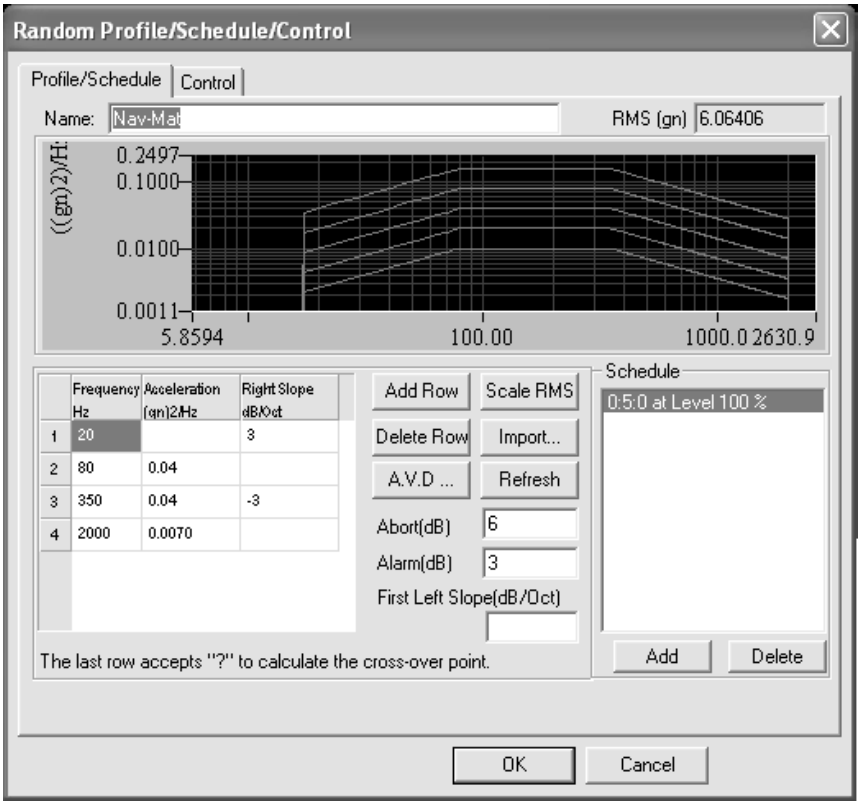
Coupling stulpelyje parenkama kokia kintama ar nuolatinė srovė bus įvesties kanale. Kintamos srovės įjungimas pašalina nuolatinės srovės komponentą įvesties

signale. Tą atlieka programinės įrangos algoritmas kuris dirba su skaitiniais duomenimis. Kintama srovė pagrinde naudojama atsitiktinių ir harmoninių virpesių testuose. Klasikinių smūgių testavimas geriau veikia kai pasirinkta nuolatinė srovė.

I.D. ir ***Location*** stulpeliai neprivalomi laukai. Jie naudojami tik dokumentacijai. *I.D.* lauke galima įvesti serijos numerį ar daviklio aprašymą. *Location* lauke nurodoma daviklio tvirtinimo vieta.

Išvesties kanalams **(*Output Channel*)** reikia parinkti tipą Output ir parinkti Max Volts reikšmę. Programinė įranga nurodys elektronikos valdymo kanalui naudoti pilną spektrą reikšmių intervale ± Max Volts.

Toliau gaunama **Profile (vaizdo)** kortelė (3 pav.)**.** Ji susideda iš dviejų langų: Profile/Schedule (vaizdas/aprašas) ir Control. Pirmajame lange matome dažnių – pagreičių diagramą, jei reikia čia pat galima ją ir keisti.



3 pav. Atsitiktinių dydžių vaizdo/aprašo kortelė

Šioje kortelėje parenkamos profilio ribinės reikšmės ir apibūdinamas reikšmių spektras. Kiekvienam atskaitos taškui sukuriama atskira eilutė, kurioje nurodoma dažnio reikšmė, pagreitis arba dažnio dešininis nuolydis. Nuolydis visada yra susijęs su dažnio atskaitos tašku.

Jei pereinamasis dažnis ar amplitudės reikšmė gaunama priklausomai nuo vidinio nuolydžio, įvedama nuolydžio reikšmė, o į dažnio ir pagreičio laukus įvedama ?. Tada paspaudžiamas Atnaujinti (Refrech) mygtukas. Pastebėkima, kad

šis įrašymo metodas gali būti naudojamas profilio kortelėje turint eilutę, kai profilio lentelė konstruojama eilutė po eilutės, norint įgauti reikiamą formą.

Į laukelius *Abort*(dB) ir *Alarm*(dB) įvedamos proceso nutraukimo ir pavojaus ribos. Pagal šias reikšmes yra nustatoma apatinė ir viršutinė proceso nutraukimo ar pavojaus ribos. Sistema neperskaičiuos naujų reikšmių kol nebus paspaustas *Refrech* (Atnaujinti) mygtukas. Jei parinkti lūžio taškai korektiški, sistema sugeneruoja naują profilio grafiką.

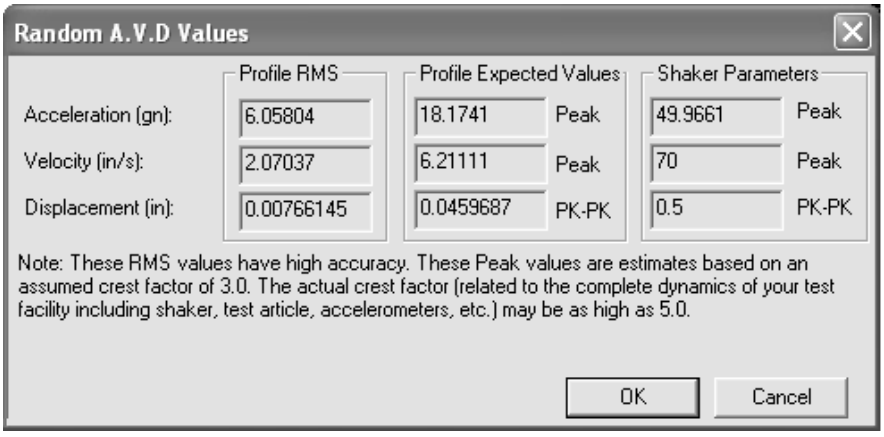
Laukelyje ***Name*** nurodomas profilio pavadinimas.

***RMS* (gn)** rodo sukurto profilio RMS reikšmę. Šis laukas yra atnaujinamas automatiškai, kai tik profilyje kas keičiama.

Mygtukas ***Add Row*** lentelės apačioje įterpia naują eilutę.

Delete Row naikina pasirinktą eilutę.

Spragtelėję ***A.V.D*** mygtuką gauname ***Random A.V.D Values*** kortelę (4 pav.), kurioje galime palyginti vibrostendo ribas su laukiamu didžiausiu (peak) pagreičiu, greičiu ir profilio (kontūro) poslinkiu (Peak-Peak).



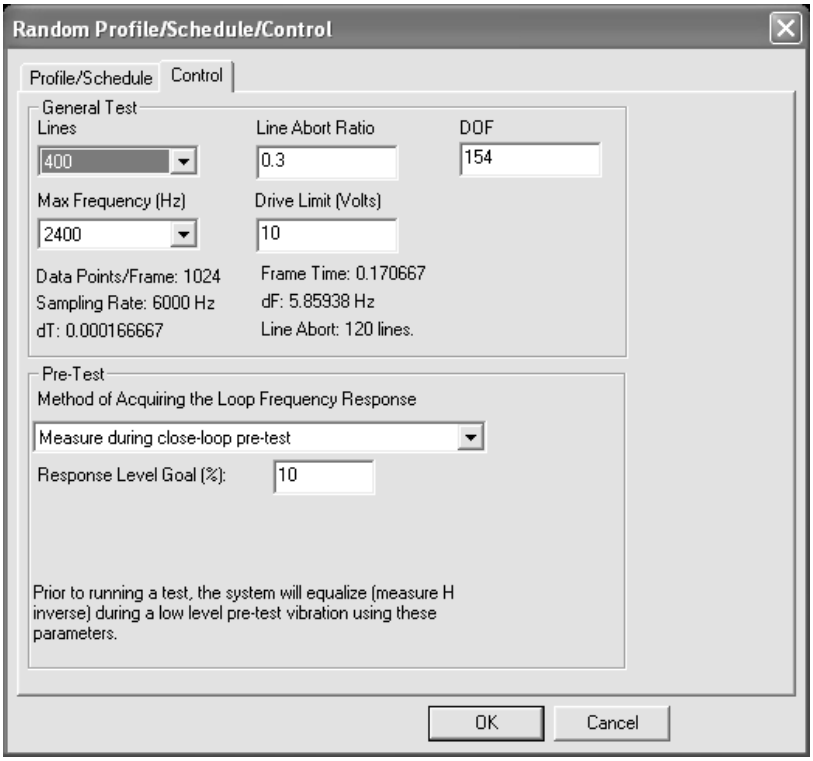
4 pav. Atsitiktinės A.V.D. reikšmės

Laukeliuose ***Profile Expected Values*** nurodomos laukiamos aukščiausios reikšmės, kurias bus matomos bandymo metu. Šios reikšmės apskaičiuojamos remiantis prielaida, kad maksimalus daugiklis (peak to RMS ratio) yra 3. Tikrasis maksimalus daugiklis stebimas testavimo metu tiesiškai priklauso nuo vibrostendo sistemos. Hidraulinis vibrostendas yra netiesinis ir maksimalus daugiklis iš 3 paprastai yra tinkamas. Tačiau elektrodinaminis vibrostendas pagrinde yra tiesinis ir maksimalus daugikllis galėtų būti artimesnis reikšmei 4.

Control kortelėje (5 pav.) galime parinkti, atsitiktinių dydžių projektui, valdymo parametrus, kortelėje yra du dialogo langai: ***General Test*** ir ***Pre-Test*** . Šis meniu yra reikalingas įvesti testo valdymo metodams bei veiksmams prieš testą.

General Test langas atsitiktiniams valdymo parametrams

Uždaro tipo valdymo apdorojimo metodas yra apibrėžiamas ***General Test*** lange, o veiksmai prieš testą nurodomi Pre-Test lange.



5 pav. Atsitiktinių virpesių parametrai.

Max Frequency (maksimalus dažnis) nustato viršutinę ribą valdymo dažnių juostoje. Valdymo procesas atliekamas nuo 0 Hz iki nurodyto didžiausio dažnio hercais. Pasirinkamas dažnių diapazonas atitinkantis reikalavimus.

Lines įvesti spektro linijos (dažnių juostos) numerį valdymo dažnių juostoje.

Maksimalus dažnis ir linijos numeris nustato dažnio didėjimą.

Pav. Jei Max dažnis = 2000 Hz ir linija = 400, dažnio didėjimas bus 5 Hz.

Line Abort Ratio (linijos veikimo nutraukimo rodiklis) tikrina, kad spektrinė linija neviršytų leidžiamo nuokrypio. Testo vykdymas bus automatiškai nutrauktas, jei spektrinės linijos rodiklis bus didesnis nei nurodytas laukelyje Line Abort Ratio. Pavyzdžiui, jei Line Abort Ratio yra 0.3, sistemos vykdymas bus nutrauktas kai spektrinė linija nuokrypis bus 30%.

DOF **(**arba laisvės laipsniai**)** numato alternatyvų metodą naudojamą vykdymo spektro vidurkio skaičiavimui.

Drive Limit nurodomas didžiausias vykdymo lygis (voltais) išėjimui į stiprintuvą. Šie parametrai taikomi tik numatytas testui. Parametrai prieš testą parenkami kitur.

Pre-Test langas atsitiktiniams valdymo parametrams

Pre- Test lange apibrėžiame parametrus pradiniams virpesiams išlyginti, kurie atsiranda prieš testo vykdymą.

Method of Acquiring the Loop Frequency Response Function dalyje pasirenkama viena iš apibrėžtų schemų:

Measure during Pre-Test (matuojama pre-test metu) tai priimtimiausias būdas pasiekti FRF numatyto bandymo metu.

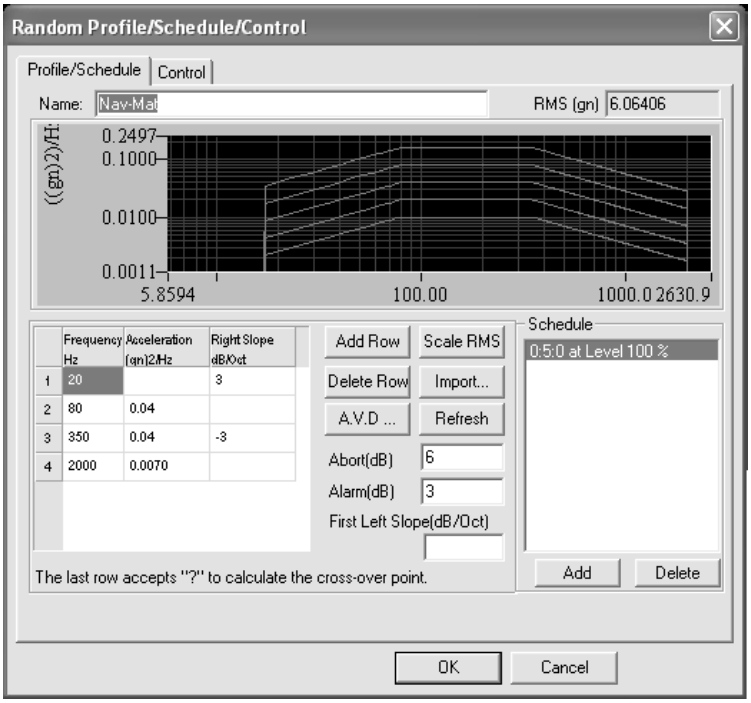
Use Current Active Function and Skip Pre-Test (naudoti esamą aktyvią funkciją ir praleisti Pre-Test) naudojama tik tada, kai testas ką tik buvo sėkmingai paleistas ir po to nieko nekeista. Pasirinkti šią funkciją reikia itin atsargiai, užtikrinant, kad bandymas yra kartojamas be jokių pakeitimų, po to kai buvo pirmą kart paleistas. Vos kelių bandymo valandų bėgyje kartais atsiranda pokyčiai, turintys didelį poveikį bandymo veiklai.

Recall Function from Disk and Skip Pre-Test (atgaminti funkciją iš disko ir praleisti Pre-Test) naudojame tik tada, kai kai esame visiškai tikri, kad diske saugoma FRF yra būtent ta, kuri tinka dabartinėms sąlygoms. Šį variantą reiktų rinktis labai atsargiai.

Response Level Goal (reakcijos lygis) reakcijos lygio tikslas yra norimas amplitudės lygis, kad būtų atlikta tinkama patikra prieš bandymą. Jei šis lygis nebus pasiektas, bandymas nebus vykdomas. Tipinės reikšmės yra parenkamos iš intervalo nuo 10% iki 50%. Kai reikiamas lygis yra pasiektas, valdymo sistemoje išsaugoma perdavimo funkcija, kuri bus naudojama numatyto testo metu.

Atsitiktinių virpesių profilio pavyzdžiai

Pateikti pavyzdžiai padės geriau suprasti atsitiktinių virpesių profilio sudarymą.



6 pav. Pradžios ir pabaigos nuolydžiai atsitiktinių virpesių profilyje

Pradžios ir pabaigos nuolydžiai atsitiktinių virpesių profilyje

Daugumoje bandymų aprašymo testo profilyje apibrėžiama minimalūs ir maksimalūs dažniai, pradžios ir pabaigos nuolydžiai ir keletas lūžio taškų.

Pavyzdžiui **NavMat** profilyje (7 pav.) yra nurodomi tokie aprašai:

Mažiausias dažnis: 20 Hz

Didžiausias dažnis: 2000 Hz

Pradžios nuolydis: 6 dB/oct

Pirmas lūžio taškas: 0,04 g^2/Hz prie 80 Hz

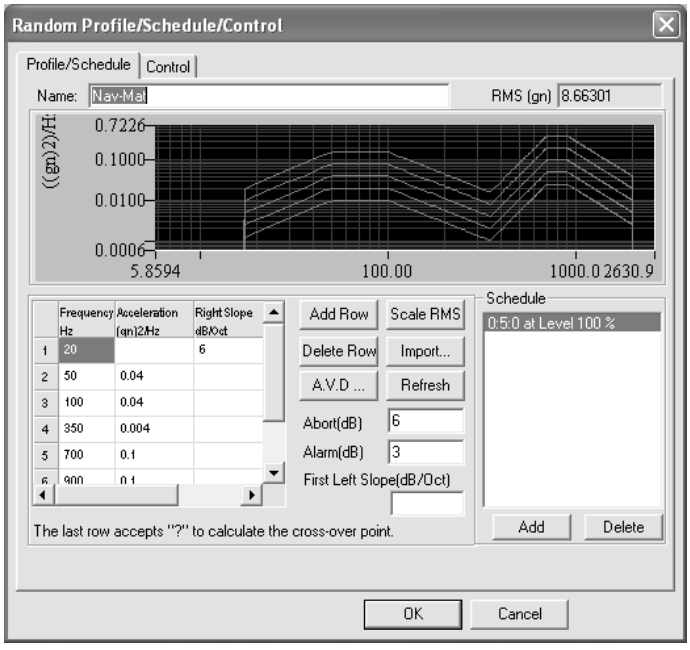
Antras lūžio taškas: 0,04 g^2/Hz prie 350 Hz

Pabaigos nuolydis: -6 dB/oct

Paveiksle (6 pav.) matoma, kad dažnių – pagreičių diagramoje kontūras prasideda nuo 20 Hz, iki 80 Hz nuolydis 3 db/oct, tada tiesi linija ties 0,04 g^2/Hz iki 350 Hz, tada nuolydis žemyn 3 dB/oct iki 2000 Hz.

Vidiniai lūžio taškai atsitiktinių virpesių kontūre

Kai kurios specifikacijos reikalauja vidinių nuolydžių. Atsitiktinių virpesių profilio lentelėje yra galimybė pasirinkti vidinius nuolydžius.

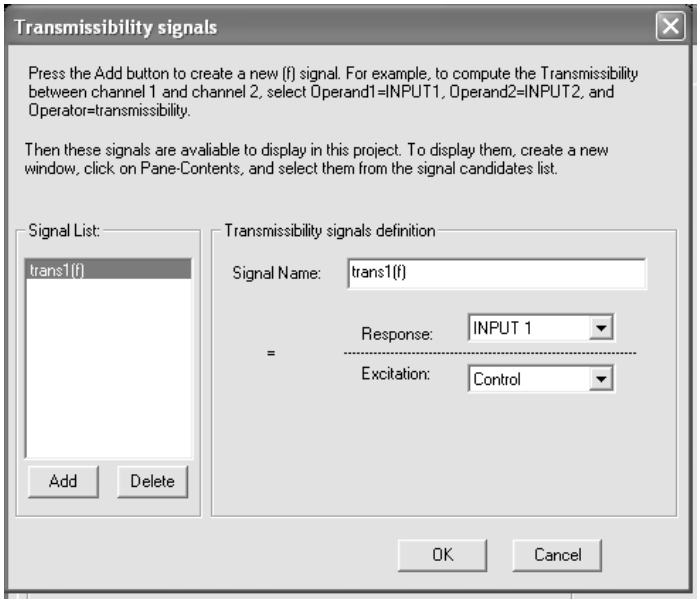


7 pav. Vidiniai nuolydžiai atsitiktinių dydžių profilyje

Vidinis nuolydis apibrėžiamas nurodant konkretų dažnį ir atskaitos tašką, tada sistema automatiškai perskaičiuoja nuolydį. 7 paveiksle matome pateiktą pavyzdį.

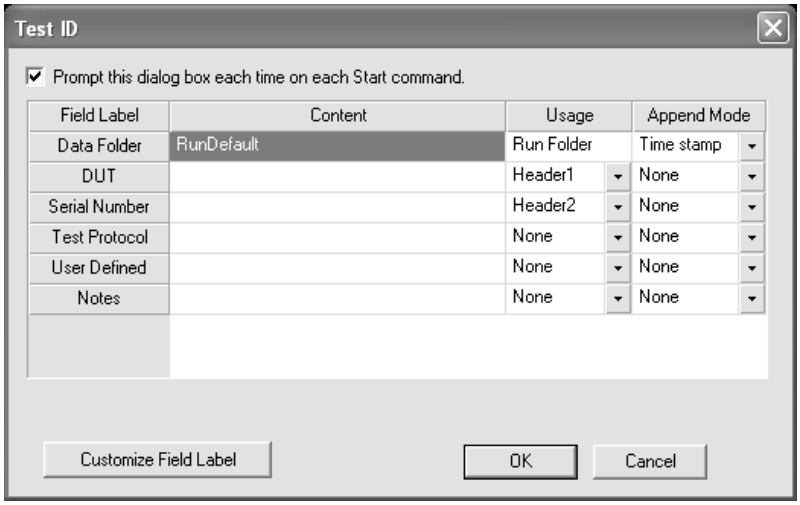
Ketvirtame etape gauname kortelę ***Transmissibility signals*.**

Šioje kortelėje (8 pav.) apibrėžiami perdavimo signalai. Galima pasirinkti įvesties kanalą ir kontrolę.



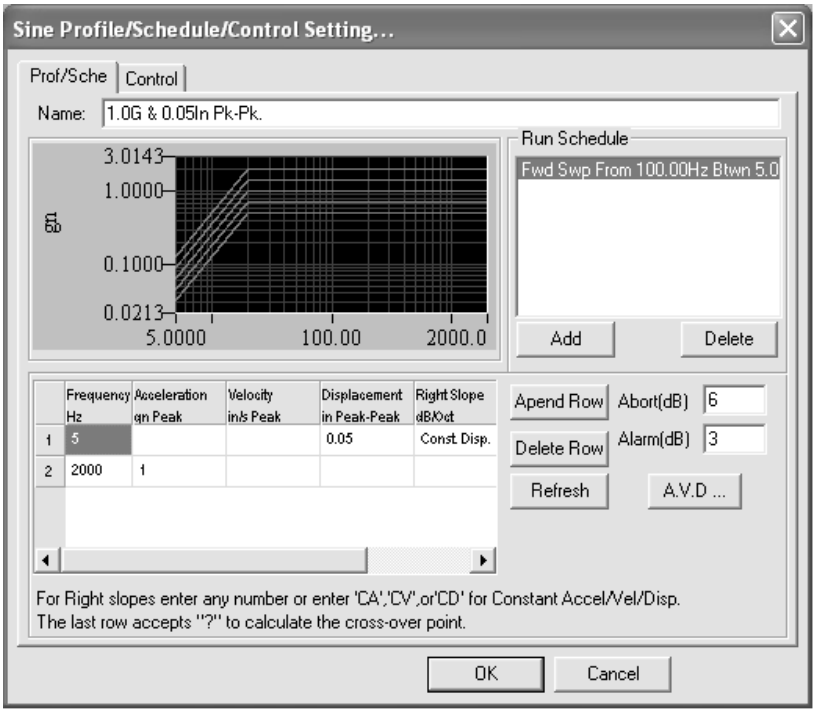
8 pav. Perdavimo signalai

Paskutinė kortelė ***Test ID*** (9 pav.) skirta testo identifikavimui ir dokumentacijai.



9 pav. Testo identifikavimas ir kontrolė

Harmoninių virpesių profilio lentelę (10 pav) sudaro du langai: ***Prof/Sche*** ir ***Control.*** *Prof/Sche* lange galima įvesti ribines reikšmes ir gauti skaičiavimo rezultatą. Lango funkcijos veikia kaip skaičiuoklės programa. Į vieną eilutę įvedus dažnio, pagreičio, greičio ar poslinkio reikšmes yra sukuriamas kiekvienas atskaitos taškas.

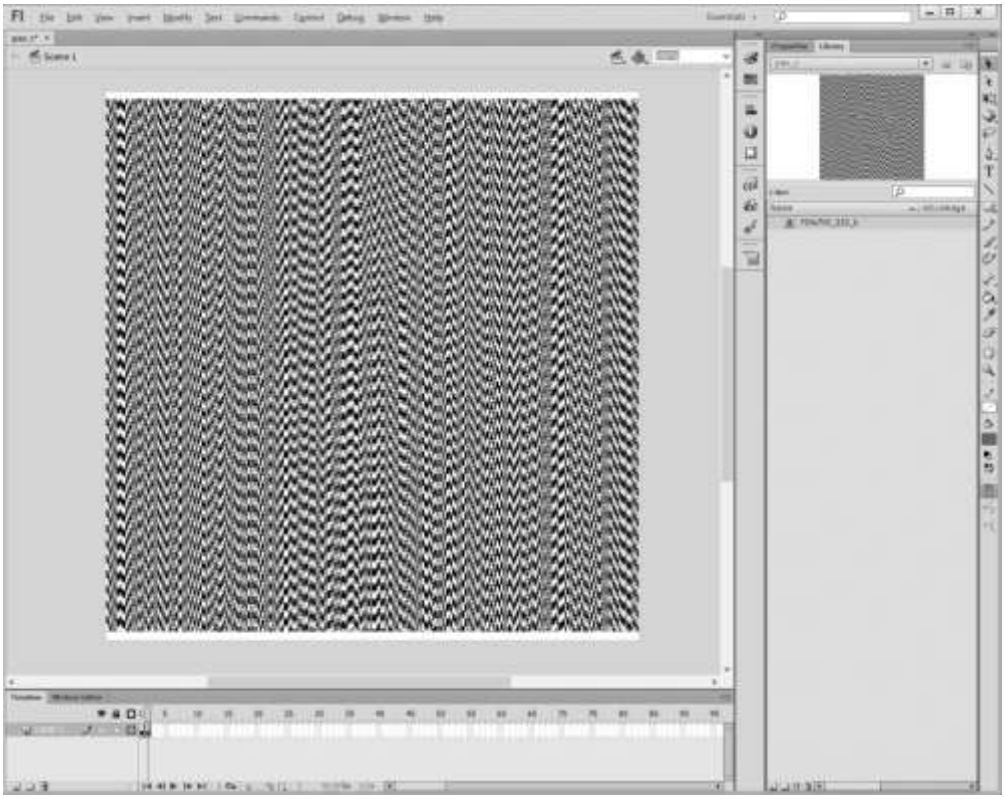


10 pav. Control lange nurodomos leistinos harmoninių virpesių parametrų ribos.

2 priedas. Dinaminės vizualinės kriptografijos pagrindu funkcionuojančio žmogaus regos sistemos tyrimo maketo aprašymas

Pagrindinė ir esminė maketo dalis – tai slapto vaizdo kodavimas stochastinėje muaro gardelėje, bei užkoduoto vaizdo virpinimas kompiuterio ekrane pagal nustatytą dėsnį. Svarbiausia maketo savybė – tai galimybė sudaryti norimą virpesių dėsnį ir reguliuoti slapto vaizdo virpesių dažnį, kai jis juda pagal nustatytąjį dėsnį. Dažnis didinamas tol, kol žmogus sugeba perskaityti užkoduotąjį vaizdą.

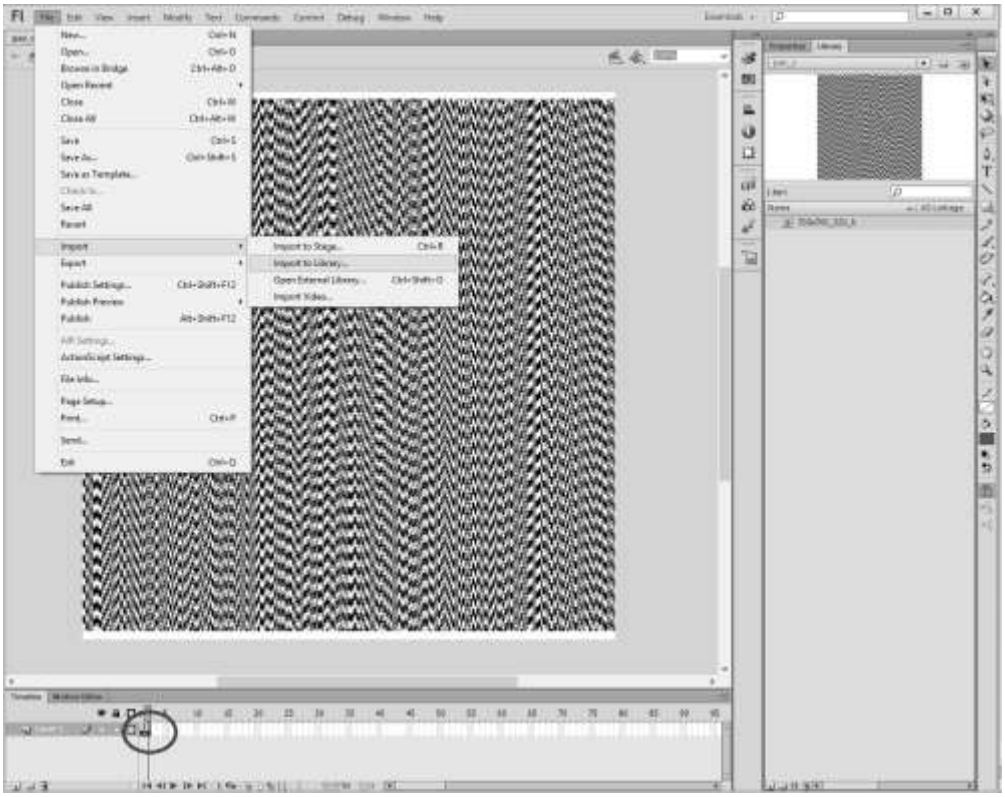
Pats slapto vaizdo kodavimo procesas reikalauja specialių algoritmų pritaikymo – su įrenginiu dirbančiam žmogui pateikiama jau paruošta užkoduotųjų vaizdų biblioteka. Aspektai susiję su slapto užkoduoto vaizdo formavimusi asmeniui, dirbančiam su tiriamaisiais, lieka nepastebimi.



11 pav. Pagrindinis programos langas

Žmogaus (gydytojo) – kompiuterio interfeisui panaudotos Adobe kompanijos programinės priemonės. 11 paveiksle pavaizduotas Adobe Flash Professional CS6 programos langas. Pagrindiniame lange (darbinėje dalyje) rodomas slaptas užkoduotas statinis vaizdas, dešinėje pusėje – importuotų (užkoduotų) vaizdų biblioteka, apatinėje dalyje – laiko juosta.

Dinaminėje vizualinėje kriptografijoje slaptas vaizdas koduojamas kompiuterio pagalba. Norėdami šį vaizdą dekoduoti, reikia statinį vaizdą virpinti žinomu dėsniu ir amplitude (iš principo dekodavimui kompiuteris nereikalingas). Šiuo atveju naudojamas ne vibrostendas, o Adobe Flash Professional CS6 programa, kuri optimaliai išnaudoja kompiuterinius resursus statinio vaizdo virpinimui pagal nustatytą dėsnį ir dažnį. Pradžioje reikia įkelti paruoštą užkoduotąjį vaizdą į programos biblioteką. Tai atliekama meniu funkcijų File -> Import -> Import to Library pagalba (12 pav.). Dešinėje pusėje matomi visi įkelti vaizdai. Kadangi dekodavimas atliekamas tik vieną vaizdą virpinant laike, tai tik šio statinio vaizdo ir tereikia.



12 pav. Importuojamas naujas slaptas vaizdas

Žmogaus regos sistemos tyrimams naudojami įvairūs slapti vaizdai, kuriuos galima pasirinkti iš standartinių iš anksto paruoštų (ir užkoduotų) vaizdų bibliotekos (13 pav.). Galima naudoti ir standartinius simbolius (apskritimo lankus) ir tekstą, susidedantį tiek iš didžiųjų, tiek ir iš mažųjų raidžių.

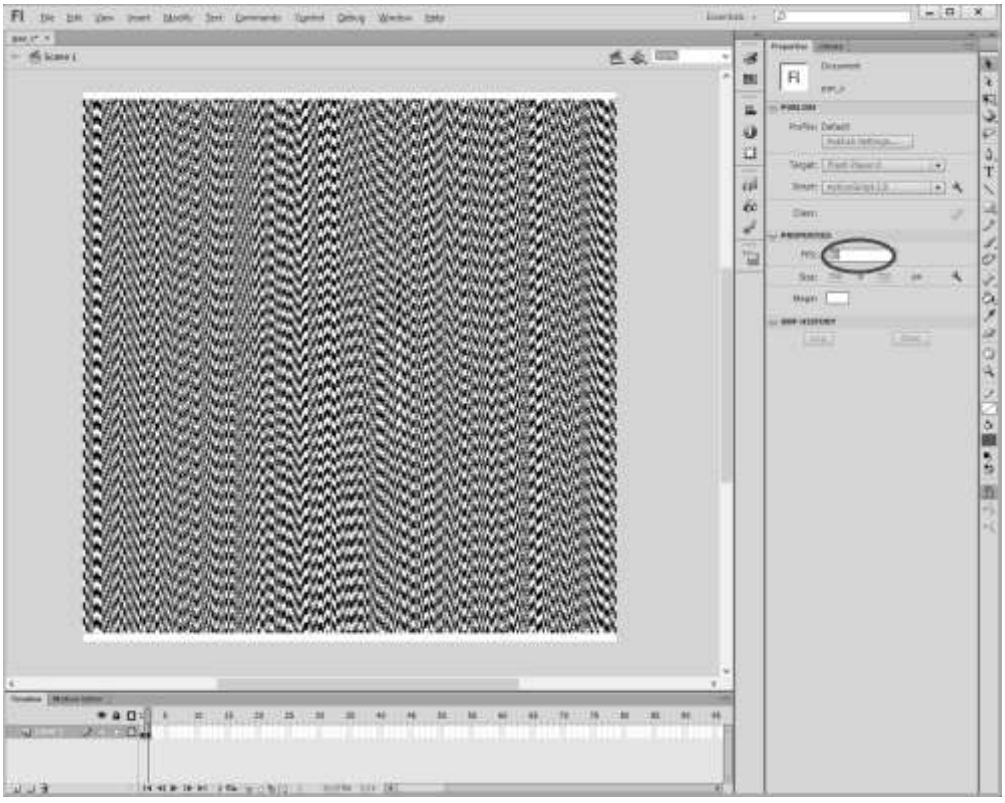
13 pav. Slaptų vaizdų biblioteka.

Formuojant kiekvieną slaptą vaizdą atsižvelgiama į stochastinės muaro gardelės struktūrą, judesio dėsnį, slaptos informacijos kiekį, kurį galima išsaugoti konkrečioje koduotoje gardelėje. Paprastai žmogui, dirbančiam su tiriamuoju, šie klausimai neaktualūs – svarbu kad žmogaus – kompiuterio sąsaja būtų kuo

paprastesnė. Bibliotekoje saugomi jau užkoduotieji vaizdai, o kiekvienam užkoduotam vaizdui priskiriama dekodavimo funkcija – dėsnis pagal kurį tas vaizdas turi būti virpinamas.

Sukurtame tuščiame dokumente užkoduotas vaizdas tiesiog užtempiamas (drag and drop) iš bibliotekos. Virpesių dėsnis nustatomas (užprogramuojamas) vieną kartą visai bibliotekai - įterpiamas naujas kadras Insert –> Timeline –> Keyframe. Skaičiuojant naujo kadro koordinates turi būti atsižvelgiama į statinio užkoduoto vaizdo stochastinės muaro gardelės periodą.

Sukurtas dokumentas jau gali būti vizualizuojamas kaip virpantis objektas. Shift+ Enter klavišų kombinacija atveria naują animacijos-virpesių langą. Vaizduojamų kadrų skaičius per sekundę nustatomas pagrindiniame lange parinkus Properties –> FPS (14 pav.). Šis parametras registruojamas žurnale kartu su tiriamojo asmens atsakymais (didinant dažnį žmogus prašomas perskaityti slaptą informaciją).



14 pav. Virpesių dažnio keitimas.

3 priedas

1 lentelė. Eksperimento metu surinkti duomenis apie kritinį virpesių dažnį, prie kurio atpažįstamas slaptas vaizdas

Nr.	Lytis	Amžius	Val.	AsK	Vgt	iFd	gerg	Meg	KTI	Gm	drej	beF	Sam
1	M	38	13.15	21	13	12	14	11	10.5	11.5	11.5	11.5	13
2	V	35	14.00	14	14	14	13.5	14	12	14	14.5	12	13
3	M	20	15.00	20	15	13	13	13	10.5	11	11	12	13
4	M	47	13.15	16.5	15	16	15	15.5	14	14	13	13	12
5	V	50	13.45	14	14	15	14	15	13	12	12.5	14	11
6	V	24	12.00	10	9.5	12.5	11	13	8.5	8	9.5	7.5	8.5
7	V	21	20.00	15	15	14	13	15	14	13	12	14	12
8	M	55	20.30	21.5	16.5	16	14	21.5	15.5	15	16	14	15
9	V	18	14.30	18	14	11.5	16	12	14	15.5	14	13	12.5
10	M	33	21.00	21	16	15	15.5	23	15.5	15	15	14	13
11	M	60	18.00	16	15	14	15	14	15	14.5	14.5	13	12
12	M	59	10.00	15	13.5	12.5	12	11.5	11	10.5	9	9	9
13	M	32	14.00	15.5	13.5	12.5	13.5	14	16	13	13	14	13
14	V	27	13.00	16	13.5	11	11	11.5	10.5	8	9.5	11	8.5
15	M	20	19.00	21	18	15	14	11.5	12.5	10	13	11.5	15
16	M	50	9.00	14.5	9.5	9	9.5	8.5	9	8.5	9.5	8.5	8
17	M	43	14.20	17	20	16	12.5	15	19	12	11	11	11
18	V	18	10.00	10	9.5	8.5	7	6	6	5.5	5	5	4.5
19	M	18	13.00	15.5	16.5	16.5	10	9	13	11	9	8	8.5
20	V	20	13.30	16	13.5	13	10.5	14	11.5	11.5	11	8.5	8.5
21	V	17	14.00	15.5	13.5	12.5	13	11	13	10	12	11	10
22	V	44	15.00	15	15.5	16.5	13	14	15	14.5	14	12	12
23	V	25	21.00	24	16	15	12	12	12.5	14.5	15	13.5	15.5
24	V	21	16.00	10.5	13	10	12.5	10.5	10	10	9.5	9.5	9
25	M	22	16.30	15	11.5	14	12	15	9.5	12.5	12	13	11
26	M	30	16.00	20	14	14	12	12.5	13.5	11	11.5	12	12.5
27	V	22	15.00	18	12.5	11	14	11.5	12	10	9.5	10	10.5
28	V	34	12.00	19.5	16	14	13	13.5	14	12.5	11	10	10.5
29	V	25	8.00	13.5	12.5	11	10	9	9.5	10	8.5	8	8.5
30	M	24	12.00	15	13	11.5	10	9.5	10.5	9.5	8	8.5	8.5
31	V	21	10.00	14	12	11	9.5	10	9.5	9.5	8.5	8.5	9
32	M	22	13.00	18	14	12.5	12.5	12	10	10.5	9.5	9	8.5
33	M	23	13.30	18.5	13.5	13.5	12	13	10	10	11.5	9.5	9.5

Nr.	Lytis	Amžius	Val.	AsK	Vgt	iFd	gerg	Meg	KTI	Gm	drej	beF	Sam
34	M	23	14.00	16	15	14	11	14.5	10	9.5	9	9.5	10
35	V	24	12.00	17	14.5	13	11.5	11.5	11	11.5	9.5	9	8.5
36	M	34	9.00	15.5	13	12	10.5	10.5	9.5	9.5	10	9	8.5
37	V	33	10.00	16	12.5	13.5	10	11.5	11.5	11	10.5	9.5	9.5
38	M	36	10.35	16	13	14	10	12	11.5	11	10	10	9.5
39	M	45	13.30	17.5	13	14	10.5	11.5	12	11.5	11	10.5	10
40	M	20	16.00	18.5	15.5	14	12.5	11	11.5	11	11	10	9.5
41	V	23	18.00	20	15.5	15.5	15	14.5	14	14.5	11.5	11	11
42	V	37	16.45	21.5	16	15.5	15	14	14	12.5	12	11.5	10
43	M	23	11.00	15.5	14	15	12.5	11.5	10.5	11	9.5	9	9
44	V	22	17.15	21	16.5	15	15.5	14.5	13.5	12	12.5	11.5	11.5
45	V	36	19.00	23	16.5	15.5	16	15	14	13	12	11	11.5
46	V	22	10.00	14.5	13	12	12	10.5	10.5	10	9	9	8
47	M	20	15.35	20	15	14.5	13	10.5	11.5	11	12	10	10
48	M	25	19.00	23.5	15.5	15.5	15	14.5	14	12.5	13.5	10.5	15
49	V	38	12.00	15	14.5	13.5	11.5	10.5	10	10.5	11	9	9.5
50	M	41	14.00	17	18	15.5	13.5	15	15.5	13.5	15	14.5	12.5
51	M	30	10.00	15	13	11.5	11.5	10	9.5	8.5	10	8	8.5
52	M	37	16.35	17.5	15	15.5	14	13	12.5	10.5	9.5	9.5	10
53	V	24	9.45	13.5	12.5	10.5	10	9	9	7.5	9	8.5	9.5
54	V	23	10.00	14.5	13	11	10	9.5	9	8	8.5	8.5	8
55	M	41	12.00	15.5	14	11.5	11.5	10.5	10	8.5	9.5	9	9
56	M	20	12.35	17	14	12	11	11.5	11	10.5	9.5	9	10
57	V	22	13.15	16	14.5	13	12.5	12	10	10.5	10	10	9.5
58	M	21	17.00	15.5	13.5	14	12	11.5	11.5	11	10.5	11	12
59	M	40	18.00	19	16	14.5	14.5	13.5	12.5	14	11	12	11.5
60	V	21	11.35	15	14	13.5	13	11.5	10	9.5	8.5	9	8