



VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
FUNDAMENTINIŲ MOKSLŲ FAKULTETAS
GRAFINIŲ SISTEMŲ KATEDRA

Oskaras Jieznys

**BINARINIO VAIZDO VANDENS ŽENKLŲ ĮTERPIMO SKAITMENINIO
GARSO ĮRAŠO AUTENTIŠKUMUI UŽTIKRINTI TAIKYMAI IR TYRIMAI**
INVESTIGATION AND APPLICATION OF BINARY IMAGE BASED
WATERMARKING FOR DIGITAL AUDIO RECORDS AUTHENTICATION

Baigiamasis magistro darbas

Informacinių technologijų studijų programa, valstybinis kodas 621E14004

Multimedijos informacinių sistemų specializacija

Informatikos inžinerijos studijų kryptis

Vilnius, 2014

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
FUNDAMENTINIŲ MOKSLŲ FAKULTETAS
GRAFINIŲ SISTEMŲ KATEDRA

TVIRTINU
Katedros vedėjas

(parašas)
Romualdas Baušys
2014 m. _____ mėn. ____ d.

Oskaras Jieznys

**BINARINIO VAIZDO VANDENS ŽENKLŲ ĮTERPIMO SKAITMENINIO
GARSO ĮRAŠO AUTENTIŠKUMUI UŽTIKRINTI TAIKYMAI IR TYRIMAI**
**INVESTIGATION AND APPLICATION OF BINARY IMAGE BASED
WATERMARKING FOR DIGITAL AUDIO RECORDS AUTHENTICATION**

Baigiamasis magistro darbas

Informacinių technologijų studijų programa, valstybinis kodas 621E14004

Multimedijos informacinių sistemų specializacija

Informatikos inžinerijos studijų kryptis

Vadovas

doc. dr. Jelena Devenson
(Moksl. laipsnis/pedag. vardas, vardas, pavardė)

(Parašas) (Data)

Konsultantas

(Moksl. laipsnis/pedag. vardas, vardas, pavardė)

(Parašas) (Data)

Konsultantas

(Moksl. laipsnis/pedag. vardas, vardas, pavardė)

(Parašas) (Data)

Lietuvių kalbos konsultantas doc. dr. Angelė Kaulakienė

(Moksl. laipsnis/pedag. vardas, vardas, pavardė)

(Parašas) (Data)

Vilnius, 2014

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
FUNDAMENTINIŲ MOKSLŲ FAKULTETAS
GRAFINIŲ SISTEMŲ KATEDRA

Informatikos inžinerijos studijų kryptis

Informacinių technologijų studijų programa, valstybinis kodas 621E14004

Multimedijos informacinių sistemų specializacija

TVIRTINU
Romualdas Baušys

(Parašas)

(Vardas, pavardė)

(Data)

**BAIGIAMOJO MAGISTRO DARBO
UŽDUOTIS**

.....Nr.
Vilnius

Studentui Oskarui Jiezniiui
(Vardas, pavardė)

Baigiamojo darbo tema: BINARINIO VAIZDO VANDENS ŽENKLŲ ĮTERPIMO SKAITMENINIO
GARSO ĮRAŠO AUTENTIŠKUMUI UŽTIKRINTI TAIKYMAI IR TYRIMAI

patvirtinta 201...m. d. dekanų potvarkiu Nr.

Baigiamojo darbo užbaigimo terminas 201...m. d.

BAIGIAMOJO DARBO UŽDUOTIS:

Magistro baigiamojo darbo užduotis yra atlikti išsamią garso įrašo ženklinimo binariniu atvaizdu metodų analizę. Pagal gautus rezultatus bei atlikus metodo patobulinimus pasiūlyti optimalų garso vandens ženklo įterpimo algoritmą, kurį naudodami galėtume įrodyti garso įrašo autentiškumą, net ir po jo signalo apdorojimo. Praktiškai ištirti siūlomo algoritmo kokybės parametrus.

Baigiamojo darbo rengimo konsultantai:

.....
.....
(Moksl. laipsnis/pedag. vardas, vardas, pavardė)

Vadovas

(Paraša)

dr. Jelena Devenson
(Moksl. laipsnis/pedag. vardas, vardas, pavardė)

Užduotį gavau

(Parašas)

(Vardas, pavardė)

(Data)

Vilniaus Gedimino technikos universitetas
Fundamentinių mokslų fakultetas
Grafinių sistemų katedra

ISBN ISSN
Egz. sk.
Data-.....-.....

Antrosios pakopos studijų **Informacinių technologijų** programos magistro baigiamasis darbas 4

Pavadinimas **Binarinio vaizdo vandens ženklų įterpimo skaitmeninio garso įrašo autentiškumui užtikrinti taikymai ir tyrimai**

Autorius **Oskaras Jieznys**

Vadovas **dr. Jelena Devenson**

Kalba: lietuvių

Anotacija

Baigiamajame magistro darbe sprendžiama muzikos kūrinių apsaugos nuo jų nelegalaus kopijavimo ir platinimo problema. Analizuojami garso žymėjimo binarinio atvaizdo vandens ženklų metodai. Pristatomi garso vandens ženklavimo algoritmų kokybės vertinimo kriterijai bei naudojantis jais nustatomas kokybiškiausių muzikos kūrinių apsaugą užtikrinantis literatūroje pateikiamas metodas. Pasirinktas algoritmas patobulinamas ir jo kokybė ištiriama praktiškai tikrinant vandens ženklų atsparumą garso signalo apdorojimui bei garso kokybės pokyčius po vandenženklų įterpimo. Taip pat tiriama garso kokybės po vandens ženklų įterpimo priklausomybė nuo jo signalo ilgio. Gauti rezultatai palyginami su pateikiamais literatūroje ir padaromos išvados. Darbo apimtis – 71 p. teksto be priedų, 38 pav., 14 lent., 34 bibliografiniai šaltiniai. Atskirai pridedami darbo priedai.

Prasminiai žodžiai: garso įrašo vandens ženklas, diskreti bangelių transformacija (DWT), kvantavimo indekso moduliacija (QIM), Arnoldo transformacija, dvejetainis atvaizdas.

Vilnius Gediminas Technical University
Faculty of Fundamental Sciences
Department of Graphical Systems

ISBN ISSN
Copies No.
Date-.....-.....

Master Degree Studies **Information Technologies** study programme Master Graduation Thesis 4

Title **Investigation and Application of Binary Image based Watermarking for Digital Audio
Records Authentication**

Author **Oskaras Jieznys**

Academic supervisor **Dr Jelena Devenson**

**Thesis
language:** Lithuanian

Annotation

The aim of this master thesis is to solve illegal copying and distribution problem of musical compositions. Methods of audio watermarking with binary image are analyzed. Quality evaluation criteria of watermarking algorithms are described and used for finding highest protection quality ensuring audio watermarking method. The selected algorithm is improved and it's quality practically tested by checking the resistance of the watermark in audio signal processing and sound quality changes after watermark insertion. Sound quality dependence of the signal length after watermark insertion is analyzed also. These results are compared with the reference literature and conclusions are drawn. Thesis consists of: 71 p. text without appendixes, 38 pictures, 14 tables, 34 bibliographical entries. Appendixes included.

Keywords: audio watermark, discrete wavelet transformation (DWT), quantization index modulation (QIM), Arnold transformation, binary image.

(Baigiamojo darbo sąžiningumo deklaracijos forma)

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Oskaras Jieznys, 20084770

(Studento vardas ir pavardė, studento pažymėjimo Nr.)

Fundamentinių mokslų fakultetas

(Fakultetas)

Informacinės technologijos, MISfm-12

(Studijų programa, akademinė grupė)

**BAIGIAMOJO DARBO (PROJEKTO)
SĄŽINGUMO DEKLARACIJA**

2014 m. birželio 2 d.

Patvirtinu, kad mano baigiamasis darbas tema „Binarinio vaizdo vandens ženklų įterpimo skaitmeninio garso įrašo autentiškumui užtikrinti taikymai ir tyrimai“ patvirtintas 2013 m. spalio 25 d. dekanų potvarkiu Nr. 367fm, yra savarankiškai parašytas. Šiame darbe pateikta medžiaga nėra plagijuota. Tiesiogiai ar netiesiogiai panaudotos kitų šaltinių citatos pažymėtos literatūros nuorodose.

Mano darbo vadovas dr. Jelena Devenson.

Kitų asmenų indėlio į parengtą baigiamąjį darbą nėra. Jokių įstatymų nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs (-usi).

(Parašas)

Oskaras Jieznys

(Vardas ir pavardė)

TURINYS

ŽYMENYS IR SANTRUMPOS	11
IVADAS	12
1. SKAITMENINIO VANDENS ŽENKLO SĄVOKA. RAIDA. APŽVALGA	14
1.1. Vandens ženklų atsiradimo raida	14
1.2. Skaitmeninio vandens ženklo apibrėžimas	15
1.3. Skaitmeninių vandens ženklų naudojimo sritys	17
1.3.1. Nuosavybės apsauga	17
1.3.2. Atpažinimas ir įsilaužimo aptikimas	17
1.3.3. Nuosavybės įrodymas	17
1.3.4. Pirštų atspaudai	18
1.3.5. Kopijavimo ir prieigos kontrolė	18
1.4. Garso vandens ženklo naudojimo reikalavimai	18
1.4.1. Suvokimo aiškumas	19
1.4.2. Vandens ženklo tvirtumas	19
1.4.3. Vandens ženklo bitų dažnis	20
2. GARSO ĮRAŠO ŽENKLINIMO VANDENS ŽENKLAIS METODAI	21
2.1. Mažiausiai svarbaus bito metodas	21
2.2. Aido slėpimo metodas	22
2.3. Išplėsto spektro metodas	23
2.4. Mišinio metodas	25
2.5. Kvantavimo indekso moduliacija	25
2.6. Alfa „ α “ statistinė moduliacija	26
2.6.1. Vandens ženklo bito įterpimo strategija naudojant „ α “	27
2.6.2. Vandens ženklo bito aptikimas naudojant „ α “	27
2.7. Garso žymėjimo skaitmeniniu vandens ženklu metodų privalumai ir trūkumai	27
3. BINARINIO VAIZDO ĮTERPIMO Į GARSO ĮRAŠĄ ALGORITMAI	29
3.1. Algoritmuose naudojama metodika bei jų vertinimo kriterijai	29
3.1.1. Paveikslėlio užšifravimas naudojant Arnoldo transformaciją	29
3.1.2. Diskrečioji bangelių transformacija	29
3.1.3. Algoritmo testavimo vertinimo kriterijai	30
3.1.4. Vienetinės vertės išskyrimas	31
3.2. Adaptyvus garso ženklavimas išskiriant vieną reikšmę iš bangelių srities	32
3.2.1. Vandens ženklo įterpimo algoritmas	32
3.2.2. Vandens ženklo išgavimas	34
3.2.3. Praktiniai rezultatai ir jų aptarimas	35
3.3. Garso įrašo ženklavimas binarinius atvaizdu naudojant diskrečiąją bangelių transformaciją	39
3.3.1. Vandens ženklo įterpimas	39
3.3.2. Vandens ženklo atpažinimas turint jau paženklintą garso įrašą	39
3.3.3. Praktiniai algoritmo bandymų rezultatai	40
3.4. Normuotos erdvės, negirdimas garso vandens ženklavimo algoritmas naudojant diskrečią bangelių transformaciją	43
3.4.1. Vandens ženklo įterpimo algoritmas	44
3.4.2. Vandens ženklo nuskaitymo algoritmas	45
3.4.3. Algoritmo testavimo rezultatai	45
3.5. Neturintis nuostolių garso ženklavimo binariniu vandens ženklu algoritmas naudojantis alfa statistinę moduliaciją	47
3.5.1. Viso vandens ženklo įterpimo procesas	47
3.5.2. Viso vandens ženklo nuskaitymo procesas	48
3.5.3. Algoritmo bandymai	49

4. OPTIMALAUS ALGORITMO PASIRINKIMAS	50
4.1. Algoritmų savybių įvertinimas	50
4.2. Muzikos pramonei optimalaus algoritmo pasirinkimas pagal įvertintus kriterijus	52
5. PRAKTINĖ DALIS	54
5.1. Pasirinkto algoritmo tobulinimas.....	54
5.2. Patobulintas normuotos erdvės garso įrašo žymėjimo binariniu atvaizdu algoritmas naudojant diskrečią bangelių transformaciją ir kvantavimo indekso moduliaciją.....	54
5.2.1. Vandens ženklų įterpimo algoritmas	55
5.2.2. Vandens ženklų nuskaitymo algoritmas.....	57
5.3. Algoritmo savybių tyrimo metodika.....	57
5.4. Darbui reikalinga programinė įranga.....	59
5.5. Algoritmo tyrimo rezultatai	60
5.6. Tyrimo rezultatų aptarimas.....	65
IŠVADOS	68
LITERATŪROS IR INFORMACINIŲ ŠALTINIŲ SĄRAŠAS	69
PRIEDAI	72
1 priedas. Binarinio atvaizdo įterpimo į garso įrašą programos kodas	73
2 priedas. Binarinio atvaizdo išgavimo iš garso įrašo programos kodas	76
3 priedas. Pažymėto binariniu atvaizdu garso įrašo apdorojimo programos kodas.....	78
4 priedas. Pažymėto binariniu atvaizdu garso įrašo testavimo programos kodas.....	80

ILIUSTRACIJŲ SĄRAŠAS

1.1 pav. Straipsnių parašytų IEEE duomenų bazėje vandens ženklų tema skaičius per metus	15
2.1 pav. LSB metodo veikimo schema [4]	22
2.2 pav. Vandens ženklavimo metodo naudojant aidą įterpimą parametrai	22
2.3 pav. Išplėsto spektro metodo veikimo schema [3]	24
2.4 pav. Pavyzdžių modifikacija naudojant QIM [5]	26
2.5 pav. „α“ Poabių skirtumo šablonas [21]	26
3.1 pav. Duomenų dimensijų sumažinimas iš 2 į 1 naudojant vienetinės vertės išskyrimą [34]	32
3.2 pav. Vandens ženklų pridėjimo algoritmas naudojant adaptyvų vandens ženklavimo metodą.....	33
3.3 pav. Dvejetainis vandens ženklas	35
3.4 pav. Atlikus dviejų lygių DWT operaciją gautos išėjimo sritys	39
3.5 pav. Originalaus vandens ženklų paveikslėlis	40
3.6 pav. Originalus instrumento garso įrašas	40
3.7 pav. Pažymėtas vandens ženklų instrumentų garso įrašas	41
3.8 pav. Originalus pop muzikos garso įrašas	41
3.9 pav. Pažymėtas vandens ženklų pop muzikos garso įrašas	41
3.10 pav. Išskleisto vandens ženklų iš instrumentinio garso įrašo būsenos po Adobe Audition apdorojimo	42
3.11 pav. Išskleisto vandens ženklų iš pop garso įrašo būsenos po Adobe Audition apdorojimo	43
3.12 pav. Negirdimo vandens ženklų įterpimo algoritmas naudojant diskrečią bangelių transformaciją ir kvantavimo indekso moduliaciją	44
3.13 pav. Negirdimo vandens ženklų išskleidimo algoritmas naudojant diskrečią bangelių transformaciją ir kvantavimo indekso moduliaciją	45

3.14 pav. Vandens ženklų įterpimas naudojant alfa statistinės moduliacijos metodą	48
3.15 pav. Vandens ženklų nuskaitymas naudojant alfa statistinės moduliacijos metodą	49
5.1 pav. Patobulinto negirdimo vandens ženklų įterpimo algoritmas naudojant diskrečią bangelių transformaciją ir kvantavimo indekso moduliaciją	56
5.2 pav. Patobulinto negirdimo vandens ženklų nuskaitymo algoritmas naudojant diskrečią bangelių transformaciją ir kvantavimo indekso moduliaciją	57
5.3 pav. Originalus garso signalas	60
5.4 pav. Originalus vandens ženklas prieš įterpimą	60
5.5 pav. Originalus vandens ženklas įterpimo metu, užšifruotas naudojant Arnoldo transformaciją	60
5.6 pav. Vandens ženklų pažymėtas garso įrašas. Jokio apdorojimo neatlikta	60
5.7 pav. Originalaus ir pažymėto vandens ženklais garso įrašų signalo palyginimas laiko tarpe tarp 19 – 20 s	61
5.8 pav. Nuskaitytas vandens ženklas iš neapdoroto garso įrašo	61
5.9 pav. Nuskaitytas vandens ženklas iš garso įrašo paveikto Baltuoju Gauso triukšmu	62
5.10 pav. Nuskaitytas vandens ženklas iš garso įrašo paveikto Gauso žemų dažnių filtru	62
5.11 pav. Nuskaitytas vandens ženklas iš garso įrašo paveikto Kaizerio žemų dažnių filtru	63
5.12 pav. Nuskaitytas vandens ženklas iš garso įrašo kuriam atliktas diskretizacijos dažnio keitimas	63
5.13 pav. Nuskaitytas vandens ženklas iš garso įrašo kuriam atliktas kvantavimo keitimas	64
5.14 pav. Nuskaitytas vandens ženklas iš garso įrašo kuriam atliktas formato keitimas į MP3 32kbps ir atgal į wav	64
5.15 pav. Nuskaitytas vandens ženklas iš garso įrašo kuriam atliktas formato keitimas į MP3 16kbps ir atgal į wav	64
5.16 pav. Nuskaitytas vandens ženklas iš garso įrašo kuriam pridėtas aidas	65
5.17 pav. Signalų – triukšmo santykio priklausomybė gauta garso įrašą pažymėjus binariniu atvaizdu, naudojant patobulintą vandens ženklavimo algoritmą	67

LENTELIŲ SĄRAŠAS

3.1 lentelė Objektivaus skirtumo standartai	31
3.2 lentelė Gauti vandens ženklų atpažinimo rezultatai	35
3.3 lentelė Džiazo garso įrašo pažymėto vandens ženklų apdorojimo rezultatai	37
3.4 lentelė Įvairių muzikos stilių garso įrašų pažymėtų vandens ženklų apdorojimo rezultatai	38
3.5 lentelė klausymo testo rezultatai	42
3.6 lentelė Normuotos erdvės, negirdimo vandens ženklavimo algoritmo testavimo rezultatai atlikus apdorojimo procedūras iš pateikto sąrašo	46
3.7 lentelė Normuotos erdvės, negirdimo vandens ženklavimo algoritmo objektyvaus įvertinimo skirtumas ir signalo – triukšmo santykis	47
3.8 lentelė Garso įrašo kokybė jį pažymėjus binariniu paveikslėliu naudojant alfa statistinę moduliaciją	49
3.9 lentelė Nuskaityto vandens ženklų kokybė naudojant alfa statistinę moduliaciją bei atliktus garso apdorojimui skirtas atakas	49

4.1 lentelė Garso įrašo ženklavimo binariniu atvaizdu algoritmų aptartų literatūros apžvalgoje bandymų rezultatai	50
4.2 lentelė Garso įrašo pažymėto binariniu vandens ženklu signalo ir triukšmo santykis naudojant literatūros apžvalgoje pristatytus algoritmus	51
4.3 lentelė Garso įrašo pažymėto binariniu vandens ženklu objektyvaus skirtumo įvertinimas naudojant literatūros apžvalgoje pristatytus algoritmus	52
5.1 lentelė Bandymo rezultatai pakeitus garso formatą iš WAV į MP3 32kbps ir 16kbps, bei atgal į WAV	64
5.2 lentelė Garso įrašo ženklavimo binariniu atvaizdu algoritmų pateiktų literatūros apžvalgoje bei patobulinto ir praktiškai išbandyto algoritmų testavimo rezultatai	65
5.3 lentelė Garso įrašo pažymėto binariniu vandens ženklu signalo ir triukšmo santykis bei objektyvaus įvertinimo skirtumas naudojant literatūros apžvalgoje pristatytus ir patobulintąjį algoritmus	66

Žymenys ir santrumpos

LSB (angl. <i>Least Significant Bit</i>)	mažiausiai svarbus bitas
MSB (angl. <i>Most Significant Bit</i>)	svarbiausias bitas
SS (angl. <i>Spread Spectrum</i>)	išplėsto spektro metodas
PRN (angl. <i>Pseudo Random Number Generator</i>)	atsitiktinių skaičių generatorius
QIM (angl. <i>Quantization Index Modulation</i>)	kvantavimo indekso moduliacija
NC (angl. <i>Normalized correlation</i>)	normalizuota koreliacija
BER (angl. <i>Bit Error Rate</i>)	bitų klaidos norma
SNR (angl. <i>Signal to Noise Ratio</i>)	signalų ir triukšmo santykis
ODG (angl. <i>Objective Difference Grade</i>)	objektyvus skirtumo įvertinimas
SVD (angl. <i>Singular Value Decomposition</i>)	vienetinės vertės išskyrimas
DWT (angl. <i>Discrete Wavelet Transformation</i>)	diskrečioji bangelių transformacija
MOS (angl. <i>Mean Opinion Score</i>)	nuomonės taškai

IVADAS

Šiuolaikinio žmogaus gyvenime internetas užima labai svarbią dalį. Jam atsiradus dar XX am., kompiuterių naudotojai ne tik gaudavo informaciją iš autentiškų šaltinių, bet ir ėmė ją dalytis tarpusavyje. Atsirado programišiai, kurie ne tik dalijosi informacija, bet ir keisdavo ją be kūrėjo žinios ir sutikimo. Tai pradėjo kelti problemų informacijos savininkams (kūrėjams), kurie prarasdavo vis daugiau ir daugiau pajamų gaunamų būtent iš savo veiklos, todėl buvo labai reikalingas sprendimas, kaip galima būtų apsaugoti skaitmeninę informaciją nuo neleistino jos panaudojimo.

Apsaugos priemonės turi būti pakankamai efektyvios, atsparios ir unikalios, kad visiškai užtikrintų autorinių failų saugumą. Technologijos plėtra padidino stenografijos mastus, tačiau kartu sumažėjo jos patikimumas. Dėl to buvo pradėtas kurti ir tobulinti naujas informacijos apsaugos mechanizmas – žymėjimas vandens ženklais (angl. *Watermarking*). Pirmiausiai ši nauja priemonė buvo pritaikyta paveikslėlių apsaugai. Ji pavadinta atvaizdo vandens ženklinimu (angl. *Image Watermarking*). Šis metodas tapo labai populiarus, tačiau programišiai pradėjo ieškoti galimybių įveikti tokio tipo apsaugą, taip sukeldami dar didesnę galvos skausmą programinės įrangos kūrėjams bei saugomos vaizdinės informacijos savininkams. Laikui bėgant, buvo pastebėta, kad vandens ženklą galima įterpti ir į garso signalus. Šis metodas buvo pavadintas garso vandens ženklinimu (angl. *Audio Watermaking*). Kadangi muzikos pramonė viena iš didžiausių pasaulyje, tokio tipo apsauga turi sustabdyti arba labai ženkliai sumažinti „piratavimo“ galimybes, leidžiant aptikti nesąžiningus naudotojus ir juos nubausti. Skaitmeninio vandens ženklinimo technologijos esmė yra apsaugoti informaciją į ją įterpiant papildomas modas, leidžiančias nustatyti duomenų kilmę. Šis apsaugos metodas turi minimaliai lemti saugomos informacijos kokybę ir būti maksimaliai atsparus kenkėjiškoms atakoms.

Darbo problema – „piratavimo“ galimybių sumažinimas ar jų visiškas sunaikinimas muzikos srityje. Baigiamajame magistro darbe pristatomas garso įrašo žymėjimo skaitmeniniais vandens ženklais tyrimas. Darbo esmė yra išanalizuoti jau pristatytus garso žymėjimo binariniu atvaizdu būdus ir, lyginant pateiktus jų bandymų rezultatus, rasti labiausiai tinkamą muzikos pramonei, t.y. metodą, kuris užtikrintų aukštą garso įrašo kokybę bei paties vandens ženklo atsparumą garso apdorojimui. Nustačius algoritmą, kuris atitinka šiuos du pagrindinius kriterijus, jis buvo patobulintas ir pritaikytas praktiniams rezultatams optimizuoti. Tyrimams ir bandymams naudojamas teoriškai rastas ir patobulintas garso žymėjimo algoritmas. Jis realiai atkurtas ir realizuotas sukuriant tam skirtą programinę įrangą. Praktiškai vandens ženklo įrašymo ir nuskaitymo algoritmo kokybė buvo vertinama nustatinėjant garsinio signalo pakeitimus bei taikant vaizdo informacijos kokybės įvertinimo standartines metodikas.

Pirmajame skyriuje aptarta vandens ženklo bei skaitmeninio vandens ženklo sąvoka, trumpa jų raida, naudojimo sritys bei jų pagrindinės savybės.

Antrasis skyrius skirtas garso žymėjimo vandens ženklų metodų pristatymui bei jų savybių palyginimui ieškant optimalaus varianto.

Trečiajame skyriuje apžvelgiama literatūra darbo tematika, pateikiami moksliniuose straipsniuose pristatomi darbo tikslą įgyvendinantys algoritmai, jų veikimo principai bei algoritmų kokybę apibūdinantys rezultatai.

Ketvirtajame skyriuje aptariamas optimalaus garso ženklavimo binariniu paveikslėliu algoritmo pasirinkimas. Jis atliekamas lyginant pateiktų algoritmų kokybės įvertinimo rezultatus.

Penktajame skyriuje aptariamas išrinkto algoritmo tobulinimas, pateikiama jo blokinė schema bei detalus veikimo aprašymas. Pristatoma praktinė algoritmo tyrimo metodika, kurios tikslas yra įvertinti garso signalo ir paveikslėlio kokybę po nuskaitymo ir skaitmeninio apdorojimo. Pateikiama gautų rezultatų analizė.

1. SKAITMENINIO VANDENS ŽENKLO SĄVOKA. RAIDA. APŽVALGA

1.1. Vandens ženklų atsiradimo raida

Nors pats popierius išrastas Kinijoje prieš maždaug tūkstantį metų, jo vandens ženklai atsirado tik 1282 m. Italijoje [2]. Ženkilai buvo daromi pridodant plonus metalinius kontūrus popieriaus ruošiniams, o juos nuėmus atitinkamose vietose popierius likdavo plonesnis ir labiau permatomas.

Pirmųjų vandens ženklų tikslas ir paskirtis nėra aiški. Jie gal būt buvo naudojami identifikuoti popieriaus ruošiniams, arba tiesiog kaip dekoracija.

Aštuonioliktame amžiuje vandens ženklai ant popieriaus tapo konkrečiau naudojami Europoje bei Amerikoje. Jie buvo taikomi prekės ženklu, popieriaus pagaminimo datai bei jo lapo dydžiui apibūdinti. Vandens ženklai pradėti naudoti kaip nesuklastojami ženklai pinigams ir dokumentams.

Pats terminas vandens ženklas (angl. *watermark*) atsirado tik aštuoniolikto amžiaus pabaigoje. Pati sąvoka nėra itin tiksli, nes vanduo realiai nėra reikalingas norint sukurti vandens ženklą. Toks pavadinimas duotas todėl, kad ženklai turi panašius efektus, kaip vanduo patekęs ant popieriaus.

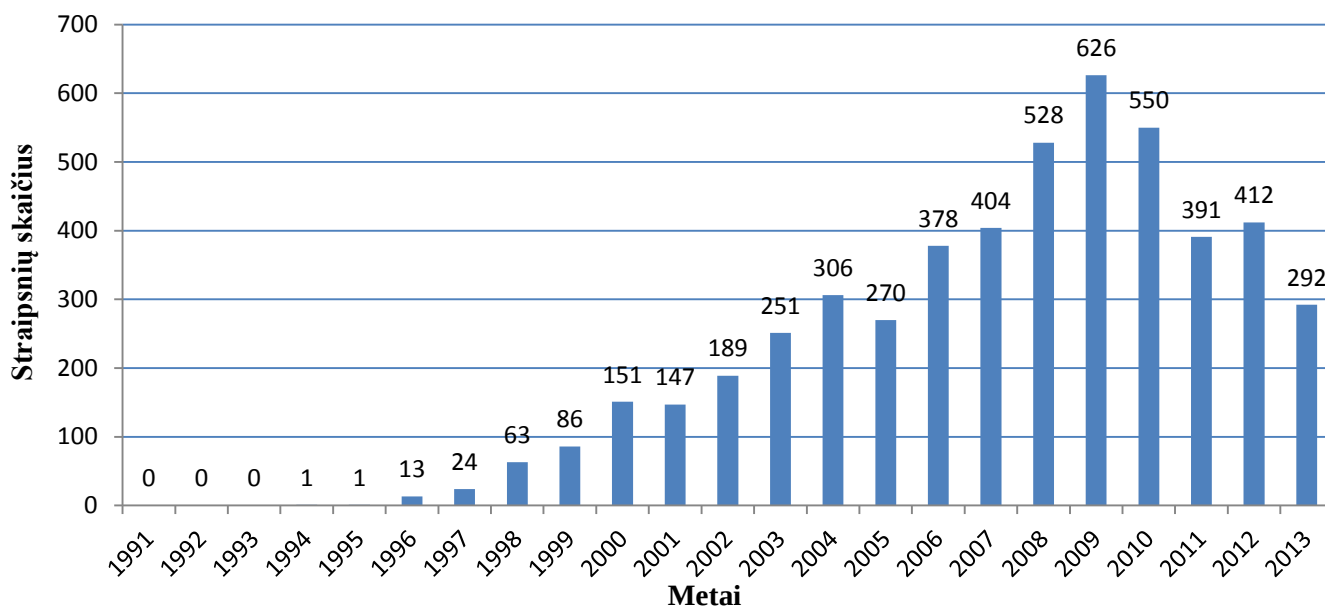
Laikui bėgant, bandyta suklastoti vandens ženklą ir tai pavyko. Klastojimas davė dingstį patobulinti vandens ženklų sistemą – Wiliamas Congreve [22] išrado spalvotų vandens ženklų gamybos technologiją, įdedant spalvotos medžiagos į popierių gamybos metu. Tokio tipo žymėjimą buvo labai sunku suklastoti, nes Anglijos Centrinis bankas atsisakė juos naudoti viešai, nes tiesiog buvo taikoma per sudėtinga gamybos technologija. Praktiškesnį metodą išrado kitas anglas Wiliamas Henris Smitas. Jis nusprendė pakeisti metalinius kontūrus kurie buvo naudojami pirmiesiems vandens ženklu į negilų reljefą turinčią plokštelę, užspaudžiamą ant popieriaus ruošinio. Ši technologija naudojama ir dabar norint išgauti prezidento Jaksono veidą 20\$ banknote.

Po 400 metų pasirodė pirmasis vandens ženklinimo pavyzdys technologijose. 1954 m. Emilis Hembrooke iš „Muzak“ korporacijos užpatentavo muzikos įrašų patentavimo technologiją. Identifikacijos kodas į garso įrašą būdavo talpinamas naudojant specialų filtrą, veikiantį 1 kHz dažniu. Pats filtras veikė brūkšnelių ir taškų principu pagal Morzės abėcėlę. Ši sistema buvo naudojama „Muzak“ korporacijos iki 1984 m. Įdomu tai, kad tokio išradimo nesuprato visuomenė ir jį laikė slapto reklamos žinučių skleidimu klausytojams.

Sunku nustatyti kada tiksliai pradėta naudoti skaitmeninio vandens ženklo sąvoka. 1979 m. Szepanskis [2] apibūdino mašininio atpažinimo modelį, kuris galėjo būti naudojamas dokumentuose tapatybės nustatymui. Po 9 metų Holtas apibūdino identifikavimo kodo įterpimo į garso signalą metodą. Tuomet pasirodė Komats ir Tominaga, kurie 1988 m. pirmą kartą pavartojo skaitmeninio vandens ženklo (angl. *digital watermark*) sąvoką, tačiau jos naudojimas išplito tik devyniasdešimtaisiais.

Apie 1996 m. susidomėjimas skaitmeniniu vandens ženkliniu pradėjo labai sparčiai didėti.

1.1 pav. matome histogramą, apibūdinančią straipsnių skaičių parašytą ta tema per metus.



1.1 pav. Straipsnių parašytų IEEE duomenų bazėje vandens ženklų tema skaičius per metus

Šiais laikais keletas organizacijų pradėjo vandens ženklavimo technologijai taikyti skirtingus standartus. Plagijavimo apsaugos techninė darbo grupė (angl. *The Copy Protection Technical Working Group*) testavo vandens ženklo įterpimo sistemas DVD diskų apsaugai. Secure Digital Music Initiative padarė vandens ženklavimo technologiją pagrindiniu jų muzikos apsaugos komponentu. Dviejuose Europos Sąjungos finansuotuose projektuose „Viva“ ir „Talisman“ buvo išbandytas vandens ženklavimas, skirtas transliacijų stebėjimui. Tarptautinė ISO organizacija susidomėjo šia technologija, kuriant pažangius MPEG standartus.

1.2. Skaitmeninio vandens ženklo apibrėžimas

Skaitmeninis vandens ženklas (angl. *Digital Watermark*) – tam tikros rūšies žymeklis, įdėtas į triukšmams atsparius signalus, tokius kaip garso arba atvaizdo duomenys [1]. Jis įprastai naudojamas nustatyti skaitmeninės informacijos kūrėjo tapatybę. Vandens ženklo įterpimas, tai procesas, kai autentiškumą užtikrinanti informacija paslepama nešančiajame signale. Ji turėtų sietis su šiuo signalu, tačiau tai nėra privaloma sąlyga, duomenys gali būti visiškai neturintys nieko bendro su jų nešliu.

Skaitmeniniai vandens ženklai gali būti naudojami patvirtinti nešlio signalo tapatumą arba vientisumą, taip pat identifikuoti savininko tapatybę. Skaitmeniniai vandens ženklai, kaip ir paprasti yra pastebimi tik tam tikromis sąlygomis, pvz., naudojant tam tikrus algoritmus, o visais kitais

atvejais yra nematomi [24]. Jeigu ši informacijos apsaugos priemonė iškraipo nešulį taip, kad jis tampa neatpažįstamas – ji nenaudojama. Įprastiniai vandens ženklai gali būti pridėti matomai informacijai, tokiai kaip atvaizdai ar vaizdo įrašai, tuo tarpu skaitmeninis ženklinimas naudojamas garse, nuotraukose, paveiksluose, vaizde, teksto arba 3D modeliams. Signalas gali būti pažymėtas keliais skirtingais vandens ženklais vienu metu. Priešingai, negu metaduomenys, kurie yra pridedami nešliui signalui, skaitmeninis vandens ženklas nekeičia to signalo dydžio [1].

Skaitmeninio vandens ženklo savybės priklauso nuo jo naudojimo srities. Žymint medija failus, autorystės informacija, skaitmeninis vandens ženklas turi būti labai atsparus nešlio signalo galimoms modifikacijoms. Kai norima užtikrinti vientisumą, tuomet naudojamas trapus vandens ženklas.

Stenografijoje ir skaitmeniniame ženklime naudojami stenografiniai metodai, skirti slapta įterpi duomenis į triukšmingus signalus. Stenografija specializuojasi į neatitikimus žmogaus pojūčiams, o skaitmeninis ženklinimo esmė yra tvirtumas [23].

Kai skaitmeninė duomenų kopija yra originali, vandens ženklas yra pasyvi apsaugos priemonė, ji tiesiog žymi duomenis, tačiau neriboja prieigos ar jų valdymo. Vandens ženklas yra integruojamas į signalą kiekviename platinimo taške. Jeigu darbo kopija randama vėliau, tada vandens ženklas gali būti gautas iš žinomo duomenų šaltinio. Ši technologija naudojama nelegaliam filmų šaltiniui nustatyti.

Vandens ženklai skirstomi į:

- Matomas. Nuotraukoje ar vaizdo įrašė yra matomas skaitmeninis vandens ženklas[24]. Paprastai tai būna tekstas ar logotipas, kuris identifikuoja savininką. Kai televizijos transliuotojas priduria savo logotipą perduodamo vaizdo kampe, tai taip pat yra matomas vandens ženklas.
- Nematomas. Nematomuose skaitmeniniuose vandens ženkuose informacija pridedama kaip skaitmeniniai garso ar vaizdo įrašo duomenys, tačiau jis nesuvokiamas kaip toks (nors įmanoma nustatyti, kad yra paslėpta informacija signale) [24]. Vandens ženklas gali būti skirtas plačiam vartojimui, todėl lengva susigrąžinti kaip iš stenografijos, kai perduodamas slaptas pranešimas įterpiant į skaitmeninį signalą.

Matomo vandens ženklo tikslas yra susieti nuosavybę ar kitokią aprašomojo pobūdžio informaciją, kad signalą būtų sunku pašalinti. Taip pat paslėptą informaciją galima naudoti kaip slaptą asmeninio bendravimo priemonę. Į failą įterpiamas pranešimas, kaip vandens ženklas, kurį gali aptikti tik žinantys, koku būdu jis buvo įterptas.

Taigi skaitmeniniai vandens ženklai dažniausiai taikomi:

- autorių teisių apsaugai;

- šaltinių sekimui (skirtingi gavėjai gauna vandens ženklus su skirtingu turiniu);
- transliacijos stebėjimas (televizijos naujienų vaizdo įrašai dažnai yra su tarptautinių agentūrų vandens ženkliais);
- slaptam bendravimui.

1.3. Skaitmeninių vandens ženklų naudojimo sritys

1.3.1. Nuosavybės apsauga

Naudojant nuosavybės apsaugos programinę įrangą, vandens ženklas, kuriame užkoduota nuosavybės informacija yra įterpiamas į norimą apsaugoti signalą [3]. Vandens ženklas, žinomas tik nuosavybės teisių savininkui, turi būti saugus ir neišnaikinamas (t.y. turi išlikti po bendrų signalo modifikacijų ir kitų tyčinių atakų) bei iškilus ginčams užtikrintai įrodyti savininko tapatybę. Vandens ženklo atpažinimas privalo būti itin tikslus ir turėti labai mažą klaidos tikimybę, tačiau vandens ženklo bitų skaičius turi būti minimalus ir užtikrinantis pakankamą saugos lygį.

1.3.2. Atpažinimas ir įsilaužimo aptikimas

Naudojant turinio atpažinimo programinę įrangą, nustatytas antrinių duomenų rinkinys pridedamas į norimą apsaugoti garso signalą ir jis vėliau taikomas įsilaužimui į nešantįjį signalą nustatyti [3]. Sudėtingas vandens ženklo pašalinimas ar jo darymas neaptinkamu yra neesminis dalykas, nebent tai svarbu pačiam programišiui, tačiau netikras savininko atpažinimas nelegaliu būdu arba modifikuotu nešliu turi būti sustabdytas. Realiose programose yra pasirenkama nustatyti ir ignoruoti netyčinius pakeitimus (pvz., atsiradusius MPEG suspaudimo metu) [25]. Aptikimas turi būti atliktas be originalaus signalo, nes bet kuris toks signalas nėra prieinamas arba jo vientisumas turi būti nustatytas. Toks vandens ženklo atpažinimo metodas įprastai vadinamas akluoju.

1.3.3. Nuosavybės įrodymas

Vis labiau reikalaujama vandens ženklą naudoti ne tik garso signalo savininko atpažinimui, bet ir jį laikyti tiesioginiu nuosavybės įrodymu. Problema iškyla tuomet, kai konkurentas nusprendžia naudodamas redagavimo programinę įrangą pakeisti originalų nuosavybės teisių turėtojo pranešimą savuoju. Pagrindinis senųjų vandens ženklų sistemų trūkumas buvo atviras tų ženklų detektorius, kurį galėjo gauti konkurentai [26]. Visi tie, kas gali atpažinti paženklintą failą, gali nesunkiai tą žymenį pašalinti. Kadangi konkurentas galėjo lengvai gauti autoriinių teisių atpažinimo programinę įrangą, tai jam buvo nesudėtinga tiesiog ištrinti originalų vandens ženklą ir jį pakeisti savuoju.

Norint pasiekti, jog vandens ženklas galėtų būti laikomas kaip nuosavybės įrodymas, būtina detektorių padaryti neprieinamu visuomenei, o be jo konkurentui ištrinti apsaugos ženklą yra nepaprastai sudėtinga. Tačiau net jeigu savininko vandens ženklas negali būti panaikintas, konkurentai vis tiek gali rasti būdų pakenkti. Jie gali tiesiog pridėti nuosavą vandens ženklą ir save priskirti prie teisėtų garso kūrinio savininkų. Ši problema gali būti išspręsta šiek tiek pakeičiant problemos apibūdinimą. Vietoj tiesioginio nuosavybės įrodymo vandens ženklo, pvz. „Tomas šio garso įrašo savininkas“, algoritmas bandys įrodyti, kad konkurento garso įrašas sukurtas iš originalaus pažymėtojo signalo. Tai darys lygindamas pradinius nuostatus ir kitus siejamų failų duomenis.

1.3.4. Pirštų atspaudai

Papildoma informacija įterpta kaip vandens ženklas yra naudojama sekti kūrėją arba multimedijos failo kopijų gavėjus [25]. Pvz., skirtingoms CD ir DVD kopijoms pridedami vandens ženklai, turintys skirtingus serijos ir nuosavybės numerius. Programinėje įrangoje naudojami pirštų atspaudų algoritmai turi būti itin stiprūs prieš iš anksto apgalvotas atakas ir signalo apdorojimą, tokį kaip filtravimas ar mažinamasis glaudinimas (angl. *lossy compression*). Pirštų atspaudai turi būti naudojami atsakingai.

1.3.5. Kopijavimo ir prieigos kontrolė

Kopijavimo kontrolės tikslais naudojamas vandens ženklas apibūdina atskiros kopijos valdymo arba jos apsaugos valdymo politiką. Šio ženklo detektorius įprastai integruojamas į įrašymo ir atkūrimo sistemas. Po to, kai vandens ženklas jau atpažintas ir turinys iššifruotas, kopijavimo ir prieigos kontrolės politika vykdoma nukreipiant aparatinės ir programinės įrangos operacijas tokias kaip įrašymo modulio įjungimas ir išjungimas [27]. Šios programos reikalauja atsparumo galimoms atakoms ir signalų savybių pokyčiams, galimybės atlikti aklą vandens ženklo aptikimą ir pridėti nedidelį bitų kiekį į nešantįjį signalą.

1.4. Garso vandens ženklo naudojimo reikalavimai

Vandens ženklinimo algoritmai gali būti apibūdinami tam tikru kiekiu nustatytų savybių. Šiame skyrelyje aptarsime svarbiausius 3 iš jų. Jos visos sudaro tris „magiškojo trikampio“ kampus vandens ženklinime, kurie negali veikti pakaitomis.

1.4.1. Suvokimo aiškumas

Daugelyje programinės įrangos, vandens ženklo įterpimo algoritmas turi prijungti papildomus duomenis nepakeičiant garso nešančiojo signalo kokybės [28]. Vandens ženklavimo algoritmo slaptumo savybės įprastai apibūdinamos panašumu tarp originalaus ir jau pažymėto garso įrašo, tačiau įprastai žymint garsą jo kokybė tampa blogesnė.

Perkoduojamo paprasto garso signalo kokybė nustatoma tiesiog lyginant jį su originalu. Pažymėtas garso signalas vertinamas panašiai. Jis gali būti analizuojamas trim metodais: garso kokybės suvokimo matavimas (angl. *Peceptual Audio Quality Measure* arba *PAQM*), garso kokybės suvokimo apskaičiavimas (angl. *Perceptual Evaluation of Audio Quality* arba *PEAQ*) ir triukšmo su kokybišku įrašu santykis (angl. *Noise to Mask Ratio* arba *NMR*) [29].

Žinoma atliekami ir paprasti klausymo testai. Daugybė muzikos žanrus apibūdinančių ištraukų naudojami kaip testavimo signalai. Pirmoje testo dalyje dalyviai klauso originalaus ir paženklinto įrašų ir tuomet apibūdina skirtumus tarp originalo ir paženklinto įrašo. Sekančioje testo dalyje klausytojams reikia atpažinti, kuris garsas tikras, kuris paženklintas. Jeigu balsai pasiskirsto maždaug po 50%, tuomet reiškia, kad paženklinto garso įrašo atskyrimas paprastam žmogui praktiškai neįmanomas. To ir yra siekiama.

1.4.2. Vandens ženklo tvirtumas

Algoritmo tvirtumas (angl. *Watermark Robustness*) yra apibūdinamas, kaip vandens ženklo savybė būti atskleistam po bendrinio garso signalo apdorojimo [9]. Norint visada atpažinti vandens ženklą, reikalingas jo atsparumas signalų apdorojimo procesams. Pvz., radijo transliacijoje pridėtas vandens ženklas turi būti atsparus signalo perdavimui reikalingam apdorojimui, įskaitant dinaminį suspaudimą, žemų dažnių filtravimą ir t.t. Tačiau kai kuriose aplikacijose vandens ženklavimo tvirtumas negali būti išlaikomas. Tokie algoritmai vadinami trapiais.

Esminis vandens ženklų sistemos tikslas yra sukurti paprastai atpažįstamą žymėjimą. Specifinio vandens ženklavimo išskleidimo patikimumas priklauso nuo originalių duomenų savybių bei specifinių ženklavimo ir signalo apdorojimo sukeltų iškraipymų. Vandens ženklo aptikimui ir iškodavimui naudojami skirtingi patikimumo matavimai. Žymėjimo metu prie nešančiojo signalo pridėdama speciali žinutė. Iškodavimo patikimumas dažnai apibūdinamas bito klaidos norma (angl. *bit error rate*). Vandens ženklas laikomas atpažintu tuomet, kai sistema pagal nuskaitytus duomenis randa atitikmenį savo duomenų bazėje.

1.4.3. Vandens ženklų bitų dažnis

Vienas iš pagrindinių garso signalo vandens ženklavimo sistemos nustatymų yra pažymėto signalo žymėjimo bitų dažnis. Jis įprastai nustatomas pagal specifinius sistemos reikalavimus. Pridėto vandens ženklų bitų dažnis yra jų skaičius telpantis nustatytam laiko vienetui, įprastai tai būna sekundė [3].

Gerai žinoma, kad nereikia daug bitų per sekundę, norint atkurti muzikos kokybę artimą gaunami iš kompaktinio disko. Tai reiškia, kad nesuspaudus muzikos, reikalingas kiekis triukšmų gali būti įterptas į signalą ir jo visiškai nepastebės galutinis vartotojas.

Įprastai stengiamasi maksimizuoti įterpto vandens ženklų bitų dažnį, tačiau didelės talpos slėpimo algoritmai dažniausiai nėra atsparūs signalų apdorojimui., tačiau autoriai [30] 2001 metais apibūdino sistemą su vandens ženklu, kurio dažnis 100 kbps ir jis nesukelia originalaus garso signalo iškraipymo ir gali puikiai išgauti paslėptus vandens ženklų bitus.

Kai kurios iš garso ženklavimo vandens ženklais aplikacijų, tokių kaip kopijavimo kontrolė, reikalauja įvesti serijos numerį ir autoriaus ID su vidutiniu 0,5 žymėjimo bitų dažniu, tačiau tokio tipo vandens ženklai yra tvirti ir gali išlikti atliekant daugumą signalo modifikacijų.

2. GARSO ĮRAŠO ŽENKLINIMO VANDENS ŽENKLAIS METODAI

Garso įrašų ženklavimo vandens ženklais technologijos gali būti skirstomos į dvi grupes [4]. Viena iš jų yra priklausoma nuo laiko, kita – nuo transformacijų. Metoduose, priklausančiose nuo laiko, vandens ženklo įterpimui nereikalinga jokia transformacija. Juose naudojami originalūs garso signalo pavyzdžiai. Viena iš žymiausių šios srities kodavimo technologijų yra mažiausiai svarbaus bito (angl. *Least Significant Bit* arba *LSB*) metodas. Šiuo būdu vandens ženklas įterpiamas į mažiausiai svarbius signalo bitus.

Priešingai negu laiko srities metodai, transformacijų vandens ženklavimo technologijos atlieka operacijas transformacijų srityje. Diskreti kosinuso transformacija (angl. *Discrete Cosine Transform*) ir diskreti bangelių transformacija (angl. *Discrete Wavelet Transform*) yra tik keletas iš transformacijų srities metodų, kurie gali būti taikomi. Naudojant vandens ženklavimo transformacijų technologijas, duomenys įterpiami į nešančiojo signalo transformuotas dalis. Šiais metodais pateikiama papildoma signalo informacija.

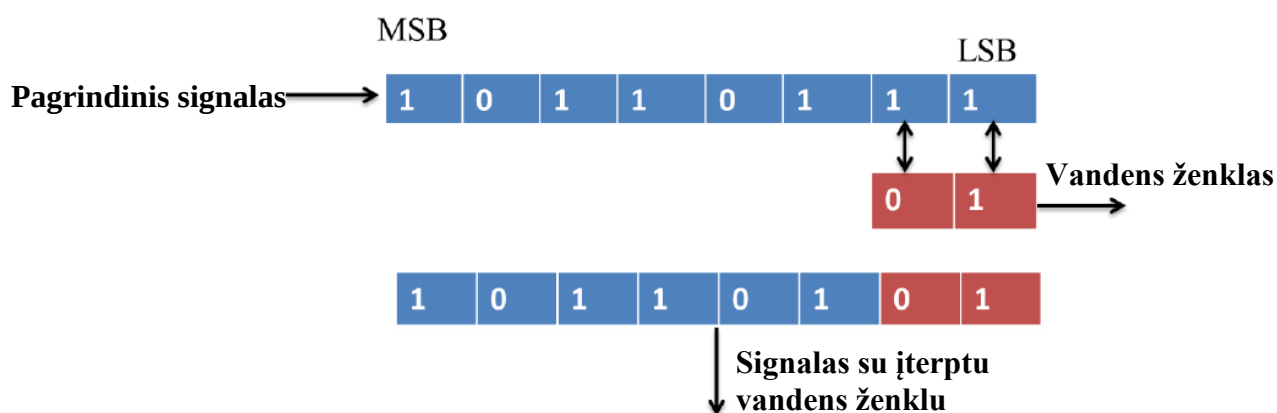
Iš esmės laiko srities metodai prasčiausiai apsaugo garso įrašą, nuo vandens ženklo pašalinimo. Net pats paprasčiausiai žemų dažnių filtras gali pašalinti tokiu būdu įterptą vandens ženklą, todėl šios apsaugos priemonės yra nerekomenduotinos autorių teisių apsaugai, bet gali būti naudojamos tapatybės patvirtinimui ar medicinai skirtose aplikacijose.

Vandens ženklo įterpimo metodai gali būti skirstomi į matomus ir nematomus. Šiame skyriuje mes aptarsime tipinius garso įrašo vandens ženklavimo metodus: mažiausiai svarbaus bito (angl. *Least Significant Bit*), išplėsto spektro (angl. *Spread Spectrum technique*), mišinio (angl. *Patchwork technique*), kvantavimo moduliacijos (angl. *Quantization Index Modulation*), fazės moduliacijos (angl. *Phase modulation*), aidų slėpimo (angl. *Echo hiding*).

2.1. Mažiausiai svarbaus bito metodas

Viena iš pirmųjų sukurtų ženklavimo vandens ženklais technologijų skirta praktiškai visiems masinės informacijos (angl. *media*) tipams yra vadinama mažiausiai svarbaus bito kodavimu arba sutrumpintai (angl. *LSB*) [31]. Jos esmė yra mažiausiai svarbius garso signalo bitus pakeisti kitais, kurie ir žymi garso įrašo autentiškumą. Naudojant LSB kodavimą, informacija įkeliami į bitą, kuris yra intervale nuo 1 MSB (angl. *Most Significant Bit*) iki 16 LSB (angl. *Least Significant Bit*). Pagrindinis šio metodo privalumas yra jo veikimo sparta. Labai greitai gali būti aptikti ir atpažinti slepiami identifikacijos bitai, nes yra tiksliai žinoma jų vieta. Techniškai šis metodas laikomas daugiau duomenų slėpimo, negu vandens ženklavimo algoritmu.

Iškodavimas paprasčiausiai vykdomas paimant reikšmes iš žinomų garso įrašo vietų ir analizuojant pasirinktą bitą. Mažiausiai svarbaus bito metodo taikymo schemą matome 2.1 paveiksle.

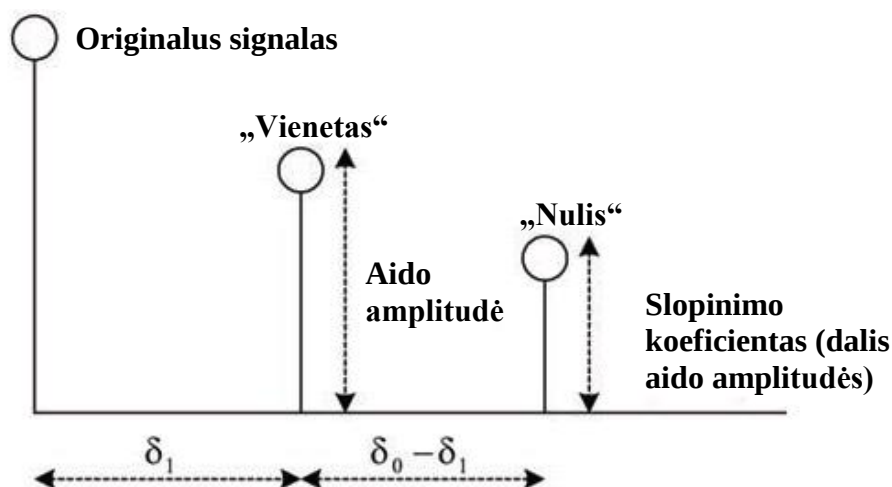


2.1 pav. LSB metodo veikimo schema [4]

2.2. Aido slėpimo metodas

Aido slėpimo metodą sukūrė Gruhl Lu Benderin. Jis pasiūlė koduoti failus pridėdam mažą, nepastebimą aidą [32]. Metodas įgyvendinamas sutapdinant aido branduolį su originalaus garso signalo branduoliu. Aido slėpimo algoritmas yra aklo vandens ženklavimo algoritmas sukurtas specialiai garso signalams. Jis labiausiai atsparus standartinėms prieš vandens ženklus nukreiptoms atakoms.

Naudojant aido slėpimo metodą, pridėjus aidą, garso signalas išlaiko tas pačias statistines ir suvokimo charakteristikas. Vėlavimas tarp originalaus ir paženklinto signalo yra labai mažas, kad jį atskirtų žmogaus ausis. Keturi pagrindiniai parametrai: signalo amplitudė, slopinimo koeficientas, „vienetas“ ir „nulis“ pateikti 2.2 paveiksle.



2.2 pav. Vandens ženklavimo metodo naudojant aido įterpimą parametrai [10]

Vandens ženklavimo procesas gali būti apibūdintas kaip sistema turinti vieną iš dviejų galimų sistemos funkcijų. Laiko ašyje sistemos funkcijos yra diskretaus eksponentinės diskretaus laiko. Jos skiriasi vėlavimu tarp impulsų. Apdorojant pagrindinį signalą per bet kurį branduolį esantį 2.2 pav. bus gaunamas koduotas signalas. Vėlavimas tarp originalaus ir apdoroto signalo priklauso nuo branduolio, kurį naudosime: δ_1 - jei naudosime „Vienetas“ ir δ_0 - jei naudosime „Nulis“ branduolį. Pagrindinis signalas yra skaidomas į mažas dalis norint užkoduoti daugiau negu vieną bitą. Kiekviena atskira dalis gali būti interpretuojama kaip nepriklausomas signalas ir norimas aidas (pasirinktas bitas) gali būti įterpiamas į jį atskirai.

Galutinis paženklintas vandens ženklų garso signalas yra sudaromas iš nepriklausomų užkoduotų signalo dalių. Sklandus perėjimas tarp koduotų signalo dalių turėtų būti reguliuojamas naudojant skirtingus metodus, taip apsaugant bendrą signalą nuo pakitimų dėl rezonanso. Aidas į originalų garso signalą įterpiamas naudojant vieną arba du vėlinimo branduolius, todėl norint gauti užkoduotą informaciją, reikia nustatyti tarpus tarp vietų, kuriose įterptas aidas. Užšifruoto signalo amplitudė lygi:

$$F^{-1}\{\log(|F(x)|^2)\}. \quad (2.1)$$

Čia F - Furje transformacija, F^{-1} - atvirkštinė Furje transformacija. Ji gali būti skaičiuojama dviejose vietose priklausomai nuo vėlinimų, branduoliuose: „Vienetas“ ir „Nulis“. Jeigu gautas rezultatas didesnis srityje δ_1 negu δ_0 , tada įterptas bitas iškoduojamas kaip „Vienetas“. Kuomet daugybė aidų bitų įterpta, randamos visos viršūnės gautos atvirkštine Furje transformacija. Tuomet suskaičiuojamas viršūnių skaičius priklausomai nuo vėlinimo „Vienetas“ ir „Nulis“ vietų, branduoliai tuomet suskaičiuojami ir palyginami. Jeigu randama daugiausiai viršūnių vėlinimo vietose su „Vieneto“ aidų branduoliu, tada vandens ženklas iškoduojamas kaip „Vienetas“.

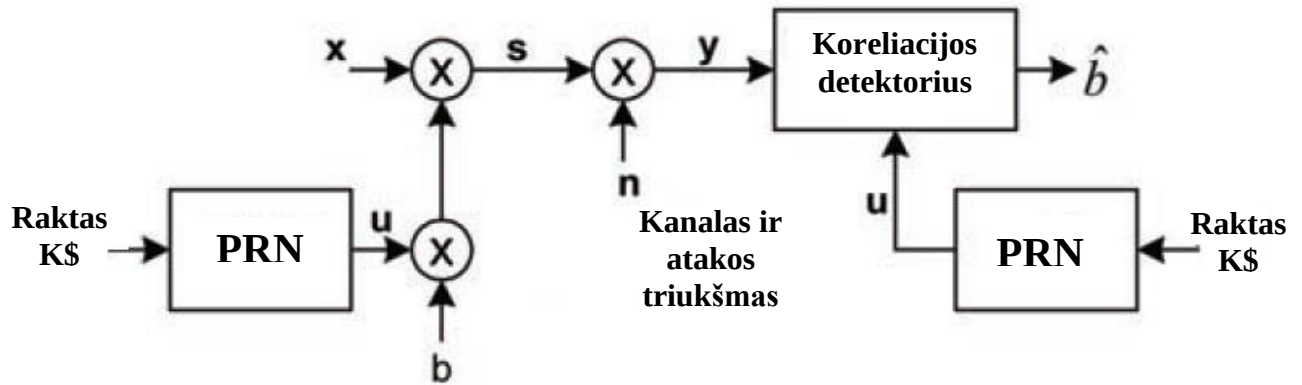
Norint padidinti vandens ženklo atsparumą modifikacijoms reikia naudoti „didelės energijos“ aidą, tačiau jį įterpus galimi dideli garso iškraipymai. Norint pasiekti optimalų variantą reikia rasti tinkamą aidą, kuris per daug neiškraipytų garso signalo. Egzistuoja keletas aidų slėpimo metodo patobulinimų. 1999 metais sukurtas keleto aidų įterpimo algoritmas, siekiant sumažinti trečiųjų šalių galimybę aptikti aidą [33].

2.3. Išplėsto spektro metodas

Išplėsto spektro metodas (angl. *Spread Spectrum Technique* arba *SS*) yra vienas dažniausiai naudojamų nuo pat vandens ženklų sąvokos atsiradimo. SS seka gali būti pridėta originalaus garso signalo dalims laiko srityje. Jeigu įterpimas vyksta transformacijų srityje, tuomet tai turi būti srityje, kuri atspari įvairioms modifikacijoms. SS metodu įterptas vandens ženklas atsparus amplitudės suspaudimui, garso formato keitimui, žemų dažnių filtravimui ir kitiems įprastiems signalų

apdorojimo metodams. SS metodo esmė yra ta, kad po tam tikros transformacijos, siekiant panaikinti vandens ženklą, garso įrašo kokybė labai suprastėja. Dėl šios priežasties išplėsto spektro metodas yra labai atsparus apdorojimui, jis yra nematomo vandens ženklinimo būdas, kurio vandens ženklo bitų dažnis nuo keleto iki dešimčių bitų per sekundę [3].

Vandens ženklas yra išskleidžiamas į didelį kiekį koeficientų ir iškraipymai išlieka nepastebimi, nes naudojami specialūs maskavimo efektai, pritaikyti slėpti garsus nuo žmogaus ausies. Kiekvieną koeficientą galima pakeisti tik labai mažai, kad jo nepastebėtų specialus koreliacijos detektorius, kuris yra labai jautrus net pačiam mažiausiam triukšmui. Pakeitimai gali būti pastebėti vėl sutraukiant koeficientus į vieną signalą. Pagrindinė išplėsto spektro metodo veikimo schema parodyta 2.3 paveiksle.



2.3 pav. Išplėsto spektro metodo veikimo schema [3]

Vektorius $\mathbf{x}$ yra originalus signalas jau atitinkamoje transformacijos srityje. Vektorius $\mathbf{y}$ yra po transformacijos srities kanalo iškraipymų gautas vektorius. Slaptą raktą $K\$$ naudoja atsitiktinių skaičių generatorius (angl. *Pseudo random number generator arba PRN*). Jis gamina plintančią seką $\mathbf{u}$ su nuline reikšme, kurios elementai yra lygūs $+\sigma_u$ arba $-\sigma_u$. Tada seka $\mathbf{u}$ pridedama arba atimama iš signalo $\mathbf{x}$. Visa tai priklauso nuo kintamojo $\mathbf{b}$ reikšmės, ten kur jis lygus $+1$ arba -1 . Signalas $\mathbf{s}$ yra jau paženklintas originalus garso įrašo signalas. Paprasta SS metodo analizė veda link klaidos apskaičiavimo tikimybės formulės:

$$\langle \mathbf{x}, \mathbf{u} \rangle = \sum_{i=0}^{N-1} X_i U_i \quad \text{ir} \quad \|\mathbf{x}\| = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle}; \quad (2.2)$$

čia N yra vektorių $\mathbf{x}, \mathbf{s}, \mathbf{u}, \mathbf{n}$ ir $\mathbf{y}$ ilgis pavaizduotas 3.3 pav. Be esmės praradimo mes pridedame vieną informacijos bitą į vektorių $\mathbf{s}$. Šį bitą apibūdina kintamasis $\mathbf{b}$, kurio reikšmė gali būti $+1$ arba -1 .

$$\mathbf{s} = \mathbf{x} + \mathbf{b}\mathbf{u}. \quad (2.3)$$

Vandens ženklą pažymėto signalo iškraipymai apibūdinami $\|\mathbf{s} - \mathbf{x}\|$. Lengva pamatyti, kad ženklinimo lygčiai mes turime:

$$D = \|\mathbf{b}\mathbf{u}\| = \|\mathbf{u}\| = \sigma_u. \quad (2.4)$$

Kanalas yra modeliuojamas kaip adityvus triukšmas $\mathbf{y}=\mathbf{s}+\mathbf{n}$ ir vandens ženklas išgaunamas įprastai skaičiuojant normalizuotą statistinį faktą r :

$$r = \frac{\langle \mathbf{y}, \mathbf{u} \rangle}{\langle \mathbf{u}, \mathbf{u} \rangle} = \frac{\langle b\mathbf{u} + \mathbf{x} + \mathbf{n}, \mathbf{u} \rangle}{\sigma_u^2} = b + x + n. \quad (2.5)$$

Pridėtą bitą įvertiname kaip $\hat{b} = \text{sign}(r)$, kur $x = \langle \mathbf{x}, \mathbf{u} \rangle / \|\mathbf{u}\|$ ir $n = \langle \mathbf{n}, \mathbf{u} \rangle / \|\mathbf{u}\|$

Paprasti statistiniai modeliai originaliam garso signalui $\mathbf{x}$ ir atakos triukšmui $\mathbf{n}$ yra priimtini. Abu vektoriai modeliuojami kaip nekoreliuoti Gauso atsitiktiniai įvykiai:

$$x_i \approx N(0, \sigma_x^2) \text{ ir } n_i \approx N(0, \sigma_n^2). \quad (2.6)$$

Tada lengva parodyti, kad statistinis kintamasis r taip pat Gauso kintamasis:

$$r \approx N(m_r, \sigma_r^2), \quad m_r = E[r] = b\sigma_r^2 = \frac{\sigma_x^2 + \sigma_n^2}{N\sigma_u^2}. \quad (2.7)$$

2.4. Mišinio metodas

Duomenys, kurie žymimi vandens ženklu, išskaidomi į du skirtingus poaibius. Viena duomenų savybė pasirenkama ir modifikuojama priešingomis kryptimis abiejuose poaibiuose [4]. Pavyzdžiui originalų signalą suskaidome į dvi dalis A ir B, tada A dalis padidinama per dydį Δ ir B dalis sumažinama per dydį Δ . Šių dviejų dalių atskyrimas ir yra slaptas raktas, kuris dar vadinamas vandens ženklo raktu. Vandens ženklo aptikimas vykdomas sekant statistines garso signalo savybes. Tarkim N_A ir N_B atspindi signalo A ir B dalis, o Δ bus pakeitimas padarytas originaliam signalui. Manykime, kad $a[i]$ ir $b[i]$ aprašo dalių vertes i_{th} pozicijoje blokuose A ir B. Skirtumas tarp dalių reikšmių gali būti aprašytas kaip [4]:

$$S = \frac{1}{N_A} \sum_{N_A} a[i] - \frac{1}{N_B} \sum_{N_B} b[i] = \frac{1}{N} \sum_N (a[i] - b[i]); \quad (2.8)$$

$$N_A = N_B = N. \quad (2.9)$$

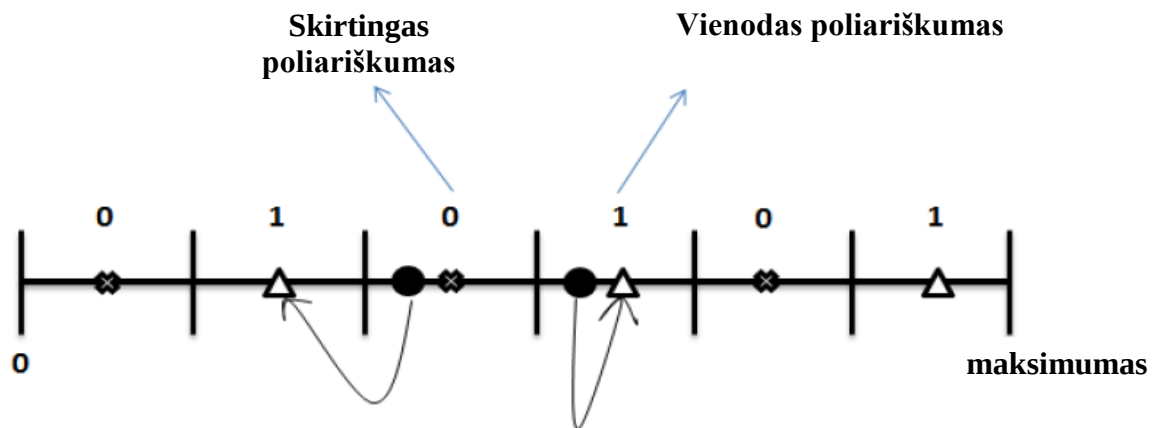
Skirtumo laukimas naudojamas išreikšti vandens ženklą, kurį apibūdina:

$$E\{S\} = \begin{cases} 2\Delta; & \text{vietai su vandens ženklu} \\ 0; & \text{vietai be vandens ženklo} \end{cases}. \quad (2.10)$$

2.5. Kvantavimo indekso moduliacija

Kvantavimo indekso moduliacija (angl. *Quantization Index Modulation* arba *QIM*) – metodas pridedantis vandens ženklą naudojant pavyzdžių (angl. *sample*) kvantavimą. Šio metodo esmė yra surasti didžiausią pavyzdžio reikšmę ir padalinti intervalą nuo 0 iki maksimalios reikšmės į intervalus, kurių žingsnio dydis Δ [5]. Intervalams priskiriama 0 arba 1 reikšmė, priklausimai nuo bet kurios atsitiktinės sekos. Kiekvienas pavyzdys turi kvantuotą reikšmę, poliariškumas priskiriamas priklausomai nuo intervalo vietos. Vandens ženklas pridedamas pakeičiant sukurto

intervalo medianą, taip pat priklauso nuo poliariškumų panašumo ir vandens ženklo bito. Norint pridėti to pačio poliariškumo bitą, mediana perkeliama į tokį patį intervalą, kaip parodyta dešiniu juodu tašku 2.4 paveikslėlyje.



2.4 pav. Pavyzdžių modifikacija naudojant QIM [5]

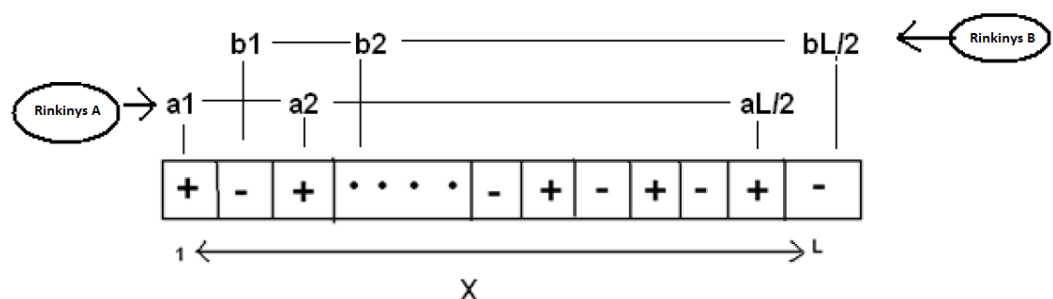
Jeigu vandens ženklo bitas ir poliariškumas yra skirtingi, tada pavyzdys perkeliamas į arčiausio kaimyninio intervalo centrą, kaip parodyta su kairiuoju juodu tašku 2.4 paveiksle. Kvantuotas pavyzdys gali būti išreikštas, kaip parodyta lygtyje apačioje.

$$Q(x) = x \pm \Delta; \quad (2.11)$$

čia x - originalaus signalo dalies vertė, $Q(x)$ - kvantuoto signalo dalies vertė, $\pm\Delta$ - kvantavimo paklaida.

2.6. Alfa „ α “ statistinė moduliacija

Duotai sekai X , kurios ilgis L gali būti suformuotos dvi skirtingos duomenų sekos A ir B , taip kaip pavaizduota 2.5 paveiksle. Poaibis $A = \{a_1, a_2, \dots, a_{L/2}\}$ susideda iš pavyzdžių pažymėtų „+“ ženklu, o kitas poaibis $B = \{b_1, b_2, \dots, b_{L/2}\}$, kuriame yra pavyzdžiai su ženklu „-“.



2.5 pav. „ α “ poabių skirtumo šablonas[21]

Kiekvienas rinkinys turi $L/2$ koeficientų. Kiekvienai duotai sekai X , tvirta „ α “ statistika apibrėžiama kaip pavyzdžių porų skirtumų aritmetinis vidurkis:

$$\alpha = \frac{1}{L/2} \sum_{i=1}^{L/2} (a_i - b_i). \quad (2.12)$$

Dauguma α reikšmių yra artimos 0. Kadangi α reikšmė priklauso nuo visų pavyzdžių savybių pasirinktame garso kadre, tai jis yra atsparus atakoms, todėl galima pasirinkti šį α kaip patikimą kiekį informacijos bito įterpimui.

2.6.1. Vandens ženklų bito įterpimo strategija naudojant „ α “

Slenksčio riba „t“ pasirenkama priklausomai nuo „ α “ pasiskirstymo originaliame garso signalo [21].

1. Jeigu skirtumo reikšmė „ α “ patenka į apibrėžtą ribą, tada:
 - a) Jei turi būti įterpiamas bitas, kurio reikšmė „1“, tada „ α “ reikšmė paslenkama į dešinę, už ribos, taip pridodant nustatyto dydžio poslinkį „S“ kiekvienai pavyzdžio reikšmei iš rinkinio A ir atimant tą pačią „S“ reikšmę iš kiekvieno pavyzdžio reikšmės, esančios rinkinyje B.
 - b) Jei turi būti įterpiamas bitas, kurio reikšmė „0“, tada kadras laikomas nepalietas, pavyzdžiai modifikuojami tik tada, kai įterpiamas „1“, todėl pasiekiamas didelis slaptumas ir tikimybė, kad egzistuoja įterptas vandens ženklų bitas yra visada 0,5.
2. Jei skirtumo reikšmė „ α “ nepatenka į nustatytas ribas, neįterpiamas joks bitas ir „ α “ yra paslenkamas toli už ribos.

2.6.2. Vandens ženklų bito aptikimas naudojant „ α “

Imtuvo dalyje statistika „ α “ skaičiuojama įterptiems garso pavyzdžiams naudojant 2.12 lygtį [21]:

1. Jeigu „ α “ yra už nustatytos ribos, tada bitas lygus „1“. Jis nuskaitymas ir garso pavyzdžiai gali būti atstatyti į pradines originalias reikšmes atimant „S“ iš kiekvieno pavyzdžio reikšmės esančios rinkinyje A ir pridodant tą patį „S“ prie kiekvienos pavyzdžio reikšmės esančios rinkinyje B.
2. Jeigu skirtumo reikšmė „ α “ patenka į nustatytas ribas, tada vandens ženklų bitas bus lygus „0“. Kai tik bitas išskleidžiamas, pažymėtas garso įrašas gali būti atstatomas į originalų su minimaliais iškraipymais. Šis metodas yra neturintis nuostolių ir atvirkštinis.

2.7. Garso žymėjimo skaitmeniniu vandens ženklų metodų privalumai ir trūkumai

Pateikti garso įrašo skaitmeninio žymėjimo vandens ženklų metodai gali būti tinkamas būdas kovoti prieš autorių teisių pažeidimus skaitmeninėje erdvėje. Per pastarąjį dešimtmetį susidomėjimas garso apsaugos nuo plagijavimo priemonėmis labai sparčiai išaugo. Mokslininkai atliko daugybę tyrimų šioje srityje ir tai prisidėjo prie garso įrašų apsaugos progreso. Buvo

pristatytas keletas labai svarbių metodų, kurie padėjo tvirtus pagrindus tolesniam skaitmeninio žymėjimo vandens ženklų tobulinimui.

Mažiausiai svarbaus bito (angl. *Least Significant Bit*) metodas pasižymi savo didele sparta. Jį naudojant galima iškoduoti bitus, kurie slepiami garso įrašė, tačiau šis metodas daugiau laikomas informacijos slėpimo negu autentiškumo patvirtinimo technika, nes vandens ženklą, kuris įterptas laiko srityje pašalinti nėra sudėtinga [31].

Aido slėpimo (angl. *Echo hiding*) metodas reikalauja daug kompiuterio resursų, o vandens ženklo nuskaitymo procesas užima daug laiko. Aidas dažniausiai įterpiamas taip, kad jis yra praktiškai negirdimas, kartais net praturtina garsą, bet šis metodas nėra nematomas, juk aidą praktiškai gali pastebėti žmogus analizuojantis garso įrašą, nes jis nėra niekaip kitaip paslėptas. Aido slėpimo metodas taip pat yra neatsparus su garso apdorojimu susijusioms atakoms [32].

Išplėsto spektro (angl. *Spread Spectrum*) metodui reikalinga psicho – akustinė adaptacija, norint įterpti negirdimą triukšmą. Ji užima gana daug laiko, tačiau daugelis ženklinimo skaitmeniniu vandens ženklų metodų reikalauja psicho – akustinio modeliavimo siekiant įterpti negirdimą vandenženklį. Dar vienas trūkumas yra sudėtingas šio metodo sinchronizavimas. Nepaisant šių dalykų, išplėsto spektro metodas garantuoja gerą vandens ženklo atsparumą įvairių tipų atakoms prieš garso įrašą: amplitudės suspaudimui, garso formato keitimui, žemų dažnių filtravimui ir t.t [3].

Mišinio (angl. *Patchwork*) metodas užtikrina tvirtą ir negirdimą garso įrašo žymėjimą vandens ženklu. Tam jis naudoja slaptą raktą, kurį nustato pagal garso segmento dydį, tačiau taip pat nėra atsparus desinchronizacijos atakoms [4].

Kvantavimo indekso moduliacija (angl. *Quantization Index Modulation*) metodas išsiskiria tuo, kad jis atsparus laiko skalės modifikacijai, juo naudojantis pačiam galima reguliuoti santykį tarp vandens ženklo tvirtumo ir garso įrašo kokybės tiesiog modifikuojant kvantavimo indeksą. Didinant indekso reikšmę prarandama kokybė, tačiau laimimas vandens ženklo tvirtumas. Mažinant indekso reikšmę – atvirkščiai. Šio metodo pagrindinė savybė yra kokybės ir tvirtumo balansas [5].

Alfa „ α “ statistinės moduliacijos (angl. *Alpha Statistic Modulation*) metodas išsiskiria tuo, kad jis gali būti naudojamas atvirkštiniu būdu. Įprastai – įterpti ir nuskaityti vandens ženklus, priešingu atveju - surasti, ištrinti žymenį ir atstatyti beveik nepakitusį pradinį garsą [21].

3. BINARINIO VAIZDO ĮTERPIMO Į GARSO ĮRAŠĄ ALGORITMAI

Daugybė efektyvių algoritmų yra pristatyta ir pritaikyta nuotraukų bei vaizdo įrašų apdorojimui, tačiau garso signalo žymėjimui vandens ženklais yra vos keletas. Taip yra todėl, kad žmogaus klausos sistema yra gerokai sudėtingesnė ir jautresnė negu regos. Šiame skyriuje išanalizuosime kitų mokslininkų pristatomus algoritmus bei juos palyginsime tarpusavyje. Magistrinio darbo tikslas yra pagal jau ištirtus ir anksčiau pristatytus garso vandens ženklinimo algoritmus surasti optimaliausią ir atspariausią išoriniam apdorojimui bei pagal išanalizuotus pavyzdžius sudaryti savąjį binarinio paveikslėlio įterpimo į garso įrašą algoritmą.

3.1. Algoritmuose naudojama metodika bei jų vertinimo kriterijai

Šiame poskyryje aprašomi dažniausiai garsų ženklinimui binariniu atvaizdu naudojami metodai, būdai, taip pat kriterijai kuriais galima įvertinti algoritmo vandens ženklo savybes. Taikant įvardintus kriterijus bus pasirinktas optimalus garso žymėjimo metodas.

3.1.1. Paveikslėlio užšifravimas naudojant Arnoldo transformaciją

Arnoldo transformacija (angl. *Arnold transform*) yra skirta binarinio atvaizdo vandens ženklo užšifravimui. Net iš garso įrašo perskaičius tokį žymenį jis tampa nebeatpažįstamas. Arnoldo transformacijos veikimo principas: skaitmeninė nuotrauka gali būti laikoma dviejų kintamųjų funkcija $f(x,y)$ plokštumoje Z . Ši funkcija aprašoma kaip $Z = f(x,y)$ kur $x,y \in \{0,1,2,3...N-1\}$. Reiškia N apibūdina skaitmeninės nuotraukos eiliškumą. Paveikslėlio taškų matricą galima pakeisti naudojant Arnoldo transformaciją, kuri ją užšifruoja ir taip garantuojamas geresnis saugumas [13]. Ši transformacija keičia tašką $point(x,y)$ į naują tašką $point(x',y')$ naudojant 3.1 ir 3.2 lygtis.

$$x' = (x+y) \bmod N; \quad (3.1)$$

$$y' = (x+2y) \bmod N. \quad (3.2)$$

Jeigu originalus paveikslukas užšifruotas keletą kartų, tai norint gauti jo pradinę matricą reikia tiek pat kartų taikyti atvirkštinę Arnoldo transformaciją.

3.1.2. Diskrečioji bangelių transformacija

Bangelės yra specialios funkcijos, kurios apibūdinant signalus analoginėje formoje naudojamos kaip bazinės. Jos teikia galingą įvairios skiriamosios gebos įrankį skirtą nestacionarių signalų su gera laiko lokalizacijos informacija analizei. Reikalingi diskrečiosios bangelių transformacijos (angl. *discrete wavelet transformation*) koeficientai gali būti paskaičiuojami reikursyviai naudojant gerai žinomą Malato piramidės algoritmą. Pagal jį vienos dimensijos diskretieji bangelių koeficientai gali būti apskaičiuojami naudojant formules:

$$WL(n, j) = \sum_m WL(m, j - 1)h_0(m - 2n); \quad (3.3)$$

$$WH(n, j) = \sum_m WL(m, j - 1)h_1(m - 2n); \quad (3.4)$$

čia $WL(n, j)$ - n -tasis mastelio koeficientas j -tajame etape, $WH(n, j)$ - n -tasis bangelių koeficientas j -tajame etape, $h_0(n)$ ir $h_1(n)$ - išsiplėtimo koeficientai paeiliui atitinkantys mastelio ir bangelių funkcijas. Norint pakeisti originalius duomenis, diskrečios bangelių transformacijos koeficientai yra apdorojami papildomu rinkiniu žemų ir aukštų dažnių filtrų, kurie išreiškiami:

$$WL(n, j) = \sum_k WL(k, j + 1)g_0(n - 2k) + \sum_l WH(l, j + 1)g_1(n - 2l); \quad (3.5)$$

čia $g_0(n)$ ir $g_1(n)$ - žemų dažnių ir aukštų dažnių sintezės filtrai atitinkantys pagrindinę bangelę. Iš 3.5 lygties pastebėta, kad j -tuosius koeficientus galima gauti iš $(j+1)$ -ojo lygio koeficientų.

Dėl puikių erdvės dažnio lokalizacijos savybių, DWT labai puikiai tinka rasti vietas, kur vandens ženklas gali būti įterptas efektyviai.

3.1.3. Algoritmo testavimo vertinimo kriterijai

- a) Normalizuota koreliacija (*angl. Normalized correlation* arba *NC*) yra naudojama tikrinti vandens ženklo tvirtumui, arba kitaip tikrinamas panašumas tarp pradinio ir nuskaityto iš garso įrašo vandens ženklų [11]. Normalizuota koreliacija randama pagal formulę:

$$NC(W, W') = \frac{\sum_{i=1}^M \sum_{j=1}^M W(i, j)W'(i, j)}{\sum_{i=1}^M \sum_{j=1}^M W(i, j)W(i, j)}, \quad (3.6)$$

čia $W(i, j)$ – originalaus vandens ženklo bitas, $W'(i, j)$ – nuskaityto vandens ženklo bitas.

- b) Bitų klaidos norma (*angl. Bit error rate* arba *BER*) yra naudojama skaičiuoti panašumui tarp originalaus bei nuskaityto vandens ženklų. Ji skaičiuojama visas bitų klaidas dalijant iš visų vandens ženklo bitų skaičiaus [12]. Bitų klaidos norma randama pagal formulę:

$$BER = \frac{\sum_{i=1}^M \sum_{j=1}^M W(i, j) \oplus W'(i, j)}{M \times M}; \quad (3.7)$$

čia $\oplus$ - sudėtis modulių 2, $M \times M$ - vandens ženklo bitų skaičius.

- c) Signalo ir triukšmo santykis (*angl. Signal to noise ratio* arba *SNR*) yra įvertis apibūdinantis vandens ženklinimo algoritmo negirdimumo savybes. Signalo ir triukšmo santykis skaičiuojamas pagal formulę:

$$SNR = 10 \log_{10} \frac{\sum_{i=1}^L X(i)^2}{\sum_{i=1}^L (X(i) - \bar{X})^2}; \quad (3.8)$$

čia X ir $\bar{X}$ - atitinkamai originalus ir paženklintas vandens ženklų garso signalai, i - garso signalo indeksas, L - garso kadrų (*angl. samples*) skaičius.

- d) Objektivus skirtumo įvertinimas (*angl. Objective difference grade* arba *ODG*) [8] yra objektivus matmuo, kuris rodo skirtumą tarp garso įrašų, kitaip – vandens ženklinimo algoritmo kokybę ir slaptumą. Šis įvertis buvo sugalvotas tuomet, kai buvo pastebėta jog

kiekvieną kartą organizuoti garso kokybės tikrinimą kviečiant atskirus klausytojus yra tiesiog per brangu ir užima daug laiko. Objektyvaus skirtumo įvertinimo algoritmas buvo sukurtas pagal subjektyvius klausymo testus, kurie ir yra modeliuojami skaičiavimais. Atliekant realų klausymo testą perklausai skiriami trys garso įrašai. A – pateikiamas originalus garso signalas, B ir C atitinkamai sumaišyti originalus ir vandens ženklų pažymėtas garsas. Klausytojas visada gali paklausti originalaus įrašo ir lyginimo metodu turi atpažinti, kuris iš jų yra modifikuotas. Atpažinus jis turi įvertinti kokybę balais, pagal pateiktą 3.1 lentelę.

3.1 lentelė Objektyvaus kokybės įvertinimo kriterijai [8]

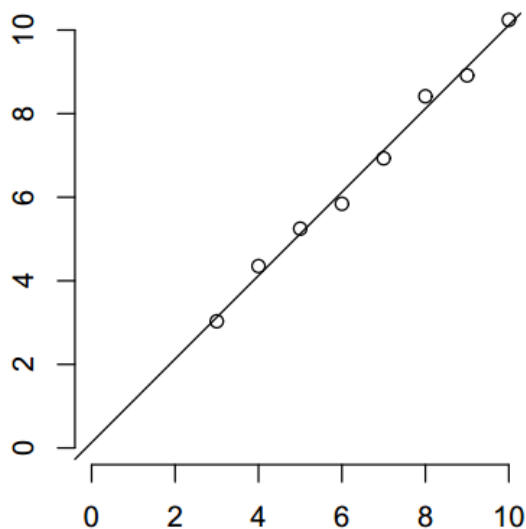
Įvertinimas	Apibūdinimas	Kokybė
0,00	Nepastebimas	Puiki
-1,00	Pastebimas, bet neerzinantis	Gera
-2,00	Šiek tiek erzinantis	Nebloga
-3,00	Erzinantis	Prasta
-4,00	Labai erzinantis	Labai bloga

Susumavus visų klausytojų pateiktus rezultatus gaunamas subjektyvus skirtumo įvertinimas (angl. *Subjective Difference Grade*). O jis modeliuojamas programine įranga ir labai panašūs rezultatai gaunami kompiuteriu. Tokiems skaičiavimams bus naudojama jau sukurta programinė įranga pritaikyta Matlab 2013a programiniam paketui - „PQevalAudio“.

3.1.4. Vienetinės vertės išskyrimas

Vienetinės vertės išskyrimas (angl. *Singular Value Decomposition* arba *SVD*) gali būti vertinamas trimis aspektais. Vienu atveju tai metodas, kuris transformuoja koreliuojančius kintamuosius į nebekoreliuojančius, tačiau geriau atspindinčius įvairius ryšius tarp originalių duomenų. SVD taip pat yra metodas skirtas identifikuoti pagrindinius taškus aplink kuriuos išsidėsto duomenys. Vienetinės vertės išskyrimas taip pat laikomas būdu rasti geriausią daugelio duomenų išreiškimą su gerokai mažesniu duomenų rodiklių skaičiumi. SVD yra duomenų kiekio sumažinimo metodas [34].

3.1 paveikslas iliustruoja SVD veikimo principą. Dviejų dimensijų duomenų taškai išreiškiami geriausia originalių duomenų aproksimacija naudojant 1 dimensijos objektą – tiesę. Jeigu iš kiekvieno duomenų taško būtų nubrėžta statmena linija į regresijos tiesę, tai jų susikirtimo taškas būtų laikomas originalaus taško aproksimacija, taip būtų supaprastintas originalių duomenų atvaizdavimas. SVD praktiškas tuomet, kai naudojami dideli duomenų kiekiai ir svarbus jų tarpusavio ryšys.



3.1 pav. Duomenų dimensijų sumažinimas iš 2 į 1 naudojant vienetinės vertės išskyrimą [34]

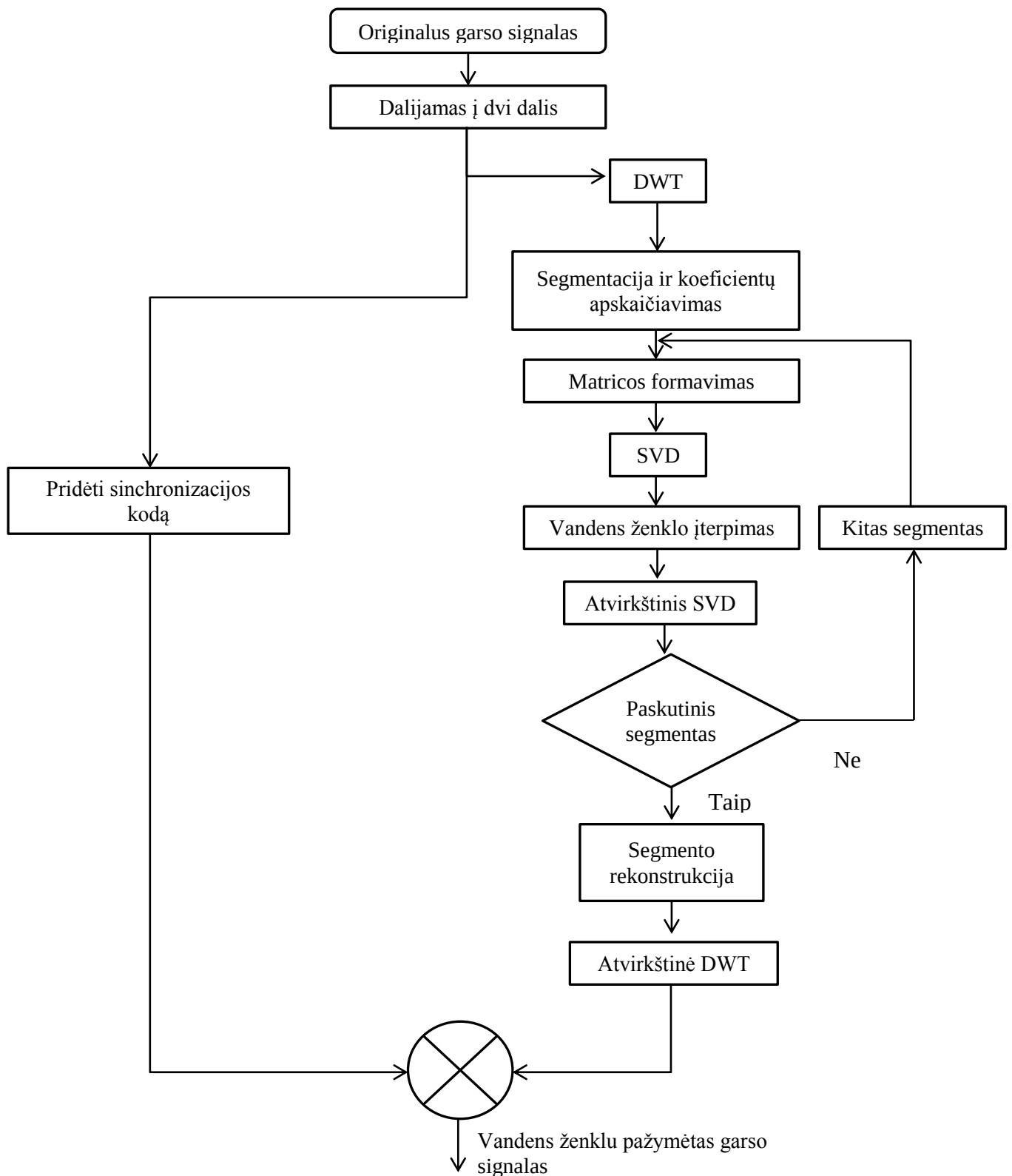
3.2. Adaptyvus garso ženklavimas išskiriant vieną reikšmę iš bangelių srities

Šiame poskyryje aprašomas garso įrašo ženklavimo binariniu atvaizdu algoritmas, kuris yra saugus, atsparus apdorojimui bei nepastebimas. Jo esmė yra vienos reikšmės išskleidimas diskrečios bangelių transformacijos srityje naudojant sinchronizacijos kodą.

3.2.1. Vandens ženklų įterpimo algoritmas

Pasaulyje sukurti vos keli garso įrašo ženklavimo vandens ženklų algoritmai, kurie naudoja sinchronizacijos kodą. Pagrindinis jų trūkumas yra atakos, kurios pažeidžia garso įrašo nustatytą sinchroniškumą. Signalo iškarpymas, paslinkimas ir panašūs poveikis gali turėti didelę žalą sinchroniškumo nustatymui ir vandens ženklas tampa neatkuriamas. Kuriant naują garso įrašo ženklavimo algoritmą buvo nutarta sinchronizacijos kodą susieti su pačiu vandens ženklų. Sinchronizacijos duomenys įterpiami prieš vandens ženklą, taip galime nustatyti tikslią garso įrašo vietą, kurioje slepiamas vandens ženklas.

Paaškinamas 3.2 paveiksle pateiktas binarinio atvaizdo vandens ženklų įterpimo algoritmas. Visas nešantysis garso signalas yra X . Jis suskaidomas į P segmentų, kurie turi dar po n skaičių garso reikšmių. Kiekvienas sinchronizacijos kodo bitas įterpiamas į kiekvieną garso įrašo segmentą. Norint vėl išgauti įterptą sinchronizavimo kodą, pirmiausiai garso įrašas paverčiamas į segmentus kaip ir įterpimo procese. Kiekvieno iš jų reikšmė apskaičiuojama. Jeigu gautoji reikšmė didesnė negu nulis, reiškia teigiamas bitas „1“ yra aptiktas.. Jei segmento reikšmė mažesnė už nulį, tai aptiktas bitas „0“.



3.2 pav. Vandens ženklo pridėjimo algoritmas naudojant adaptyvų vandens ženklavimo metodą

Vandens ženklo įterpimo procesas:

- Pirmo lygio skaitmeninė bangelių transformacija (angl. *Digital Wavelet Transformation* arba *DWT*) pritaikoma antrai garso įrašo daliai X_2 . Ji gaunama naudojant Haro bangelių filtrą.

- Gauti žemo dažnio bangelių koeficientai segmentuojami į 2-D matricos blokus. Kiekvienam blokui paskaičiuojama SVD.
- Kiekvienam blokui skaičiuojami reikalingi koeficientai: vektoriaus norma, standartinis nuokrypis.
- Norint padidinti tvirtumą ir sumažinti iškraipymus naudojamas adaptyvus kvantavimo žingsnio pasirinkimo metodas, kuris yra geresnis negu nustatyto kvanto žingsnio naudojimas.
- Kiekvienas vandens ženklų bitas $w(i,j)$ pridedamas naudojant kvantavimo indekso moduliaciją.
- Pritaikoma atvirkštinė SVD ir gaunama modifikuotų blokų matrica.
- Pertvarkomas garso signalas iš visų modifikuotų blokų $\tilde{D}_j$. Atliekama atvirkštinė DWT ir gaunamas paženklintas garso signalas $\tilde{X}$.

3.2.2. Vandens ženklų išgavimas

Norint surasti tikslią garso įrašo vandens ženklų vietą, pirmiausiai reikia iš garso signalo išgauti įterptą sinchronizavimo kodą. Šis metodas naudoja standartinę kadrų sinchronizacijos technologiją taikomą skaitmeninėms komunikacijoms.

Sinchronizacijos kodo paieška:

- Nustatomas gauto pradinio signalo indeksas.
- Išskleidžiama informacija įterpta pavyzdžiuose.
- Skaičiuojamas išskleisto ir originalaus sinchronizacijos kodo panašumas:

$$\rho(v, \tilde{v}) = \frac{\sum_{i=1}^p v(i)\tilde{v}(i)}{\sqrt{\sum_{i=1}^p v^2(i)}\sqrt{\sum_{i=1}^p \tilde{v}^2(i)}}; \quad (3.9)$$

Čia v ir $\tilde{v}$ - atitinkamai originalus ir išskleistas sinchronizavimo kodas. Jeigu tas santykis tarp šių dydžių yra lygus arba didesnis nustatytam jautrumui e , tada $\tilde{v}$ laikomas sinchronizacijos kodu ir praleidžiamas sekantis žingsnis.

Vandens ženklų nuskaitymas:

- Naudojant sinchronizacijos kodo paieškos metodą nustatoma vandens ženklų pažymėto garso įrašo pradžios pozicija (angl. *beginning position*).
- Pritaikoma pirmo lygio skaitmeninė bangelių transformacija naudojant Haaro bangelių filtrą garso įrašo daliai po pradinės pozicijos.
- Gauti žemo dažnio bangelių koeficientai segmentuojami į 2-D matricos blokus.
- Iš kiekvieno bloko nuskaityama po vandens ženklų bitą ir iš jų suformuojamas paveikslėlis.

3.2.3. Praktiniai rezultatai ir jų aptarimas

Klausymo testas:

Šis testas apibūdina žmogaus galimybę atskirti paženklintą vandens ženklų garso įrašą nuo originalaus. Kuo mažesnė atskyrimo galimybė, tuo ženklinimo metodas optimaliausias. Norint išbandyti pateiktą garso vandens ženklinimo algoritmą buvo pasitelktas dvejetainis testas. Paprastas žmogaus klausymo testas, bei signalo su triukšmu santykio (angl. *signal to noise ratio*) skaičiavimas. Vandens ženklui buvo naudojamas dvejetainis vandens ženklas pateiktas 3.3 paveiksle.



3.3 pav. Dvejetainis vandens ženklas [18]

3.2 lentelė Gauti klausymo testo rezultatai[18]

Muzikos stilius	SNR, dB	Vidutinis MOS
Klasikinė	26,84	4,6
Kantri	25,13	4,5
Bliuzas	23,01	4,4
Džiazas	24,76	4,5
Pop	22,11	4,3

Klausymo testo rezultatai buvo vertinami penkiabalėje sistemoje. 5 balai reiškia, kad vandens ženklo garsui padaryti pokyčiai negirdimi, o 1 – pašaliniai garsai labai erzinantys. Signalų ir triukšmo santykis skaičiuojamas pagal 3.8 formulę.

Gauti bandymo rezultatai pateikti 3.2 lentelėje. Signalų ir triukšmo santykiui viršijant 20 dB gautas rezultatas atitinka IFPI standartą. Kaip matome iš rezultatų lentelės visiems muzikos stiliams garso vandens ženklinimo algoritmas išskiriant vieną reikšmę iš bangelių srities viršijo 20 dB, taip pat iš klausymo testo rezultatų galima spręsti, kad paženklintas garso įrašas praktiškai neatskiriamas jį klausančiam žmogui.

Vandens ženklinimo tvirtumo testas:

Garso vandens ženklo tvirtumas, tai savybė būti atpažintam ir po įvairaus išorinio poveikio garso įrašui. Garso apdorojimo bandymai atlikti naudojant Adobe Audition 1.0 programinę įrangą.

Panaudoti bandymo metodai:

- Papildomas Baltasis Gauso triukšmas:** Baltasis Gauso triukšmas įterpiamas į garso įrašą tol, kol jo signalo su triukšmu santykis pasiekia 20 dB ribą.

- b) Diskretizacijos dažnio keitimas (angl. *resampling*):** garso signalo su įterptu vandens ženklų diskretizacijos dažnis yra 44,1 kHz, kuris keičiamas į 22,05 kHz ir vėliau dažnis atstatomas atgal į 44,1 kHz.
- c) Žemų dažnių filtravimas:** naudojamas antros eilės Butervorto (angl. *Butterworth*) filtras, kurio nukirtimo dažnis yra 11025 Hz.
- d) Perkvantavimas (angl. *Requantization*):** 16 bitų paženklintas vandens ženklų garso signalas kvantuojamas į 8 bitų signalą ir vėl gražinamas pradinis bitų skaičius.
- e) MP3 suspaudimas 64 kbps:** pritaikomas MPEG-1 trečio sluoksnio suspaudimas. Pažymėtas garso įrašas suspaudžiamas iki 64 kbps bitų dažnio, o tada išskleidžiamas atgal į WAVE formatą.
- f) MP3 suspaudimas 32 kbps:** pritaikoma MPEG-1 trečio sluoksnio suspaudimas. Pažymėtas garso įrašas suspaudžiamas iki 32 kbps bitų dažnio, o tada išskleidžiamas atgal į WAVE formatą.
- g) Iškarpymas:** iš garso įrašo pašalinami 5 segmentai turintys po 100 pavyzdžių (angl. *samples*) ir jie pakeičiami tokiais pačiais, tik paveiktas žemų dažnių filtravimo bei išorinio baltojo Gauso triukšmo.
- h) Aido pridėjimas:** pridedamas aidas su 98 ms vėlavimu bei 41% nykimu.
- i) Triukšmų šalinimas (angl. *Denoising*):** pažymėto garso įrašo triukšmai šalinami naudojant „Hiss removal“ funkciją programoje GoldWave.

Norint įvertinti skirtumus tarp originalaus garso įrašo pažymėto binarinio atvaizdo vandens ženklų bei tokio pat įrašo tik apdoroto paminėtais metodais, naudojamos dvi pagrindinės sąvokos: normalizuota koreliacija (angl. *normalized correlation*) iš 3.6 formulės bei bitų klaidų norma (angl. *bit error rate*) iš 3.7 formulės. Jeigu $NC(W, \tilde{W})$ yra artimas 1, tada W ir $\tilde{W}$ ir labai panašūs. Jei $NC(W, \tilde{W})$ yra artimas 0, tada panašumas tarp W ir $\tilde{W}$ labai mažas.

Bitų klaidų norma naudojama apibūdinti vandens ženklo klaidingų bitų dalį, po garso signalo apdorojimo operacijos. 3.3 ir 3.4 lentelėse reprezentuojami rezultatai, gauti atliekant garso vandens ženklo atsparumo testus naudojant aptartus apdorojimo metodus. Matoma, kad pasirinktas vandens ženklinimo algoritmas turi didelę normalizuotą koreliaciją ir mažus bitų klaidų lygius, tai aiškiai parodo, kad pasirinktas vienos reikšmės iš bangelių srities išskyrimo algoritmas puikiai veikia prieš įvairius garso apdorojimo metodus.

3.3 lentelė Džiazo garso įrašo pažymėto vandens ženklų apdorojimo rezultatai [18]

Atakos tipas	NC	BER, %	Nuskaitytas vandens ženklas
Jokios atakos	1	0	
Baltasis Gauso triukšmas	1	0	
Diskretizacijos dažnio keitimas	0,9854	2	
Žemų dažnių filtras	0,9993	0	
Perkvantavimas	1	0	
MP3 64 kbps	0,9980	0	
MP3 32 kbps	0,9907	1	
Aidas	0,9847	2	
Triukšmų filtravimas	0,9634	5	

3.3 lentelėje pateiktas džiazo garso įrašo pažymėto binarinio atvaizdo vandens ženklų, apdorojimo rezultatai. Iš jų matoma, kad neatlikus jokio garso signalo apdorojimo, pridėjus baltąjį Gauso triukšmą, nukirpus dalį signalo ar perkvantavus rezultatai išlieka tokie patys: normalizuota koreliacija lygi 1, o bitų klaidų norma yra 0, tai yra idealus atvejis. Atsiradus originalaus ir nuskaityto vandens ženklo nepanašumams, normalizuota koreliacija mažėja, o bitų klaidų norma didėja. Stebint kitus lentelėje pateiktus rezultatus matoma, kad atlikus garso signalo apdorojimą rezultatai išliko artimi idealiams. Didžiausi pakitimai fiksuojami šalinant triukšmus, kur NC = 0,9634, o BER = 5. Tačiau ir su tokiais gautais rezultatais binarinis atvaizdas nesunkiai atpažįstamas.

Iš garso vandens ženklo apdorojimo rezultatų pateiktų 3.4 lentelėje galima spręsti, kad dėl išorinio poveikio garso signalui, atsirandantys nesutapimai priklausomi ir nuo muzikos stiliaus.

Visumoje klaidų pasitaikė labai nedaug. Pats blogiausias rezultatas buvo klasikinės muzikos garso įrašui pridėjus aidą, tai yra $NC = 0,9442$, o $BER = 8$.

3.4 lentelė Įvairių muzikos stilių garso įrašų pažymėtų vandens ženklų apdorojimo rezultatai [18]

Muzikos stilius	Atakos tipas	NC	BER, %
Klasikinė	Jokios atakos	1	0
	Baltasis Gauso triukšmas	1	0
	Diskretizacijos dažnio keitimas	0,9974	0
	Žemų dažnių filtras	0,9987	0
	Perkvantavimas	1	0
	MP3 64 kbps	1	0
	MP3 32 kbps	1	0
	Aidas	0,9442	8
	Triukšmų filtravimas	1	0
Kantri	Jokios atakos	1	0
	Baltasis Gauso triukšmas	1	0
	Diskretizacijos dažnio keitimas	0,9947	1
	Žemų dažnių filtras	0,9980	0
	Perkvantavimas	1	0
	MP3 64 kbps	1	0
	MP3 32 kbps	0,9941	0
	Aidas	0,9934	1
	Triukšmų filtravimas	0,9974	0
Bliuzas	Jokios atakos	1	0
	Baltasis Gauso triukšmas	1	0
	Diskretizacijos dažnio keitimas	1	0
	Žemų dažnių filtras	1	0
	Perkvantavimas	1	0
	MP3 64 kbps	1	0
	MP3 32 kbps	0,9980	0
	Aidas	0,9907	1
	Triukšmų filtravimas	1	0
Pop	Jokios atakos	1	0
	Baltasis Gauso triukšmas	1	0
	Diskretizacijos dažnio keitimas	1	0
	Žemų dažnių filtras	1	0
	Perkvantavimas	1	0
	MP3 64 kbps	1	0
	MP3 32 kbps	1	0
	Aidas	0,9960	1
	Triukšmų filtravimas	1	0

Šiame poskyryje aptartas adaptyvus garso ženklinimo vandens ženklų algoritmas, kurio esmė vienos reikšmės gavimas iš bangelių srities naudojant sinchronizacijos kodą. Vandens ženklo duomenų bitai įterpiami į originalaus garso įrašo atskiras bangelių blokų reikšmes. Eksperimentų rezultatai parodo, kad pažymėti garso įrašai yra praktiškai neatskiriami nuo originalių juos atitinkančiųjų. Vandens ženklo aptikimas yra efektyvus ir nematomas, nors tam ir reikia kvantavimo parametrų, tačiau nebūtina turėti originalaus garso signalo. Pateiktas algoritmas yra labai atsparus MP3 suspaudimui, iškarpymui, žemų dažnių filtravimui, triukšmų pridėjimui, diskretizacijos dažnio keitimui, aidui.

3.3. Garso įrašo ženklėjimas binarinius atvaizdu naudojant diskrečiąją bangelių transformaciją

Šiame poskyryje aptariamas dar vienas garso vandens ženklėjimo algoritmas naudojantis diskrečiąją bangelių transformaciją. Toks transformavimas išskaido nešantįjį signalą į keletą skirtingų dalių ir taip suteikia galimybę algoritmo naudotojams atrasti labiausiai tinkamas garso signalo dalis ir į jas įterpti vandens ženklų bitus. Pateikiamame algoritme naudojama žemų dažnių garso įrašo dalis, kad atsparumas bei garso įrašo kokybė nenukentėtų.

3.3.1. Vandens ženklų įterpimas

Binarinio atvaizdo vandens ženklų įterpimo į garso įrašą procedūra susideda iš trijų pagrindinių operacijų: vandens ženklų pirminio apdorojimo, diskrečiąjai bangelių transformacijai reikalingo garso signalo dažnio išskyrimo ir vandens ženklų įterpimo į garso signalo koeficientus, kurie gauti atlikus DWT. Visa tai galima suskaidyti į šiuos žingsnius:

- Nespalvotas vandens ženklui naudojamas paveikslėlis išreiškiamas kaip dviejų dimensijų matrica, kurios dydis $M1 \times M2$
- Dviejų dimensijų paveikslėlio matrica yra konvertuojama į viendimensį vektorius W , kurio ilgis $M1 \times M2$.
- Atliekama vienos dimensijos vektoriaus W normalizacija dalinant kiekvieną elementą iš 255.
- Kairiajam stereo garso įrašo kanalui pritaikoma antro lygio diskrečioji bangelių transformacija. DWT operacija sukuria vienos dimensijos sritis pateiktas 3.4 paveiksle.

A2	D2	D1
----	----	----

3.4 pav. Atlikus dviejų lygių DWT operaciją gautos išėjimo signalo sritys [19]

Čia A2 - aproksimacijos sritis, D1 bei D2 - pirmo ir antro lygio detalių sritys.

- Į antro lygio kairiojo kanalo detalių sritį $D2$ įterpiamas normalizuotas vandens ženklų vektorius W_n . Vandens ženklų įterpimo procedūra sukuria antro lygio sritis ($WD2$).

3.3.2. Vandens ženklų atpažinimas turint jau paženklintą garso įrašą

Vandens ženklų nuskaitymo operacija skirta garso įrašo savininkui išgauti vandens ženklą iš jo pažymėto garso įrašo. Ši procedūra reikalauja žinių apie originalų įrašą bei vandens ženklų savybes. Žinant visa tai galima atpažinti patį vandens ženklą. Binarinio atvaizdo vandens ženklų atpažinimas yra visiškai atvirkštinis jo įterpimui procesas ir susideda iš šių žingsnių:

- Originaliam ir paženklintam garso įrašui pritaikoma dviejų lygių diskrečioji bangelių transformacija. Kiekvienas iš jų sukuria vieną apytikslę ir dvi detales dalis.

- Apskaičiuojamas vandens ženklavimo vektorius W_t .
- W_t dalijamas iš vandens ženklo stiprinimo faktoriaus α ir gaunamas normalizuotas vandens ženklo vektorius W_n .
- W_n dauginamas iš 255 ir taip pakeičiamas originalus nespaltotas vandens ženklo paveikslėlis.
- Gautas W konvertuojamas atgal į dviejų dimensijų matricą, kuri ir apibūdina paveikslėlį.

3.3.3. Praktiniai algoritmo bandymų rezultatai

Praktiniams tyrimams naudojami WAV formato 11 sekundžių trukmės garso failai. Kiekvienas iš jų diskretizuotas 44,1 kHz dažniu ir kvantuotas iki 16 bitų per pavyzdį (angl. *Sample*). Garso failai yra stereo, turintys kairį ir dešinį kanalus. Vandens ženklui naudojamas 108 x 57 dydžio nespaltotas paveikslėlis pateiktas 3.5 paveiksle. Binarinio atvaizdo dydis buvo pasirinktas pagal garso failo ilgį.

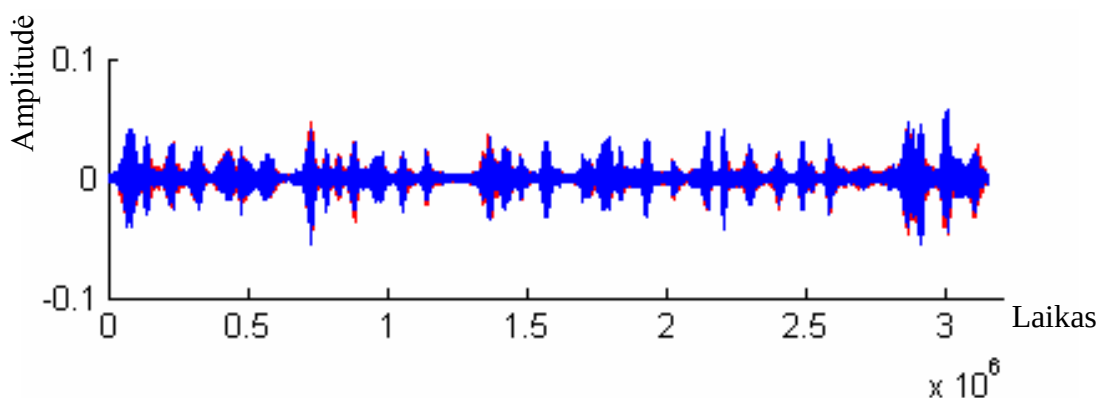


3.5 pav. Originalaus vandens ženklo paveikslėlis [19]

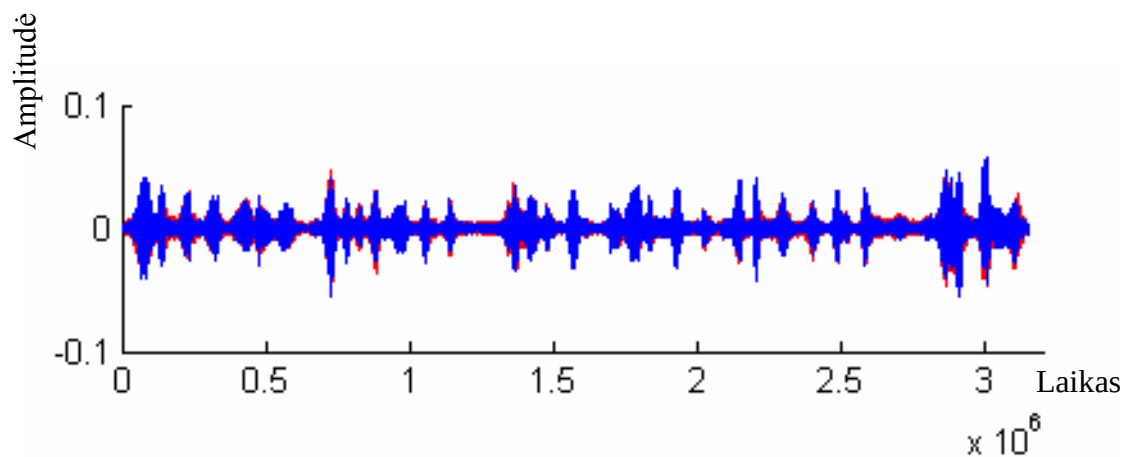
Garso vandens ženklo algoritmo savybės vertinamos pagal du pagrindinius rodiklius: slaptumą arba kitaip vandens ženklo nepastebimumą bei atsparumą apdorojimui.

Vandens ženklo slaptumas, tai savybė vandens ženklui likti neišgirstam ir nepastebėtam klausytojo. Ji yra matuojama signalo – triukšmo santykiu (angl. *signal to noise ratio arba SNR*).

3.6, 3.7, 3.8 ir 3.9 paveiksluose pateikiami garso originalių ir pažymėtų binarinio atvaizdo vandens ženklu garsų signalogramų atvaizdai. Nagrinėjant pačias signalogramas akivaizdžių skirtumų nepastebime.

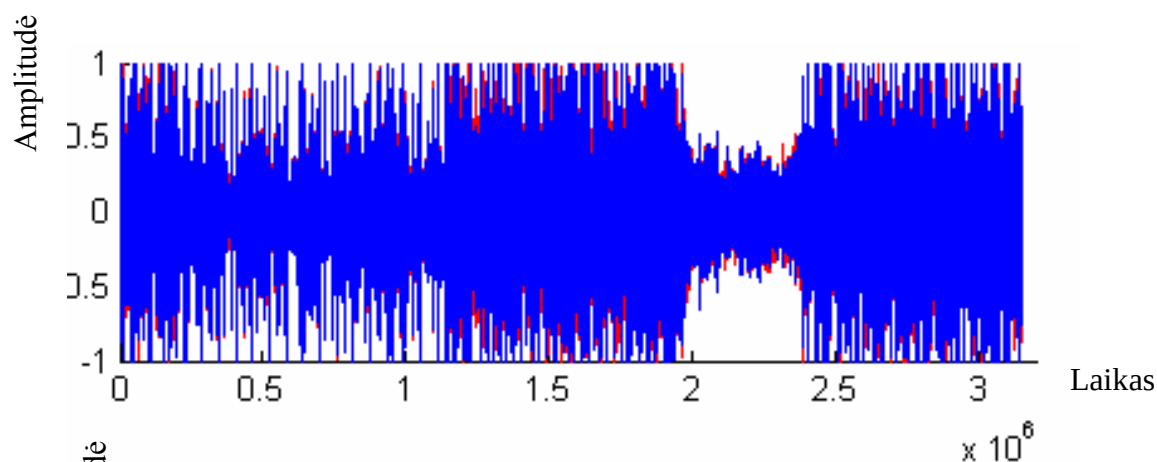


3.6 pav. Originalus instrumento garso įrašas [19]

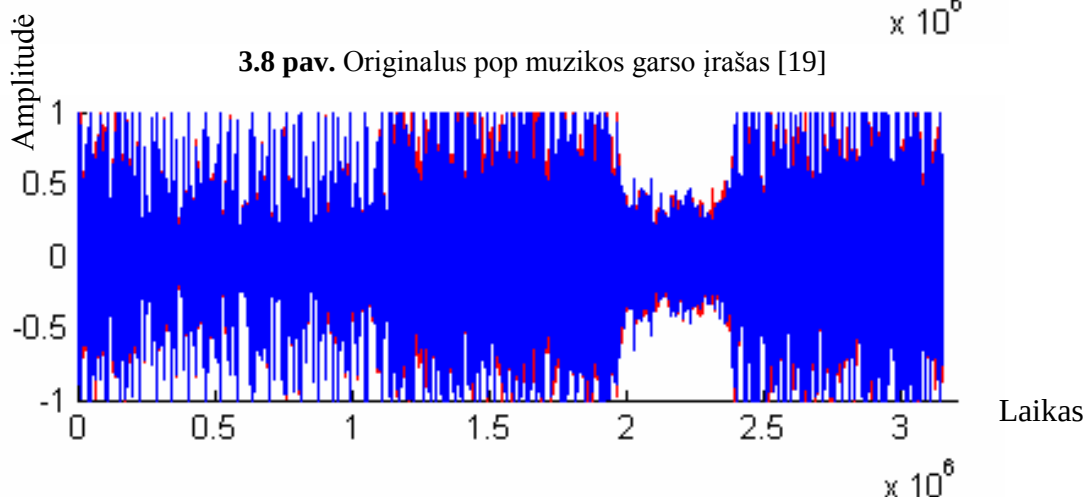


3.7 pav. Pažymėtas vandens ženklų instrumentų garso įrašas [19]

Palyginus 3.6 ir 3.7 paveiksluose pateiktus garso įrašo signalus skirtumas beveik nematomas, tai reiškia, kad įterptas vandens ženklas mažai pakeitė patį garsą.



3.8 pav. Originalus pop muzikos garso įrašas [19]



3.9 pav. Pažymėtas vandens ženklų pop muzikos garso įrašas [19]

Taip pat buvo atliktas ir klausymo testas. Jame dalyvavo 5 asmenys. Pirmiausia klausytojams buvo pateikti originalus ir paženklintas garso įrašai ir jie turėjo nurodyti ar jaučiamas kažkoks skirtumas tarp šių signalų. Rezultatus matome 3.5 lentelėje.

3.5 lentelė klausymo testo rezultatai [19]

Muzikos stilius	SNR, dB	MOS
Instrumentinė	28,5525	5,0
Pop	25,0314	5,0

MOS (angl. *Mean Opinion Score*) - nuomonės taškai. Jie gali būti skiriami nuo 1 iki 5. 1 taškas reiškia, kad garso įrašai visiškai skirtingi ir tai gali išgirsti paprastas klausytojas, o 5 – garso įrašų skirtumo išgirsti neįmanoma.

Kita pagrindinė testuoto vandens ženklavimo algoritmo veiksnio savybė yra vandens ženklo atsparumas garso signalo apdorojimui ar kitam išoriniam poveikiui. Testavimas atliktas naudojant Adobe Audition 3 programinę įrangą. Originalaus ir paženklinto signalų panašumas skaičiuojamas pagal 3.6 formulę. Šiuo atveju normalizuota koreliacija NC žymima ženklu ρ . Žemiau pateikti gauti bandymų rezultatai:



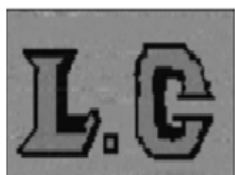
Pridedamas rūkas
($\rho = 0.963$)



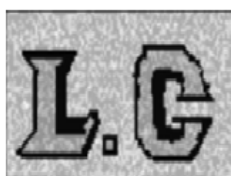
Pridedamas triukšmas 20dB
($\rho = 0.968$)



Aido ataka
($\rho = 0.966$)



Stiprinimas
($\rho = 0.915$)



Glodinimas
($\rho = 0.939$)



Statiškumas
($\rho = 0.950$)



Pakeitimas
($\rho = 0.973$)



Extra stereo
($\rho = 0.971$)

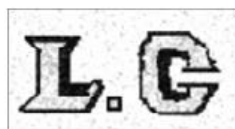


Nulio susikirtimo
($\rho = 0.970$)

3.10 pav. Išskleisto vandens ženklo iš instrumentinio garso įrašo būsenos po Adobe Audition apdorojimo [19]



Pridedamas rūkas
($\rho = 0.944$)



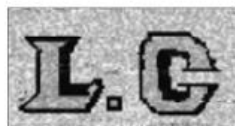
Pridedamas triukšmas 20dB
($\rho = 0.938$)



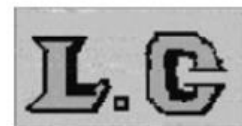
Aido ataka
($\rho = 0.06$)



Stiprinimas
($\rho = 0.865$)



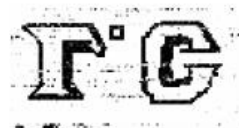
Glodinimas
($\rho = 0.910$)



Statistikumas
($\rho = 0.940$)



Pakeitimas
($\rho = 0.732$)



Extra stereo
($\rho = 0.870$)



Nulio susikirtimo
($\rho = 0.020$)

3.11 pav. Išskleisto vandens ženklų iš pop garso įrašo būsenos po Adobe Audition apdorojimo [19]

3.10 ir 3.11 paveiksluose matomi išskleisti vandens ženklų paveikslėliai po garso įrašo apdorojimo įvairiais metodais, po kiekvienu iš jų pateikti panašumo į originalą įverčiai. Iš 3.10 ir 3.11 paveiksluose pateiktų rezultatų matoma, kad garso signalo apdorojimas turėjo didesnę poveikį pop garso įrašui paslėptam vandens ženklui, negu žymeniui įterptam į instrumentinę muziką. Taip yra todėl, kad pop muzika yra gerokai sudėtingesnės formos ir aukštesnių dažnių signalas, tad ir menkas triukšmas jam turi didelės įtakos. Apdorojus instrumentinės muzikos įrašą gauti paveikslėliai mažai skiriasi nuo originalo ir yra lengvai atpažįstami. Abiejų signalų panašumo įvertis ρ negautas mažesnis negu 0,915. Gerokai prastesni rezultatai gauti su pop muzikos garso įrašu. Atlikus aido pridėjimo bei nulio susikirtimo atakas vandens ženklas tapo visiškai neatpažįstamas, taip pat didelis poveikis padarytas atliekant pakeitimo ataką. Tai ir yra pagrindiniai šio algoritmo trūkumai.

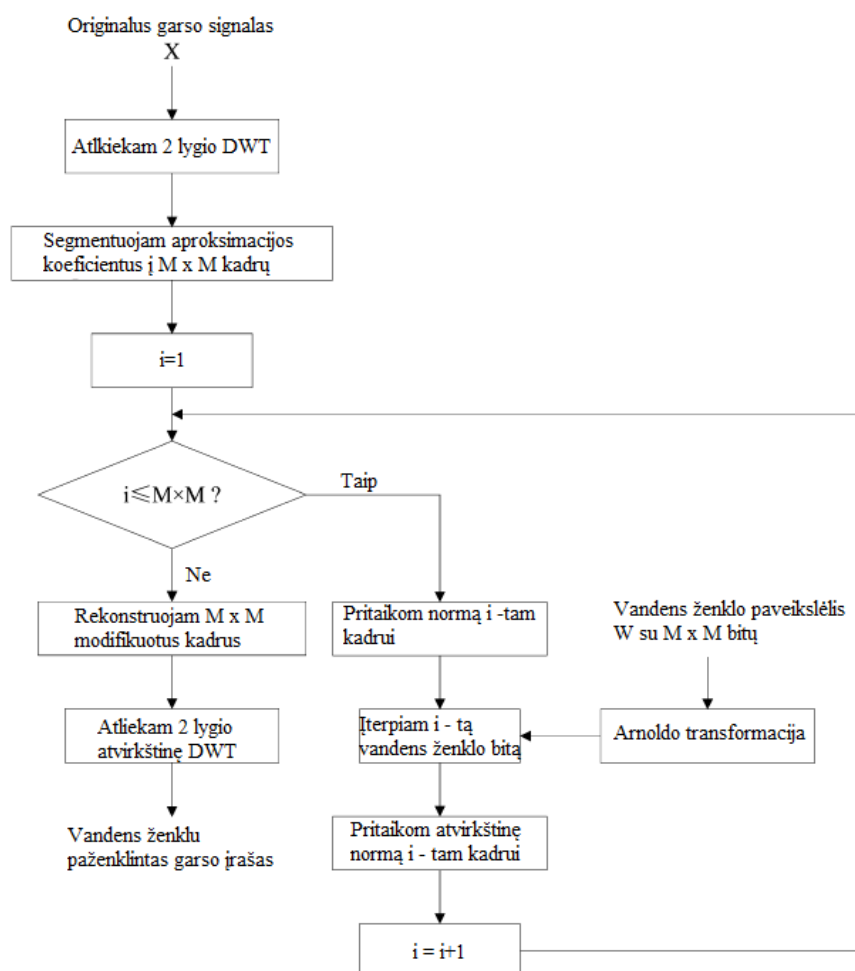
3.4. Normuotos erdvės, negirdimas garso vandens ženklavimo algoritmas naudojant diskrečią bangelių transformaciją

Šiame poskyryje pristatomas negirdimai į garsą įterpiantis vandens ženklų algoritmas. Pirmiausiai užšifruotas binarinis paveikslėlis kaip vandens ženklas įterpiamas į garso signalo segmentuotų diskrečios bangelių transformacijos koeficientų vektorių normas. Įterpimo procesas vykdomas naudojant kvantavimo indeksų moduliaciją su pasirinktu kvantavimo žingsniu. Paskui paženklintas garso signalas testuojamas su 10 tipų įvairių atakų, po apdorojimo išskleidžiamas vandens ženklas, analizuojami rezultatai.

3.4.1. Vandens ženklų įterpimo algoritmas

3.12 pav. matome pristatomą vandens ženklų įterpimo algoritmą. Detalus algoritmo aprašymas yra toks:

1. Originaliam garso signalui pritaikoma antro lygio diskrečioji bangelių transformacija su 4 Daubešo (angl. *Daubechies*) koeficientais (db4).
2. Aproximacijos komponentai dalijami į $M \times M$ nepersidengiančių kadrų. Kiekvienas iš kadrų gali talpinti po vieną binarinio atvaizdo vandens ženklą, kurio dydis $M \times M$ bitų. Naudojama tik ketvirtadalis koeficientų, nes vandens ženklas įterpiamas tik 1/4 garso įrašo ilgio dalį.
3. Kiekvienam gautam kadrui skaičiuojama vektoriaus norma.
4. Skaičiuojami kvantavimo indekso moduliacijos parametrai.
5. Panaudojus Arnoldo transformaciją yra gaunamas užšifruotas vandens ženklų paveikslėlis, kuris įterpiamas į originalų garso įrašą naudojant kvantavimo indekso moduliaciją.



3.12 pav. Negirdimo vandens ženklų įterpimo algoritmas naudojant diskrečią bangelių transformaciją ir kvantavimo indekso moduliaciją [20]

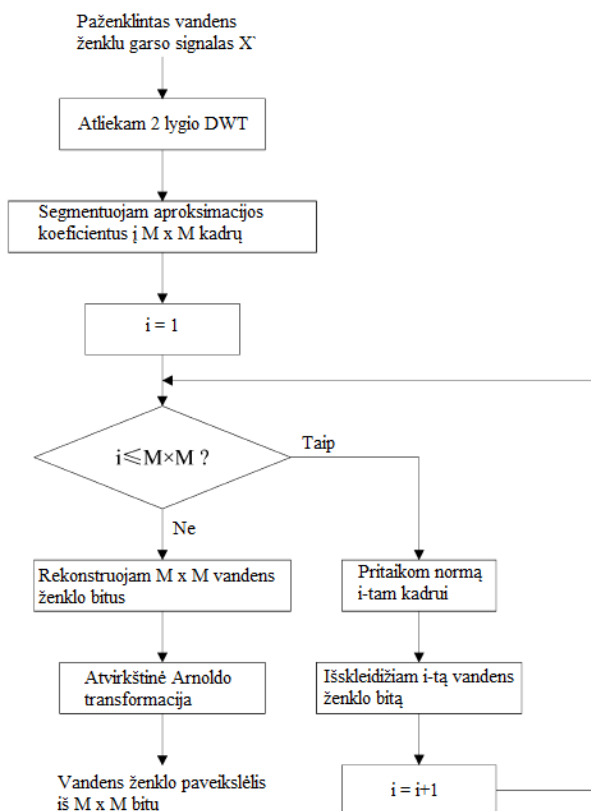
6. Iš modifikuotos vektoriaus normos gaunamas modifikuotas kadras.
7. Pertvarkomi aproksimacijos koeficientai ir jie sujungiami kartu.

8. Atliekama dviejų lygių atvirkštinė bangelių transformacija aproksimacijos komponentams. Gaunamas vandens ženklų pažymėtas garso įrašas X' .

3.4.2. Vandens ženklo nuskaitymo algoritmas

3.13 pav. pateiktas algoritmas, skirtas nuskaityti vandens ženklą iš garso įrašo, pažymėto pagal anksčiau pateiktą algoritmą (3.12 pav.).

1. Atliekama 2 lygio diskrečioji bangelių transformacija vandens ženklų pažymėtam garso įrašui X' . Gaunami aproksimacijos komponentai, kurie yra padalinti pagal binarinio atvaizdo matmenis $M \times M$.
2. Kiekvienam vektoriui pritaikoma vektoriaus norma.
3. Iš kiekvieno kadro nuskaityama po vieną vandens ženklo bitą. Jie yra rekonstruojami į $M \times M$ matricią.
4. Atlikus atvirkštinę Arnoldo transformaciją gaunamas dvejetainis paveikslėlis.



3.13 pav. Negirdimo vandens ženklo išskleidimo algoritmas naudojant diskrečią bangelių transformaciją ir kvantavimo indekso moduliaciją [20]

3.4.3. Algoritmo testavimo rezultatai

Bandymai atlikti naudojant Matlab 7.10 programinę įrangą. Apdorojimui pasirinktas 16 bitų garso signalas „original.wav“, kuris trunka 10 sekundžių, o jo diskretizacijos dažnis 44,100 Hz.

Vandens ženklui naudotas binarinis paveikslėlis, kurio taškų skaičius $M \times M = 32 \times 32 = 1024$. Vandens ženklo šifravimui panaudota Arnoldo transformacija.

Algoritmo bandymams pritaikytos šios apdorojimo procedūros:

1. Baltasis Gauso triukšmas (angl. *Additive white Gaussian noise*): baltasis Gauso triukšmas pridamas prie paženklinto vandens ženklu garso įrašo su 18 dB SNR.
2. Gauso žemų dažnių filtras (angl. *Gaussian Low-pass filter*): simetriškas Gauso žemų dažnių filtras su standartiniu nuokrypiu $\Sigma = 0,3$.
3. Kaizerio žemų dažnių filtras (angl. *Kaiser Low-pass filter*): žemų dažnių filtras su filtravimo intervalu nuo 10 kHz iki 12 kHz. Garso diskretizacijos dažnis 44,1 kHz.
4. Garso diskretizacijos dažnio keitimas (angl. *Resampling*): keičiamas paženklinto vandens ženklu garso įrašo diskretizacijos dažnis iš originalaus 44,1 kHz į 22,05 kHz ir atgal į 44,1 kHz.
5. Kvantavimo keitimas (angl. *Requantizing*): 16 bitų paženklintas vandens ženklu garso įrašas kvantuojamas į 8 bitus ir atgal į 16.
6. MP3 suspaudimas (angl. *MP3 compression*) į 32 kbps arba 16 kbps: MPEG-1 layer-3 suspaudimas pritaikomas vandens ženklu pažymėtam garso signalui, taip pakeičiamas garso įrašo formatas iš wav į mp3 bet atgal vėl į wav.
7. Aidas (angl. *Echo*): aidas su 100 ms vėlumu bei 40 % slopinimu pridamas paženklintam vandens ženklu garso įrašo signalui.

Bandymo rezultatai:

3.6 lentelė Normuotos erdvės, negirdimo vandens ženklinimo algoritmo testavimo rezultatai atlikus apdorojimo procedūras iš pateikto sąrašo [20]

Atakos tipas	NC	BER, %	Nuskaitytas vandens ženklas
Jokios atakos	1,0000	0,00	
Baltasis Gauso triukšmas	1,0000	0,00	
Gauso žemų dažnių filtras	1,0000	0,00	
Kaizerio žemų dažnių filtras	1,0000	0,00	
Diskretizacijos dažnio keitimas	1,0000	0,00	
Perkvantavimas	1,0000	0,00	
MP3 32 kbps	1,0000	0,00	

MP3 16 kbps	1,0000	0,00	
Aidas	1,0000	0,00	

3.7 lentelė Normuotos erdvės, negirdimo vandens ženklavimo algoritmo objektyvaus įvertinimo skirtumas ir signalo – triukšmo santykis[20]

	ODG	SNR, dB
Pristatytas algoritmas	-0,53	22,46

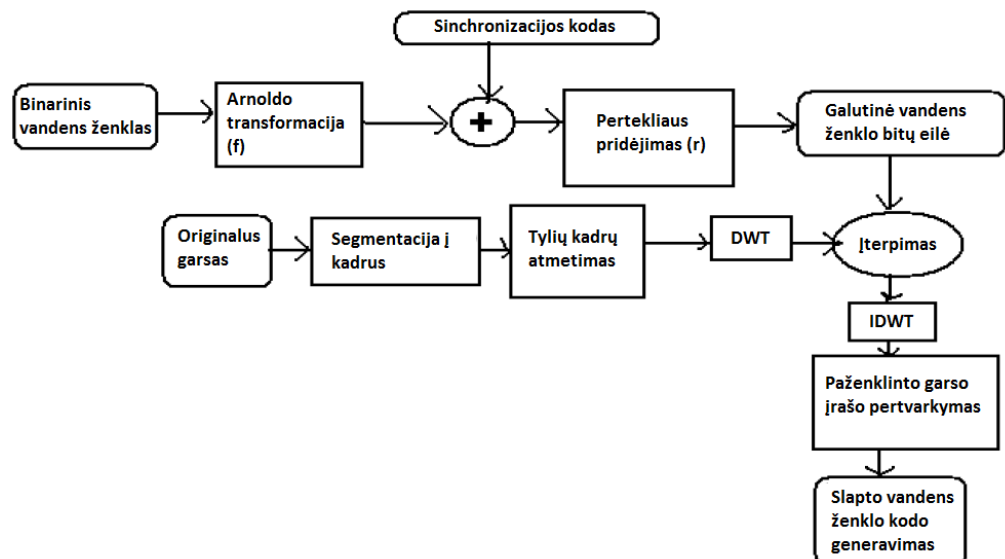
3.5. Neturintis nuostolių garso ženklavimo binariniu vandens ženklu algoritmas naudojantis alfa statistinę moduliaciją

Algoritmo įgyvendinimui panaudota alfa statistinė moduliacija. Ji skirta įterpti ir nuskaityti vandens ženklo bitus. Šis metodas gali veikti ir atvirkštiniu principu, ištrinti vandens ženklą bei atkurti garsą, kuris yra labai panašus originaliam nežymėtam garsui.

3.5.1. Viso vandens ženklo įterpimo procesas

1. Pritaikoma 3.1.1 skyrelyje aprašoma Arnoldo transformacija.
2. Gautas užšifruotas binarinis paveikslėlis konvertuojamas į vienos dimensijos masyvą, taip padidinama sistemos klaidų aptikimo tikimybė. Ši bitų eilė yra kopijuojama pagal pertekliaus faktorių r .
3. Pristatytas algoritmas naudoja 16 bitų Barkerio kodą sinchronizacijai, nustatyti paslėptų vandens ženklo bitų vietas.
4. Garso apdorojimo etape pirmiausiai originalus signalas suskaidomas į nepersidengiančius kadrus, kurių dydis M pavyzdžiui. Jei $X = (x(1), x(2), \dots, x(N))$ apibūdina originalų garso signalą, kurio dydis N , kur $x(i) \in (-1, 0; +1, 0)$ pavyzdžių reikšmės normalizuojamos duotame intervale.
5. Kadangi iškraipymai girdimi tyliose garso įrašo vietose, tai jos praleidžiamos ir vandens ženklo bitai įterpiami tik ten, kur egzistuoja garsas.
6. Nusprendžiama kokia bus poslinkio reikšmė, naudojama įterpimo etape $S = S_0$. Šis S yra priklausomas nuo reikalingos mažiausios signalo – triukšmo reikšmės po vandens ženklo įterpimo. Jis taip valdo vandens ženklo slaptumą.
7. Naudojama 2 lygio diskrečioji bangelių transformacija pritaikant Haaro bangeles. Gauti koeficientai atskiriami ir pasirenkamos tik žemo dažnio garso dalys.

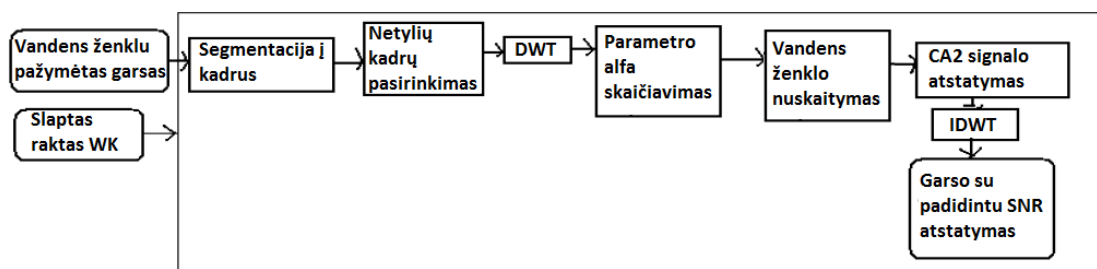
8. Pasirinktas garso kadras suskaidomas į du skirtingus rinkinius A ir B, tada pagal 2.12 formulę skaičiuojama statistika „ α “. Vandens ženklo bitai įterpiami naudojant „ α “ moduliaciją aptartą anksčiau.
9. Sujungiant visus kadrus paeiliui pertvarkomas pažymėtas garsas. Šio įrašo signalo ir triukšmo santykis skaičiuojamas ir lyginamas su numatyta SNR ir poslinkio reikšme „S“ bei keičiamas pagal tai.
10. Atliekama atvirkštinė 2 lygio bangelių transformacija.
11. Sukuriamas unikalus vandens ženklo raktas ir paskirstomas per visą garso įrašą. Jam naudojami skirtingi įterpimo proceso faktoriai: energijos ribos faktorius „ E_{th} “, pertekliaus faktorius „r“, pasirinkta žingsnio reikšmė „S“, Arnoldo transformacijos parametrai ir t.t. Tik turėdamas raktą vartotojas gali pašalinti vandens ženklą iš garso įrašo su mažiausiai iškreipymais.



3.14 pav. Vandens ženklo įterpimas naudojant alfa statistinės moduliacijos metodą [21]

3.5.2. Viso vandens ženklo nuskaitymo procesas

Garso vandens ženklo nuskaitymo proceso schema pateikta 3.16 paveiksle. Šis veiksmas yra visiškai atvirkštinis aptartam garso žymėjimui. Visi reikalingi parametrai gaunami iš slapto rakto. Garso signalas suskaidomas į nepersidengiančius kadrus, kurių dydis M pavyzdžiui. Tylieji kadrai atmetami ir pasirenkami tik tie, kuriuose užkoduotas signalas. Skirtumo reikšmė „ α “ skaičiuojama CA2 koeficientams, kurie pasirinkti kiekvienam garso kadrai diskrečiųjų bangelių srityje. Jeigu skirtumo reikšmė „ α “ nepatenka į ribas, tada nuskaitytas bitas = „1“ ir CA2 reikšmės gali būti atstatytos į pradinę būseną. Jeigu skirtumo reikšmė „ α “ patenka į nustatytas ribas tada gautas bitas = „0“. Šiuo būdų vandens ženklo bitus galima išskleisti kartu su sinchronizacijos kodu. Kai tik visi vandens ženklo bitai nuskaityti, tada jis gali būti atstatytas į pradinę formą, o garso kokybė pagerinta sumažinant iškreipymus.



3.15 pav. Vandens ženklų nuskaitymas naudojant alfa statistinės moduliacijos metodą [21]

3.5.3. Algoritmo bandymai

Algoritmo veikimo vertinimui pagal 3.14 ir 3.15 paveiksluose pateiktus algoritmus panaudota 30 skirtingų tipų mono garso signalų, kurių trukmė yra 20 sekundžių. Šių CD kokybės garso signalų diskretizacijos dažnis 44,1 KHz, o raiška – 16 bitų. Nuosavybės informacijos identifikavimui panaudotas vandens ženklų paveikslėlis, kurio dydis 32 x 32. Pertekliaus faktorius pasirinktas $r = 3$.

Kokybė matuojama signalo ir triukšmo santykiu, kuris jau aptartas anksčiau. Bandymo rezultatai pateikti 3.8 lentelėje.

3.8 lentelė Garso įrašo kokybė jį pažymėjus binariniu paveikslėliu naudojant alfa statistinę moduliaciją [21]

Vandens ženklų pažymėtas garsas SNR, dB	Atstatytas garsas panaudojus nuskaitytą vandens ženklą SNR, dB	Atstatytas garsas panaudojus originalų vandens ženklą SNR, dB
33,14	46,47	80,44

Vandens ženklų tvirtumui nustatyti buvo atlikti bandymai apdorojant garso įrašą. Apdorojimui panaudotos atakos bei gauti rezultatai pateikti 3.9 lentelėje.

3.9 lentelė Nuskaityto naudojant alfa statistinę moduliaciją vandens ženklų kokybė po garso signalo apdorojimo [21]

Apdorojimo/atakos tipas	Tvirtumas	
	BER, %	NC
Jokios atakos	0,0	1,00
Baltasis triukšmas	9,2	0,92
Diskretizacijos dažnio keitimas (22,05 kHz)	4,79	0,89
Diskretizacijos dažnio keitimas (11,025 kHz)	9,25	0,76
Diskretizacijos dažnio keitimas (8,00 kHz)	12,18	0,64
Perkvantavimas (8 bitai)	0,0	1,00
Perkvantavimas (24 bitai)	0,0	1,00
Žemų dažnių filtras (22,05 kHz)	9,11	0,82
MP3 48 kbps	13,30	0,75
MP3 32 kbps	16,44	0,69
Amplitudės modifikavimas (padidinta 0,2)	4,00	0,91
Amplitudės modifikavimas (padidinta 0,4)	5,18	0,89

4. OPTIMALAUS ALGORITMO PASIRINKIMAS

Optimalaus ir labiausiai tinkamo garso įrašo žymėjimo binariniu atvaizdu algoritmo pasirinkimas priklauso nuo keleto iš jau anksčiau aptartų pagrindinių veiksnių: vandens ženklo tvirtumo (angl. *Watermark robustness*) ir suvokimo aiškumo (angl. *Perceptual transparency*). Be to, muzikos pramonei reikalingas garso žymėjimo metodas, kuris turėtų minimalią įtaką garso įrašo kokybei ir būtų maksimaliai atsparus įvairaus tipo garso atakoms.

4.1. Algoritmų savybių įvertinimas

Pristatyti algoritmai yra ištestuoti ir bandymų rezultatai taip pat pateikti 3 skyriuje. Šiuos rezultatus lyginant yra renkamas apibūdintas savybes labiausiai atitinkantis algoritmas. Pagrindiniai įvertiniai bus 3.1.3 skyrelyje pateikti algoritmo vertinimo kriterijai: normalizuota koreliacija, signalo ir triukšmo santykis, bitų klaidų norma, objektyvus įvertinimo skirtumas. Palyginimui išrinkti rezultatai su analogiškais panaudotais apdorojimo metodais ir sudaryta 4.1. lentelė.

4.1 lentelė Garso įrašo ženklavimo binariniu atvaizdu algoritmų aptartų literatūros apžvalgoje bandymų rezultatai

Atakos tipas	Adaptivus algoritmas naudojantis vienetinės vertės išskyrimą [18]	Algoritmas naudojantis diskrečiąją bangelių transformaciją [19]	Normuotos erdvės, negirdimas algoritmas [20]	Neturintis nuostolių ir naudojantis „ α “ statistinę moduliaciją algoritmas [21]
Jokio atakos	NC = 1 BER = 0 %	-	NC = 1 BER = 0 %	NC = 1 BER = 0 %
Baltasis Gauso triukšmas	NC = 1 BER = 0 %	NC = 0,938 BER = - %	NC = 1 BER = 0 %	NC = 0,92 BER = 9,2 %
Gauso žemų dažnių filtras	NC = 0,9993 BER = 0 %	-	NC = 1 BER = 0 %	NC = 0,82 BER = 9,11 %
Kaizerio žemų dažnių filtras	-	-	NC = 1 BER = 0 %	-
Garso diskretizacijos dažnio keitimas	NC = 0,9854 BER = 2 %	-	NC = 1 BER = 0 %	NC = 0,89 BER = 4,79 %
Kvantavimo keitimas	NC = 1 BER = 0 %	-	NC = 1 BER = 0 %	NC = 1 BER = 0 %
MP3 suspaudimas 32 kbps	NC = 0,9907 BER = 1 %	-	NC = 1 BER = 0 %	NC = 0,69 BER = 16,44 %
Aidas	NC = 0,9847 BER = 2 %	NC = 0,06 BER = - %	NC = 1 BER = 0 %	-

4.1 lentelėje pateikti garso apdorojimo metodai ir jais gauti literatūroje pateikiami bandymų rezultatai. Rezultatai paimti iš atskirų kiekvieno iš 4 algoritmų bandymų bei jie apjungti pagal tokius pačius pritaikytus apdorojimo metodus. Algoritmai išdėstyti pagal poskyrio, kuriame jie pateikti numerius. Analizuojant gautus rezultatus reikia išrinkti tvirčiausią ir atspariausią apdorojimui garso įrašo žymėjimo binariniu atvaizdu algoritmą. Lentelėje paryškinti langeliai

apibūdina geriausią rezultatą ir mažiausius pažeidimus atakos metu, pagal tai bus išrinktas didžiausią apsaugą užtikrinantis algoritmas.

Neatlikus jokio garso apdorojimo beveik visais algoritmais gauti optimalūs rezultatai, t. y. $NC = 1$ ir $BER = 0\%$, tik algoritmo „naudojančio diskrečiąją bangelių transformaciją“ rezultatai labai skiriasi nuo visų kitų, nes jo testavimui buvo pasitelkti skirtingi garso apdorojimo metodai. Paveikus garsą baltuoju Gauso triukšmu geriausi rezultatai pasiekti naudojant „adaptyvų su vienetinės vertės išskyrimu“ ir „normuotos erdvės negirdimą“ algoritmus. Gauso žemų dažnių filtravimas mažiausią poveikį turėjo „normuotos erdvės negirdimam“ algoritmui. Visais kitais bandymo etapais geriausi rezultatai gauti naudojant „normuotos erdvės negirdimą“ algoritmą, išskyrus perkvantavimą, kur optimalus rezultatas pasiektas dar dviem kitais vandens ženklinimo metodais. Taigi daugiausiai paryškintų langelių ir geriausiais atsparumo rezultatais pasižymi – „normuotos erdvės, negirdimas garso vandens ženklinimo algoritmas“.

Dar vienas labai svarbus garso žymėjimo binariniu atvaizdu algoritmo įvertinimo kriterijus yra signalo ir triukšmo santykis, kuris apibūdina paženklinto ir originalaus garso signalo panašumą. Kuo didesnis SNR, tuo garso kokybė didesnė. Pristatytų algoritmų signalo ir triukšmo santykių palyginimas pateiktas 4.2 lentelėje.

4.2 lentelė Garso įrašo pažymėto binariniu vandens ženklu signalo ir triukšmo santykis naudojant literatūros apžvalgoje pristatytus algoritmus

	Adaptyvus algoritmas naudojantis vienetinės vertės išskyrimą [18]	Algoritmas naudojantis diskrečiąją bangelių transformaciją [19]	Normuotos erdvės, negirdimas algoritmas [20]	Neturintis nuostolių ir naudojantis „ α “ statistinę moduliaciją algoritmas [21]
Signalas – triukšmo santykis (SNR), dB	22,11	25,0314	22,46	33,14

Lyginami signalo ir triukšmo santykio rezultatai gaunami vandens ženklo įterpimui pasirinkus pop muzikos stiliaus garso įrašą. Geriausia garso kokybė pasižymi „neturintis nuostolių naudojantis alfa statistinę moduliaciją algoritmas“. Jo SNR gerokai didesnis negu visais kitais algoritmais gautų garso įrašų, tačiau signalo ir triukšmo santykis nevisai tiksliai atspindi girdimo garso kokybę, nes daugelis triukšmų, kuriuos jis apibūdina tiesiog gali būti negirdimi žmogaus ausimi.

Klausytojų girdimai garso kokybei įvertinti labiausiai tinka objektyvaus įvertinimo skirtumas – tai įvertis, kuris gaunamas sudarius matematinį garso kokybės įvertinimo modelį, atitinkantis klausymo testų rezultatus. Kadangi vienuose algoritmuose pateikti klausymo testų rezultatai, kitur būtent šis įvertinimas, todėl prieš tai jie bus sulyginti ir priskirti bendrai sistemai. Klausymo testas vertinamas nuo 1 iki 5 balų. 1 – triukšmas erzina, 5 – garsas kokybiškas ir triukšmai negirdimi. Objektyvaus įvertinimo skirtumo vertinimų skalė pateikta 3.1 lentelėje. 0 – labai kokybiškas garsas

ir triukšmai negirdimi, -4 – triukšmas erzinantis. Visi garso žymėjimo algoritmai lyginamo ODG skalėje, todėl norint sutapatinti rezultatus, iš klausymo testo gaunamo skaičiaus atimama 5. Gauti rezultatai pateikiami 4.3 lentelėje.

4.3 lentelė Garso įrašo pažymėto binariniu vandens ženklų objektyvaus skirtumo įvertinimas naudojant literatūros apžvalgoje pristatytus algoritmus

	Adaptivus algoritmas naudojantis vienetinės vertės išskyrimą [18]	Algoritmas naudojantis diskrečiąją bangelių transformaciją [19]	Normuotos erdvės, negirdimas algoritmas [20]	Neturintis nuostolių ir naudojantis „α“ statistinę moduliaciją algoritmas [21]
Objektyvaus skirtumo įvertinimas (ODG)	- 0,7	0	- 0,53	-

Objektyvaus įvertinimo skirtumas pateiktas literatūros apžvalgoje pateiktiems algoritmams, išskyrus „neturinčiam nuostolių ir naudojančiam „α“ statistinę moduliaciją“, nes bandymuose jis nepateikiamas. Geriausias rezultatas gautas pasitelkus algoritmą „naudojančią diskrečiąją bangelių transformaciją, ODG = 0 , tačiau šiam algoritmui konkretus objektyvaus įvertinimo skirtumas nebuvo skaičiuotas, jis gautas pagal klausymo testo rezultatus, kurie šiuo atveju negali būti labai tikslūs. Iš gautų rezultatų galima spręsti, kad visais pateiktais atvejais (išskyrus [21] algoritmą, nes nėra pateikti kokybės vertinimo rezultatai) garse vandens ženklas nėra girdimas/silpnai pastebimas, nes atsirandantys trikdžiai nedideli ir praktiškai negirdimi žmogaus ausiai.

4.2. Muzikos pramonei optimalaus algoritmo pasirinkimas pagal įvertintus kriterijus

Egzistuoja daugybė garso įrašo žymėjimo vandens ženklų metodų, tačiau visi jie skiriasi savo savybėmis. Dauguma atsparūs tik tam tikro tipo apdorojimo metodams, o kiti gali visiškai pažeisti vandens ženklą ir padaryti jį nebeatpažįstamu. Mokslininkai pasiūlė ir tokių metodų, kurie yra atsparūs daugybei atakų nukreiptų prieš garsą, bet jie patys žymėjimo metu pakeičia signalo struktūrą taip, kad atsiranda trikdžiai, kuriuos girdi klausytojas. Toks būdas taip pat nėra tinkamas muzikos pramonei. Problemos sprendimas – labiausiai atsparus ir mažiausiai įtakojantis garso kokybės pasikeitimą vandens ženklo įterpimo metodas.

Pagrindinis pasirinkimo rodiklis yra vandens ženklo tvirtumas, mažiau svarbus – garso įrašo kokybė, todėl iš 4.1 lentelės matome, jog pats atspariausias įvairiems apdorojimo metodams yra „normuotos erdvės negirdimas“ algoritmas. Šioje srityje jis gerokai lenkia savo konkurentus ir absoliučiai visais atvejais gaunami geriausi rezultatai. Garso įrašo kokybę klausytojo atžvilgiu geriausiai įvertina objektyvaus įvertinimo skirtumas, kuris geriausias gaunamas algoritmui „naudojančiam diskrečiąją bangelių transformaciją“, tačiau taikant kitus garso ženklinimo metodus

jis labai panašus. Triukšmų pagal SNR mažiausiai generuoja „neturintis nuostolių ir naudojantis „ α “ statistinę moduliaciją“ algoritmas, tačiau kitais atvejais pažymėto garso kokybė išlieka taip pat labai aukšta.

Įvertinus rezultatus muzikos pramonei labiausiai tinkamas yra „normuotos erdvės, negirdimas garso vandens ženklavimo algoritmas“. Jis išliko visiškai nepaveiktas apdorojant muzikos signalą, taip pat garsą pažymėjus vandens ženklu signalo kokybė pasikeičia negirdimai klausytojui. Šis garso žymėjimo vandens ženklu metodas vienintelis neturintis didelių trūkumų. Jis mažai įtakoja garso kokybę ir garantuoja vandens ženklo tvirtumą. Kiti analizuoti metodai yra geri tik vienoje arba jokioje iš kokybės ir tvirtumo sričių.

5. PRAKTINĖ DALIS

Šioje dalyje pateiktas pasirinkto algoritmo tobulinimo procesas, detalus veikimo aprašymas po atnaujinimo, praktiniai šio algoritmo skirto garso žymėjimui binariniu paveikslėliu bandymai ir tyrimai pagal pasirinktą testavimo planą. Vandens ženklų atsparumo kokybės vertinimui naudojami analogiški garso įrašo apdorojimo metodai, kaip ir jau prieš tai aptartuose ir lygintuose algoritmuose.

5.1. Pasirinkto algoritmo tobulinimas

Išanalizavus pateiktus garso ženklavimo binariniu atvaizdu algoritmų testavimo rezultatus, pasirinktas „normuotos erdvės negirdimas“ ženklavimo metodas. Veikimo principas jame glaustai paaiškintas, o šiame poskyryje pateikiame algoritmo pakeitimus, kurie turi pagerinti reikalingas garso ženklavimo savybes.

Vandens ženklų tvirtumas nebus keičiamas. Pagal 4.1 lentelę jis yra optimalus ir apdorojimo procedūros neturėjo jokios įtakos nuskaityto vandens ženklų kokybei. Šiuo atveju pagerinti galima gautą garso kokybę, t. y. padidinti signalo ir triukšmo santykį bei objektyvaus skirtumo įvertinimą.

Peržiūrėjus visą 3.4 poskyryje pateiktą „normuotos erdvės negirdimą“ garso žymėjimo algoritmą, matoma, kad vandens ženklas įterpiamas į abu garso kanalus naudojant 1/4 viso įrašo ilgio. Siekiant pagerinti garso kokybę binarinį paveikslėlį įterpsime tik į vieną - kairįjį kanalą bei naudosime visą garso signalo ilgį. Vandens ženklą pridėdant trumpoje garso dalyje, toje vietoje garsas labai iškraipomas, didelė dalis originalių garso bitų pakeičiama vandens ženklų, todėl dideli triukšmai girdimi toje trumpoje signalo dalyje, o kitur jų visai nėra. Siekiant žymėjimą padaryti dar mažiau girdimą, vandens ženklą išskaidysime per visą garso įrašą.

Antras kokybės gerinimo etapas yra vandens ženklų įterpimas tik į kairįjį stereo garso kanalą, o dešinįjį paliekant originalų. Klausant muziką tuo pat metu kairėje bus girdimas pažymėtas garsas, o dešinėje – originalus, tai garsams susijungus, klausytojui bus dar sunkiau suprasti, jog garsas apsaugotas. Vandens ženklą įterpiančiam į abu stereo kanalus iškraipymai atsirastų abiejuose garso kanaluose ir būtų labiau girdimi.

5.2. Patobulintas normuotos erdvės garso įrašo žymėjimo binariniu atvaizdu algoritmas naudojant diskrečiąją bangelių transformaciją ir kvantavimo indekso moduliaciją

Šiame poskyryje pateikiamas detalus patobulinto garso įrašo žymėjimo binariniu atvaizdu algoritmo veikimo paaiškinimas. Padarius aptartus pakeitimus muzikos pramonei labiausiai tinkamas ir siūlomas algoritmas yra pateiktas 5.1 paveiksle.

Vektoriaus normos tvirtumas šiame algoritme panaudojamas įterpti vandens ženklui. Vektoriaus normą apskaičiuojame:

$$\sigma = \|A\| = \sqrt{\sum_{i=1}^n a_i^2}; \quad (5.1)$$

Kai $A = (a_1, a_2, \dots, a_n)$ yra $1 \times n$ vektorius, o σ yra jo norma:

$$A = \sigma u^T; \quad (5.2)$$

u yra $n \times 1$ vektorius:

$$u = \frac{A^T}{\|A\|} = \frac{A^T}{\sigma}. \quad (5.3)$$

5.2.1. Vandens ženklo įterpimo algoritmas

Vandens ženklo įterpimo algoritmas pateiktas 5.1 paveiksle. Detalus jo veikimo aprašymas yra toks:

1. Antro lygio diskrečioji bangelių transformacija su 4 Daubešo (angl. *Daubechies*) koeficientais (db4) pritaikoma skaitmeniniam signalui. $X = \{x(i) | 1 \leq i \leq L\}$, kuris yra originalus garso signalas trunkantis T sekundžių ir sudarytas iš L skaičiaus pavyzdžių (angl. *samples*). Gaunami aproksimacijos koeficientai $C = \{c(i) | 1 \leq i \leq L\}$.
2. Aproksimacijos komponentai dalijami į $M \times M$ nepersidengiančių kadrų Z_i ($1 \leq i \leq M \times M$). Kiekvienas iš kadrų gali talpinti po vieną binarinio atvaizdo vandens ženklo, kurio dydis $M \times M$ bitų. Kadro Z_i ilgis yra $p = \lfloor L / (M \times M) \rfloor$.
3. Kiekvienam gautam kadrai skaičiuojama vektoriaus norma σ_i ($1 \leq i \leq M \times M$) pagal 5.1 formulę.
4. Skaičiuojami kvantavimo indekso moduliacijos parametrai:

$$e = \left\lfloor \frac{\sigma_i}{\Delta} \right\rfloor; \quad (5.4)$$

$$d = \sigma_i \bmod \Delta. \quad (5.5)$$

Čia Δ - kvantavimo žingsnis. Didinant Δ , įterptas vandens ženklas tampa tvirtesnis, tačiau prarandama garso įrašo kokybė, SNR mažėja. Mažinant – atvirkščiai. Tai suteikia algoritmui lankstumo ir galimybę pasirinkti norimą tvirtumą bei garso įrašo kokybę.

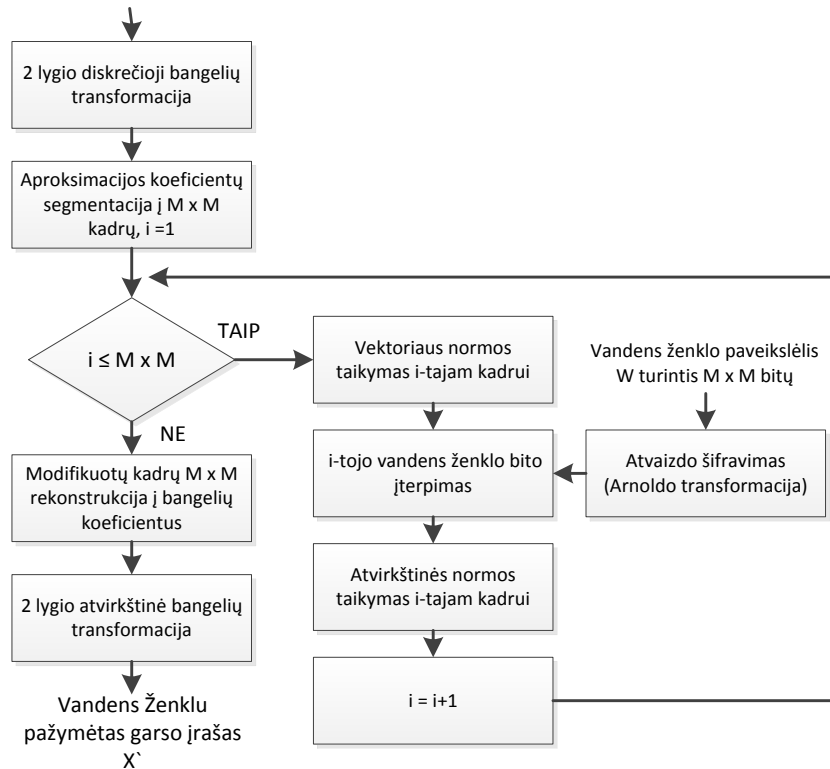
5. Vandens ženklo bitas $w(i, j)$ gali būti gautas iš dvejetainio vandens ženklo paveikslėlio $W = \{w(i, j) | 1 \leq i \leq M, 1 \leq j \leq M\}$. Panaudojus Arnoldo transformaciją yra gaunamas užšifruotas vandens ženklo paveikslėlis. $\bar{W} = \{\bar{w}(i, j) | 1 \leq i \leq M, 1 \leq j \leq M\}$, kuris įterpiamas į originalų garso įrašą.

Jeigu $\bar{W}(i, j) = 1$, tada σ_i modifikuojama taip:

$$\sigma_i' = \begin{cases} \sigma_i + \frac{\Delta}{2} - (\sigma_i \bmod \Delta) & \text{jei } (e \bmod 2 = 1) \\ \sigma_i + \Delta + \frac{\Delta}{2} - (\sigma_i \bmod \Delta) & \text{jei } (e \bmod 2 = 0 \text{ ir } d > \Delta/2) \\ \sigma_i + \Delta + \frac{\Delta}{2} - (\sigma_i \bmod \Delta) & \text{jei } (e = 0 \text{ ir } d < \Delta/2) \\ \sigma_i - \Delta + \frac{\Delta}{2} - (\sigma_i \bmod \Delta) & \text{jei } (e \bmod 2 = 0 \text{ ir } d < \frac{\Delta}{2} \text{ ir } e \neq 0) \end{cases}; \quad (5.6)$$

Jeigu $\bar{W}(i, j) = 0$, tada σ_i modifikuojama taip:

$$\sigma_i' = \begin{cases} \sigma_i + \frac{\Delta}{2} - (\sigma_i \bmod \Delta) & \text{jei } (e \bmod 2 = 0) \\ \sigma_i + \Delta + \frac{\Delta}{2} - (\sigma_i \bmod \Delta) & \text{jei } (e \bmod 2 = 1 \text{ ir } d > \Delta/2) \\ \sigma_i - \Delta + \frac{\Delta}{2} - (\sigma_i \bmod \Delta) & \text{jei } (e \bmod 2 = 1 \text{ ir } d < \frac{\Delta}{2}) \end{cases}. \quad (5.7)$$



5.1 pav. Patobulinto negirdimo vandens ženklų įterpimo algoritmas naudojant diskrečią bangelių transformaciją ir kvantavimo indekso moduliaciją

6. Su modifikuota vektoriaus norma σ_i' gaunamas modifikuotas kadras $Z_i'(1 \leq i \leq M \times M)$

$$\bar{\sigma}_i = |\sigma_i|; \quad (5.8)$$

$$Z_i' = \bar{\sigma}_i u_i^T. \quad (5.9)$$

7. Visi modifikuoti kadrai Z_i' sujungiami paeiliui.

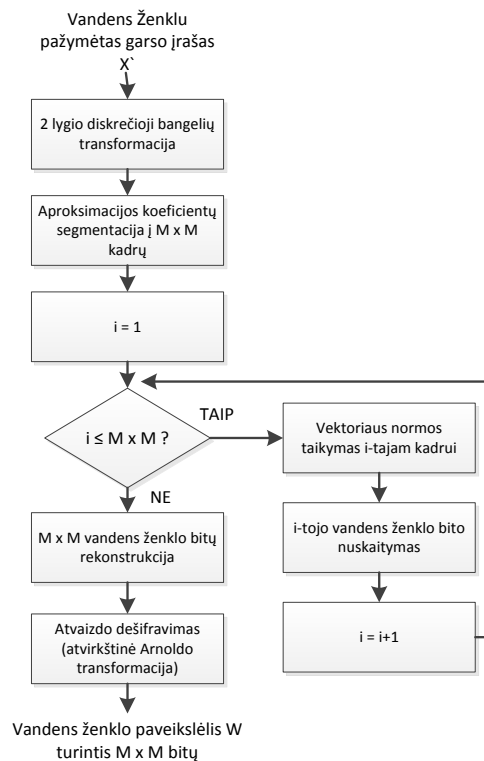
8. Atliekama dviejų lygių atvirkštinė bangelių transformacija aproksimacijos komponentams $C = \{c'(i) | 1 \leq i \leq L\}$. Gaunamas vandens ženklų pažymėtas garso įrašas X' .

5.2.2. Vandens ženklų nuskaitymo algoritmas

5.2 pav. pateiktas vandens ženklų iš garso įrašo nuskaitymo algoritmas. Detalus jo veikimo aprašymas yra toks:

1. Vandens ženklų pažymėtam garso įrašui X' atliekama 2 lygio diskrečioji bangelių transformacija. Gaunami aproksimacijos komponentai $C' = \{c'(i) | 1 \leq i \leq L\}$, kurie yra padalinami pagal binarinio atvaizdo matmenis $M \times M$ į nepersidengiančius kadrus $Z'_i (1 \leq i \leq M \times M)$. Kadro ilgis $p = \lceil L / (M \times M) \rceil$.
2. Kiekvienam vektoriui Z'_i pritaikoma vektorių norma, gaunama $\sigma'_i (1 \leq i \leq M \times M)$.
3. Skaičiuojama $e = \lfloor \frac{\sigma'_i}{\Delta} \rfloor$, jei $e \bmod 2 = 0$, tada įterpto vandens ženklų bitas yra 0, priešingu atveju – 1. Atlikus atvirkštinę Arnoldo transformaciją gaunamas dvejetainis paveikslėlis.

$$W = \{w(i, j) | 1 \leq i \leq M, 1 \leq j \leq M\}. \quad (5.10)$$



5.2 pav. Patobulinto negirdimo vandens ženklų nuskaitymo algoritmas naudojant diskrečią bangelių transformaciją ir kvantavimo indekso moduliaciją

5.3. Algoritmo savybių tyrimo metodika

Algoritmo kokybės testavimas ir tyrimas susideda iš trijų etapų:

1. Garso signalo ir vandens ženklų kokybės vertinimas po vandens ženklų įterpimo: modeliuojamas klausymo testas (ODG), skaičiuojamas signalo – triukšmo santykis (SNR).
2. Nuskaityto vandens ženklų kokybės įvertinimas pagal 3.1.3 skyrelyje pateiktas charakteristikas neatlikus garso signalo apdorojimo.

3. Nuskaityto vandens ženklų kokybės įvertinimas pagal 3.1.3 skyrelyje pateiktas charakteristikas po garso signalo apdorojimo.
4. Signalų – triukšmo santykio priklausomybės nuo pažymėto vandens ženklų garso įrašo ilgio analizė.

Pirmiems trimis tyrimo etapams įgyvendinti sudaromas garso signalo apdorojimo metodų sąrašas. Jie turi būti tinkami kokybiškam garso vandens ženklų tvirtumo įvertinimui bei palyginimui, todėl pasirenkami [7] šaltinyje pateikiami garso apdorojimo būdai:

1. Jokio poveikio. Šis etapas yra skirtas garso įrašo ir binarinio atvaizdo kokybės pokyčių vertinimui po vandens ženklų įterpimo. Pirmiausiai matuojamos garso pažymėto vandens ženklų charakteristikos iškart po ženklinimo procedūros ir neatlikus jokio apdorojimo. Viena iš svarbiausių šio etapo užduočių yra sužinoti signalo ir triukšmo santykį bei objektyvaus skirtumo įvertinimą.

2. Baltasis Gauso triukšmas (angl. *Additive white Gaussian noise*): baltasis Gauso triukšmas pridamas prie paženklinto vandens ženklų garso įrašų su 18 dB SNR. Šis triukšmas yra įprastas kiekvienam komunikacijos kanalui, jis yra atsitiktinis radijo triukšmas apibūdinamas plačiu dažnių intervalu, priklausomai nuo signalo ir ryšio kanalo. Triukšmas yra pridėtinis, nes gautas signalas būna lygus jo paties ir trikdžių sumai, kuomet triukšmas ir signalas yra statistiškai nepriklausomi. Triukšmas laikomas baltuoju, nes jo energijos spektras yra platus, todėl autokoreliacija laiko srityje lygi nuliui, o trikdžių pavyzdžiai pasiskirstę pagal Gauso skirstinį [14].

3. Gauso žemų dažnių filtras (angl. *Gaussian Low-pass filter*): simetriškas Gauso žemų dažnių filtras su standartiniu nuokrypiu $\Sigma = 0,3$. Filtras, kurio atsakas yra Gauso funkcija. Gauso filtrai turi neviršyti įėjimo signalo, kol mažinamas kilimo ir kritimo laikas. Toks filtras laikomas idealiu laiko srityje [15].

4. Kaizerio žemų dažnių filtras (angl. *Kaiser Low-pass filter*): žemų dažnių filtras su filtravimo intervalu nuo 10 kHz iki 12 kHz. Garso diskretizacijos dažnis 44,1 kHz. Šis filtras gaunamas naudojant Kaizerio langą (angl. *Kaiser window*), taip pat žinomą kaip Kaizerio – Beselio langą. Jis plačiai naudojamas skaitmeninių signalų apdorojimui.

5. Garso diskretizacijos dažnio keitimas (angl. *Re-sampling*): keičiamas paženklinto vandens ženklų garso įrašo diskretizacijos dažnis iš originalaus 44,1 kHz į 22,05 kHz ir atgal į 44,1 kHz. Diskretizacijos dažnio keitimas yra procesas, kai keičiamas diskretaus laiko signalo atskaitų (angl. *samples*) dažnis. Jis reikalingas todėl, kad skirtingos sistemos naudoja skirtingus pavyzdžių dažnius. Pvz. skirtingos garso sistemos naudoja 44,1, 48 arba 96 kHz įrašus. Garso kokybė labai priklauso nuo diskretizacijos dažnio, nes jis būtent ir nusako, kiek atskaitų per sekundę naudojama atkurti garsui, tad įprastai šis dažnis mažinamas siekiant sumažinti signalo užimamą vietą kompiuteryje [16].

6. Kvantavimo keitimas (angl. *Requantizing*): 16 bitų paženklintas vandens ženklų garso įrašas kvantuojamas į 8 bitus ir atgal į 16. Muzikoje kvantavimas yra procesas atliekamas garso natoms, kurias skaitmeninė technika gali šiek tiek netiksliai išreikšti, tad po šio veiksmo netikslumai yra pašalinami. Gautos natos išreiškiamos muzikos ritmu ar ritmo grupėmis. Būtinis ritmo keitimo vietos nustatymas yra pagrindinė kvantavimo problema [16].

7. MP3 spūda (angl. *MP3 compression*) į 32 kbps ir 16 kbps: MPEG-1 layer-3 suspaudimas pritaikomas vandens ženklų pažymėtam garso signalui, taip pakeičiamas garso įrašo formatas iš wav į mp3, o paskui vėl atgal į wav. MPEG-1 arba MPEG-2 Audio Layer III dažniausiai vadinami tiesiog MP3. Tai yra skaitmeninio garso kodavimo formatas, kuris gaunamas sumažinant duomenų kiekį iki mažiausio reikalingo atkurti nustatytos kokybės garsą. MP3 yra visiškai įprastas šiuolaikinėje skaitmeninėje pramonėje, šiuo formatu duomenys laikomi skaitmeninėse laikmenose, kietuosiuose diskuose, taip pat transliuojami iš radijo stočių. Garso signalą konvertuojant į MP3, visi jo pavyzdžiai iš laiko srities perkeliama į dažnių sritį ir ten diskretizuojami, išrenkami tik tie, kurių reikia garso įrašo atkūrimui, kiti pašalinami, taip sutaupoma daugybė vietos kietajame diske. Vėliau norint garso formatą pakeisti į wav vykdomas atvirkštinis veiksmas, tačiau jo pradinė kokybė jau nebeatgaunama [17].

8. Aidas (angl. *Echo*): aidas su 100 ms vėlinimu bei 40 % slopinimu pridedamas paženklintam vandens ženklų garso įrašo signalui. Aidas – atsispindėjęs nuo paviršiaus garsas, girdimas vėliau už originalųjį. Šiuo atveju tai atsikartojantis garsas, kuris atsilieka 100 ms ir yra 40% tylesnis.

5.4. Darbui reikalinga programinė įranga

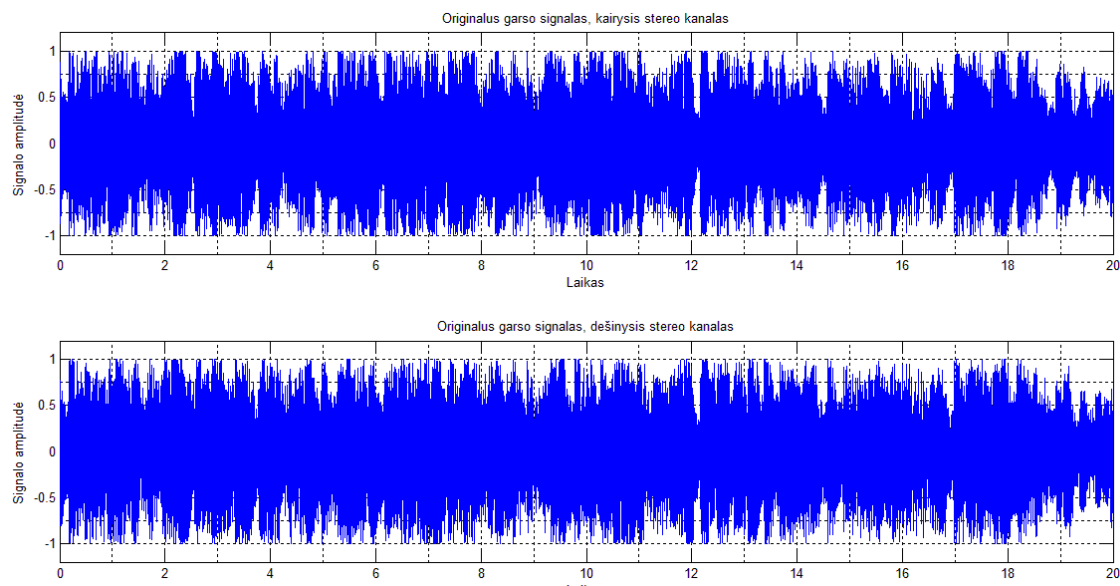
Praktinio darbo metu reikia sukurti programinę įrangą, kuri realizuotų pasirinktą ir patobulintą garso žymėjimo algoritmą bei ištestuotų vandens ženklo įterpimo algoritmo kokybę. Praktiniam patobulinto garso ženklinimo binariniu atvaizdu algoritmo įgyvendinimui bus naudojamas „Matlab 2013a“ programinis paketas. Jis pasirinktas todėl, kad savyje turi daugybę realizuotų sudėtingų funkcijų bei veiksmų, o programuotojui tereikia jas iškviesti ir pasinaudoti. Nors šis programinis paketas nėra skirtas programų skirtų masiniam naudojimui kūrimui, tačiau bandymams jo visiškai pakanka. „Matlab 2013a“ naudojamas ne tik algoritmo realizacijai, bet ir jo kokybės rodmenų skaičiavimui: SNR, BER, ODG, NC. Jis taip pat 1 – 4 numeriais pažymėtų garso apdorojimo metodų įgyvendinimui.

Antroji darbui reikalinga programa yra „Adobe Audition 6“. Tyrime ji naudojama binariniu atvaizdu pažymėto garso įrašo apdorojimui, tiksliau atliekami 5 – 8 sąrašo bandymai. „Adobe Audition 6“ pasirinkta naudojimui todėl, kad turi visas suplanuotam tyrimui reikalingas funkcijas.

5.5. Algoritmo tyrimo rezultatai

Atlikus visus pateiktus bandymus gauti rezultatai pateikiami žemiau. Jų forma atitinka užduoties punktus. Rezultatų vertinimo kriterijai pateikti 3.1.3 skyrelyje. Normalizuota koreliacija – optimalus rezultatas yra 1, mažesnis yra atitinkamai blogesnis. Klaidingų bitų norma – geriausias rezultatas yra 0 %, didėjant neatitinkančių bitų skaičiui ši norma taip pat didėja. Signalų – triukšmo santykis – idealus variantas yra begalybė, atsirandant garso triukšmams jis mažėja. Objektivaus įvertinimo skirtumas atitinka subjektyvius klausymo testus, tačiau modeliuojamas kompiuteriu. Jo vertinimo kriterijai: 0 – garso trikdžiai visiškai nepastebimi, -4 – triukšmas yra erzinantis klausytoją. Detali ODG vertinimo skalė pateikta 3.1 paveiksle. Algoritmo kokybės tyrimo rezultatai:

Originaliam garso įrašui nevykdytas joks apdorojimas nei ženklinimas. 5.3 paveiksle pateikia stereo garso įrašo signalogramą. Naudojamas tik kairysis kanalas, nes jame įterpiamas vandens ženklas, dešinysis išliks nepakeistas ir įterpus paveikslėlį. 5.4 ir 5.5 paveiksluose pateikiami vandens ženklo binariniai atvaizdai įterpimo metu.



5.3 pav. Originalus stereo garso signalas

Vandens ženklą pasirinktas 32 x 32 taškų binarinis paveikslėlis. Kuo mažesnis įterpiamas dvejetainis atvaizdas, tuo jis silpniau įtakoja garso įrašo kokybės pasikeitimus po jo pažymėjimo. Nustatytas vandens ženklo dydis pasirinktas toks pats kaip literatūroje tiriamuose algoritmuose todėl, kad pristatomo metodo tyrimų rezultatai turėtų prasmę ir būtų lengvai palyginami. Įterpiamo vandens ženklo paveikslėlis – baigiamojo darbo autoriaus Oskaro Jieznio pirmosios vardo ir pavardės raidės.

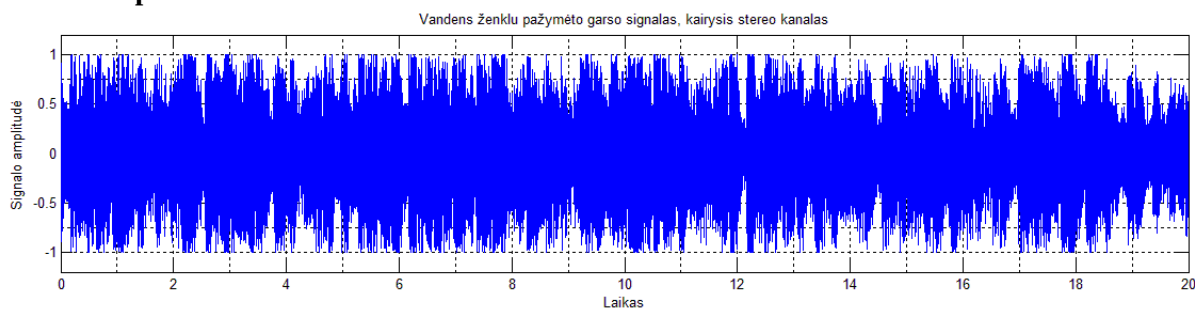


5.4 pav. Originalus vandens ženklas prieš įterpimą



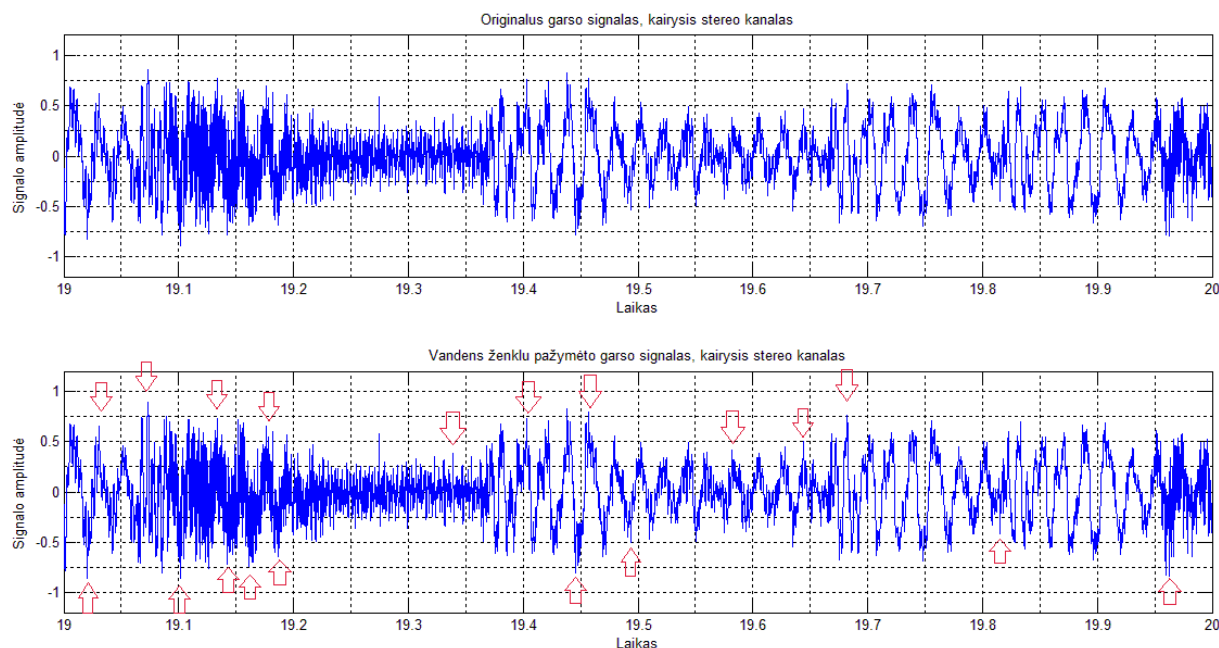
5.5 pav. Originalus vandens ženklas įterpimo metu, jau užšifruotas naudojant Arnoldo transformaciją

1. Jokio poveikio:



5.6 pav. Vandens ženklų pažymėtas garso įrašas. Jokio apdorojimo neatlikta

5.6 paveiksle pateikta binariniu atvaizdu pažymėto garso signalo signalograma. Ją palyginus su originaliojo garso kairiojo kanalo signalograma pateikta 5.3 paveiksle joks akivaizdus signalo skirtumas nežvelgtas. Norint išskirti garso signalo pokytį po vandens ženklo įterpimo, 5.7 paveiksle pateikiama 1 s. trukmės iškarpa iš viso garso įrašo. Jame gretimai atvaizduoti originalus ir pažymėtas signalai laiko etape tarp 19 ir 20 s. Raudonos rodyklės žymi pastebėtus skirtumus. Jie yra labai nedideli. Įterptas vandens ženklas tam tikrose signalo vietose pakeitė garso amplitudę – ji sumažėjo arba padidėjo. Vandens ženklo bitai buvo įterpiami į garso žemus dažnius.



5.7 pav. Originalaus ir pažymėto vandens ženklais garso įrašų signalo palyginimas laiko tarpe tarp 19 – 20 s.



5.8 pav. Nuskaitytas vandens ženklas iš neapdoroto garso įrašo

Rezultatai:

Normalizuota koreliacija (angl. *Normalized Correlation*) arba toliau $NC = 1$. Bitų klaidos norma (angl. *Bit error rate*) arba toliau $BER = 0 \%$. Signalų ir triukšmo santykis (angl. *Signal to Noise Ratio*) arba toliau $SNR = 31,6514 \text{ dB}$. Objektivus skirtumo įvertinimas (angl. *Objective difference grade*) arba toliau $ODG = -0,013$.

Kaip matoma 5.8 paveiksle nepaveikus garso įrašo jokiais apdorojimo priemonėmis, vandens ženklas gautas nepasikeitęs. Normalizuota koreliacija lygi 1, tai reiškia, kad lyginamas originalus ir nuskaitytas vandens ženklas visiškai sutampa. Bitų klaidos norma lygi 0%, reiškia klaidingų bitų nuskaitytame paveikslėlyje nerasta. Nuskaitytas vandens ženklas atitinka originalųjį.

Gautas SNR yra didelis, nes trikdžių ženklinant garso įrašą beveik nebuvo sukelta. Sumodeliuotas klausymo testo rezultatas ODG artimas nuliui, tai yra idealiam variantui. Kuo jis mažesnis, tuo daugiau triukšmų girdi klausytojas. Iš gautų rezultatų matoma, kad garso žymėjimo binariniu atvaizdu procesas nesukėlė didelių garso įrašo pakitimų, vandens ženklas nuskaitymas puikiai, o garso trikdžiai negirdimi. Lyginant 5.3 ir 5.6 paveikslėlius matome, kad garso signalas su įterptu vandens ženklu akivaizdžiai beveik nesiskiria.

2. Baltasis Gauso triukšmas (angl. *Additive white Gaussian noise*):



Rezultatai:

NC = 1;

BER = 0 %;

SNR = 17,8190 dB;

ODG = -3,797.

5.9 pav. Nuskaitytas vandens ženklas iš garso įrašo paveikto Baltuoju Gauso triukšmu

Nuskaitytas vandens ženklas visiškai identiškas originaliam. Garso įrašą paveikus baltuoju Gauso triukšmu aiškiai girdimi trikdžiai, tai mums parodo ir signalo ir triukšmo santykis, kuo jis mažesnis, tuo didesni triukšmai. Objektyvaus skirtumo įvertinimas labai prastas, tai reiškia, kad garso kokybei poveikis labai didelis, bet normalizuota koreliacija ir bitų klaidų norma yra visiškai nepakitę, vandens ženklo tai nepaveikė.

3. Gauso žemų dažnių filtras (angl. *Gaussian Low-pass filter*):



Rezultatai:

NC = 1;

BER = 0 %;

SNR = 31,4683 dB;

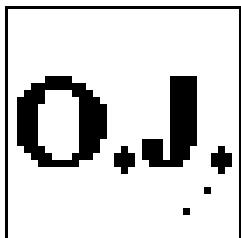
ODG = - 0,338.

5.10 pav. Nuskaitytas vandens ženklas iš garso įrašo paveikto Gauso žemų dažnių filtru

Nuskaitytas vandens ženklas visiškai identiškas originaliam. Paveikslėlis išliko nepasikeitęs. Gauta normalizuota koreliacija ir bitų klaidų norma tai patvirtina. Jokių klaidų nerasta, visi vandens

ženklų bitai atitinka pradinius. Signalo ir triukšmo santykis yra didelis, artimas vandens ženklų pažymėtam ir neapdorotam garso įrašui. Taip yra todėl, kad dalis pasikeitusių signalo vietų yra nufiltruota žemų dažnių filtro. Objektivaus skirtumo įvertinimas mažesnis nei 1 bandymo punkte, nes girdima kokybė šiek tiek prastesnė, tačiau tai labai sunkiai pajuntama. 5.10 paveiksle matoma, kad garso signalas labai nežymiai skiriasi nuo originalaus, tiesiog dalis garso modų pašalinta.

4. Kaizerio žemų dažnių filtras (angl. *Kaiser Low-pass filter*)



Rezultatai:

NC = 0,9978;

BER = 1,5625 %;

SNR = 0,3709 dB;

ODG = - 2,340.

5.11 pav. Nuskaitytas vandens ženklas iš garso įrašo paveikto Kaizerio žemų dažnių filtru

Panaudojus Kaizerio žemų dažnių filtrą garso įrašui ir nuskaičius vandens ženklą jis gautas šiek tiek pažeistas. 5.11 paveiksle matomas gautas vandens ženklų paveikslėlis, jame yra keletas aiškiai pastebimų juodų taškų. Normalizuota koreliacija ir bitų klaidų norma aiškiai apibūdina pokyčius. Kadangi 1,5625 % vandens ženklų bitų neatitinka originalo, o jo matmenys 32 x 32, tai reiškia visas paveikslėlio taškų skaičius yra 1024. Iš to aišku, jog klaidingų bitų yra 16. Signalo ir triukšmo santykis artimas nuliui, tai parodo, kad visas garsas tapo triukšmu ir yra labai pakitęs, bet klausant tie pokyčiai nėra taip jaučiami, todėl klausytojo poziciją geriausiai atspindi objektyvaus įvertinimo skirtumas. Jis rodo geresnę garso kokybę negu paveikus Baltuoju Gauso triukšmu, klausant visa tai puikiai atitinka, nors SNR rezultatai priešingi.

5. Garso diskretizacijos dažnio keitimas (angl. *Re-sampling*):



Rezultatai:

NC = 1;

BER = 0 %;

SNR = 20,8551 dB;

ODG = - 2,229.

5.12 pav. Nuskaitytas vandens ženklas iš garso įrašo kuriam atliktas diskretizacijos dažnio keitimas

Šiame tyrimo etape buvo keičiamas diskretizacijos dažnis iš 44,1 kHz į 22,05 kHz ir atgal. Nuskaitytas vandens ženklų paveikslėlis gautas analogiškas originaliam. Stebint jį neįžvelgiami jokie skirtumai, taip pat pagrindiniai rodikliai t.y. normalizuota koreliacija ir bitų klaidų normos lygios idealiam variantui. Ši apdorojimo priemonė nei kiek nepakenkė įterptam vandens ženklui,

nors signalo - triukšmo santykis ir objektyvaus įvertinimo skirtumai sumažėjo, o tai reiškia garso kokybės ženklų suprastėjimą, kuris jau girdimas ir klausytojui.

6. Kvantavimo keitimas (angl. *Requantizing*):



5.13 pav. Nuskaitytas vandens ženklas iš garso įrašo kuriam atliktas kvantavimo keitimas

Rezultatai:

NC = 1;

BER = 0 %;

SNR = 22,5941 dB;

ODG = - 3,09.

Atlikus kvantavimo keitimą iš 16 bit į 8 bit ir atgal, nuskaitytas vandens ženklas yra visiškai nepažeistas. Jis identiškas originaliam. Klaidingų bitų gauta 0 %. Šis apdorojimo metodas nei kiek nepaveikė vandens ženklo būsenos, nors garso įrašo signalo ir triukšmo santykis šiek tiek sumažėjo, tai reiškia signalo kokybė pablogėjo. Objektyvaus skirtumo įvertinimas pasikeitė labiau, todėl ir klausant garso įrašo kokybė gerokai prastesnė, tačiau įterptam paveikslėliui tai įtakos neturėjo.

7. MP3 spūda (angl. *MP3 compression*) į 32 kbps ir 16 kbps.

5.1 lentelė Bandymo rezultatai pakeitus garso formatą iš WAV į MP3 32kbps ir 16kbps, bei atgal į WAV.

Duomenys iš MP3 32 kbps	Duomenys iš MP3 16 kbps
 5.14 pav. Nuskaitytas vandens ženklas iš garso įrašo kuriam atliktas format keitimas į MP3 32kbps ir atgal į wav	 5.15 pav. Nuskaitytas vandens ženklas iš garso įrašo kuriam atliktas format keitimas į MP3 16kbps ir atgal į wav
Rezultatai: NC = 1; BER = 0 %; SNR = 17,9210 dB; ODG = -2,674.	Rezultatai: NC = 1; BER = 0 %; SNR = 12,7935 dB; ODG = -3,120.

Atlikus garso formato keitimą iš WAV į MP3 32kbps bei 16kbps ir vėl formatą pakeitus atgal į WAV, abiem atvejais nuskaityti vandens ženklai gauti identiški originalui. Jie visiškai nepasikeitė, pažymėtam garsui atlikus spūdos operaciją. Bitų klaidų norma abiem atvejais lygi 0, todėl klaidingų bitų nerasta, nors pats garso signalas labai pasikeitė. Prarasta didelė dalis aukštų dažnių ir tai jaučiamą jau klausant patį įrašą. Panaudojus MP3 32kbps gauta gerokai aukštesnė garso kokybė,

negu MP3 16kbps, tai puikiai atvaizduoja SNR ir ODG skirtumai. $SNR_{32kbps} > SNR_{16kbps}$, bei $ODG_{32kbps} > ODG_{16kbps}$.

8. Aidas (angl. *Echo*):



Rezultatai:

NC = 1;

BER = 0 %;

SNR = 19,5997 dB;

ODG = - 0,987.

5.16 pav. Nuskaitytas vandens ženklas iš garso įrašo kuriam pridėtas aidas

Pažymėtam vandens ženklui garso įrašui pridėjus aidą, nuskaitytas binarinis paveikslėlis liko nepažeistas ir yra identiškas originaliam. Rastas klaidingų bitų skaičius lygus 0, nors paties garso kokybė ir suprastėjo, tai parodo sumažėjęs signalo ir triukšmo santykis bei objektyvaus įvertinimo skirtumas, lyginant su paženklinytu garsu, kuriam neatlikti jokie apdorojimai. Trikdžiai nedideli, todėl praktiškai klausant juos sunku išgirsti, o vandens ženklo kokybė išliko nepaveikta.

5.6. Tyrimo rezultatų aptarimas

Norėdami tinkamai įvertinti gautus tyrimo rezultatus juos palyginame su moksliniuose straipsniuose pateikiamais duomenimis. Lyginimui sudarytos trys lentelės, kuriose pateikiami praktiškai tyrimais gauti, bei kitų mokslininkų straipsniuose aprašomi rezultatai.

5.2 lentelė Garso įrašo ženklinimo binariniu atvaizdu algoritmų pateiktų literatūros apžvalgoje bei patobulinto ir praktiškai išbandyto algoritmų testavimo rezultatai

Atakos tipas	Mūsų pristatytas patobulintas algoritmas	Adaptivus algoritmas naudojantis vienietinės vertės išskyrimą [18]	Algoritmas naudojantis diskrečiąją bangelių transformaciją [19]	Normuotos erdvės, negirdimas algoritmas [20]	Neturintis nuostolių ir naudojantis „α“ statistinę moduliaciją algoritmas [21]
Jokio atakos	NC = 1 BER = 0 %	NC = 1 BER = 0 %	-	NC = 1 BER = 0 %	NC = 1 BER = 0 %
Baltasis Gauso triukšmas	NC = 1 BER = 0 %	NC = 1 BER = 0 %	NC = 0,938 BER = - %	NC = 1 BER = 0 %	NC = 0,92 BER = 9,2 %
Gauso žemų dažnių filtras	NC = 1 BER = 0 %	NC = 0,9993 BER = 0 %	-	NC = 1 BER = 0 %	NC = 0,82 BER = 9,11 %
Kaizerio žemų dažnių filtras	NC = 0,9978 BER = 1,5625 %	-	-	NC = 1 BER = 0 %	-
Garso diskretizacijos dažnio keitimas	NC = 1 BER = 0 %	NC = 0,9854 BER = 2 %	-	NC = 1 BER = 0 %	NC = 0,89 BER = 4,79 %
Kvantavimo keitimas	NC = 1 BER = 0 %	NC = 1 BER = 0 %	-	NC = 1 BER = 0 %	NC = 1 BER = 0 %

MP3 suspaudimas 32 kbps	NC = 1 BER = 0 %	NC = 0,9907 BER = 1 %	-	NC = 1 BER = 0 %	NC = 0,69 BER = 16,44 %
MP3 suspaudimas 16 kbps	NC = 1 BER = 0 %	-	-	NC = 1 BER = 0 %	-
Aidas	NC = 1 BER = 0 %	NC = 0,9847 BER = 2 %	NC = 0,06 BER = - %	NC = 1 BER = 0 %	-

Atlikus patobulinto algoritmo kokybės tyrimus ir jo tvirtumo rezultatus pateikus 5.2 lentelėje matoma, kad siekiant pagerinti garso kokybę šiek tiek sumažėjo įterpto vandens ženklo atsparumas naudojant Kaizerio žemų dažnių filtrą, tačiau kitais bandymo etapais gauti vandens ženklo tvirtumo rezultatai yra optimalūs.

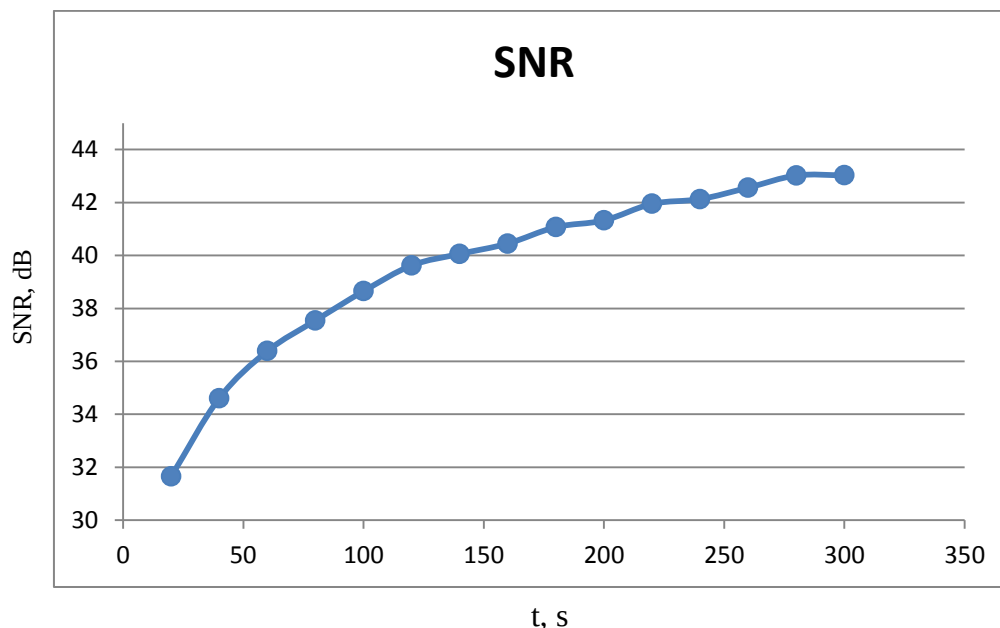
5.3 lentelė Garso įrašo pažymėto binariniu vandens ženklu signalo ir triukšmo santykis bei objektyvaus įvertinimo skirtumas naudojant literatūros apžvalgoje pristatytus ir patobulintąjį algoritmus

Algoritmai	Signalas – triukšmo santykis (SNR), dB	Objektyvaus skirtumo įvertinimas (ODG)
Mūsų pristatytas patobulintas algoritmas	31,65	-0,013
Adaptivus algoritmas naudojantis vienietinės vertės išskyrimą [18]	22,11	- 0,700
Algoritmas naudojantis diskrečiąją bangelių transformaciją [19]	25,03	0
Normuotos erdvės, negirdimas algoritmas [20]	22,46	- 0,530
Neturintis nuostolių ir naudojantis „α“ statistinę moduliaciją algoritmas [21]	33,14	-

5.3 lentelėje pateikti patobulintu bei literatūroje pristatomais algoritmais paženklintų garso įrašų kokybės įvertinimai. Palyginus gautus rezultatus aiškiai matoma, kad pristatomo algoritmo signalo – triukšmo santykis padidėjo lyginant su pradiniu jo variantu – „normuotos erdvės, negirdimo“ algoritmu gautu rezultatu. SNR pokytis yra: $31,65 - 22,46 = 9,19$ dB. Prieauglis yra didelis ir tai reiškia, kad sumažėjo triukšmai atsirandantys vandens ženklo įterpimo metu.

Objektyvaus skirtumo įvertinimas yra subjektyvaus klausymo testo rezultato atitikmuo, tik jis gaunamas klausymo testą modeliuojant kompiuteriu. Modeliavimo metu neapibrėžiamas subjektyvaus testo dalyvių skaičius, nes gautas rezultatas priklauso nuo paties garso įrašo savybių. Maksimali ir geriausia garso kokybę apibūdinanti reikšmė yra 0. Pagal 5.3 lentelės duomenis mūsų patobulintu garso žymėjimo binariniu atvaizdu algoritmų gaunami rezultatai labai arti optimaliems. Atlikus aptartus algoritmo patobulinimus gautas geresnis ODG rezultatas: $- 0,013 - (- 0,53) = 0,517$. Kaip matoma objektyvaus įvertinimo skirtumas padidėjo 0,4. Šis prieauglis reiškia, kad patobulinus

vandens ženklavimo algoritmą ženkliai sumažėjo girdimi trikdžiai atsiradę po vandens ženklo įterpimo. Pakeisti originalaus garso bitai tapo praktiškai negirdimi žmogaus ausiai, o tai ypatingai svarbu slaptai ženklinant muzikos kūrinius.



5.17 pav. Signalų – triukšmo santykio priklausomybė gauta garso įrašą pažymėjus binariniu atvaizdu, naudojant patobulintą vandens ženklavimo algoritmą

Pažymėjus garsą vandens ženklu buvo nustatytas signalų – triukšmo santykis, tačiau šis dydis nėra pastovus. Buvo nuspręsta išmatuoti jo priklausomybę nuo garso signalo trukmės. Pasirinktas laiko intervalas 20 – 300 s. Maksimali įrašo trukmė yra 5 minutės, nes įprastai internete platinami ar radijuje grojantys muzikos kūriniai trunka nuo 3 iki 5 minučių. Bandymo metu buvo naudojamas 20 s. trukmės įrašas, kuris buvo apdorojamas prieš tai aptartame tyrime. Signalų ilgis buvo didinamas pasirinktą įrašą kopijuojant, nes tik taip galima tinkamai įvertinti kokybės pokyčius priklausančius nuo garso įrašo trukmės. Šiam bandymui vientisas ilgas muzikos kūrinys nebūtų tinkamas dėl to, kad jo signalograma visą grojimo laikotarpį kinta. Gauti rezultatai pateikti 5.17 paveiksle atvaizduotoje kreivėje. Darant šį bandymą vandens ženklo bitų skaičius išliko pastovus, keitėsi tik garso pavyzdžių kiekis. Pateiktoje kreivėje matoma, jog didėjant garso įrašo trukmei, didėja signalų – triukšmo santykis, o tai reiškia, kad ženklavimo metu atsirandantys triukšmai mažiau įtakoja garso kokybės pokyčius. Iš gautų rezultatų galima spręsti, kad pristatyto patobulinto garso ženklavimo binarinio atvaizdo vandens ženklu algoritmo kokybiniai parametrai labai priklauso nuo garso įrašo ilgio. Didėjant trukmei - mažėja iškraipymai atsirandantys ženklavimo metu.

IŠVADOS

- Vandens ženklo įterpimui panaudotas tik kairysis stereo kanalas bei visas garso įrašo ilgis pagerino garso įrašo signalo – triukšmo santykio bei kompiuteriu modeliuojamo klausymo testo rezultatus. Atlikus šiuos pakeitimus vandens ženklo įterpimo metu sukurti triukšmai sumažėjo ir tapo nebegirdimi klausytojui. Paženklinto garso kokybė pagerėjo. Vandens ženklo tvirtumas išliko toks pats kaip ir prieš algoritmo tobulinimą, išskyrus vieną atvejį, kai panaudotas Kaizerio žemų dažnių filtras, ir tvirtumas tapo mažesnis.
- Panaudota diskrečioji bangelių transformacija atskiria aukšto ir žemo dažnio garso signalo sritis. Pasirinkti žemieji dažniai, nes jie atsparūs signalų apdorojimams – metodas didina vandens ženklo tvirtumą.
- Pristatomu algoritmu pažymėto garso kokybė yra priklausoma nuo jo įrašo trukmės. Didėjant signalo ilgiui, gerėja ir signalo kokybė, mažėja atsirandantys triukšmai. Ypatingai garso kokybė kinta, kai signalo trukmė yra mažesnė negu 50 s. Mažėjant įrašo trukmei – įterpti vandens ženklo bitai turi didesnę įtaką neigiamiems kokybės pokyčiams.
- Literatūros apžvalgoje pateikto algoritmo patobulinimai yra itin svarbūs ir suteikia galimybę egzistuoti negirdimo garso žymėjimo binariniu atvaizdu metodui, kuris užtikrina vandens ženklo tvirtumą ir galimybę būti nuskaitytam po garso apdorojimo. Algoritmas tinkamas naudoti muzikos kūrinių apsaugai nuo nelegalaus kopijavimo bei kūrinio autentiškumo užtikrinimui. Pristatytas algoritmas atitinka visus darbo užduotyje keliamus reikalavimus.

LITERATŪROS IR INFORMACINIŲ ŠALTINIŲ SĄRAŠAS

1. Katzenbeisser, S.; Petitcolas, F. 2000. *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House, Boston. 99 – 103. ISBN 1-58053-035-4.
2. *Digital Watermarking and Stenography* [interaktyvus]. 2008m. Ingemar J.Cox , Matthew L. Miller, Jefrey A. Bloom, Ton Kalker [žiūrėta 2013 m. sausio 10d.] Prieiga per internetą: <<http://www.amazon.com/Watermarking-Steganography-Kaufmann-Multimedia-Information/dp/0123725852> >
3. Al – Haj, A. M. 2010. *Advanced Techniques in Multimedia Watermarking: Image, Video and Audio Applications*. Hershey: IGI Global. United States.128 – 139. ISBN 978-1-61520-904-0
4. Arnold, M.; Schmucker, M.; Wolthusen, S. D. 2003. *Techniques and Applications of Digital Watermarking and Content Protection*. Boston, London: Artech House.
5. Wang, J. Y.; Lai, M. S.; Liang, K. W.; Chang, P. C. 2006. *Adaptive Wavelet Quantization Index Modulation Technique for Audio Watermarking*. Taipei, Taiwan.
6. Khan, M. I. ; Sarker, M. I. H.; Deb, K.; Furhad, H. 2012. A new audio watermarking method based on discrete cosine transform with gray image in *International Journal of Computer Science & Information Technology*, Chittagong-4349, Bangladesh.
7. Wang, X.; Wang, P.; Zhang, P.; Xu, S.; Yang, H. 2012. A norm-space, adaptive, and blind audio watermarking algorithm by discrete wavelet transform in *Signal Processing volume 93*, Tsinghua University, Beijing 100084, China
8. Thilo, T. 1999. *Perceptual Audio Quality Assessment using a Non-Linear Filter Bank*, [žiūrėta 2014 kovo 15 d.]. Prieiga per internetą: <<http://www.mp3-tech.org/programmer/docs/scriptHF021.pdf>>
9. Matheson, L. R.; Mitchell, S. G.; Shamoan, T. G.; Tarjan, R. E.; Zane, F. 1998. *Robustness and Security of Digital Watermarks*. Sunyvale, USA. 8 – 10.
10. Goenka, V. K.; Patil, P. K. 2012. *Overview of Audio Watermarking Techniques*. Sevagram, India. 68 – 69. ISSN 2250-2459.
11. Ali, M. A. 2010. *Advanced Techniques in Multimedia Watermarking: Image, Video and Audio Applications*. Jor-dan. 126–140.
12. Breed, G. 2003. *Bit Error Rate: Fundamental Concepts and Mea-surment Issues* [žiūrėta 2014 kovo 16 d.]. Prieiga per internetą: <http://www.highfrequencyelectronics.com/Archives/Jan03/HFE0103_Tutorial.pdf>.
13. Li, M.; Liang, T.; He, Y. 2013. Arnold Transform Based Image Scrambling Method, in *3rd International Conference on Multimedia Technology (ICMT 2013)*. Atlantis press. 1309 – 1316.
14. Shafiul, A. 2008. *Effect of Additive White Gaussian Noise (AWGN) on the Transmitted Data*. [žiūrėta 2014 balandžio 3 d.]. Prieiga per internetą: <http://atmshafiulalam.webs.com/IDC-Ex-3-additive_white_Gaussian_noise.pdf>

15. Pu, C.; Harris, J. G. 1998. Theory and implementation of a Gaussian decay low-pass filter, in *Circuits and Systems, 1998. ISCAS'98. Proceedings of the 1998 IEEE International Symposium on*, vol. 1. Florida. 193–196.
16. Oppenheim, A. V.; Schafer, R. W.; Buck, J. R. 1998. *Discrete – Time Signal Processing*. Prentice-Hall inc. Upper Saddle River, New Jersey. 140 – 149, 377 - 390. ISBN 0-13-754920-2.
17. Jacaba, S. J. 2001. *Audio Compression Using Modified Discrete Cosine Transform: The MP3 Coding Standart*. Diliman, Quezon City. 2 – 4.
18. Vivekanada, B., K.; Indranil, S.; Abhijit, D. 2010. *An adaptive audio watermarking based on the singular value decomposition in the wavelet domain*. Kharagpur 721302, India. 1 – 12.
19. Al-Haj, A.; Mohammad, A.; Bata, L. 2011. DWT-Based Audio Watermarking, in *The International Arab Journal of Information Technology*, Vol. 8, No. 3, July 2011. Jordan. 326 – 333.
20. Wang, X.; Wang, P.; Zhang, P.; Xu, S.; Yang, Huazhong. 2013. A norm-space, adaptive, and blind audio watermarking algorithm by discrete wavelet transform, in *Signal Processing 93 (2013)*. China. 913 – 922.
21. Dhavale, S. V.; Deodhar, R. S.; Patnaik, L. M. 2012. Loseless Audio Watermarking Based On The Alpha Statistic Modulation, in *The International Journal of Multimedia & Its Applications (IJMA) Vol.4, No.4, August 2012*. India. 109 – 119.
22. Smith, L. D. 2003. *Counterfeiters And Sir William Congreve`s Triple Paper Colored Watermarks* [žiūrėta 2014 kovo 20 d.]. Prieiga per internetą: <<http://www.motherbedford.com/watermarks/Watermark1B6.htm>>.
23. Johson, N. F. 2012. *Information Hiding: Steganography & Digital Watermarking* [žiūrėta 2014 kovo 20 d.]. Prieiga per internetą: <<http://www.jjtc.com/Steganography/>>.
24. Wang, F.; Pan, J.; Jain, L. C. 2009. *Innovations in Digital Watermarking Techniques*. Berlin. 16 p.
25. Trappe, W.; Wu, M.; Wang, Z. 2003. Anti-collusion Fingerprinting for Multimedia, in *IEEE Transactions on Signal Processing*, 51(4). 1069 – 1087
26. Cox, I.; Miller, M. 2001. Electronic watermarking: The first 50 years, in *Proceedings of the IEEE Workshop on Multimedia Signal Processing*. 225 – 230.
27. Termont, P.; De Stycker, L.; Vandewege, J.; Beeck, M.; Haitsma, J.; Kalker, T. 2000. How to achieve robustness against scaling in a real – time Digital watermarking system for broadcast monitoring, in *Proc. IEEE International Conference on Image Processing*, Vancouver, Canada. 407 – 410.
28. Zwicker, E.; Fastl, H. 1999. *Psychoacustics: Facts and models*. Berling: Springer –Verlag.
29. Brandenburk, K.; Sporer, T. 1992. NMR and masking flag: Evaluation of quality using perceptual criteria, in *Proceedings of the International Audio Engineering Society Conference on Audio Test and Measurement*. 169 – 179.
30. Chou, J.; Ramchandran, K.; Ortega, A. 2001. High capacity audio data hiding for noisy channels, in *Proceedings of the International Conference on Information Technology: Coding and Computing*. 108 – 111.

31. Fridrich, J.; Goljan, M.; Du, R. 2002. Loseless data emgedding – New paradigm in digital watermarking, in *Applied Signal Processing*, (2). 185 – 196.
32. Bender, W.; Gruhl, D.; Morimoto, N.; Lu, A. 1996. Techniques for data hiding, in *IBM Systems Journal*, 35(3). 313 – 336.
33. Xu, C.; Wu, J.; Sun, Q.; Xin, K. 1999. Applications of watermarking technology in audio signals, in *Journal of the Audio Engineering Society*. *Audio Engineering Society*, 47(10).
34. Kirk, B. 2005. *Singular Value Decomposition Tutorial*. [žiūrėta 2014 balandžio 23 d.]. Prieiga per internetą: <http://www.ling.ohio-state.edu/~kbaker/pubs/Singular_Value_Decomposition_Tutorial.pdf>.

PRIEDAI

- 1 priedas. Binarinio atvaizdo įterpimo į garso įrašą programos kodas**
- 2 priedas. Binarinio atvaizdo išgavimo iš garso įrašo programos kodas**
- 3 priedas. Pažymėto binariniu atvaizdu garso įrašo apdorojimo programos kodas**
- 4 priedas. Pažymėto binariniu atvaizdu garso įrašo testavimo programos kodas**

1 priedas. Binarinio atvaizdo įterpimo į garso įrašą programos kodas

```
% Binarinio vaizdo vandens ženklų įterpimo skaitmeninio garso įrašo autentiškumui
užtikrinti taikymai ir tyrimai

% Oskaras Jieznys MISfm-12

% Normuotos erdvės, adaptyvus ir nematomas vandens ženklinimo algoritmas naudojant
diskrečią bangelių transformaciją
% Vandens ženklo įterpimas

clear all;
close all;
clc;

% Įvesties failai, pasirenkami garso įrašo bei binarinio paveikslėlio
% failai
audio_input = uigetfile('*.wav','Garso failas, kuris bus zenklinamas vandens zenklu
(WAV)');
watermark_input=uigetfile('*.bmp','Binarinio atvaizdo failas (BMP)');

% Išvestis. Paženklintas garso įrašas ir suformatuotas vandens ženklas.
output_marked='watermarked_audio.wav';
wm_output='watermark_scaled.bmp';

% Nuskaitom garso failą ir nustatom galimą vandens ženklo dydį.
[data,Fs,nbits]=wavread(audio_input);
data_graf=data;
% Kadangi garso įrašas yra stereo, tai jame du kanalai, padarom kaip viena
% matricą ir bendrai įterpiam vandens ženklą
data1=data(:,1);
data2=data(:,2);

data_ilgis=length(data1);
data=data1(1:data_ilgis);

% *****
% 1 etapas: Dviejų lygių db4 bangelių transformacija.
[cA,cD] = dwt(data,'db4'); %1 lygis
[cAA,cDD] = dwt(cA,'db4'); %2 lygis
coef = cAA;
coef_length = length(coef);

% *****
% 2 etapas: Gautus koeficientus segmentuojame į M x M matricą, priklausomai
% nuo vandens ženklo dydžio. M x M yra vandens ženklo pikselių skaičius.

% Nuskaitom vandens ženklo paveikslėlį.
wm1=imread(watermark_input);
z1=size(wm1,1);
z2=size(wm1,2);
%wm_temp=rgb2gray(wm1);

% Vandens ženklo bitus sumaišom su arnoldo transformacija
wm1 = im2bw(wm1,0.65);
wm_scratched = arnold(wm1,1);
wm_restored = iarnold(wm_scratched,1);

% Atvaizduojam vandens ženklo paveikslėlius
figure;
subplot(3,1,1); imshow(watermark_input);
title('Pradinis vandens ženklas'); axis('image');

subplot(3,1,2); imshow(wm1);
```

```

title('Binarinis vandens zenklas'); axis('image');

subplot(3,1,3); imshow(wm_scratched);
title('Uz koduotas vandens zenklas'); axis('image');

% Blokų skaičius
block_count = z1*z2;
% kiek koeficientų nuimta.
coef_count=0;

% Mažinam koeficientų ilgį, kad būtų lyginis skaičius
while mod(coef_length,block_count) ~=0
    coef_length=coef_length-1;
    coef_count=coef_count+1;
end

% Pakeičiam koeficientų skaičius
coef = coef(1:coef_length);

% Pagal vandens ženklo dydį nustatom bloko dydį.
block_size = length(coef)/(z1*z2);

% *****
% 3 etapas. Skaičiuojam kiekvieno kadro vektoriaus normas, kurios lygios kiekvieno
% bloko vektoriaus elementų kvadratų sumos šakniai.

x=1;
last_block = block_size;
norma = 1:block_count;
u = {1:1:block_count};

% Ciklas užpildo kintamąjį norma su gautomis normų reikšmėmis.
for i=1:block_count,

    norma(i) = norm(coef(x:1:last_block));
    u{i}=transpose(coef(x:(x+1):last_block))/norma(i);
    u{i} = transpose(coef(x:1:last_block))/norma(i);
    last_block = last_block+block_size;
    x = x+block_size;

end

% *****
% 4 etapas. Kvantavimas

% Pasirenkam kvantavimo žingsnį. Nuo jo priklauso vandens ženklo tvirtumas,
% bei ženklo girdimumo savybės. Kuo didesnis kvantavimo žingsnis, tuo
% vandens ženklas atsparesnis apdorojimui, tačiau labiau girdimas pačiam
% garso įrašui. Mažinant kvantavimo žingsnį mažėja vandens ženklo atsparumas
% garso signalo apdorojimui, tačiau jis tampa mažiau girdimas klausytojui.
% Kvantavimo indeksą renkamės 0,53, nes būtent toks pasirinktas jau tiriant
% pateiktą algoritmą.

q_index = 0.65;

% Skaičiuojam "e" ir "d" kintamuosius reikalingus kvantavimui.

e = 0:1:block_count;
d = 0:1:block_count;

% Ciklas užpildo kintamąjį norma su gautomis normų reikšmėmis.
for i=1:block_count,
    e(i) = floor(norma(i) / q_index);
    d(i) = mod(norma(i),q_index);

```

```

end

% Tikrinam sąlyga, užkoduoto vandens ženklo paveikslėlio reikšmė lygi 1 ar
% 0. Anksčiau deklaruoti z1 ir z2 yra paveikslėlio kraštinių ilgiai
% pikseliais.

% Aprašom modifikuota norma.
norma_ = 0:1:block_count;
counter = 1;

for i=1:z1,
    for j=1:z2,

        % Pirma sąlyga, jei užkoduoto vandens ženklo bitas lygus 1
        if wm_scratched(i,j) ==1

            if mod(e(counter),2)==1
                norma_(counter)= norma(counter)+(q_index/2)-mod(norma(counter),q_index);
            end

            if mod(e(counter),2)==0 && d(counter) > (q_index/2)
                norma_(counter)= norma(counter)+q_index+(q_index/2)-
mod(norma(counter),q_index);
            end

            if e(counter)==0 && d(counter) < (q_index/2)
                norma_(counter)= norma(counter)+q_index+(q_index/2)-
mod(norma(counter),q_index);
            end

            if mod(e(counter),2)==0 && d(counter) < (q_index/2) && e(counter)~=0
                norma_(counter)= norma(counter)-q_index+(q_index/2)-
mod(norma(counter),q_index);
            end

            counter = counter+1;

        end

        % Antra sąlyga, jei užkoduoto vandens ženklo bitas lygus 0

        if wm_scratched(i,j) ==0

            if mod(e(counter),2)==0
                norma_(counter)= norma(counter)+(q_index/2)-mod(norma(counter),q_index);
            end

            if mod(e(counter),2)==1 && d(counter) > (q_index/2)
                norma_(counter)= norma(counter)+q_index+(q_index/2)-
mod(norma(counter),q_index);
            end

            if mod(e(counter),2)==1 && d(counter) < (q_index/2)
                norma_(counter)= norma(counter)-q_index+(q_index/2)-
mod(norma(counter),q_index);
            end

            counter = counter+1;

        end

    end

end

% 5 etapas. Naudodami gautas modifikuotas vektoriaus normas mes galime

```

```

% gauti modifikuotus kadrus.

coef_={1:1:block_count};

for i=1:block_count,

coef_{i}=norma_(i)*transpose(u{ i}) ;

end

% Apjungiam koeficientų blokus į vieną matricą.
coef_=cell2mat(coef_);
coef_=reshape(coef_,[],1);

%Kad atgautume prarastus koeficientus, juos prijungiame iš cAA, kur tie
%koeficientai nebuvo modifikuoti vandens ženklų.
coef_=vertcat(coef_,cAA(coef_length+1:length(cAA)));
cA_=idwt(coef_,cDD,'db4');

% Kadangi čia gaunam cA_ vienu ilgesnį, tai sumažinam.
cA_=cA_(1:length(cA_));

% Gaunam vandens ženklų pažymėtą garsi įrašą, vientisą, mono signalas.
watermarked_audio = idwt(cA_,cD,'db4');
watermarked_audio=vertcat(watermarked_audio,data1(length(watermarked_audio+1):length(data
1)-1 ));
watermarked_audio=horzcat(watermarked_audio,data2);

% Garso įrašą įrašom į projekto direktoriją.
wavwrite(watermarked_audio,Fs,nbits,output_marked);

%Atvaizduojam garso signalą
L=length(data_graf);
t= linspace(0, L/Fs, L);

L_w=length(watermarked_audio);
t_w= linspace(0, L_w/Fs, L_w);
%figure,
%plot(t, watermarked_audio); title('Garso signalas'); xlabel('Laikas'); ylabel('Signalų
amplitudė');
figure,
subplot(2,1,1); plot(t, data_graf); title('Originalus garso signalas'); xlabel('Laikas');
ylabel('Signalų amplitudė');
subplot(2,1,2); plot(t_w, watermarked_audio); title('Vandens ženklų pažymėto garso
signalas'); xlabel('Laikas'); ylabel('Signalų amplitudė');
grid on;

```

2 priedas. Binarinio atvaizdo išgavimo iš garso įrašo programos kodas

```

% Binarinio vaizdo vandens ženklų įterpimo skaitmeninio garso įrašo autentiškumui
užtikrinti taikymai ir tyrimai

% Oskaras Jieznys MISfm-12

% Normuotos erdvės, adaptyvus ir nematomas vandens ženklinimo algoritmas naudojant
diskrečią bangelių transformaciją
% Vandens ženklo įterpimas

clear all;
close all;
clc;

% Įvesties failai, pasirenkamas garso įrašas paženklintas vandens ženklų.

```

```

audio_input = uigetfile('*.wav','Garso failas, kuris bus zenklinamas vandens zenklu
(WAV)');
% Išvestis. Nuskaitytas vandens ženklas.
wm_output='watermark_detected.bmp';

% Nuskaitom garso failą ir nustatom galimą vandens ženklo dydį.
[data,Fs,nbits]=wavread(audio_input);

% Kadangi garso įrašas yra stereo, tai jame du kanalai, mes naudosim tik
% kairįjį vieną garso kanalą, todėl jį ir pasirenkam:
data1=data(:,1);
data_ilgis=floor(length(data1));
data=data1(1:data_ilgis);

% *****
% 1 etapas: Dviejų lygių db4 bangelių transformacija.

[cA,cD] = dwt(data,'db4'); %1 lygis
[cAA,cDD] = dwt(cA,'db4'); %2 lygis
coef = cAA;
coef_length = length(coef);

% *****
% 2 etapas: Gautus koeficientus segmentuojame į M x M matricą, priklausomai
% nuo vandens ženklo dydžio. M x M yra vandens ženklo pikselių skaičius.

% Nuskaitom vandens ženklo paveikslėlį, taip gauname mums reikalingų
% skaičių. Jis gaunamas pagal paveikslėlio dydį.
[wml=imread(watermark_input);
%z1=size(wml,1);
%z2=size(wml,2);

% Kadangi bandymą darom su nustatytų matenų paveikslėliu, tai išvengiant
% vandens ženklo dydžio nuskaitymo nuo pačio originalaus vandens ženklo,
% rankiniu būdu nustatome, kad jo dydis yra M x M = 32 x 32
% Blokų skaičius
z1=32;
z2=32;
block_count = z1*z2;

%kiek koeficientų nuimta.
koef_count=0;

%Mažinam koeficientų ilgį, kad būtų lyginis skaičius
while mod(coef_length,block_count) ~=0
    coef_length=coef_length-1;
    coef_count=coef_count+1;
end

%Pakeičiam koeficientų skaičius
coef = coef(1:coef_length);

% Pagal vandens ženklo dydį nustatom bloko dydį.
block_size = length(coef)/(z1*z2);

% *****
% 3 etapas. Skaičiuojam kiekvieno kadro vektoriaus normas, kurios lygios kiekvieno
% bloko vektoriaus elementų kvadratų sumos šakniai.
x=1;
last_block = block_size;
norma = 1:block_count;
u={1:1:block_count};

% Ciklas užpildo kintamąjį norma su gautomis normų reikšmėmis.
for i=1:block_count,

```

```

        norma(i) = norm(coef(x:1:last_block));
        %u(i)=transpose(coef(x:(x+1):last_block))/norma(i);
        u{i} = transpose(coef(x:1:last_block))/norma(i);
        last_block = last_block+block_size;
        x = x+block_size;

end

% Apibrėžiam kvantavimo indeksą.
q_index = 0.65;
% Deklaruojam e .
e = 0:1:block_count;

% Užpildom e reikšmes.
for i=1:block_count,
    e(i) = floor(norma(i) / q_index);
end

%Nuskaitom sumaišyto vandens ženklo bitus.
wm_scratched=[1:1:z1;1:1:z2];
counter=1;

for i=1:z1
    for j=1:z2
        if mod(e(counter),2)==0
            wm_scratched(i,j)=0;
        end

        if mod(e(counter),2)==1
            wm_scratched(i,j)=1;
        end
        counter=counter+1;
    end
end

% Sumaišyto vandens ženklo bitams atliekam atvirkštinę Arnoldo
% transformaciją.
wm_restored=iarold(wm_scratched,1);

% Atvaizduojam gautus rezultatus
figure;
subplot(2,1,1); imshow(wm_scratched);
title('Nuskaitytas užšifruotas vandens ženklas'); axis('image');
subplot(2,1,2); imshow(wm_restored);
title('Iš koduotas vandens ženklas'); axis('image');

% Įrašiom iš koduotą vandens ženklą į failą
imwrite(wm_restored,wm_output,'bmp');

```

3 priedas. Pažymėto binariniu atvaizdu garso įrašo apdorojimo programos kodas

% Binarinio vaizdo vandens ženklų įterpimo skaitmeninio garso įrašo autentiškumui užtikrinti taikymai ir tyrimai

% Oskaras Jieznys MISfm-12

```

% Normuotos erdvės, adaptyvus ir nematomas vandens ženklinimo algoritmas naudojant
diskrečią bangelių transformaciją
% Garso įrašo paženklinto vandens ženklų apdorojimas.
% Skripto veikimas:
% 1 pasirenkam jau pažymėtą vandens ženklų garso įrašą.
% 2 Programa pati atlieka trijų tipų apdorojimą, pridėda baltąjį Gauso
% triukšmą, filtruoja naudojant Gauso žemų dažnių bei Kaizerio žemų dažnių

```

```

% filtrus. Gautis rezultatus išsaugo atsikruose garso įrašų failuose.

% Išvalom ekraną ir kintamuosius
clear all;
clc;

% Pasirenkam garso failą paženklinatą vandens ženklų.
audio_input = uigetfile('*.wav','Vandens ženklų paženklintas garso failas (WAV)');
[data,Fs,nbits]=wavread(audio_input);

% Pridedam 18dB SNR baltąjį gauso triukšmą.
y = awgn(data(:,,:),18,'measured') ;

% Garso įrašą įrašom į projekto direktoriją.
wavwrite(y,Fs,nbits,'watermarked_audio_awgn.wav');

%*****

% Gauso žemų dažnių filtras. Sukuriam filtrą.
h = fspecial('gaussian',[3 3],0.3);

% Atvaizduojam sukurtą filtrą.
figure,surfc(h),title('Gauso žemų dažnių filtras');

% Filtruojam garso įrašą.
gaussian_lowpass_filter = filter2(h,data(:,:));

% Atvaizduojam garso įrašą prieš ir po Gauso žemų dažnių filtravimo
figure,
subplot(2,1,1),plot(data(:,:)),title('Originalus garso įrašas');
subplot(2,1,2),plot(gaussian_lowpass_filter(:,:)),title('Garso įrašas po Gauso žemų
dažnių filtro');

% Garso įrašą įrašom į projekto direktoriją.
wavwrite(gaussian_lowpass_filter,Fs,nbits,'watermarked_audio_gaussian.wav');

%*****

% Kaizerio žemų dažnių filtras. Pradinis dažnis 10kHz, galutinis dažnis
% 12kHz. Pradžios bangos kraštinė 0,05 , pabaigos bangos kraštinė 0,01.

c = kaiserord([10000 12000],[1 0],[0.05 0.01],44100,'cell');
b = fir1(c{:});

% Atvaizduojam Kaizerio žemų dažnių filtrą.
[H,f] = freqz(b,1,1024,44100);
figure,
plot(f,abs(H)),title('Kaizerio žemų dažnių filtras'), grid on

% Filtruojam pažymėtą garso įrašą naudojant sukurtą Kaizerio filtrą.
kaiser_lowpass_filter = filter(b,1,data(:,:));

% Atvaizduojam originalų ir filtruotą garso įrašus.
figure,
subplot(2,1,1),plot(data(:,:)),title('Originalus garso įrašas');
subplot(2,1,2),plot(kaiser_lowpass_filter(:,:)),title('Garso įrašas po Kaizerio žemų
dažnių filtro');

% Įrašom gautą signalą į projekto direktoriją.
wavwrite(kaiser_lowpass_filter,Fs,nbits,'watermarked_audio_kaiser.wav');

```

4 priedas. Pažymėto binariniu atvaizdu garso įrašo testavimo programos kodas

```
% Binarinio vaizdo vandens ženklų įterpimo skaitmeninio garso įrašo autentiškumui
užtikrinti taikymai ir tyrimai

% Oskaras Jieznys MISfm-12

% Normuotos erdvės, adaptyvus ir nematomas vandens ženklinimo algoritmas naudojant
diskrečią bangelių transformaciją
% Vandens ženklo tvirtumo po apdorojimo testavimas.

% Pradžia. Pasirenkame du vandens ženklus. Originalų ir nuskaitytą, kad
% juos galėtume palyginti.
clear all;
close all;
clc;

% Įvesties failai.
% Pasirenkam originalų ir nuskaitytą vandens ženklo failus, kad galėtume
% palyginti juos.
original_watermark = uigetfile('*.bmp','Originalus vandens ženklo failas (BMP)');
read_watermark = uigetfile('*.bmp','Nuskaityto iš garso įrašo vandens ženklo failas
(BMP)');
original_watermark=imread(original_watermark);
read_watermark=imread(read_watermark);

% Originalaus vandens ženklo dydis
z1=size(original_watermark,1);
z2=size(original_watermark,2);

%*****
%*****
% Skaičiuojam normalinę koreliaciją:
NC =
sum(read_watermark(:, :).*original_watermark(:, :))/sum(original_watermark(:, :).*original_w
atermark(:, :))
%*****
%*****
% Skaičiuojam Bit error ratio
[number, ratio] = biterr(original_watermark, read_watermark)
BER_ = number*100/(z1*z2)

%% SNR - signal to noise ratio skaičiavimas

% Pasirenkam originalų ir vandens ženklų pažymėtą garso įrašus palyginimui.
original_audio = uigetfile('*.wav','Originalus garso įrašas');
watermarked_audio = uigetfile('*.wav','Vandens ženklų pažymėtas garso įrašas');

[data_original, Fs1, nbits1]=wavread(original_audio);
[data_watermarked, Fs2, nbits2]=wavread(watermarked_audio);

%Atskiriam 2 kintamuosius reikalingus garso signalo amplitudei.
data_original1 = data_original;
data_watermarked1 = data_watermarked;

% Apjungiam abu kanalus į vieną, kad pilnai išmatuoti SNR.
data_original=vertcat(data_original(:,1),data_original(:,2));
data_watermarked=vertcat(data_watermarked(:,1),data_watermarked(:,2));

%vienam atvejui
%data_original = data_original(1:length(data_watermarked));
```

```

bitV=0; bitA = 0;

for i=1:length(data_original)

    bitV = bitV+(data_original(i))^2;
    bitA = bitA+ (data_original(i)-data_watermarked(i))^2;

end
%snr = 20*log(norm(original_watermark,'fro')/norm(original_watermark-
read_watermark,'fro'))
SNR =10*log10(bitV/bitA)

% Atvaizduojam originalų į pažymėtą garso signalus

L=length(data_original1);
t= linspace(0, L/Fs1, L);

L_w=length(data_watermarked1);
t_w= linspace(0, L_w/Fs1, L_w);
%figure,
%plot(t, watermarked_audio); title('Garso signalas'); xlabel('Laikas'); ylabel('Signalų
amplitudė');
figure,
subplot(2,1,1); plot(t, data_original1(:,1)); title('Originalus garso signalas, kairysis
stereo kanalas'); xlabel('Laikas'); ylabel('Signalų amplitudė'); grid on;grid minor;

subplot(2,1,2); plot(t_w, data_watermarked1(:,1)); title('Vandens ženklų pažymėto garso
signalas, kairysis stereo kanalas'); xlabel('Laikas'); ylabel('Signalų amplitudė');grid
on; grid minor; ylim([-0.5,0.5]);

```