KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

Juras Biliūnas

LSB STEGANOGRAFIJOS ALGORITMO TAIKYMAS VOIP PROTOKOLUI

Baigiamasis magistro darbas

Vadovas
prof. Algimantas Venčkauskas

KAUNAS, 2016

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

LSB STEGANOGRAFIJOS ALGORITMO TAIKYMAS VOIP PROTOKOLUI

Baigiamasis magistro darbas
Informacijos ir informacinių technologijų sauga (kodas 621E10003)

Vadovas
(parašas) prof. Algimantas Venčkauskas
(data)

Recenzentas
(parašas) doc. Tomas Adomkus
(data)

Projektą atliko
(parašas) Juras Biliūnas
(data)

KAUNAS, 2016

KAUNO TECHNOLOGIJOS UNIVERSITETAS

Informatikos protokolas

(Fakultetas)

Juras Biliūnas

(Studento vardas, pavardė)

Informacijos ir informacinių technologijų sauga, 621E10003

(Studijų programos pavadinimas, kodas)

„LSB steganografijos algoritmo taikymas VOIP protokolui“

AKADEMINIO SĄŽININGUMO DEKLARACIJA

20 16 m. gegužės 23 d.

Kaunas

Patvirtinu, kad mano **Juro Biliūno** baigiamasis projektas tema „LSB STEGANOGRAFIJOS ALGORITMO TAIKYMAS VOIP PROTOKOLUI“ yra parašytas visiškai savarankiškai, o visi pateikti duomenys ar tyrimų rezultatai yra teisingi ir gauti sąžiningai. Šiame darbe nei viena dalis nėra plagijuota nuo jokių spausdintinių ar internetinių šaltinių, visos kitų šaltinių tiesioginės ir netiesioginės citatos nurodytos literatūros nuorodose. Įstatymų nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs.

Aš suprantu, kad išaiškėjus nesąžiningumo faktui, man bus taikomos nuobaudos, remiantis Kauno technologijos universitete galiojančia tvarka.

(vardą ir pavardę įrašyti ranka) *(parašas)*

Biliūnas, J. „LSB steganografijos algoritmo taikymas VOIP protokolui“. Magistro baigiamasis projektas / vadovas prof. Algimantas Venčkauskas; Kauno technologijos universitetas, Informatikos fakultetas, Kompiuterių katedra.

Kaunas, 2016. 50 p.

SANTRAUKA

VOIP yra plačiausiai naudojama paslauga IP tinkle. Vaizdo ir balso pokalbiai yra nepamainoma priemonė tarptautinėms organizacijoms bendrauti tarp nutolusių departamentų ar tiekti palaikymo paslaugą, bet kurioje žemės vietoje, kurioje veikia IP tinklai. Šiuo metu konfidenciali informacija yra vertinga prekė. Ją atskleidus konkurentai gali sukurti pigesnę paslaugą, sutrukdyti organizacijos veiklą ar sužlugdyti ją. Todėl atsirado poreikis saugiai keistis informacija nekeičiant savo įpročių bei nediegiant sudėtingų ir brangių sprendimų. Šiam tikslui pasiekti gali būti panaudoti steganografiniai metodai, skirti paslėpti slaptą informaciją VOIP tinkle.

Dėl šios priežasties, baigiamojo darbo tikslas yra patobulinti standartinį LSB steganografinį algoritmą, kuris būtų atsparus duomenų pakeitimams VOIP tinkle. Sukurtas metodas privalo tenkinti minimalius slepiamos informacijos metodų taikymo reikalavimus: būti saugus, sunkiai randamas ir netrukdyti VOIP paslaugos tiekimo dėl pašalinio triukšmo. Sprendimo analizei yra lyginami kiti panašūs metodai vertinant šias tris charakteristikas.

Galutinis baigiamojo darbo rezultatas algoritmo realizacija VOIP tinkle. Atlikus eksperimentus yra nustatomas algoritmo tinkamumas slaptiems duomenis perduoti bei jo saugumas nuo stegoanalizės atakų.

Raktažodžiai: *steganografija, sauga, interneto telefonija, algoritmai, LSB*

Biliūnas, J. *STEGANOGRAPHIC LSB ALGORITHM ENHANCEMENT FOR VOIP PROTOCOL*: *Master's* thesis / supervisor prof. Algimantas Venčkauskas. Department of Computer Science, Faculty of Informatics, Kaunas University of Technology.

Kaunas, 2016. 50 p.

Key words: *steganography, security, VOIP, algorithm, LSB*

SUMMARY

VOIP is the most widely used IP network service; the communication of video and voice between remote departments or to provide support anywhere on Earth is an irreplaceable tool for international organizations. Confidential information is a highly valued commodity; exposed information provides competitors knowledge to create less expensive services or potential vulnerabilities to ruin a organization. This has resulted in an emerging demand for secure exchange of information without changing habits and without installing complicated expensive solutions. Stegnographic techniques can achieve this objective of hiding sensitive information in a VOIP network.

With the aim of improving the standard LSB stegnograpic algorithm resistant to changes of VOIP network data, a method must be developed to meet the minimum information obscurification requirements: be safe, difficult to penetrate, and not introduce extraneous noise that interferes with VOIP services. The decision analysis is a comparison of these three assessment characteristics across competing similar methods.

The final result is an algorithm implementation for VOIP network. Based on experiments, the algorithm is evaluated by its suitability for secret data transfer and its resistance for stego- analysis attacks.

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

TERMINŲ IR SANTRUMPŲ ŽODYNAS

1. **LSB** (angl. *Least Significant Bit*) – mažiausiai svarbus bitas.
2. **Stego-failas** – tai audio failas, kuriame yra paslėpti duomenys.
3. **Stego-paketas** – tai realizuotas steganografinis LSB paketas, kuriame yra įterpiama slepiama informacija.
4. **OSI modelis** (angl. *open system interconnection model*) – tai abstraktus ryšio protokolų aprašymas paskirstant juos į 7 lygius.
5. **VOIP** (angl. *Voice over IP*) – balsas IP protokole, dažniau vadinamas interneto telefonija ar IP telefonija.

ĮVADAS

Baigiamasis magistro darbas „LSB steganografijos algoritmo taikymas VOIP protokolui“ priklauso informacijos ir informacinių technologijų saugos studijų programai.

VOIP yra plačiausiai naudojama paslauga IP tinkle. Vaizdo ir balso pokalbiai yra vienintelė priemonė tiesiogiai bendrauti klietui su paslaugų teikėjais bei sprendžiant iškilusias problemas realiu laiku. Įmonės ir organizacijos gali dalintis savo planais ir kita svarbia informacija, iš bet kurios vietos, kur yra interneto ryšys. Todėl atsirado poreikis saugiai keistis informacija nekeičiant savo įpročių bei nediegiant sudėtingų ir brangių sprendimų. Šiam tikslui pasiekti gali būti panaudoti steganografiniai metodai, skirti paslėpti slaptą informaciją VOIP tinkle.

Todėl remiantis šiais pastebėjimais buvo suformuotas darbo tikslas:

sukurti išplėstą LSB steganografinį algoritmą atsparų apsaugotų duomenų pakeitimams VOIP tinkle.

Tikslui pasiekti buvo įgyvendinti šie uždaviniai:

- atlikta literatūros analizę tiriamąjai sričiai apibūdinti;
- išanalizuoti esami LSB sprendimai bei pritaikytos jų charakteristikos algoritmo realizacijoje;
- algoritmas bus pritaikytas realaus laiko duomenų siuntimui VOIP tinkle;
- duomenų apsikeitimai vyks saugiu komunikacijos kanalu;
- bus atliktas sukurto sprendimo eksperimentas bei rezultatų analizė.

Darbą sudaro trys dalys. Probleminės srities analizėje atlikta literatūros šaltinių analizė bei apžvelgti taikymo aplinkos (VOIP) bruožai, išnagrinėti šiuo metu taikomi VOIP steganografijos algoritmai, analizės dalyje apibrėžtai problemai spręsti. Antroje dalyje yra projektuojamas baigiamojo darbo sprendimas. Jis yra sudarytas iš dviejų dalių: algoritmo realizacijos ir VOIP aplinkos simuliacijos. Trečioje dalyje atliktas algoritmo saugumo tyrimas bei jo pritaikymas VOIP aplinkoje.

1. PROBLEMINĖS SRITIES ANALIZĖ

Tobulėjant programinei įrangai ir mažėjant techninės įrangos kaštams vis daugiau vartotojų gali naudotis naujausiomis technologijomis ir pasiekti informaciją internetu. Tačiau internete pilna pavojų, į kuriuos vartotojas gali įkliūti ir gauti materialinės ar nematerialinės žalos. Todėl yra taikomi metodai bei kuriamos sistemos, kurios padeda išsaugoti informacijos vientisumą ir konfidencialumą bei apsaugoti vartotojo duomenis nuo neautorizuotų vartotojų.

Informacijos apsaugą galima išskirstyti į 2 koncepcinius modelius:

1. Informacijos apsaugą;
2. Informacijos kanalo apsaugą.

Informacijos apsaugai galima priskirti duomenų šifravimo metodus (kriptografija) bei informacijos slėpimo metodus (steganografija (*toliau tekste - stego*) [1]). Tuo tarpu informacijos kanalo apsaugai plačiau naudojami komunikacijos kanalo šifravimo (SSL, TLS, SSH [2] [3] ir kt.) metodai ir duomenų siuntimo standartai bei protokolai (IPsec grupė ir VPN).

Tiriamajame darbe bus panaudota informacijos apsauga panaudojant stego metodus.

1.1. Steganografijos metodai

Steganografija – tai metodas palėpti įvarius informacijos objektus (tekstas, garso failas, vaizdas, paveikslėlis) kituose informacijos objektuose. Stego tikslas yra apsaugoti duomenis taip, kad tikimybė juos aptikti informacijos pernešimo paketuose kuo mažesnė. Tuo tarpu kriptografija stengiasi, kad duomenys būtų apsaugoti nuo peržiūrėjimo panaudojant specialius algoritmus.

Pagrindiniai skirtumai tarp kriptografijos ir steganografijos yra pavaizduoti 1 lentelėje.

1 lentelė. Steganografijos skirtumas nuo kriptografijos

Steganografija	**Kriptografija**
Nežinomas žinutės tekstas	Žinutės tekstas žinomas
Steganografija užkerta kelią paslėptų duomenų **egzistencijos** radimui	Kodavimas užkertą kelią trečiąjam asmeniui peržiūrėti žinutės **turinį**
Mažai žinoma technologija	Plačiai taikoma technologija
Technologija yra vis dar tobulinama	Nauji algoritmai atsiranda retai
Jei žinutė yra aptinkama, ji yra lengvai perskaitoma	Stiprūs algoritmai yra apsaugoti nuo jų nulaužimo atakų, reikalinga didelė skaičiavimo galia norint išgauti duomenis iš šifrogramos
Steganografija nepakeičia duomenų struktūros paslėptoje žinutėje	Kriptografija pakeičia paslėptos žinutės duomenų struktūrą

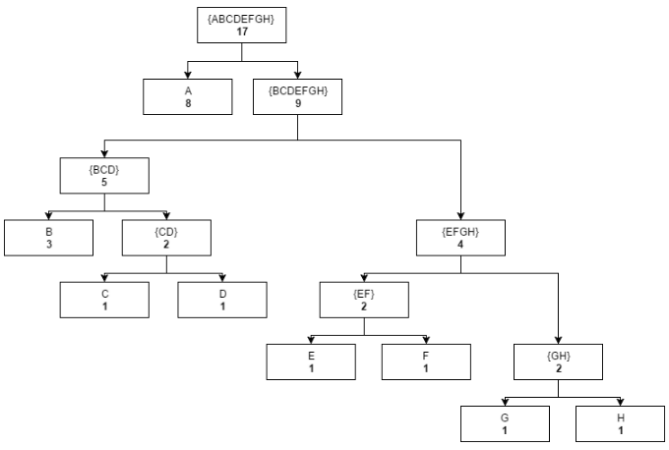
Kaip parodyta lentelėje pagrindinis steganografijos trūkumas yra silpna apsauga nuo žinutės perskaitymo, jei paslėpta žinutė yra aptikta. Todėl šiuo metu yra vykdomi tyrimai, kaip galima geriau apsaugoti duomenis panaudojant abu aukščiau išvardintus metodus ir atliekant jų įvairias kombinacijas [4] [5].

Visi steganografijos metodai gali būti padalinti į 3 grupes [6]:

1. **Grynoji steganografija:** ši technika naudoja įprastus steganografijos algoritmus be jokių kombinacijų su kitais metodais. Jis naudojamas tiesioginiam duomenų slėpimui siunčiant juos duomenų nešliui.
2. **Hibridinė steganografija**:
    a. **Slapto rakto steganografija**: ši technika naudoja steganografijos metodus kombinuojant juos su slapto rakto kriptografinėmis technikomis. Pagrindinė idėja yra apsaugoti slepiamus duomenis slaptu raktu prieš išsiunčiant juos duomenų nešliui.
    b. **Viešojo rakto steganografija**: ši technika naudoja viešojo rakto kriptografijos algoritmą kartu su steganografijos metodais. Panaudojus viešąjį raktą užkoduoti duomenis ir tada juos išsiųsti gavėjui, kuris su savo privačiuoju raktu galėtų peržiūrėti informaciją.

Pagal slepiamų duomenų nešlius steganografija yra skirstoma į penkis tipus:

1. **Teksto steganografija**: sunkiausiai įgyvendinama technika dėl teksto vientisumo palyginus su audioįrašu ar paveikslėliu. Tačiau jos įgyvendinimui reikia mažiau atminties. Vienas iš metodų naudojamų teksto steganografijoje būtų duomenų kompresija: ji užkoduoja informaciją kitu formatu, kuris gali užimti mažiau atminties. Plačiausiai žinomas kodavimas būtų Huffmano duomenų kompresijos algoritmas, dar kitaip vadinamas Huffmano kodavimo medžiu [7] [8] (1 paveikslėlis).



1 pav. Huffman‘o kodavimo medis panaudojant pirmų abėcėlės raidžių analogija su nurodytais koeficientais

2. **Paveikslėlių steganografija**: ši technika plačiausiai naudojama paslėpti slaptos žinutės bitus tiesiogiai į paveikslėlį, nekeičiant jos formato kaip, kad buvo su teksto steganografijos pavyzdžiu. Pagrindinė idėja yra tokia: žinutės bitai yra slepiami triukšmingose paveikslėlio vietose, kur žmogaus akis nekreipia dėmesio, t. y. duomenys slepiami vietose, kur didelė spalvų variacija. Visa paveikslėlių steganografija yra klasifikuojama į:
    a) Mažiausiai svarbaus bito (LSB) integraciją,
    b) Maskavimo ir filtravimo,
    c) Perteklinio šablono kodavimo (angl. *Redundant Pattern Encoding*),
    d) Šifravimo ir sklaidos (angl. *Encrypt & Scatter*),
    e) Algoritmų ir transformacijų,

    metodus.
3. **Garso/balso įrašų steganografija**: Garso steganografija yra sudėtingiau įgyvendinama lyginant su paveikslėlių steganografija. Šio metodo esmė yra paslėpti informaciją skaimeniniame garso signale. Slėpimo technika gali būti naudojama trims garso formatams (*MP3, AU* ir *WAV*) koduoti. Visa tai gali būti atliekama pakeičiant audiofailo binarinę seką, panaudojant vieną iš apačioje nurodytų technikų:
    a) LSB kodavimas;
    b) Pariteto kodavimas;
    c) Signalo fazės kodavimas;
    d) Skleisties spektro (angl. *Spread spectrum*) kodavimas;
    e) Aido slėpimas.
4. **Vaizdo įrašų steganografija**: ši steganografija panaudoja ir garso, ir paveikslėlio steganografijos metodų kombinacijas. Didžiausias šio metodo privalumas – dideli slepiamos informacijos kiekiai, kadangi informacija gali būti slepiama ir garso signale, ir vaizdo sraute.
5. **Protokolų steganografija**: tai steganografijos metodai skirti pakeisti esamus komunikacijos protokolus, nepažeidžiant jų pagrindinėms dalims, kad komunikacija vyktų ir visos tinklo dalys neatpažintų anomalijų siunčiamuose paketuose. Šis metodas yra saugiausias tarp visų steganografijos metodų, nes sunku aptikti pakeitimus ir eliminuoti juos, kadangi jie yra 4-ame OSI sluoksnyje (2 lentelė).

2 lentelė. OSI sluoksnių klasifikacija su perduodamų duomenų pavyzdžiais

	Sluoksnis	**Perduodami**	**Pavyzdys**
7	Taikymo	duomenys	Apibrėžia tinklo teikiamas paslaugas vartotojo programoms. Pvz.: Telnet, HTTP
6	Prezentacijos	duomenys	Nusako duomenų kodavimo sesijos metu taisykles. Pvz.: MIME
5	Sesijos	duomenys	Aprašo duomenų apsikeitimo tarp galinių sistemų taisykles vienos jungties ribose. Pvz.: SIP sesijos užmezgimas prdedant VOIP skambutį
4	Transporto	segmentai	Tiekia skaidrų duomenų perdavimą tarp tinklo vartotojų su norimomis patikimumo garantijomis. Pvz.: TCP, UDP
3	Tinklo	paketai	Aprašo, kaip duomenų sekos turi būti perduodamos visame tinkle. Pvz.: IP
2	Ryšio	kadrai	Aprašo ryšį tarp tinklo komponentų. Pvz.: Ethernet
1	Fizinis	bitai	Aprašo fizinius perduodamo signalo ir terpės, kuria jis perduodamas, parametrus. Pvz.: UTP kabelis

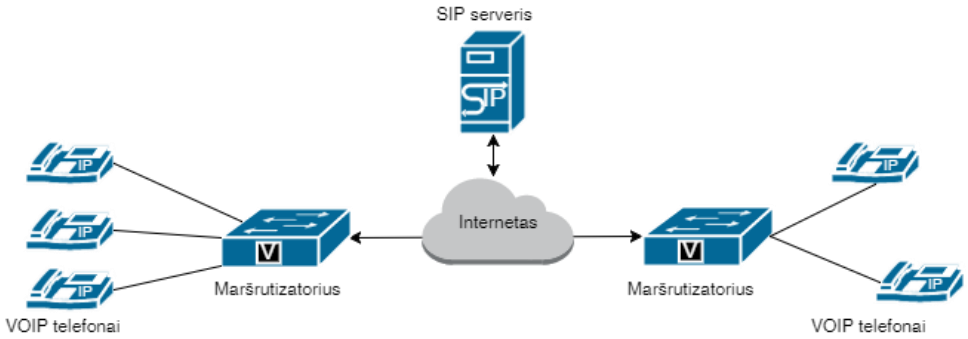
Pavyzdžiui, Mazurczyko, Frączeko ir Szczypiorski‘o [9] tiriami steganografijos algoritmai naudoja srauto siuntimo valdymo protokolą (angl. *Stream Control Transmission Protocol (SCTP)*), kuris priklauso 4-am OSI sluoksniui ir teigia, kad norint užkirsti kelią 16-ai aprašytų steganografijos metodų, kurie yra grėsmė tinklo saugumui, reikia pakeisti SCTP standartą. Tuo tarpu paveikslėlio steganografija yra aprašoma prezentacijos sluoksnyje. Įvertinus šias dvi priklausomybes galima teigti, kad kuo aukštesnis OSI sluoksnis, tuo lengviau yra integruoti apsaugos modelius iškraipančius duomenis bei sukurti metodus perimti steganogramas.

1.2. VOIP

Šiame skyriuje bus apžvelgtas garso perdavimas IP protokolu, kuris sudaro pagrindinį ryšio kanalą realizuojamame projekte.

VOIP, dar kitaip vadinama IP telefonija, – tai yra metodologijų ir technologijų rinkinys, skirtas pateikti balso komunikaciją ir multimedijų sesijas IP protokolo tinklu. Šis terminas atskiria kitą balso perdavimo būdą telefono linijomis, dar kitaip vadinamą PSTN tinklu.

VOIP technologija leidžia vartotojams naudotis balso perdavimo ir multimedijos sesijų per interneto tinklą, paslauga. Naudojantis VOIP paslauga, analoginis balso signalas yra keičiams skaitmeniniu ir siunčiams IP paketais, t. y. tradicinė analoginė telefono paslauga keičiama į duomenų perdavimą.



2 pav. Bendroji VOIP sistemos architektūra

Kaip pavaizduota 2 pav., VOIP architektūrą sudaro:

1. VOIP telefonai

VOIP telefonai skirti balsui perduoti per IP. Jie yra padalinti į dvi grupes: programiniai telefonai (PT) (angl. *softphone*) ir techninės įrangos telefonai (TĮT) (angl. *hardphone*). PT telefonai – yra sukurtos programinės įrangos **programos** tokios kaip „Skype“, „Lync“ ir kt. naudojamos kompiuteriuose. Kita grupė (TĮT) yra **prietaisai**, kurie turi funkcijas prisijungti prie IP tinklo ir tokiu būdu siųsti balso srautą.

2. Maršrutizatorius

Maršrutizatorius yra naudojamas kontroliuoti prisijungimus tarp grandininio ir paketinio duomenų perdavimo tinklų (angl. *circuit-switched and packet-switched network*). Šiuo metu dauguma šiuolaikinų maršrutizatorių yra dekomponuoti į skambučio agentus (angl. *Call Agent*) ir medijų tinklų sietuvą (angl. *Media Gateway*). Skambučio agentas skirtas skambučio nukreipimui, sesijų užmezgimui, kitiems skambučio servisams valdyti. Tuo tarpu medijų tinklų sietuvas sujungia skirtingų medijų srautus kartu ir sukuria ištisinį (angl. *end-to-end*) kelią balsui ir duomenims sklisti VOIP skambučio metu.

3. SIP serveris

Šis serveris yra naudojamas VOIP sesijoms registruoti ir užmegzti su nutolusiu vartotoju prijungto prie to paties VOIP serviso, kurie naudoja SIP protokolą sesijoms užmegzti. Galima realizacija be tarpinio SIP serverio. Tačiau šis tarpinis serveris yra naudojamas saugumui pagerinti, kadangi sukurti sesijas gali tik registruoti vartotojai.

VOIP paslauga yra įgyvendinama paketų perdavimo tinkluose, naudojant tinklų valdančiuosius protokolus. Pagrindiniai du protokolai yra H.323 ir SIP.

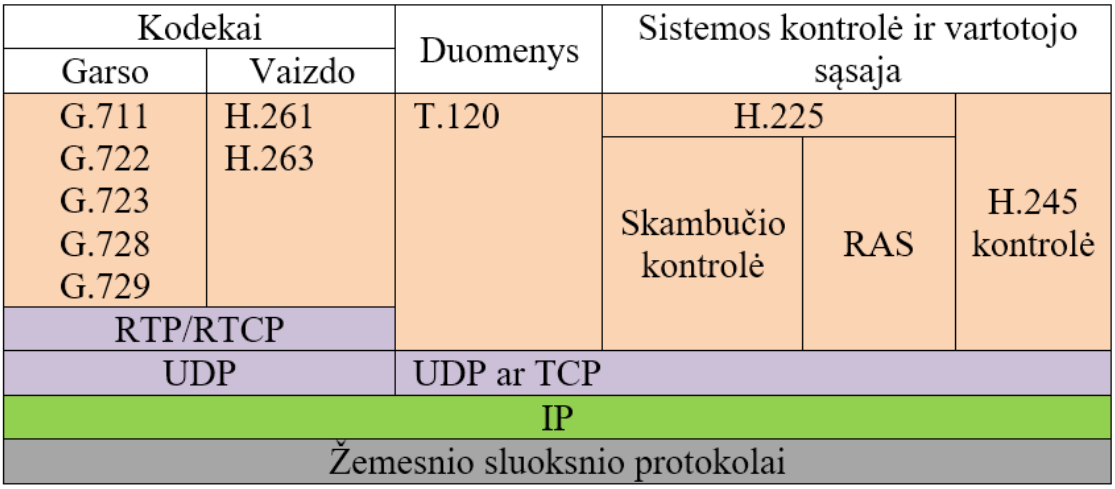
SIP – tai signalinis protokolas naudojamas sukurti, valdyti ir baigti sesijas IP tinkluose. Sesija galėtų būti paprastu dvikrypčiu telefoniniu skambučiu ar gali būti daugiamedijine konferencine sesija. Protokolas yra standartizuotas pagal tarptautinius dokumentus (RFC 3261), nors protokolas yra vis dar

augantis ir evoliucionuojantis. SIP protokolas skirtas tik sesijos užmezgimui ir valdymui, norint perduoti duomenis reikia naudoti kitus protokolus (RTP, TCP/IP ir kt.).

H.323 protokolas yra audiovizualinės komunikacijos protokolų rinkinys skirtas, bet kokiam paketinių duomenų tinklui. Šis standartas yra patvirtintas ITU sąjungos. Šis standartas nusako visas VOIP įgyvendinimo detales.

Pagrindiniai H.323 standarto komponentai yra:

1. Terminalai. Terminalais vadinami įrenginiai skirti VOIP ryšiui užtikrinti.
2. Tarptinklinės sąsajos. Šie įrenginiai skirti dviems tinklams sujungti. Dažniausiai jie yra naudojami sujungti su papildomais VOIP servisais, tokiais kaip PSTN ar ISDN.
3. Tarptinkliniai derintuvai (angl. *gatekeepers*). Jų pagrindinės funkcijos yra adresavimas, autentifikavimas ir legalumo nustatymas, pralaidumo ir apkrovų apskaita bei maršrutizavimas. Dažnai šie tinklo mazgai yra įgyvendinami kaip darbo stotys, kuriose veikia VOIP pokalbiui reikalinga įranga.
4. MCU (angl. *Multiple Control Unit*). Šie įrenginiai skirti konferenciniams pokalbiams organizuoti ir valdyti.



3 pav. H.323 naudojamų protokolų hierarchija pagal OSI sluoksnius nuo aukščiausio viršuje (oranžinė spalva) iki žemiausio (pilka spalva)

Kaip parodyta 3 pav., VOIP skambučiui užmegzti yra naudojami skirtingi protokolai kiekvienam veiksmui tinkle. Kodekai naudojami užkodavimui ir dekodavimui atskirai. Skambučio kontrolei yra naudojamas kitas H.225 protokolas, skirtas sujungti du ir daugiau terminalų. Duomenys keliauja dar vienu papildomu T.120 protokolu. H.323 standartas yra pilnai susiformavęs ir nekinta, todėl jis yra saugesnis negu palyginti neseniai susiformavęs SIP signalizavimo protokolas.

Kiti palyginimo rezultatai yra pavaizduoti 3 lentelėje.

3 lentelė. SIP ir H.323 charakteristikų analizės rezultatai

Charakteristikos	**SIP**	**H.323**
Paslaugų kokybės užtikrinimas (QoS)	Neturi savo standarto. Remiasi RSVP, COPS ar kt. protokolais	Tinklo srauto valdymas ir priėmimas kontroliuojamas H.323 tarptinkliniais derintuvais
Lankstumas	Labai lanksti. Nėra priklausomas nuo techninės ar programinės įrangos. Leidžia vartotojui keisti savo buvimo vietą tinkle	Nelanksti. **Vartotojo terminalas** privalo būti prijungtas prie jam skirto tarptinklinio derintuvo.
Naudojami apsaugos protokolai	Neriklausomas nuo jokių. Gali būti naudojami TLS ar IPSec apsaugos protokolai.	Naudojamas H.235 standartas. Užtikrina pranešimų saugumą ir autentifikaciją.
Kontrolės mechanizmas	**Vartotojo programose**	Centralizuotame serveryje
Kodavimas	Tekstas	Binariniai duomenys (ASN.1)
Architektūra	Monolitinė, viskas viename serveryje	Gali būti paskirstyta tarp keletos serverių
Patikimumas	Neužtikrina klaidų aptikimą ir šalinimą	Sukurta reguliuoti klaidas tinkle

Palyginus abu VOIP signalinius protokolus pavyko nustatyti, kad skirtumai tarp šių protokolų yra nedideli, tačiau SIP protokolo lankstumas leidžia panaudoti mažiau resursų VOIP sistemos realizacijai, tuo tarpu H.323 sistemos kaštai didėja, nes protokolas yra priklausomas nuo tam tikrų tinklo įrenginių.

Žemiau yra palyginti VOIP tinkle naudojami garso kodekai.

4 lentelė. ITU rekomenduojami balso kodavimo kodekai [10]

Kodekas	**Aprašymas**
G.711	Aukštos kokybės garso kodekas. Pilnai dupleksinis algoritmas yra naudojamas VOIP, PSTN tinkluose, pritaikomas ISDN, skaitmeninių PBX skaitmeniniuose telefonuose, skaitmeninėse palydovinėse sistemose. Balsą konvertuoja iš/į IKM signalą 64 bitų sparta. Kodekas suderinamas su H.320 ir H.323 ITU protokolais.

G.722	Kalbos kodekas, kuris konvertuoja balsą į 48, 56 ir 64 kbps skaitmeninių signalų spartą. Diskretizuoja garso signalą 16 kHz dažniu, kai tuo tarpu dauguma kodekų diskretizuoja 8 kHz dažniu.
G.726	Tai adaptyvios diferencialinės impulsinės–kodinės moduliacijos balso kodekas. Skaitmeninį signalą perduoda 16, 24, 32 ir 40 kbps sparta.
G.729	Kalbos kodekas, naudojantis jungiamosios struktūros algebrinį kodu sužadintą tiesinės prognozės algoritmą. Skaitmeninį signalą perduoda 8 kbps sparta. Taikomas VOIP, skaitmeninėse palydovinėse sistemose, PSTN, ISDN, skirtinėse linijose, garso sulaikymo sistemose.
G.729ab	Kalbos kodekas, sumažinantis naudojamo kanalo juostos pločio reikalavimus, kadangi iš signalo pašalina balso pauzes. Naudoja jungiamosios struktūros algebrinį kodu sužadintą tiesinės prognozės algoritmą ir pasiekia signalo suspaudimo laipsnį 16:1 proporcija. Signalo vėlavimas kodeke – 15 ms.
G.729e	Kodekas skirtas PSTN kokybiniams reikalavimams pagerinti. Perduodamo signalo sparta yra 11.8 kbps, kuri naudojama pagrindiniam signalo srautui formuoti, tokiam kaip muzikinis srautas.
G.990	Naujas standartas didelės talpos srautams. Užtikrina iki 2 Mbps simetrinius dvikrypčius srautus ir iki 640 kbps asimetrinius dvikrypčius srautus. Tai oficialus DSL linijos tipo architektūros standartas, nors šis standartas nebūtinai taikomas DSL linijose.

Remiantis 4 lentele, yra nustatyta, kad G.711 kodekas yra labiausiai tinkamas naudoti realizuojamame projekte, kadangi kuriamas algoritmas naudoja daugiau duomenų nei standartinis LSB, todėl padidintą duomenų kiekį reikia kompensuoti didesniu pralaidumu (> 40 kbps). G.990 kodekas turi didesnį pralaidumą nei G.711, tačiau jo įgyvendinimas C# kalboje yra menkai ištirtas. Be to šio kodeko viešai prieinamų ir naudojamų bibliotekų nebuvo rasta.

1.3. VOIP steganografija

VOIP steganografija yra metodų rinkinys, skirtas paslėpti duomenis visose skambučio etapuose. Literatūroje nurodyta, kad VOIP steganografija gali būti skirstoma į 3 dalis [11] :

1. Tiesioginės protokolo duomenų (angl. *protocol data unit (PDU)*) modifikacijos.
2. Tiesioginės PDU modifikacijos laiko dedamojoje.
3. Hibridinės modifikacijos.

Pirmoje grupėje esantys metodai modifikuoja PDU: tinklo protokolų antraštes ar duomenų segmentus (angl. *payload*). Šio sprendimo pavyzdžiai būtų IP, UDP ar RTP protokolų antraščių modifikacijos vykstant pokalbiui (pagal Mazurczyk and Kotulski [12]), signalinių protokolų modifikacijos (pagal Murdoch and Lewis [13]) ar pakeičiamas vartotojo sukurtas turinys panaudojus vieną iš slėpimo algoritmą (pvz.: LSB), kuris perduodamas RTP duomenų segmentuose.

Antroje grupėje esantys metodai modifikuoja PDU laike. Pavyzdžiui, siunčiant duomenis visi PDU paketai yra užvėlinami (pagal Wang 2005 [14]), įtakojant PDU paketų eilę (pagal Kundur ir Ahsan 2003 [15]) ar sąmoningas PDU paketų praradimas (pagal Servetto ir Vetterli 2001 [16]).

Trečioje grupėje esantys hibridiniai metodai modifikuoja ir PDU paketą, ir jo laiko priklausomybę. Šios grupės pavyzdys būtų LACK metodas(Mazurczyk 2008 [17]).

1.3.1. Tiesioginės PDU modifikacijos metodai

Šiame skyriuje bus apžvelgti pirmos grupės metodai, jų privalumai ir trūkumai.

1.3.1.1. Paketų praradimo maskavimo algoritmas

Paketų praradimo maskavimo (angl. *packet loss concealment* (PLC)) metode yra naudojama aukšto tono signalo replikacijos (angl. *pitch waveform replication* (PWR)) technika. Visa tai padeda sutaisyti balso signalą kopijuojant į atsiradusį tarpą aukšto tono signalą, kol atsiradęs tarpas, dėl duomenų paketų praradimo, yra pilnai užpildomas. Taip pat ši technika padeda pagerinti balso kokybę ją perduodant IP tinklu.

4 pav. pavaizduotas sugadinto balso signalo atkūrimas. Pirmiausiai yra surandamas sugadinto signalo kadras *k*. Tada paimamas prieš tai buvusio kadro aukščiausio tono *b* šablonas (4 pav. 2 dalis). Tolimesnis veiksmas yra pasiimti sekančio kadro aukščiausio tono signalo *f*, šabloną. Gavus abu šablonus yra skaičiuojama jų diskretinė sąsukos (angl. *convolution*) funkcija:

$$(f * b)[n] = \sum_{m=-M}^{M} f[n-m]b[m], \qquad \textbf{(1)}$$

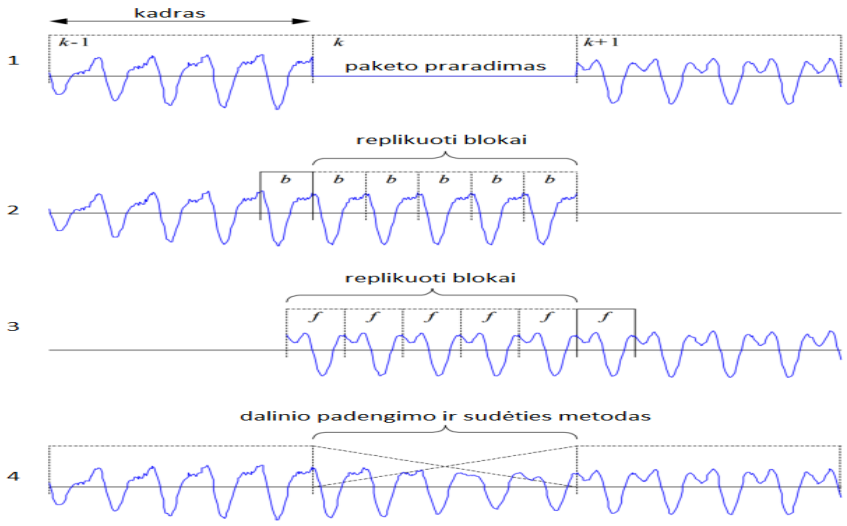
kur *f* ir *g* – yra kompleksinės funkcijos, { *-M , -M +1 , ... , M - 1 , M* } – baigtinio impulso dėmenys.

Tada panaudojus sąsukos funkcijos rezultatus su esamu baigtiniu signalu gauname dalinio padengimo ir sudėties funkcijos realizaciją:

$$y[n] = x[n] * h[n] \stackrel{\text{def}}{=} \sum_{m=-\infty}^{\infty} h[m] \cdot x[n-m] = \sum_{m=1}^{M} h[m] \cdot x[n-m] \qquad \textbf{(2)}$$

, kur x[n] yra baigtinis signalas, h[x] – sąsukos funkcija.

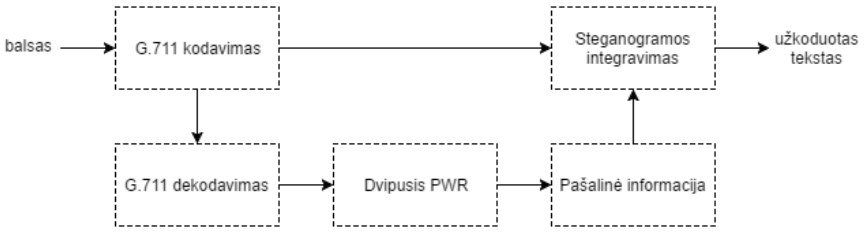
Šios funkcijos rezultatas yra rekonstruotas signalas (4 pav. 4 dalis)



4 pav. Dvipusio PWR procedūros schema

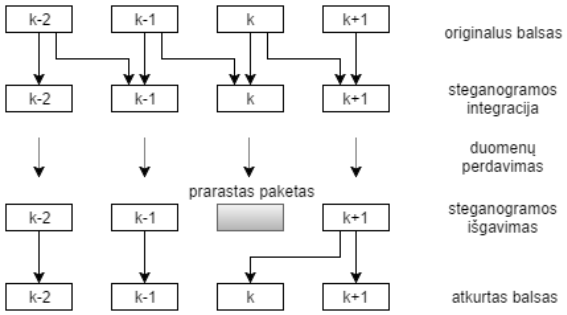
Aoki pasiūlytame sprendime [18] yra naudojamas šis dvipusis PWR, kurio signalo langas (kadras) yra lygus 20 ms, o PWR – 5ms. Paieškos langas PWR algoritme yra pasirinktas 15 ms. Pagal šias sąlygas, maksimalus aukščiausio tono periodas taip pat lygus 15 ms. Tokio ilgio langas padengia nuo 5 iki 12 ms vyriško balso ir nuo 2 iki 7 ms – moteriško balso informaciją.

Kaip parodyta 5 pav. šalutinė informacija yra iš anksto ištraukta (angl. *extracted*) siuntėjo programoje norint sumažinti bangos fazės ir gaubtinės (angl. *wave phase and envelope*) neatitikimus rekonstruojant signalą gavėjo kompiuteryje.



5 pav. Balso kodavimo procedūros Aoki pasiūlytame sprendime

Norint persiųsti šalutinę informaciją, kurios dydis lygus 26 bitams, reikalingą atkurti paslėptą žinutę, yra naudojamas aukščiau įvardintas PLC algoritmas. Tam pasiekti yra panaudotos papildomos manipuliacijos su G.711 kodeku bei PWR algoritmu. Šalutinė informacija *k*-tąjame kadre yra siunčiama lygiagrečiai kaip steganograma kartu su balso duomenimis *k+1* kadre. (6 pav.).

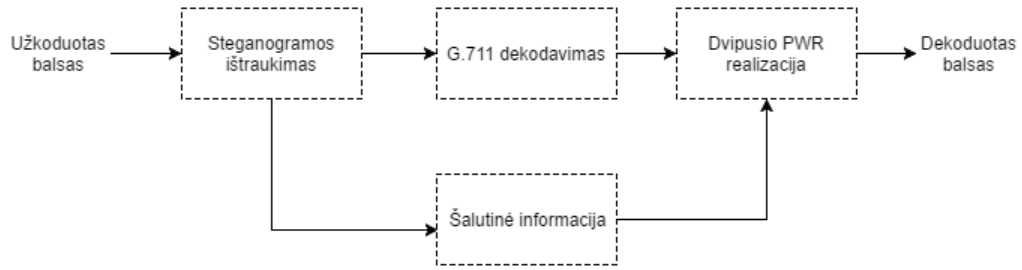


6 pav. Schematinės PLC procedūros panaudojant steganografiją

Duomenų įterpimo ir iškraipymo sumažinimui dėl logaritminio kvantizavimo G.711 algoritme, steganograma yra įterpiama po balso bitų rikiavimo didėjimo tvarka, kuris yra sudarytas iš 160 signalo ėminių kiekviename kadre palyginant absoliutinę amplitudę pagal:

$$|s(n)| = \begin{cases} 2\left\lfloor \frac{s(n)}{2} \right\rfloor + 1, & s(n) \geq 0 \\ -2\left\lfloor \frac{s(n)}{2} \right\rfloor, & s(n) < 0 \end{cases} \quad \textbf{(3)}$$

kur $\lfloor x \rfloor$ – didžiausias sveikas skaičius mažesnis ar lygus x. LSB bitai kiekviename signalo ėminyje yra ignoruojami rikiavimo proceso metu. Tokiu būdu, 0 ir 1 yra vienodai vertinami. Pabaigus rikiavimą, pirmi 26 signalo ėminiai yra pasirenkami ir jų LSB bitai yra pakeičiami steganogramos bitais. Signalo dekodavimui yra naudojamas atvirkščias procesas balso kodavimui.(7 pav.)



7 pav. Balso atkodavimo procedūros Aoki pasiūlytame sprendime

Prarastas kadras yra rekonstruojamas pagal dvipusį PWR algoritmą panaudojant *k-1* ir *k+1* kadrus. Buvo gautas rezultatas, kad balso kokybė yra blogesnė, jei įterpiamų steganogramos bitų yra mažai (mažiau nei 40 bitų). Didėjant steganogramos bitų skaičiui tarp atsitiktinio ir pasirinktinio steganogramos bitų integracijos metodų signalo triukšmingumo lygis mažėja, todėl balso kokybė nukenčia mažiau po bitų integracijos.

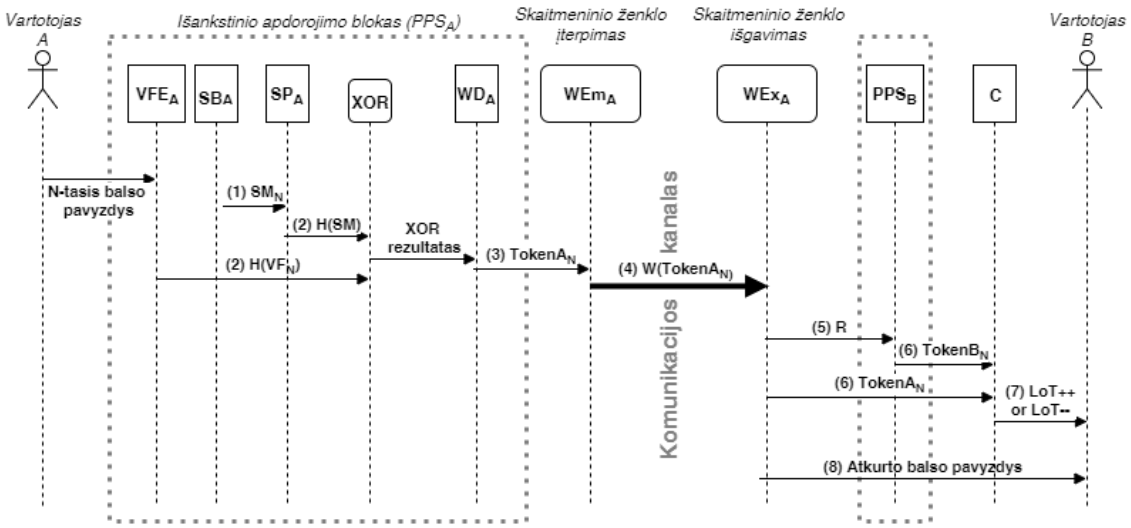
Aoki pasiūlytas metodas padeda išsaugoti balso vietisumą dėl prarastų kadrų, tačiau naudojamas steganografijos metodas yra skirtas užtikrinti prarastų duomenų rekonstrukciją, bet netinka slaptų duomenų perdavimui, kadangi duomenys nėra tiksliai atkuriami, o statistiškai atkuriami.

1.3.1.2. Paslėpto skaitmeninio vandenženklio metodas (SVM) kontroliniame protokole

Skaitmeninis vandenženklio metodas (toliau – skaitmeninis ženklinimas) yra vis plačiau naudojamas norint apsaugoti skaitmeninius autorinius kūrinius, tokius kaip fotografija, muzikinis įrašas ir kt. Todėl kaip nurodo kiti šios srities tyrinėtojai [19] panaudojus skaitmeninį ženklinimą galima pagerinti VOIP sistemos apsaugą. Autoriai gali įterpti duomenis, kurie yra panašūs į kriptografines maišos funkcijas, į savo darbus ir pagal tai atpažinti failo autentiškumą. Kadangi tik autorius žinos, kur yra paslėptas šis skaitmeninis ženklas, leis atskleisti kitas failo manipuliacijas. Mazurczyko ir Kotulski‘o pasiūlytas sprendimas privalo turėti tam tikras savybęs, tokias kaip patvarumas (angl. *robustness*), sauga, skaidrumas (angl. *transparency*), sudėtingumas, talpa, patikimumas (angl. *verification*) ir grįžtamumas (angl. *invertibility*). SVM savybių optimizacija yra pagrindinis audio sistemos tikslas. Aukščiau paminėti tyrėjai savo realizacijoje naudoja aukštą patvarumą (tol kol tekstogramos semantika nėra sunaikinta), aukštą saugumą bei neaptinkamumą. Reikia atkreipti dėmesį, kad jų kuriamas metodas naudoja realaus laiko mechaniką, todėl realizacija yra sudėtingesnė nei įprasto steganografijos metodo taikymas garso įraše.

Apžvelgus pagrindines metodo dalis galima išskirti du blokus (8 pav.):

1. Skaitmeninio ženklo įterpimas ir išgavimas
2. Išankstinio apdorojimo blokas (PPS)



8 pav. Skaitmeninio ženklinimo architektūros detalizacija

PPS_B ir PPS_A blokai veikia analogiškai, todėl padetalizuotas yra tik išankstinio apdorojimo blokas PPS_A. Taip pat yra manoma, kad signalizavimo fazėje keletas signalinių žinučių (SM_N) jau yra išsiųsta ir saugoma SB bloke. Tuo tarpu patikrinimo fazėje PPS_A ir PPS_B yra tikrinamas jų identiškumas. Algoritmo veikimas yra toks:

1. Kai pokalbis prasideda, pirmasis balso pavyzdys atsiranda VFE_A bloke ir sinchroniškai tuo pačiu metu yra siunčiama pirmoji signalinė žinutė(*SM*) iš buferio (SB_A) į SP_A bloką (1 žingsnis 8 pav.). VFE_A bloke yra atliekamas balso pavyzdžio duomenų maišos funkcijos reikšmės skaičiavimas ($H(VF_N)$).Tuo pačiu metu taip pat atliekama maišos funkcijos reikšmės skaičiavimas signalizavimo žinutei SP_A bloke $H(SM_A)$ (2 žingsnis 8 pav.).
2. Maišos funkcijų rezultatams yra atliekama *XOR* operacija. Gautas rezultatas yra persiunčiamas į WD_A bloką, kur *TokenA* yra sukuriamas kartu su kitais parametrais, tokiais kaip atsitiktinių skaičių generatoriaus reikšmė (*R*), bendras slaptažodis (*PASS*), globalus *A* srauto identifikatorius (ID_A) bei nebūtinas parametras – laiko žymė (*TS*).
3. *TokenA* parametras yra siunčiamas į skaimteninio ženklinimo įterpimo funkciją (WEm_A) ir sukurta informacija yra išsaugoma skambinančio vartotojo A balse. Tokiu būdu sukurtas balso srautas yra siunčiamas komunikacijos kanalu ($W(TokenA)$).
4. Prieš tai, kol yra pasiekiamas balso srauto iš A vartotoją B, skaitmeninis ženklas yra išgaunamas (WEx_A bloke) ir siunčiamas į komparatorių *C* (5 ir 6 žingsniai 8 pav.), kur yra patikrinamas *TokenA* su *TokenB*:

$$TokenA_N = TokenB_N = H\left(\left(H(SM_N) \oplus H(VF_N)\right) \| \begin{pmatrix} TS \\ PASS \\ ID_A \end{pmatrix} \| R \right) \| R \qquad \textbf{(4)}$$

5. Išgautas ženklas kartu su atsitiktiniu skaičiumi R yra siunčiamas į PPS_B bloką, kur įvyksta duomenų apdorojimas. Jei R reikšmė neegzistuoja, tada yra nutraukiamas balso srautas. Gautas rezultatas yra persiunčiamas į komparatorių *C*.
6. Jei *TokenA* yra lygus *TokenB* (6), tada patikimumo parametro (angl. *level of trust* (*LoT*)) reikšmė yra padidinama, kitu atveju *LoT* reikšmė sumažėja. Remiantis *LoT* reikšme yra sprendžiama ar nutraukti skambutį, ar ne.

Jei *LoT* reikšmė pasiekia kritinę ribą (CL), tada *LoT* skaitiklis yra sumažinamas. Tačiau tai yra gana didelė saugumo spraga. Ji leidžia VOIP tinlo atakuotojui laukti, kol *LoT* reikšmė pasieks $LoT = (a * x) - 1$ ir tada jis galės įsilaužti į srautą ir apsimesti, kad jis yra tas pats vartotojas A. Tačiau saugus LoT skaitiklio intervalas yra tarp:

$$[0;\ (a * x) - 1 - (CL + 1)], \qquad \textbf{(5)}$$

kur *a,* - kritinės ribos reikšmė ir *x,* - *LoT* reikšmė gauta iš siuntėjo.

Jei yra tinkamai pasirenkami a ir x parametrai, atakuotojas neturi galimybės įsiterpti į siunčiamą balso srautą. Šio aprašyto metodo privalumas yra jo nepriklausomumas nuo naudojamo kontrolės protokolo (gali būti naudojama ir SIP ir H.323 signalizavimo protokolai) ir mažas tinklo rauto naudojimas, kadangi duomenų persiuntimui naudojamas SVM metodas. Tuo pačiu metu yra užtikrinamas siunčiamo balso srauto autentiškumas.

1.3.1.3. LSB algoritmai ir jų modifikacijos

Mažiausiai svarbaus bito (LSB) kodavimas yra paprasčiausias būdas paslėpti informaciją skaitmeninėje rinkmenoje. Priklausomai nuo naudojamo duomenų perdavimo protokolo šis algoritmas gali pernešti daug informacijos, kadangi visi svarbios informacijos bitai yra saugomi paskutiniame kiekvieno baito bite. Pavyzdžiui, jei duomenų perdavimui yra naudojamas vieno kanalo WAV failas, kurio imties rodiklis (angl. *sample rate*) yra lygus 44kHz, tai perduodamų duomenų kiekis siekia 44.1 kbps, jei kiekviename baite bus išsaugomas vienas slaptos žinutės bitas.

Kaip nurodyta literatūroje, duomenų slėpimui gali būti naudojimas ne tik paskutinis kiekvieno baito bitas. Remiantis [20] tyrimu, paslėpti galima nuo 4-o iki 7-o sluoksnio bitų kiekviename baite, tačiau tada bus pažeista viena iš pagrindinių steganografijos aksiomų, - duomenų slaptumas, t.y. paslėpta žinutė neturi būti matoma slepiamame objekte. Tai įvyks dėl atsiradusio triukšmo signale, kadangi dalis informacijos bus prarasta dėl pasikeitusių bitų. Dažnai literatūroje minimas balto Gauso triukšmo terminas, norint apibrėžti atsiradusį atsitiktinį triukšmą audiofaile.

Antras trūkumas yra neatsparumas statistinėms atakoms. Tai vyksta todėl, kad slaptos žinutės ilgis privalo būti mažesnis negu ėminių kiekis audiofaile. Jei slaptos žinutės ilgis yra 24 baitai, o audiofailas yra 2 MB dydžio, tai panaudojus įprastą LSB algoritmą gausime, kad mažiau nei 1 procentas audiofailo dydžio bus užpildytas stego-žinute. Ir panaudojus vizualinį statistikos algoritmą, gausime, kad signalo pradžioje vyksta anomalijos, o likusi dalis, kur audiofailas buvo nepakeistas duomenys nukrypsta dėsningai. Todėl rekomenduojama naudoti tik du paskutiniu bitus informacijai slėpti. Yra sukurtą įvairių metodų, kaip būtų galima pagerinti šį trūkumą, kurie yra aprašyti žemiau.

Paprasčiausias būdas yra įvesti baitų praleidimo algoritmą, kuris praleistų 3 baitus ir tik tada įrašyti į pasirinktą baitą stego-žinutės bitus. Tačiau šis metodas taip pat turi trūkumą, kad atradus dėsningumą, kas kiek yra praleidžiami baitai ir kuriame baite yra saugoma informacija, statistiniais algoritmais bus galima rasti paslėptą žinutę. Kitas šio metodo trūkumas yra sumažėjęs perduodamos informacijos kiekis. Jei vartotojas pasirenka gana didelį žingsnį tarp įrašomų duomenų, tai lygiai tiek pat kartų yra sumažėjusi audiofailo naudingoji talpa slaptoms žinutės perduoti.

Šį metodą galima pagerinti įvedus stego-raktą atsitiktiniam žingsniui apskaičiuoti. Pavyzdžiui, pasirenkamas toks stego-raktas, kurio baitų kiekis yra didesnis už slepiamos žinutės bitų kiekį. Tada pirmas bitas yra įrašomas į garso failą praleidus tiek baitų, kokia yra pirma stego-rakto baito reikšmė. Tokiu būdu yra išsaugoma visa žinutė nevienodo intervalo žingsniu, todėl statistinės

atakos neparodys slepiamų duomenų dėsningumus. Šio metodo trūkumas yra toks, kad ir siuntėjas ir gavėjas turi turėti tokį patį stego-raktą. Jis taip pat kaip ir prieš tai aprašytas būdas sumažina perduodamos naudingosios talpos dydį, tačiau čia galima panaudoti, ne vieno bito slėpimą, bet dviejų bitų slėpimą audio failo baituose, kas padvigubina talpą.

Tian [21] sukurė realaus laiko steganografijos sistema, kurios esmė nėra LSB algoritmo pagerinimas, bet jo pritaikymas realaus laiko sistemoje panaudojus M-eilės šifravimo metodą eliminuoti koreliaciją tarp slaptų žinučių paketų ir padidinti atsparumą statistiniams stegoanalizės metodams. Papildomai prie šių metodų dar yra naudojama protokolo steganografija RSA raktams perduoti, kad būtų užtikrintas slaptos žinutės rekonstrukcijos procesas. Sistema buvo įvertinta kiekybiniais parametrais (MOS rodiklis, pralaidumas), kurie parodė, kad sukurtas metodas sumažina steganografinių duomenų kiekio pralaidumą iki 0.8 – 2.6 kbps ir MOS rodiklio sumažėjimą - nuo 0.3 iki 1, palyginus su originaliu audiofailu.

Miao ir Huang [22] pasiūlė adaptyvią steganografiją grindžiamą balso bloko lygumu (angl. *smoothness*). Metodas pasirenka mažesnį bitų integracijos lygį žemesnio dažnio blokuose ir didesnį bitų integracijos lygį aukštesnio dažnio blokuose. Ir tokiu būdu padidina slepiamos informacijos saugumą. Ekspertimentas parodė, kad šis metodas leidžia persiųsti 7.5 kbps slaptų duomenų ir tuo pačiu metu sumažina balso kokybę mažiau nei 0.5 MOS rodiklio vienetais.

Xu [23] sukurtas AVIS metodas yra sudarytas iš dviejų komponentų: VAMI, kuris yra atsakingas už dinaminį bitų pasirinkimą remiantis VOIP sektoriaus reikšme ir VADDI, kuris dinamiškai keičia bitų integracijos žingsnius (intervalus). Metodo implemantacijai buvo panaudotas G.711 kodekas, kuris įrodė, kad pasiūlytas AVIS metodas yra sunkiau aptinkamas negu įprastas LSB. Šis algoritmas gali perduoti iki 114 bps steganografinių duomenų ir tokiu būdu sumažinti perduodamo balso kokybę 0,1 – 0,4 MOS rodiklio vienetais.

Wu ir Yang [24] aprašė patobulintą LSB algoritmą, kuris naudoja G.711 kodeką balso kodavimui ir balso signalo energijos statistiką LSB bito slėpimo vietai nustatyti. Šio metodo rezultatas yra padidinta naudingoji talpa, kuri leidžia persiųsti iki 20 kbps bei siunčiamuose duomenyse atsiranda mažesnis balso kokybės nuvertėjimas (angl. *degradation*).

5 lentelė. Aprašytų LSB algoritmų savybių palyginimo lentelė

	Algoritmo pagerinimai		
	Neaptinkamumas	Patvarumas	Staganografinis pralaidumas
LSB	Žemas	Žemas	Aukštas
Tian	Aukštas	Žemas	Žemas
Miao ir Huang	Aukštas	Žemas	Vidutinis
Xu	Aukštas	Žemas	Aukštas

Wu ir Yang	Aukštas	Vidutinis	Aukštas

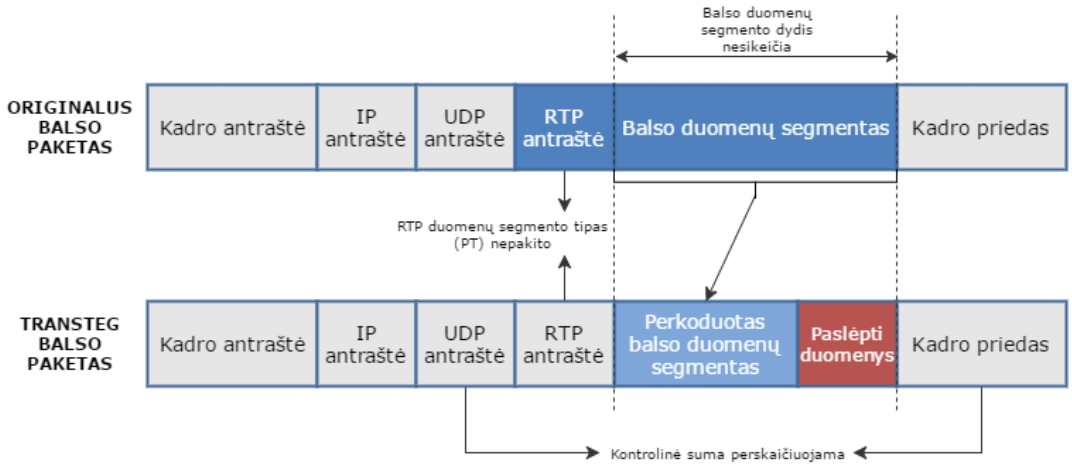
5 lentelėje yra apibendrinti aukščiau aprašyti LSB algoritmai. Visi įvertinimai yra aprašyti remiantis LSB algoritmu kaip pagrindu, t.y. jei nurodytas autoriaus algoritmas pagerinimo standartinę LSB algoritmo savybę, tai algoritmas yra įvertinamas **Aukštu** įvertinimo kriterijumi. Jei algoritmo savybė yra žemesnė nei standartinio LSB – algoritmas vertinamas **Žemu** įvertinimu. Kaip parodyta lentelėje visi aukščiau apibūdinti metodai yra esamo LSB algoritmo plėtiniai

1.3.2. Tiesioginės PDU modifikacijos laiko dedamojoje

Šiame skyriuje bus apžvelgti metodai, kurie remiasi PDU modifikacijomis tam tikrame laiko intervale.

1.3.2.1. Perkodavimo steganografijos metodas (TranSteg)

Daugelis prieš tai minėtų steganografijos algoritmų naudojamų VOIP protokole naudoja vienkartinę balso kodavimo funkciją. Tačiau TransSteg algoritmas remiasi tuo, kad daro daugiau nei vieną balso perkodavimą, tokiu būdu dirbtinai padidinama talpa paslėpti reikiamus duomenis (steganogramas) RTP protokolo duomenų segmentuose (9 pav.).



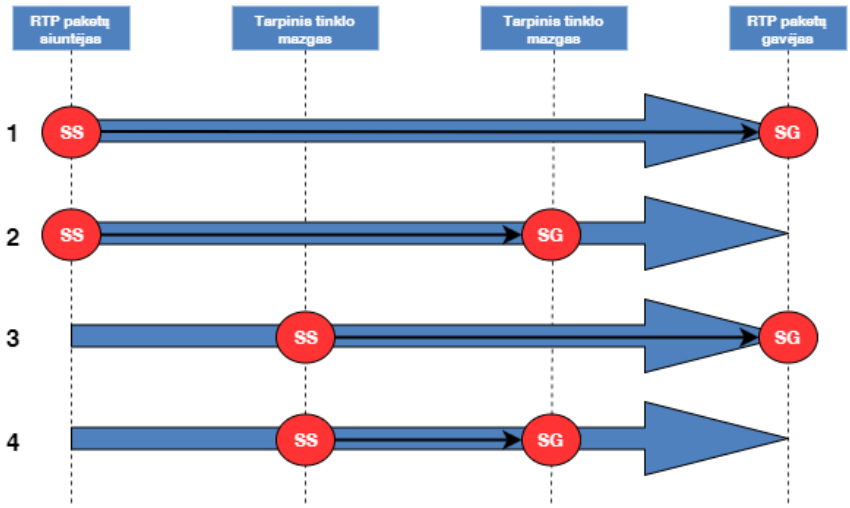
9 pav. Originalaus balso paketo palyginimas su TransSteg balso paketu

Šio metodo esmė yra panaudoti du kodekus: vieną atvirą visiems žinomą ir kitą slaptą. Kaip parodyta 9 pav. originalaus balso paketas yra užkoduotas vienu kodeku, pvz.: G.711. Tada kitas kodekas gali būti panaudotas sumažinti jau prieš tai užkoduoto balso duomenis. Tokiu būdu informacija yra sumažinama. Tam, kad duomenų atkūrimas būtų įmanomas, rekomenduojama naudoti abu balso kodekus, kurie geba atkurti visus suspaustus bitus.

Kaip teigia autoriai [25], TranSteg algoritmas gali būti integruotas keturiuose scenarijuose:

1. Pirmas scenarijus yra kai steganogramomis keičiasi du tinklo taškai be tarpinių tinklo mazgų įsikišimo.

2. Antras scenarijus - steganograma išsiunčiama RTP paketų siuntėjo mazge, tačiau steganograma nuskaitoma tarpiniame gavėjo tinklo mazge.
3. Trečias scenarijus – steganograma išsiunčiama iš siuntėjo tarpinio tinklo mazgo, tačiau steganograma atkuriame RTP paketų gavėjo mazge.
4. Ketvirtas scenarijus – steganograma išsiunčiama ir gaunama tarpiniuose tinklo mazguose, todėl RTP srauto gavėjas gali ir nežinoti, kad buvo perduodami duomenis jo kanalu.



10 pav. Slaptos komunikacijos scenarijai TranSteg algoritmui

10 pav. pavaizduoti perdavimo mazgai ir paslėptų kodekų buvimo vietos (raudonas apskritimas schemoje). Juodomis rodyklėmis yra nurodytos slaptos komunikacijos kryptys, tuo tarpu mėlynos rodyklės yra RTP srautas.

Pirmo scenarijaus privalumas yra lankstus panaudojimo būdas, kadangi SS mazgas (steganogramos siuntėjas) gali pasirinkti slaptą kodeką ir taip įtakoti siunčiamo srauto pralaidumą. Taip pat šis scenarijus turi mažiausią delsos laiką lyginant su kitais scenarijais, kadangi nenaudoja laiko balso srauto kodavimui. Šiame mazge išsiunčiamas srautas jau yra apdorotas abiems kodekais. Šiame scenarijuje reikia modifikuoti tik VOIP klientą, todėl yra lengvesnė jo realizacija. Įvertinus, kad komunikacijos kanalas turi būti apsaugotas, t. y. šifruotas SRTP protokolu, tai padaryti yra nesunku nes sesijos užmezgimo metu yra pasikeičiami kriptografiniai raktai ir toliau vyksta duomenų apsikeitimas tarp siuntėjo ir gavėjo.

Antrame scenarijuje norint įgyvendinti saugaus komunikacijos kanalo realizaciją, reikia perduoti kriptografinius raktus tarpiniam tinklo mazgui, todėl pirmas išsiųstas RTP paketas privalo būti nešifruotas ir vietoj steganogramos, likusioje vietoje (Transteg balso paketas „Slaptų duomenų“ bloke 9 pav.), perduoti kriptografinį raktą. Kadangi SS mazgas yra RTP paketų išsiuntimo pradžioje, tai įtakoja išsiunčiamo balso paketų pralaidumą, tačiau atsiranda papildomas delsos laikas gavėjo

mazge, nes reikia atkoduoti slaptu kodeku visą ateinantį RTP srautą bei perskaičiuoti kiekvieno atėjusio balso paketo CRC reikšmę, kad gavėjas neįtartų pakeitimo. Šio scenarijaus trūkumas yra viso RTP srauto stebėjimas SG mazge (steganogramos gavėjas). Kuriant šį sprendimą yra nustatyta pradinė sąlyga, kad tarpinis gavėjo mazgas SG galės stebėti visą RTP srautą, Jei ši sąlyga yra neįvykdyta, tai slapta komunikacija yra negalima.

Trečias scenarijus koduoja slaptu kodeku duomenis tarpiniame siuntėjo tinklo mazge, o steganograma yra gauname RTP srauto gavėjo mazge. Gavėjo mazgas SG yra atsakingas už slapto kodeko pasirinkimą abiejuose mazguose ir perdavimą SS mazgui signalizavimo protokolu (SIP ar kitu). SRTP prtokolo panaudojimas yra alternatyvus kaip ir antrame scenarijuje. Atsiradusi delsa tarp RTP srauto siuntėjo ir gavėjo yra vėlinama SS mazge.

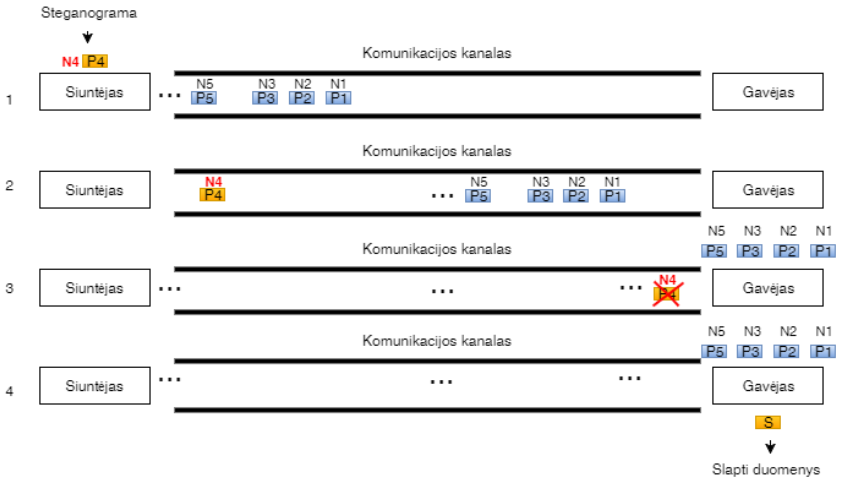
Ketvirtas scenarijus yra 2 ir 3 scenarijaus mišinys, kur nei RTP srauto siuntėjas, nei gavėjas valdo slapto kodeko pasirinkimą. Kadangi nei viena iš šių pusių (SS ir SG) nevaldo kodeko pasirinkimo, tai steganografinio srauto pralaidumas yra žemas, o delsos laikas yra didžiausias palyginus su kitais TranSteg scenarijais. Tačiau tuo pačiu yra sudėtingiau aptikti slaptą srautą tarp pokalbio dalyvių, kadangi nei vienas iš mazgų nėra slapto duomenų srauto iniciatorius.

1.3.3. Hibridinės PDU modifikacijos

Šiame skyriuje bus apžvelgti hibridinių PDU modifikacijų metodai.

1.3.3.1. LACK algoritmas

LACK (angl. *Lost Audio Packet Algorithm*) algoritmo esmė yra pavėlinti išsiunčiamus audio paketus tam, kad gavėjo programinė įranga nustatytų, kad siunčiami paketai yra perdėti (angl. *exccesive*). Tuo pačiu metu gavėjo programinė įranga nustačiusi šį požymį iškarto atmeta gautą paketą, neįvertinus, kad siunčiamas paketas yra reikalingas steganografijos technikai. Būtent tuo naudojasi aukščiau paminėtas algoritmas, kuris surenka atmestus paketus pagal atmetimo eilę ir rekostruoja persiunčiamą steganogramą. Principinė šio scenarijaus schema yra pavaizduota 11 pav.



11 pav. LACK algoritmo scenarijaus schema

Pirmas scenarijus nurodo, kad yra pasirenkamas vienas N-tasis paketas (N4) iš RTP srauto ir jo PDU duomenys (P4) yra pakeičiami steganograma. Antrame scenarijuje pasirinktas paketas yra užvėlinamas tam tikrą laiko intervalą ir tik tada yra išsiunčiamas komunikacijos kanalu. Trečias scenarijus parodo, kad pavėlintas N4 paketas pasiekia gavėją, kur gavėjo programinė įranga atmeta gautą pavėluotą paketą. Tačiau 4 scenarijus nurodo, kad gautas pavėlintas paketas nėra ištrinamas, o apdorojamas steganogramos gavimo mechanizmu ir ištraukima slapta žinutė S. Šio algoritmo autoriai nori pabrėžti, kad šis algoritmas yra taikymo OSI lygmenyje, todėl RTP paketų modifikacijas yra lengviau atlikti nei UDP ar IP protokoluose.

Kadangi yra naudojamas paketų vėlinimas reikia nustatyti, kokios yra maksimalios paketų praradimo ribos tam tikruose garso kodekuose, kadangi to neįvertinus nukenčia balso kokybė. Pagal Na ir Yoo [26], maksimalus praradimo tolerancijos lygis G.723.1 protokole yra 1%, G.729A protokole – 2% ar G.711 – 3%. Jei yra panaudojamas kartu su LACK, anksčiau aprašytas PLC metodas, tai paketų praradimų lygis gali didėti, pvz.: G.711 kodeko atveju iki 5%. Kodėl yra svarbus šis parametras – remiantis juo yra nustatoma maksimali duomenų perdavimo apkrova: G.711 kodekas geba perduoti iki 64 kb/s ir pasirinktas duomenų paketo sudarymo langas yra lygus 20 ms, tai panaudojus LACK metodą su 0.5% paketų praradimo tikimybe gauname, kad paslėptos komunikacijos perduodamų duomenų kiekis lygus 320 b/s.

Tam, kad užvėlinti paketai gavėjo programinėje būtų atpažinti kaip prarasti, reikia nustatyti tinkamą drebėjimo lygį (angl. *jitter*). LACK vėlinimo laikas privalo būti didesnis nei gavėjo anti-drebėjimo buferis. LACK vartotojai turi apsikeiti drebėjimo buferio reikšmėmis, tam kad LACK metodas veiktų sėkmingai.

LACK metodas yra naujas hibridinis algoritmas, kuris yra atsparus statistinėms stegoanalizėms, tačiau dėl sudėtingo slaptų paketų paskirstymo algoritmo jo steganografinis pralaidumas yra mažesnis nei tiesioginių PDU modifikacijų metodų kokių kaip LSB, tačiau aukštesnis nei PDU modifikacijų laiko dedamojoje.

1.4. Analizės išvados

Apžvelgus visas nagrinėtas VOIP steganografijos algoritmų grupes gauname tokias išvadas:

1. Kiekvieną steganografinį metodą galima įvertinti trimis charakteristikomis: steganografinis pralaidumas, nepastebimumas ir patvarumas. Remiantis šiomis charakteristikomis ir derinant jas tarpusavyje turi būti kuriami VOIP steganografijos metodai. Idealus variantas būtų, jei metodas būtų patvarus modifikacijoms ir sunkiai aptinkamas, tuo pačiu išlaikant didelį pralaidumą. Tačiau praktikoje yra parodoma, kad tenka balansuoti tarp šių charakteristikų, taip gaunant geriausią sprendimą esamai situacijai pagerinti.

2. Norint įvertinti steganografinio metodo taikymo kainą, reikia įvertinti informacijos nešlio tikslumą, t. y. apskaičiuoti, kiek duomenų yra prarandama ir iškaraipoma persiunčiant balso failą IP protokolu bei panaudojus balso kodeką balsui suspausti. Visa tai yra tiesiogiai susiję su slaptų duomenų neaptinkamumu balse. Šiai charakteristikai apskaičiuoti yra naudojami empiriniai statistiniai metodai: MSE ir PSNR. Taigi taikymo kaina gali būti išreikšta balso kokybės sumažėjimu panaudojus steganografinį metodą.
3. Steganografijos taikymas yra galimas 4 scenarijuose (10 pav.) Tarp aparašytų scenarijų Transteg metodas gali būti integruotas kiekviename iš 4 scenarijų, tuo tarpu LSB algoritmas gali būti panaudotas tik 1 scenarijuje, kadangi kituose scenarijuose bus prarandamas LSB steganografijai būdingas pralaidumas (> 20 kbps). Tai įvyksta dėl duomenų perkodavimo tarpiniuose tinklo mazguose.
4. Didžiausias steganografinių duomenų pralaidumas yra būdingas PDU duomenų segmentų modifikacijų algoritmams, tokiems kaip LSB, skaitmeninio vadenženklio metodai ar kiti panašūs metodai. Tuo tarpu metodai keičiantys PDU laiko dedamojoje peduoda mažiau duomenų nei metodai keičiantys PDU duomenis, bet daugiau nei hibridiniai PDU modifikacijų metodai.
5. Apžvelgus literatūrą apie persiuntimo protokolo naudojimą VOIP tinkle, nustatyta, kad beveik visi steganografijos sprendimai naudoja RTP kartu su UDP protokolu. Nei vienas projekte nagrinėtas metodas nenaudoja TCP protokolo dėl jo pagrindinės savybės – atkurti prarastus paketus, kas yra netinkama realaus laiko komunikacijai. Kai TCP protokolas bando atkurti prarastą paketą, kiti paketai turi laukti, kol bus pakartotas prarastas paketas, kas sukelia laikinį balso trikdį ir duomenų perdavimas sustoja. Šis sustojimas įtakoja ne tik balso, bet ir teikiamos paslaugos kokybę.
6. Remiantis LSB algoritmų analize, nustatyta, kad LSB yra labiausiai neapsaugotas algoritmas nuo duomenų pakeitimų VOIP tinkle.

Todėl remiantis šiais pastebėjimais buvo suformuotas darbo tikslas:

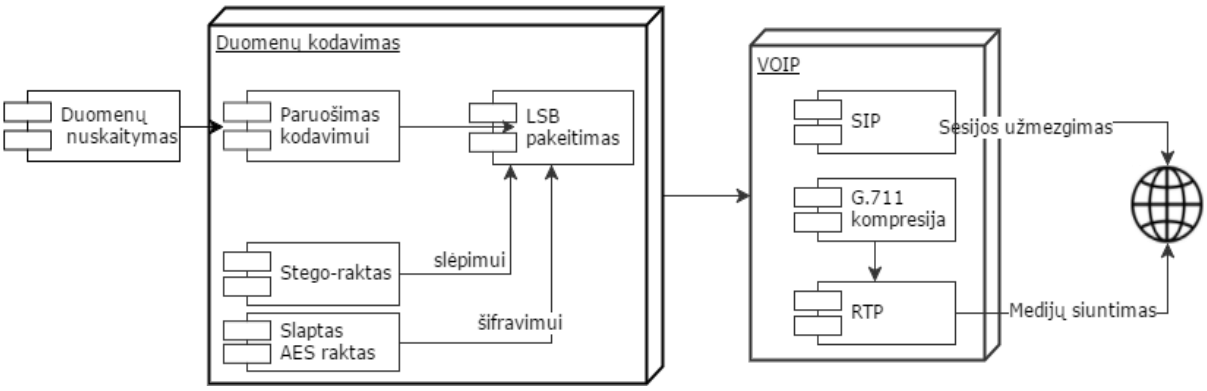
sukurti išplėstą LSB steganografinį algoritmą atsparų apsaugotų duomenų pakeitimams VOIP tinkle.

Tikslui pasiekti yra naudojami šie uždaviniai:

- atlikti literatūros analizę tiriamąjai sričiai apibūdinti;
- išanalizuoti esamus LSB sprendimus ir pritaikyti jų charakteristikas algoritmo kūrime;
- pritaikyti algoritmą realaus laiko duomenų siuntimui VOIP tinkle;
- keistis duomenimis saugiu komunikacijos kanalu;
- atlikti sukurto sprendimo eksperimentą ir rezultatų analizę.

2. SISTEMOS REALIZACIJA

Šiame skyriuje aprašytas algoritmo realizacijos etapas bei VOIP sistemos diegimas bei projektavimas. Visas darbo modelis sudarytas iš dviejų dalių: pirmoje dalyje vyksta steganogramos slėpimas audio sraute ar slaptų duomenų išgavimas; antroje dalyje yra projektuojamas algoritmo pritaikymas VOIP tinkle panaudojus trečiųjų šalių įrankius.



12 pav. Projektuojamos sistemos komponentai

2.1. Patobulinto LSB algoritmo realizacija

Projektuojant LSB algoritmą buvo remiamasi analizės rezultatais, kurie parodė, kad LSB trūkumas yra duomenų nepatvarumas; kai yra randamas požymis, kad čia yra paslėpta slapta žinutė, surinkus visus bitus į baitų masyvą galima perskaityti slaptą pranešimą.Todėl kuriant esamą sprendimą buvo atsižvelgta į šį požymį. Kitas ne mažiau svarbus algoritmo aspektas, kuris susijęs su duomenų patvarumu yra duomenų praradimas neidealioje tinklo aplinkoje. Persiunčiant duomenis IP protokolu neišvengiamai tenka susidurti su begale tinklo įrenginių, kurie įtakoja UDP paketų praradimą, jei nėra užtikrintas QoS. Todėl kuriamas alogritmas turi aukštą toleranciją dėl prarastų paketų ar atsiradusio triukšmo audioįraše.

Algoritmas buvo kūriamas remiantis Satisho ir Avinasho [27] idėja, kad siunčiamą steganogramą reikia perkurti ir tik tada slėpti LSB bituose. Satishas savo sprendime naudoja 21 baito piramidę, kuri šiuo atveju veikia kaip siunčiamų duomenų buferis. Tada pasirenka baitą iš buferio, kuris yra artimiausias slaptai žinutei. Ištraukiant iš gauto balso srauto slaptas žinutes yra naudojamas tas pats principas, kai visi gauti duomenys yra buferizuojami į 180 baitų langą ir jame yra ieškoma slaptos žinutės paketai.

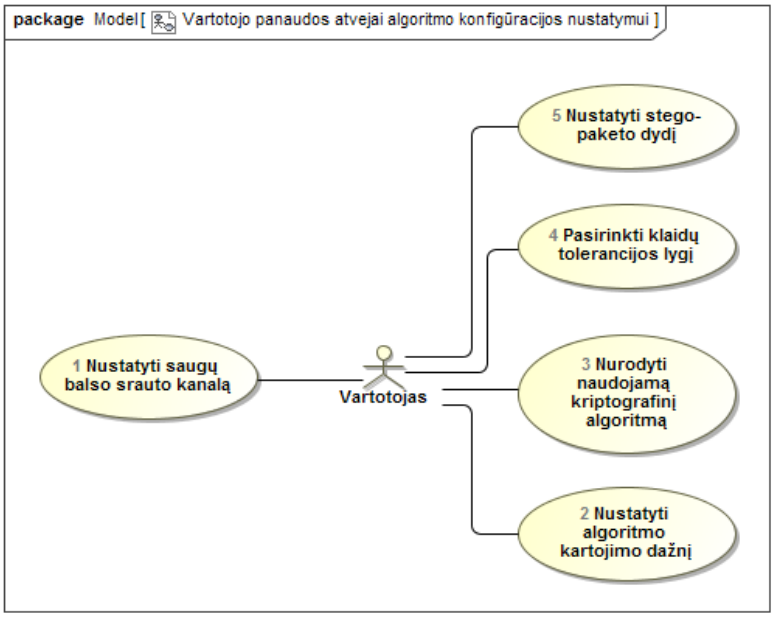
Kaip buvo paminėta buvo reikalingas sprendimas, kad siunčiant duomenis būtų išlaikyta žinutės eiliškumo tvarka (išlaikytas duomenų vientisumas). Tokiu būdu buvo sukurtas stego paketas, kuris plačiau bus aprašytas duomenų slėpimo algoritmo skiltyje

2.1.1. Patobulinto LSB algoritmo panaudos atvejai

Tam, kad kuriamas sprendimas būtų lankstus, vartotojams yra paliekamas pagrindinių algoritmo nustatymų konfigūracijos procesas. Priklausomai nuo nurodytų parametrų:

1. SRTP protokolo naudojimas,
2. Stego-paketo kartojimo dažnis balso sraute,
3. Kriptografinis metodas,
4. Stego paketų klaidų tolerancijos lygį,
5. Stego-paketo dydis,

yra didinamas arba mažinamas algoritmo saugumas, siunčiamos steganogramos talpa bei atkūrimo galimybė didesnio tinklo triukšmingumo atveju (13 pav.). Žemiau yra nurodytas kiekvieno iš panaudos atvejų detalus aprašymas.



13 pav. Vartotojo nustatomų parametrų panaudos atvejų diagrama

1. Komunikacijos kanalo apsauga. Priklausomai nuo VOIP telefono siunčiamas balso srautas yra šifruojamas arba paliekamas nešifruotu. Kuriamo projekto sprendime galima pasirinkti šį parametrą. Rekomenduojama jį palikti, kad apsaugoti siunčiamą turinį nuo pasiklausymo, pvz.: turint prieigą prie tarpinių tinklo įrenginių esančių tarp balso srauto siuntėjo ir gavėjo galima surinkti visus RTP paketus ir tokiu būdu atkurti siunčiamą balso pavyzdį. SRTP protokolas šifruoja ryšio kanalą, todėl jei programišius norėtų peržiūrėti siunčiamą srautą privalo turėti kriptografinį raktą paketams iššifruoti.

2. Stego-paketo kartojimų dažnis. Šis parametras yra tiesiogiai susijęs su duomenų slėpimu siuntėjo programinėje įrangoje. Kuo didesnis pasirinktas dažnis, tuo labiau užtikrintas steganogramos gavimas gavėjo programinėje įrangoje. Tačiau jei perduodamo balso srautas yra mažas palyginus su dideliu stego-paketų kartojimo dažnumu, tai perduodamos steganogramos talpa mažėja tiek kartų, kiek yra kartojamas tas pats paketas. Šioje vietoje reikia rasti balansą tarp perduodamų duomenų kiekio ir tinklo apkrovos, kuri galėtų būti UDP paketų numetimų priežastimi.
3. Kriptografijos metodo panaudojimas. Duomenų šifravimas nėra privalomas šio algoritmo tikslas, tačiau sumažinus klaidų skaičiui iki minimumo, kad duomenys bus garantuotai atkurti, galima ne tik paslėpti žinutė balso sraute, bet kartu apsaugoti žinutę nuo jos perskaitymo, jei žinutė bus atrasta stegoanalizės metodais.
4. Stego-paketų klaidų tolerancijos lygis. Šis parametras yra skirtas nufiltruoti netinkamus paketus, kurie atsiranda dėl balso signaluose atsiradusio triukšmo bei nustatyto 180 baitų duomenų apdorojimo buferio. Kuo šis parametras yra arčiau paketų kartojimo skaičiaus, tuo klaidų tolerancijos lygis yra mažesnis. Jei klaidų tolerancijos lygis yra lygus stego-paketų pasikartojimo dažniui reiškia gavėjo programinė įranga privalo gauti visus išsiųstus paketus.
5. Stego paketo dydis. Šis parametras skirtas aprašyti perduodamo stego paketo bitų kiekį. Kuo didesnis stego-paketas, tuo didesnis turi būti perduodamo balso srautas pernešti tą pačią informaciją. Plačiau apie stego-paketą yra aprašyta duomenų slėpimo algoritmo skyriuje.

2.1.2. Duomenų slėpimo algoritmas

Realizuojamas sprendimas yra sudarytas iš dviejų dalių:

1. Originalaus failo apdorojimas
2. Slaptos žinutės apdorojimas prieš įrašant į audio failą.

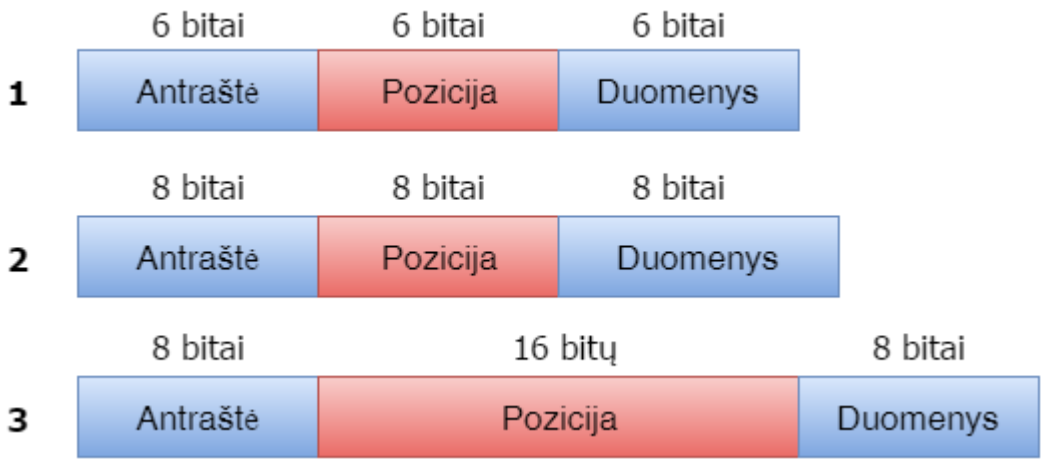
Pirmiausiai bus apibrėžtas, koks yra reikalingas audiofailo paruošimas prieš slaptos žinutės integraciją. Kaip buvo minėta anksčiau, projekto realizacijai yra naudojamas vieno kanalo WAV audiofailo formatas. Šis formatas pasižymi gera garso kokybe, nepraranda duomenų (angl. *lossless*) (iki 1%), tačiau šis formatas yra riboto dydžio. (2^{32}-1 baito). Kaip yra parodyta 14 pav., kai garso failas yra paverčiamas į baitų masyvą steganograma gali būti įrašoma nuo 44 garso srauto pozicijos. Tai yra todėl, kad pirmuose 44 baituose yra saugoma WAV failo antraštė, kurią pažeidus nei vienas garso įrašų skaitytuvas neleis perklausyti failo duomenų. Tada likusį failo srautą galima panaudoti slaptos žinutės integracijai.

Kaip parodyta schemoje (1 priedas), yra galimas slaptos žinutės šifravimas. Šiame bloke nėra apibrėžiamas naudojamas algoritmas, kadangi jis neįtakos galutinio rezultato, tačiau reikia atkreipti dėmesį, kad saugesnis algoritmas užims daugiau vietos. Realizacijoje bus panaudotas AES šifravimo algoritmas.

Sekantis žingsnis būtų sumažinti duomenų kiekį. Tam yra pasitelkta specialiųjų simbolių lentelė. Jeigu prieš šį žingsnį yra panaudotas šifravimo algoritmas, tada pasitelkiama išplėsta lentelė su pakeistų simbolių reikšmėmis, tuo pačiu padidinant siunčiamo stego-paketo dydį 8 bitais. Jei žinutėje nėra panaudotas kriptografinis algoritmas, tada siunčiamo stego-paketo dydis padidėja tik 6 bitais.

Pagrindinis algoritmo žingsnis yra stego-paketo sudarymas. Stego-paketas yra sudarytas iš trijų dalių:

1. Antraštė: saugomas unikalus šablono kodas,
2. Pozicija: saugoma kiekvieno baito pozicija slaptoje žinutėje,
3. Duomenų: slaptos žinutės simbolis.



14 pav. Stego-paketų sudarymo scenarijai

Pirmasis scenarijus yra numatytasis (angl. *default*) steganografinio algoritmo paketas. Panaudojus šį paketą galima perduoti 62 unikalius paketus slaptos žinutėms pozicijos nurodyti. Paketų skaičius priklauso nuo pozicijos dydžio, t. y. jei 1 atveju pozicijos dydis lygus 6 bitams, tai pavertus į skaitinę vertę gauname 2^6-2 reikšmių. Reikšmių kiekis yra lygus 62, o ne 63 dėl paketo antraštės šablono, kuris lygus *0xFE* (šešioliktaine išraiška).

Antras scenarijus yra numatytasis steganografinis paketas, jei yra naudojama kriptografija užšifruoti slaptą žinutę. Duomenų segmentas padidėja iki 8 bitų, nes reikalinga pilna ASCII simbolių lentelė atvaizduoti šifrogramą. Teoriškai, antras scenarijus yra efektyvesnis dėl didesnio paketų skaičiaus, tačiau visas paketas padidėja dar 6 bitais, kas mažina pralaidumą įrašant paketą į balso

srautą. Šis metodas yra praktiškiausias iš visų trijų scenarijų dėl baitų skaičiaus kartotinio (perduodamas kiekis lygus 3 baitams), kas leidžia atlikti greitesnį slaptos žinutės išgavimą.

Trečias scenarijus yra skirtas padidinti siunčiamų žinučių kiekį. Kadangi pozicija lygi 2 baitams, tai maksimaliai leidžia supakuoti apie 60 kB duomenų. Antraštei ir duomenims perduoti yra skirta po 8 bitus. Jei būtų panaudotas šifravimas ir šiam scenarijui, analogiškai kaip ir antram scenarijui, antraštės ir duomenų dydis išlieka tas pats.

Tada suformavus visus paketus, jie yra pakartojami pagal nustatytą kartojimo dažnį.

Paskutinis žingsnis prieš integruojant suformuotus paketus į balso srautą yra jų atsitiktinis surikiavimas. Kadangi perduodami duomenys yra atsparūs duomenų vietų sukeitimui, šis veiksmas trukdo programišiams atlikti stegoanalizę ir taip išgauti steganogramą. Tai vyksta todėl, kad dauguma kitų apibūdintų algoritmų duomenis dėlioja linijiniu principu, kas padidina talpą, bet sumažina atsparumą atsiradusiam triukšmui. Kai yra įrašomas pirmas stego-paketas, sekantis paketas turi būti pastumiamas per *X* baitų ir tada veiksmas yra kartojamas, kol nelieka neįrašytų paketų.

2.1.3. Duomenų atkūrimo algoritmas

Duomenų atkūrimas vyksta tokiu scenarijumi (2 priedas):

1. Gautas balso srautas yra pastumiamas per 44 baitus, tam kad nesugadinti audio formato antraštės.
2. Tada užpildomas 180 baitų buferis balso srauto duomenimis saugoti.
3. Duomenų buferyje yra ieškomas stego-paketo antraštės šablonas.
4. Kai buferyje yra randamas stego paketo šablonas yra nuskaitomas visas stego-paketas ir išsaugomas sąraše.
5. Jeigu buferyje dar yra neapdorotų duomenų, tai ieškomas sekantis stego-paketas pagal tą patį paieškos šabloną (angl. *pattern*).
6. Kai yra nuskaitomas visas balso srautas, paskaičiuojama visų paketų histograma, kuri parodo, koks yra kiekvieno paketo dažnumas. Lyginimo parametrai yra stego-paketo pozicija ir duomenys.
7. Iš sudarytos histogramos yra išrenkami tik tie unikalūs paketai, kurių kiekis yra artimas išsiųstų paketų kiekiui, t. y. jei pasirinktas paketų kartojimų dažnis (T_n) 10, tai kuo paketų kiekis (P_n) yra artimesnis šiam parametrui ($P_n \leq T_n$), tuo didesnė tikimybė, kad surastas paketas yra siunčiamos slaptos žinutės bitai. P_n – dar kitaip vadinamas klaidų tolerancijos lygis. Kuo šis parametras yra didesnis, tuo mažiau klaidingų paketų turi perduoti VOIP tinklas sėkmingam žinutės dekodavimui.
8. Gavus visus paketus yra vykdomas paketų duomenų sujungimas į steganogramą pagal simbolių žemėlapį (angl. *char mapping*).

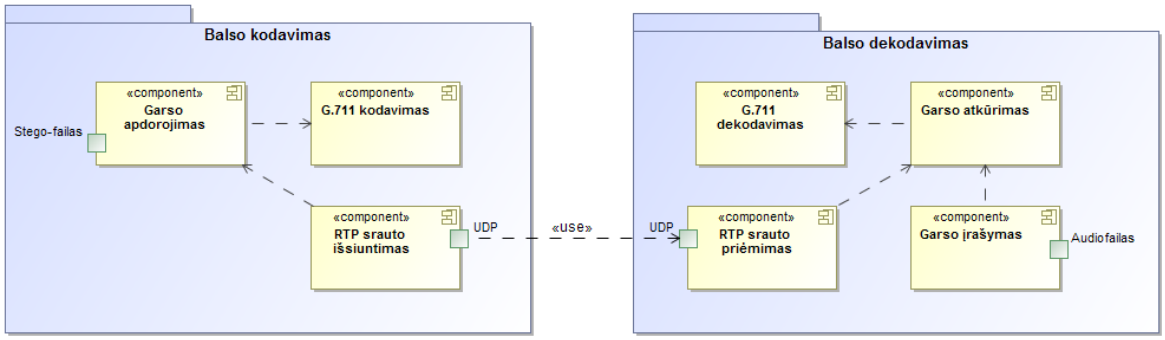
9. Jei duomenys buvo šifruoti, jie yra iššifruojami vartotojo kriptografiniu raktu.

Tokiu būdu yra išgaunama slapta žinutė iš steganografinio balso srauto.

2.2. VOIP sistemos simuliacijos kūrimas

Buvo kuriama VOIP sistemos simuliacija panaudojant StreamCoders įmonės produkto bandomąja versiją – „MEDIA SUITE .NET 4“. Šis produktas yra multimedijų platforma, skirta valdyti garso ir vaizdo kodekus, bei duomenų siuntimo srautus RTP protokolu. Šis produktas buvo pasirinktas dėl lanksčios sąsajos valdyti balso kodekus ir juos persiųsti UDP transportavimo protokolu. Kituose alternatyviuose sprendimuose yra sudėtinga valdyti siunčiamus ir gautus duomenis panaudojus balso kodekus. Pavyzdžiui, Ozeki VOIP SDK yra tinkamesnis sukurti VOIP sistemą, tačiau dėl uždaro programinio paketo negalima įtakoti balso (garso) persiuntimo proceso.

Realizuota simuliacija neužmezga duomenų persiuntimo sesijos SIP kontrolės protokolu, bet ją užmezga vidiniu RTCP protokolu. Yra nustatyta sąlyga, kad sesija jau yra užmegzta ir simuliacija privalo tik užkoduoti failą balso kodeku ir jį persiųsti RTP(UDP) protokolu. Tuo tarpu gavėjo procesas privalo dekoduoti gautą balso signalą ir grąžinti suformuotą failą.



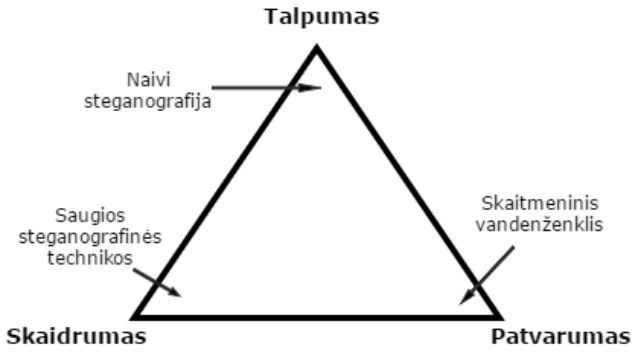
15 pav. Simuliacijos komponentų diagrama

Ryšio kanalas tarp dviejų vartotojų yra apsaugotas SRTP protokolu. Raktas, abiejose programos versijose, yra naudojamas tas pats. Simuliacijoje nėra realizuotas dvipusis bendravimo kanalas, t. y. duomenys yra siunčiami tik į vieną pusę. Pasirinktas šis komunikacijos būdas, nes jis pilnai užtikrina stego-failo perdavimo scenarijų. Papildomas funkcionalumas nekeičia slaptos komunikacijos scenarijaus, kadangi sukurtas sprendimas nėra skirtas perduoti slaptus duomenis į abi puses vienu metu.

Šių komponentų realizacija yra sukurta C# programavimo kalba.

2.3. Projektavimo ir realizacijos išvados

Šiame skyriuje buvo atliktas patobulinto LSB algoritmo projektavimas. Sudarinėjant algoritmą buvo vertinamas jo saugumas, tuo tarpu duomenų talpumas buvo apibrėžtas kaip mažiau svarbi charakteristika algoritme (15 pav.). Pagal algoritmo vertinimo trikampį buvo apibrėžtos trys sritys, kurių realizacija ir balansavimas padeda sukurti steganografinį algoritmą. Projektuojant buvo nupręsta didinti LSB algoritmo patvarumą, aukojant talpumą. Steganografiniam skaidrumui užtikrinti buvo panaudotas duomenų šifravimo algoritmas.



16 pav. Steganografinio algoritmo vertinimo trikampis

Atsižvelgiant į analizės rezultatus buvo suformuotas paketinis slepiamų duomenų modelis, kuris nepriklauso nuo siunčiamos pozicijos. Realizavus keletą skirtingų paketų tipų buvo pastebėta, kad didžiausią paketo segmentų dydį sudaro baito pozicijos aprašymas. Kuo jis didesnis, tuo daugiau duomenų gali pernešti balso įrašo failas.

Paketo antraštė buvo parinkta ištestavus keletos antraščių variantų. Buvo pastebėta tendencija, kad paketo antraštei parinkus minimalią ar maksimalią antraštės segmento dydžio reikšmę buvo gauta daugiau triukšmo paketų. Idealiausias variantas yra 2^N -2 nuo maksimaliai galimos antraštės reikšmės, kur N – bitų kiekis antraštėje.

VOIP sistemos simuliacija yra įgyvendinta supaprastinus pagrindinį VOIP architektūros bruožą, - užmezgant sesija tiesiogiai be kontrolės paketų įsikišimo. Tokiu būdu bus gautas maksimalus našumas, norint ištestuoti visus testinius variantus tyrimo dalyje.

3. KURIAMOS SISTEMOS SAUGUMO IR BALSO KOKYBĖS TYRIMAS

3.1. Tyrimo metodikos

Tyrimas yra pradėtas nuo patobulinto LSB algoritmo sukūrimo ir realizacijos. Kuriamo algoritmo prototipas yra realizuotas C# programavimo kalba, o statistinių koeficientų skaičiavimui yra panaudotas MATLAB R2016a programinis paketas.

Kuriamo sprendimo įvertinimui yra panaudoti 3 pagrindiniai metodai:

1. MOS rodiklis (angl. *mean opinion score*)
2. PSNR rodiklis (angl. *peak signal-to-noise ratio*)
3. MSE rodiklis (angl. *mean squared error*)

MSE rodiklis. Tai yra matmuo, kuris parodo kiek duomenys skiriasi nuo etaloninio signalo. Pagal termino apibrėžimą matosi, kad kuo mažesnis šis parametras, tuo signalas turi mažiau triukšmo. Tai yra labai svarbu slaptai komunikacijai, kad žmogaus garso atpažinimo sistema (angl. *human voice recognition* (HVR)) neišgirstų nenatūralų triukšmą signale. MSE yra apskaičiuojamas pagal formulę:

$$MSE(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - y_i)^2$$

Kur x_i,- yra originalaus signalo reikšmė, y_i, - modifikuoto signalo reikšmė.

PSNR rodiklis. Šis parametras skirtas apskaičiuoti lygį tarp maksimalios signalo galios reikšmės ir signalo triukšmo galios, iškreipiančios originalų signalą. Kadangi daugumas signalų turi platų dinaminį diapazoną, PSNR rodiklis yra išreiškiamas decibelais (dB) logaritminėje skalėje. Šis parametras plačiau naudojamas apskaičiuoti triukšmo lygį po signalo kompresijos. Testuojamoje aplinkoje, jei signalo reikšmės yra išreiškiamos 8 bitais, tai maksimali signalo reikšmė yra 255 [27] [28]. Tokiu būdu gauname, kad:

$$PSNR = 10\log_{10}\left(\frac{255}{MSE}\right)$$

MOS rodiklis [29]. Šis parametras pateikia skaitinę suvokiamo garso kokybės išraišką, gauto vykstant VOIP pokalbiui po kodekų kodavimo ir dekodavimo. MOS turi penkias reikšmes:

- 1 – gautas balso įrašas yra nesuvokiamas dėl triukšmo. Neįmanoma išgirsti balsą.
- 2 – gautas balso įrašas labai erzina klausą. Beveik neįmanoma išgirsti balso.
- 3 – gautas balso įrašas erzina, bet žmogaus kalbą galima suvokti.

- 4 – gautas balso įrašas yra geros kokybės. Šiek tiek triukšmo yra girdima, tačiau garsas yra aiškus.
- 5 – gautas balso įrašas yra idealus. Balsas yra aiškus lyg tiesioginio pokalbio metu tarp pašnekovų.

MOS yra apskaičiuojamas išvedant vidurkio reikšmę, kurią pateikia garso įrašą perklausę testo dalyviai. Pagal ITU standartus, turi būti sudarytos specialios sąlygos [30], kad aplinkinis triukšmas neįtakotų balso kokybės įvertinimo sprendimo, tačiau vertinant rezultatus buvo manoma, kad sąlygos yra kaip numatyta MOS specifikacijos dokumente.

Tyrimas vyks trimis etapais:

1. Pirmame etape bus ištestuotas sukurto algoritmo veikimas panaudojant komponentų testavimą (angl. *unit testing*) bei sukurtą grafinę sąsają. Gauti audiofailų rezultatai bus palyginti pagal 4 scenarijus: 18 bitų paketo ralizacija, 24 bitų paketo realizacija, 24 bitų paketo realizacija su AES šifravimu bei 32 bitų paketo realizacija. Visuose scenarijuose yra naudojamos fiksuoto dydžio slaptos žinutės: 14 baitų, 200 baitų ir 1024 baitai.
2. Antrame etape bus palyginti rezultatai tarp realizuoto algoritmo ir nemodifikuoto LSB algoritmo. Palyginimo kriterijai yra aukščiau įvardyti statistiniai modeliai: MSE, PSNR ir MOS.
3. Trečias etapas yra algoritmo realizacija VOIP tinkle. Tinklo realizacijai yra naudojama komercinė biblioteka (*StreamCoders „MediaSuite 4“*). Šiame etape taip pat buvo atliktas garso kokybės tyrimas panaudojus *G.711* balso kodeką bei slaptos žinutės atkūrimas po dekodavimo.

3.2. Patobulinto LSB algoritmo paketų tyrimas

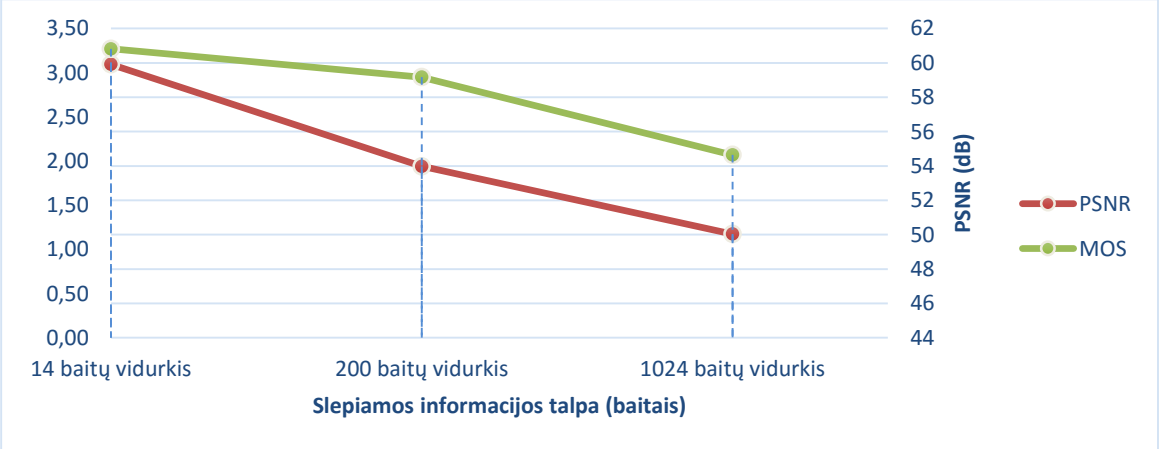
Pirmasis testas buvo sukurtas norint išsiaiškinti, ar egzistuoja tiesinė priklausomybė, tarp garso kokybės ir algoritmo modifikacijų. Šiame scenarijuje yra yra naudojamas tas pats audio failas (*thunder_clap.wav*), kur 1 scenarijaus atveju yra naudojamas 18 bitų paketas, 2 scenarijus – 24, scenarijus naudoja 24 bitų paketą kartu su AES 128 kriptografiniu algoritmu. Paskutinis scenarijus naudojs padidinto talpos paketą – 32 bitų paketą. Slapta žinutė buvo generuojama pasitelkiant internetinį atsitiktinio teksto generatorių – Lorem Ipsum. [31]

6 lentelė. Pirmo audiofailo rezultatai panaudojus skirtingas algoritmo modifikacijas

Garso įrašo pavadinimas	Failo dydis (baitais)	Slaptos žinutės dydis (baitais)	MSE	PSNR	MOS
Scenarijus 1 (test1.wav)	3 930 014	14	0,00022	60,6083	3,73
Scenarijus 1 (test1_1.wav)		200	-	-	-
Scenarijus 1 (test1_2.wav)		1024	-	-	-
Scenarijus 2 (test2.wav)		14	0,00025	59,9837	3,35
Scenarijus 2 (test2_1.wav)		200	0,00096	54,2112	2,8
Scenarijus 2 (test2_2.wav)		1024	-	-	-
Scenarijus 3 su AES (test3.wav)		14	0,00027	59,6942	2,9
Scenarijus 3 su AES (test3_1.wav)		200	0,00098	54,1251	3
Scenarijus 3 su AES (test3_1.wav)		1024	-	-	-
Scenarijus 4 (test4.wav)		14	0,00029	59,3583	3,1
Scenarijus 4 (test4_1.wav)		200	0,00111	53,5901	3,05
Scenarijus 4 (test4_2.wav)		1024	0,00252	50,0375	2,07

Gauto tokie rezultatai (6 lentelė):

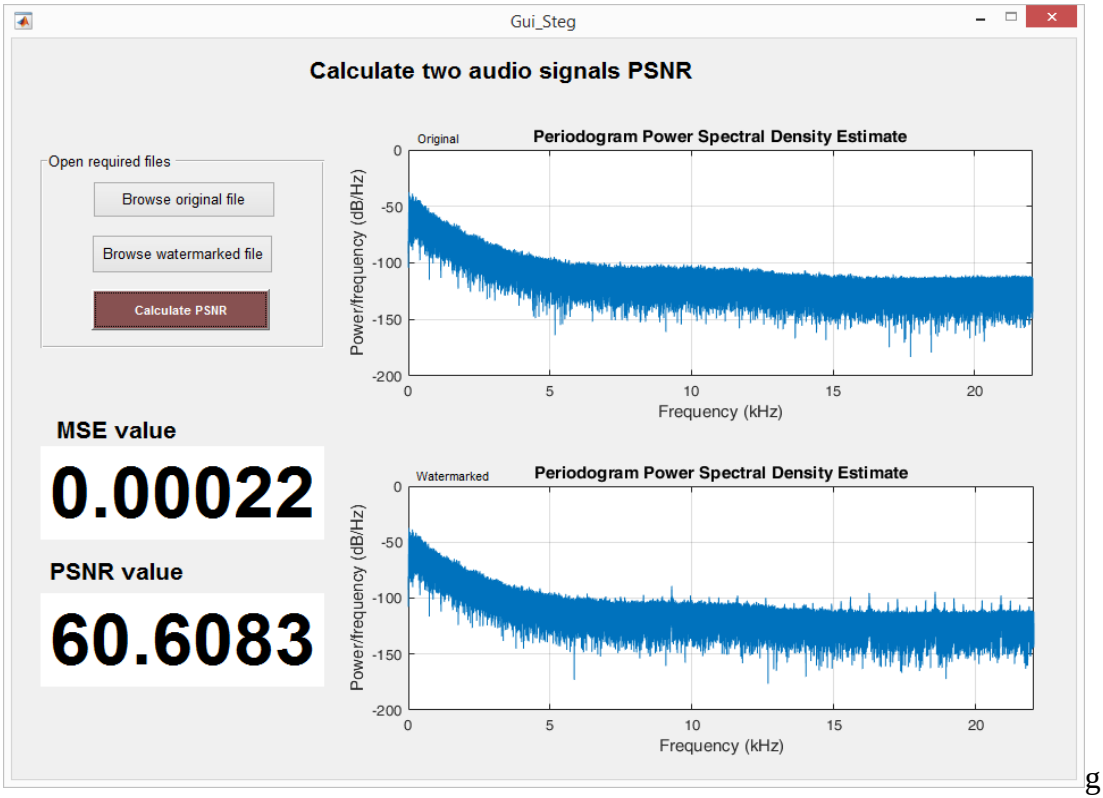
1. Kaip ir buvo testo pradžioje nuspėta, paketo pozicijos dydis įtakoja slepiamos informacijos kiekį. Jei parenkamas padidintos pozicijos paketą su 8 bitų duomenų segmentu, gauname, kad maksimaliai galima perduoti iki 65533 unikalių paketų pozicijų. Pirmo scenarijaus atveju maksimaliai galima perduoti tik 62 baitus duomenų.



17 pav. MOS reikšmės ir PSNR reikšmės priklausomybė nuo skirtingo dydžio slaptos žinutės

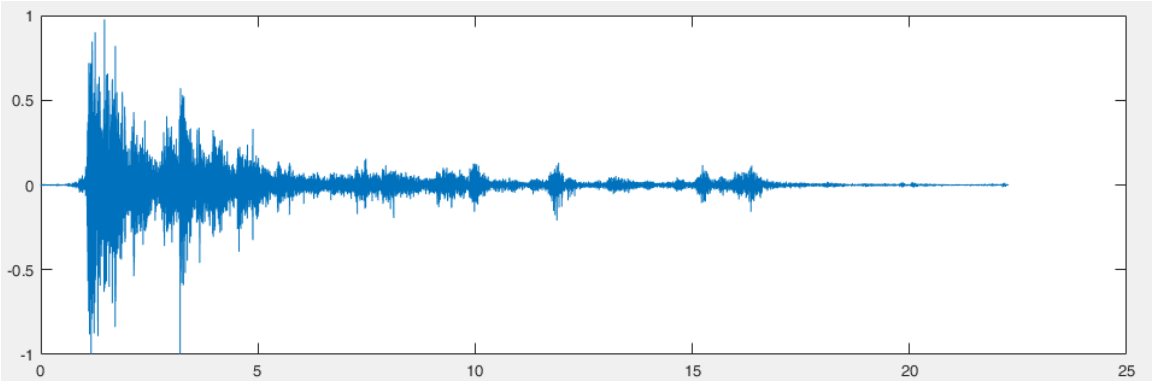
2. Jeigu slepiamos žinutės kiekis neviršyja neviršyja 200 baitų, balso kokybė prastėja lėčiau. Peržengus šią ribą yra girdimas nemalonus triukšmas, kuris trukdo klausyti balso arba balsas tampa silpniau girdimas nei triukšmas.

Apačioje apskaičiuotas spektrinis galios tankis tarp originalaus balso signalo (viršuje) ir pirmu scenarijumi paslėptų 14 baitų spektrinės galios tankio (apačioje).



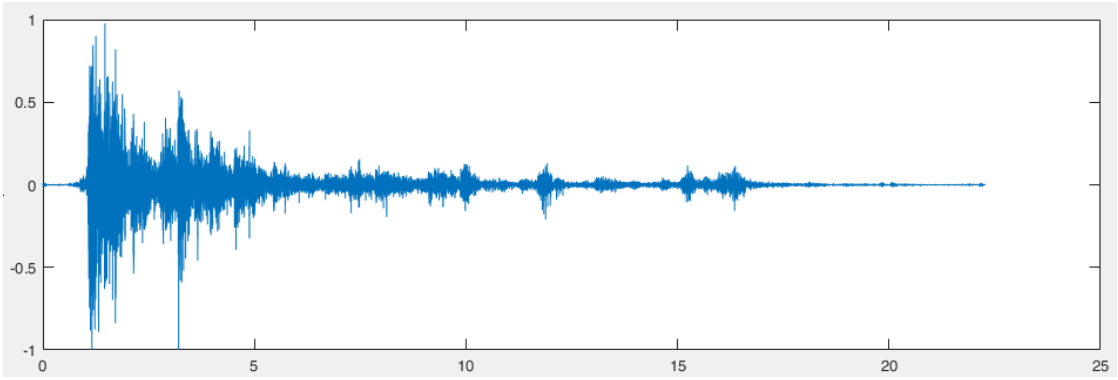
18 pav. Pirmo testavimo senarijaus spektrogramos palyginimas su originaliu signalu

Spektrinės galios tankio skaičiavimas leidžia grafiškai pamatyti pakeistas originalaus signalo vietas steganogramoje. Geriausiai tai matoma, kai lyginamos spektrogramos nuo 15 kHz dažnio. Pakeistame signale matomi ryškūs galios šuoliai, kurie leidžia daryti prielaidą, kad čia pakeisti duomenys. Tuo tarpu, jei lyginsime to pačio signalo amplitudes, tai gauname, kad jos skiriasi nežymiai:



19 pav. Originalaus failo amplitudinės moduliacijos spektrograma

X ašyje yra pavaizduotos sekundės, Y ašyje – signalo reikšmės.



20 pav. Stegofailo amplitudinės moduliacijos spektrograma panaudojus 1 scenarijaus algoritmą

Todėl atliekant audio failo stegoanalizę remtis erdvine (amplitudine) srities spektrogramos analize negalima, kadangi visa tai neteiks jokios informacijos. Tuo tarpu dažninė srities analizė parodė, kuriuose dažniuose gali būti slepiami duomenys.

3. Viršyjus maksimaliai galimą unikalaus paketų dydį duomenys tapo neatkuriami, todėl rezultatų lentelėje nėra apibrėžti.
4. Remiantis algoritmų palyginimo lentele, matoma, kad užšifravus duomenis AES algoritmu taip pat atsiranda daugiau triukšmo, kas įtakoja balso kokybę, todėl MOS reikšmės yra apie 3,0.

3.3. Patobulinto LSB algoritmo palyginimas su standartiniu LSB algoritmu

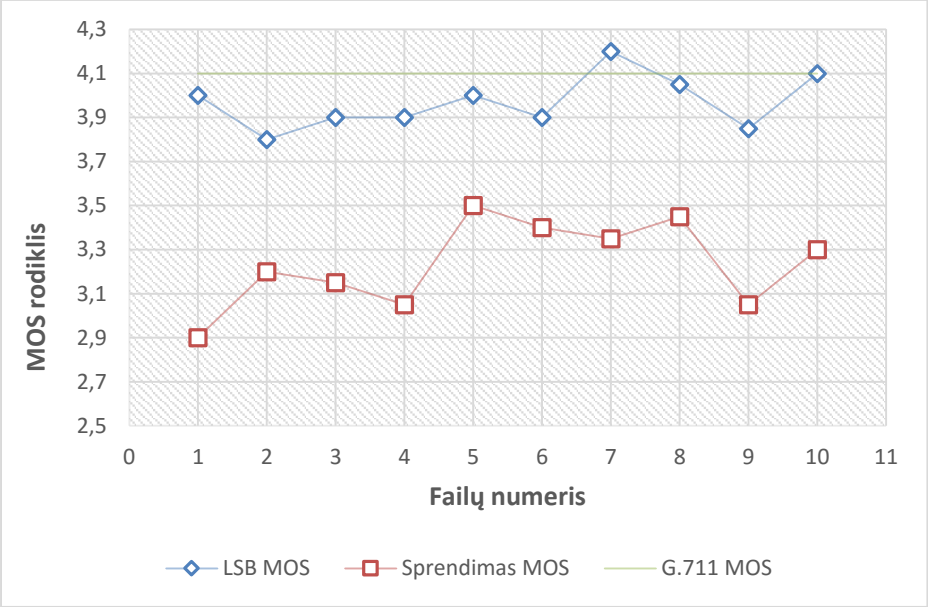
Šis tyrimas bus atliktas panaudojus 10 balso įrašų, kuriame jau yra sugeneruotas triukšmas. Balso pavyzdžiai buvo atrinkti iš NOIZEUS duomenų bazės [32]. Visi šioje duomenų bazėje esantys balso pavyzdžiai buvo surinkti TDT įranga, kurios mėginių ėmimo dažnumas yra 25kHz, tačiau vėliau mėginių ėmimo dažnumas buvo sumažintas iki 8kHz. Šiame tyrime buvo pasirinkti 5 vyriško balso failai ir 5 moteriško balso failai. Visuose failuose buvo slepiamas ta pati frazė: „**Juras Biliunas, IFN-4/3 gr.**“

Atlikus duomenų slėpimą buvo gauti šie rezultatai:

7 lentelė. LSB algoritmo palyginimas su realizuotu sprendimu

		1 failas	**2 failas**	**3 failas**	**4 failas**	**5 failas**	**6 failas**	**7 failas**	**8 failas**	**9 failas**	**10 failas**
LSB	**PSNR (dB)**	57,98	58,14	57,54	57,99	57,58	57,76	58,09	58,17	57,97	58,17
	MOS	4,00	3,80	3,90	3,90	4,00	3,90	4,20	4,05	3,85	4,10
Realizacija	**PSNR (dB)**	49,26	49,12	48,73	48,92	49,04	48,91	49,08	49,32	49,03	49,28
	MOS	2,90	3,20	3,15	3,05	3,50	3,40	3,35	3,45	3,05	3,30

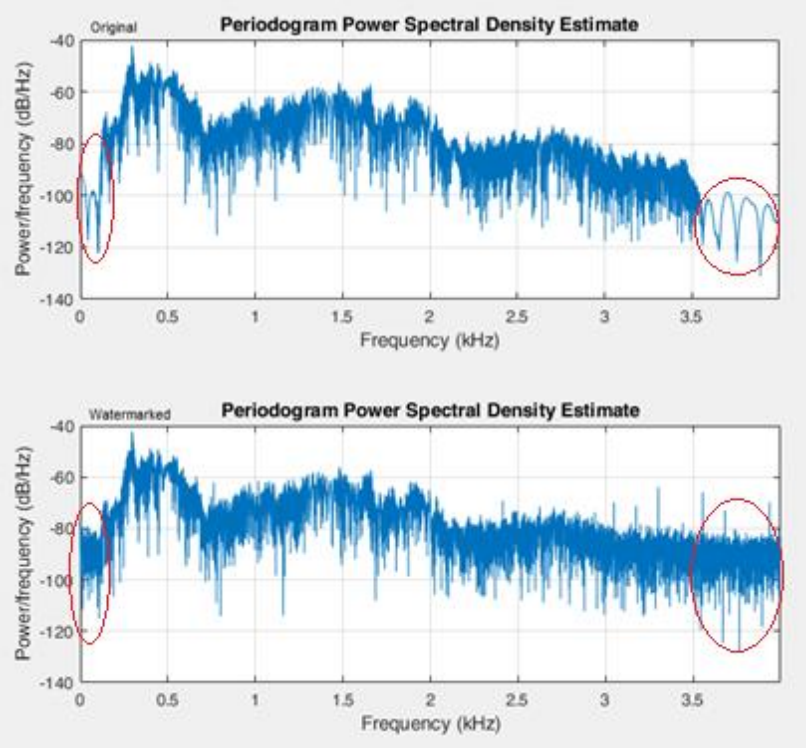
Pagal duomenis yra nustatyta, kad standartinio LSB algoritmo triukšmo lygio rodiklis PSNR varijuoja nuo 57 iki 58,5 dB. Tuo tarpu realizuoto sprendimo PSNR rodiklis varijuoja tarp 48 ir 50 dB. Pagal šiuos rodiklius galima teigti, kad realizuojamas sprendimas gauna apie 10 dB daugiau triukšmo siunčiamame signale. Visuose testuojamuose failuose buvo atkurtos paslėptos žinutės.



21 pav. LSB MOS rodiklių palyginimas su realizuotu sprendimu

Kaip teigė kiti šios srities tyrėjai [29] [28], egzistuoja tiesioginė priklausomybė tarp PSNR ir MOS reikšmės. Šiuo tyrimo etapu buvo patikrinta, kad mažesnį PSNR turintys audiofailai perneša daugiau triukšmo, kas įtakoja balso kokybei.

Palyginus 1 failo spektrinės galios tankį tarp LSB ir kuriamo sprendimo buvo gauti tokie rezultatai:



22 pav. LSB ir kuriamo sprendimo palyginimas spektriniame galios tankyje

Didžiausias audioįrašo pokytis atsiranda žemo dažnio srityse (nuo 0 Hz iki 0,2 kHz) ir aukštesnio dažnio srityse (daugiau nei 3,5 kHz). Ta pati tendencija galioja abiejuose garso įrašuose (21 ir 22 pav. sritys apibrėžtos raudona elipse)

3.4. Algoritmo įtaka garso kokybei VOIP tinkle

Balso persiuntimui buvo panaudoti audioįrašai, gauti antrame etape kaip rezultatų failai. Visi 10 balso signalų buvo perduodami į G.711 duomenų suspaudimo kodeką, o po to išsiųsti RTP protokolu į nutolusį kompiuterį. Abu kompiuteriai buvo sujungti tame pačiame tinklo potinklyje, todėl gausime žemiausią paketų praradimo lygį.

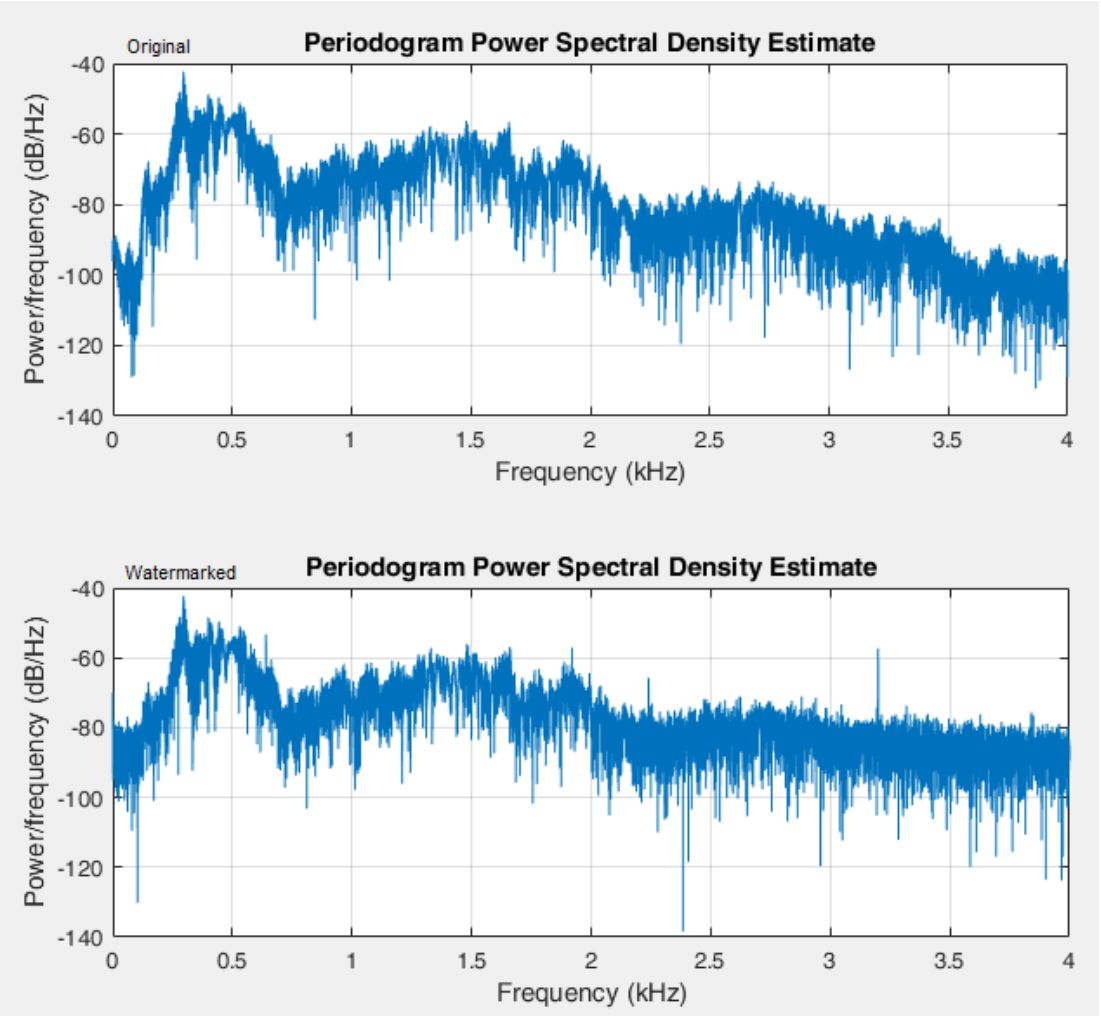
8 lentelė. LSB algoritmo palyginimas su realizuotu sprendimu persiuntus simuliuojamu VOIP tinklu

		1 failas	2 failas	3 failas	4 failas	5 failas	6 failas	7 failas	8 failas	9 failas	10 failas
LSB	PSNR (dB)	37,7325	36,3123	36,6509	36,071	36,4678	36,003	35,9599	36,0879	35,9359	36,1962
	MOS	3,95	3,8	3,9	4	3,85	3,9	4	3,85	3,8	4
	Pokytis	**-20,2452**	**-21,8301**	**-20,8853**	**-21,9143**	**-21,1091**	**-21,7547**	**-22,1261**	**-22,0786**	**-22,0369**	**-21,9718**
Realizacija	PSNR (dB)	37,7075	36,2088	36,6364	36,0652	36,4591	35,9955	35,9548	36,0829	35,9292	36,1923
	MOS	3,05	3,3	3,2	2,95	3,35	3,4	3,35	3,5	3	3
	Pokytis	**-11,5519**	**-12,9062**	**-12,0955**	**-12,8578**	**-12,581**	**-12,9118**	**-13,1236**	**-13,2405**	**-13,1009**	**-13,088**

Gauti tokie tyrimo rezultatai:

1. Abiejuose sprendimuose triukšmo lygis padidėjo (23 pav.) Persiuntus abu *sp01_lsb_stego.wav* (23 pav. viršutinė diagrama) ir *sp01_my_stego.wav* (23 pav.

apatinė diagrama) failus gauname, kad po kodeko panaudojimo jų spektrogramų galios tankis tapo panašus. Tai atsitinka dėl kodeko dekodavimo. Kai failas nėra apdorotas kodeku, tai nežymus jo skirtumas pakeitus LSB bitą nėra toks ryškus, tačiau dekodavimo matrica yra vienoda abiem failams, todėl ji išlygino rezultatus. Tai įrodo galios tankio spektrograma, kurioje matomi nežymūs skirtumai, kur palyginus su (22 pav.) nepersiųstais duomenimis. Skirtumai aukšo ir žemo dažnio juostoje yra skirtingi.



23 pav. Pirmo testuojamo failo galios tankio spektrogramos tarp persiųstų failų

2. Persiunčiant duomenis buvo nustatyti nežymūs duomenų praradimai (nuo 1 iki 200 baitų), kurie įtakojo PSNR lygį, tuo tarpu balso kokybė išliko panaši kaip ir prieš failo kompresiją.
3. Persiuntus stego-failus RTP protokolu nebuvo atkurta nei viena slapta žinutė. Galima įtarti, kad duomenų kompresija/dekompresija sunaikino ryšius tarp duomenų, todėl realizauotas sprendimas negalėjo atkurti nei vieno paketo. Standartinis LSB algoritmas negalėjo atkurti duomenų, nes pirmuose 5 baituose, kur yra saugomos žinutės ilgis ir slepiamo bito pozicija buvo nulinės reikšmės.

4. Palyginus stego-failą prieš siuntimą ir po jo gavimo nustatyta, kad standartinis LSB metodas praranda daugiau originalaus failo duomenų, kadangi PSNR rodiklis visuose failuose sumažėjo 20 dB. Tuo tarpu realizuotas algoritmas paranda kartus mažiau duomenų – PSNR rodiklis sumažėjo 10 dB.

4. IŠVADOS

Baigiamojo darbo tikslas yra sukurti išplėstą LSB steganografinį algoritmą atsparų apsaugotų duomenų pakeitimams VOIP tinkle. Buvo realizuotas išplėstas LSB algoritmas bei ištirtas jo panaudojimas VOIP tinkle. Sudarinėjant algoritmą buvo vertinamas jo saugumas. Pagal steganografinio algoritmo vertinimo trikampį buvo apibrėžtos trys sritys, kurių realizacija ir balansavimas padeda sukurti steganografinį algoritmą. Projektuojant buvo nupręsta didinti LSB algoritmo patvarumą, aukojant talpumą. Steganografiniam skaidrumui užtikrinti buvo panaudotas šifravimo algoritmas.

Projektuojant sistemą buvo panaudota UML modeliavimo kalba algoritmo veikimui apibūdinti, komponentų diagramai nubraižyti bei algoritmo panaudos atvejams pavaizduoti. Algoritmo realizacija atlikta C# programavimo kalba. Ištyrus stegoanalizės metodus palyginti standartinį LSB metodą su kuriama realizacija buvo nuspręsta panaudoti tris vertinimo kriterijus algoritmo tinkamumui nustatyti: PSNR rodiklis, MSE rodiklis ir MOS reikšmė.

1. Atlikus literatūros analizę išryškėjo tendencija, kad VOIP tinkluose TCP protokolas nėra naudojamas dėl praktinių apribojimų. Siunčiamos VOIP paslaugos kokybė nukenčia, jei TCP prtokolas bando atstatyti prarastus paketus. Todėl realizacijoje buvo simuliuojamas VOIP tinklo veikimas, kai duomenys persiunčiami UDP protokolu.
2. Išanalizavus LSB metodus nustatyta, kad dauguma LSB metodų duomenis įrašinėja linijiniu principu, t. y. visi slaptos žinutės bitai yra įrašinėjami iš eilės, ir bet kokia bito eilės manipuliacija iškraipo steganogramą. Panaudotas mechanizmas, leidžia realizacijoje siųsti duomenis atsitiktine pozicija, neprarandant steganogramos eiliškumo.
3. Ištęstavus ir palyginus rezultatus su standartiniu LSB algoritmu nustatyta, kad realizuotas algoritmas turi per daug perteklinių duomenų balso sraute (vietoj vieno išsaugoto baito, jis yra pakeičiamas 2-4 baitais). Sukurtas stego-paketo padidina siunčiamą informaciją nuo 2 iki 4 kartų, kas sumažina perduodamų duomenų steganografinį pralaidumą.
4. Dėl padidintos perteklinių (angl. *redundant*) bitų integracijos audioįraše atsiranda daugiau triukšmo, todėl balso kokybė nukenčia labiau nei standartiniame LSB algoritme. Realizuojant sprendimą buvo apskaičiuota, kad sukurtas metodas padidina balso įrašo triukšmingumą apie 10 dB.
5. Simuliuojant VOIP tinklo veikimą nustatyta, kad balso kodekai iškraipo, kadangi duomenų spaudimas vyksta naudojant statistinius modelius, kurių atkuriamų reikšmių paklaida svyruoja nuo 0,1 – 1% (G.711 atveju).

6. Buvo sukurta VOIP tinklo simuliacija ir nustatyta, kad balso kodekų panaudojimas sunaikina ryšius tarp duomenų todėl nepavyko atkurti nei vienos slaptos žinutė užkodavus juos ir standartiniu LSB algoritmu, ir realizuotu sprendimu.
7. Buvo patikrintas G.711 kodekų veikimas VOIP sistemoje. Atlikus tyrimą buvo nustatyta, kad įterpus steganogramą į balso failą ir persiuntus jį SRTP protokolu į nutolusį kompiuterį, balso kokybė pakito nežymiai. Tai parodė atliktas MOS rodiklio skaičiavimas.
8. Sukurtas algoritmas veikia lėtai, todėl realaus-laiko programoms yra netinkamas. Jei duomenų slėpimas vyksta iki 2 s, tai iš to pačio failo slapti duomenys yra rekonstruojami per 5-13 sekundžių.

Rekomenduojama nenaudoti šio algoritmo VOIP tinkluose, jei nėra įvertinta balso kodeko kompresijos/dekompresijos įtaka galutiniam rezultatui. Realizuotas algoritmas privalo būti naudojamas su kitais metodais, kurie padeda atkurti prarastus duomenis, arba slėpti duomenis aukštesniuose LSB bituose tam, kad po kompresijos būtų atkurti originalūs bitai.

Literatūros sąrašas

[1] G. Shrivastava, A. Pandey ir K. Sharma, „Steganography and Its Technique: Technical Overview,“ įtraukta *Proceedings of the Third International Conference on Trends in Information, Telecommunication, and Computing*, Kochi, India, Springer, 2012, pp. 615-620.

[2] J. Viega, M. Messier ir P. Chandra, Network Security with OpenSSL, O'Reilly Media, 2002.

[3] D. J. Barrett, R. E. Silverman ir R. G. Byrnes, SSH, The Secure Shell: The Definitive Guide, 2nd Edition, O'Reilly Media, 2005.

[4] M. H. Sharma, M. M. Arya ir M. D. Goyal, „Secure Image Hiding Algorithm using Cryptography and Steganography,“ *IOSR Journal of Computer Engineering (IOSR-JCE)*, t. 13, nr. 5, 2013.

[5] G. Sawant, K. Jadeja, K. Bhat ir P. J. Dalal, „The New Cryptography Algorithm with Dynamic Steganography,“ *International Research Journal of Computer Science (IRJCS)*, t. 2, nr. 2, pp. 10-17, 2015-02.

[6] B. Zaidan, A. Zaidan, A. Al-Frajat ir H. Jalab, „On the Differences between Hiding Information and Cryptography Techniques: An Overview,“ *Journal of Applied Sciences*, t. 10, nr. 15, pp. 1650-1655, 2010.

[7] H. Abelson ir G. J. Sussman, Structure and Interpretation of Computer Programs, Cambridge, Massachusetts; London, England: The MIT Press, 1999.

[8] E. Satir ir H. Isik, „A Huffman compression based text steganography method,“ *Multimedia Tools and Applications*, t. 70, nr. 3, pp. 2085-2110, 2014-06.

[9] W. Frączek, W. Mazurczyk ir K. Szczypiorski, „Stream Control Transmission Protocol Steganography,“ Warsaw, Poland , 2010-06.

[10] S. Kašėta ir T. Adomkus, „Telefonijos informacijos ir VoIP sauga,“ Kaunas, Vitae Litera, 2008, p. 101.

[11] W. Mazurczyk, „VoIP Steganography and Its Detection - A Survey,“ Warsaw University of Technology, Warsaw, Poland, 2012.

[12] W. Mazurczyk ir Z. Kotulski, „New VoIP Traffic Security Scheme with Digital Watermarking,“ Warsaw, 2006a.

[13] S. J. Murdoch ir S. Lewis, „Information Hiding,“ įtraukta *7th International Workshop, IH 2005*, Barselona, Spain, 2005.

[14] X. Wang, S. Chen ir S. Jajodia, „Tracking Anonymous Peer-to-Peer VoIP Calls on the Internet,“ įtraukta *ACM CCS'05*, Alexandra, Virginia, USA, 2005.

[15] D. Kundur ir K. Ahsan, „Practical Data Hiding in TCP/IP,“ įtraukta *ACM Workshop on Multimedia Security*, Juan-les-Pins, France, 2002.

[16] S. D. Servetto ir M. Vetterli, „Communication using phantoms: covert channels in the Internet,“ įtraukta *Information Theory, 2001. Proceedings. 2001 IEEE International Symposium on*, Washington, USA, 2001.

[17] W. Mazurczyk, „Lost Audio Packets Steganography: The First Practical Evaluation,“ Warsaw University of Technology, Institute of Telecommunications, Warsaw, Poland, 2008.

[18] N. Aoki, „A Packet Loss Concealment Technique for VoIP using Steganography,“ įtraukta *2003 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS 2003)*, Awaji Island, Japan, 2003.

[19] J. Dittmann, A. Mukherjee ir M. Steinebach, „Media-independent Watermarking Classification and the need for combining digital video and audio watermarking for media authentication,“ įtraukta *Proceedings of the International Conference on Information Technology*, Las Vegas, USA, 2000.

[20] N. Cvejic ir T. Seppänen, „Reduced distortion bit-modification for LSB audio steganography,“ *Signal Processing, 2004. Proceedings. ICSP '04. 2004 7th International Conference on,* t. 3, pp. 2318 - 2321, 2004.

[21] H. Tian, K. Zhou, H. Jiang, J. Liu, Y. Huang ir D. Feng, „An M-sequence based steganography model for voice over IP,“ *In Proc. of IEEE Int Conf Communications (ICC 2009),* pp. 1-5, 2009a.

[22] R. Miao ir Y. Huang, „An approach of covert communication based on the adaptive steganography scheme on Voice over IP,“ įtraukta *IEEE Int Conf Communications (ICC 2011),* Kyoto, Japan, 2011.

[23] E. Xu, B. Liu, L. Xu, Z. Wei, B. Zhao ir J. Su, „Adaptive VoIP Steganography for Information Hiding within Network Audio Streams,“ *Network-Based Information Systems (NBiS), 2011 14th International Conference on,* p. 612 – 617, 2011.

[24] Z. J. Wu, W. Yang ir Y. X. Yang, „ABS-based Speech Information Hiding Approach,“ *IEEE Electronics Letters,* t. 39, pp. 1617-1619, 2003.

[25] W. Mazurczyk, P. Szaga ir K. Szczypiorski, „Using Transcoding for Hidden Communication in IP Telephony,“ Warsaw University of Technology, Warsaw, Poland, 2011.

[26] S. Na ir S. Yoo, „Allowable Propagation Delay for VoIP Calls of Acceptable Quality,“ įtraukta *Advanced Internet Services and Applications*, Seoul, Korea, Springer Berlin Heidelberg, 2002, pp. 469-480.

[27] S. Bhalshankar ir A. K. Gulve, „Audio Steganography: LSB Technique Using a Pyramid Structure and Range of Bytes,“ *International Journal of Advanced Computer Research (IJACR),* t. 5, nr. 20, pp. 233-248, 2015.

[28] M. Zamani, A. B. A. Manaf, S. M. Abdullah ir S. S. Chaeikar, „Correlation between PSNR and Bit per Sample Rate in Audio Steganography,“ įtraukta *Proceedings of the 11th international conference on Telecommunications and Informatics, Proceedings of the 11th international conference on Signal Processing*, Stevens Point, Wisconsin, USA, 2012.

[29] ITU, „P.800 : Methods for subjective determination of transmission quality,“ International Telecommunication Union, 31 07 2006. [Tinkle]. Available: http://www.itu.int/rec/T-REC-P.800-199608-I/en. [Kreiptasi 05 05 2016].

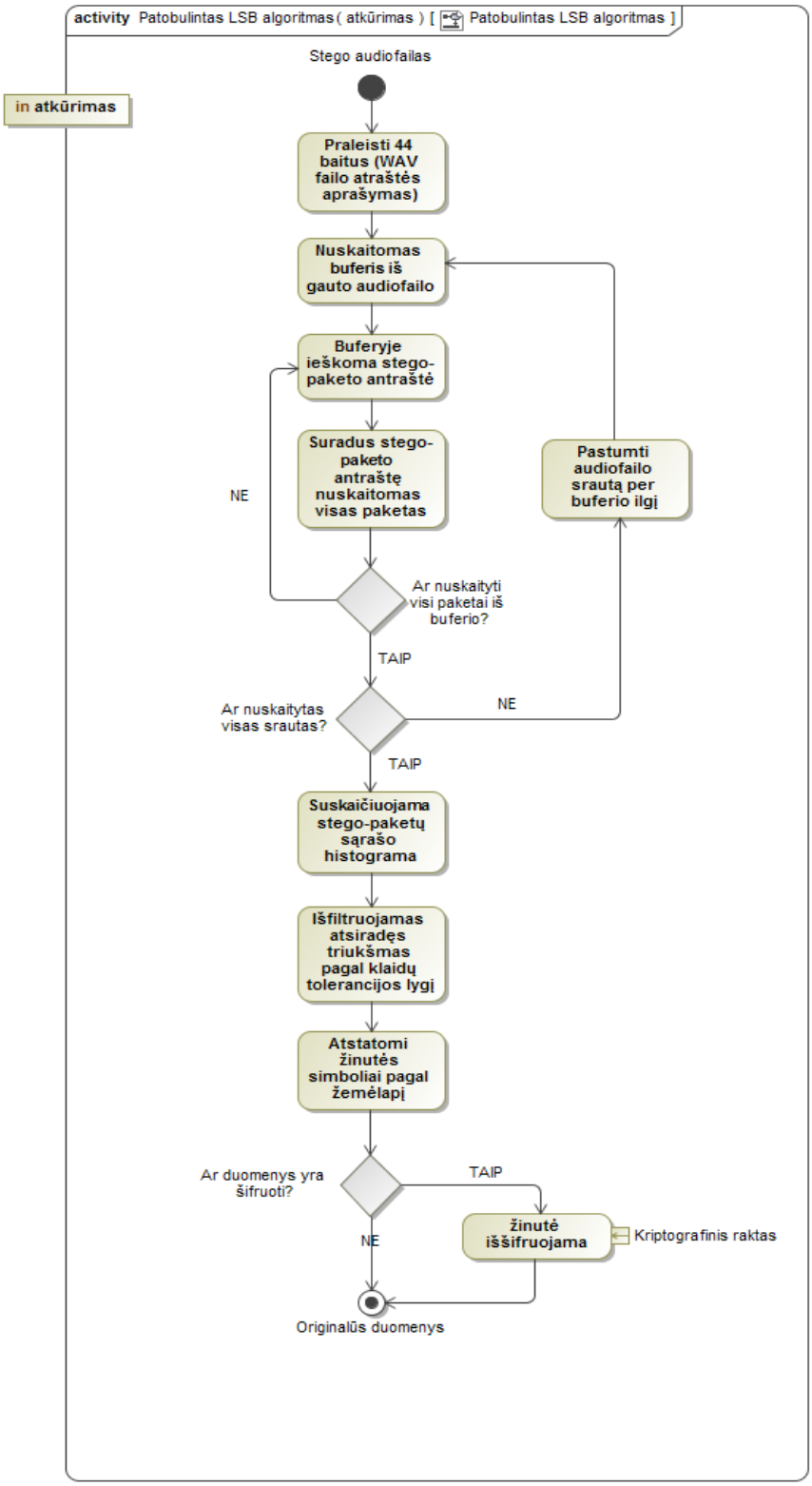
[30] ITU, „P.800.2 : Mean opinion score interpretation and reporting,“ International Telecommunication Union, 05 2013. [Tinkle]. Available: https://www.itu.int/rec/T-REC-P.800.2/. [Kreiptasi 06 05 2016].

[31] nežinoma, „Lorem Ipsum,“ [Tinkle]. Available: htttp://lt.lipsum.com. [Kreiptasi 12 05 2016].

[32] D. P. Loizou, „NOIZEUS: A noisy speech corpus for evaluation of speech enhancement algorithms,“ Erik Jonsson School of Engineering & Computer Science, 2007. [Tinkle]. Available: http://ecs.utdallas.edu/loizou/speech/noizeus/. [Kreiptasi 06 05 2016].

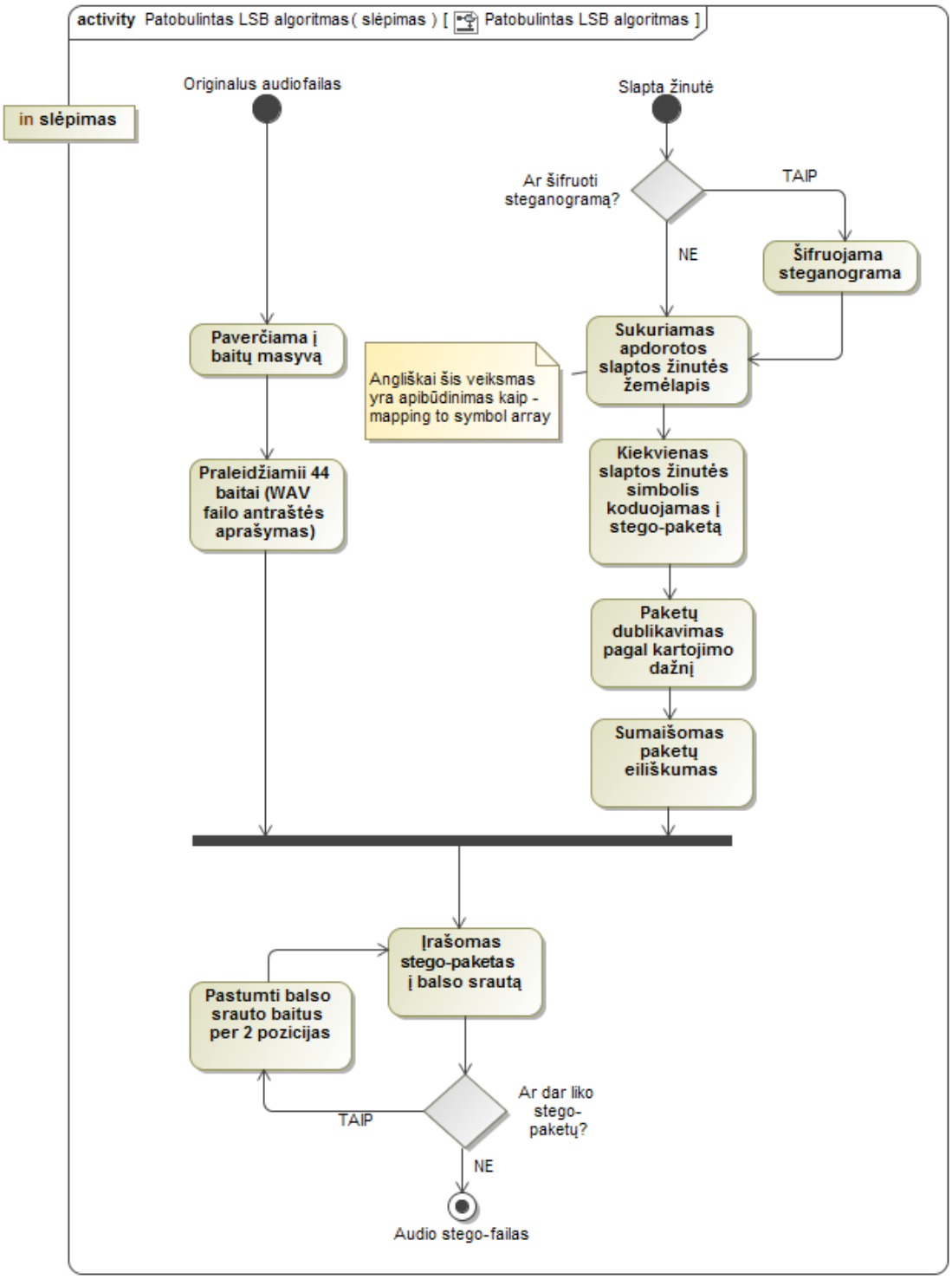
5. PRIEDAI

1 priedas. Duomenų atkūrimo algoritmas



24 pav. Patobulinto LSB algoritmo slaptos žinutė atkūrimo fazė

2 priedas. Duomenų slėpimo algoritmas



25 pav. Patobulinto LSB algoritmo slėpimo fazė